VAPT REPORT FOR E-COMMERCE WEBSITE.
LIFESTYLE STORE : A WEB BASED APPLICATION

Report by: Arjun shetty

Introduction:

- This is the vulnerability assessment and penetration testing (VAPT) report for “Lifestyle Store”.
- I have reported all the vulnerabilities found on this store
- I have also provided business risks and expert recommendations to tackle those vulnerabilities.

Security Status: EXTREMELY CRITICAL

SQLi :Hackers can steal all records from the databases of the website.

Hackers can take complete controlof the website including view, edit, add or delete files and folders via shell upload.

IDOR : Hackers can extract mobile numbers of all customers using user-id.

Hackers can change the source code and can upload any malicious code, **phishing** etc. in the website via shell upload.

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

Vulnerability Statistics:

CRITICAL	SEVERE	MODERATE	LOW
12	7	3	3

Vulnerabilities Found:

SEVERITY	VULNERABILITY	COUNT
MODERATE	CLIENT SIDE FILTER BYPASS	2
SEVERE	SERVER MISCONFIGURATION	2
CRITICAL	PII LEAKAGE	4
CRITICAL	OPEN REDIRECTION	2
SEVERE	CSRF	2
CRITICAL	SQL INJECTION	2
SEVERE	STORED AND REFLECTED XSS	2
CRITICAL	IDOR	3
SEVERE	RATE LIMITING FLAW	4
CRITICAL	INSECURE FILE UPLOAD	2

SQL Injection

CRITICAL

Below mentioned URL is vulnerable to SQL injection attack.

Relevant URL :

http://52.66.203.250/products.php?cat=1

Affected Parameters :

category (GET)

Payload:

cat=1’

URL Vulnerable to SQLi :

URL #1 :

http://52.66.203.250/products.php?cat=4’

PAYLOAD:

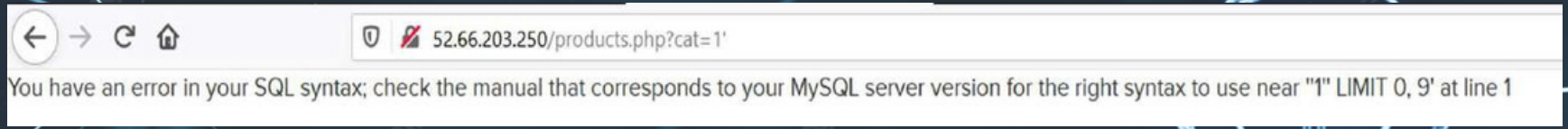
cat=1’

Observations :

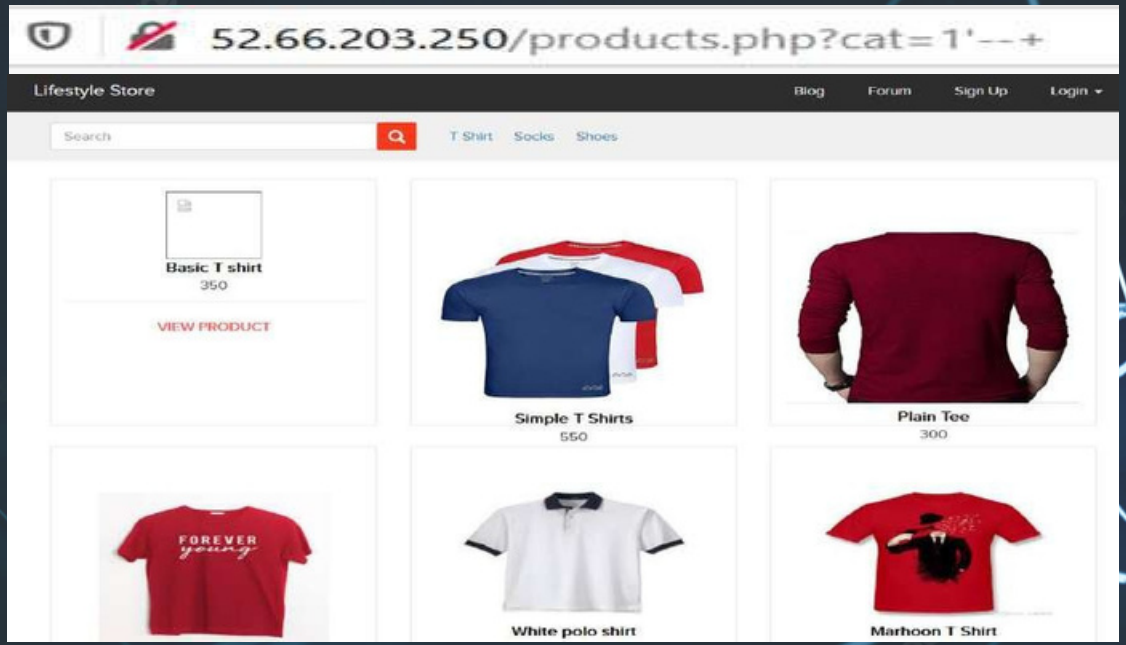
the following observation are being made related to the vulnerabilities of the website

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

When you apply a single quote (‘) in the get parameter,
you get a MySQL error.



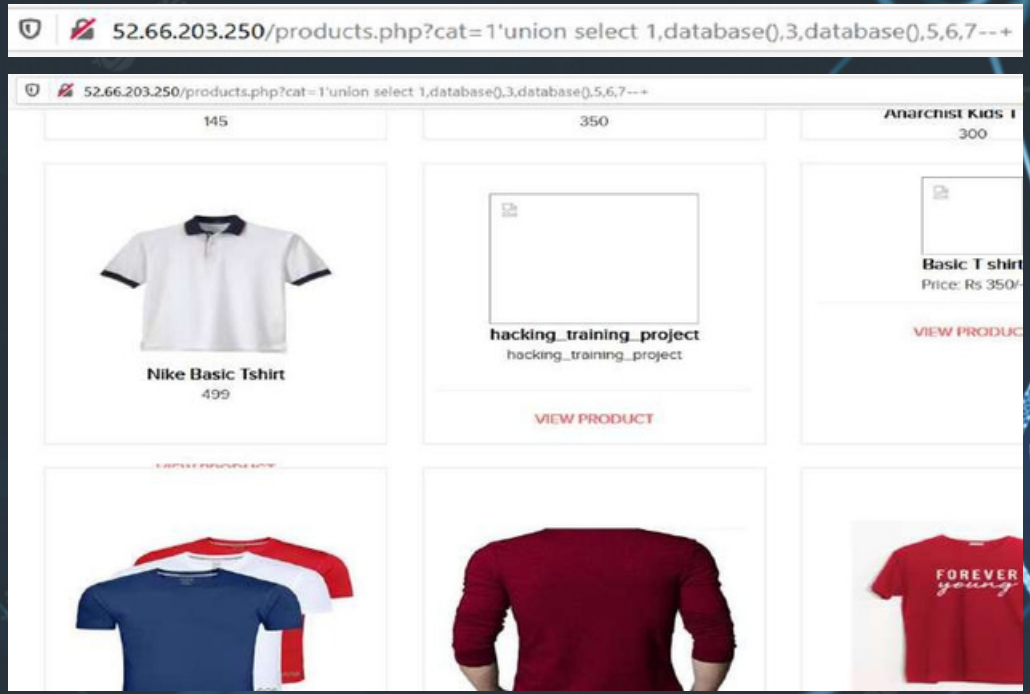
To confirm the MySQL error, you canput “--+” in the end of the parameter, and the page loads in its original format, this confirms the error.



