Lifestyle Store

Detailed Developer Report

Security Status: Vulnerable

- Anyone can steal valuable data from Lifestyle Store(SQLi)
- Hacker can take complete control over the server(Shell upload and Weak passwords)
- Hacker can send multiple requests(Rate limiting flaw)
- Hacker can change the source code of the website to host malware, phishing or even clear content (Shell Upload)
- Hacker can get account details of customers like changing their address or phonr number in edit link(IDOR)
- Hacker can get seller information(PII)
- Hacker can add/remove products from cart(CSRF)
- Use of http instead of https

Vulnerability Status

Critical	Severe	Moderate	Low
06	13	08	02

Vulneabilities

Serial No	Status	Vulnerability	Count
1	Critical	SQL Injections	01
2	Critical	Arbitrary/Insecure File Upload	01
3	Critical	Admin Panel Access	01
4	Critical	Admin Access via OTP Bypass	01
5	Critical	Command Execution	02
6	Severe	Cross Site Scripting	02
7	Severe	Crypto Configuration Flaw	01
8	Severe	Common Passwords	02
9	Severe	Unauthorized availability of details	06
10	Severe	Open Redirections	02
11	Moderate	Information Disclosure by Default Pages	05
12	Moderate	Unnecessary Details about Seller	01
13	Moderate	Components with known Vulnerabities	02
14	Low	Default Error Display	02

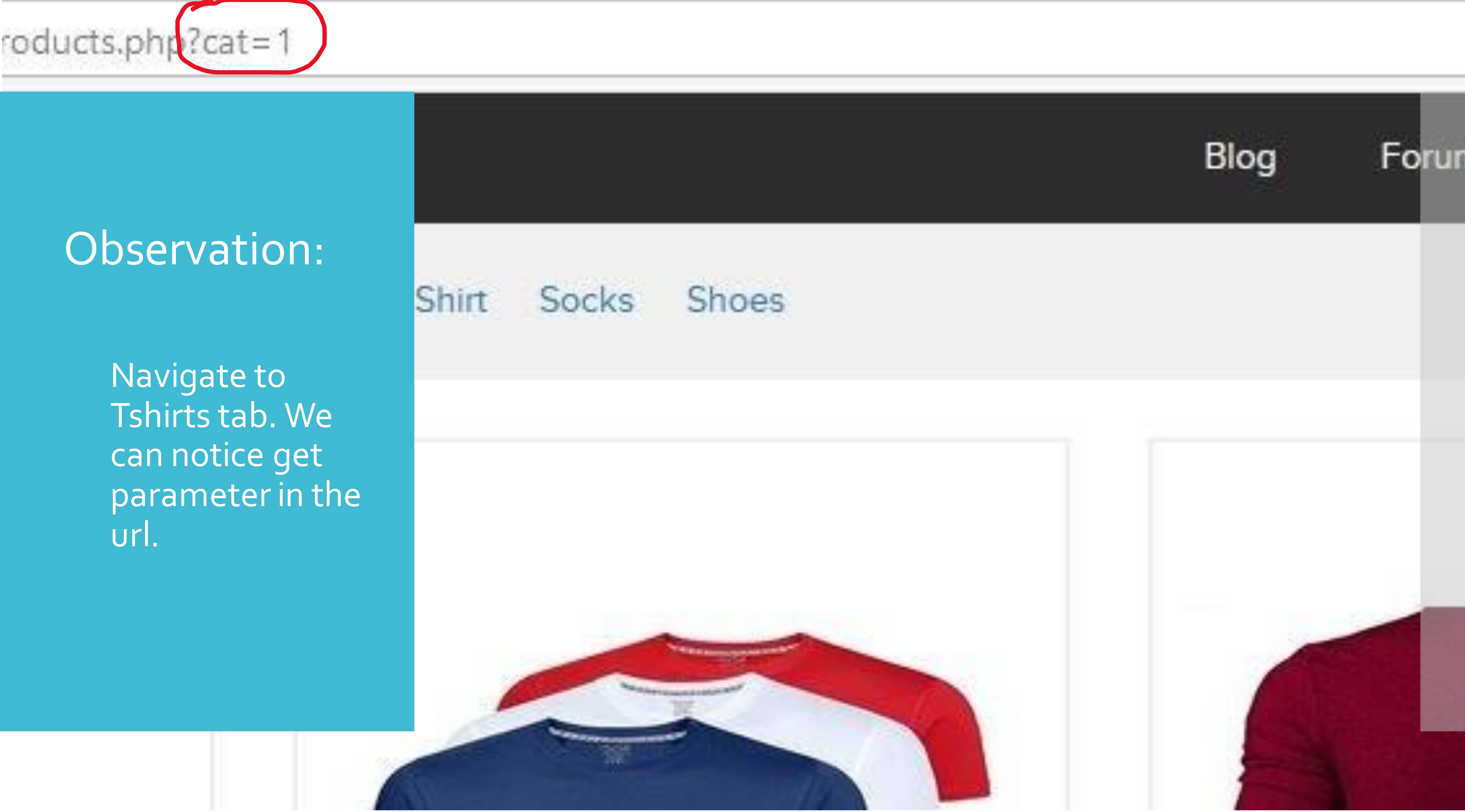
1. SQL Injection

It allows hacker to inject server side codes or commands. These are the flaws that allows a hacker to inject his own codes/commands into the web server that can provide illegal access to the data.

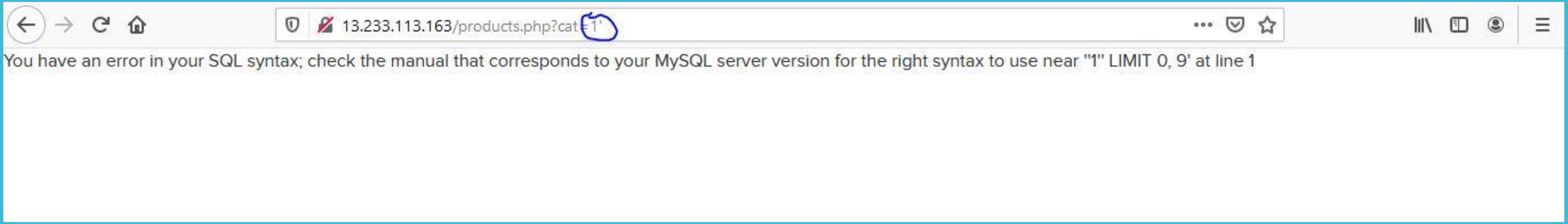
SQL Injection (Critical)	**URL mentioned below from Tshirt/Socks/Shoes module is vulnerable to SQLi** **URL:** http://3.6.92.171/products.php?cat=1 Parameter: Cat (GET Parameter) Payload: cat=1'

Observation:

Navigate to Tshirts tab. We can notice get parameter in the url.



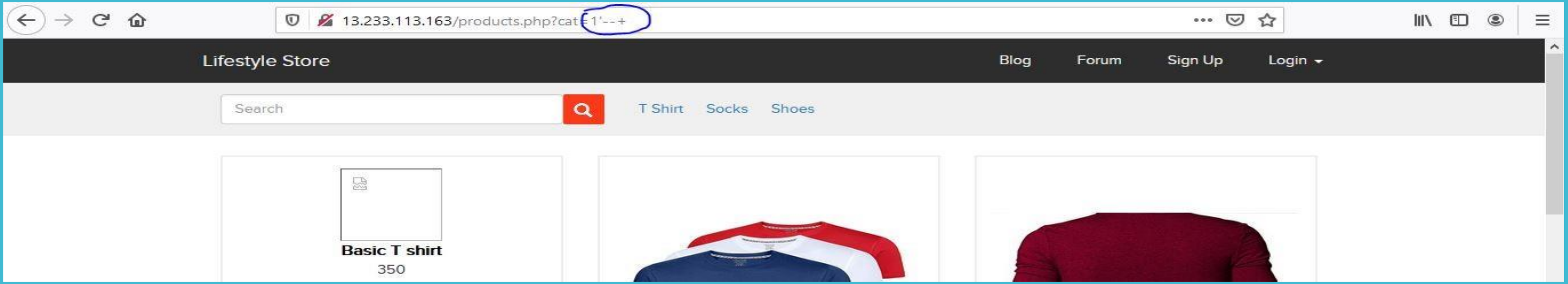
- We apply single quote at the end of the url ab observe that an error is displayed stating error in SQL syntax.



13.233.113.163/products.php?cat=1'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' LIMIT 0, 9' at line 1

- We then add '--+' after the single quote to check if the error is solved and since the error is solved we conclude the SQLi vulnerability.

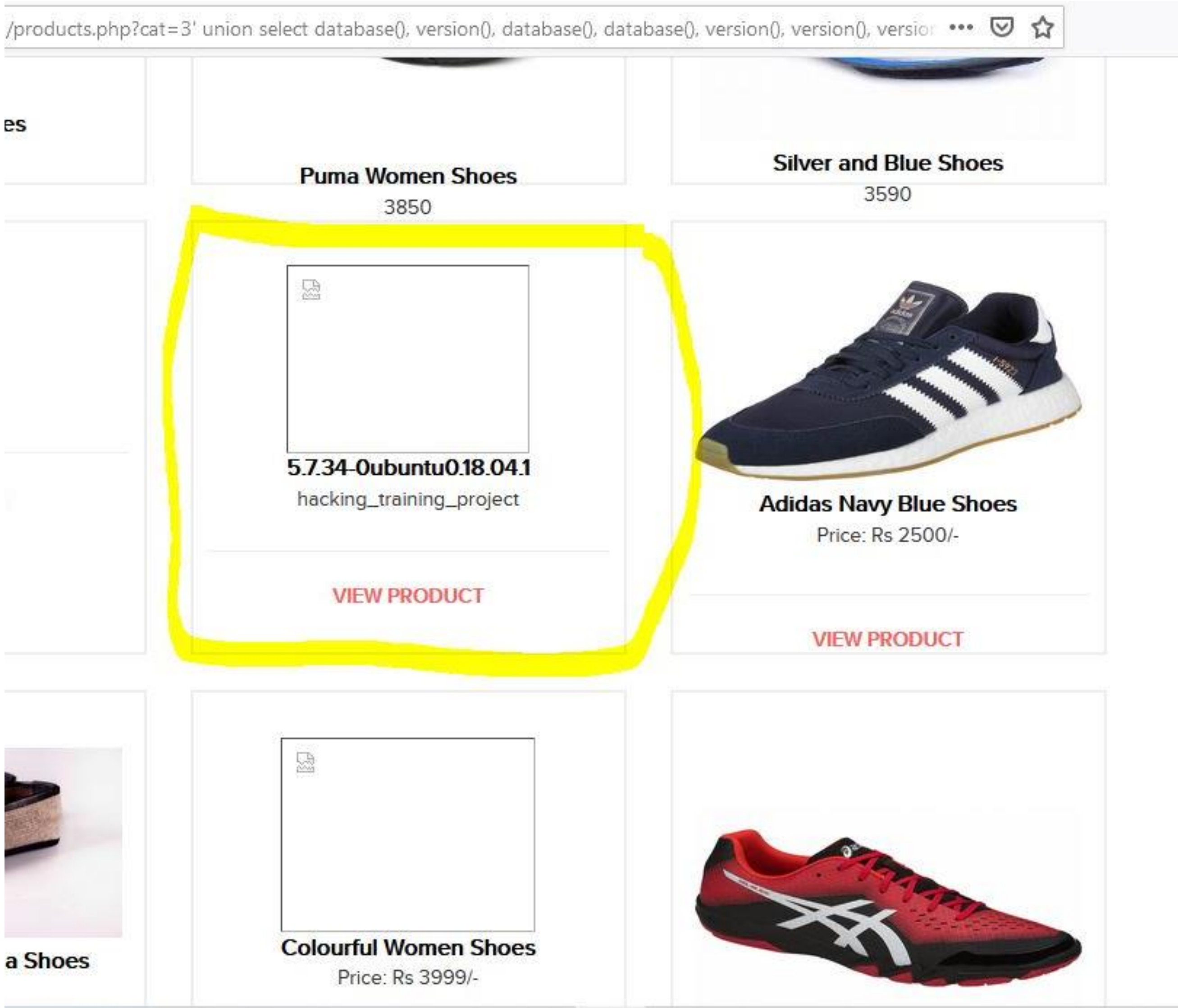


13.233.113.163/products.php?cat=1'--+

PoC (Proof of Concept):

Attacker can now execute SQL commands in the URL to extract sensetive data.

http://13.233.148.87/products.php?cat=3%27%20union%20select%20database(),version(),database(),database(),version(),version(),version()--+



/products.php?cat=3' union select database(), version(), database(), database(), version(), version(), versior

es

Puma Women Shoes
3850

Silver and Blue Shoes
3590

5.7.34-0ubuntu0.18.04.1
hacking_training_project

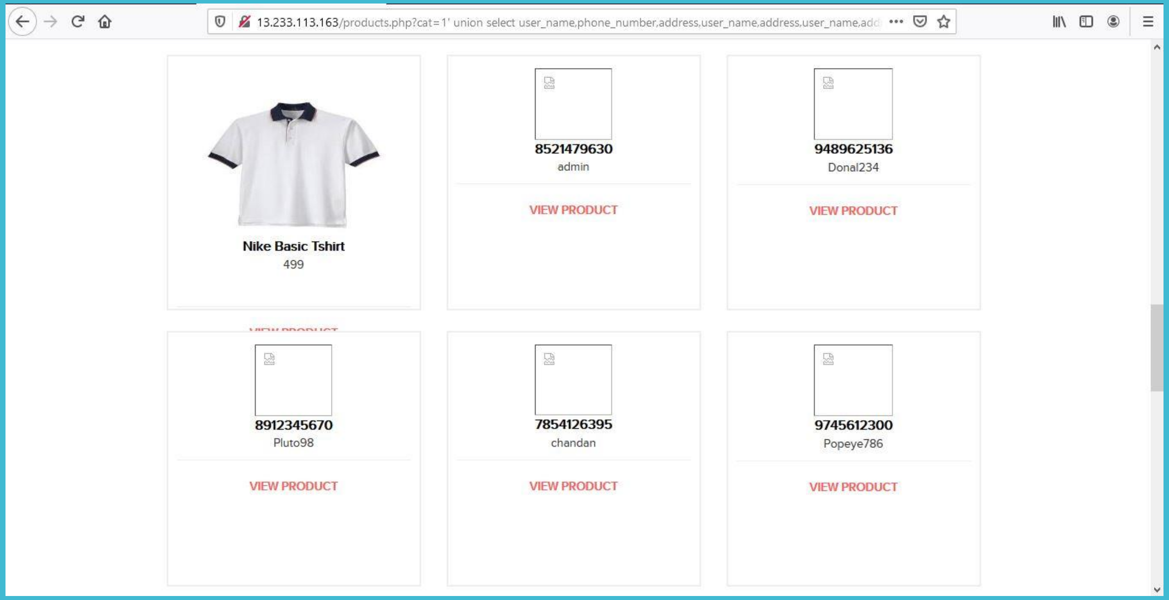
VIEW PRODUCT

Adidas Navy Blue Shoes
Price: Rs 2500/-

VIEW PRODUCT

a Shoes

Colourful Women Shoes
Price: Rs 3999/-



13.233.113.163/products.php?cat=1' union select user_name,phone_number,address,user_name,address,user_name,add

Nike Basic Tshirt
499

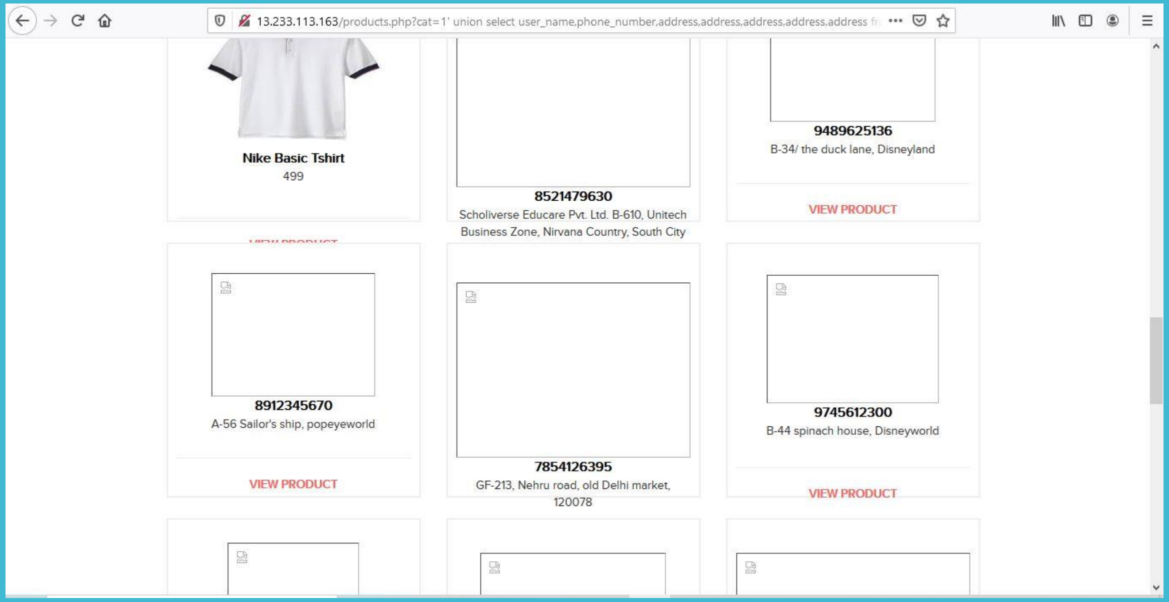
8521479630
admin
VIEW PRODUCT

9489625136
Donal234
VIEW PRODUCT

8912345670
Pluto98
VIEW PRODUCT

7854126395
chandan
VIEW PRODUCT

9745612300
Popeye786
VIEW PRODUCT



13.233.113.163/products.php?cat=1' union select user_name,phone_number,address,address,address,address,address fr

Nike Basic Tshirt
499

8521479630
Scholiverse Educare Pvt. Ltd. B-610, Unitech Business Zone, Nirvana Country, South City

9489625136
B-34/ the duck lane, Disneyland
VIEW PRODUCT

8912345670
A-56 Sailor's ship, popeyeworld
VIEW PRODUCT

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

9745612300
B-44 spinach house, Disneyworld
VIEW PRODUCT

Business Impact:

- 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.

