Lifestyle Store

Detailed Developer Report

INTRODUCTION :

- This is the vulnerability project and penetration testing (VAPT) report for “Lifestyle Store”.
- All vulnerabilities found on this store with their screenshots and links are reported.
- I have also provided business risks and expert recommendations to tackle those vulnerabilities.

SECURITY STATUS: Extremely Vulnerable

SQLi: Hackers can steal all records from the databases of the website. Hackers can take complete control of the website including view, edit, add or delete files and folders via shell upload.

IDOR: Hackers can extract mobile numbers of all customers using user-id. Hackers can change the source code and can upload any malicious code, phishing etc. in the website via shell upload.

XSS: Hackers can trick users to click on malicious pop up links and steal information via cross-site-scripting.

VULNERABILITY STATISTICS:

Critical	Severe	Moderate	Low
12	7	3	3

VULNERABILITIES FOUND:

S NO.	CONDITION	VULNERABILITY	COUNT
1.	CRITICAL	SQL INJECTION	2
2.	SEVERE	STORED AND REFLECTED XSS	3
3.	CRITICAL	IDOR	4
4.	SEVERE	RATE LIMITING FLAW	2
5.	CRITICAL	INSECURE FILE UPLOAD	2
6.	MODERATE	CLIENT SIDE FILTER BYPASS	2
7.	SEVERE	SERVER MISCONFIGURATION	2
8.	CRITICAL	PII LEAKAGE	4
9.	CRITICAL	OPEN REDIRECTION	4

1. SQL INJECTION

(CRITICAL)

Below mentioned URL is vulnerable to SQL injection attack.

Relevant URL:

- http://13.127.120.228/products.php?cat=1

Affected Parameters:

- category (GET)

Payload:

- cat=1’

Other similar URLs vulnerable to SQLi:

URL #1:

- http://13.127.120.228/products.php?cat=2

URL #2:

- http://13.127.120.228/products.php?cat=3

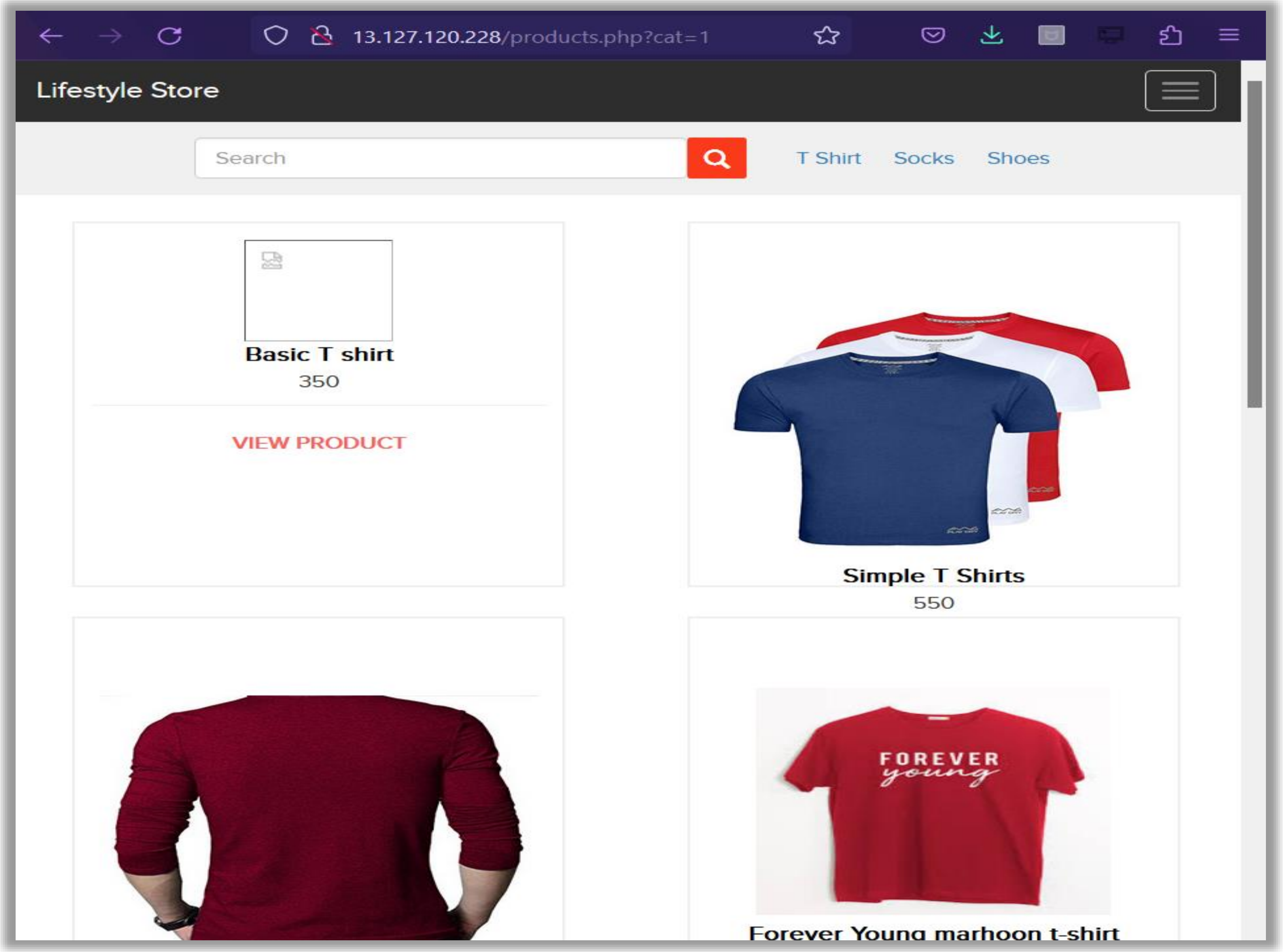
PAYLOAD:

- cat=1’

Observations:

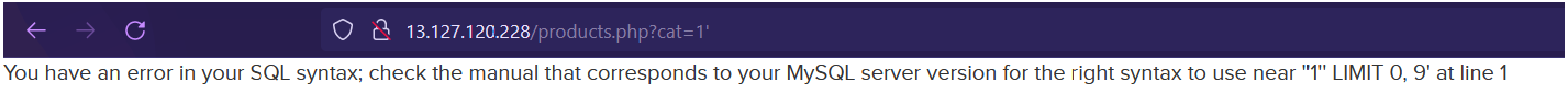
Following slides have details about the vulnerability observed.

- Go to the categories option from the homepage of the e-commerce website and click on “T-Shirt”, “Socks” or “Shoes” to get into the URL, you will see products as per the option you have chosen but notice the get parameter in the URL.



13.127.120.228/products.php?cat=1

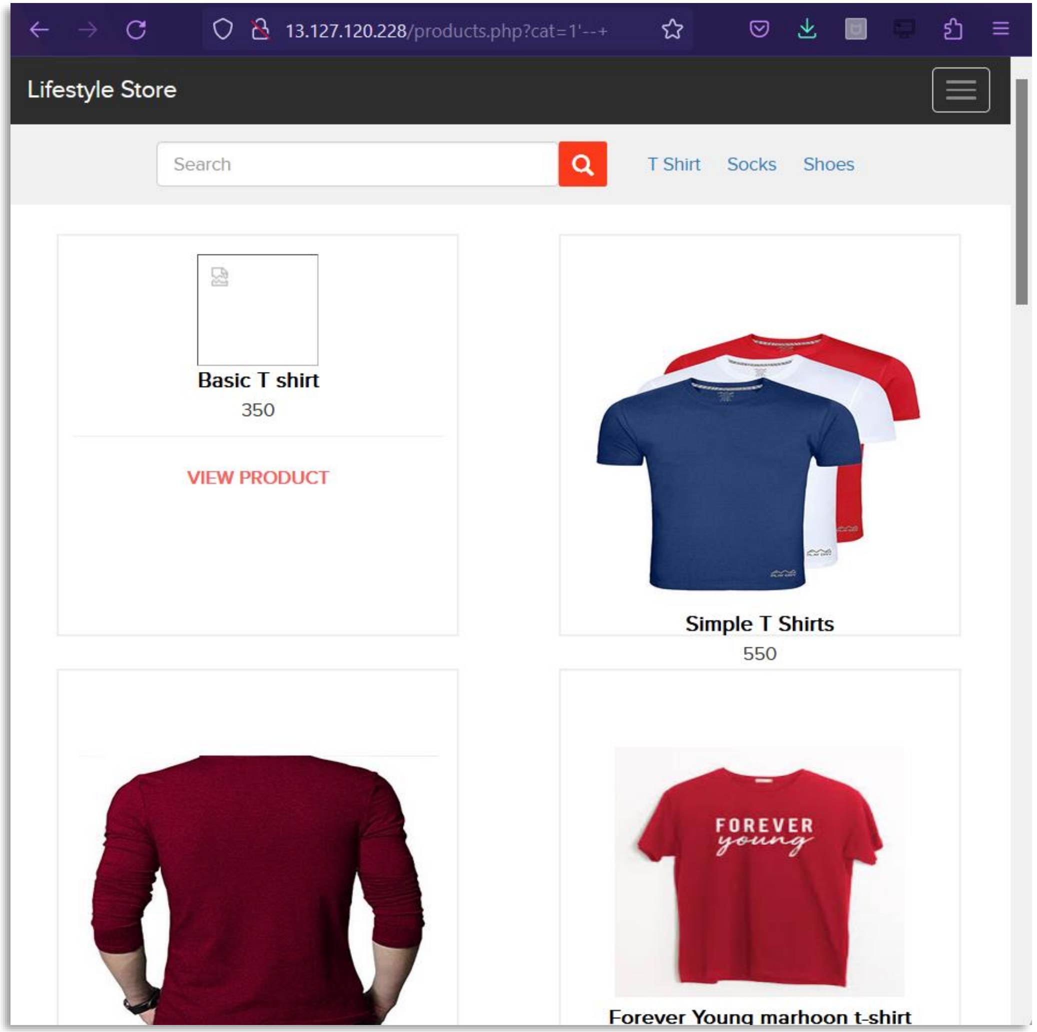
- When you add a single quote ‘ in the get parameter, you get a MySQL error.



```
13.127.120.228/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
```

- Recheck, you can put “--+” in the end of the parameter, and the page loads in its original format, this confirms the error.

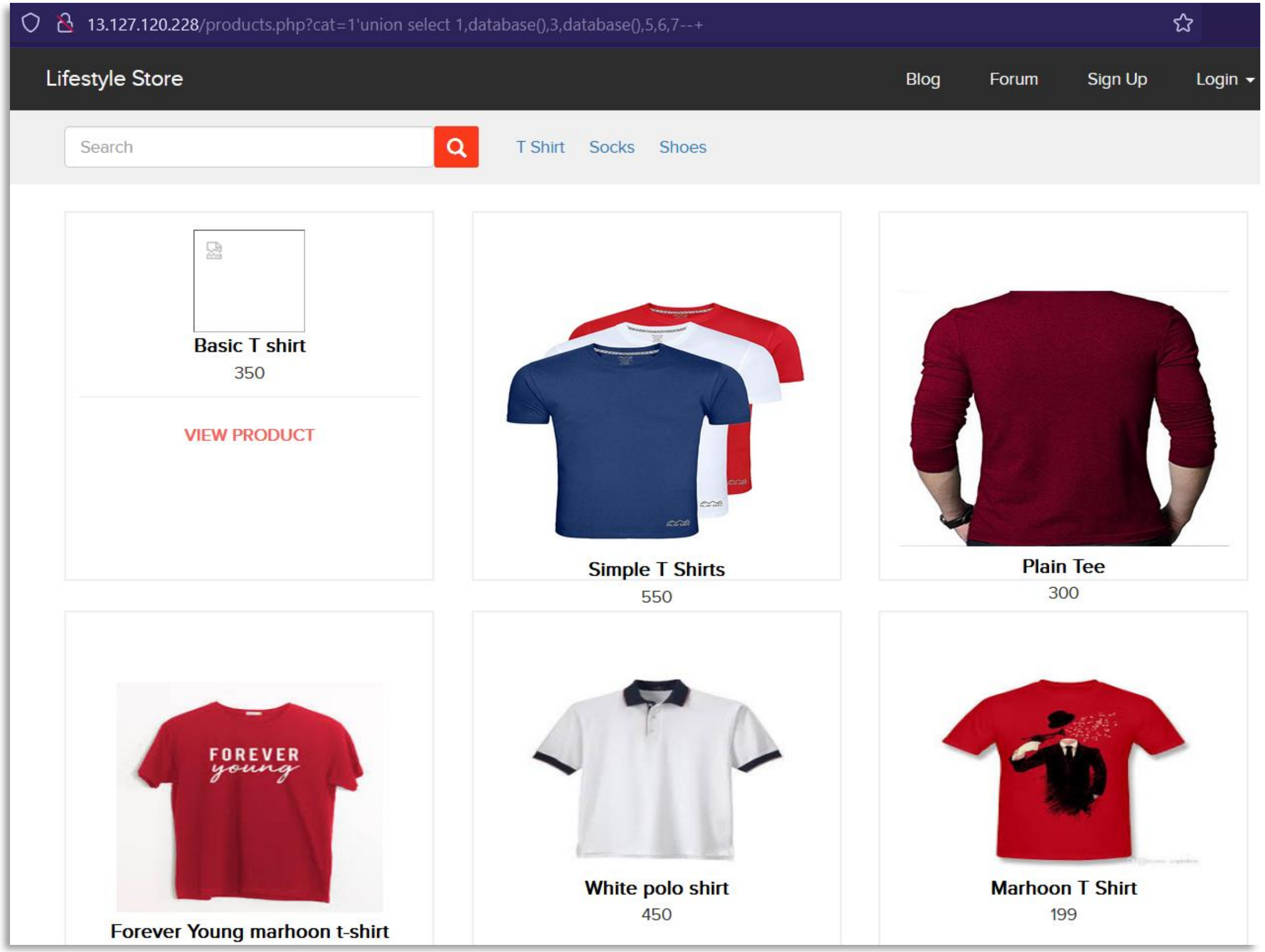


13.127.120.228/products.php?cat=1'--+

Proof of concept:

Following slides have the proof and risks of the proposed vulnerability.

- Hacker can execute commands as shown below to get critical information, here we have used the payload to find the name of the database of MySQL.



```
13.127.120.228/products.php?cat=1'union select 1,database(),3,database(),5,6,7--+
```

Proof of concept:

No. of Databases: 2

- Information_Schema
- Hacking_training_project

No. of tables in “Hacking_training_project”: 10

- order_items
- brands
- cart_items
- categories
- customers
- orders
- product_reviews
- products
- users
- sellers

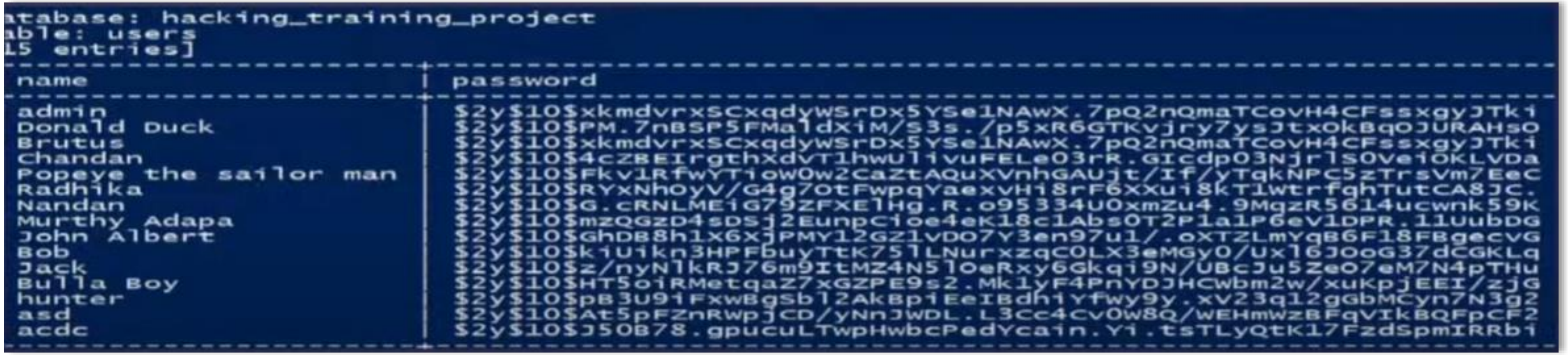
Business Impact:

The impact on the company if the vulnerability is exploited.

Business Impact:

Using this vulnerability, the attacker can execute arbitrary SQL commands on Lifestyle Store’s server and gain complete access to the internal database, which also makes all customer data inside it visible.

