

# SHOPPING WEB APPLICATION (LIFESTYLESTORE)

DETAILED WEB DEVELOPER REPORT

MADE BY HRITIK .S. BHAMARE

SUBMITTED ON-08/10/2021

# SECURITY STATUS – EXTREMELY VULNERABLE

- HACKERS CAN STEAL ALL RECORDS FROM THE DATABASES OF THE WEBSITE(SQLI).
- HACKERS CAN TAKE COMPLETE CONTROL OF THE WEBSITE INCLUDING VIEW ,EDIT , ADD OR DELETE FILES AND FOLDERS VIA SHELL UPLOAD.
- HACKERS CAN EXTRACT MOBILE NUMBERS OF ALL CUSTOMERS USING USER-ID (IDOR).
- HACKERS CAN CHANGE THE SOURCE CODE AND CAN UPLOAD ANY MALICIOUS CODE , PHISHING ETC. IN THE WEBSITE VIA SHELL UPLOAD.
- HACKERS CAN TRICK USERS TO CLICK ON MALICIOUS POP UP LINKS AND STEAL INFORMATION VIA CROSS-SITE-SCRIPTING.(XSS)

# VULNERABILITY STATISTICS

Critical

12

Server

7

Moderate

3

Low

3

# VULNERABILITIES FOUND

NO	SEVERITY	VULNERABILITY	COUNT
1	CRITICAL	SQL INJECTION	5
2	SEVERE	CROSS SITE SCRIPTING(XSS)	6
3	CRITICAL	ACCOUNT TAKEOVER(OTP BYPASS)	1
4	CRITICAL	PII LEAKAGE	4
5	CRITICAL	UNAUTHORIZED ACCESS TO CUSTOMER DETAILS	5
6	MODERATE	REDIRECTION	2
7	SEVERE	DIRECTORY LISTINGS	1
8	LOW	INFORMATION DISCLOSURE	2
9	CRITICAL	SERVER SIDE ERRORS	1

# 1.SQL INJECTION

SQL INJECTION  
(CRITICAL)

Below mentioned URL is vulnerable to SQL injection attack.

**AFFECTED URL:** <http://52.66.203.250/products.php?cat=1>

**AFFECTED PARAMETERS :** category(get parameter)

**PAYLOAD :** Cat=1'

# 1.SQL INJECTION

SQL INJECTION  
(CRITICAL)

Here are other similar SQLi in the web application

**AFFECTED URL:**

- <http://52.66.203.250/products.php?cat=2'>
- <http://52.66.203.250/products.php?cat=3'>

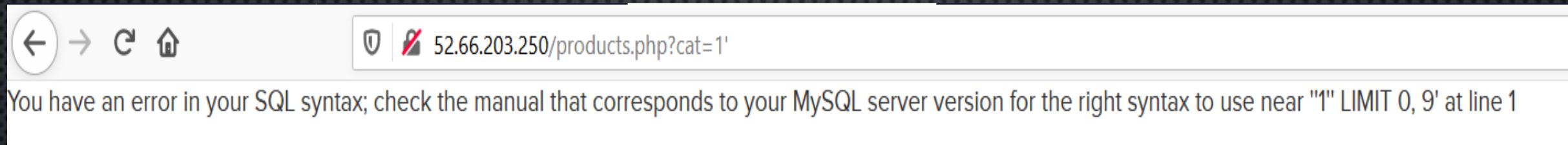
# OBSERVATION

- NAVIGATE TO THE MAIN PAGE OF THE WEBSITE WHERE YOU WILL SEE CATEGORIES OPTION , CLICK ON “T-SHIRT” OR “SOCKS” OR “SHOES” TO GET INTO THIS URL ,YOU WILL SEE PRODUCTS AS PER THE OPTION YOU HAVE CHOSEN BUT NOTICE THE GET PARAMETER IN THE URL.



# OBSERVATION

- APPLY A SINGLE QUOTE IN THE GET PARAMETER AND IT WILL THROW AN MYSQL ERROR.



# OBSERVATION

- WHEN WE PUT “--+” IN THE END OF THE PARAMETER WE’LL GET THE PAGE BACK TO ITS ORIGINAL FORM, CONFIRMING THE MYSQL ERROR.

Lifestyle Store

Blog Forum Sign Up Login

Search

T Shirt Socks Shoes

Basic T shirt 350

Simple T Shirts 550

Plain Tee 300

FOREVER young

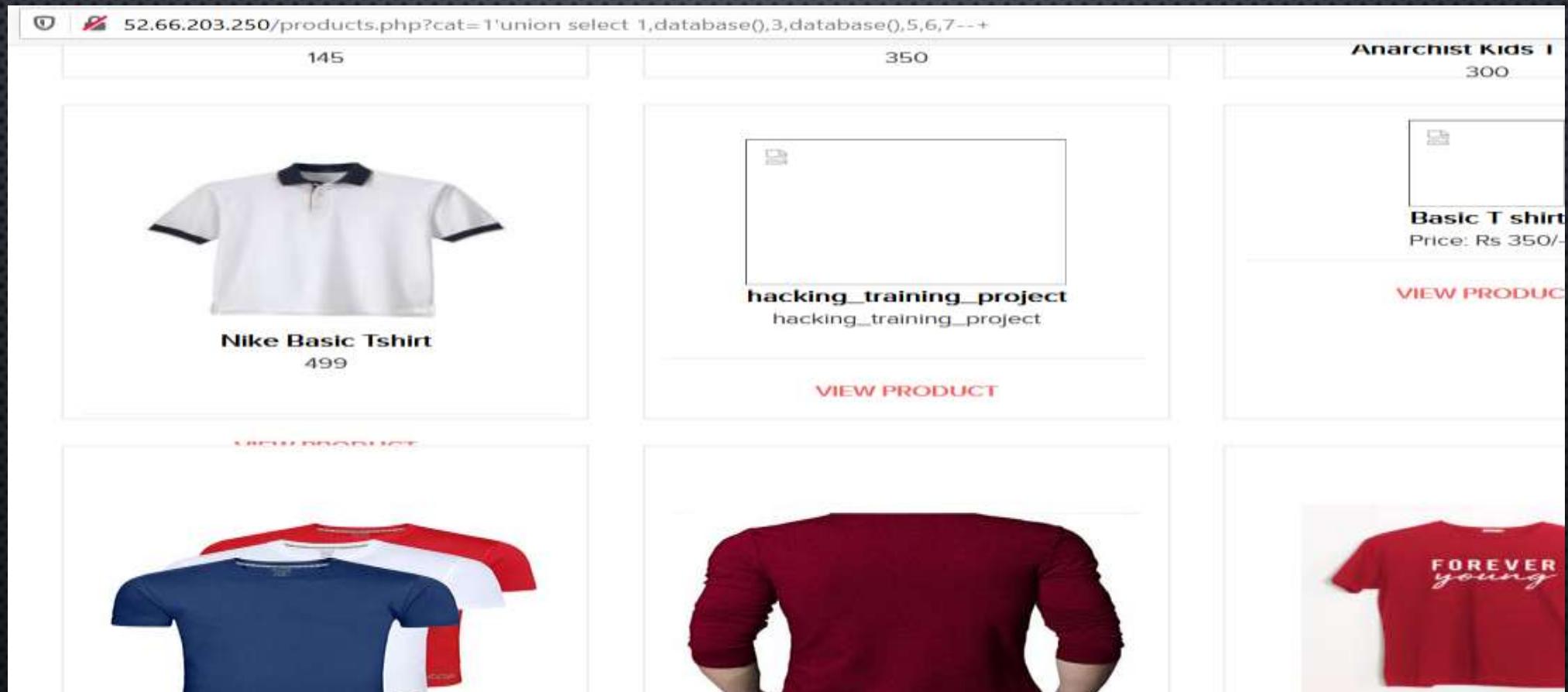
White polo shirt

Marhoon T Shirt

52.66.203.250/products.php?cat=1--+

# PROOF OF CONCEPT(POC)

- ATTACKER CAN EXECUTE COMMANDS AS SHOWN BELOW TO GET CRITICAL INFORMATION ,HERE WE HAVE USED THE BELOW PAYLOAD TO FIND THE NAME OF THE DATABASE OF MYSQL.