Proof Of Concept :

Following Slides Have The Proof and Risks Of The Proposed Vulnerability.

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



Proof Of Concept :

No. Of Databases : 2

- Information_Schema
- Hacking_training_project

No. Of Tables in “Hacking_training_Project” : 9

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

Business Impact:

Using this vulnerability, the attacker can execute arbitrary SQL commands on Lifestyle Store's server and gain complete access to the internal database, which also makes all customer data inside it visible.
This is the screenshot of users table which shows user credentials being leaked.

```
atabase: hacking_training_project
able: users
15 entries]
+-----------------------+--------------------------------------------------------------+
| name                  | password                                                     |
+-----------------------+--------------------------------------------------------------+
| admin                 | $2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki |
| Donald Duck           | $2y$10$PM.7nBSP5FMaldXiM/S3s./p5xR6GTKvjry7ysJtxOkBqOJURAHsO |
| Brutus                | $2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki |
| Chandan               | $2y$10$4cZBEIrgthXdvT1hwUlivuFELeO3rR.GIcdpO3NjrlSOveiOKLVDa |
| Popeye the sailor man | $2y$10$FkvlRfwYTioW0w2CaZtAQuXVnhGAUjt/If/yTqkNPC5zTrsVm7EeC |
| Radhika               | $2y$10$RYxNhOyV/G4g7OtFwpqYaexvHi8rF6XXui8kT1WtrfqhTutCA8JC. |
| Nandan                | $2y$10$G.cRNLMEiG79ZFXElHg.R.o95334UOxmZu4.9MqzR5614ucwnk59K |
| Murthy Adapa          | $2y$10$mzQGzD4sDSj2EunpCioe4eK18c1AbsOT2P1a1P6eV1DPR.11UubDG |
| John Albert           | $2y$10$GhDB8h1X6XjPMY12GZ1vDO7Y3en97u1/.oXTZLmYqB6F18FBgecvG |
| Bob                   | $2y$10$kiUikn3HPFbuyTtK75lLNurxzqCOLX3eMGyO/Ux16JOoG37dCGKLq |
| Jack                  | $2y$10$z/nyNlkRJ76m9ItMZ4N5lOeRxy6Gkqi9N/UBcJu5ZeO7eM7N4pTHu |
| Bulla Boy             | $2y$10$HT5oiRMetqaZ7xGZPE9s2.Mk1yF4PnYDJHCWbm2w/xuKpjEEI/zjG |
| hunter                | $2y$10$pB3U9iFxwBgSbl2AkBpiEeIBdhiYfwy9y.xV23q12gGbMCyn7N3g2 |
| asd                   | $2y$10$At5pFZnRWpjCD/yNnJWDL.L3Cc4CvOW8Q/WEHmWzBFqVIkBQFpCF2 |
| acdc                  | $2y$10$J50B78.gpucuLTwpHwbcPedYcain.Yi.tsTLyQtK17FzdSpmIRRbi |
+-----------------------+--------------------------------------------------------------+
```

Recommendations:

1.Prepared Statements : Use SQL prepared statements available in all web development languages and frameworks to avoid attacker being able to modify SQL query.

2.Do not run Database Service as admin/rootuser.

3.Disable/remove default accounts, passwords.

4.Character Encoding : Convert the simple codes to different characters like ‘~’/’^’. It is also suggested to follow HTML and other encodings.

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

Relevant URL :

- http://52.66.203.250/login/admin.php

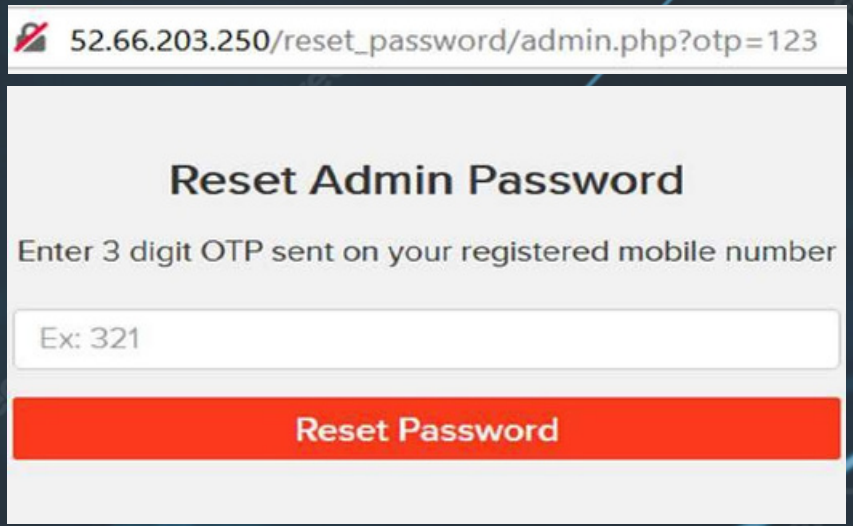
Affected Parameters :

- OTP (POST)

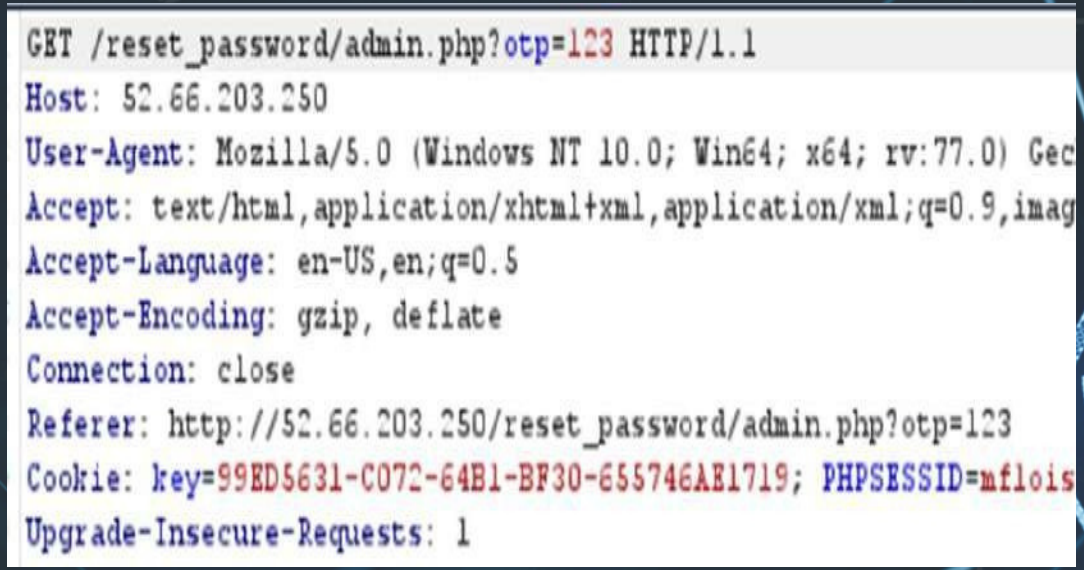
Observations :

the following observation are being made related to the vulnerabilities of the website