Recommendations:

- **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 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

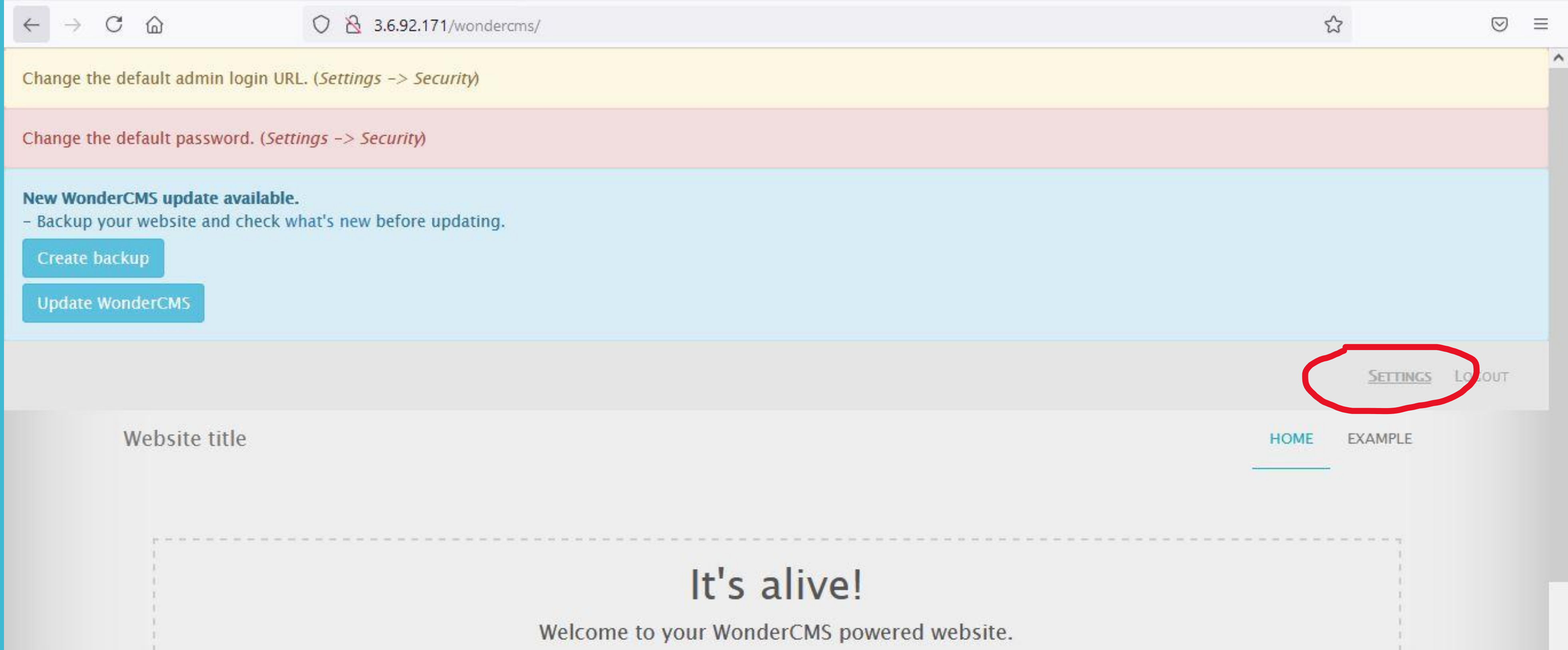
2. Arbitrary/Insecure File Upload:

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.

Arbitrary/Insecure File Upload (Critical)	The attacker can upload insecure shells or files and gain access over the entire database and login as the admin. URL: http://3.6.92.171/wondercms/ Parameter: File Upload (POST Parameter)

Observation:

- Login using any of the user’s details on the Lifestyle store and navigate to Blog tab . Now click on Login and put the password - admin.
- We can see the following page and then click on Settings tab.



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

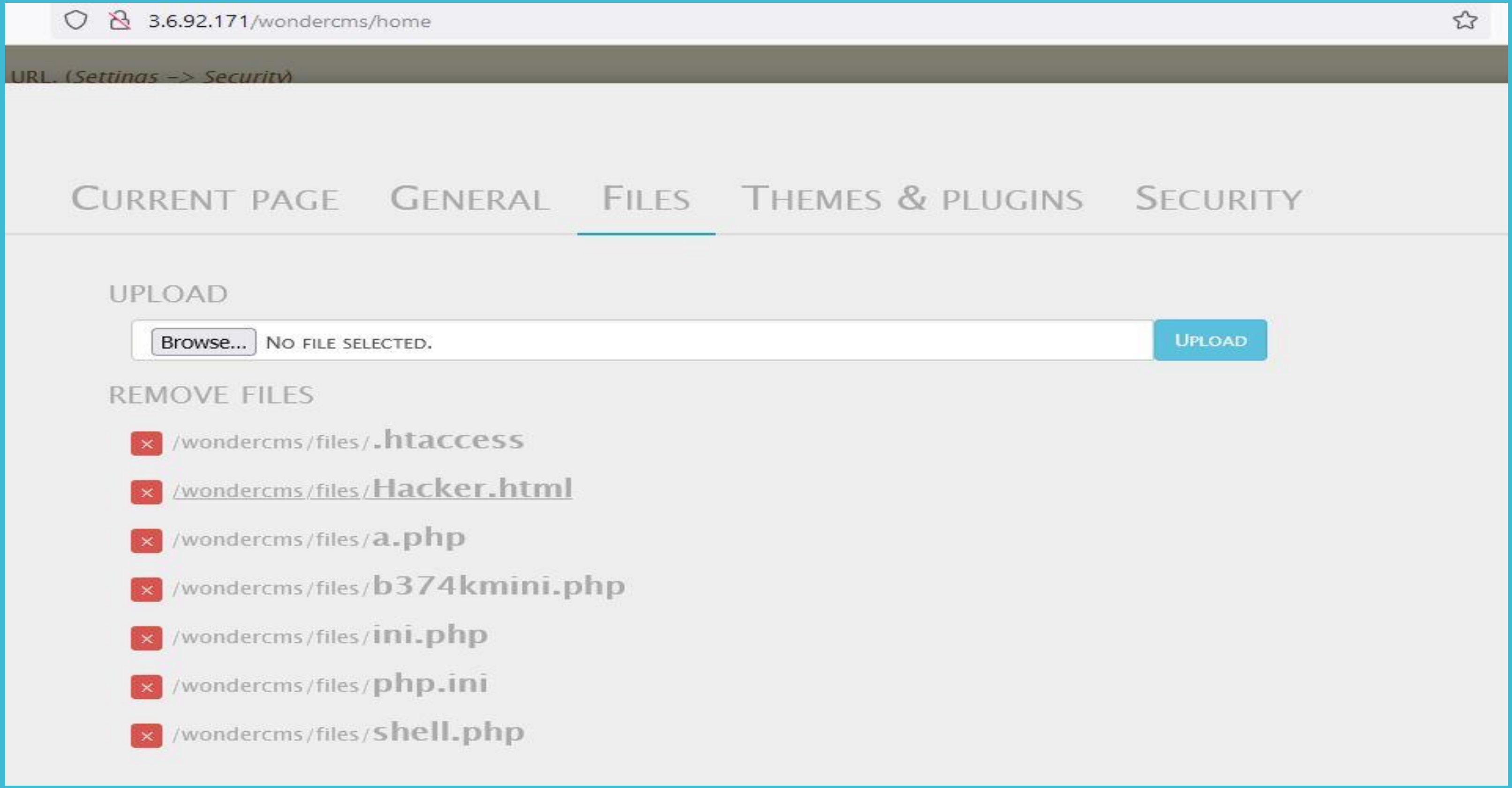
Change the default password. (*Settings -> Security*)

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

It's alive!

Welcome to your WonderCMS powered website.

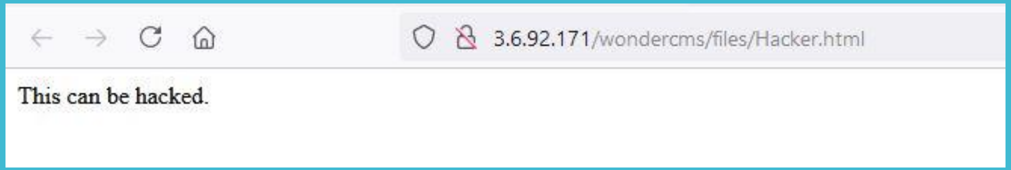
- Click on Files. Here attacker can upload any file as shown below.



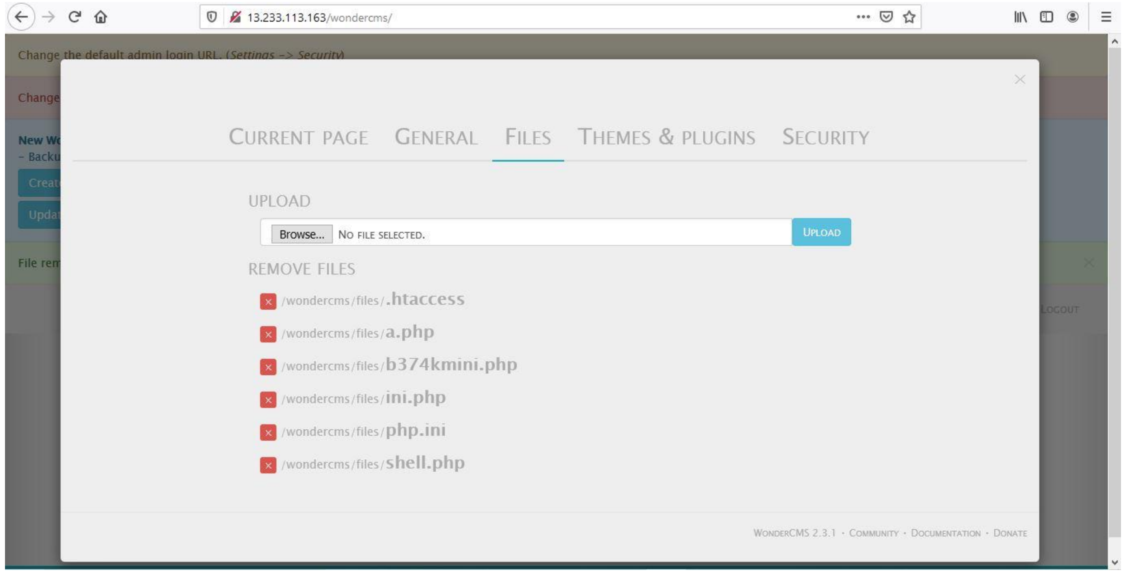
No file selected.

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

- Click on Hacker.html to open the file.



This can be hacked.



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

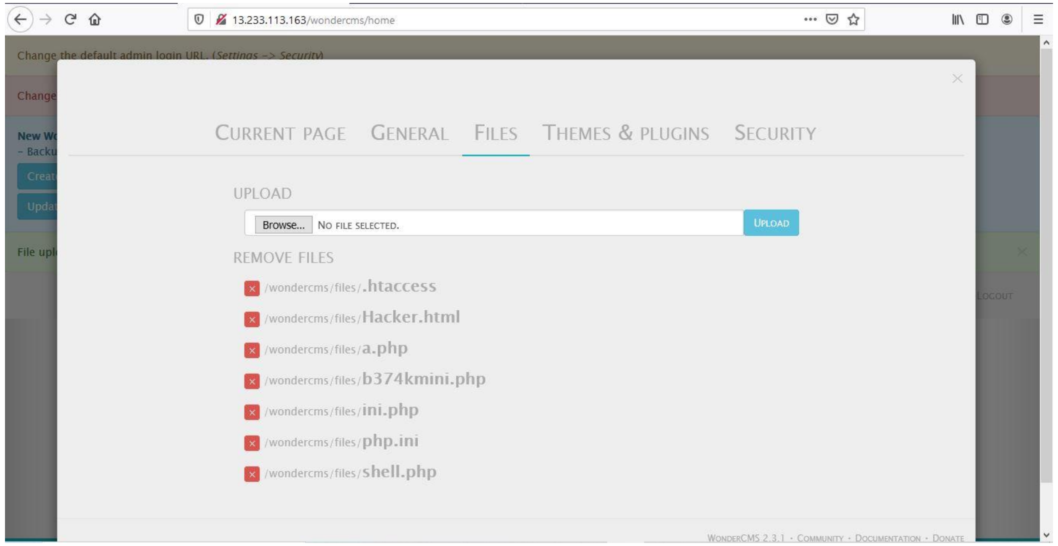
UPLOAD

No file selected.

REMOVE FILES

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

WonderCMS 2.3.1 · Community · Documentation · Donate



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

UPLOAD

No file selected.

REMOVE FILES

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

WonderCMS 2.3.1 · Community · Documentation · Donate

PoC (Proof of Concept):

Weak Password: admin
Arbitrary File Inclusion

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:

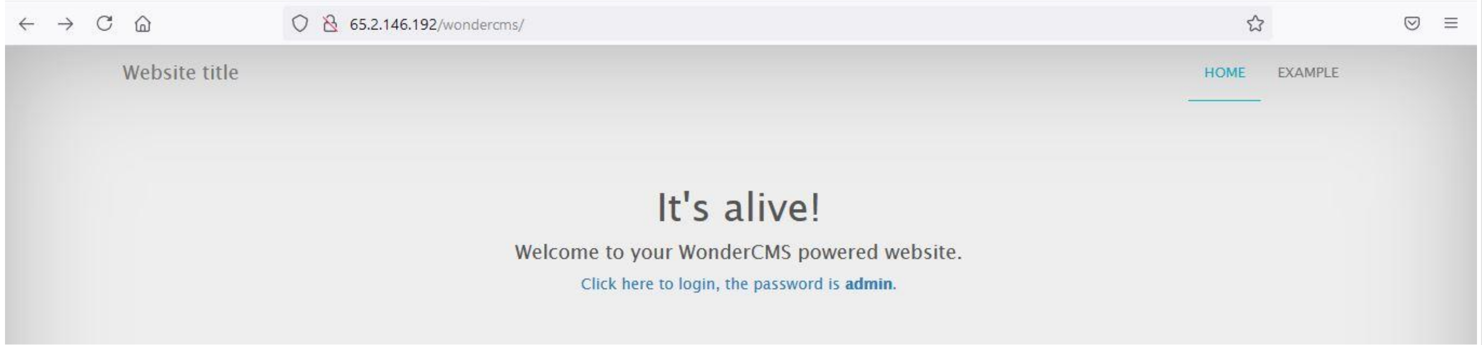
- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://www.opswat.com/blog/file-upload-protection-best-practices

3. Admin Panel Access:

Access to Admin Panel (Critical)	Below mentioned URL is vulnerable to Arbitrary File Upload and making other admin level changes. URL: http://3.6.92.171/wondercms/loginURL

Observation:

When we navigate to http://35.154.145.178/wondercms/ we can see we are already given the login password as admin.



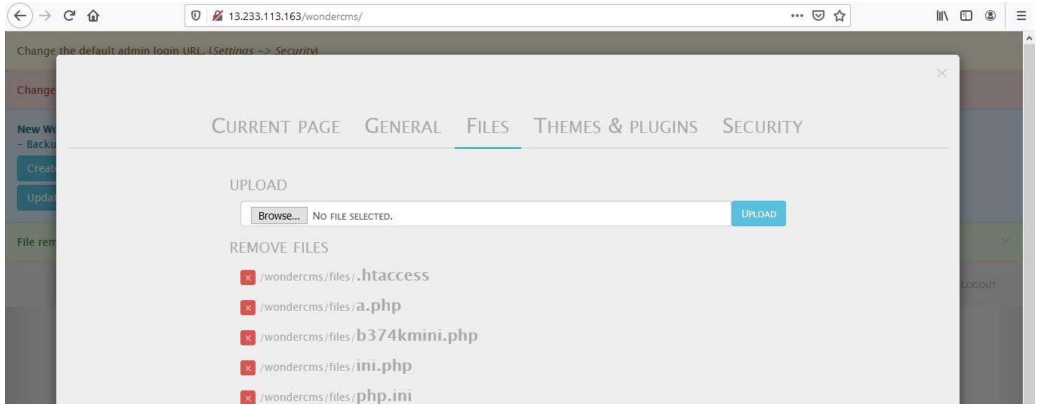
It's alive!

Welcome to your WonderCMS powered website.

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

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.