# POC

- **NO OF DATABASES: 2**
  - INFORMATION\_SCHEMA
  - HACKING\_TRAINING\_PROJECT
- **NO OF TABLES IN HACKING\_TRAINING\_PROJECT: 10**
  - ORDER\_ITEMS
  - BRANDS
  - CART\_ITEMS
  - CATEGORIES
  - CUSTOMERS
  - ORDERS
  - PRODUCT\_REVIEWS
  - PRODUCTS
  - USERS
  - SELLERS

# BUSINESS IMPACT

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 USERS TABLE WHICH SHOWS USER CREDENTIALS BEING LEAKED, ALTHOUGH THEY ARE IN ENCRYPTED FORM BUT DECRYPTION IS QUITE EASY FOR HACKERS.

name	password
admin	\$2y\$10\$xmldvrxscxdywsrdx5Yse1NAwx.7pQ2nQmATcovH4CFssxgyJTk1
Donald Duck	\$2y\$10\$nmBSP5Fma1dxim/S3s./p5xR6GtKvjry7ysJtxokBqoJURAHso
Brutus	\$2y\$10\$xmldvrxscxdywsrdx5Yse1NAwx.7pQ2nQmATcovH4CFssxgyJTk1
Chandan	\$2y\$10\$4czBEirgthxdvt1hwu1ivuFELe03rr.Gicdp03NjrlsOveiOKLVDa
Popeye the sailor man	\$2y\$10\$Fkv1RfwYTioWw2CaZtAQuXvnhGAUjt/If/yTqkNPc5zTrsvm7EeC
Radhika	\$2y\$10\$RYxNhoYV/G4g7otFwpqYaexvHi8rf6Xxui8kt1wtrfghTutCA8JC.
Nandan	\$2y\$10\$G.cRNLMEiG79ZFXElHg.R.o95334U0xmZu4.9MqZR5614ucwnk59K
Murthy Adapa	\$2y\$10\$mzQGzd4sdsj2EuNpc1oe4ek18c1Abs0T2P1a1P6eV1DPR.11uubDG
John Albert	\$2y\$10\$GhDB8h1x6XjPMY12Gz1vb07Y3en97u1/.oXTZLmYqb6F18FBgecvG
Bob	\$2y\$10\$kiuikn3HPFbuTTk757LNurxzqCOLX3emGy0/ux16j0oG37dCGKLq
Jack	\$2y\$10\$z/nyN1krj76m9itMz4N51oeRxy6Gkqi9N/UBcJu5ze07eM7N4ptHu
Bulla Boy	\$2y\$10\$HT5oiRMetqaz7xGZPE9s2.Mk1yF4PnYDJHCwbm2w/xuKpjEEI/zjG
hunter	\$2y\$10\$pb3U9iFxwBgsb12AkBpiEeIBdhijfwy9y.xV23q12ggbMCyn7N3g2
asd	\$2y\$10\$At5pFZnRwpjCD/yNnjWDL.L3Cc4Cv0w8Q/WEHmwzBFqVIkBQFpCF2
acdc	\$2y\$10\$J5OB78.gpucuLTwpHwbcPedYcain.Y1.tstLyQtK17FzdspmIRrb1

ATTACKER CAN USE THIS INFORMATION TO 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

- TAKE THE FOLLOWING RECOMMENDATIONS TO SECURE AND AVOID SQL DATABASE EXPLOITATION.
- PREPARED STATEMENTS: USE SQL PREPARED STATEMENTS AVAILABLE IN ALL WEB DEVELOPMENT LANGUAGES AND FRAMEWORKS TO AVOID ATTACKER BEING ABLE TO MODIFY SQL QUERY.
- DO NOT RUN DATABASE SERVICE AS ADMIN/ROOT USER.
- DISABLE/REMOVE DEFAULT ACCOUNTS, PASSWORDS AND DATABASES .
- ASSIGN EACH DATABASE USER ONLY THE REQUIRED PERMISSIONS AND NOT ALL PERMISSIONS
- CHARACTER ENCODING: CONVERT THE SIMPLE LOOKING CODES TO DIFFERENT CHARACTERS LIKE ‘~’/’^’.IT IS ALSO SUGGESTED TO FOLLOW HTML AND OTHER ENCODINGS.

# 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.ACOUNT TAKEOVER VIA OTP BY PASS

Account  
takeover using  
OTP  
bypass(CRITICAL)

Below mentioned login page allows login via OTP which can be brute-forced.

**AFFECTED URL:** <http://52.66.203.250/login/admin.php>

**AFFECTED PARAMETERS:**OTP(POST)

# OBSERVATION

- NAVIGATE TO <HTTP://52.66.203.250/LOGIN/ADMIN.PHP> YOU WILL SEE A “FORGOT PASSWORD” HYPERLINK WHICH ASKS FOR OTP WHICH IS SENT TO VICTIM’S MOBILE NUMBER ,WRITE ANY ANONYMOUS 3 DIGIT OTP AND INTERCEPT THE REQUEST WITH BURP SUITE.

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

festyle Store

Reset Admin Password

Enter 3 digit OTP sent on your registered mobile number

Ex: 321

Reset Password

# OBSERVATION

- FOLLOWING REQUEST WILL BE GENERATED IN BURP USING OTP PARAMETER (GET).

```
GET /reset_password/admin.php?otp=123 HTTP/1.1
Host: 52.66.203.250
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Geck
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://52.66.203.250/reset_password/admin.php?otp=123
Cookie: key=99ED5631-C072-64B1-BF30-655746AE1719; PHPSESSID=mflois
Upgrade-Insecure-Requests: 1
```

# OBSERVATION

- WE'LL BRUTE FORCE BY GETTING ALL COMBINATION OF 3 DIGIT OTP'S AND WRITE THE CORRECT ONE TO BY PASS.

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload position.

Attack type: **Sniper**

```
1 GET /reset_password/admin.php?otp=$1$2$3$ HTTP/1.1
2 Host: 52.66.203.250
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://52.66.203.250/reset_password/admin.php?otp=123
```

# BUSINESS IMPACT

A MALICIOUS HACKER CAN GAIN COMPLETE ACCESS TO ADMIN ACCOUNT JUST BY BRUTE-FORCING DUE TO RATE LIMITING FLAW AS A HACKER CAN ATTEMPT AS MANY TIMES AS HE WANTS AS THERE IS NO BOUNDS IN NO OF TRIES SO,THIS LEADS TO COMPLETE COMPROMISE OF PERSONAL USER DATA OF EVERY CUSTOMER.  
ATTACKER ONCE LOGS IN CAN THEN CARRY OUT ACTIONS ON BEHALF OF THE VICTIM WHICH COULD LEAD TO SERIOUS FINANCIAL LOSS TO HIM/HER.

# RECOMMENDATIONS

- TAKE THE FOLLOWING PRECAUTIONS
  - USE RATE LIMITING CHECKS ON THE NO OF TIMES THE OTP REQUEST AND CHECKING.
  - OTP SHOULD BE AT LEAST OF 6 DIGITS AS IT IS MORE SECURE BY HAVING A LONGER OTP THAN JUST A 3 DIGIT OTP.
  - OTP SHOULD EXPIRE IN A PARTICULAR TIME LIKE 2 MINUTES OR 10 TO MAKE AUTHORIZATIO IT MORE SECURE.

### 3.UNAUTHORIZED ACCESS TO CUSTOMER DETAILS

Unauthorized Access to Customer Details (critical)	<p>The My Orders section of the website suffers from an Insecure direct Object Reference(IDOR), THAT Allows Hackers to get access to any other customers order details and more.</p> <p><b>AFFECTED URL:</b> <a href="http://52.66.203.250/orders/orders.php?customer=2">http://52.66.203.250/orders/orders.php?customer=2</a></p> <p><b>AFFECTED PARAMETERS:</b>CUSTOMER NO. (GET)</p>

# UNAUTHORIZED ACCESS TO CUSTOMER DETAILS

Unauthorized  
Access to  
Customer Details  
(critical)

SIMILAR ISSUES ON THIS URL ALSO.,

**AFFECTED URL:** [http://52.66.203.250/products/details.php?p\\_id=7](http://52.66.203.250/products/details.php?p_id=7)

**AFFECTED PARAMETERS:** P\_ID (GET)

# OBSERVATION

- LOGIN TO YOUR ACCOUNT AND GO TO “MY ORDERS” SECTION, YOU’LL SEE A GET PARAMETER AS SHOWN BELOW, “CUSTOMER=2”

Lifestyle Store      My Cart      My Profile      My Orders      Blog

## My Orders

**Order Id:** 7B1D17C63974

PRODUCTS:	INR 145
Adidas Socks	INR 145
White polo shirt	INR 450
<b>Total</b>	<b>INR 595</b>
SHIPPING DETAILS:	PAYMENT MODE
Name - Donald Duck	Cash on delivery
Email - donald@lifestylestore.com	
Phone - 9489625136	
Address - B-34/ the duck lane, Disneyland	

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

# OBSERVATION

- CHANGE THE CUSTOMER NUMBER TO ANY OTHER RANDOM NUMBER IN OUR CASE I AM GOING TO WRITE 3 AND YOU'LL SEE OTHER CUSTOMER'S ORDER DETAILS.