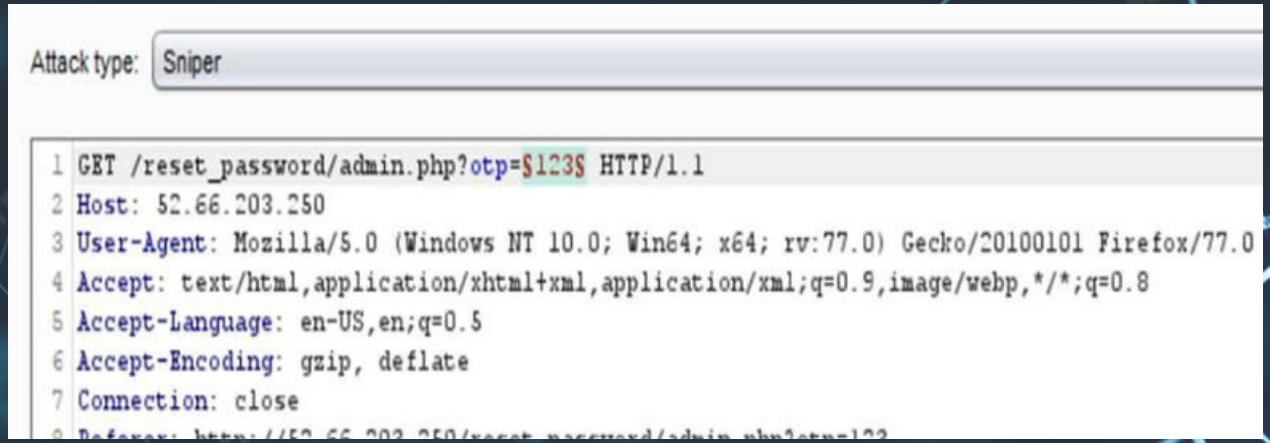
Navigate to http://52.66.203.250/login/admin.php you will see a “forgot password” hyperlink which asks for OPT which is sent to victim’s mobile number ,input any anonymous 3 digit OPT and intercept the request with burp suite.



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



We'll brute force by getting all combination of 3 digit OTP's and input the correct one to bypass.



Business Impact:

A hacker can gain complete access to admin account just by brute-forcing due to rate limiting flaw as a hacker can attempt as many times as he wants as there is no bounds in number of trials.

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

Recommendations:

Take the following precautions :

1.Use rate limiting checks on the number of times the OTP request is generated.

2.OTP should be at least of 6 digits, a 3 digit OTP can be guessed or brute-forced easily.

3.OTP should expire in a particular time like 2 minutes or 5 minutes to make authorization process more secure.

The “My Orders” section shows an Insecure Direct Object Reference (IDOR),
This allows hackers to get access to any customer’s order details and more.

Relevant URL :

- http://52.66.203.250/orders/orders.php?customer=2
  http://52.66.203.250/products/details.php?p_id=7.

Affected Parameters

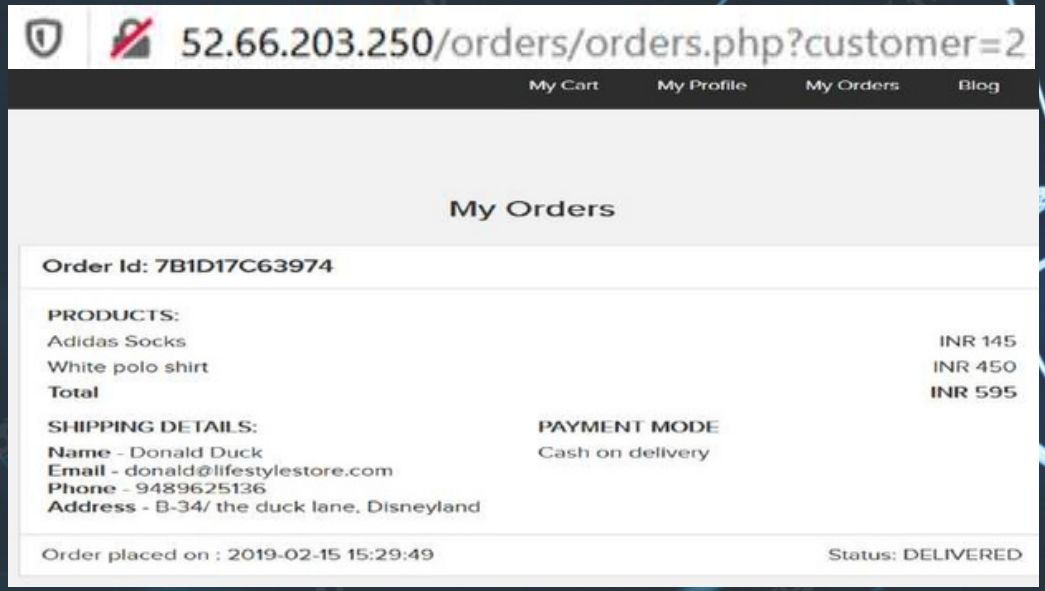
- Customer Data (GET)

Observations :

the following observation are being made related to the vulnerabilities of the website

Login to your account and go to “My Orders” section, you’ll see a GET parameter as shown below, “customer=2”.

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



Business Impact:

This vulnerability can be exploited by hackers to carry out targeted phishing attacks on the users and the information can also be sold to the black-market.

As there is no rate limiting checks, attacker can brute-force the “user_id” for all possible values and get bill information of each and every user of the organization resulting is a massive information leakage.

Recommendations:

Take the following precautions :

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

These parameters are vulnerable to XSS.

Relevant URL :

13.234.113.207/products/details.php?p_id=2

Affected Parameters :

Comment / Review Box

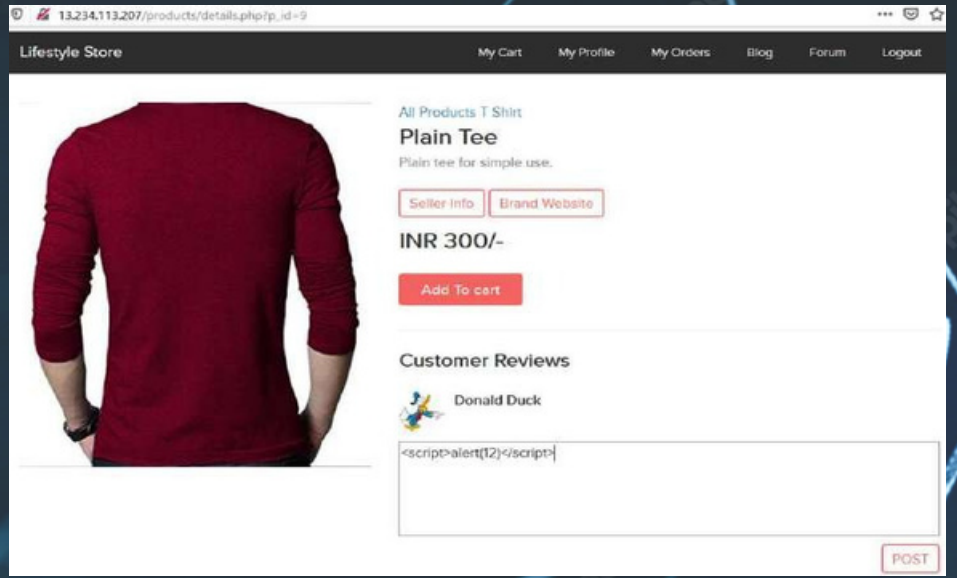
Payload :

<script>alert(1)</script>

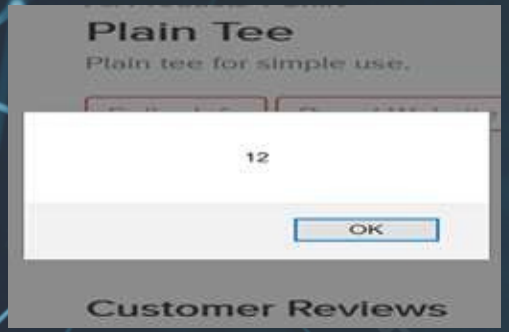
Observations :