13.233.113.163/wondercms/

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

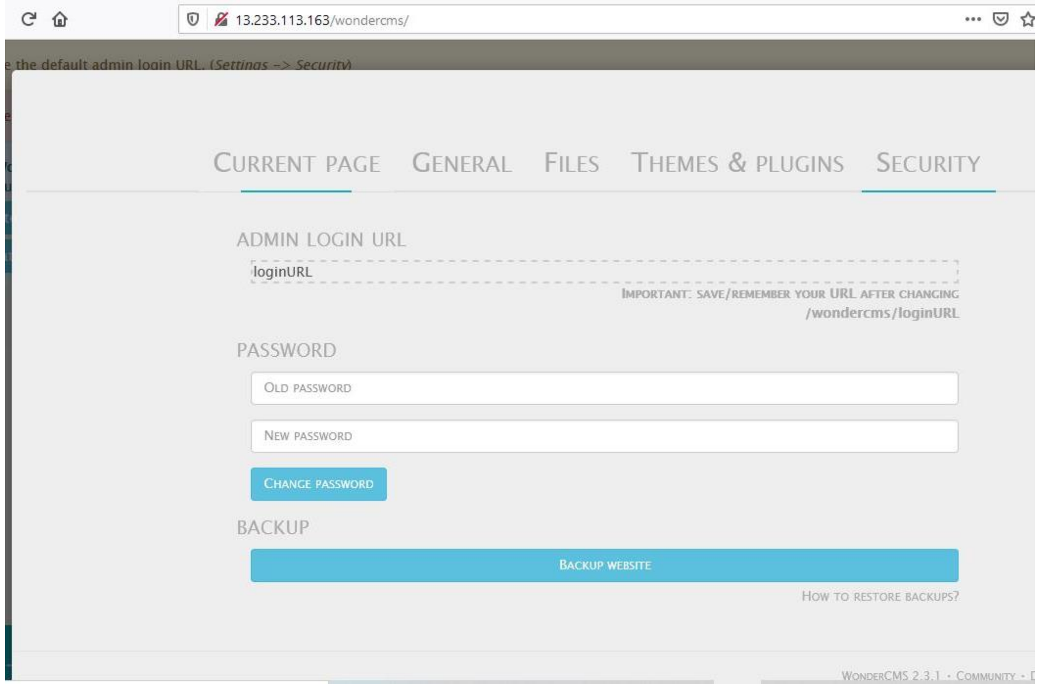
/wondercms/files/.htaccess

/wondercms/files/a.php

/wondercms/files/b374kmini.php

/wondercms/files/ini.php

/wondercms/files/php.ini



13.233.113.163/wondercms/

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

Admin login URL: loginURL

Important: save/remember your URL after changing /wondercms/loginURL

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 it is 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:

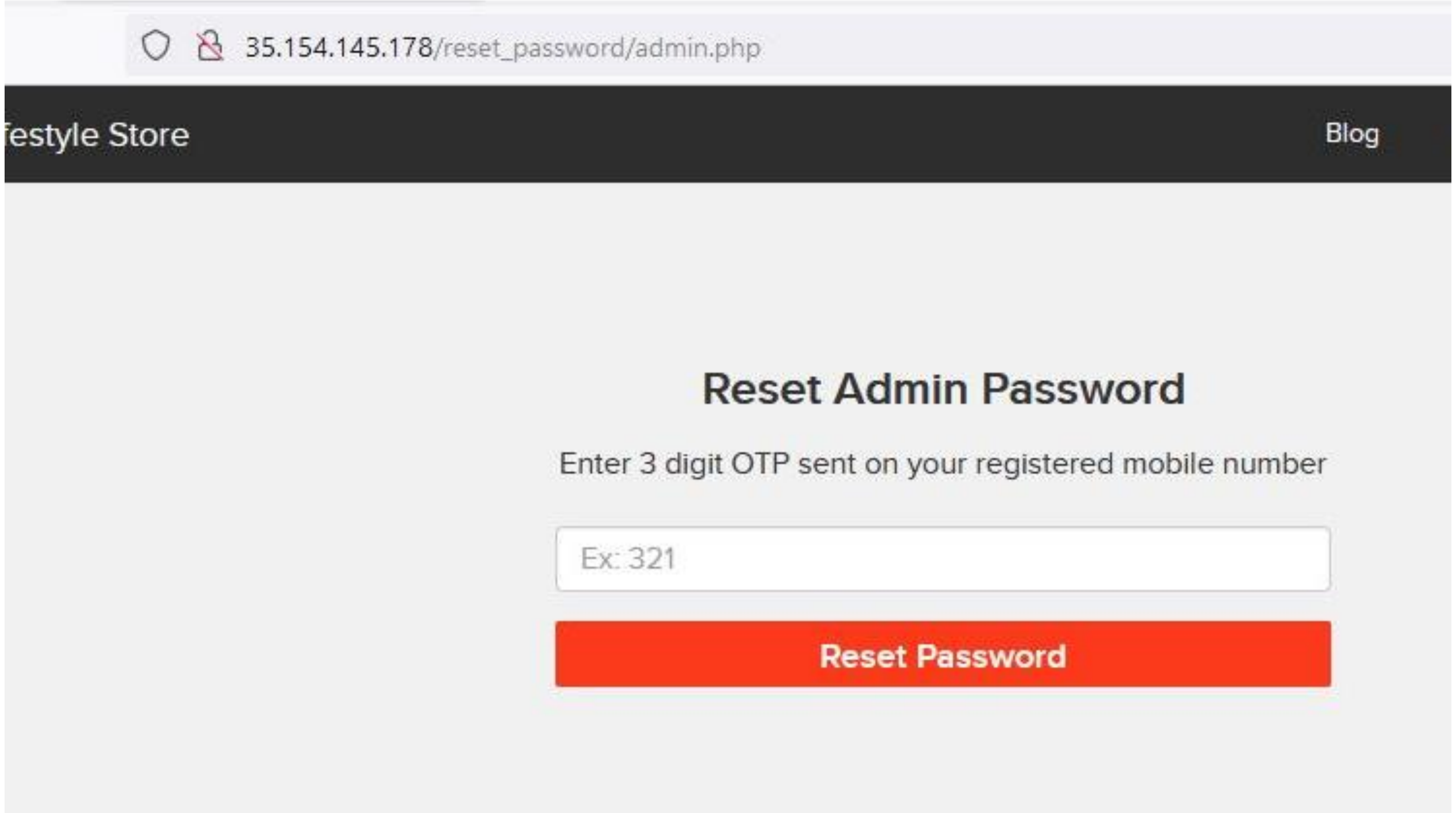
- https://www.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009)
- https://www.owasp.org/index.php/Default_Passwords
- https://www.us-cert.gov/ncas/alerts/TA13-175A

4. Admin 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. URL: http://35.154.145.178/reset_password/admin.php Parameters: OTP (GET Parameters) Payload Used: 352

Observation:

Navigate to http://35.154.145.178/reset_password/admin.php We will see reset password page via OTP. Enter random OTP while capturing requests in a local proxy .



35.154.145.178/reset_password/admin.php

Reset Admin Password

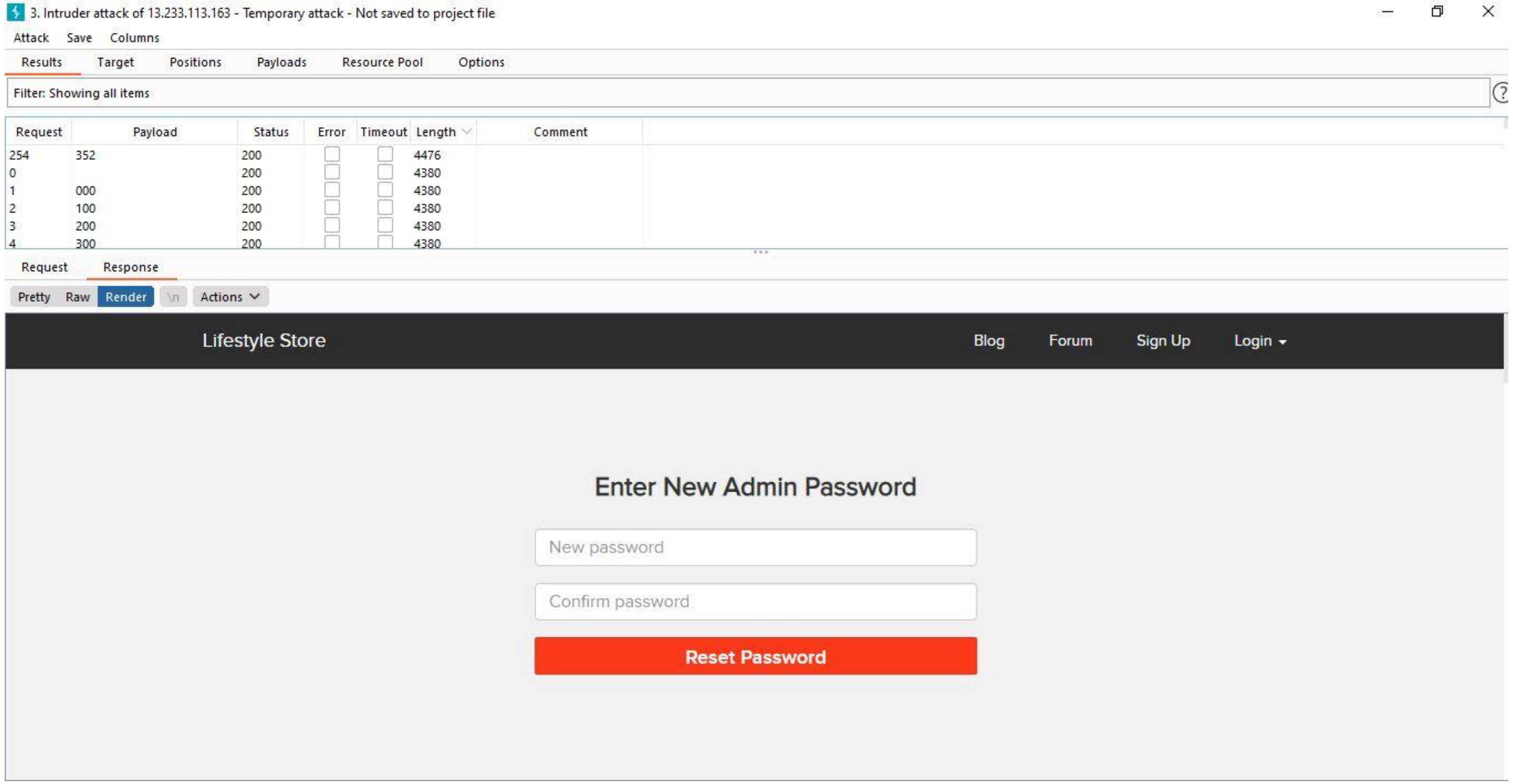
Enter 3 digit OTP sent on your registered mobile number

Ex: 321

Reset Password

On brute forcing the 3 digit OTP , under the length column the value which is distinct from others yields the correct OTP - 352.

Enter this OTP in the captured request.



3. Intruder attack of 13.233.113.163 - Temporary attack - Not saved to project file

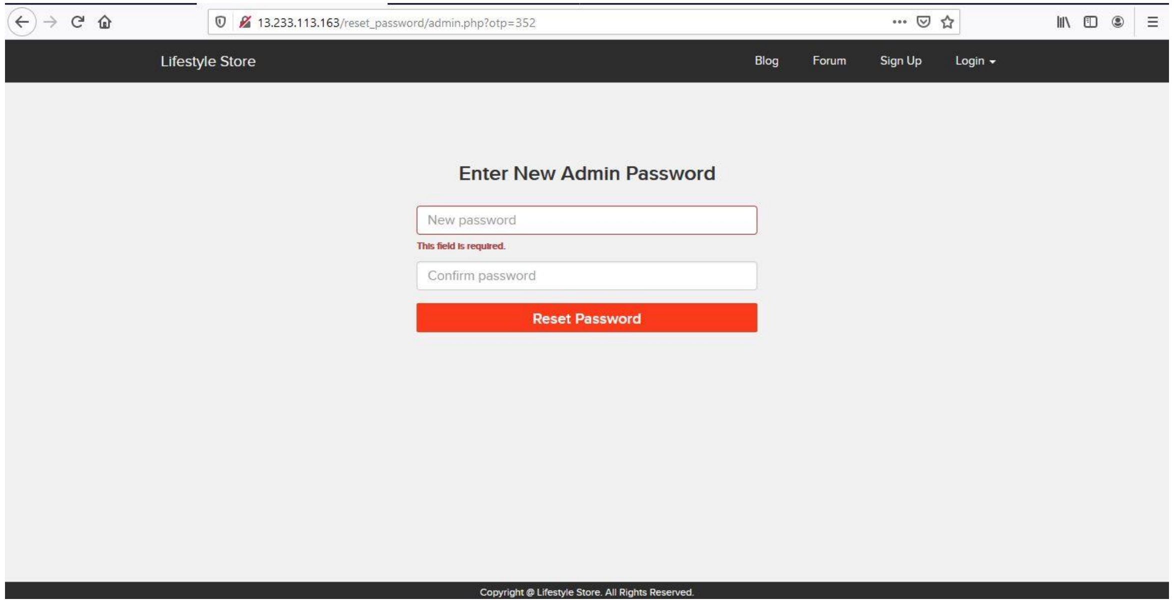
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
254	352	200	□	□	4476	
0		200	□	□	4380	
1	000	200	□	□	4380	
2	100	200	□	□	4380	
3	200	200	□	□	4380	
4	300	200	□	□	4380	

Enter New Admin Password

- After entering the OTP in the captured request forward the same and we will be redirected to new password page in browser.

  Navigate to http://35.154.145.178/login/admin.php and enter the new password and username as admin.



13.233.113.163/reset_password/admin.php?otp=352

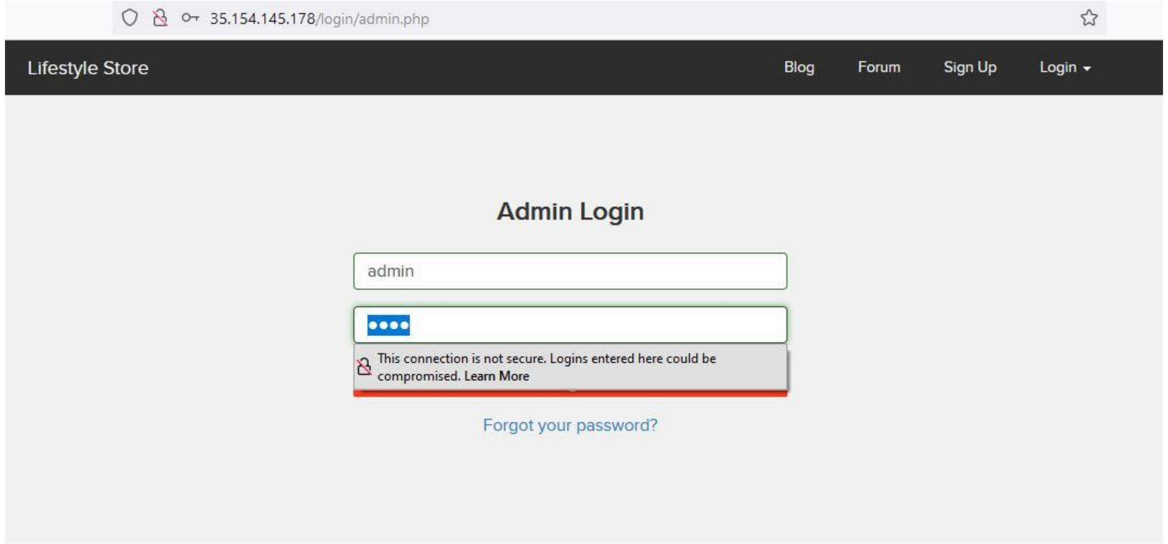
Enter New Admin Password

New password

This field is required.

Confirm password

Copyright @ Lifestyle Store. All Rights Reserved.