The screenshot shows a web browser window with the URL [52.66.203.250/orders/orders.php?customer=3](http://52.66.203.250/orders/orders.php?customer=3). The page is titled "lifestyle Store" and features navigation links for "My Cart", "My Profile", "My Orders", and "Blog". The main content area is titled "My Orders" and displays an order with the following details:

Order Id: 8699CEC4FDEA	
<b>PRODUCTS:</b>	
Red and Black Shoes	INR 2999
Marhoon T Shirt	INR 199
<b>Total</b>	<b>INR 3198</b>
<b>SHIPPING DETAILS:</b>	
Name - Brutus	<b>PAYMENT MODE</b> Cash on delivery
Email - Pluto@lifestylestore.com	
Phone - 8912345670	
Address - A-56 Sallor's ship, popeyeworld	
Order placed on : 2019-02-15 16:35:31	Status: DELIVERED

# BUSINESS IMPACT-EXTREMELY HIGH

- 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/BALCKMARKET.
- MORE OVER, AS THERE IS NO RATELIMITING 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 WILL ONLY SEE HIS/HER DATA ONLY.
  - 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

## 4. REFLECTED CROSS-SITE-SCRIPTING(XSS)

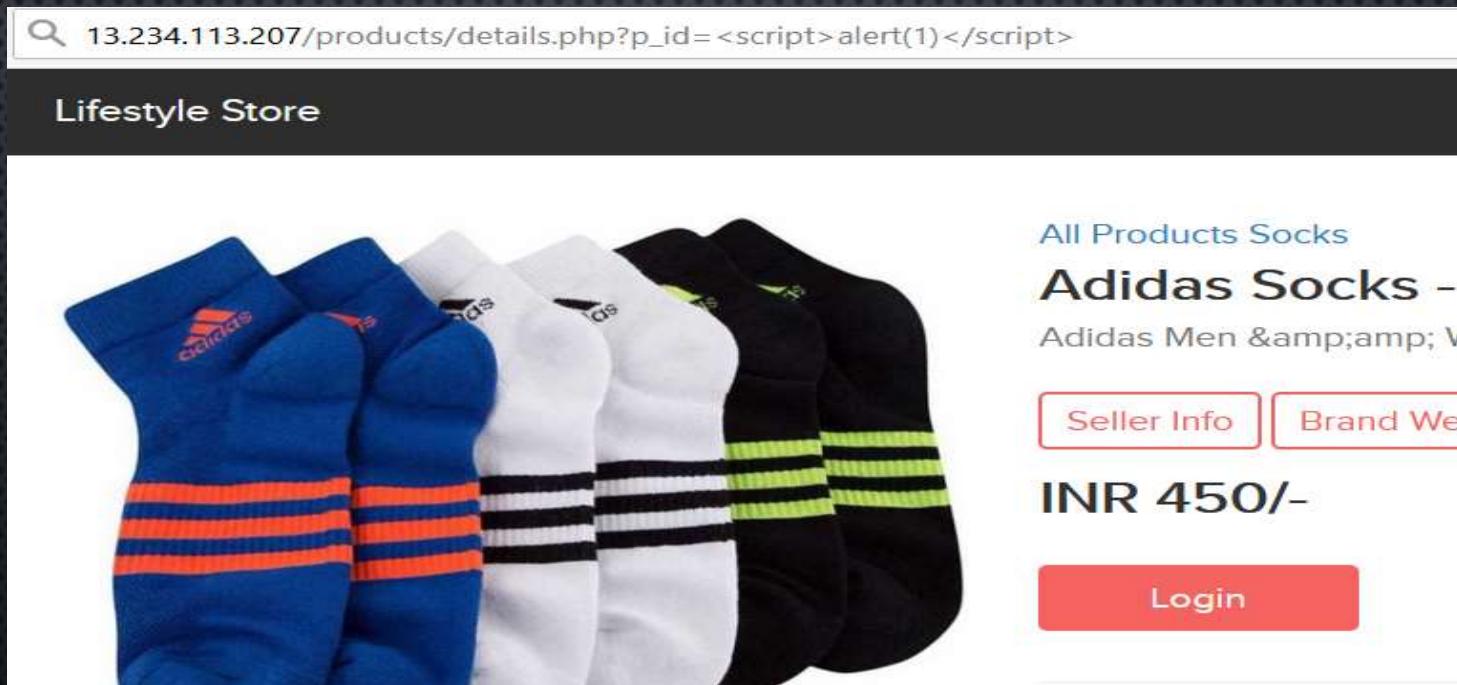
REFLECTED CROSS-SITE- SCRIPTING(XSS) (SEVERE)	<p>Below mentioned parameters are affected to XSS.</p> <p><b>Affected URL:</b> 13.234.113.207/products/details.php?p_id=2</p> <p><b>AFFECTED PARAMETER:</b> URL(any thing after p_id)</p> <p><b>PAYLOAD:</b></p> <ul style="list-style-type: none"><li>• &lt;script&gt;alert(1)&lt;/script&gt;</li></ul>

## 4. REFLECTED CROSS-SITE-SCRIPTING(XSS)

REFLECTED CROSS-SITE- SCRIPTING(XSS) (SEVERE)	<p>Below mentioned parameters are also affected to XSS.</p> <p><b>AFFECTED URL:</b> 13.234.113.207/products/details.php?p_id=2</p> <p><b>Affected Parameter:</b> comment(review box)</p> <p><b>PAYLOAD:</b></p> <ul style="list-style-type: none"><li>• In review comment box &lt;script&gt;alert(1)&lt;/script&gt;</li></ul>