Below is the screenshot of users table which shows user credentials being leaked.



```
atabase: hacking_training_project
able: users
15 entries]
+------------------------+-----------------------------------------------------------------+
| name                   | password                                                        |
+------------------------+-----------------------------------------------------------------+
| admin                  | $2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki |
| Donald Duck            | $2y$10$PM.7nBSP5FMaldXiM/S3s./p5xR6GTKvjry7ysJtxOkBqOJURAHsO |
| Brutus                 | $2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki |
| Chandan                | $2y$10$4cZBEIrgthXdvT1hwUlivuFELeO3rR.GIcdpO3NjrlSOveiOKLvDa |
| Popeye the sailor man  | $2y$10$Fkv1RfwYTiowOw2CaZtAQuXVnhGAUjt/If/yTqkNPC5zTrsVm7EeC |
| Radhika                | $2y$10$RYxNhoyV/G4g7OtFwpqYaexvHi8rF6XXui8kT1wtrfghTutCA8JC. |
| Nandan                 | $2y$10$G.cRNLMEiG79ZFXElHg.R.o95334UOxmZu4.9MgzR5614ucwnk59K |
| Murthy Adapa           | $2y$10$mzQGzD4sDSj2EunpCioe4eK18c1AbsOT2P1a1P6ev1DPR.11uubDG |
| John Albert            | $2y$10$GhDB8h1X6xjPMY12GZ1vDO7Y3en97ul/.oXTZLmYqB6F18FBgecvG |
| Bob                    | $2y$10$kiUikn3HPFbuyTtK75lLNurxzqC0LX3eMGyO/Ux16JOoG37dCGKLq |
| Jack                   | $2y$10$z/nyNlkRJ76m9ItMZ4N5lOeRxy6Gkqi9N/UBcJu5ZeO7eM7N4pTHu |
| Bulla Boy              | $2y$10$HT5oiRMetqaZ7xGZPE9s2.Mk1yF4PnYDJHCWbm2w/xuKpjEEI/zjG |
| hunter                 | $2y$10$pB3U9iFxwBgSbl2AkBpiEeIBdh1YfWy9y.xV23q12gGbMCyn7N3g2 |
| asd                    | $2y$10$At5pFZnRwpjCD/yNnJWDL.L3Cc4Cv0W8Q/WEHmWzBFqVIkBQFpCF2 |
| acdc                   | $2y$10$J5OB78.gpucuLTwpHwbcPedYcain.Yi.tsTLyQtK17FzdSpmIRRbi |
+------------------------+-----------------------------------------------------------------+
```

The data above can be decoded using Burp Suite, the attacker can decode and use this information to login to admin panel 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

Recommendations:

Take the following recommendations
to secure and avoid SQL database exploitation.

Recommendations:

- Prepared statements: Use SQL prepared statements available in all web development languages and frameworks to avoid attacker being able to modify SQL query.
- Do not run Database service as admin/root user.
- Disable default accounts, passwords and databases.
- Assign each Database user only the required permissions and not all permissions.
- Character encoding: Convert simple codes into different characters like '~'/"^'. It is also suggested to follow HTML and other encodings.

References:

- https://owasp.org/www-community/attacks/SQL_Injection
- https://en.wikipedia.org/wiki/SQL_injection

2. ACCOUNT TAKEOVER VIA OTP BYPASS

(CRITICAL)

Below mentioned page has a login form that follows login via OTP that can be brute forced.

RELEVANT URL:

- http://13.127.120.228/login/admin.php

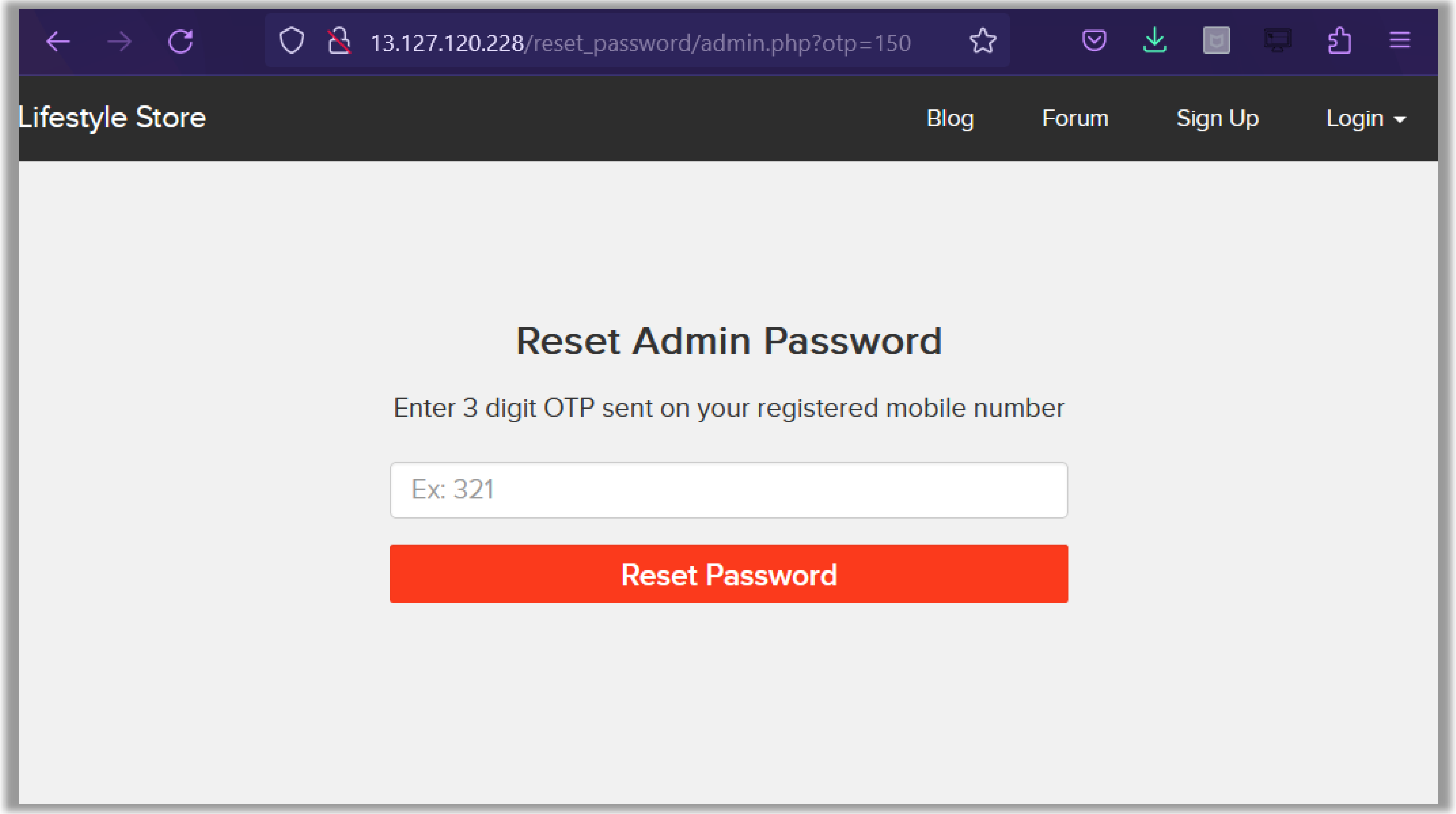
AFFECTED PARAMETERS:

- OTP (POST)

Observations:

Following slides have the details about the vulnerability observed.

- Navigate to http://13.127.120.228/login/admin.php you will see a “forgot your password” hyperlink which asks for OTP which is sent to victim’s mobile number, input any anonymous 3 digit OTP and intercept the request with burp suite.



13.127.120.228/reset_password/admin.php?otp=150

Reset Admin Password

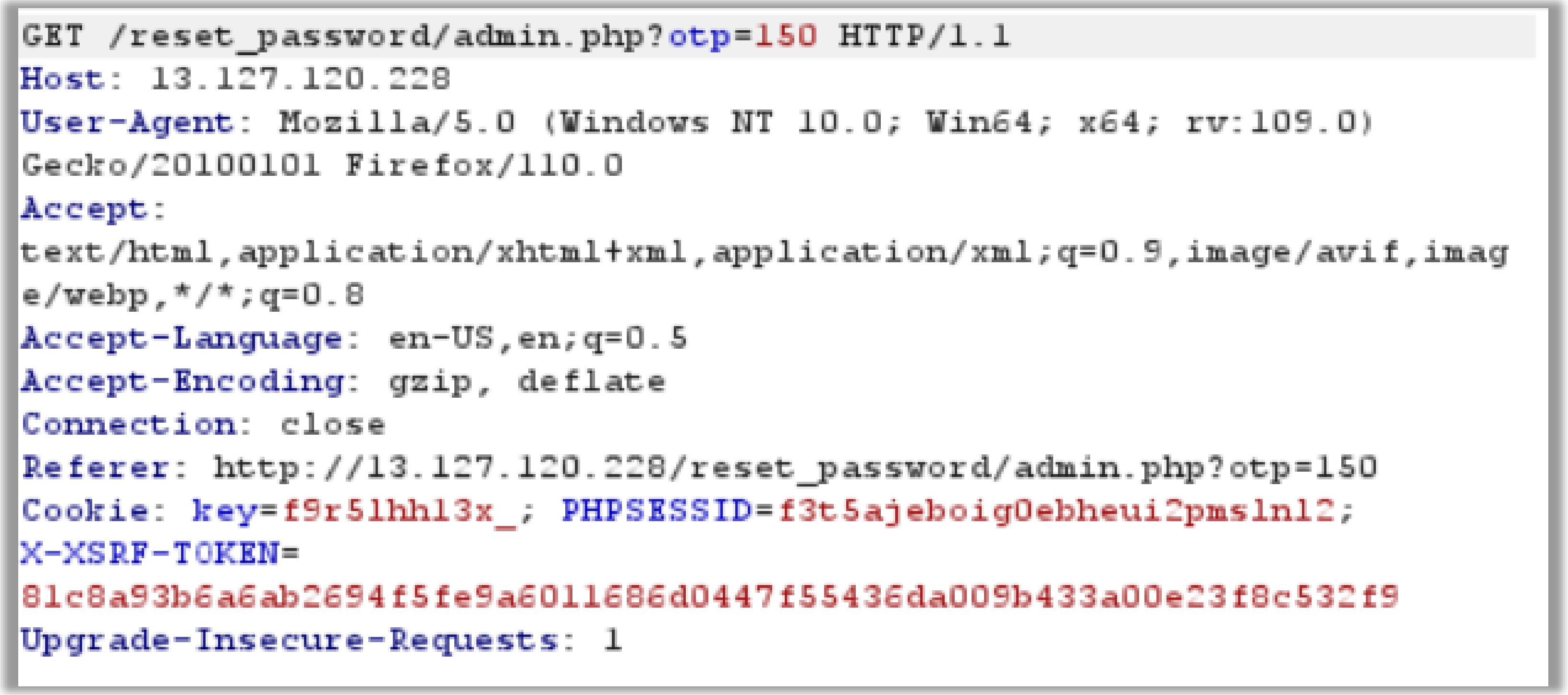
Enter 3 digit OTP sent on your registered mobile number

Ex: 321

Proof of concept:

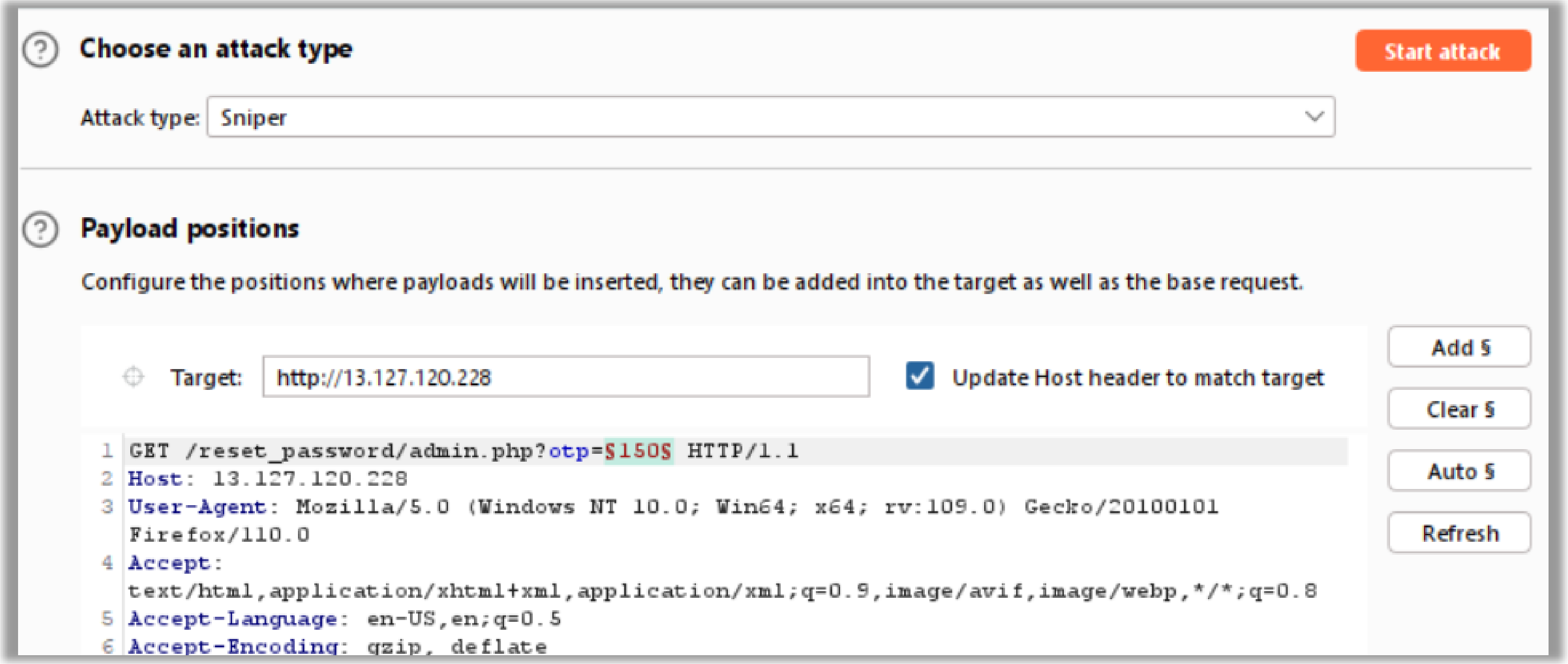
Following slides have the proof and risks of the proposed vulnerability.

- The request below will be generated in burp suite using GET parameter.



```
GET /reset_password/admin.php?otp=150 HTTP/1.1
Host: 13.127.120.228
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/110.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://13.127.120.228/reset_password/admin.php?otp=150
Cookie: key=f9r5lhhl3x_; PHPSESSID=f3t5ajeboig0ebheui2pmsln12;
X-XSRF-TOKEN=
81c8a93b6a6ab2694f5fe9a6011686d0447f55436da009b433a00e23f8c532f9
Upgrade-Insecure-Requests: 1
```

- We will brute force by getting all combinations of 3 digit OTPs and input the correct one to bypass.