35.154.145.178/login/admin.php

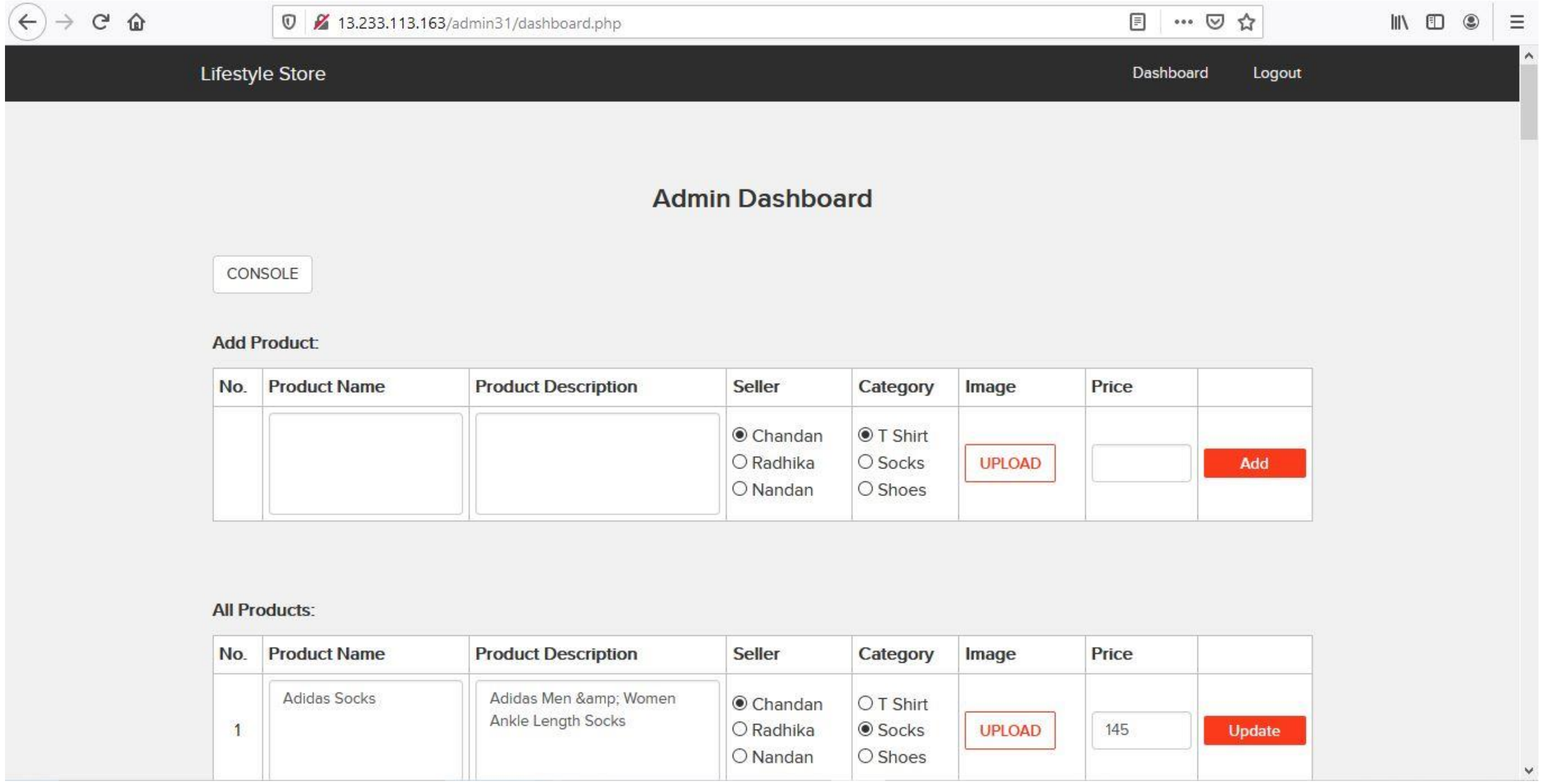
Admin Login

admin

••••

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

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



13.233.113.163/admin31/dashboard.php

Lifestyle Store

Admin Dashboard

CONSOLE

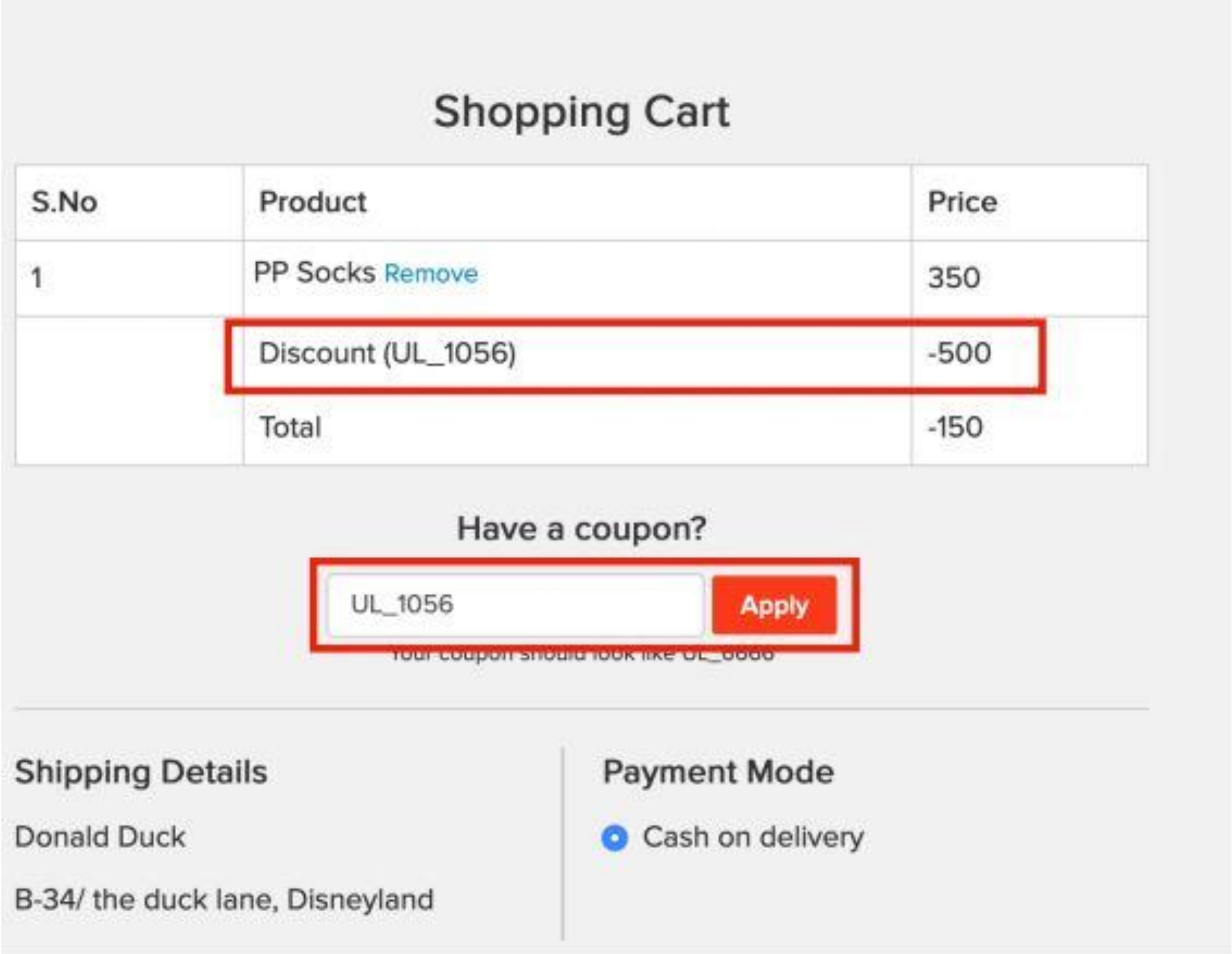
Add Product:

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

PoC (Proof of Concept)



Shopping Cart

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

Have a coupon?

Your coupon should look like UL_0000

Shipping Details

Donald Duck

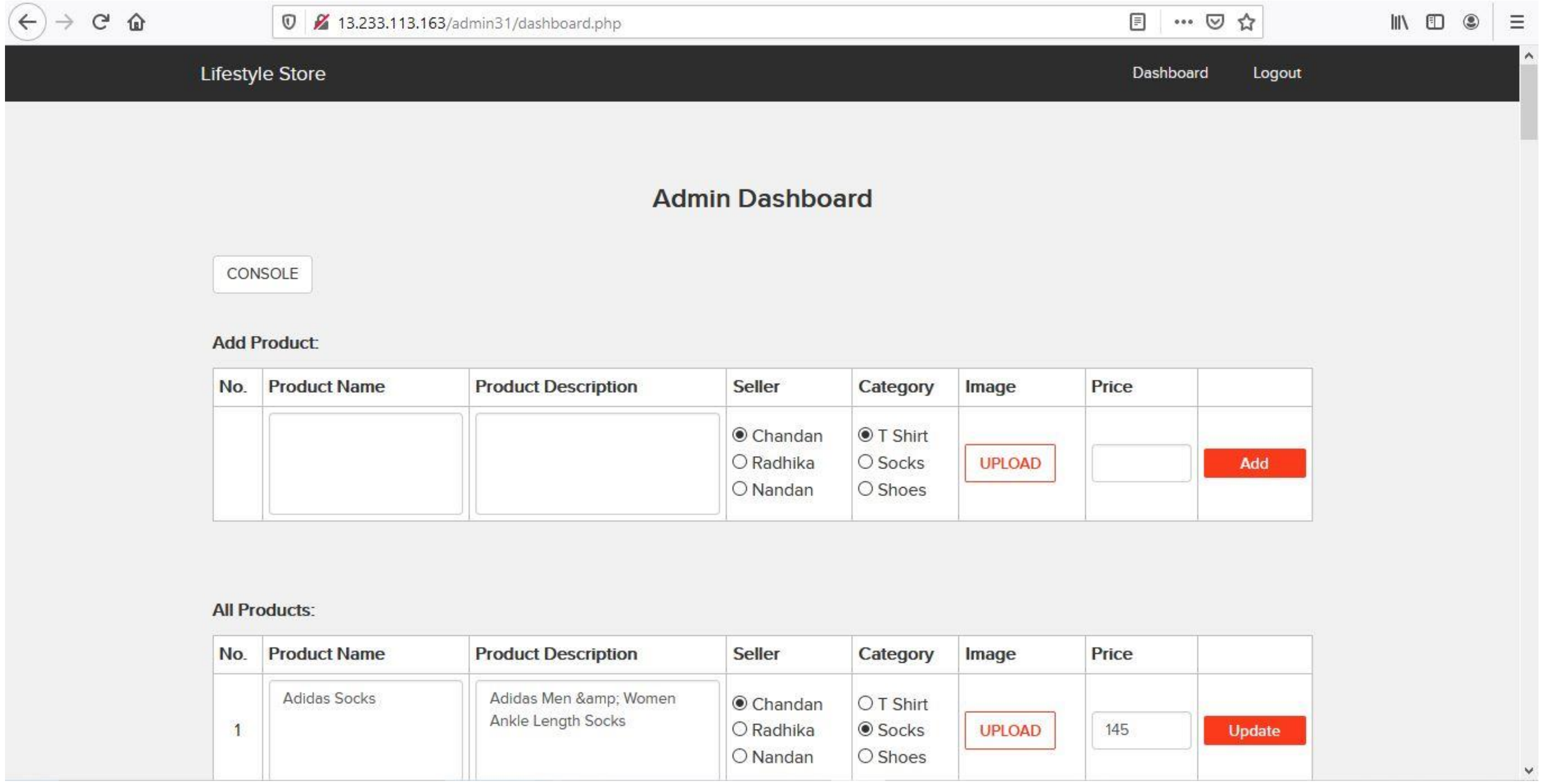
B-34/ the duck lane, Disneyland

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.



Admin Dashboard

CONSOLE

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

Recommendation:

- 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:

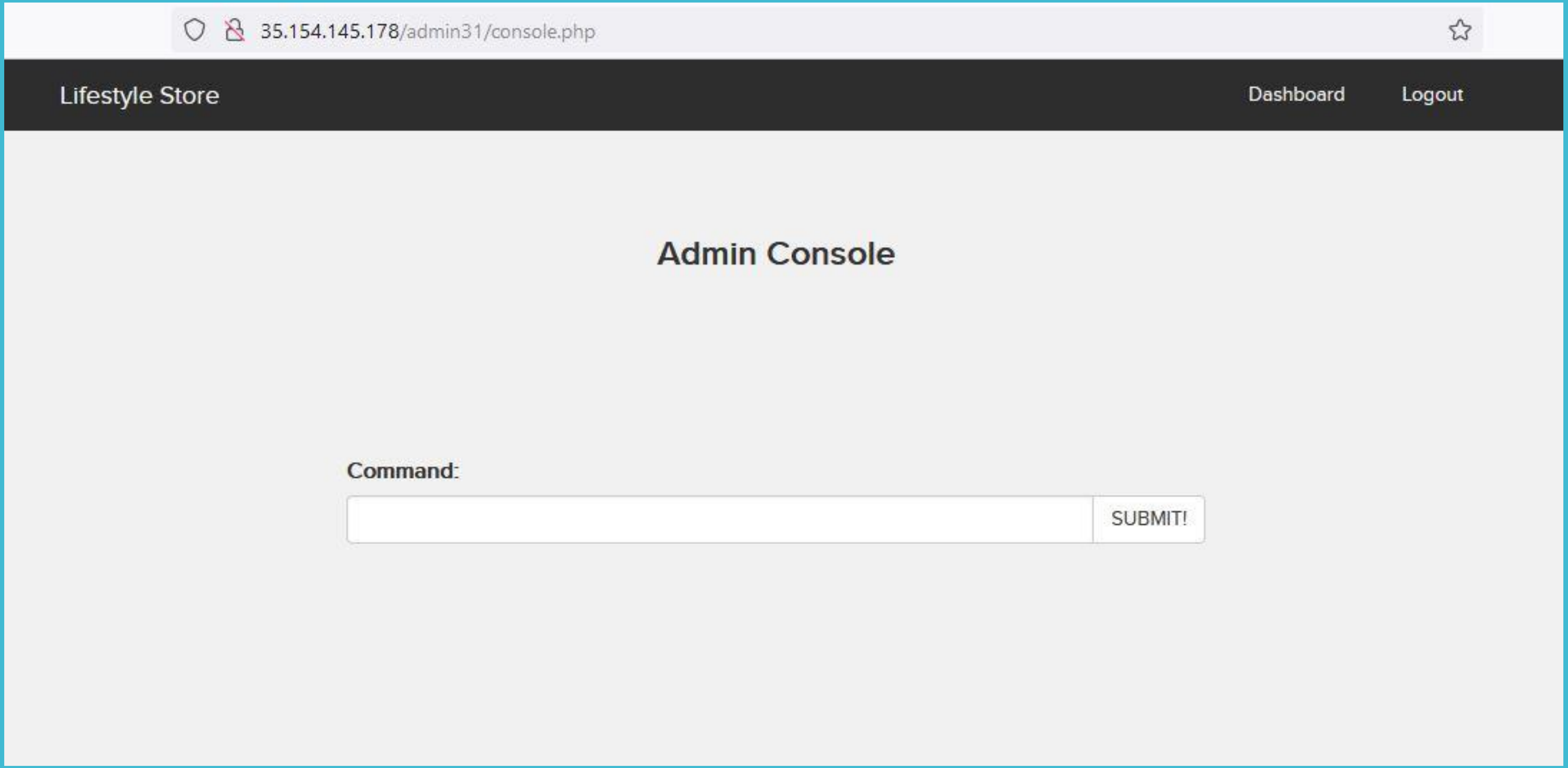
- https://www.owasp.org/index.php/Testing_Multiple_Factors_Authentication_(OWASP-AT-009
- https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

5. Command Execution Vulnerability:

Command Execution Vulnerability (Critical)	Below mentioned URLs is vulnerable to Command Execution. URL: • http://http://35.154.145.178/admin31/console.php • Shell can be uploaded at files tab to access the server details at http://http://35.154.145.178/wondercms/ Parameters: Command (POST parameter)

Observation:

Navigate to http://35.154.145.178/admin31/console.php after logging in as the admin and you will see the following page.



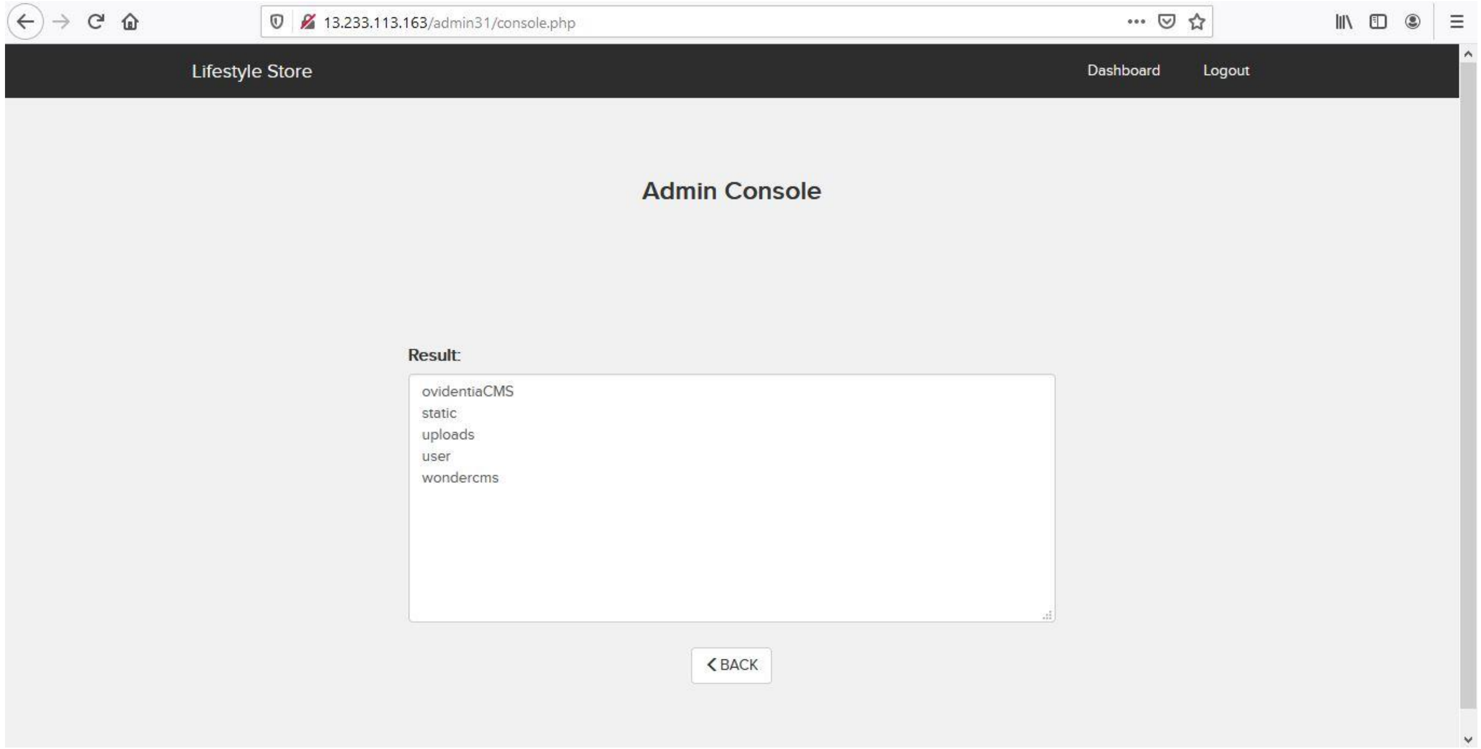
35.154.145.178/admin31/console.php

Lifestyle Store

Dashboard Logout

Admin Console

Command:



Admin Console

Result:

```
ovidentiaCMS
static
uploads
user
wondercms
```

PoC (Proof of Concept):

When ls command is executed the output is completely visible.