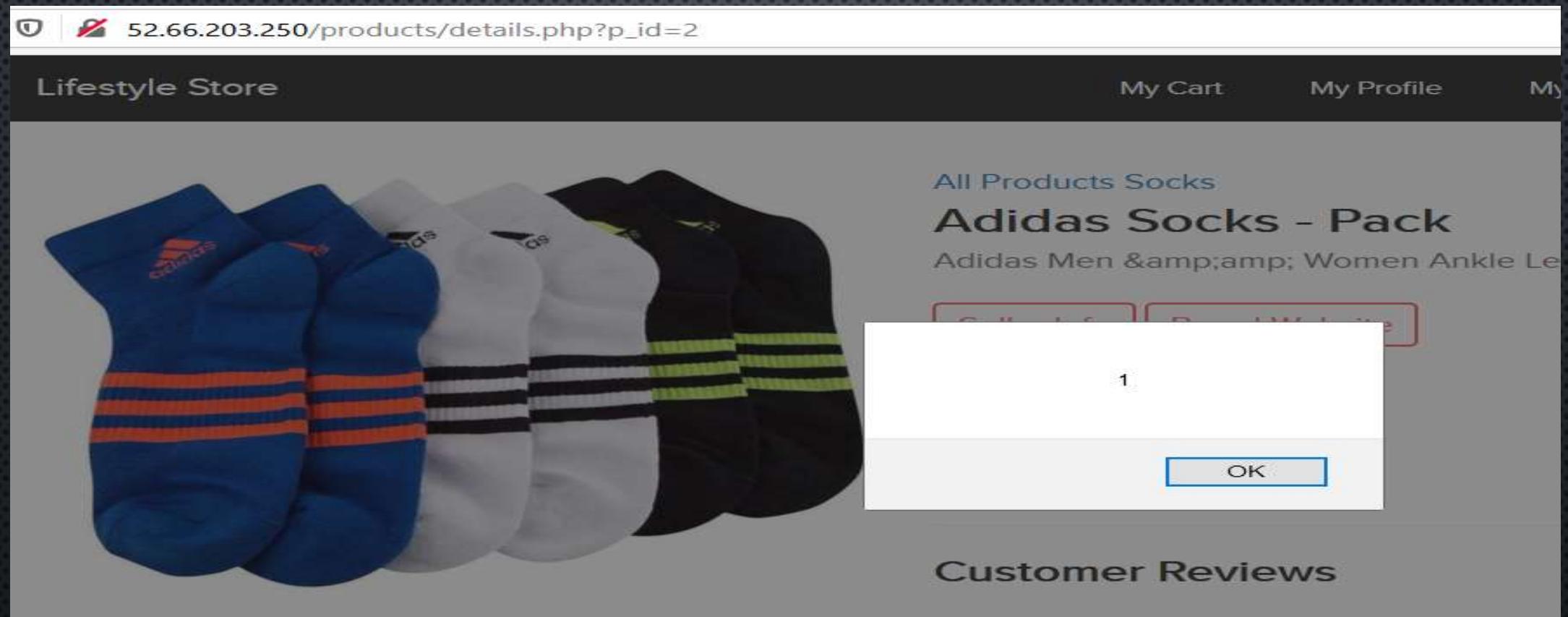
# OBSERVATION

- NAVIGATE TO THE SITE AND LOG IN TO YOUR ACCOUNT GO TO PRODUCTS AND SELECT ANY PRODUCT. NOW URL SHOWS THE ID OF THE PRODUCT YOU ARE ON, REPLACE THAT WITH THE SHOWN PAYLOAD.



# OBSERVATION

- AFTER ENTERING THE PAYLOAD PRESS ENTER THE PAGE WILL REDIRECT YOU TO HOME PAGE BUT WHEN YOU CLICK ON THE SAME PRODUCT AGAIN IT WILL SHOW THE SHOWN RESULT.



POC

# IN REVIEW/COMMENT SECTION XSS IS PRESENT ALSO.

13.234.113.207/products/details.php?p\_id=9

Lifestyle Store      My Cart      My Profile      My Orders      Blog      Forum      Logout



All Products T Shirt  
**Plain Tee**  
Plain tee for simple use.

Seller Info      Brand Website

**INR 300/-**

Add To cart

**Customer Reviews**

Donald Duck

<script>alert(12)</script>

POST

POC

13.234.113.207/products/details.php?p\_id=9

estyle Store My Cart My Profile My Order



All Products T Shirt  
**Plain Tee**  
Plain tee for simple use.

12

OK

Customer Reviews

 Donald Duck

This screenshot shows a product detail page for a plain t-shirt. The URL in the address bar is 13.234.113.207/products/details.php?p\_id=9. The page title is 'estyle Store'. The main image on the left shows a person wearing a red t-shirt. To the right, the product is identified as 'Plain Tee' with the description 'Plain tee for simple use.' Below the product information is a modal dialog box containing the number '12' and an 'OK' button. Further down the page, there is a section titled 'Customer Reviews' featuring a small icon of Donald Duck.

## BUSINESS IMPACT-HIGH

AS ATTACKER CAN INJECT ARBITRARY HTML CSS AND JAVASCRIPT VIA THE URL, ATTACKER CAN PUT ANY CONTENT ON THE PAGE LIKE PHISHING PAGES, AND EVEN HOST EXPLICIT CONTENT THAT COULD COMPROMISE THE REPUTATION OF THE ORGANIZATION.

ALL ATTACKER NEEDS TO DO IS SEND THE LINK WITH THE PAYLOAD TO THE VICTIM AND VICTIM WOULD SEE HACKER CONTROLLED CONTENT ON THE WEBSITE. AS THE USER TRUSTS THE WEBSITE, HE/SHE WILL TRUST THE CONTENT.

# RECOMMENDATIONS

- TAKE THE FOLLOWING PRECAUTIONS
  - SECURE THE USER INPUT BY BLOCKING ALL THE INPUT YOU DON'T WANT.
  - CONVERT THE HTML SPECIAL CHARACTERS IN AN ENCODED FORM 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)

## 5.DIRECTORY LISTINGS

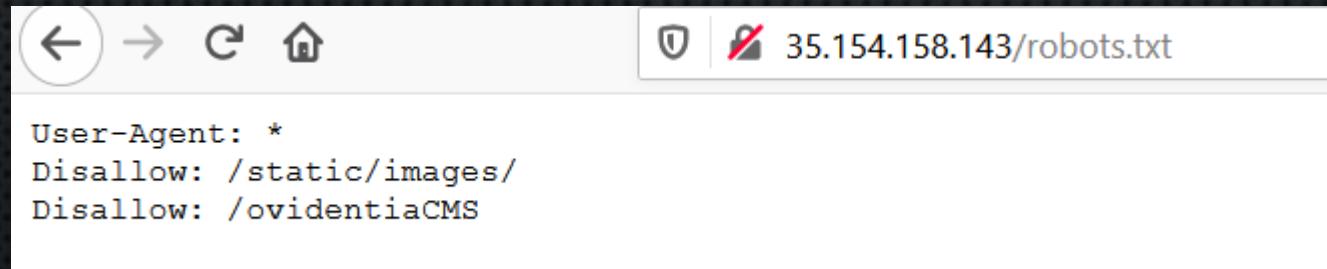
DIRECTORY  
LISTINGS  
(Severe)

Below affected URL are vulnerable to reflected XSS.

**Affected URL:** <http://35.154.158.143/robots.txt>

# OBSERVATION

- GO TO <HTTP://35.154.158.143/ROBOTS.TXT>
- COMPLETE LIST AND DIRECTORIES OF THE CUSTOMER AND IMAGES OF PRODUCTS AND ALL THE PRODUCTS PAGE INFO AND ALSO THE ADMINISTRATOR DIRECTORY IS ALSO SHOWN.
- ALSO THIS SUFFERS WITH WEAK PASSWORD FLAW IN OVEDENTIACMS, WHICH LETS AN ATTACKER GET INSIDE THE ADMINISTRATOR PANEL WITHOUT MUCH TRYING.



POC



The screenshot shows a web browser window with the URL `35.154.158.143/static/images/`. The page title is "Index of /static/images/". The left sidebar contains a list of directory entries, while the main content area displays a table of files with their last modified date, time, and size.

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

# POC

The screenshot shows a web browser window with two tabs open. The left tab is titled 'Ovidentia' and displays information about the OVIDENTIA CMS. The right tab is titled 'Ovidentia.org' and displays news articles from the Ovidentia community.

**Ovidentia CMS (Left Tab):**

- Ovidentia**
- OVIDENTIA** est un outil permettant de publier avec une grande aisance et très rapidement un portail intranet, extranet ou internet. En commençant par ses fonctions de système de gestion de contenus (CMS) telles que :
  - publier des informations (éditeur WYSIWYG, arborescence d'articles, catégorisation),
  - Mise en place de circuits d'approbations (permettant de définir des schémas d'approbations, du plus simple au plus complexe),
  - Un moteur de recherche,
  - ...
- ... **OVIDENTIA** intègre aussi de puissants outils de travail collaboratif :
  - Gestion des utilisateurs, agendas partagés, notifications, annuaires,
  - Un gestionnaire de fichiers (avec gestion du versioning)
  - Forums,
  - FAQ,
  - Gestionnaire de congés (avec circuit de validation)
  - Possibilité de gérer des groupes avec administration déléguée (dans un certain périmètre et pour certaines fonctions uniquement)
  - ...
- Son architecture, complètement modulaire, permet d'y installer des modules développés par la communauté **OVIDENTIA**. Pour plus d'informations : <http://www.ovidentia.org>.

**Les prochains événements**

**Ovidentia.org (Right Tab):**

- Ovidentia.org**
- Nouvel environnement de mise à disposition des modules et du noyau**  
Afin de faciliter la mise à disposition des dernières versions des modules et du noyau (stable et développement), un "store applicatif" dédié à Ovidentia vient d'être intégré.  
Modules
- LibFileManagement (0.4.2)  
26/03 -
- orgchart (0.13.10)  
28/02 -

## BUSINESS IMPACT-HIGH

- A HACKER CAN GET ALL THE INFORMATION ON THE CMS AND ALSO GET TACKLE WITH THE ADMINISTRATOR LOG INS AND COMPROMISE THE WHOLE NAME OF THE COMPANY
- A MALICIOUS HACKER CAN TAKE IMPORTANT INFORMATION FROM SELLER POINT OF VIEW AND WHAT PRODUCTS EVERY SELLER IS SELLING AT WHAT PRICE AND ALSO THE INFORMATION OF USERS.