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://13.127.120.228

☑ Update Host header to match target

```
GET /reset_password/admin.php?otp=§150§ HTTP/1.1
Host: 13.127.120.228
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/110.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

Business impact:

The impact on the company
if the vulnerability is exploited.

Business Impact:

- A malicious hacker can gain complete access to admin account just by brute-forcing due to rate limiting flaw as a hacker can attempt as many times as he wants as there is no bounds in number of trials.
- This leads to complete compromise of personal user data of every customer.
- Attacker can login, then carry out actions on behalf of the victim which could lead to serious financial loss.

Recommendations:

Take the following recommendations to secure and avoid OTP bypass.

Recommendations:

- Use rate limiting checks on the number of times the OTP request is generated.
- OTP should be at least of 6 digits, a 3 digit OTP can be guessed or brute-forced easily.
- OTP should expire in a particular time like 2 to 5 minutes to make authorization process more secure.

References:

- https://owasp.org/www-project-mobile-app-security/

3. UNAUTHORIZED ACCESS TO CUSTOMER DETAILS

(CRITICAL)

The “My orders” section of the website shows am Insecure Direct Object Reference (IDOR), this allows hackers to get access to any customer’s order details and more.

RELEVANT URL:

- http://13.127.120.228/orders/orders.php?customer=18

AFFECTED PARAMETERS:

- Customer data (GET)

Other URL with similar issues

RELEVANT URL:

- http://13.127.120.228/products/details.php?p_id=5

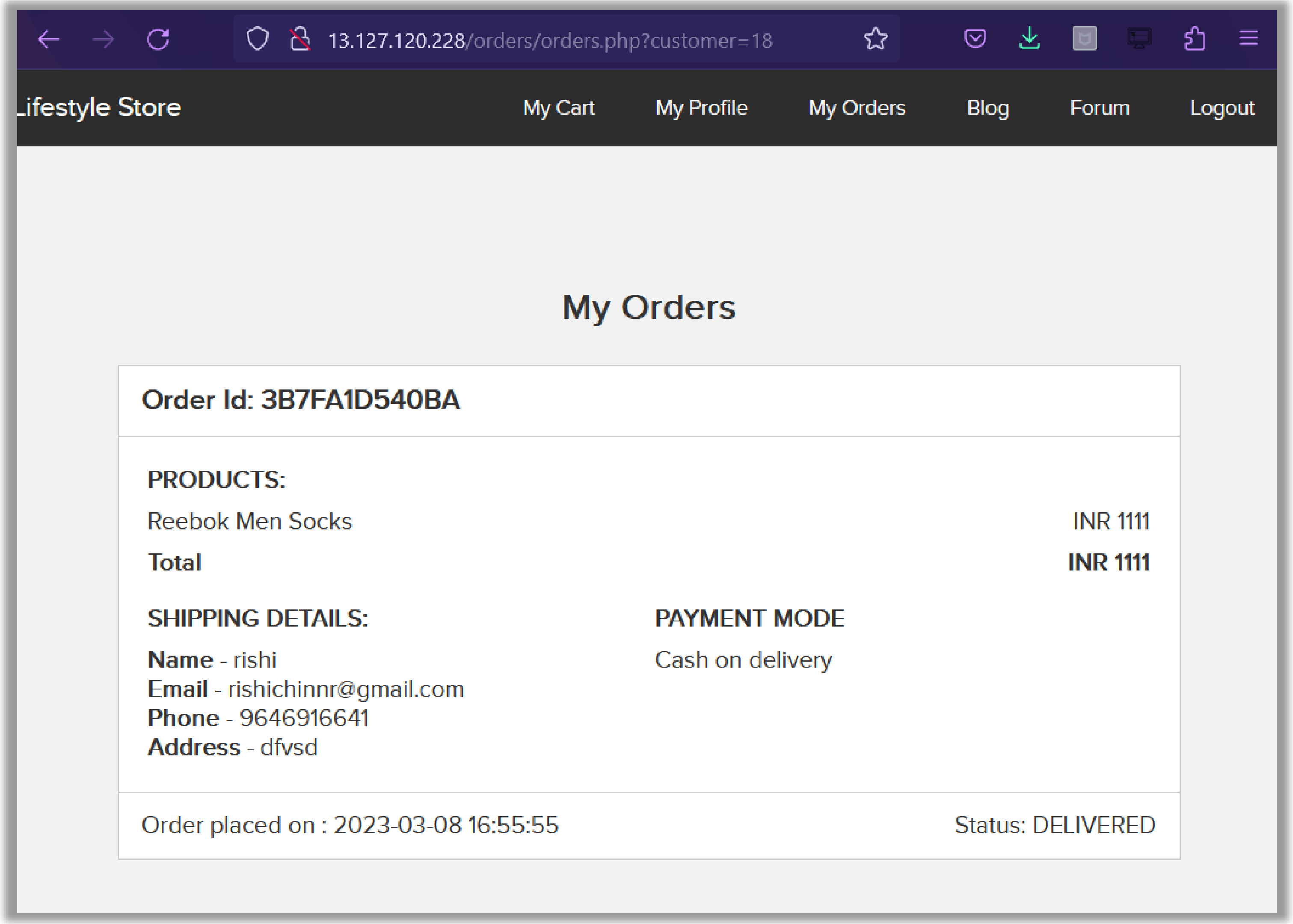
AFFECTED PARAMETRS:

- P_ID (GET)

Observations:

Following slides have the details about the vulnerability observed.

- Login to your account and go to “My orders” section, you will see a GET parameter as shown below “customer=18”



My Orders

Order Id: 3B7FA1D540BA

PRODUCTS:

Reebok Men Socks	INR 1111
Total	INR 1111

SHIPPING DETAILS:

Name - rishi
Email - rishichinnr@gmail.com
Phone - 9646916641
Address - dfvsd

PAYMENT MODE

Cash on delivery

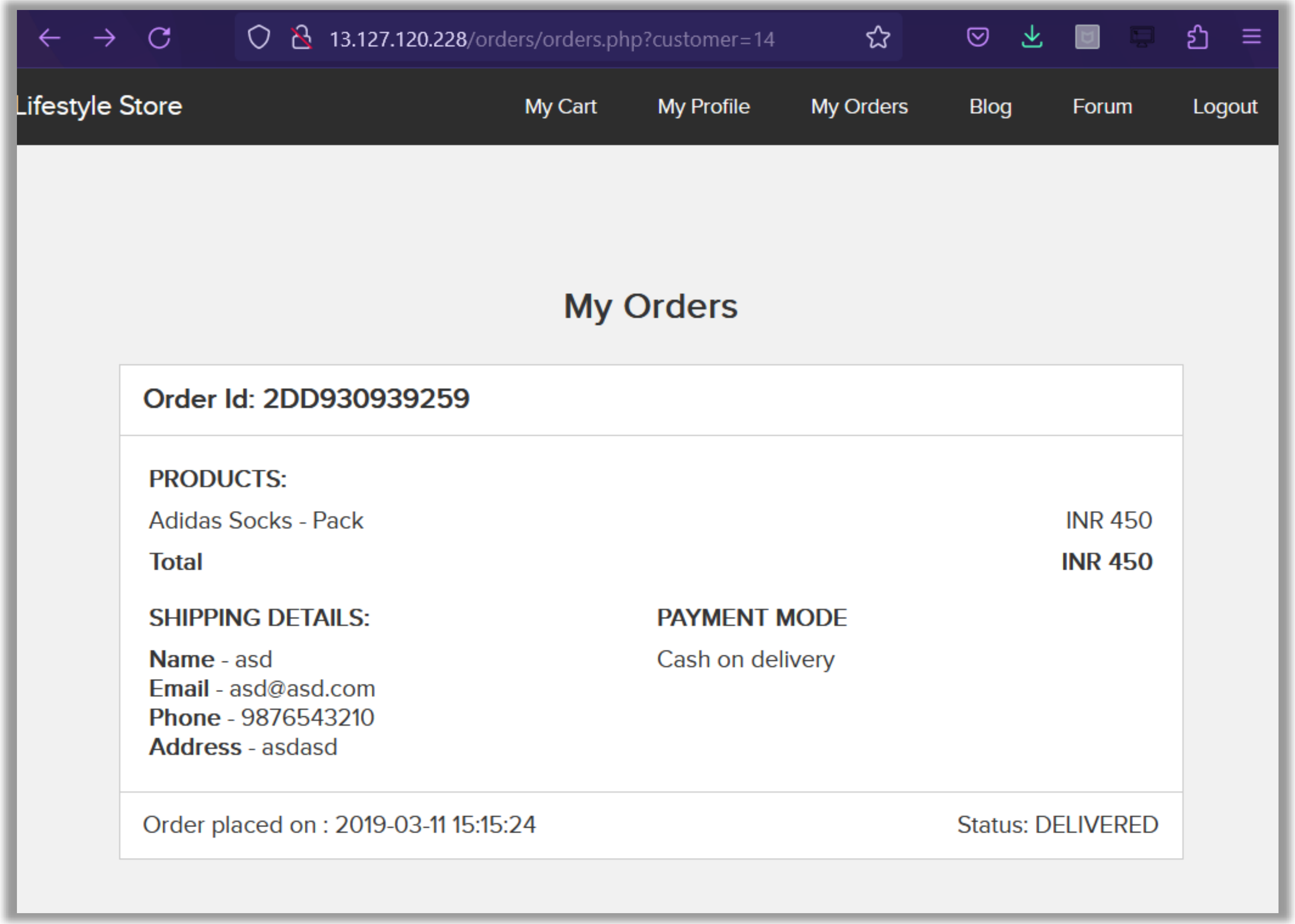
Order placed on : 2023-03-08 16:55:55

Status: DELIVERED

Proof of concept:

Following slides have the proof and risks of the proposed vulnerability.

- Change the customer number to any random number, and we get the details of the new customer ID.



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

Business impact:

The impact on the company
if the vulnerability is exploited.

Business Impact:

- This vulnerability can be exploited by malicious hackers to carry out targeted phishing attacks on the users and the information can be sold to the competitors/black-market.
- More over, as there is no rate limiting checks, attacker can brute-force 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.

Recommendations:

Take the following recommendations to secure and avoid OTP bypass.

Recommendations:

- Make sure user have the access to self data.
- Use proper rate limiting checks on the number of request comes from a single user in a small amount of time.
- Implement proper authentication and authorization checks to make sure that the user has permission to the data which is being requested.

References:

- https://owasp.org/www-chapter-ghana/
- https://portswigger.net/web-security/access-control/idor

4. REFLECTED CROSS SITE SCRIPTING

(SEVERE)

These parameters are vulnerable to XSS

RELEVANT URL:

- http://13.127.120.228/products/details.php?p_id=4

AFFECTED PARAMETERS:

- URL (GET)

PAYLOAD:

- <script>alert(1)</script>

Other parameters with similar issues.

RELEVANT URL:

- http://13.127.120.228/products/details.php?p_id=29

AFFECTED PARAMETERS:

- Review box

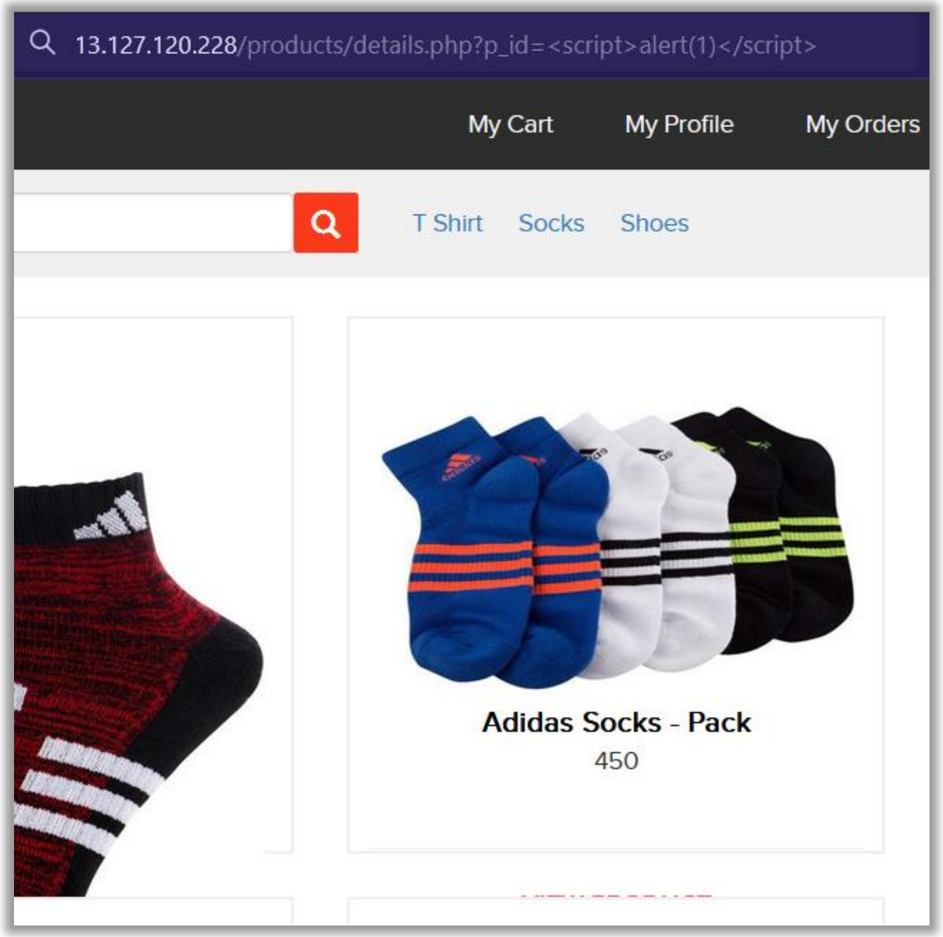
PAYLOAD:

- <script>alert(12)</script>

Observations:

Following slides have the details about the vulnerability observed.

- Navigate to the site and login your account.
- Go to products and select any product. Now, the URL shows the id of the product you are on, you can replace that with the payload.

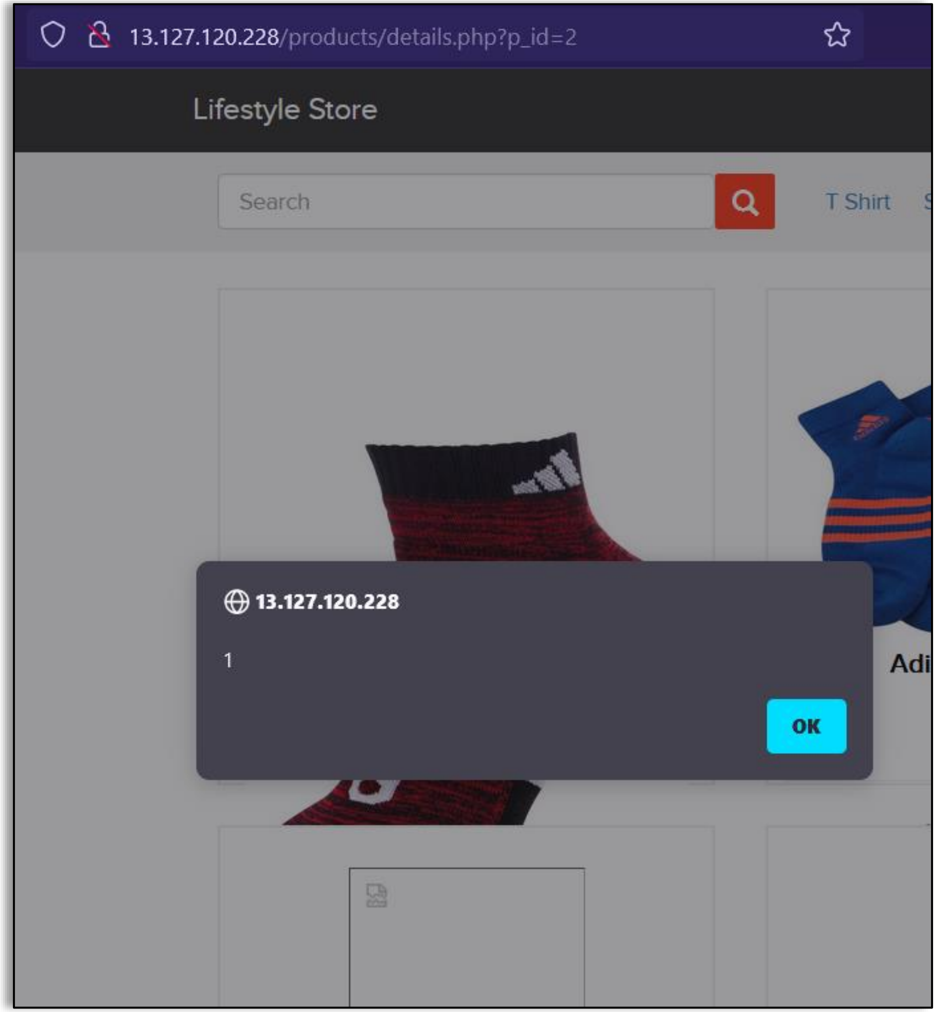