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 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.
- 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

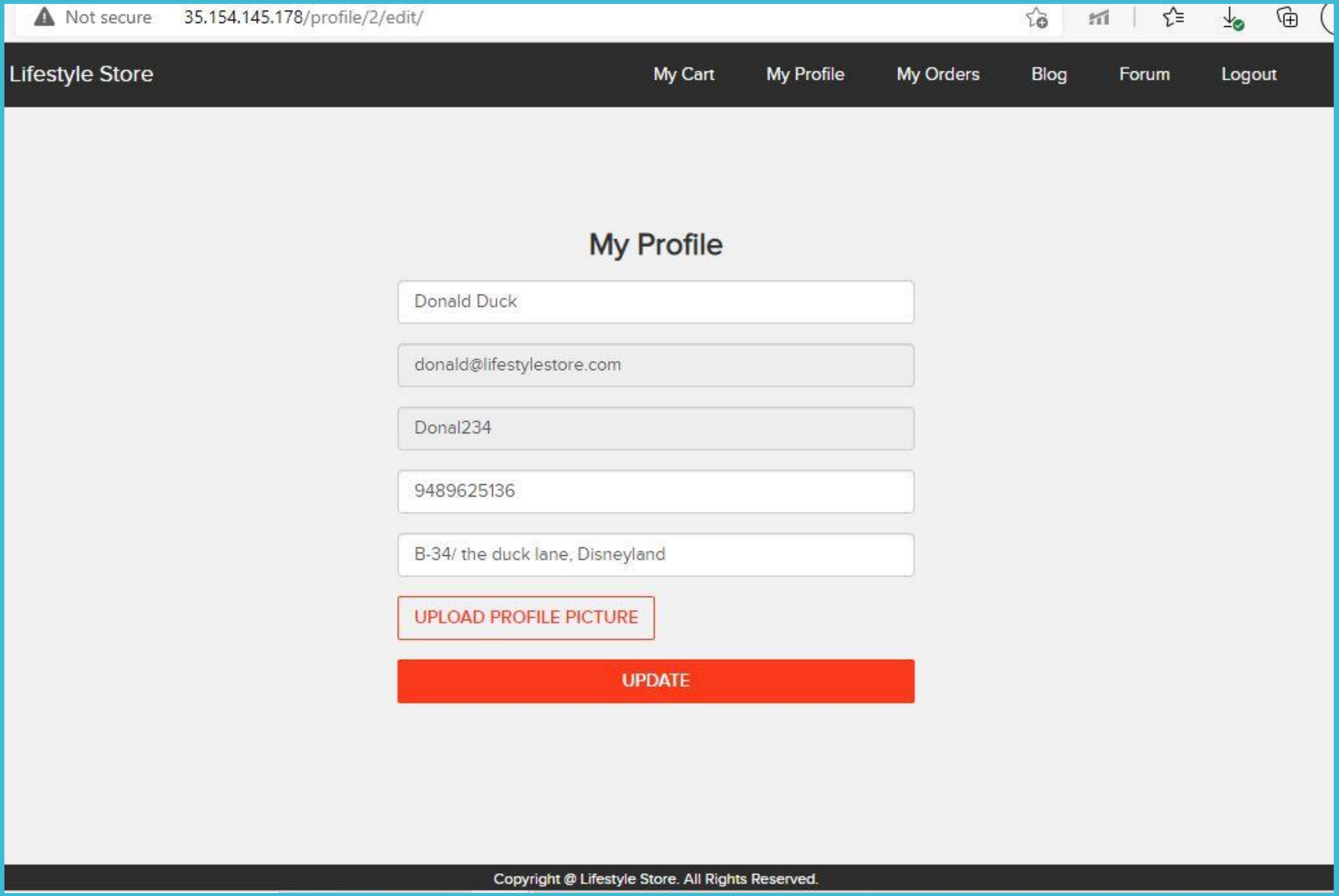
6. Cross Site Scripting:

This happens when a user controlled input is reflected somewhere else in an HTML page and is not encoded/ sanitised properly. This leads to an attacker being able to inject HTML code in the affected page.

Cross Site Scripting (Severe):	Below mentioned parameters are vulnerable to reflected XSS URL: http://35.154.145.178/products/details.php?p_id=2 Parameters: POST button under Customer Review (POST parameters) Payload: <script>alert(1)</script> URL: http://35.154.145.178/profile/2/edit/ Parameters: Address (POST parameters) Payload: <script>alert(0)</script>

Observation:

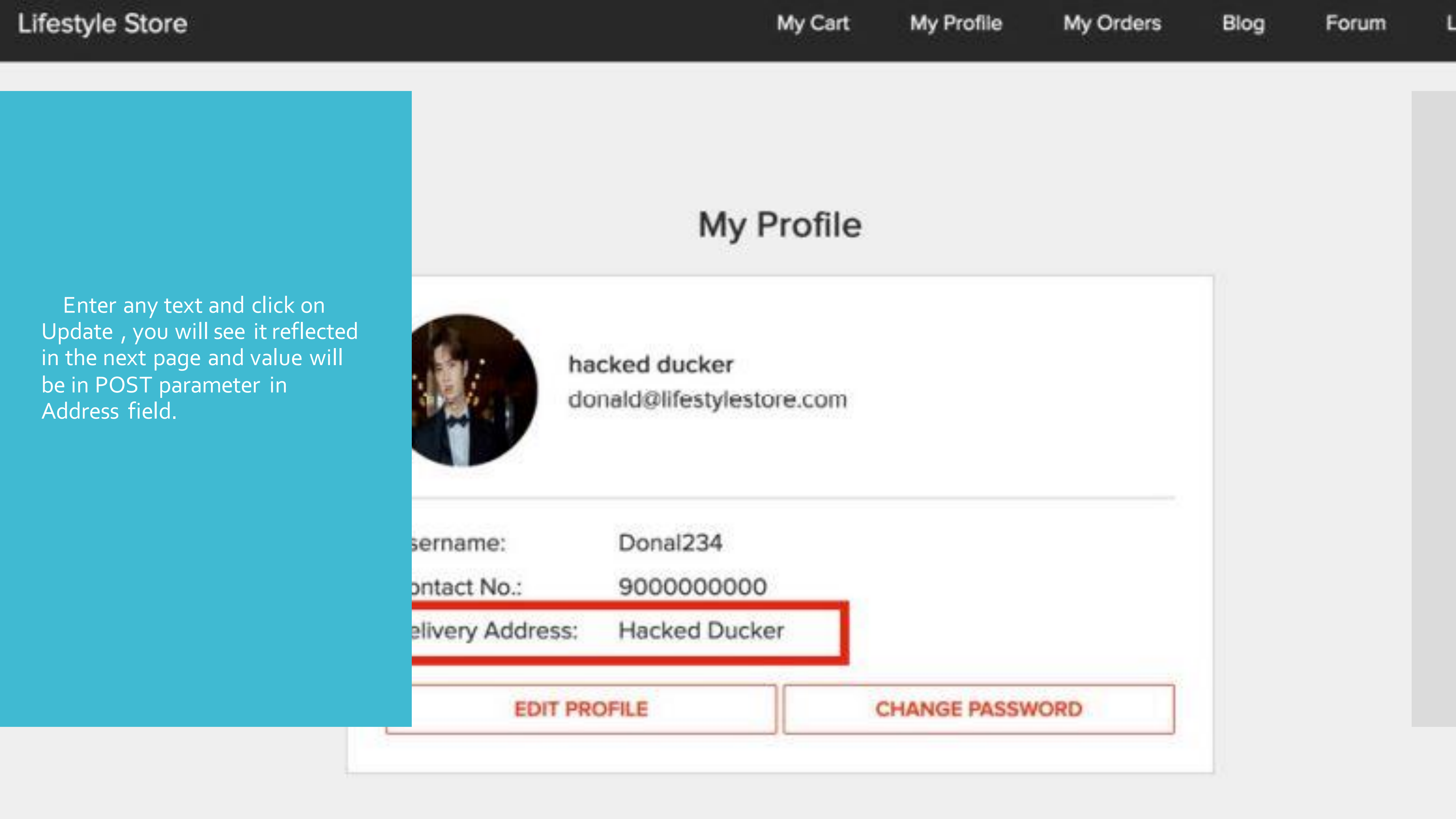
Navigate to http://35.154.145.178//profile/2/edit/ .We can see user’s details.



My Profile

Donald Duck
donald@lifestylestore.com
Donal234
9489625136
B-34/ the duck lane, Disneyland

Enter any text and click on Update , you will see it reflected in the next page and value will be in POST parameter in Address field.



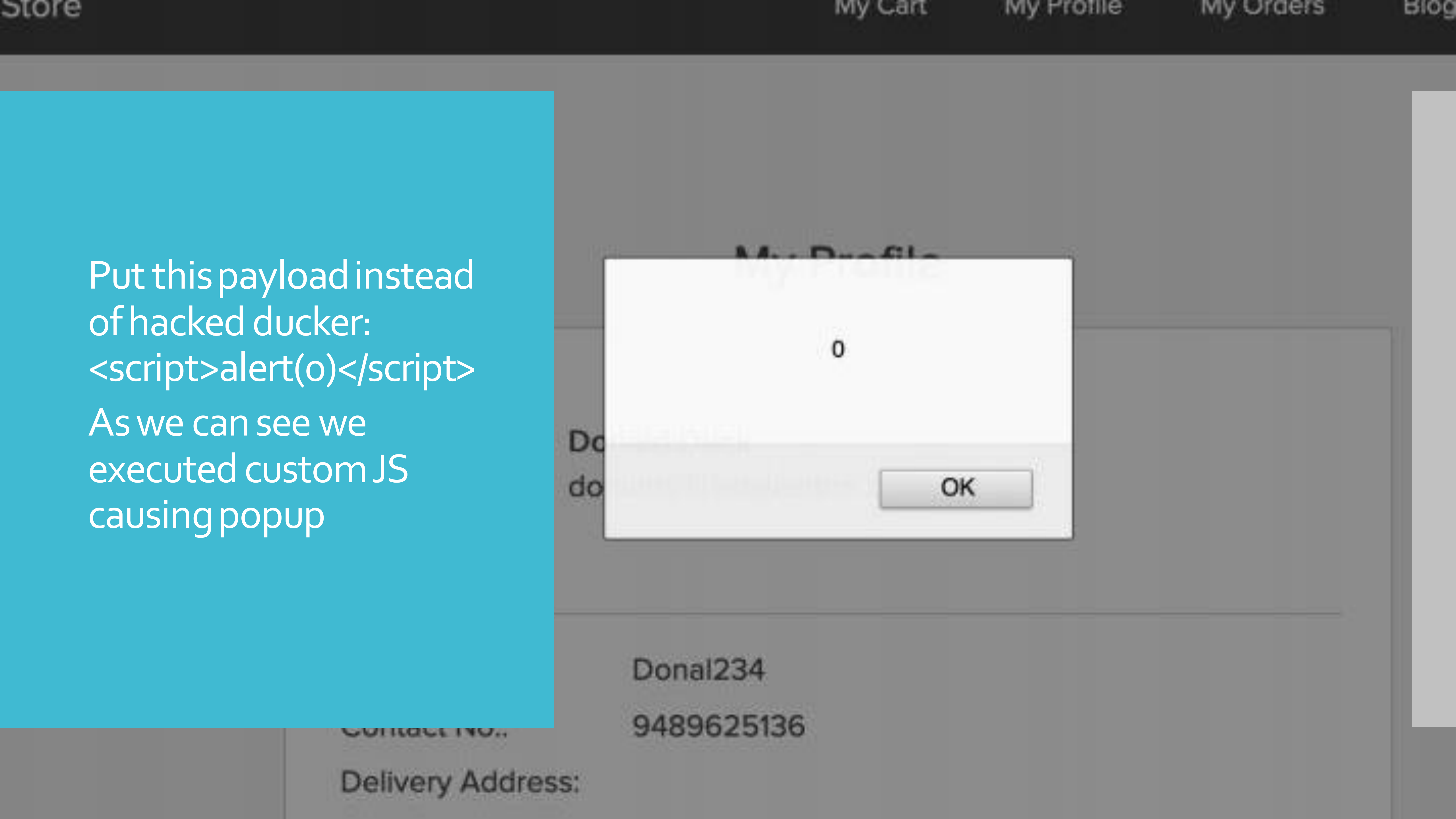
My Profile

hacked ducker
donald@lifestylestore.com

sername: Donal234
ontact No.: 9000000000
elivery Address: Hacked Ducker

Put this payload instead of hacked ducker: <script>alert(o)</script>

As we can see we executed custom JS causing popup



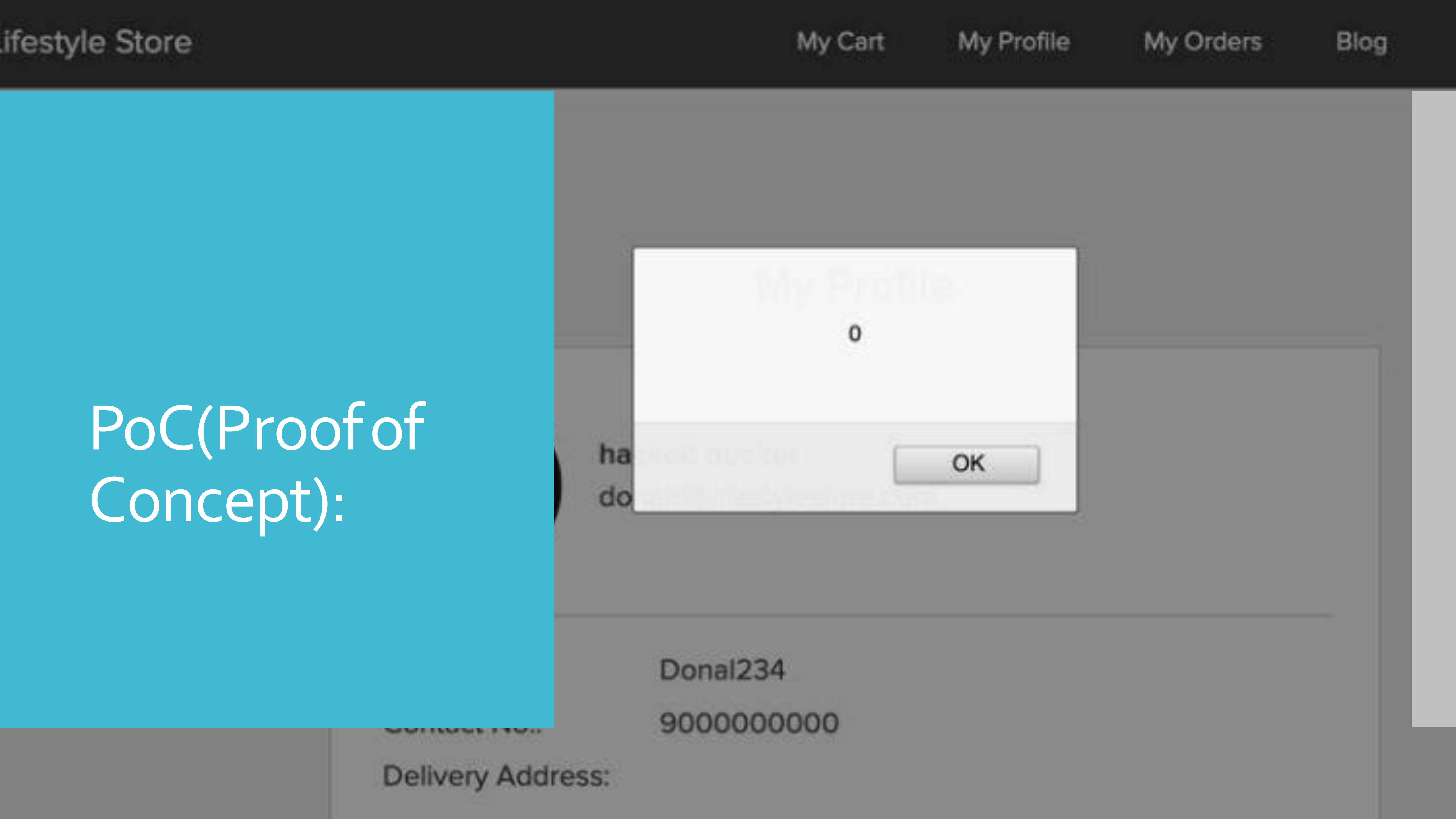
0

Donal234

Contact No.: 9489625136

Delivery Address:

PoC(Proof of Concept):



ha

do

Donal234

9000000000

Delivery Address:

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 organisation .
- 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:

- Sanitise 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:

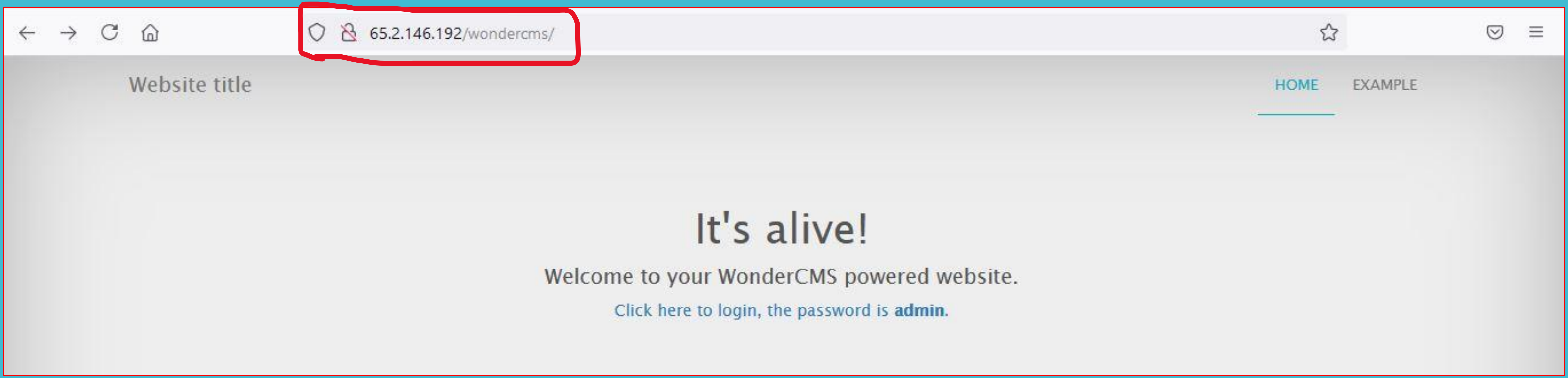
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.w3schools.com/html/html_entities.asp

7. Crypto Configuration Flaws

Crypto Configuration Flaw((Severe)	Crypto Configuration Flaws are found in the modules below. URL: http://13.233.149.44/ All the webpages ,blogs ,forum

Observation:

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



It's alive!