# RECOMMENDATIONS

- DISABLE ALL THE DIRECTORY LISTINGS.
- INCLUDE A INDEX.HTML IN ALL FOLDERS WITH DEFAULT MESSAGES.
- REMOVE ALL THE DEFAULT PASSWORDS AND ADD YOUR OWN NEW STRONG PASSWORDS WHICH MUST HAVE A SPECIAL CHARACTER AND A NUMBER AND MUST BE GREATER OR EQUAL TO 8 DIGITS FOR MAXIMUM SECURITY.

## 6.INFORMATION DISCLOSURE

INFORMATION DISCLOSURE (LOW)	<p>Below affected URL are vulnerable to reflected XSS.</p> <p><b>Affected URL:</b> <a href="http://35.154.158.143/Server-status">http://35.154.158.143/Server-status</a></p>

# OBSERVATION

GO TO [HTTP://35.154.158.143/SERVER-STATUS](http://35.154.158.143/SERVER-STATUS) AND INFORMATION WILL BE SHOWN LIKE BELOW.

← → ⌛ ⌂ 35.154.158.143/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	

.....  
.....

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,  
"T" Idle cleanup of worker, "O" Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-0	1709	0/1/1	_	0.92	17771	89	0.0	0.00	0.00	127.0.0.1	localhost:8000	GET / HTTP/1.1
0-0	1709	0/1/1	_	9.64	34	1	0.0	0.00	0.00	127.0.0.1	localhost:8000	GET /server-status HTTP/1.1
0-0	1709	0/1/1	_	9.58	170	0	0.0	0.00	0.00	127.0.0.1	localhost:8000	GET /favicon.ico HTTP/1.1

# BUSINESS IMPACT-MODERATE

ALTHOUGH THIS VULNERABILITY IS NOT HAVE A DIRECT IMPACT ON SERVER OR CLIENT BUT A MALICIOUS HACKER CAN KNOW THINGS LIKE MAPPING THE SERVER-ARCHITECTURE AND MAP HIS PLAN FURTHER ON WHAT AND HOW TO ACHIEVE.

## RECOMMENDATIONS:

**DISABLE** OFF ANY DIRECTORY LISTINGS AND ALSO SERVER-STATUS.

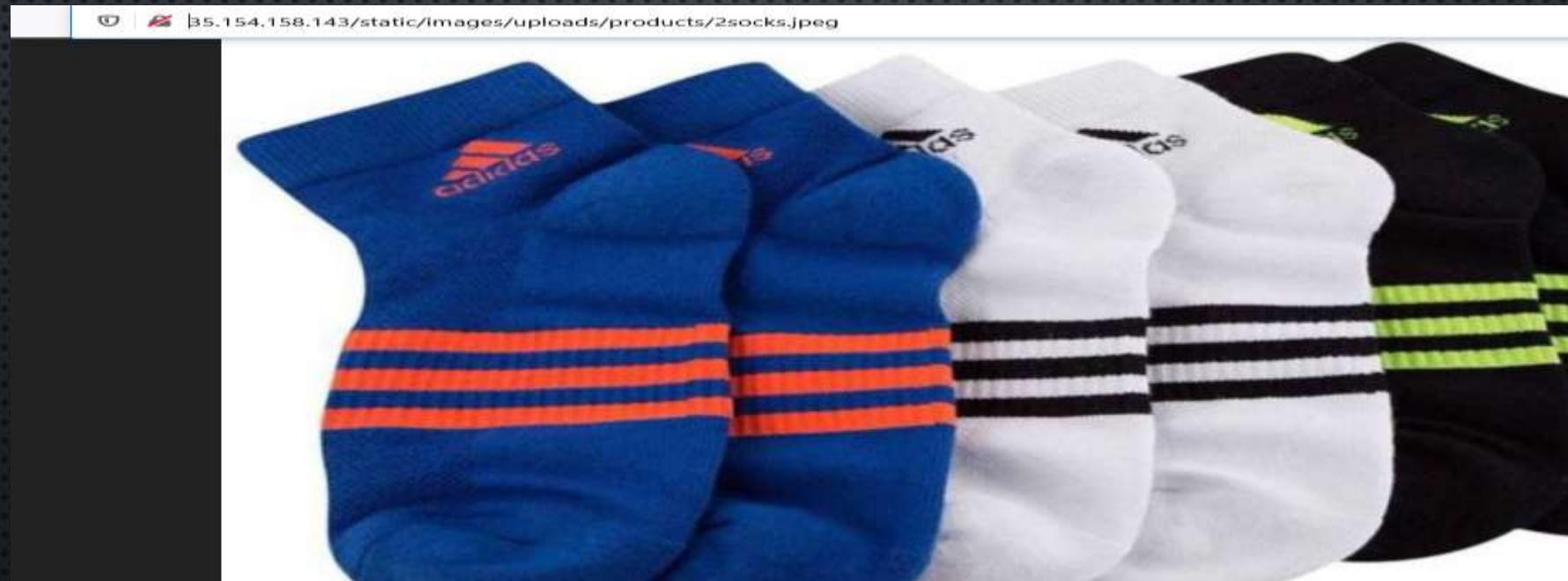
- REFERENCES:
- [HTTPS://VULDB.COM/?ID.88482](https://vuldb.com/?id.88482)
- [HTTPS://HTTPD.APACHE.ORG/DOCS/CURRENT/MOD/MOD\\_STATUS.HTML](https://httpd.apache.org/docs/current/mod/mod_status.html)

## 7.PII LEAKAGE

PII LEAKAGE (CRITICAL)	<p>Below mentioned URL LEAKS Critical information via PII leakage.</p> <p><b>Affected URL:</b> <a href="http://35.154.158.143/static/images/uploads/products/2socks.jpeg">http://35.154.158.143/static/images/uploads/products/2socks.jpeg</a></p> <p><b>Affected parameters:</b> IMAGE(every image after “products/”)</p>