```
13.127.120.228/products/details.php?p_id=<script>alert(1)</script>
```

Proof of concept:

Following slides have the proof and risks of the proposed vulnerability.

- After entering the payload press enter. The page will redirect you to home page but when you click on the same product again it will show the alert you had just input.

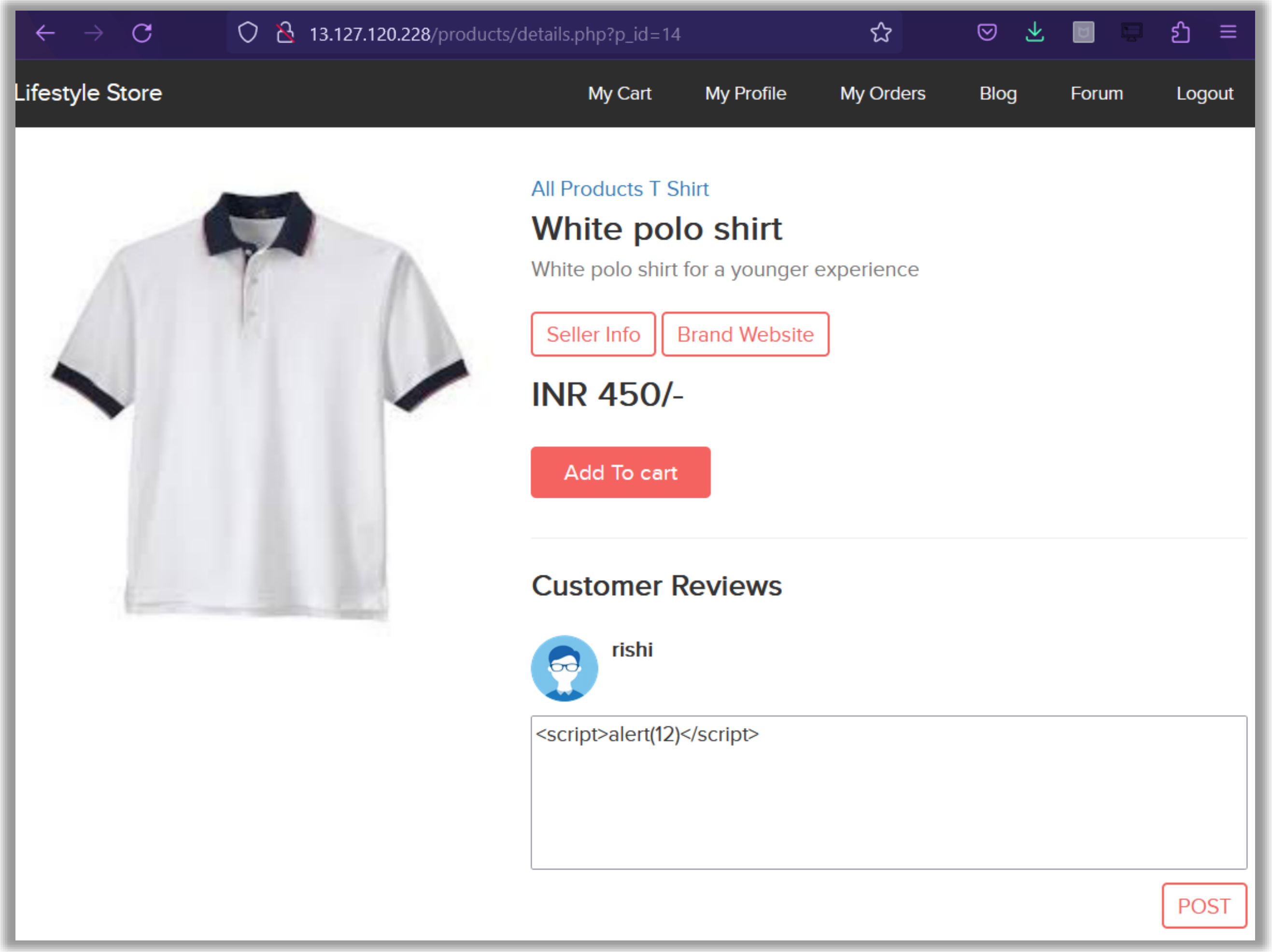


13.127.120.228/products/details.php?p_id=2

13.127.120.228

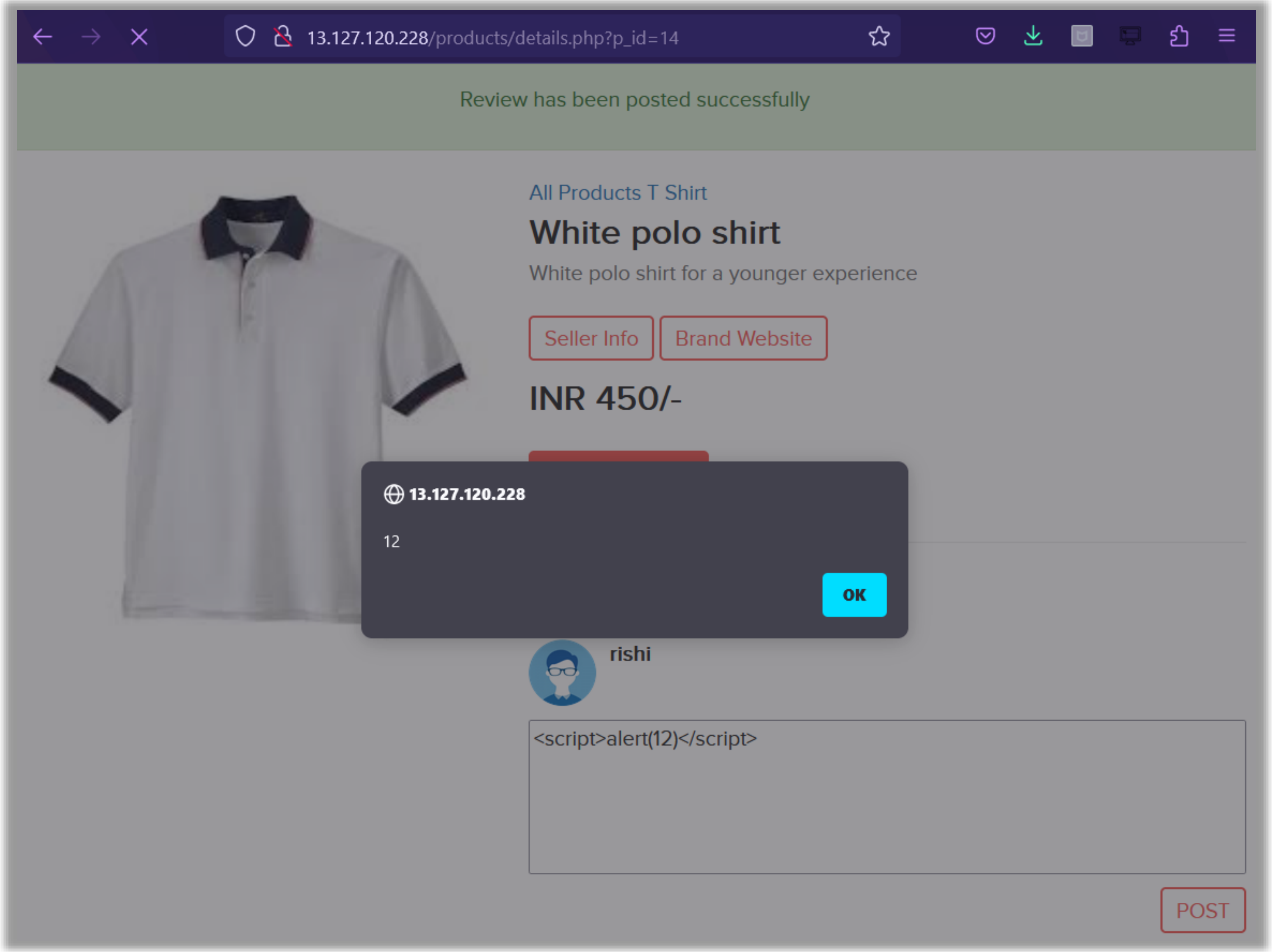
1

- We have a similar issue in the review box.
- Inject payload <script>alert(12)



```
<script>alert(12)</script>
```

- We get the alert by the website.



13.127.120.228/products/details.php?p_id=14

Review has been posted successfully

White polo shirt

White polo shirt for a younger experience

INR 450/-

13.127.120.228

12

<script>alert(12)</script>

Business impact:

The impact on the company
if the vulnerability is exploited.

Business Impact:

- As the attacker can inject arbitrary HTML, CSS and Javascript via the URL, they can put any content on the page like phishing pages, and can even host explicit content that could compromise the reputation of the organization.
- When the attacker sends the link with the payload to the victim, the victim sees a modified content on the website. As the user trusts the website, user will trust the content as well.

Recommendations:

Take the following recommendations to secure and avoid OTP bypass.

Recommendations:

- Secure the user input by blocking other inputs which you don’t want.
- Encode the HTML/CSS special characters and codes in an encoded form before printing them on the website.

References:

- https://owasp.org/www-community/attacks/xss/
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.w3schools.com/cybersecurity/cybersecurity_web_applications_attacks.php

5. DIRECTORY LISTINGS

(SEVERE)

This URL is vulnerable

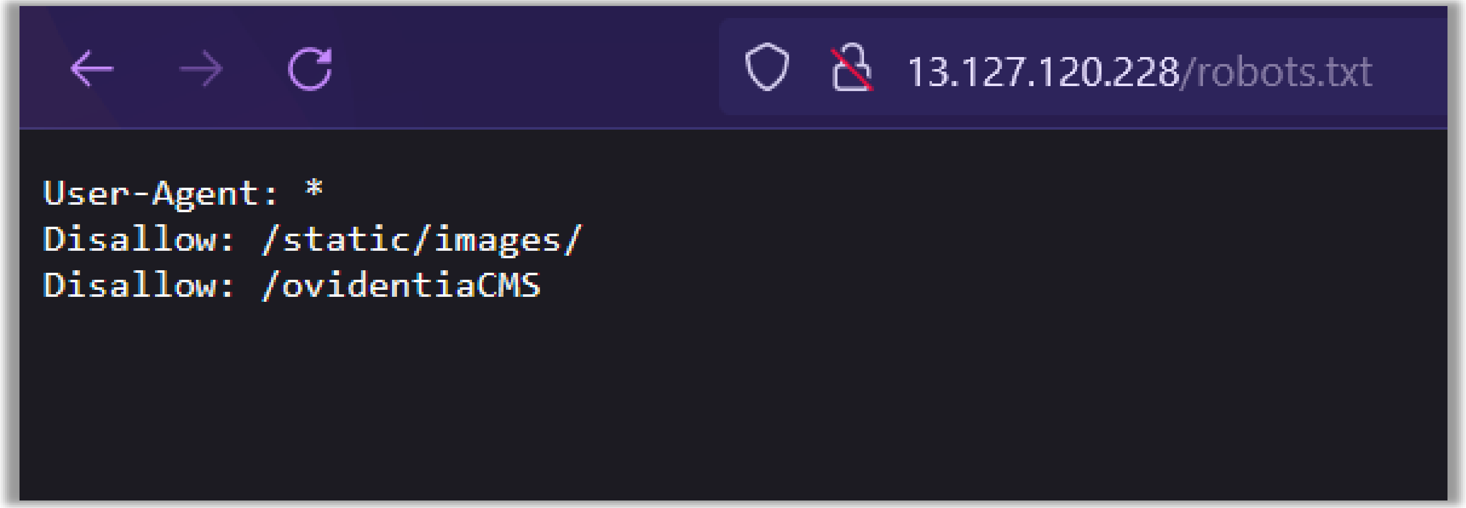
RELEVANT URL:

- http:// 13.127.120.228/robots.txt

Observations:

Following slides have the details about the vulnerability observed.

- Go to http:// 13.127.120.228/robots.txt
- Here, we can see a complete list and directories of the customers, images of products and all the products-page info.
- We can also see the administrator directory.
- This has a weak password flaw in Ovidentia CMS, which lets an attacker access the administrator panel without much trials.

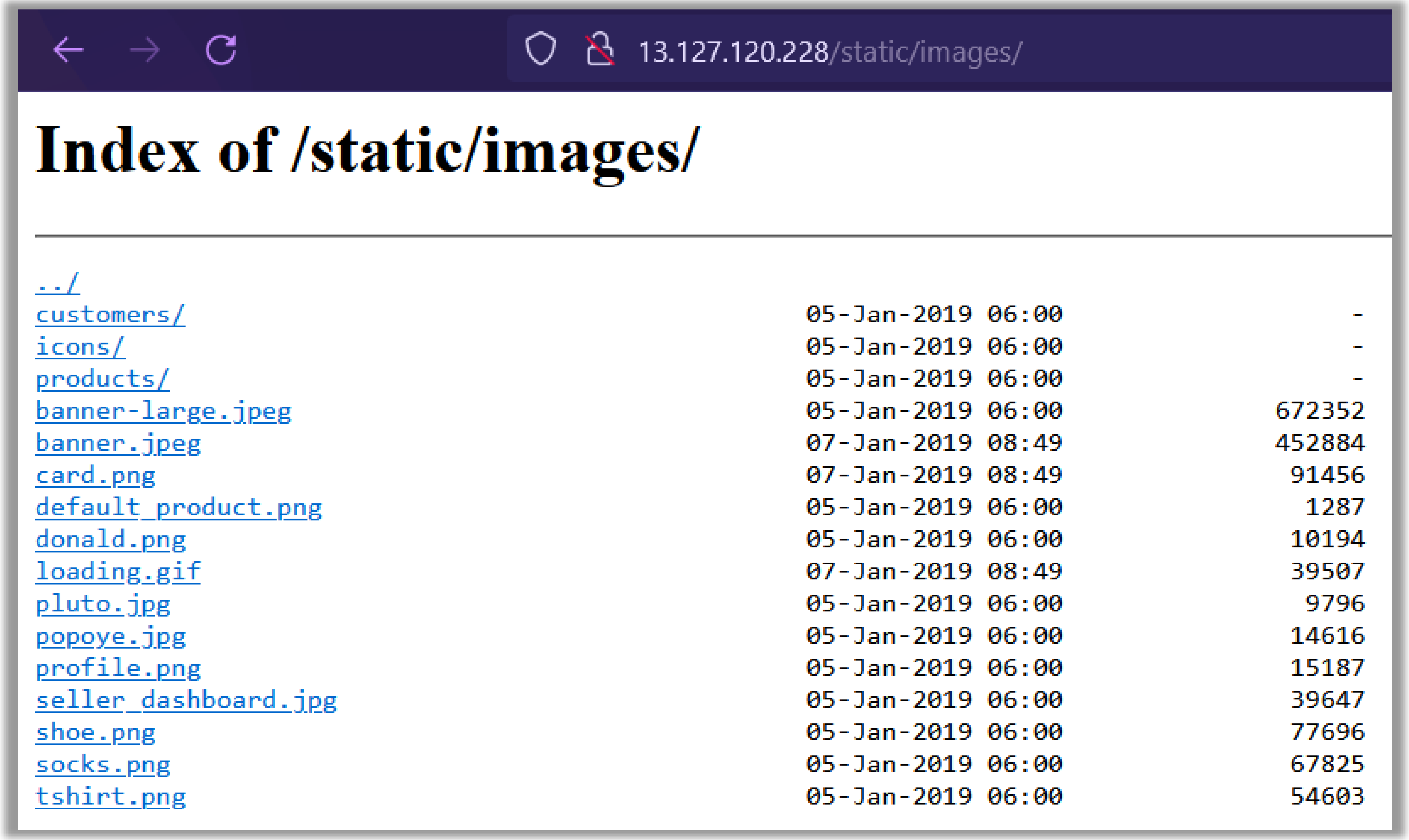


```
User-Agent: *
Disallow: /static/images/
Disallow: /ovidentiaCMS
```

Proof of concept:

Following slides have the proof and risks of the proposed vulnerability.

/static/images

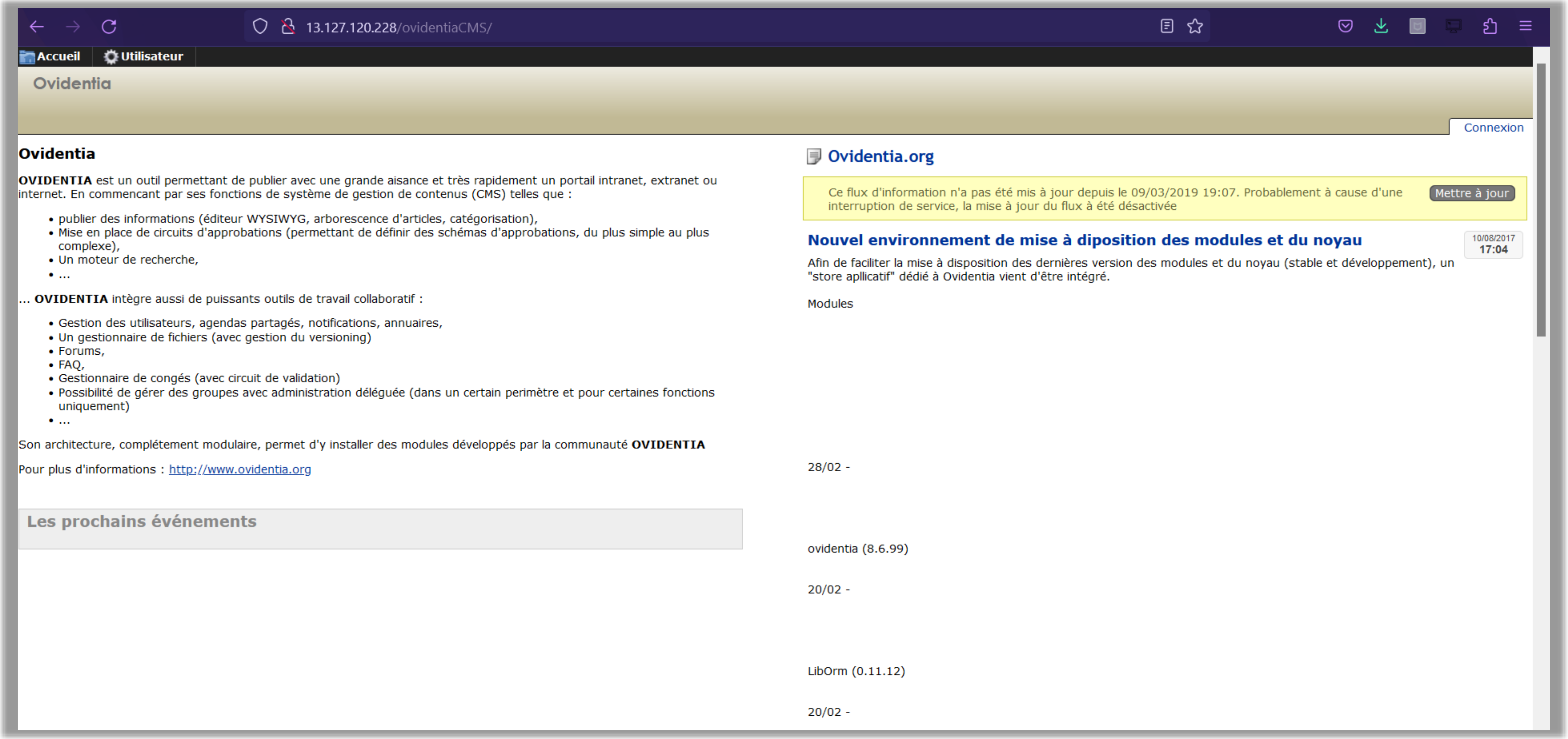


13.127.120.228/static/images/

Index of /static/images/