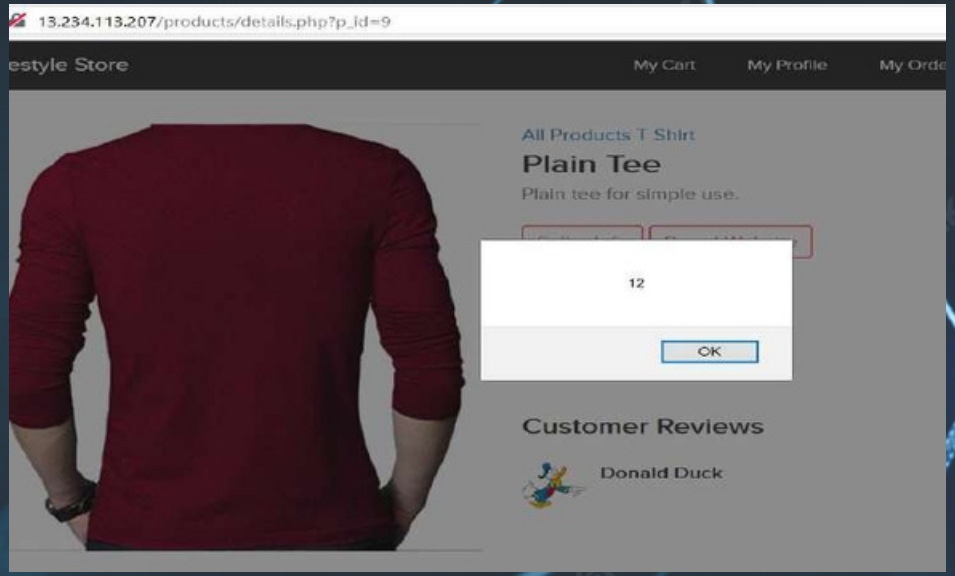
the following observation are being made related to the vulnerabilities of the website

- We have an issue, in the review / comment section.
- Inject payload <script>alert(12)</script>



An alert is registered in the pop-up when submitting.





Business Impact:

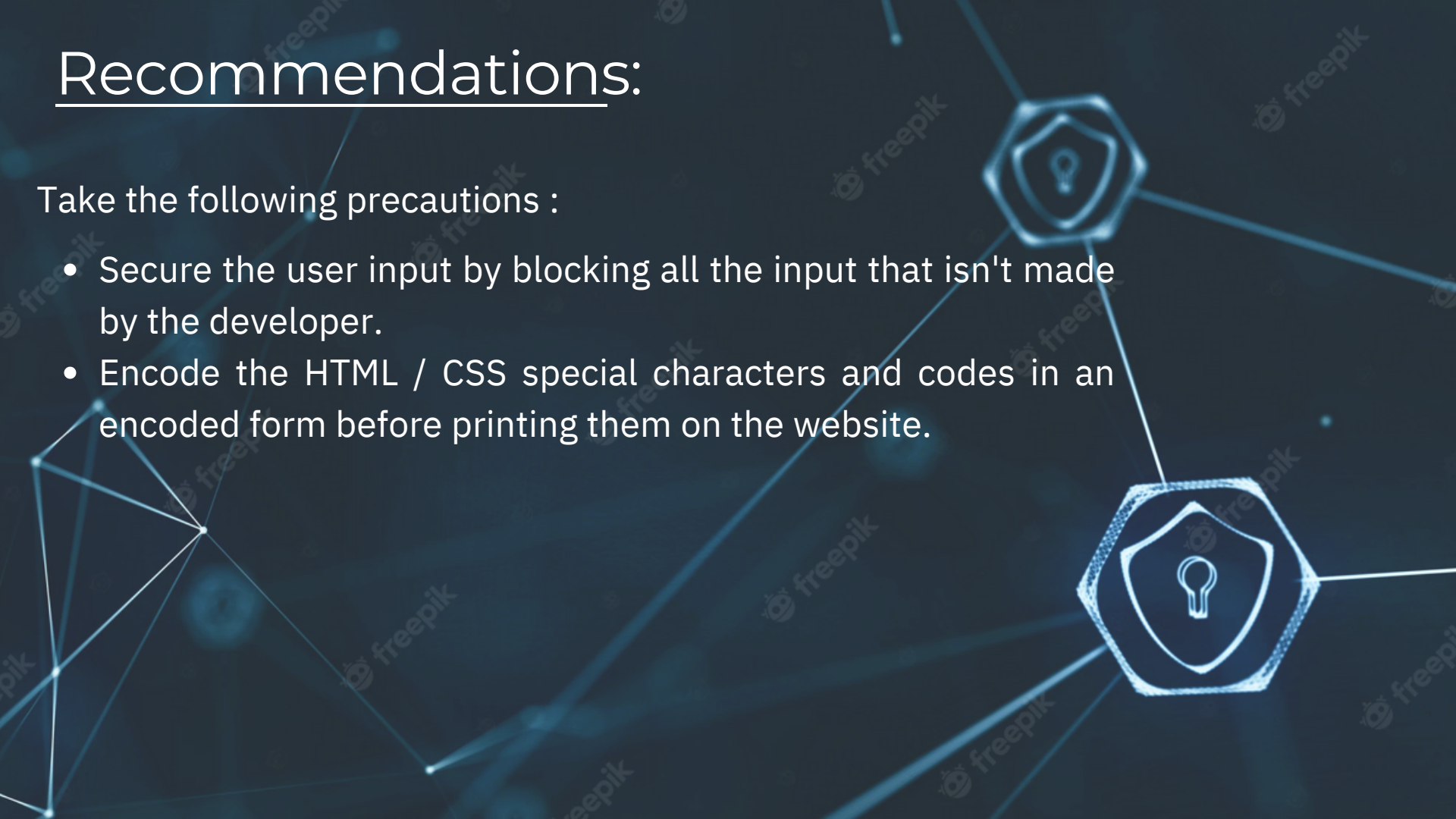
- As the attacker can inject arbitrary HTML, CSS and JavaScript via the URL, he/she can put any content on the page like phishing pages, and can even host explicit content that could compromise the reputation of the organization.

- When the attacker sends the link with the payload to the victim, the victim sees a modified content on the website. As the user trusts the website, he/she will trust the content.

Recommendations:

Take the following precautions :

- Secure the user input by blocking all the input that isn't made by the developer.
- Encode the HTML / CSS special characters and codes in an encoded form before printing them on the website.



This URL is vulnerable.