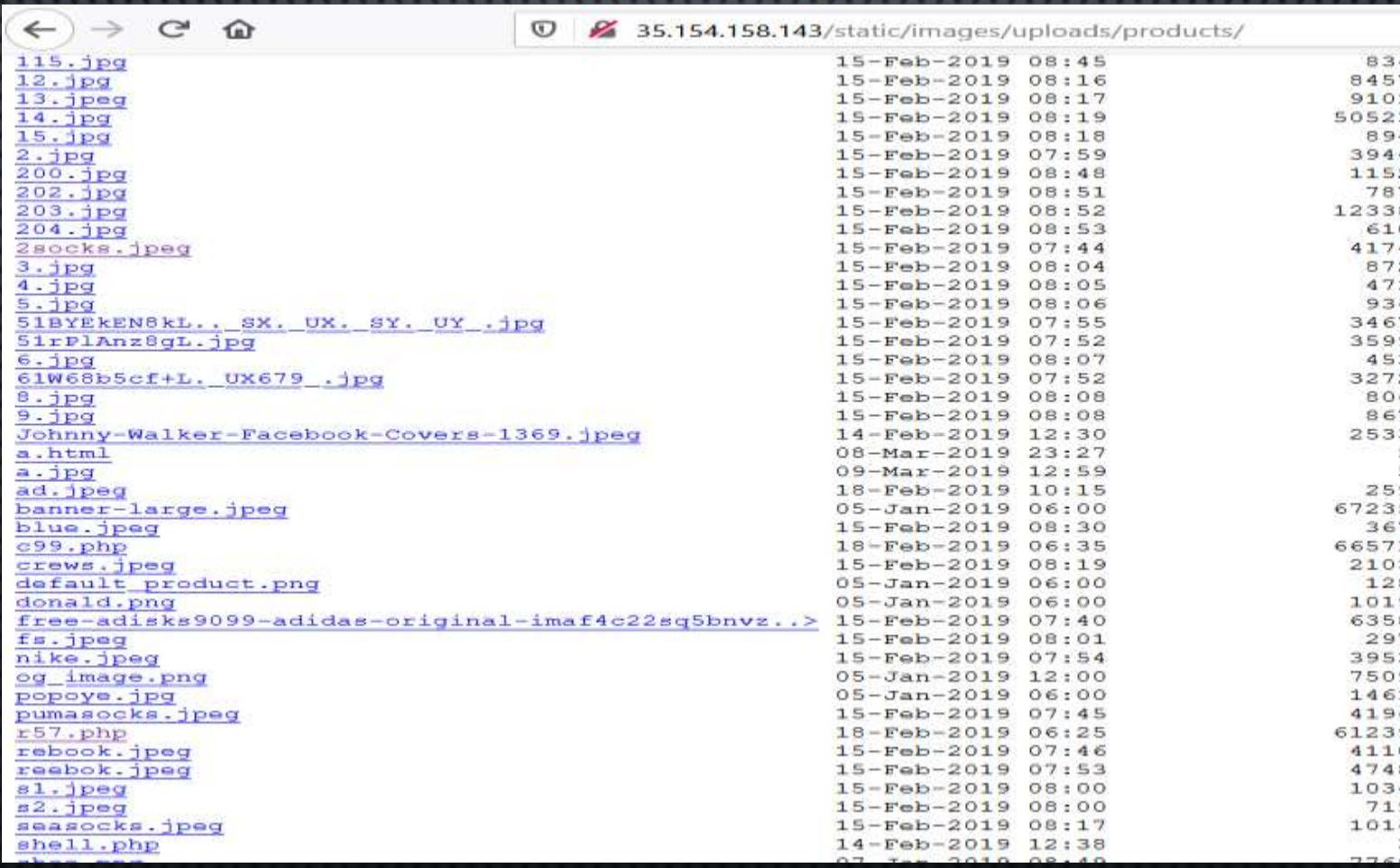
# OBSERVATION

- GO TO `HTTP://35.154.158.143/PRODUCTS.PHP` , NOW CLICK AND DRAG ANY PRODUCT IMAGE IN A NEW TAB, THE FOLLOWING PAGE WILL LOOK LIKE THE ONE SHOWN BELOW WITH THE IMAGE OF THE PRODUCT YOU CHOSE,



# OBSERVATION

- NOW, WE REMOVE THE IMAGE NAME, I.E."2SOCKS.JPG" IN OUR CASE AND HIT ENTER, THE FOLLOWING PAGE WITH DETAILS WILL BE SHOWN,



The screenshot shows a web browser window with the URL `35.154.158.143/static/images/uploads/products/`. The left side of the screen displays a list of file names, many of which are underlined and blue, suggesting they are links. The right side shows a table of file details.

File Name	Last Modified	Size
115.jpg	15-Feb-2019 08:45	834
12.jpg	15-Feb-2019 08:16	845
13.jpeg	15-Feb-2019 08:17	910
14.jpg	15-Feb-2019 08:19	5052
15.jpg	15-Feb-2019 08:18	894
2.jpg	15-Feb-2019 07:59	3946
200.jpg	15-Feb-2019 08:48	115
202.jpg	15-Feb-2019 08:51	78
203.jpg	15-Feb-2019 08:52	12336
204.jpg	15-Feb-2019 08:53	610
2socks.jpeg	15-Feb-2019 07:44	4174
3.jpg	15-Feb-2019 08:04	874
4.jpg	15-Feb-2019 08:05	471
5.jpg	15-Feb-2019 08:06	934
51BYEkEN8kl.._SX_.UX_.SY_.UY_.jpg	15-Feb-2019 07:55	3461
51rP1Anz8gI.jpg	15-Feb-2019 07:52	3590
6.jpg	15-Feb-2019 08:07	450
61W68b5cf+L_.UX679_.jpg	15-Feb-2019 07:52	327
8.jpg	15-Feb-2019 08:08	804
9.jpg	15-Feb-2019 08:08	864
Johnny-Walker-Facebook-Covers-1369.jpeg	14-Feb-2019 12:30	253
a.html	08-Mar-2019 23:27	8
a.jpg	09-Mar-2019 12:59	12
ad.jpeg	18-Feb-2019 10:15	259
banner-large.jpeg	05-Jan-2019 06:00	6723
blue.jpeg	15-Feb-2019 08:30	361
c99.php	18-Feb-2019 06:35	6657
crews.jpeg	15-Feb-2019 08:19	210
default_product.png	05-Jan-2019 06:00	12
donald.png	05-Jan-2019 06:00	1019
free-adisks9099-adidas-original-imaf4c22sq5bnvz..>	15-Feb-2019 07:40	6356
fs.jpeg	15-Feb-2019 08:01	297
nike.jpeg	15-Feb-2019 07:54	395
og_image.png	05-Jan-2019 12:00	7509
popoye.jpg	05-Jan-2019 06:00	1464
pumasocks.jpeg	15-Feb-2019 07:45	4196
r57.php	18-Feb-2019 06:25	6123
rebook.jpeg	15-Feb-2019 07:46	4110
reebok.jpeg	15-Feb-2019 07:53	4748
s1.jpeg	15-Feb-2019 08:00	1034
s2.jpeg	15-Feb-2019 08:00	719
seasocks.jpeg	15-Feb-2019 08:17	1014
shell.php	14-Feb-2019 12:38	776
shoes.jpg	07-Jan-2019 08:40	776

# BUSINESS IMPACT-HIGH

- A MALICIOUS HACKER CAN GAIN ACCESS TO THE SHELL APPLICATION AND VARIOUS OTHER HTML FILES WHICH HAS BEEN SHOWN IN THE LISTINGS AND ALSO IT HAS A WEAK-PASSWORD FLAW AS WELL.
- A HACKER CAN GET ACCESS TO SHELL AND UPLOAD HIS OWN MALICIOUS CODES TO MAKE THE SITE WHICH IS TRUSTED BY THE USER VULNERABLE AND HACKERS ROOM FOR PHISHING AND TRICKING USERS. WHICH WILL RESULT IN DEFAMATION OF THE WEBSITE.

# RECOMMENDATIONS

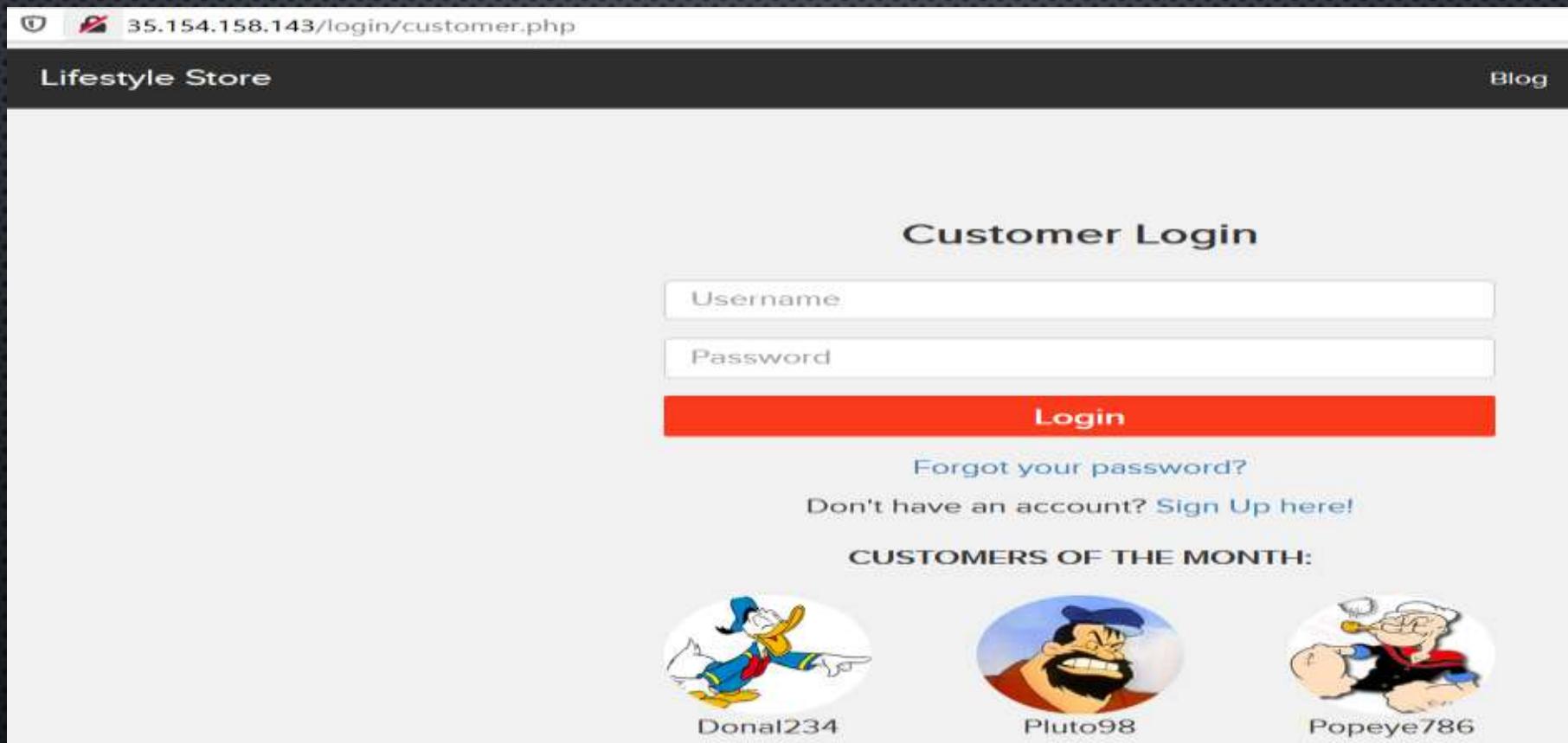
- 2- FACTOR AUTHENTICATIONS FOR SENSITIVE DATA SHOULD BE ADDED WITH STRONG PASSWORDS.
- FIND ALL PII STORED AND ENCRYPT THEM WITH VARIOUS TECHNIQUES AND ALSO DISABLE ALL THE LISTINGS.