```
../
customers/                                         05-Jan-2019 06:00                   -
icons/                                             05-Jan-2019 06:00                   -
products/                                          05-Jan-2019 06:00                   -
banner-large.jpeg                                  05-Jan-2019 06:00              672352
banner.jpeg                                        07-Jan-2019 08:49              452884
card.png                                           07-Jan-2019 08:49               91456
default_product.png                                05-Jan-2019 06:00                1287
donald.png                                         05-Jan-2019 06:00               10194
loading.gif                                        07-Jan-2019 08:49               39507
pluto.jpg                                          05-Jan-2019 06:00                9796
popoye.jpg                                         05-Jan-2019 06:00               14616
profile.png                                        05-Jan-2019 06:00               15187
seller_dashboard.jpg                               05-Jan-2019 06:00               39647
shoe.png                                           05-Jan-2019 06:00               77696
socks.png                                          05-Jan-2019 06:00               67825
tshirt.png                                         05-Jan-2019 06:00               54603
```

/ovidentiaCMS/



Ovidentia

OVIDENTIA est un outil permettant de publier avec une grande aisance et très rapidement un portail intranet, extranet ou internet. En commencant par ses fonctions de système de gestion de contenus (CMS) telles que :

- publier des informations (éditeur WYSIWYG, arborescence d'articles, catégorisation),
- Mise en place de circuits d'approbations (permettant de définir des schémas d'approbations, du plus simple au plus complexe),
- Un moteur de recherche,
- ...

... **OVIDENTIA** intègre aussi de puissants outils de travail collaboratif :

- Gestion des utilisateurs, agendas partagés, notifications, annuaires,
- Un gestionnaire de fichiers (avec gestion du versioning)
- Forums,
- FAQ,
- Gestionnaire de congés (avec circuit de validation)
- Possibilité de gérer des groupes avec administration déléguée (dans un certain perimètre et pour certaines fonctions uniquement)
- ...

Son architecture, complétement modulaire, permet d'y installer des modules développés par la communauté **OVIDENTIA**

Pour plus d'informations : http://www.ovidentia.org

Les prochains événements

Ovidentia.org

Ce flux d'information n'a pas été mis à jour depuis le 09/03/2019 19:07. Probablement à cause d'une interruption de service, la mise à jour du flux à été désactivée

Nouvel environnement de mise à diposition des modules et du noyau

10/08/2017
17:04

Afin de faciliter la mise à disposition des dernières version des modules et du noyau (stable et développement), un "store apllicatif" dédié à Ovidentia vient d'être intégré.

Modules

28/02 -

ovidentia (8.6.99)

20/02 -

LibOrm (0.11.12)

20/02 -

Business impact:

The impact on the company
if the vulnerability is exploited.

Business Impact:

- The hacker can get all the information on the CMS and also get the privileges to tackle with the administrator login credentials and compromise the complete name of the company.
- A malicious hacker can take important information from seller point of view and what products every seller is selling at what price and also the information of users.

Recommendations:

Take the following recommendations
to secure and avoid defacing/data altering.

Recommendations:

- Disable all the directory listings.
- Include a index.html in all folders with default messages.
- Remove all the default passwords and add your own new strong passwords which must have a special character and a number and must be greater or equal to 8 digits for maximum security.

References:

- http://www.securitytracker.com/
- https://www.w3schools.com/

6. INFORMATION DISCLOSURE

(LOW)

This URL is vulnerable

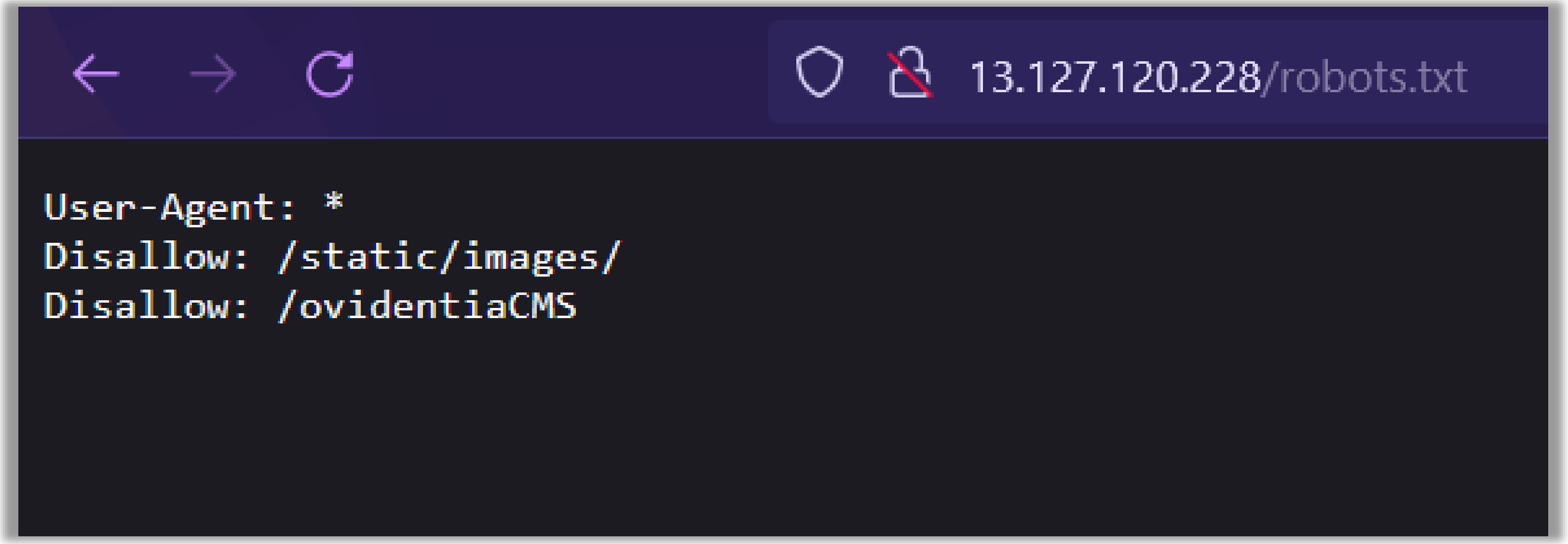
RELEVANT URL:

- http://13.127.120.228/server-status

Observations:

Following slides have the details about the vulnerability observed.

- Go to http:// 13.127.120.228/robots.txt
- Complete list and directories of the customer and images of products and all the products page info and also the administrator directory is also shown.
- Also this has a weak password flaw in Ovidenta CMS, which lets an attacker access the administrator panel without much trials.



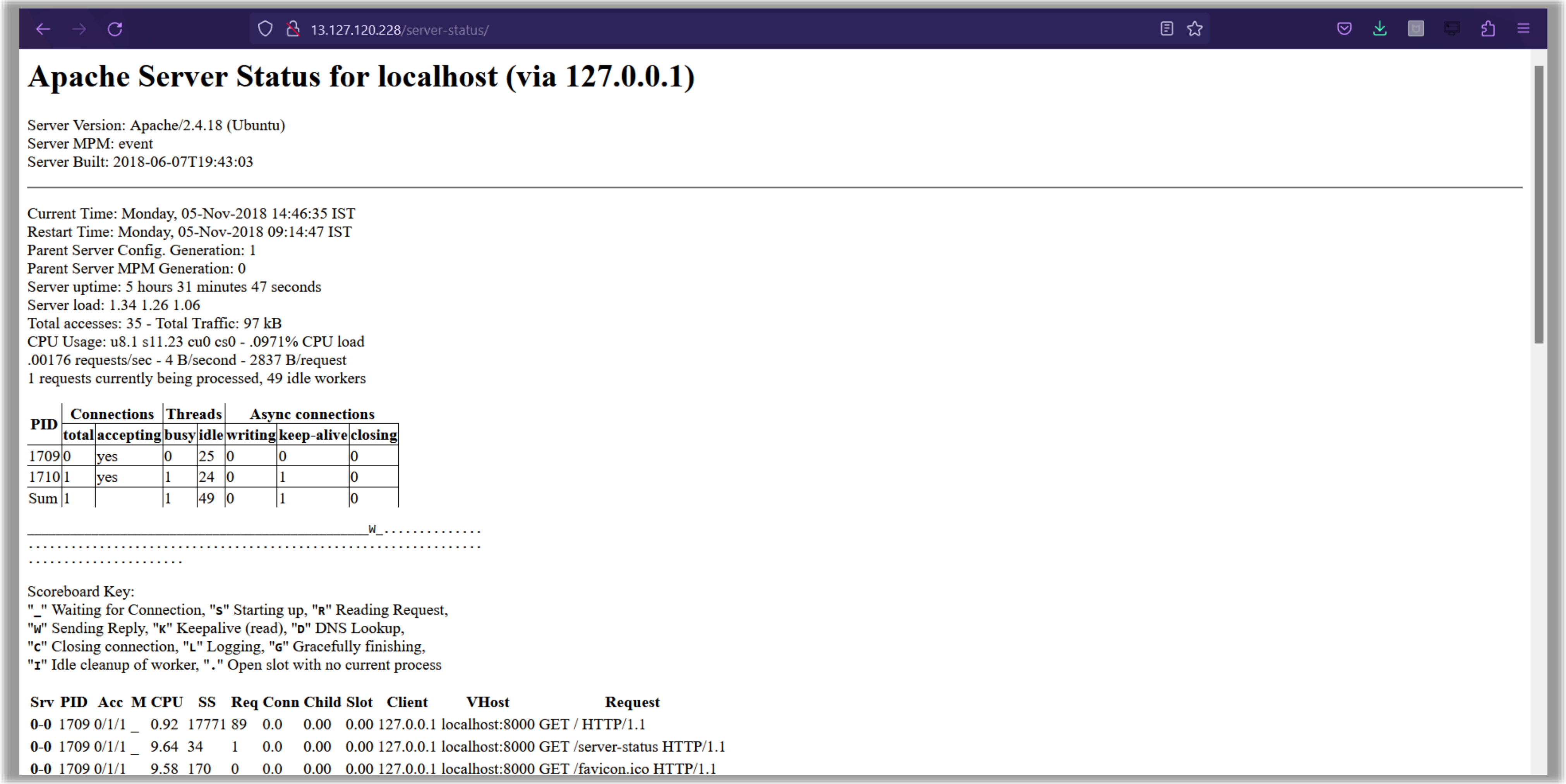
13.127.120.228/robots.txt

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

Proof of concept:

Following slides have the proof and risks of the proposed vulnerability.

- Go to http://13.127.120.228/server-status and the critical server information will be shown as seen below.



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

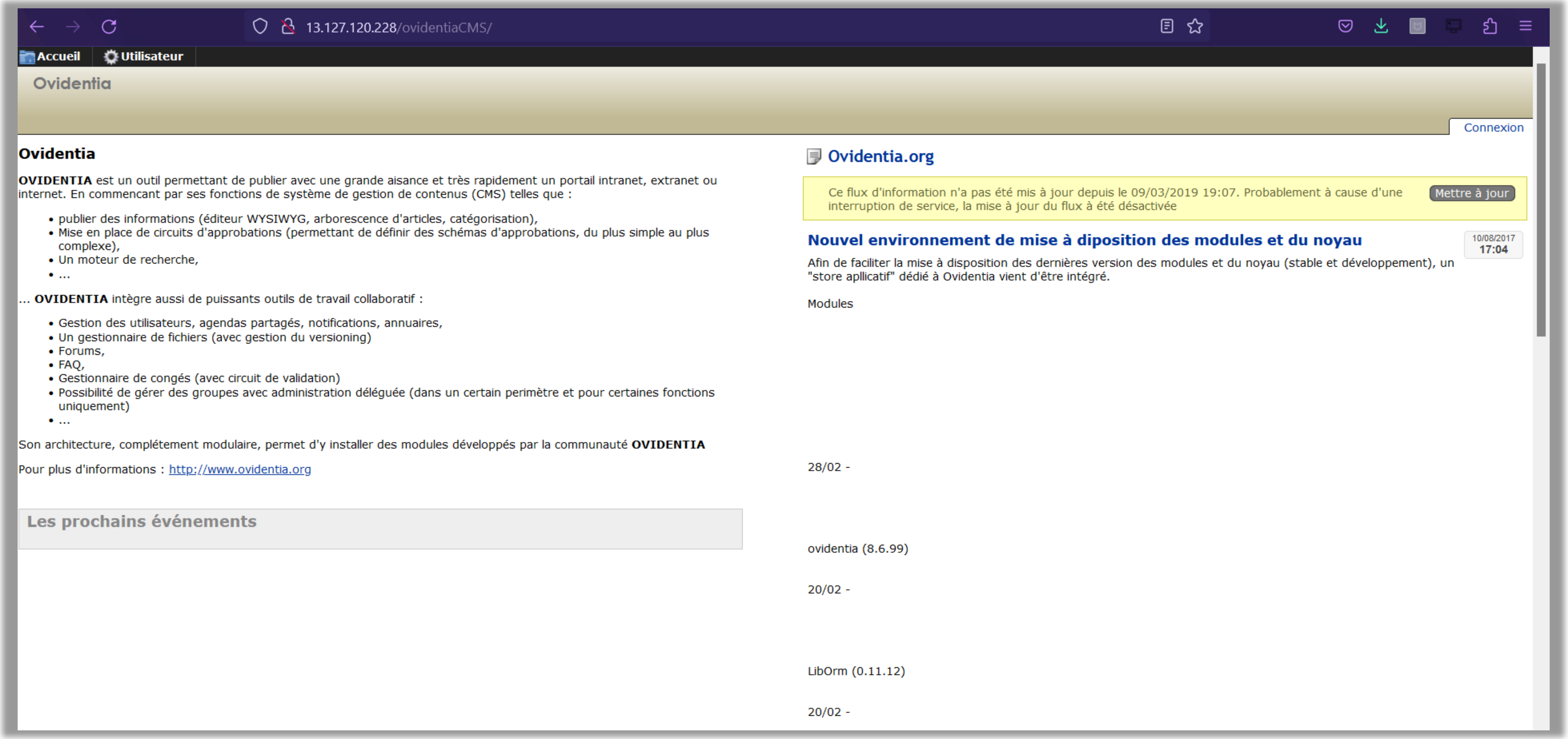
PID	Connections		Threads		Async connections		
	total	accepting	busy	idle	writing	keep-alive	closing
1709	0	yes	0	25	0	0	0
1710	1	yes	1	24	0	1	0
Sum	1		1	49	0	1	0

```
________________________________________________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

/ovidentiaCMS/



Ovidentia

OVIDENTIA est un outil permettant de publier avec une grande aisance et très rapidement un portail intranet, extranet ou internet. En commencant par ses fonctions de système de gestion de contenus (CMS) telles que :

- publier des informations (éditeur WYSIWYG, arborescence d'articles, catégorisation),
- Mise en place de circuits d'approbations (permettant de définir des schémas d'approbations, du plus simple au plus complexe),
- Un moteur de recherche,
- ...

... **OVIDENTIA** intègre aussi de puissants outils de travail collaboratif :

- Gestion des utilisateurs, agendas partagés, notifications, annuaires,
- Un gestionnaire de fichiers (avec gestion du versioning)
- Forums,
- FAQ,
- Gestionnaire de congés (avec circuit de validation)
- Possibilité de gérer des groupes avec administration déléguée (dans un certain perimètre et pour certaines fonctions uniquement)
- ...

Son architecture, complétement modulaire, permet d'y installer des modules développés par la communauté **OVIDENTIA**

Pour plus d'informations : http://www.ovidentia.org

Les prochains événements

Ovidentia.org

Ce flux d'information n'a pas été mis à jour depuis le 09/03/2019 19:07. Probablement à cause d'une interruption de service, la mise à jour du flux à été désactivée

Nouvel environnement de mise à diposition des modules et du noyau

10/08/2017
17:04

Afin de faciliter la mise à disposition des dernières version des modules et du noyau (stable et développement), un "store apllicatif" dédié à Ovidentia vient d'être intégré.

Modules

28/02 -

ovidentia (8.6.99)

20/02 -

LibOrm (0.11.12)

20/02 -

Business impact:

The impact on the company
if the vulnerability is exploited.

Business Impact:

- Although this vulnerability does not have a direct impact on the server or the client but a malicious hacker can know things like mapping the server-architecture and map his hacking plan further on what and how to compromise.

Recommendations:

Take the following recommendations
to secure and avoid defacing/data altering.

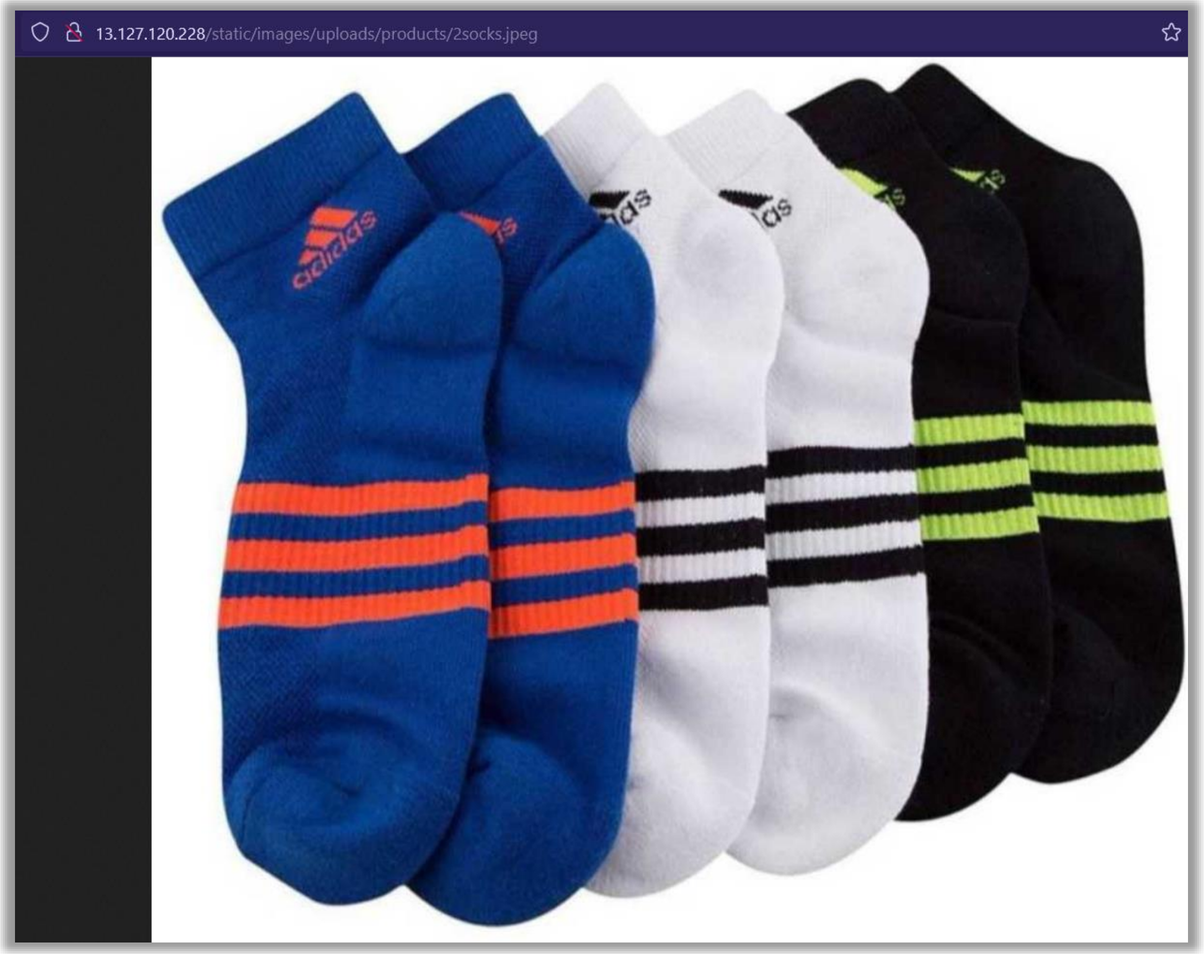
Recommendations:

- Disable all the directory listings.
- Disable the server-status.