Relevant URL :

- http://35.154.158.143/robots.txt

Observations :

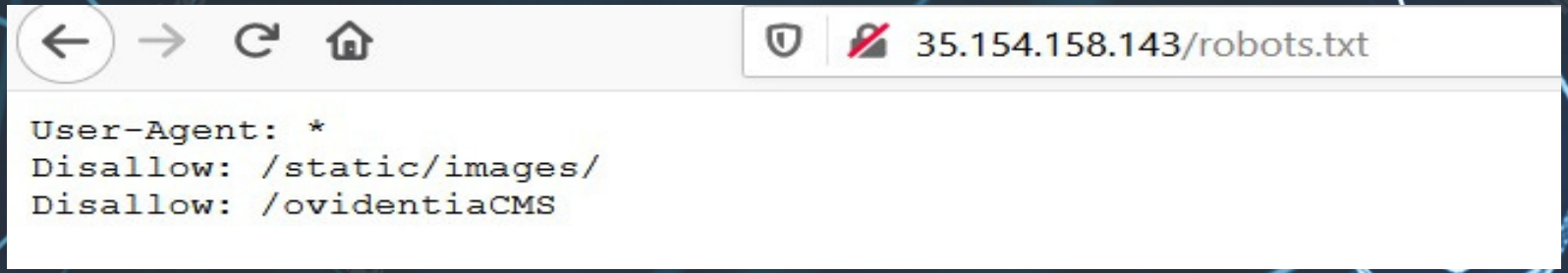
the following observation are being made related to the vulnerabilities of the website

Go to http://35.154.158.143/robots.txt

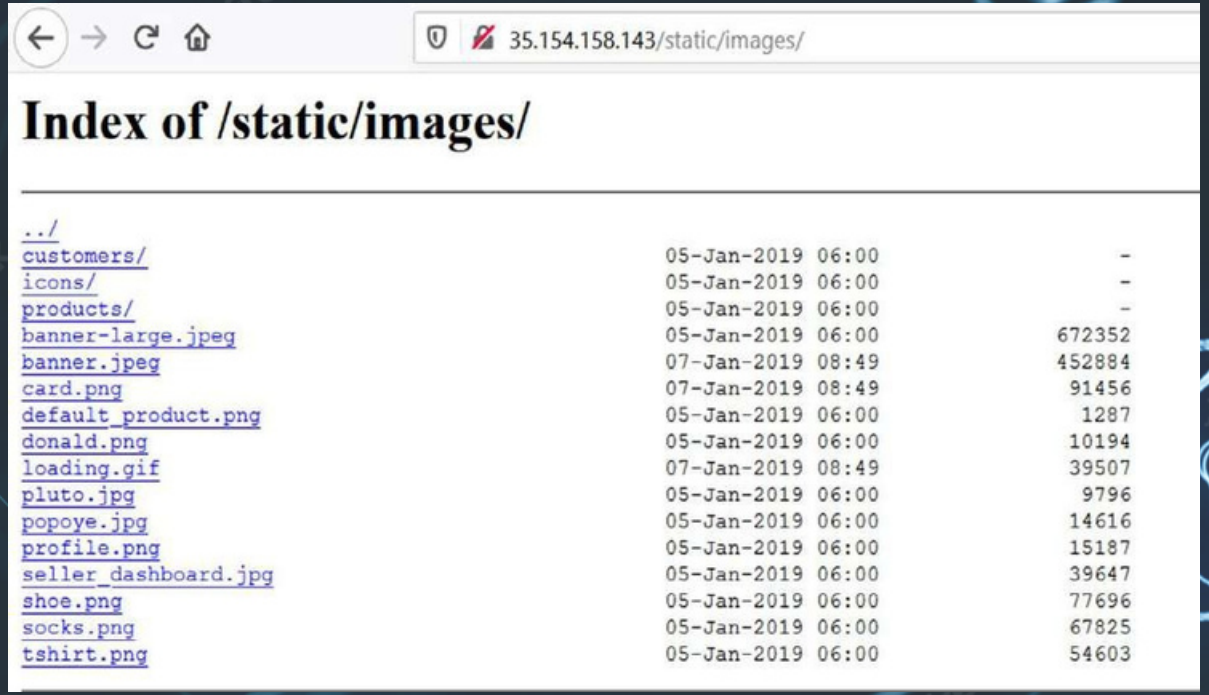
Here, we can see a complete list and directories of the customers, images of products and all the products-page info.

We can also see the administrator directory.

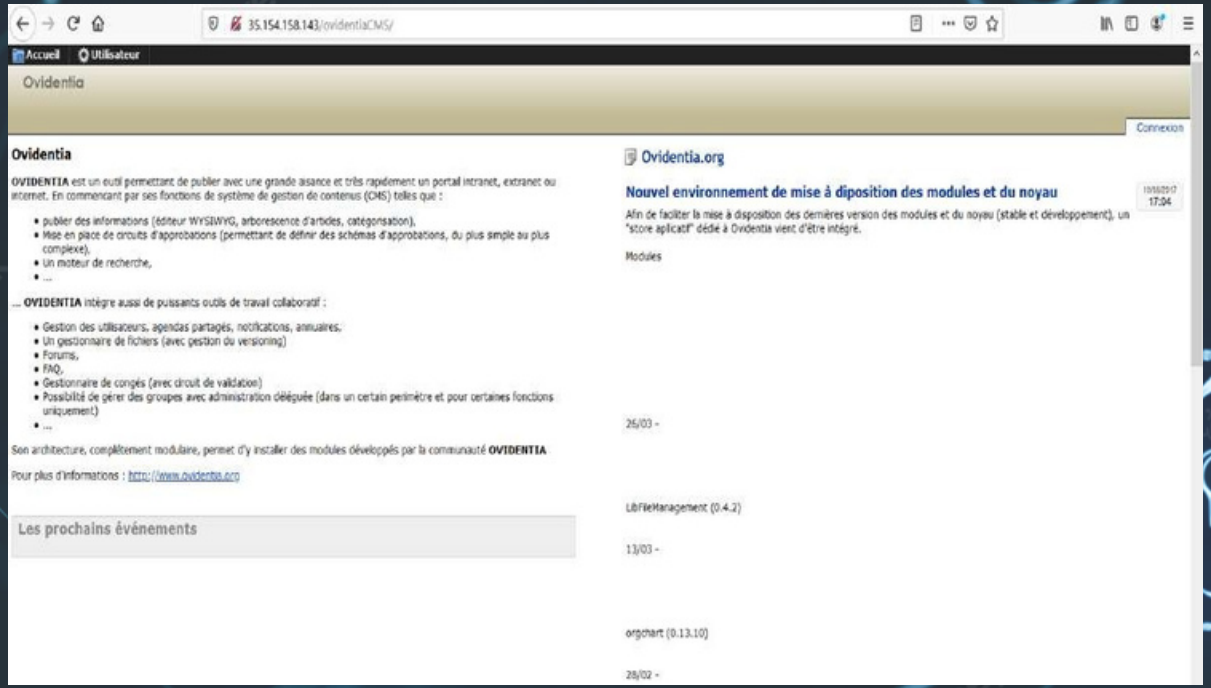
This has a weak password flaw in Ovidentia CMS, which lets an attacker access the administrator panel without much trials.



- /static/images



- /ovidentiaCMS/



Business Impact:

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

Recommendations:

Take the following precautions :

- Disable all the directory listings.
- Include a index.html in all folders with default messages.
- Remove all the default passwords and add your own new strong passwords which must have a special character and at least 8 character long for maximum security

Below mentioned URL LEAKS Critical information via PII leakage.

Relevant URL :

http://35.154.158.143/static/images/uploads/products/2socks.jpeg

Affected Parameters :

IMAGE (every image after “products/”)

Observations :

the following observation are being made related to the vulnerabilities of the website

Go to http://35.154.158.143/products.phpand drag any drop product image in a new tab, the following page will look like the one shown below with the image of the product you chose.

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

Business Impact:

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

Recommendations:

Take the following precautions :

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

Below mentioned URL has a major development flaw , as it redirects to password reset link without authentication.