Welcome to your WonderCMS powered website.

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

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

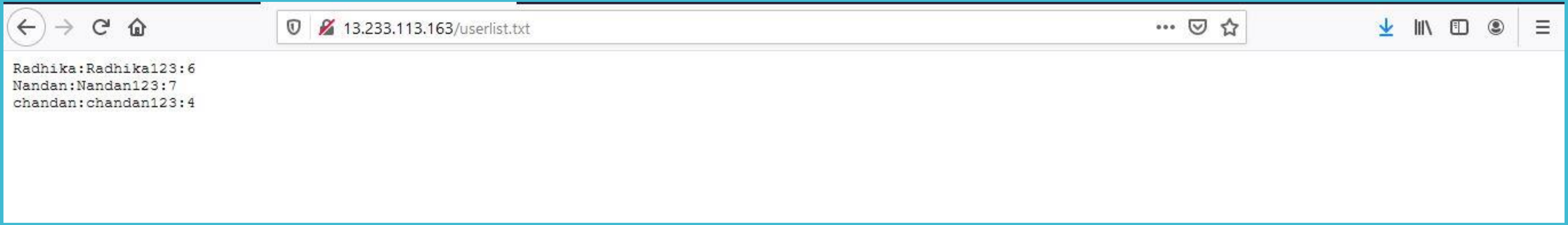
https://www.owasp.org/index.php/Category:Cryptographic_Vulnerability
https://www.w3.org/Protocols/rfc2616/rfc2616-sec15.html

8. Common Passwords

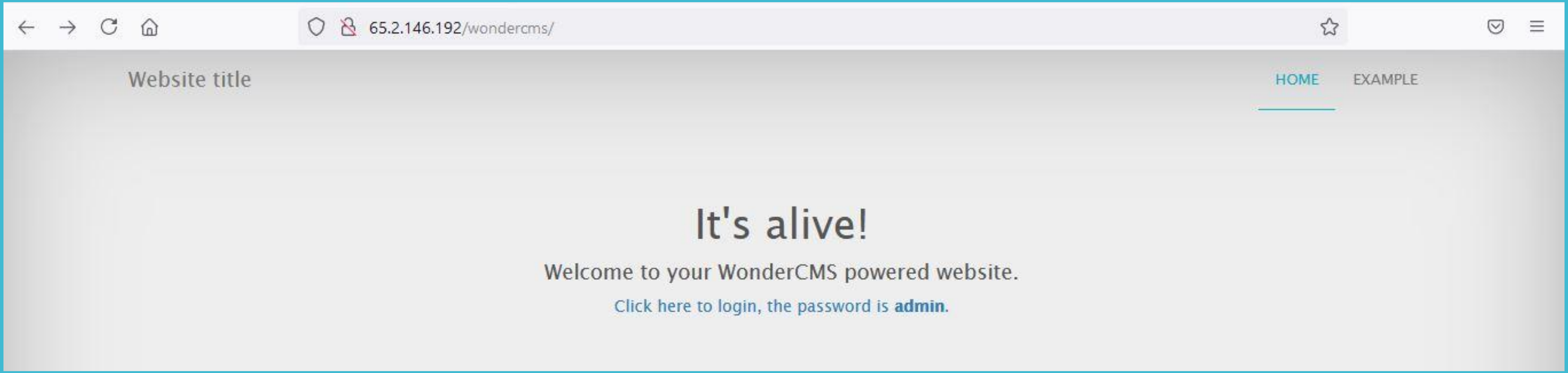
Weak Password Flaw (Severe)	Below given urls have weak passwords. URL: http://13.233.149.44/login/seller.php http://13.233.149.44/wondercms/

Observation:

The passwords of sellers and ,admin of blog ,is very common and easily predictable.



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



It's alive!

Welcome to your WonderCMS powered website.

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

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 ,alphanumerics ,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)

9. Unauthorised availability of Details

Unauthorised Access to Customer Details (Severe)

Similarly other vulnerable urls are given below.

URL:
http://13.233.149.44/orders/orders.php?customer=14
http://13.233.149.44/orders/orders.php?customer=5
http://13.233.149.44/orders/orders.php?customer=13
http://13.233.149.44/orders/orders.php?customer=8
http://13.233.149.44/orders/orders.php?customer=2

The Show My Orders module is vulnerable from an Insecure Direct Object Reference (IDOR) that allows attacker see to anyones Bill details

URL:
http://13.233.149.44/profile/2/edit/

Parameters :
user_id (GET parameters)

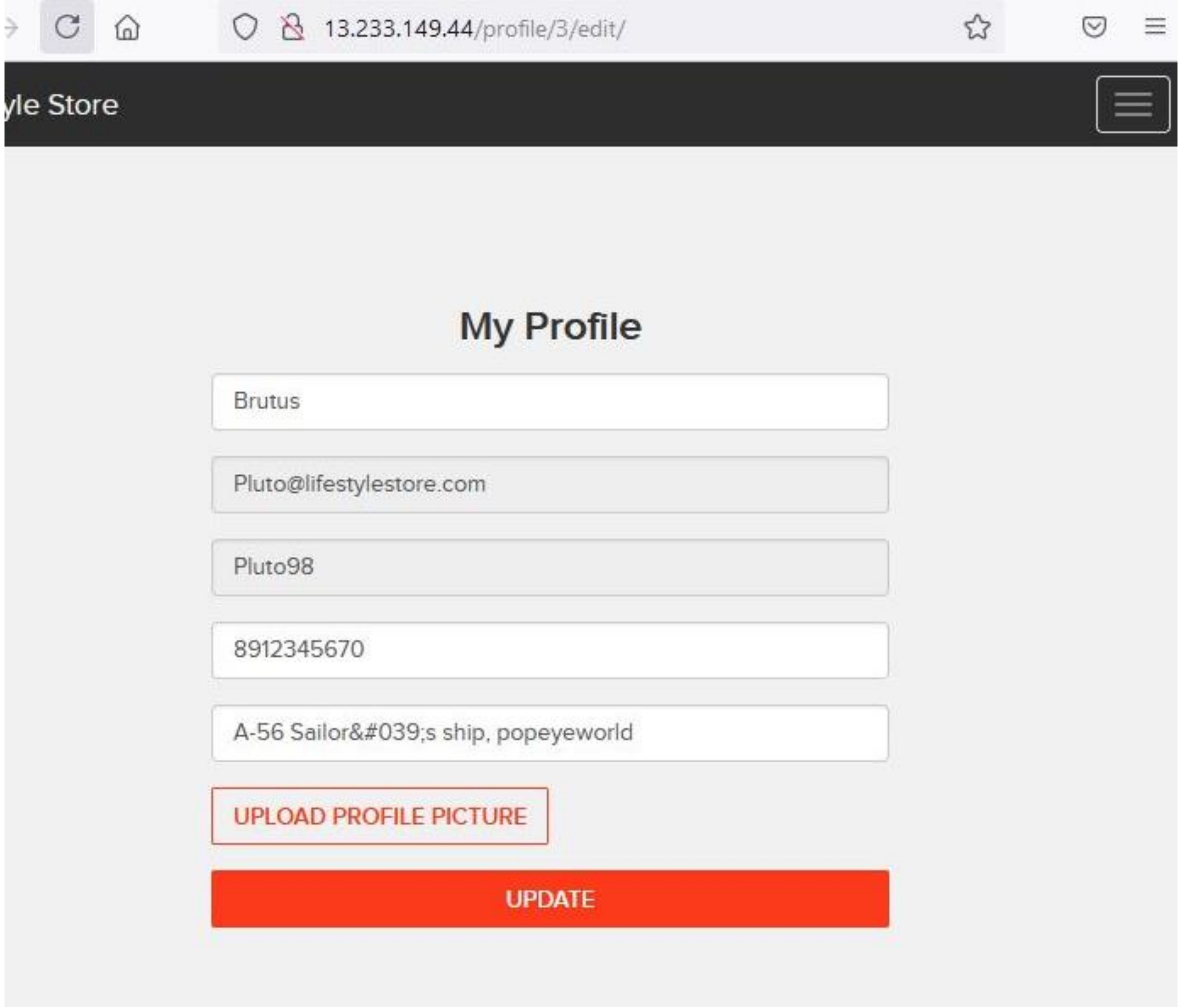
Payload:
http://13.233.149.44/profile/3/edit/

Observation:

Login using any customer details. Then navigate to the below link. http://13.232.3.22/profile/2/edit/

Now remove 2 and insert 3 in the url like shown in the given screenshot and you will see the details of another

user .



13.233.149.44/profile/3/edit/

My Profile

Brutus

Pluto@lifestylestore.com

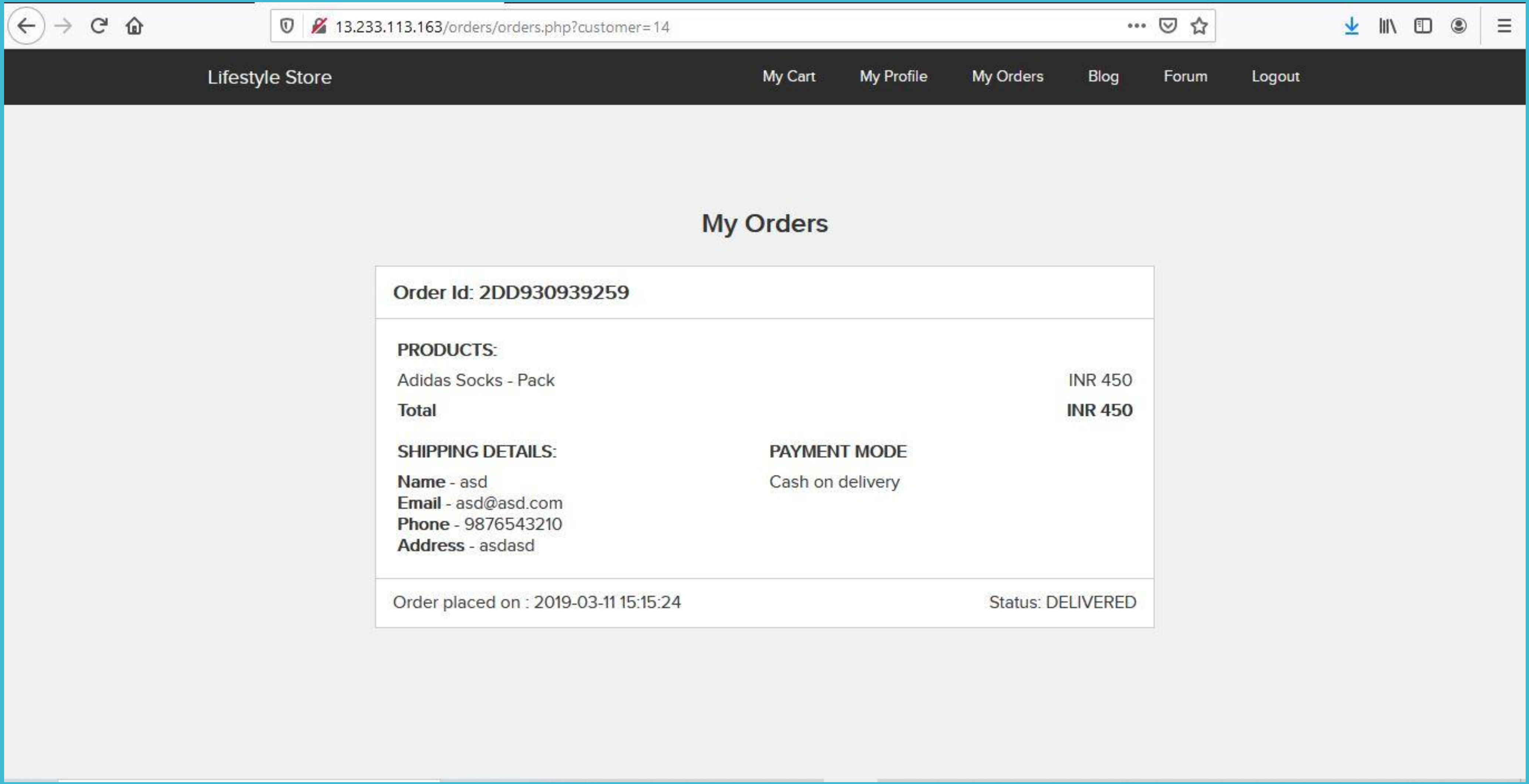
Pluto98

8912345670

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

Proof of Concept (PoC)

Below is the screenshot of the bill details of another user accessed from attacked user’s account.



13.233.113.163/orders/orders.php?customer=14

My Orders

Order Id: 2DD930939259

PRODUCTS:

Adidas Socks - Pack	INR 450
Total	**INR 450**

SHIPPING DETAILS:

Name - asd
Email - asd@asd.com
Phone - 9876543210
Address - asdasd

PAYMENT MODE

Cash on delivery

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

Status: DELIVERED

Business Impact – 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/blackmarket.
- More over, as there is no ratelimiting checks, attacker can bruteforce the user_id for all possible values and get bill information of each and every user of the organization resulting is a massive information leakage.

Recommendation:

- 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.

Reference:

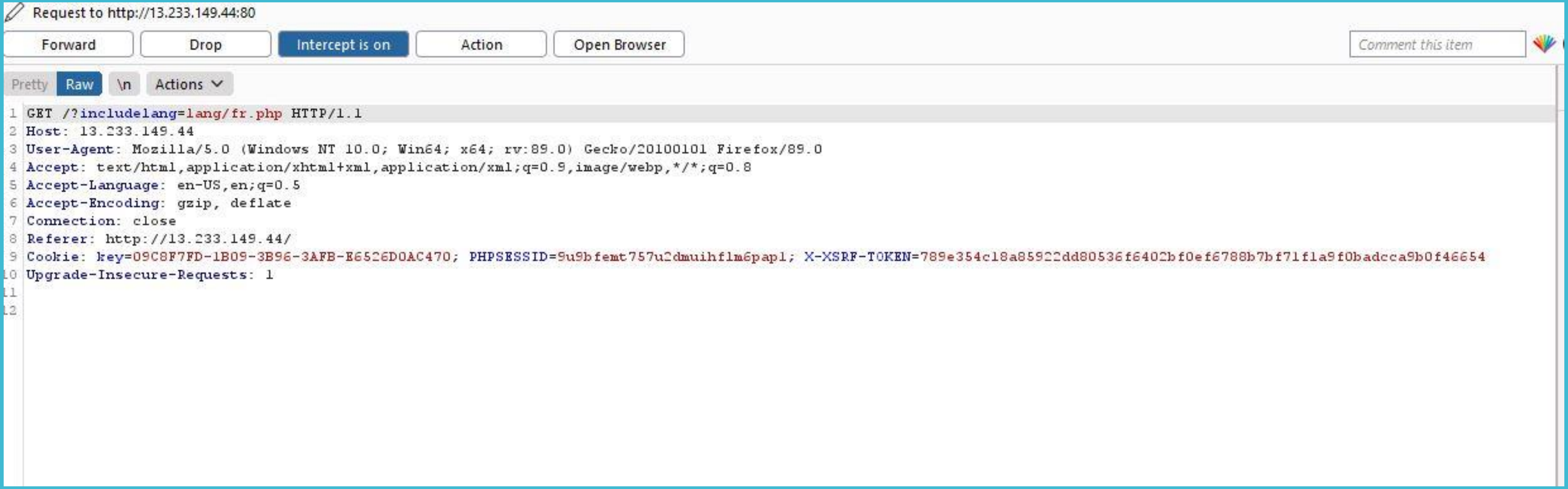
- https://www.owasp.org/index.php/Insecure_Configuration_Management
- https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

10.Open Redirection

Open Redirection (Severe)	The Lang module is vulnerable to open redirection. URL: http://13.233.149.44/?includelang=lang/en.php http://13.233.149.44/?includelang=lang/fr.php Parameters : lang (GET parameters) **Payload:** http://13.233.149.44/?includelang=https://google.com/?lang/en.php

Observation:

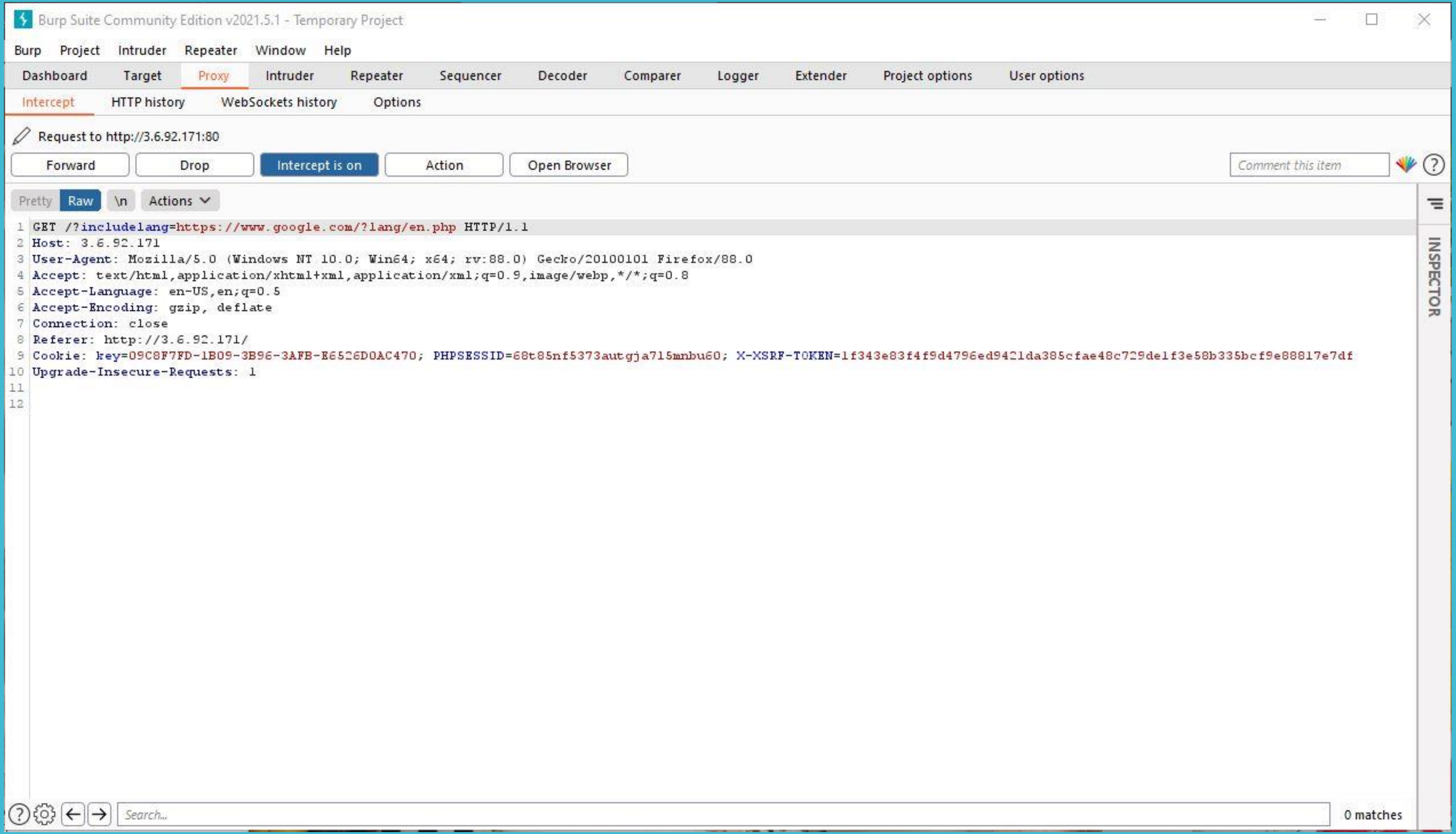
- Navigate to http://http://13.233.149.44/ and under the Lang tab click on French.
- Capture this request in local proxy .



```
GET /?includelang=lang/fr.php HTTP/1.1
Host: 13.233.149.44
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://13.233.149.44/
Cookie: key=09C8F7FD-1B09-3B96-3AFB-E6526D0AC470; PHPSESSID=9u9bfemt757u2dmuihflm6pap1; X-XSRF-TOKEN=789e354c18a85922dd80536f6402bf0ef6788b7bf71f1a9f0badcca9b0f46654
Upgrade-Insecure-Requests: 1


```

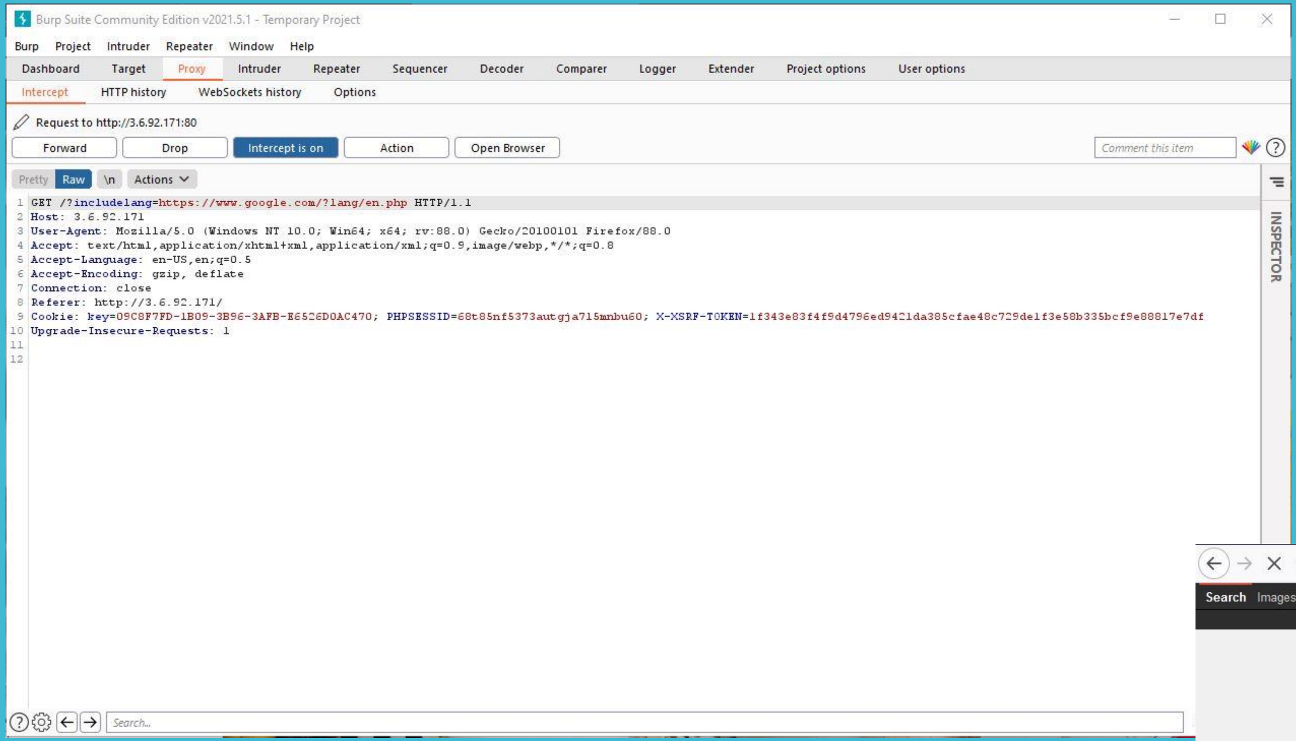
- Now edit the request like this : GET /?includelang=https://google.com/?lang/en.php HTTP/1.1
- Then pass this request in the browser. You will see the google.com


Burp Suite Community Edition v2021.5.1 - 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
Request to http://3.6.92.171:80
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR
Search...
0 matches

```
GET /?includelang=https://www.google.com/?lang/en.php HTTP/1.1
Host: 3.6.92.171
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
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://3.6.92.171/
Cookie: key=09C8F7FD-1B09-3B96-3AFB-E6526D0AC470; PHPSESSID=68t85nf5373autgja715mnbu60; X-XSRF-TOKEN=1f343e83f4f9d4796ed9421da385cfae48c729de1f3e58b335bcf9e88817e7df
Upgrade-Insecure-Requests: 1


```

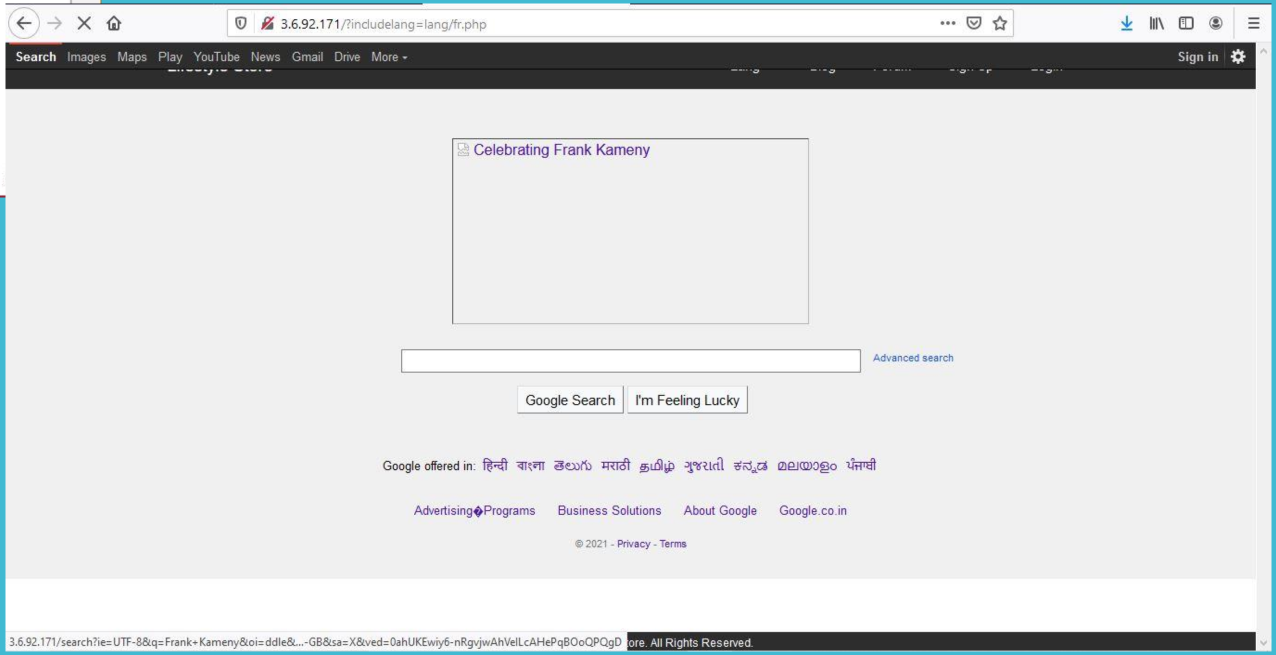
Proof of Concept (PoC)


Burp Suite Community Edition v2021.5.1 - 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
Search...

Request to http://3.6.92.171:80

```
GET /?includelang=https://www.google.com/?lang/en.php HTTP/1.1
Host: 3.6.92.171
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
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://3.6.92.171/
Cookie: key=09C8F7FD-1B09-3B96-3AFB-E6526D0AC470; PHPSESSID=68t85nf5373autgja715mnbu60; X-XSRF-TOKEN=1f343e83f4f9d4796ed9421da385cfae48c729de1f3e58b335bcf9e88817e7df
Upgrade-Insecure-Requests: 1


```


3.6.92.171/?includelang=lang/fr.php
Search Images Maps Play YouTube News Gmail Drive More
Sign in
Celebrating Frank Kameny
Advanced search
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
Advertising�Programs Business Solutions About Google Google.co.in
© 2021 - Privacy - Terms
3.6.92.171/search?ie=UTF-8&q=Frank+Kameny&oi=ddle&...-GB&sa=X&ved=0ahUKEwiy6-nRgvjwAhVelLcAHePqBOoQPQgD
tore. All Rights Reserved.

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:

References:

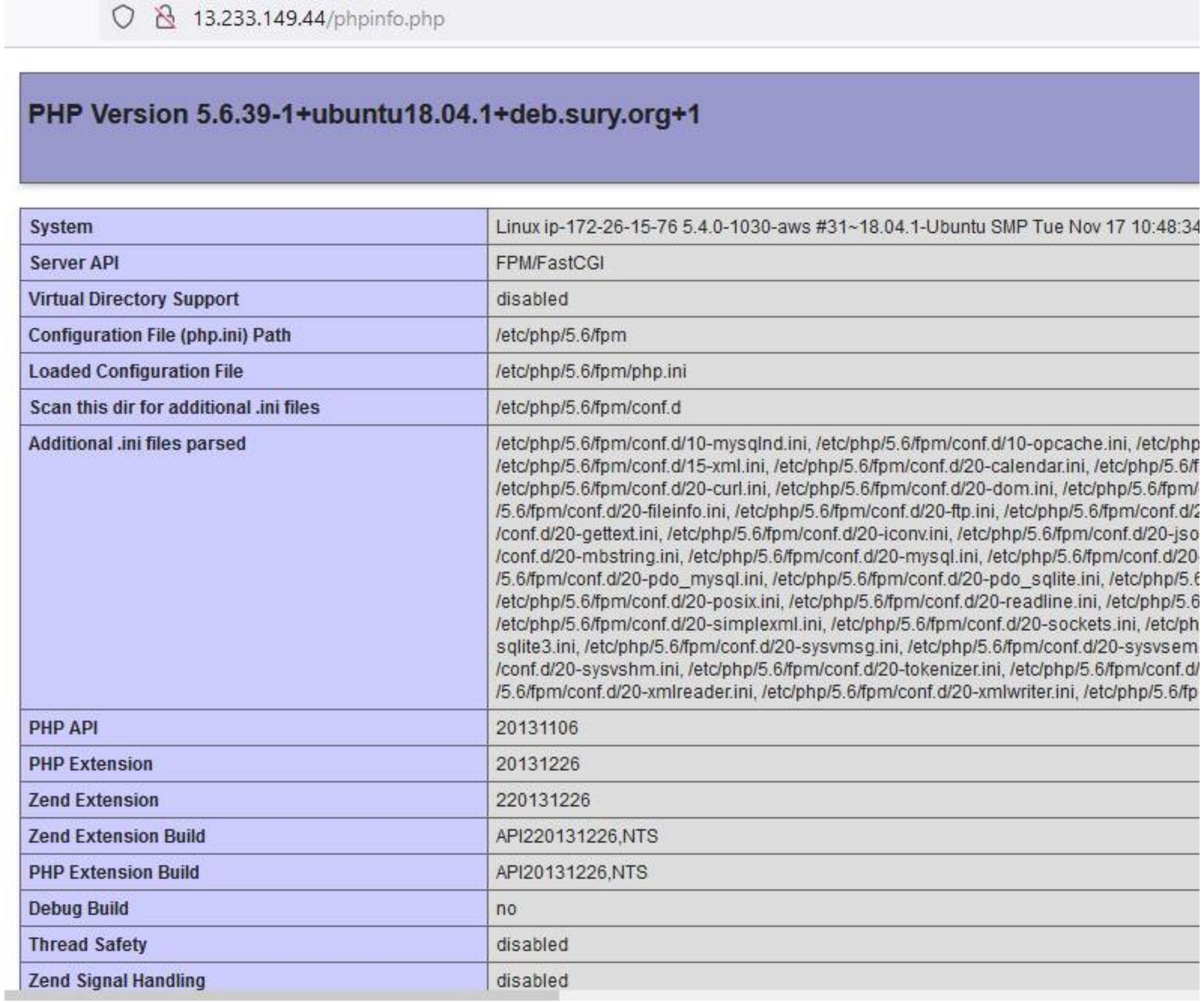
- https://cwe.mitre.org/data/definitions/601.html
- https://www.hacksplaining.com/prevention/open-redirects

11. Information disclosure due to Default Pages

Directory Listing (Moderate)	Below mentioned URLs disclose server information. URL: http://13.233.149.44/phpinfo.php http://13.233.149.44/robots.txt http://13.233.149.44/composer.lock http://13.233.149.44/composer.json http://13.233.149.44/userlist.txt

Observation:

Navigate to http://13.233.149.44/phpinfo.php and you will see the below page.



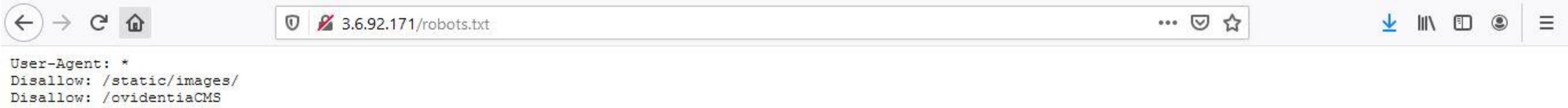
13.233.149.44/phpinfo.php

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

System	Linux ip-172-26-15-76 5.4.0-1030-aws #31~18.04.1-Ubuntu SMP Tue Nov 17 10:48:34
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 /etc/php/5.6/fpm/conf.d/15-xml.ini, /etc/php/5.6/fpm/conf.d/20-calendar.ini, /etc/php/5.6/f /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/ /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/2 /conf.d/20-gettext.ini, /etc/php/5.6/fpm/conf.d/20-iconv.ini, /etc/php/5.6/fpm/conf.d/20-jso /conf.d/20-mbstring.ini, /etc/php/5.6/fpm/conf.d/20-mysql.ini, /etc/php/5.6/fpm/conf.d/20 /5.6/fpm/conf.d/20-pdo_mysql.ini, /etc/php/5.6/fpm/conf.d/20-pdo_sqlite.ini, /etc/php/5.6 /etc/php/5.6/fpm/conf.d/20-posix.ini, /etc/php/5.6/fpm/conf.d/20-readline.ini, /etc/php/5.6 /etc/php/5.6/fpm/conf.d/20-simplexml.ini, /etc/php/5.6/fpm/conf.d/20-sockets.ini, /etc/ph sqlite3.ini, /etc/php/5.6/fpm/conf.d/20-sysvmsg.ini, /etc/php/5.6/fpm/conf.d/20-sysvsem /conf.d/20-sysvshm.ini, /etc/php/5.6/fpm/conf.d/20-tokenizer.ini, /etc/php/5.6/fpm/conf.d/ /5.6/fpm/conf.d/20-xmlreader.ini, /etc/php/5.6/fpm/conf.d/20-xmlwriter.ini, /etc/php/5.6/fp
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

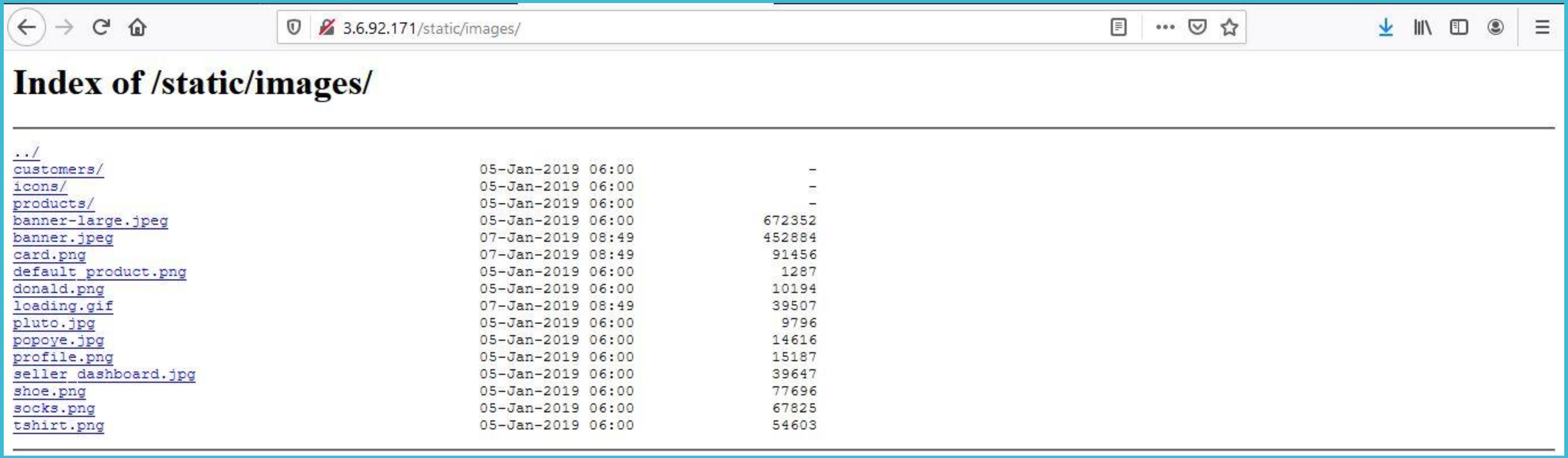
Navigate to http://13.233.149.44/robots.txt and you will see the following page.