## 8.SELF REDIRECTION/HTML/DEVELOPER FLAW

DEVELOPER FLAW/HTML FLAW (SEVERE)	<p>Below mentioned URL has a major development flaw , as it redirects to password reset link without authentication.</p> <p>Affected URL:<a href="http://35.154.158.143/reset_password/customer.php">http://35.154.158.143/reset_password/customer.php</a></p> <p>Affected Parameter: Password reset</p>

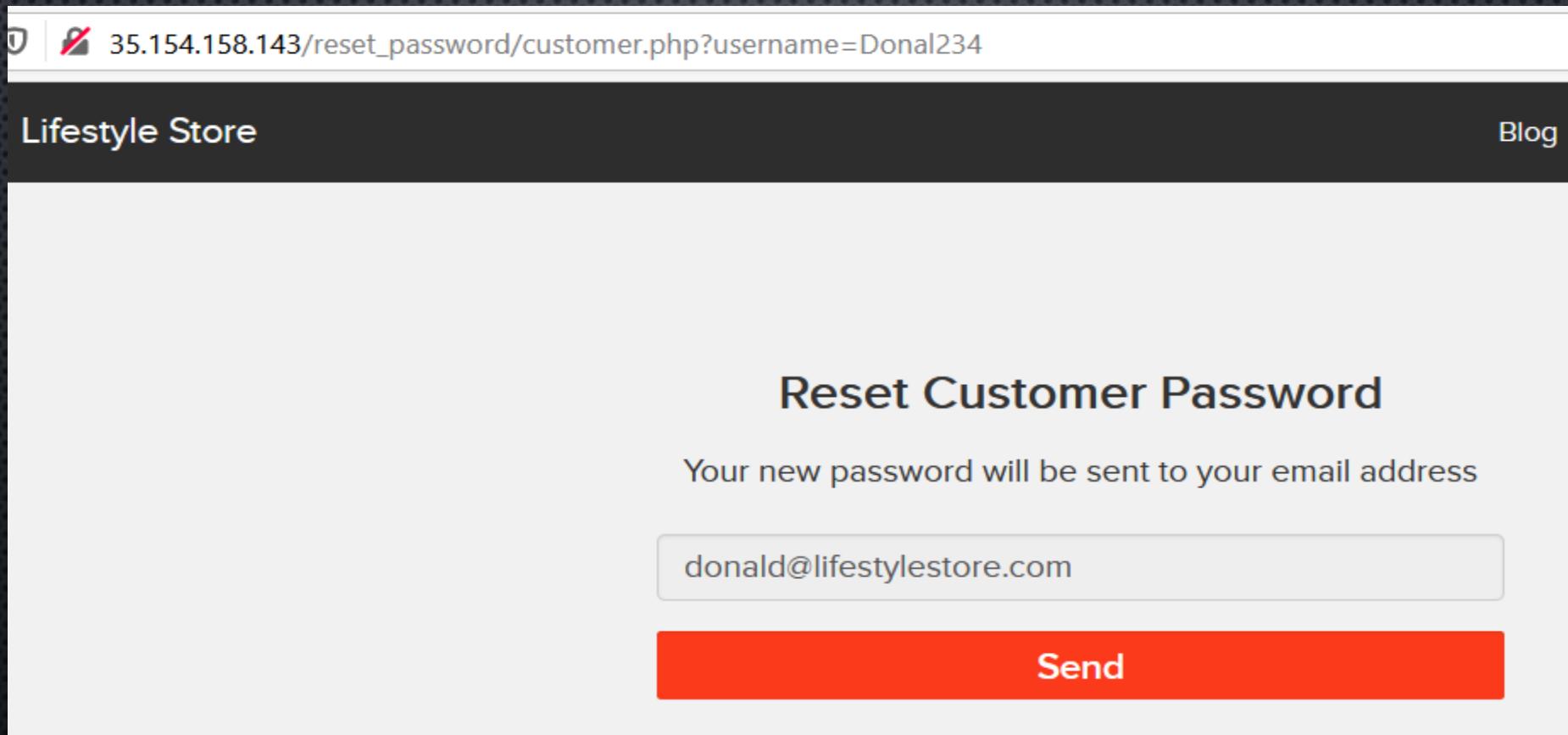
# OBSERVATION

- GO TO [HTTP://35.154.158.143/LOGIN/CUSTOMER.PHP](http://35.154.158.143/login/customer.php) AND YOU WILL SEE , NAMES OF TOP CUSTOMERS ,AS SHOWN BELOW, MEMORIZE ANY USERNAME.



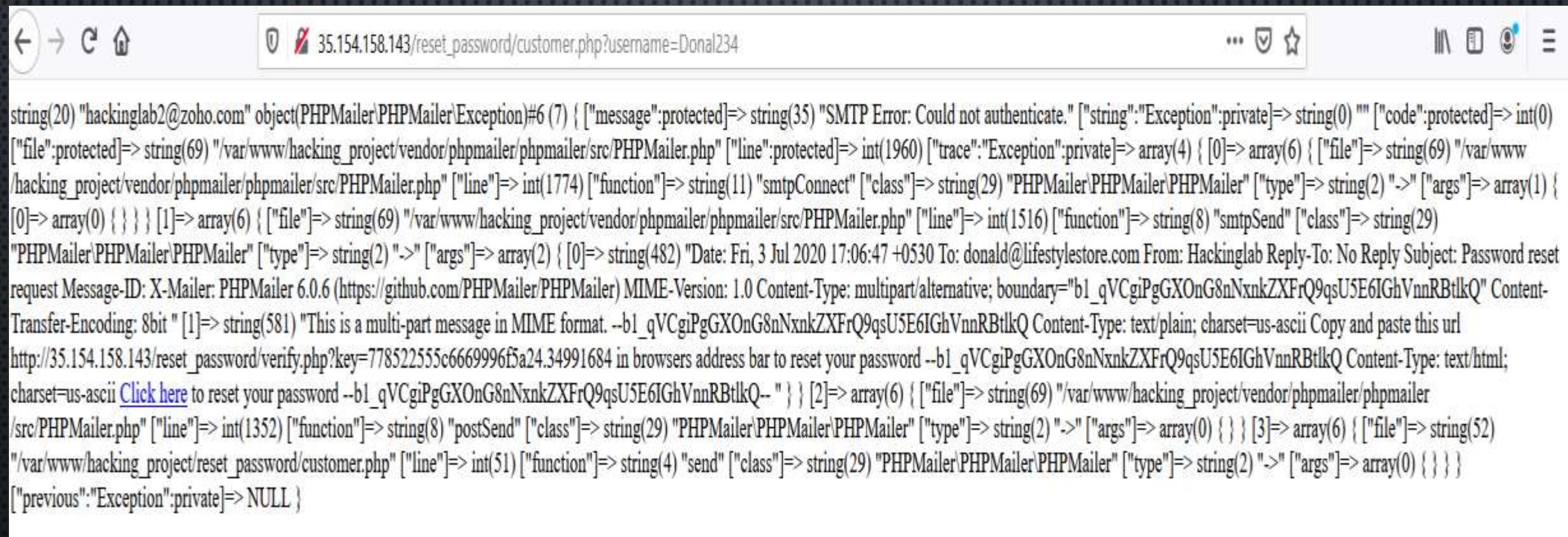
# OBSERVATION

- AFTER MEMORIZING ANY USERNAME , CLICK “FORGOT YOUR PASSWORD” AND THEN WRITE THE MEMORIZED USERNAME AND CLICK “RESET PASSWORD” AND THEN AND WE’LL SEE THE PAGE LIKE THIS, CLICK SEND,



# OBSERVATION

- CLICK SEND AND THEN YOU'LL SEE 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.