Relevant URL :

http://35.154.158.143/reset_password/customer.php

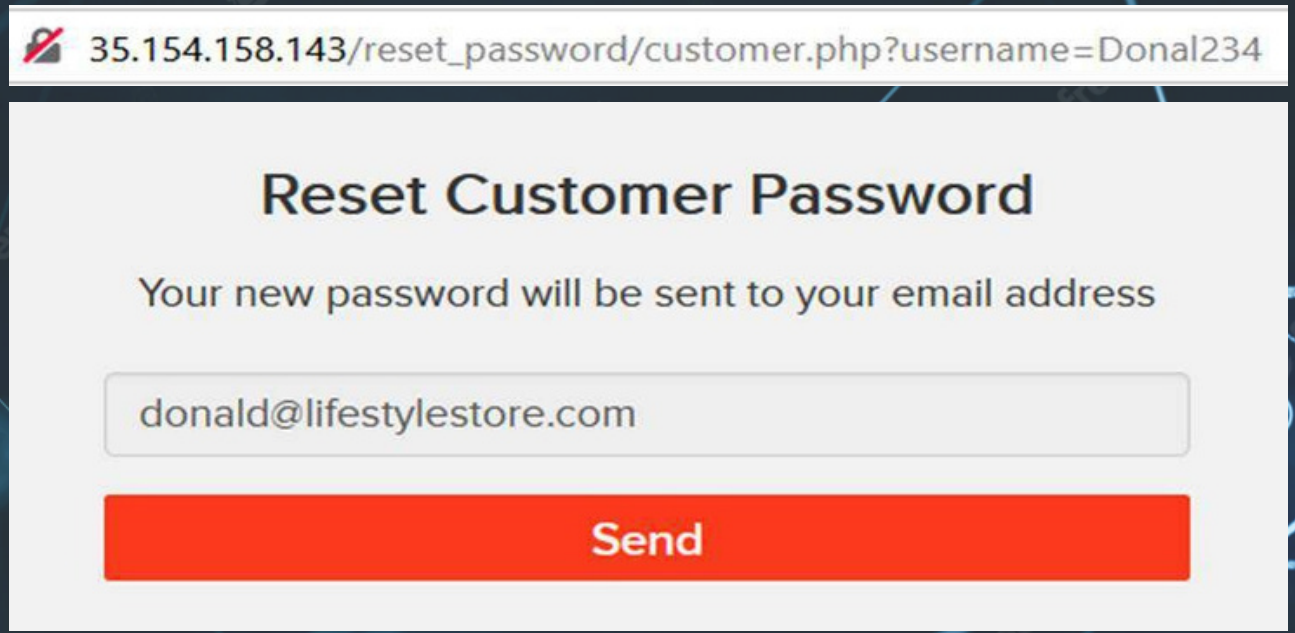
Affected Parameters :

Password Reset

Observations :

the following observation are being made related to the vulnerabilities of the website

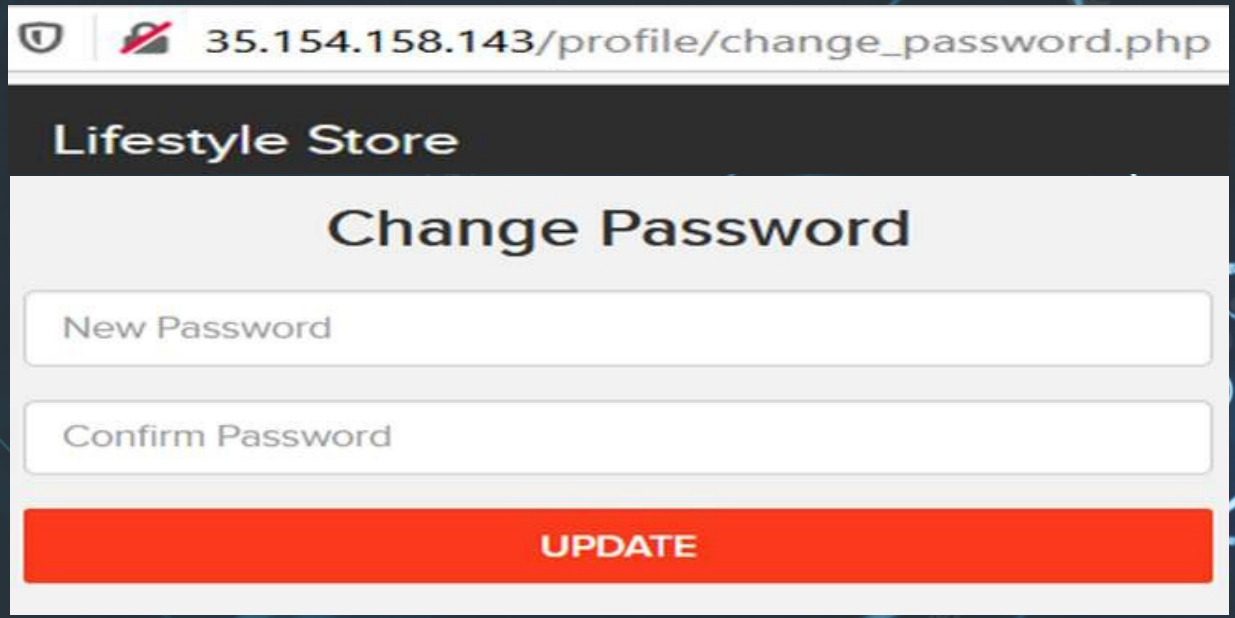
- After adding any username , click “forgot your password” and then input the used username and click “reset password”. We’ll see the page like this, click send.



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

#4

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



Business Impact:

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

Recommendations:

Take the following precautions :

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


Multiple vulnerabilities found in blog site
(PII leakage , temporary XSS and more)
(CRITICAL)

Below are the affected parameters.

URL of the Blog Site : http://15.206.75.142/wondercms/

Relevant URL :

- http://15.206.75.142/wondercms/files/b374kmini.php

Affected Parameters :

- File Upload (POST)

Relevant URL :

- http://15.206.75.142/wondercms/home

Affected Parameters :

- Files (GET)

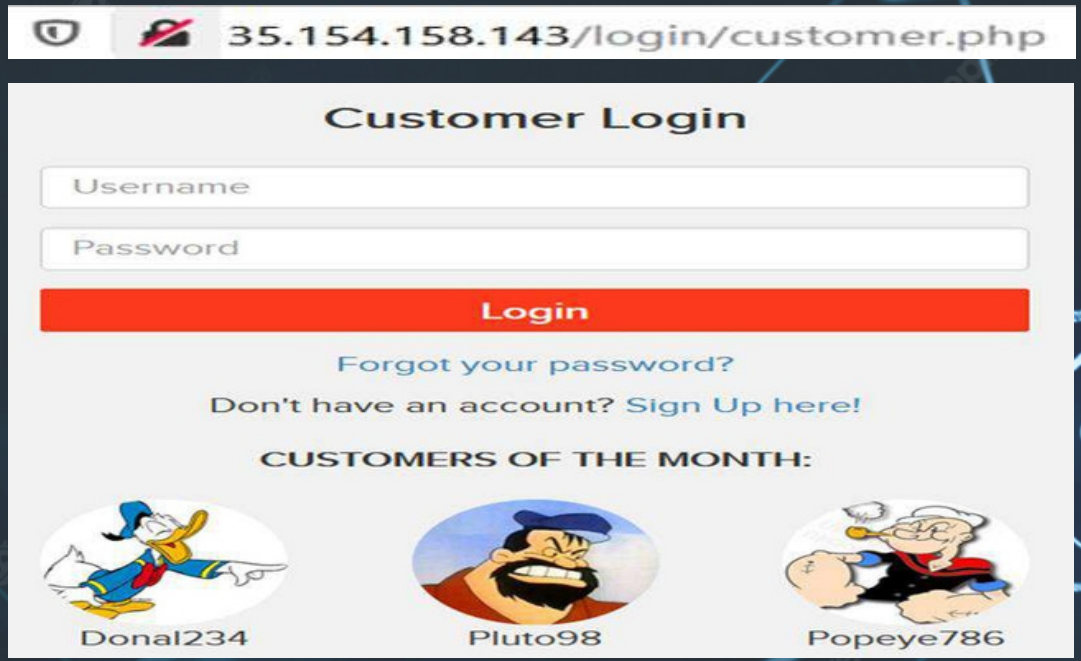
Relevant URL :