Next you can navigate to any of the listed files.



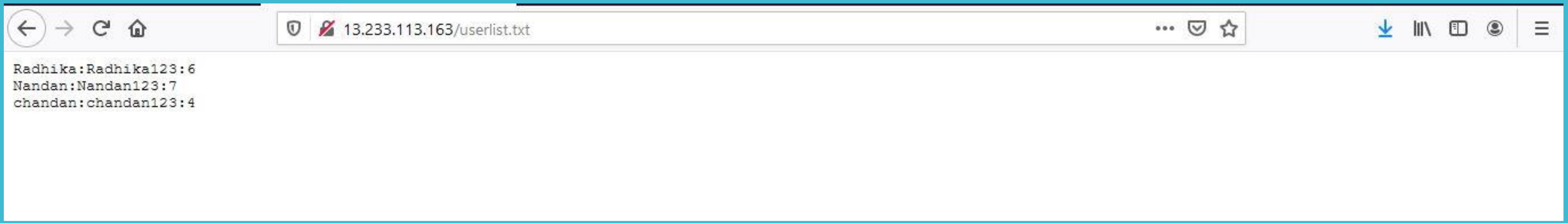
```
User-Agent: *
Disallow: /static/images/
Disallow: /ovidentiaCMS
```

Proof of Concept(PoC):



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
```



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

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:

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

References:

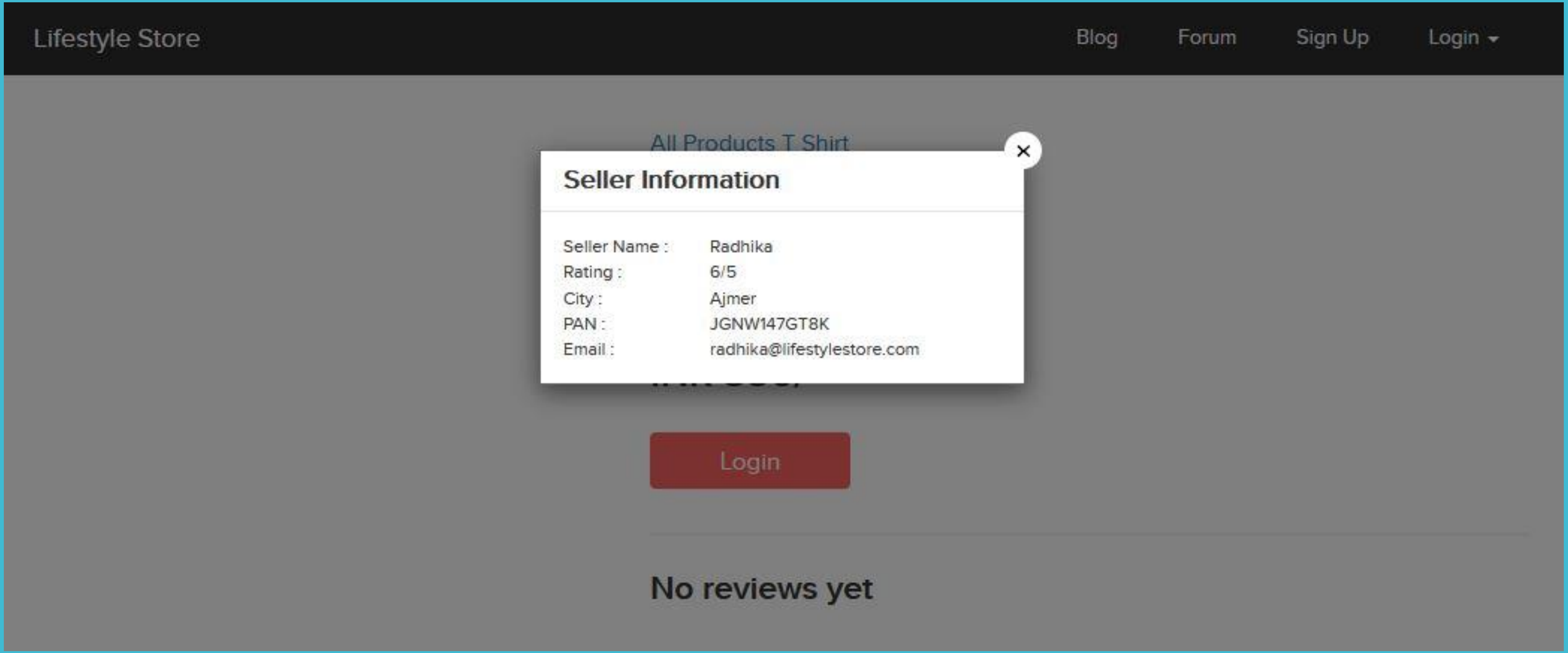
- https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/
- https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/information-disclosure-phpinfo/

12. Unnecessary Details about Sellers

Unnecessary Details about Sellers (Moderate)	Below mentioned URL gives the unnecessary details about the seller (PII). URL: http://13.233.149.44/products/details.php?p_id=2

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

No reviews yet

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:

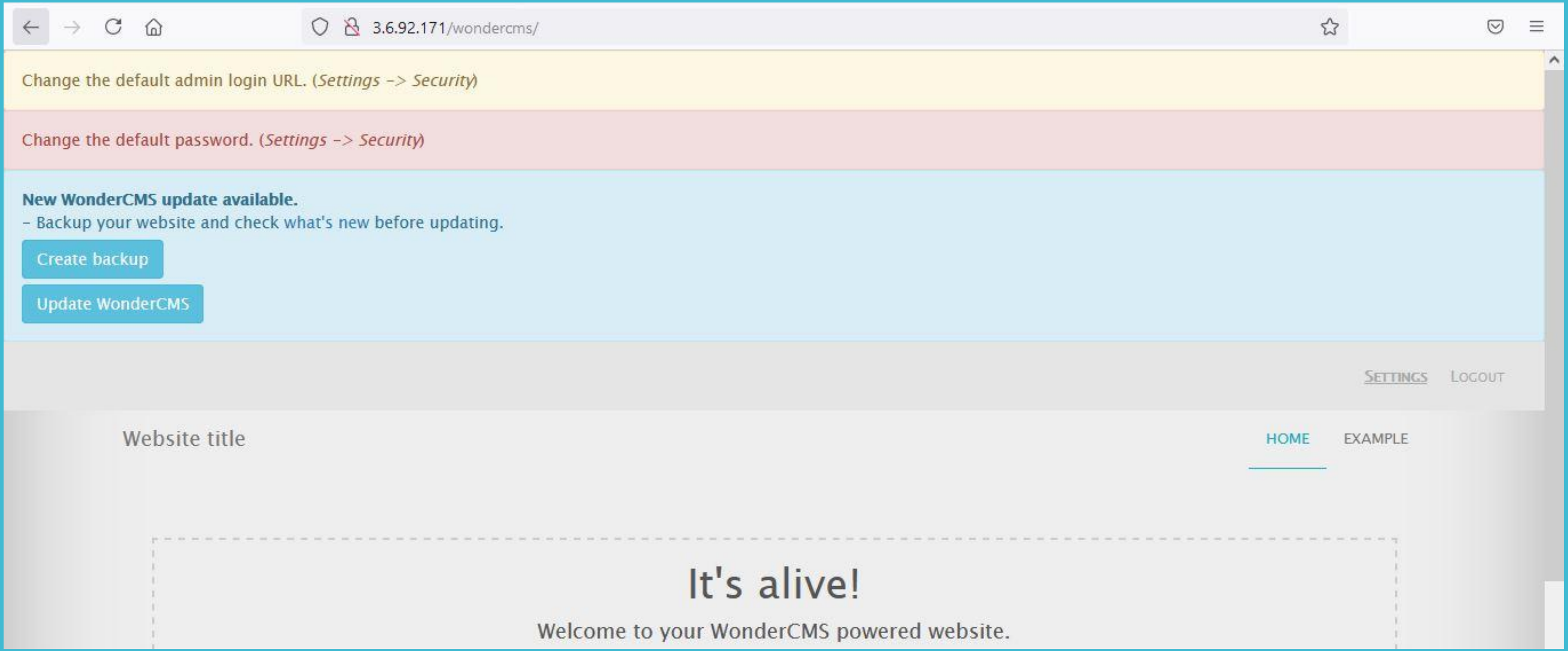
- https://digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or-compromise

13. Components with known vulnerabilities

Components with known Vulnerabilities (Moderate)	• 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.



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.

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:

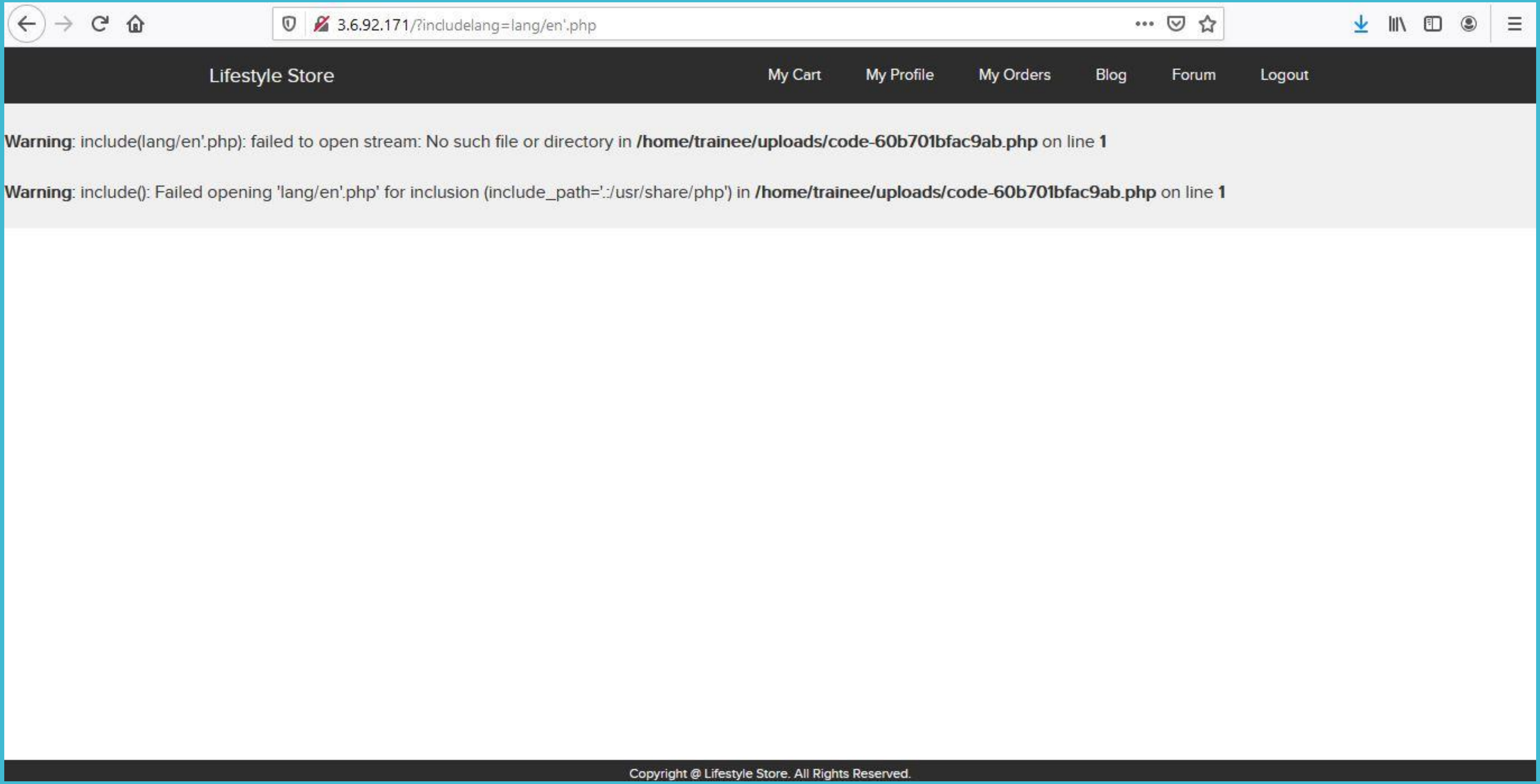
- https://usn.ubuntu.com/4099-1/
- http://securitywarrior9.blogspot.com/2018/01/vulnerability-in-wonder-cms-leading-to.html

14.Default Error Display

Default Error Display (Low)	Below mentioned urls have default error displaying on fuzzing: URL: http://13.233.149.44/?includelang=lang/en.php Payload : en’.php (GET Parameter) URL: http://13.233.149.44/search/search.php Parameter: q (GET Parameter) Payload: q='

Observation:

The default error with the path is displayed as:



3.6.92.171/?includelang=lang/en'.php
Lifestyle Store
My Cart
My Profile
My Orders
Blog
Forum
Logout

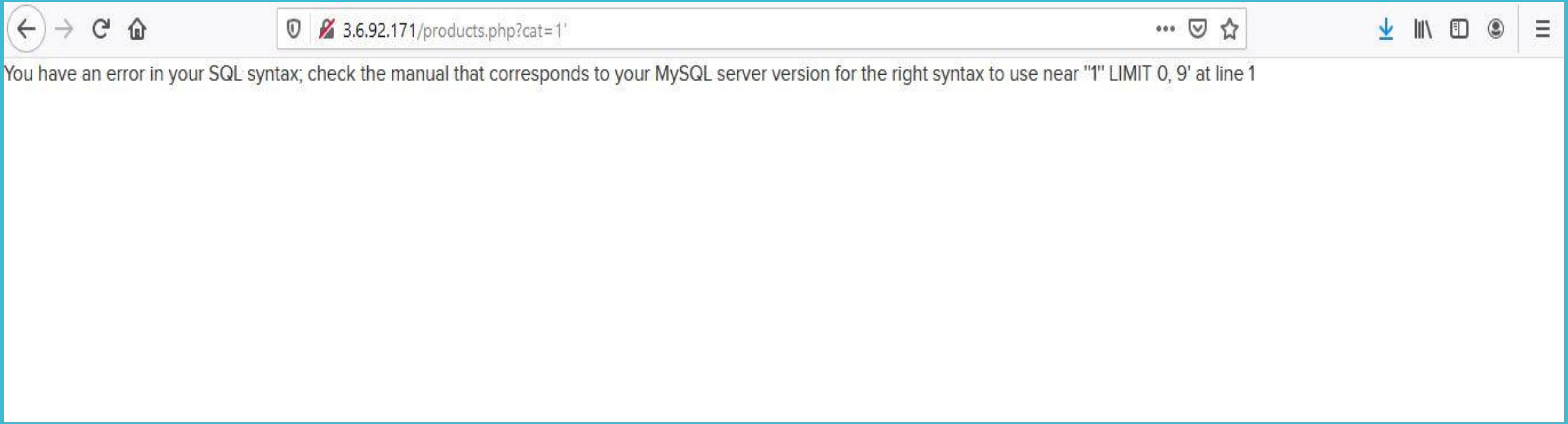
```
Warning: include(lang/en'.php): failed to open stream: No such file or directory in /home/trainee/uploads/code-60b701bfac9ab.php on line 1

Warning: include(): Failed opening 'lang/en'.php' for inclusion (include_path='.:/usr/share/php') in /home/trainee/uploads/code-60b701bfac9ab.php on line 1
```

Copyright @ Lifestyle Store. All Rights Reserved.

Proof of Concept (PoC):

When we give socks' in the search option of the home page ,we get the error as:



```
3.6.92.171/products.php?cat=1'
```

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' LIMIT 0, 9' at line 1
```

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

ThankYou

For any further assistance contact

Jason_hacker@otpmail.com