7. PERSONALLY IDENTIFIED INFORMATION LEAKAGE

(CRITICAL)

- Go to http://13.127.120.228/static/images/uploads/products/2socks.jpeg and drag any drop product image in a new tab, the following page will look like the one shown with the image of the product you chose.

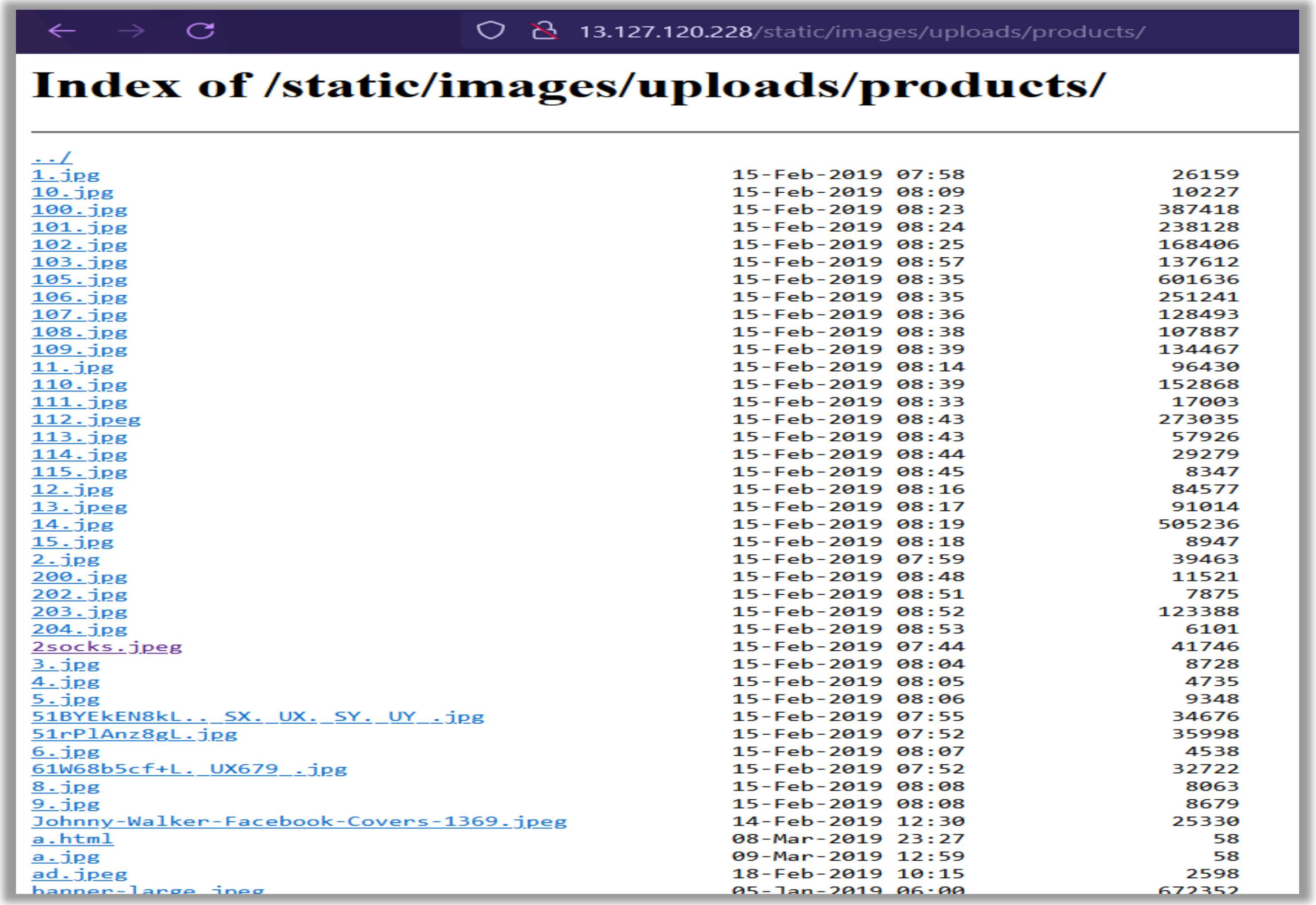


13.127.120.228/static/images/uploads/products/2socks.jpeg

Proof of concept:

Following slides have the proof and risks of the proposed vulnerability.

- Now, we remove the image name, i.e. “2socks.jpeg” in our case and it enter, the following page with details will be shown.



Index of /static/images/uploads/products/

```
../
1.jpg                                              15-Feb-2019 07:58               26159
10.jpg                                             15-Feb-2019 08:09               10227
100.jpg                                            15-Feb-2019 08:23              387418
101.jpg                                            15-Feb-2019 08:24              238128
102.jpg                                            15-Feb-2019 08:25              168406
103.jpg                                            15-Feb-2019 08:57              137612
105.jpg                                            15-Feb-2019 08:35              601636
106.jpg                                            15-Feb-2019 08:35              251241
107.jpg                                            15-Feb-2019 08:36              128493
108.jpg                                            15-Feb-2019 08:38              107887
109.jpg                                            15-Feb-2019 08:39              134467
11.jpg                                             15-Feb-2019 08:14               96430
110.jpg                                            15-Feb-2019 08:39              152868
111.jpg                                            15-Feb-2019 08:33               17003
112.jpeg                                           15-Feb-2019 08:43              273035
113.jpg                                            15-Feb-2019 08:43               57926
114.jpg                                            15-Feb-2019 08:44               29279
115.jpg                                            15-Feb-2019 08:45                8347
12.jpg                                             15-Feb-2019 08:16               84577
13.jpeg                                            15-Feb-2019 08:17               91014
14.jpg                                             15-Feb-2019 08:19              505236
15.jpg                                             15-Feb-2019 08:18                8947
2.jpg                                              15-Feb-2019 07:59               39463
200.jpg                                            15-Feb-2019 08:48               11521
202.jpg                                            15-Feb-2019 08:51                7875
203.jpg                                            15-Feb-2019 08:52              123388
204.jpg                                            15-Feb-2019 08:53                6101
2socks.jpeg                                        15-Feb-2019 07:44               41746
3.jpg                                              15-Feb-2019 08:04                8728
4.jpg                                              15-Feb-2019 08:05                4735
5.jpg                                              15-Feb-2019 08:06                9348
51BYEkEN8kL.._SX._UX._SY._UY_.jpg                  15-Feb-2019 07:55               34676
51rPlAnz8gL.jpg                                    15-Feb-2019 07:52               35998
6.jpg                                              15-Feb-2019 08:07                4538
61W68b5cf+L._UX679_.jpg                            15-Feb-2019 07:52               32722
8.jpg                                              15-Feb-2019 08:08                8063
9.jpg                                              15-Feb-2019 08:08                8679
Johnny-Walker-Facebook-Covers-1369.jpeg            14-Feb-2019 12:30               25330
a.html                                             08-Mar-2019 23:27                  58
a.jpg                                              09-Mar-2019 12:59                  58
ad.jpeg                                            18-Feb-2019 10:15                2598
banner-large.jpeg                                  05-Jan-2019 06:00              672352
```

Business impact:

The impact on the company
if the vulnerability is exploited.

Business Impact:

- A malicious hacker can gain access to the shell application and various other html files which have been shown in the listings.
- It can also has a weak-password flaw.
- A hacker can get access to the shell and upload his own malicious codes to make the trusted site a hacker room for phishing and tricking users. This will result in defamation of the website.

Recommendations:

Take the following recommendations
to secure and avoid defacing/data altering.

Recommendations:

- Enable 2-factor authentication for sensitive data, and also use stronger passwords of at least 8 characters of different types.
- Find all PII stored, and encrypt them with various techniques and also disable all the listings.

References:

- https://www.cloudcodes.com/blog/casb-help-organizations-pii-compliance.html
- https://www.hackerone.com/resources/reporting

8. SELF REDIRECTION HTML DEVELOPER FLAW

(SEVERE)

It redirects to password reset link without authentication.

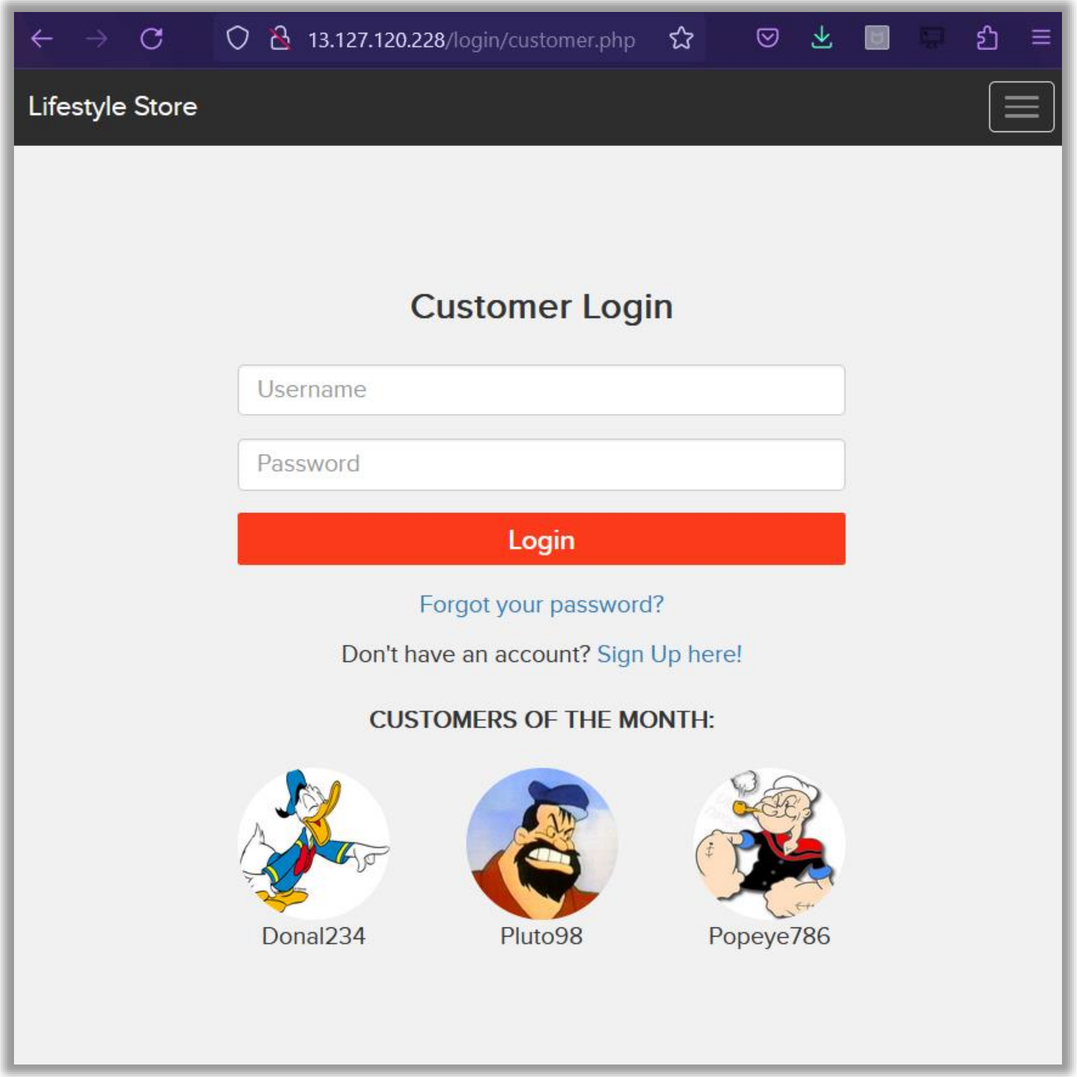
RELEVANT URL:

- http://13.127.120.228/reset_password/customer.php

AFFECTED PARAMETERS:

- Password reset

- Go to http://13.127.120.228/login/customer.php and you will see names of top customers as shown below, take note of any username.



13.127.120.228/login/customer.php

Lifestyle Store

Customer Login

Username

Password

Login

Forgot your password?

Don't have an account? Sign Up here!

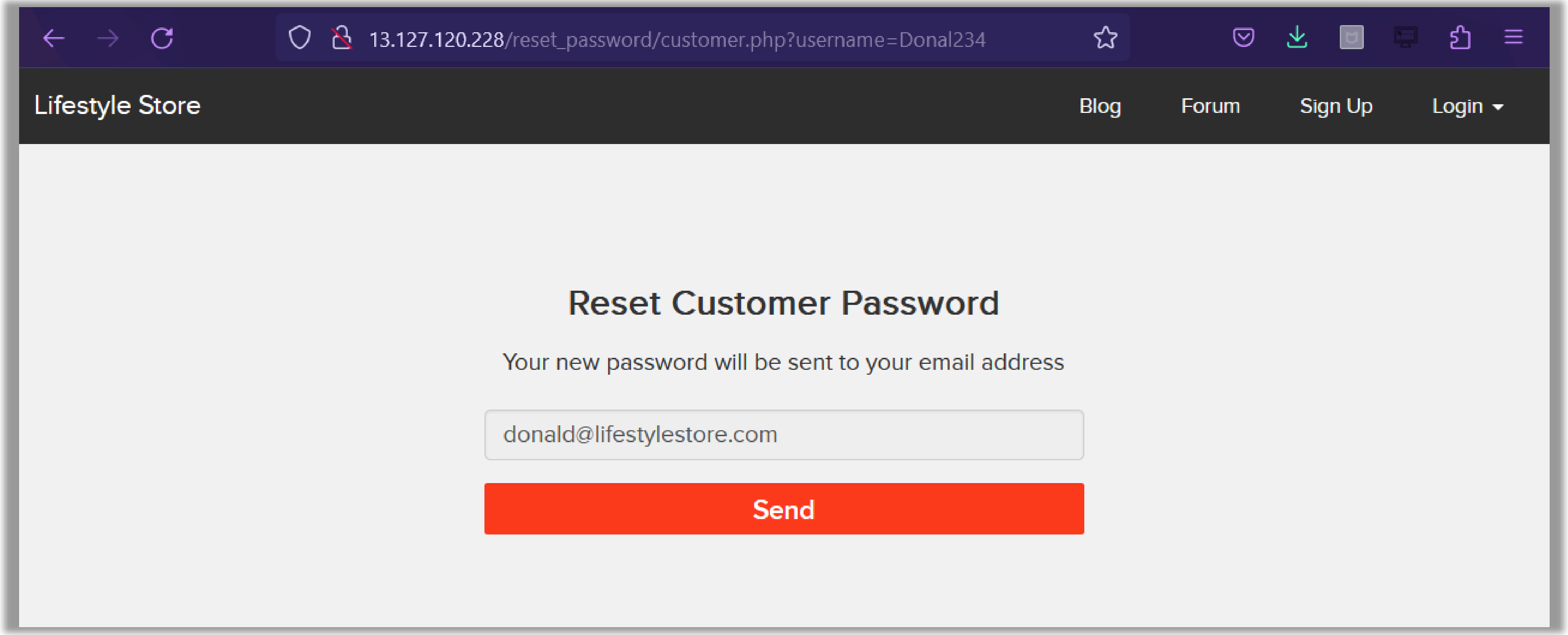
CUSTOMERS OF THE MONTH:

Donal234

Pluto98

Popeye786

- Now, click “forgot your password” and then input the memorized username and click “reset password”. We will see the interface like this, click send.