- http://13.235.0.176/wondercms/files/minisell.php

Affected Parameters :

- Shell Upload

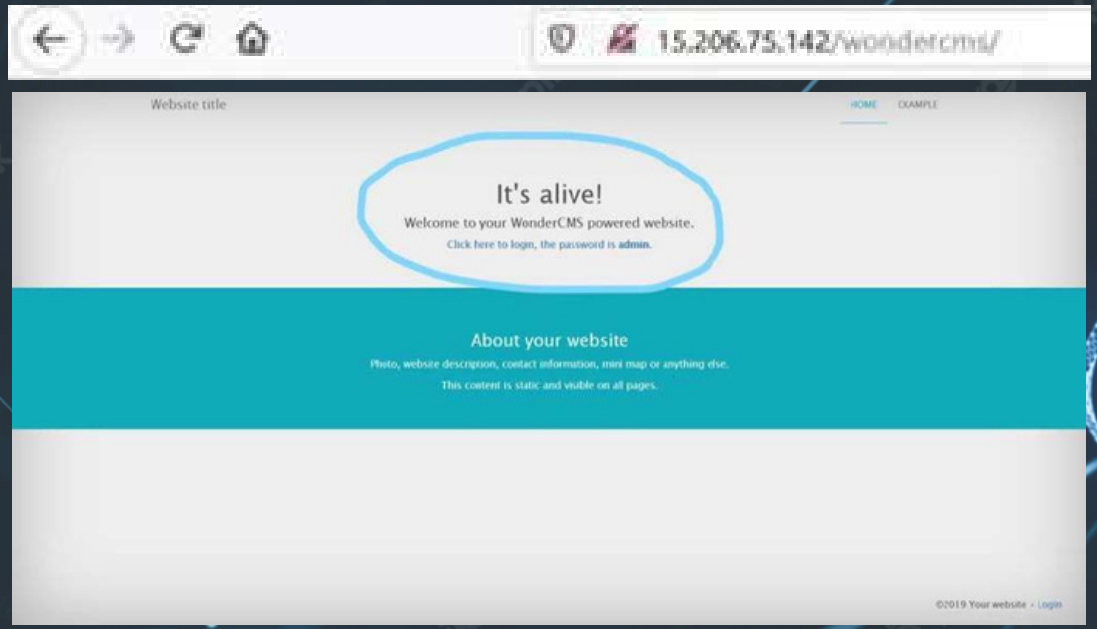
Go to http://35.154.158.143/login/customer.php and you will see names of top customers ,as shown below, take note of any username. ,



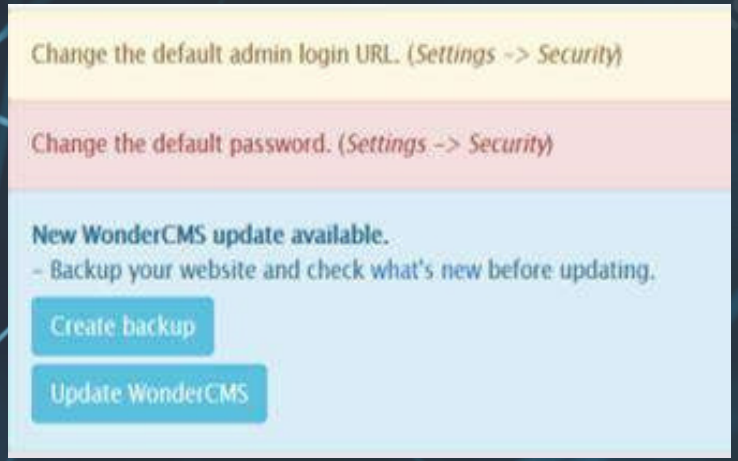
Observations :

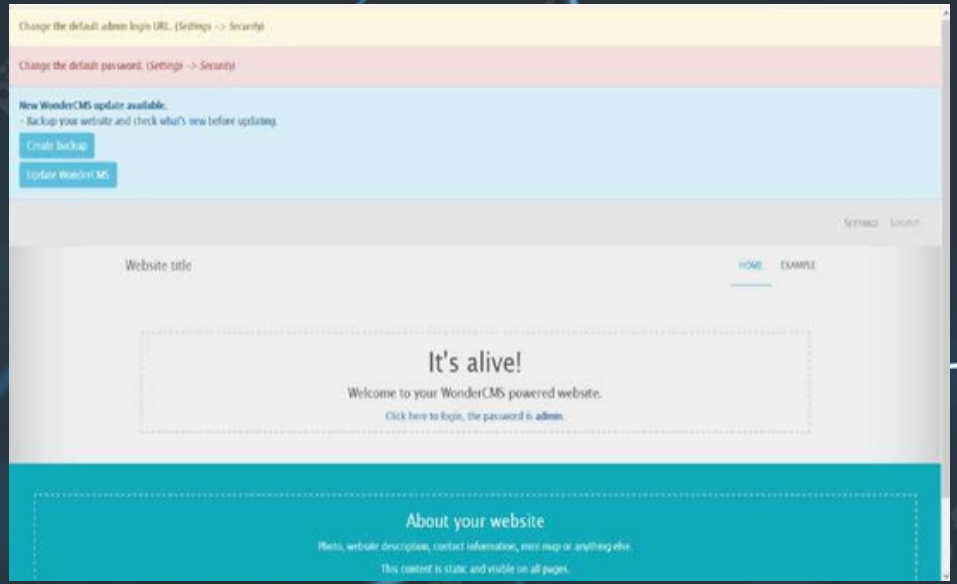
the following observation are being made related to the vulnerabilities of the website

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



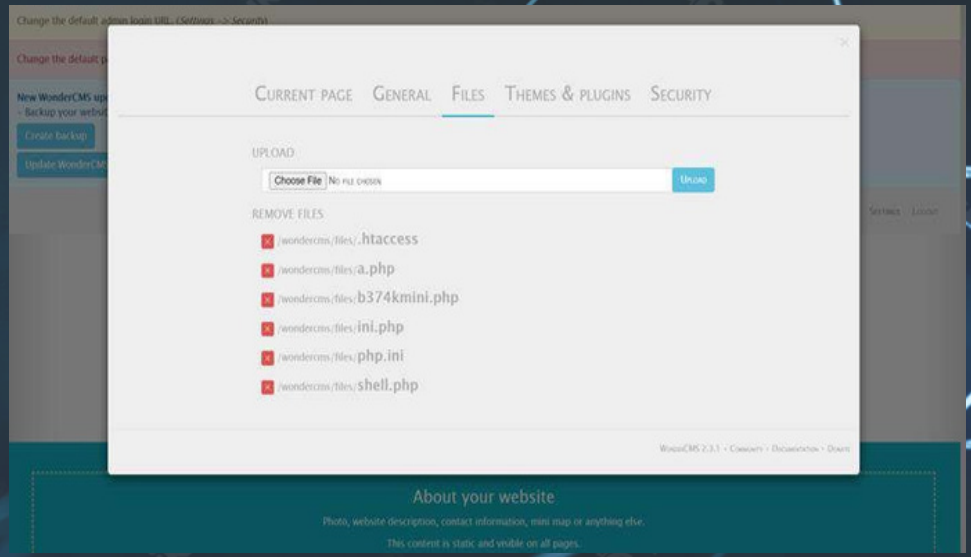
When we log-in as the admin ,at the first page of the site we can see some text written as “It’s alive !” if we click on it , the html codes just starts running.
A hacker can easily make changes and can use the page as his/her phishing portal . This is a classic example of temporary XSS.



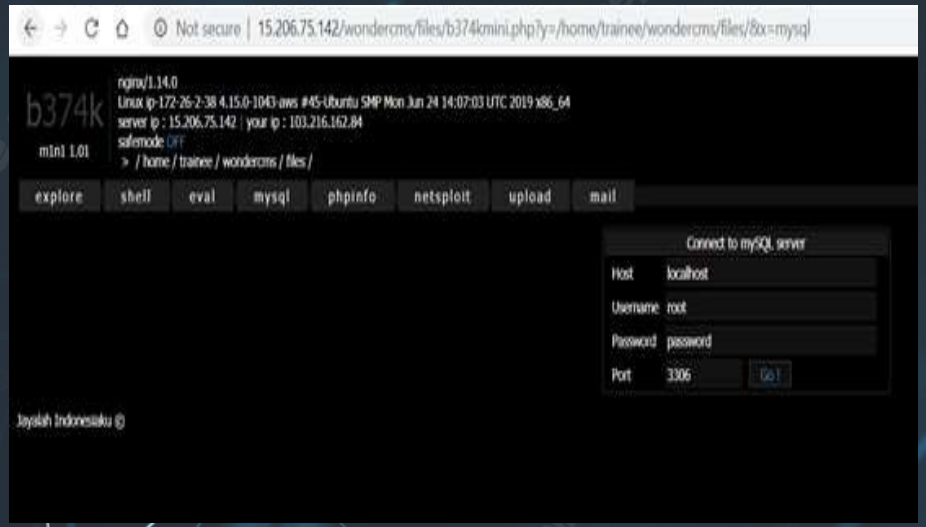


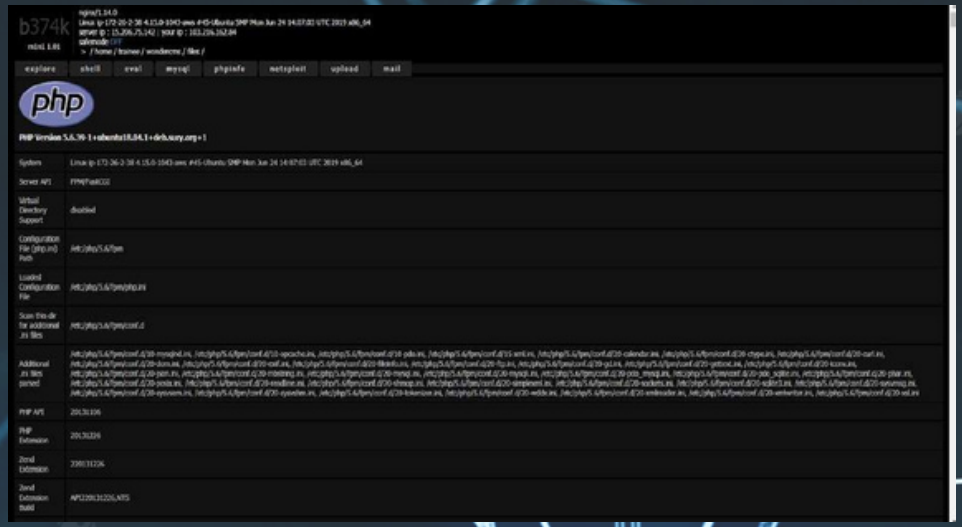
Here, if we select the ‘/wondercms/files/b374kmini.php’ option it will redirect us to a page which will give us many crucial information like server IP address, Linux IP address , the server type, the database, shell, the php info, uploads.

As we are inside the admin account if we select the settings option and go to ‘files’ menu we can see some files with extension ‘.php’ which can give information about the site and also very much capable of taking over the site.

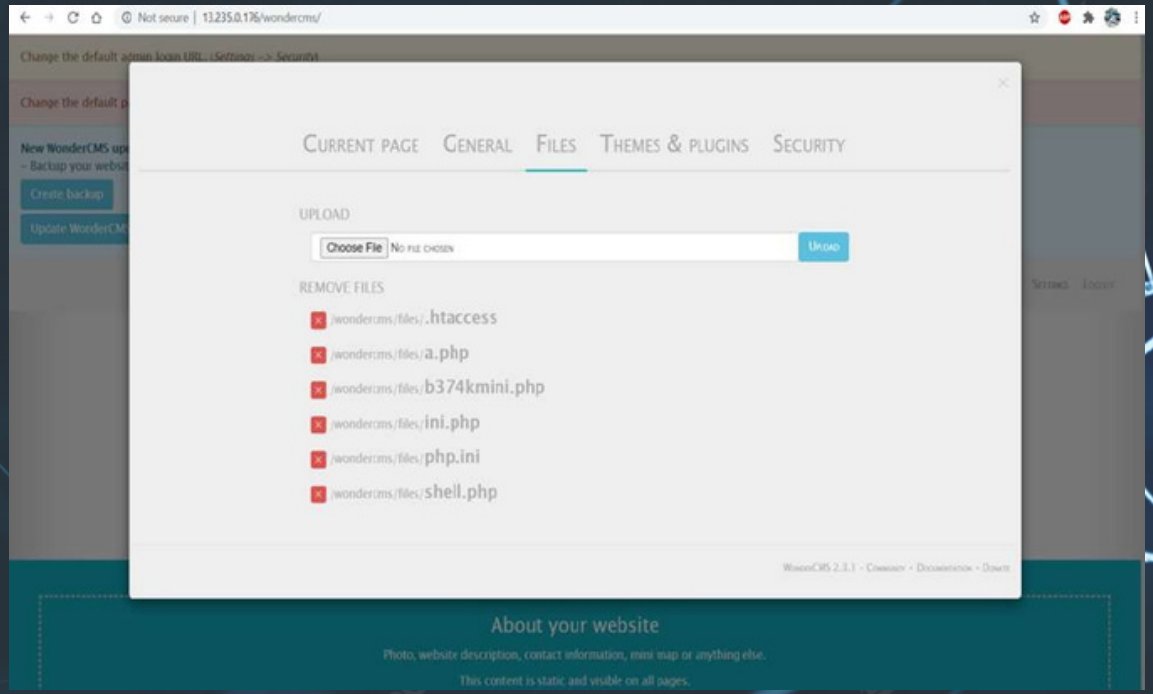


The page is found using the b374K mini shell from which a attacker can know all system (backend) details like versions, and more.





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



Business Impact:

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

Recommendations:

Take the following precautions :

- The website should have proper two factor authentication.
- Try to develop the back end more stronger and secure.
- Remove all directory listings and add proper sanitization

THANK YOU

My name is **Arjun Shetty!!**
my linkedln profile:
https://www.linkedin.com/in/arjun-shetty-255049229
you can contact me on :
91+ 9686630424
my GitHub account :
https://github.com/shettyarjun