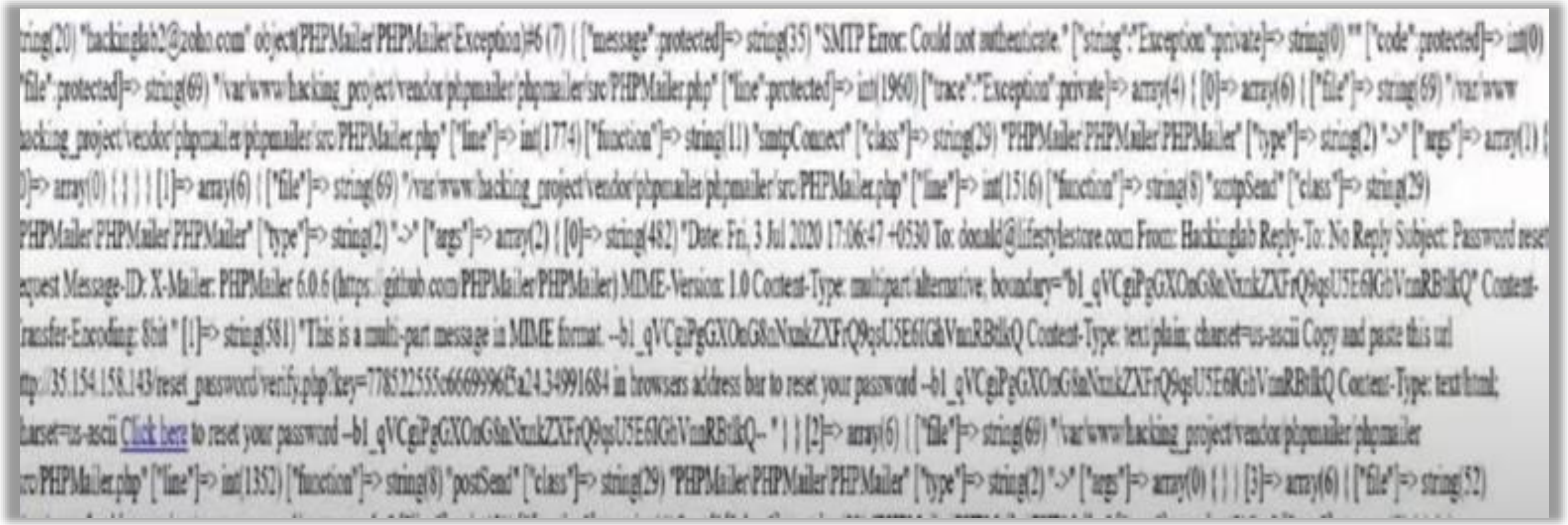
13.127.120.228/reset_password/customer.php?username=Donal234

Reset Customer Password

Your new password will be sent to your email address

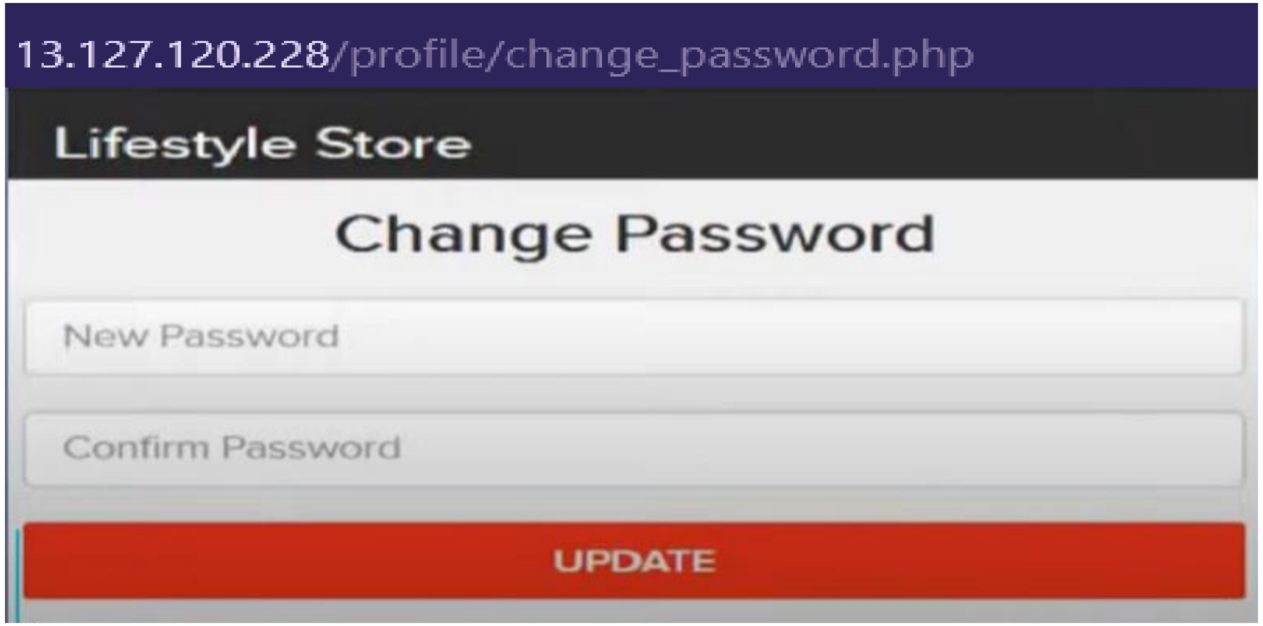
donald@lifestylestore.com

- When you click send you are directed to a page like this due to development/authentication error, “click here” button and you will be redirected to change password of the customer.



```
ring(20) "hackinglab2@zoho.com" object(PHPMailer\PHPMailer\Exception)#6 (7) { ["message":protected]=> string(35) "SMTP Error: Could not authenticate." ["string":"Exception":private]=> string(0) "" ["code":protected]=> int(0)
"file":protected]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line":protected]=> int(1960) ["trace":"Exception":private]=> array(4) { [0]=> array(6) { ["file"]=> string(69) "/var/www
acking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line"]=> int(1774) ["function"]=> string(11) "smtpConnect" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(1) {
0]=> array(0) { } } } [1]=> array(6) { ["file"]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line"]=> int(1516) ["function"]=> string(8) "smtpSend" ["class"]=> string(29)
PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(2) { [0]=> string(482) "Date: Fri, 3 Jul 2020 17:06:47 +0530 To: donald@lifestylestore.com From: Hackinglab Reply-To: No Reply Subject: Password reset
equest Message-ID: X-Mailer: PHPMailer 6.0.6 (https://github.com/PHPMailer/PHPMailer) MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="b1_qVCgiPgGXOnG8nNxnkZXFrQ9qsU5E6lGbVmRBtlkQ" Content-
ransfer-Encoding: 8bit " [1]=> string(581) "This is a multi-part message in MIME format. --b1_qVCgiPgGXOnG8nNxnkZXFrQ9qsU5E6lGbVmRBtlkQ Content-Type: text/plain; charset=us-ascii Copy and paste this url
ttp://35.154.158.143/reset_password/verify.php?key=778522555c66699965a24.34991684 in browsers address bar to reset your password --b1_qVCgiPgGXOnG8nNxnkZXFrQ9qsU5E6lGbVmRBtlkQ Content-Type: text/html;
harset=us-ascii Click here to reset your password --b1_qVCgiPgGXOnG8nNxnkZXFrQ9qsU5E6lGbVmRBtlkQ-- " } } [2]=> array(6) { ["file"]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer
src/PHPMailer.php" ["line"]=> int(1352) ["function"]=> string(8) "postSend" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(0) { } } [3]=> array(6) { ["file"]=> string(52)
```

- You will be redirected to change password of the customer id, and you will be automatically logged in to that customer’s account even if you don’t change the password, you can change the password for complete takeover of the customer id.



13.127.120.228/profile/change_password.php

Business impact:

The impact on the company
if the vulnerability is exploited.

Business Impact:

- The impact on the business is high, as a malicious hacker can get access to every user in the website and can login and perform tasks for their benefits and can also make the site vulnerable for security of customers.
- This will result in the defamation of the website as the users trust it.

Recommendations:

Take the following recommendations
to secure and avoid defacing/data altering.

Recommendations:

- Better authentication should be provided and re-direction site must be re-checked before action.
- There must be a proper authorization access

References:

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/11-Testing_Multi-Factor_Authentication

9. MULTIPLE VULNERABILITIES FOUND IN BLOG SITE (PII LEAKAGE, TEMPORRARY XSS AND MORE)

(SEVERE)

Parameters:
URL of the blog site: http://13.127.120.228/wondercms/

RELEVANT URL:

- http://13.127.120.228/wondercms/files/b374kmini.php

AFFECTED PARAMETERS:

- File upload (POST)

RELEVANT URL:

- http://13.127.120.228/wondercms/home

AFFECTED PARAMETERS:

- Files (GET)

RELEVANT URL:

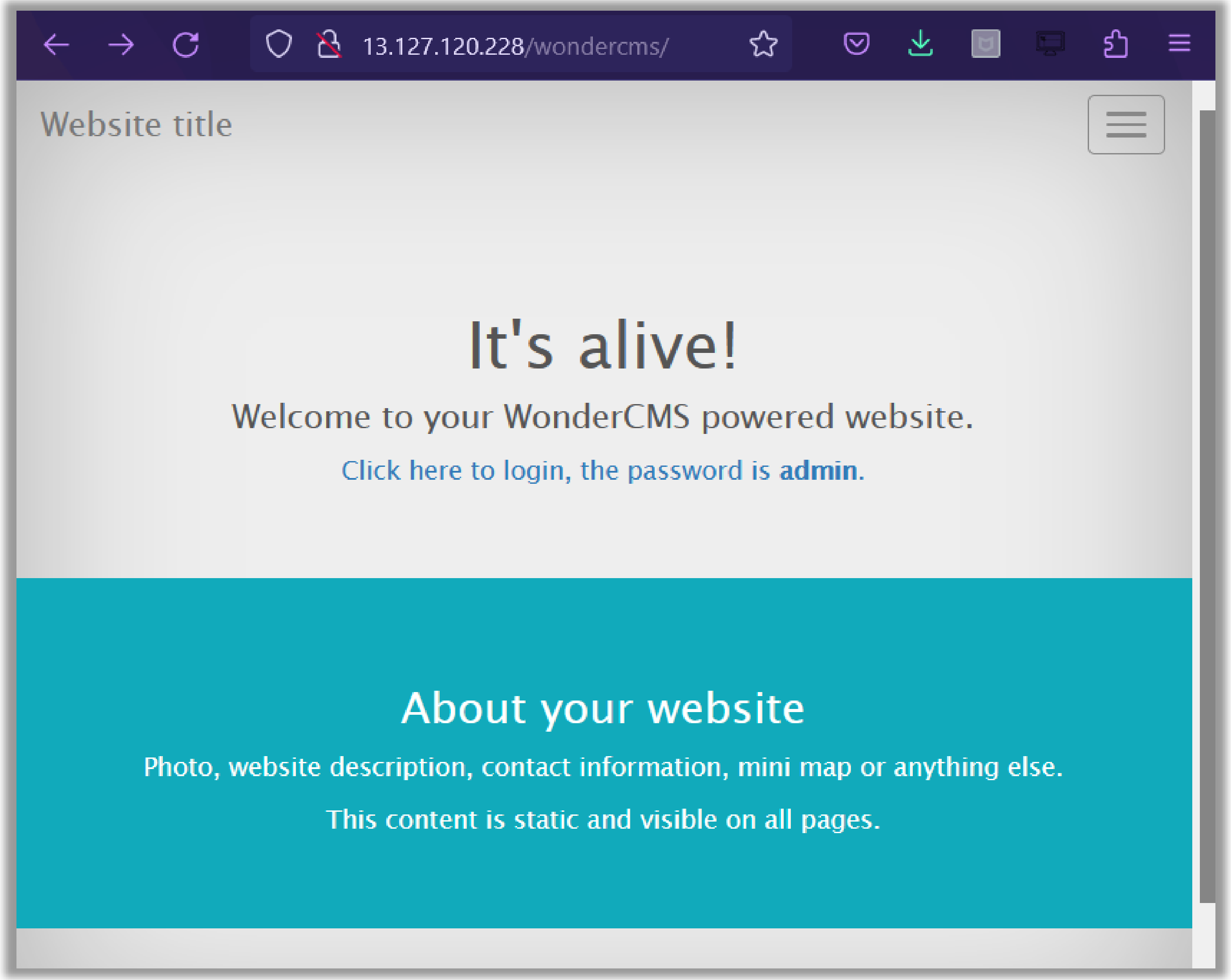
- http://13.127.120.228/wondercms/files/minisell.php

AFFECTED PARAMETERS:

- Shell upload

- At the front page of the blog site we can directly find the login option, that says “Click here to login, the password is admin” by clicking on it, it will redirect us to the login page where just by entering ‘admin’ as password one can get access to the admin account of this site.
- This is a proper example of server side misconfiguration.

- This is how the login page looks like.



13.127.120.228/wondercms/

Website title

It's alive!

Welcome to your WonderCMS powered website.

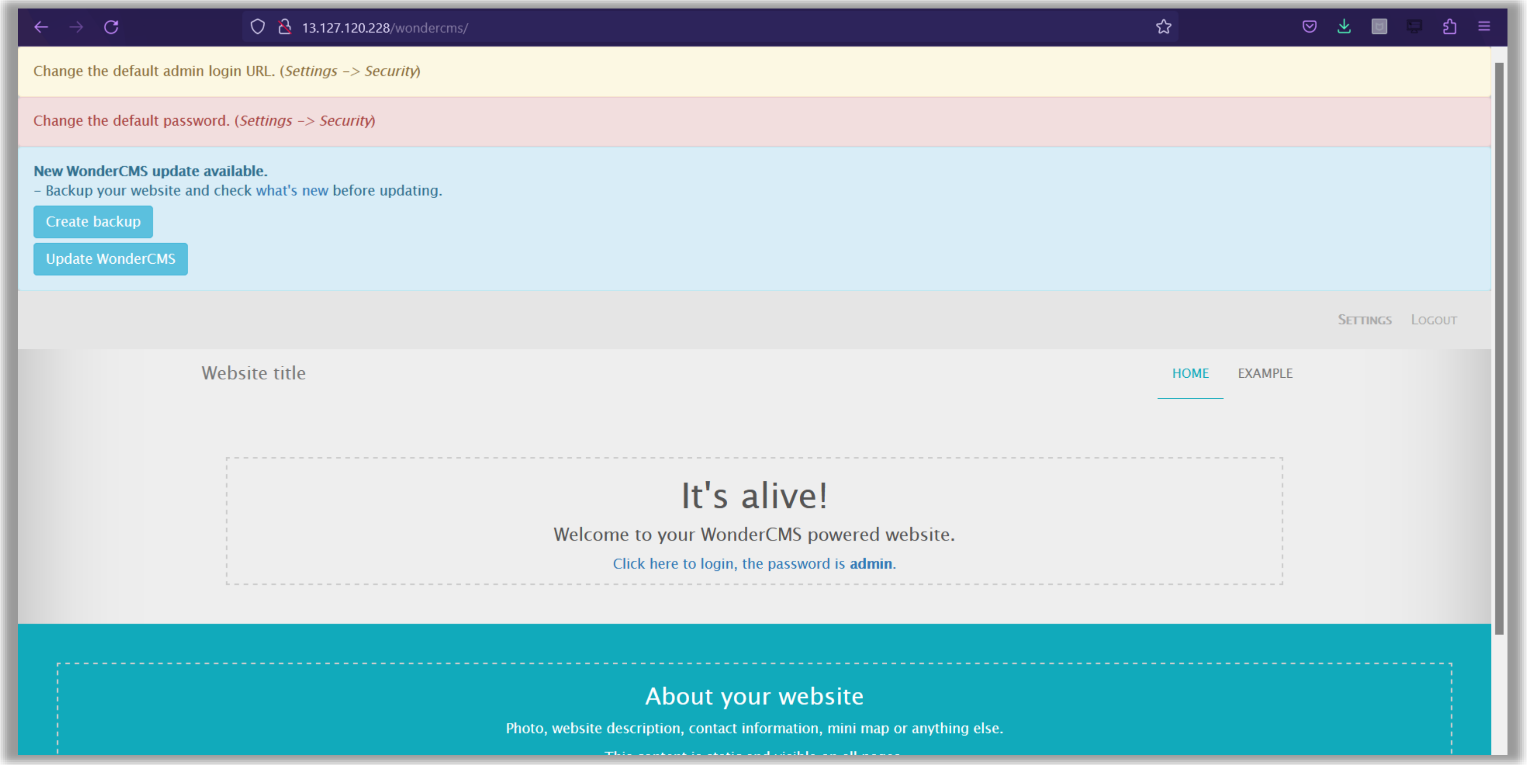
Click here to login, the password is **admin**.

About your website

Photo, website description, contact information, mini map or anything else.

This content is static and visible on all pages.

- When we log-in as the admin, at the first page of the site we can see some text written “It’s alive!.” If we click on it, the HTML code just starts running and a malicious hacker can easily make changes and can use the page as their phishing portal. This is a classic example of temporary XSS



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.

It's alive!

Welcome to your WonderCMS powered website.

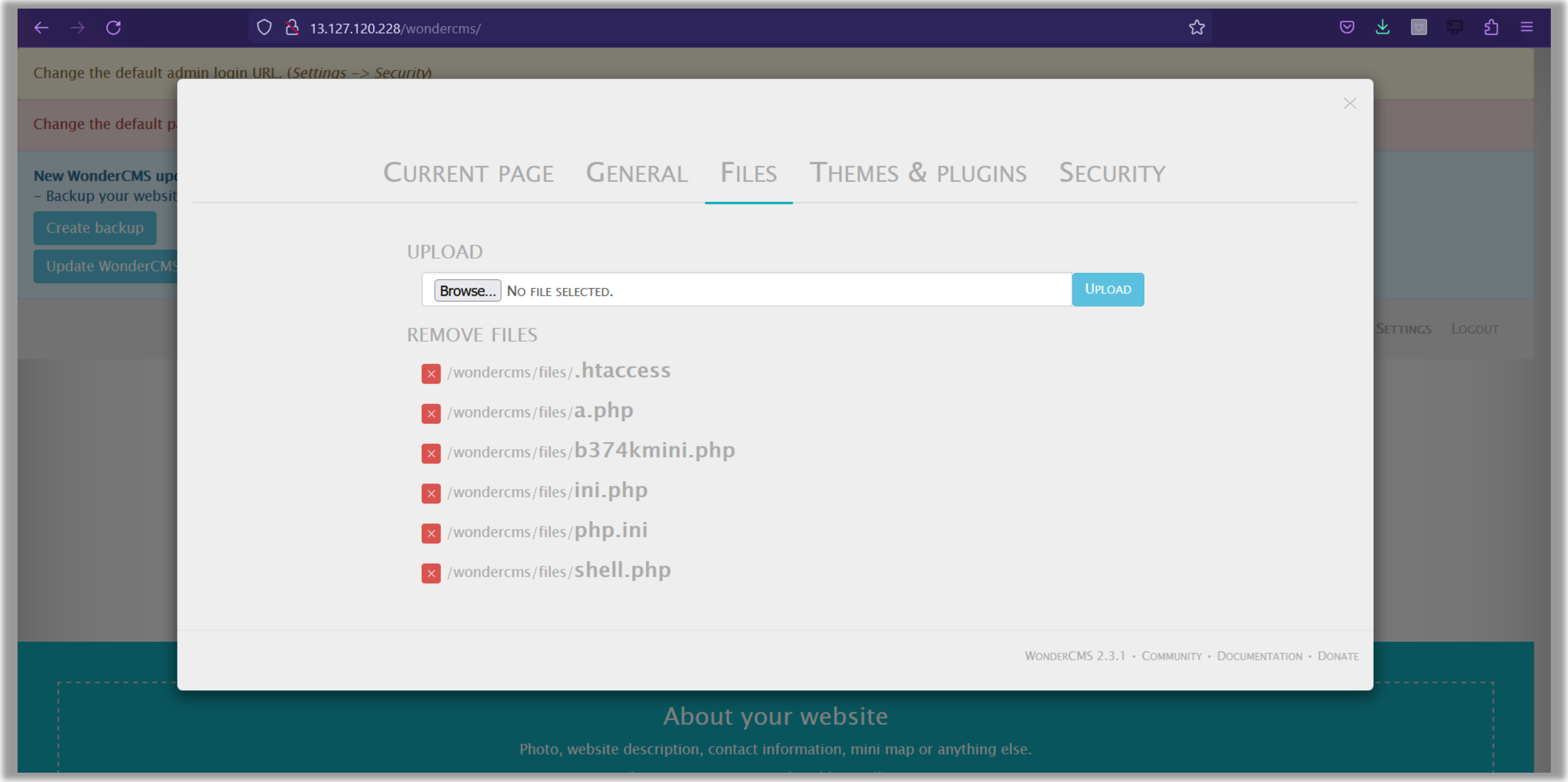
Click here to login, the password is **admin**.

About your website

Photo, website description, contact information, mini map or anything else.

This content is static and visible on all pages.

- As we are inside the admin account if we select the settings option and go to ‘files’ menu we can see some files with extension ‘.php’ which can give information about the site and also very much capable of taking over the site.
- Here, if we select the ‘/wondercms/files/b374kmini.php’ option, it will redirect us to a page which will give us many crucial information like server IP address, Linux IP address, the server type, the database, shell, the php info, uploads.
- The hacker can also mail someone with the admin compromising many factors one of which is the site reputation.



13.127.120.228/wondercms/

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

Change the default p

New WonderCMS up
– Backup your websit

Create backup
Update WonderCMS
Settings
Logout

CURRENT PAGE GENERAL FILES THEMES & PLUGINS SECURITY

UPLOAD

No file selected.

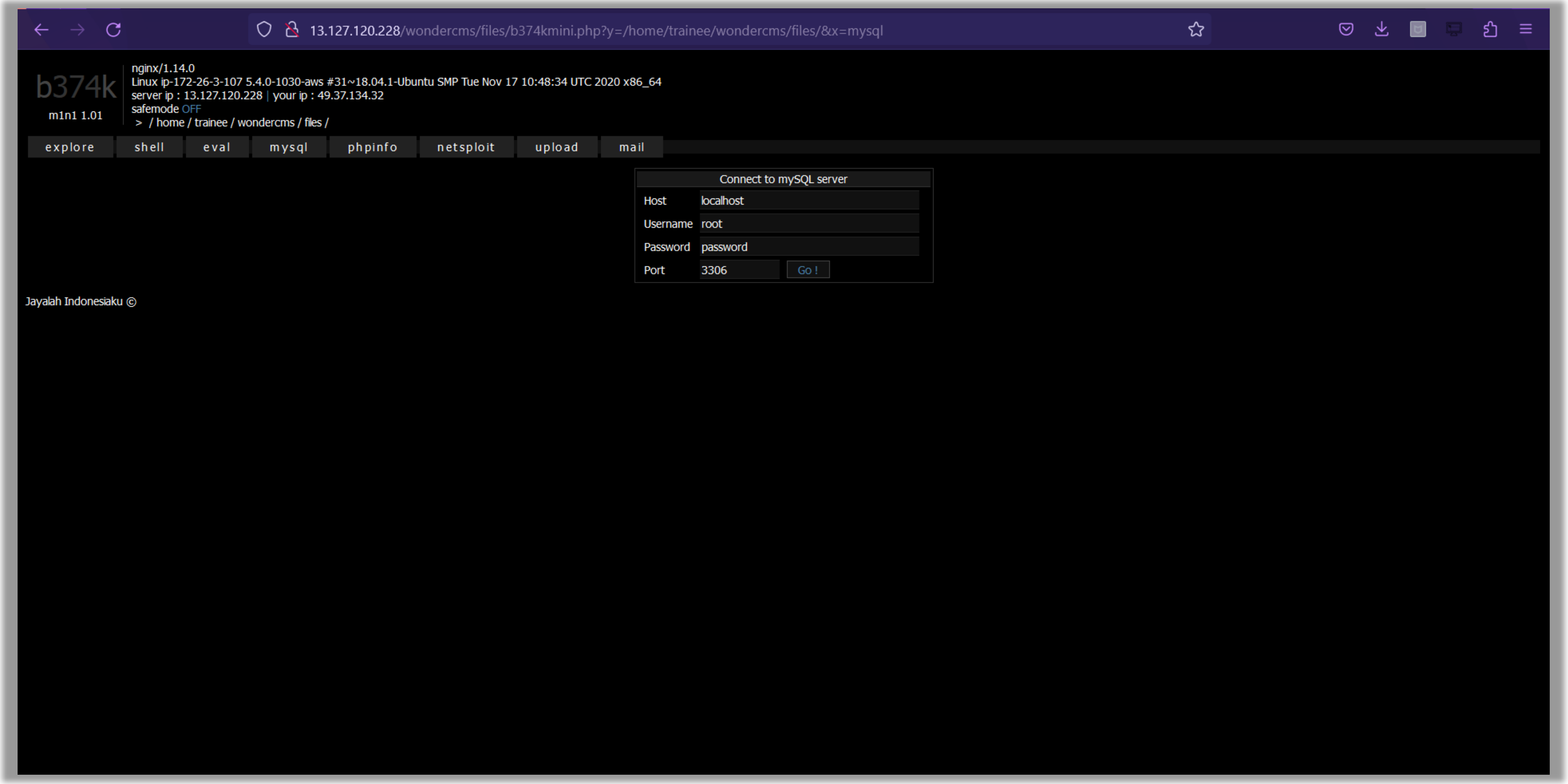
REMOVE FILES

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

WonderCMS 2.3.1 • Community • Documentation • Donate

About your website

Photo, website description, contact information, mini map or anything else.



13.127.120.228/wondercms/files/b374kmini.php?y=/home/trainee/wondercms/files/&x=mysql

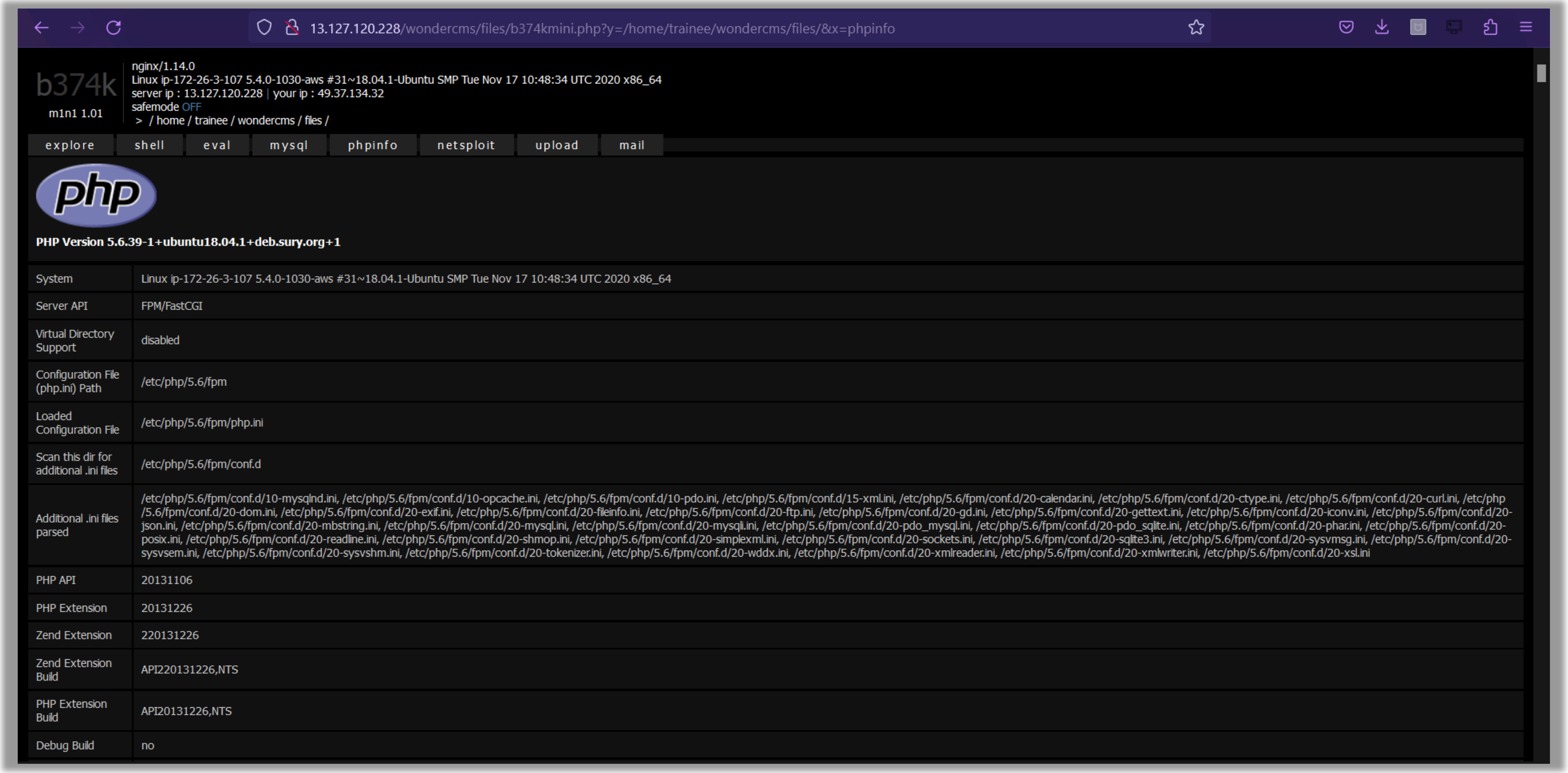
b374k
m1n1 1.01

nginx/1.14.0
Linux ip-172-26-3-107 5.4.0-1030-aws #31~18.04.1-Ubuntu SMP Tue Nov 17 10:48:34 UTC 2020 x86_64
server ip : 13.127.120.228 | your ip : 49.37.134.32
safemode OFF
> / home / trainee / wondercms / files /

Connect to mySQL server

Host	localhost
Username	root
Password	password
Port	3306

Jayalah Indonesiaku ©



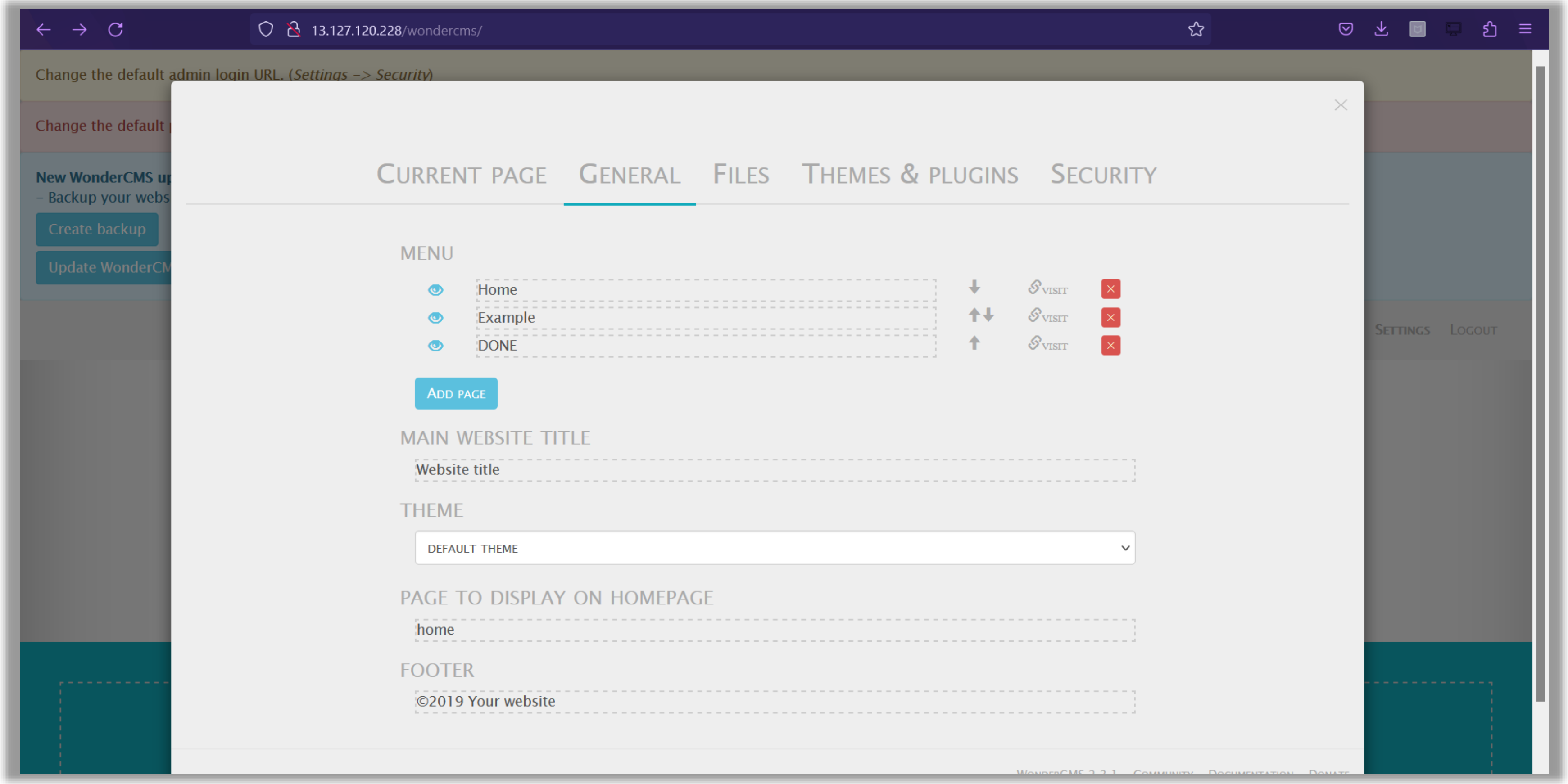
13.127.120.228/wondercms/files/b374kmini.php?y=/home/trainee/wondercms/files/&x=phpinfo

```
b374k     nginx/1.14.0
          Linux ip-172-26-3-107 5.4.0-1030-aws #31~18.04.1-Ubuntu SMP Tue Nov 17 10:48:34 UTC 2020 x86_64
m1n1 1.01 server ip : 13.127.120.228 | your ip : 49.37.134.32
          safemode OFF
           > / home / trainee / wondercms / files /
```

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

System	Linux ip-172-26-3-107 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

- When we are in the admin account and if we go to the general options found in the settings tab. We can see input fields, where a malicious hacker can inject and execute malicious client side scripts which gets permanently stored in the database.



13.127.120.228/wondercms/

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

Change the default

New WonderCMS up
– Backup your webs

MENU

Home

Example

DONE

MAIN WEBSITE TITLE

Website title

THEME

DEFAULT THEME

PAGE TO DISPLAY ON HOMEPAGE

home

FOOTER

©2019 Your website

- On the same page under settings, click on files here we have a file upload option , which has no limitations on the type of file which can be uploaded.
- We can upload files of any extension. Here, when we upload a shell into the site, it will give access to take over the whole website.
- This will be a great breakage of the site.

Business impact:

The impact on the company
if the vulnerability is exploited.

Business Impact:

- As the blog site has multiple vulnerabilities such as temporary XSS, server side errors and development flaws the site is extremely vulnerable as a malicious hacker can indulge in the site and can use all the vulnerable components to do phishing and other attacks on user and perform malicious activities.
- This will result in defamation of the name of the company, money loss and customers will never trust the website again.

Recommendations:

Take the following recommendations
to secure and avoid defacing/data altering.

Recommendations:

- The website should have proper two factor authentication.
- Try to develop the backend more stronger and secure.
- Remove all directory listings and add proper sanitization techniques at checks of the website.

References:

- https://cwe.mitre.org/data/definitions/548.html
- https://www.w3schools.com/

THANK YOU