The screenshot shows a web browser window with the URL `35.154.158.143/reset_password/customer.php?username=Donald234`. The page content is a detailed PHPMailer exception message:

```
string(20) "hackinglab2@zoho.com" object(PHPMailer\PHPMailer\Exception){#6 (7) { ["message":protected]=> string(35) "SMTP Error: Could not authenticate." ["string":"Exception":private]=> string(0) "" ["code":protected]=> int(0) ["file":protected]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line":protected]=> int(1960) ["trace":"Exception":private]=> array(4) { [0]=> array(6) { ["file"]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line"]=> int(1774) ["function"]=> string(11) "smtpConnect" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(1) { [0]=> array(0) { } } } [1]=> array(6) { ["file"]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line"]=> int(1516) ["function"]=> string(8) "smtpSend" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(2) { [0]=> string(482) "Date: Fri, 3 Jul 2020 17:06:47 +0530 To: donald@lifestylestore.com From: Hackinglab Reply-To: No Reply Subject: Password reset request Message-ID: X-Mailer: PHPMailer 6.0.6 (https://github.com/PHPMailer/PHPMailer) MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="b1_qVCgiPgGXOnG8nNxnkZXFrQ9qsU5E6IGhVnnRBtlkQ" Content-Transfer-Encoding: 8bit" [1]=> string(581) "This is a multi-part message in MIME format. --b1_qVCgiPgGXOnG8nNxnkZXFrQ9qsU5E6IGhVnnRBtlkQ Content-Type: text/plain; charset=us-ascii Copy and paste this url http://35.154.158.143/reset_password/verify.php?key=778522555c6669996f5a24.34991684 in browsers address bar to reset your password --b1_qVCgiPgGXOnG8nNxnkZXFrQ9qsU5E6IGhVnnRBtlkQ Content-Type: text/html; charset=us-ascii Click here to reset your password --b1_qVCgiPgGXOnG8nNxnkZXFrQ9qsU5E6IGhVnnRBtlkQ--" } } [2]=> array(6) { ["file"]=> string(69) "/var/www/hacking_project/vendor/phpmailer/phpmailer/src/PHPMailer.php" ["line"]=> int(1352) ["function"]=> string(8) "postSend" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(0) { } } [3]=> array(6) { ["file"]=> string(52) "/var/www/hacking_project/reset_password/customer.php" ["line"]=> int(51) ["function"]=> string(4) "send" ["class"]=> string(29) "PHPMailer\PHPMailer\PHPMailer" ["type"]=> string(2) "->" ["args"]=> array(0) { } } ["previous":"Exception":private]=> NULL }
```

# OBSERVATION

- YOU'LL BE REDIRECTED TO CHANGE PASSWORD OF THE CUSTOMER ID ,AND ALSO 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.(THE PAGE COMES UP LOOKS LIKE THIS)

The screenshot shows a web browser window with the following details:

- Address Bar:** Displays a shield icon, a refresh icon, and the URL `35.154.158.143/profile/change_password.php`.
- Header:** A dark navigation bar with the text "Lifestyle Store" on the left and "My Cart", "My Profile", and "My Ord" on the right.
- Content Area:** A white page titled "Change Password". It contains two input fields: "New Password" and "Confirm Password", both currently empty. Below these fields is a large orange button labeled "UPDATE".

## BUSINESS IMPACT-HIGH

- BUSINESS IMPACT IS HIGH AS A MALICIOUS HACKER CAN GET ACCESS TO EVERY USER IN THE WEBSITE AND CAN LOGIN AND DO AND PERFORM TASK FOR HIS BENEFITS AS CAN ALSO MAKE THE SITE VULNERABLE FOR SECURITY OF CUSTOMERS. AND WILL RESULT IN THE DEFAMATION OF THE WEBSITE AS THE USERS TRUST IT.

# RECOMMENDATION

- BETTER AUTHENTICATION SHOULD BE PROVIDED AND RE-DIRECTION SITE MUST BE RE-CHECKED BEFORE IN ACTION.
- PROPER AUTHORISATION ACCESS SHOULD BE THERE.

## 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))*

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

Multiple vulnerabilities in blog site  
(PII LEAKAGE,  
TEMPORARY XSS AND  
MORE)  
{CRITICAL}

Below are the affected parameters and URL of Blog Site.

Affected url:<http://15.206.75.142/wondercms/>

Affected URL:<http://15.206.75.142/wondercms/files/b374kmini.php>

Affected parameters: file upload(post)

AFFECTED URL: <http://15.206.75.142/wondercms/home>

AFFECTED PARAMETERS: FILES(GET)

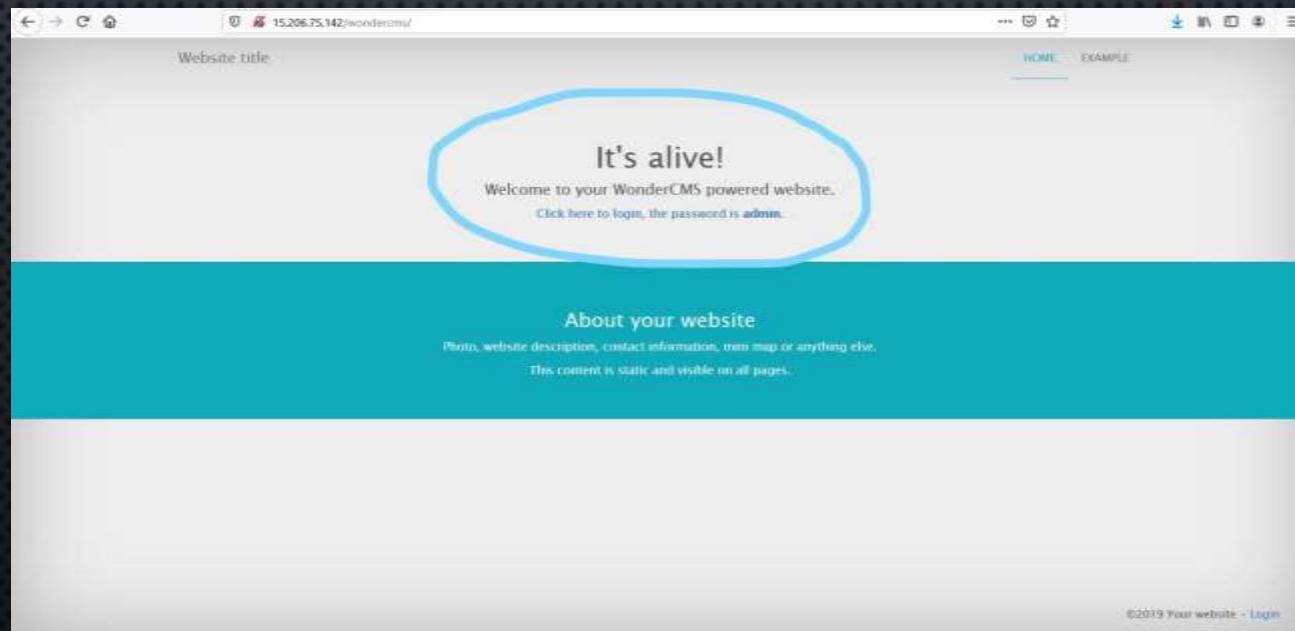
AFFECTED URL: <http://13.235.0.176/wondercms/files/minisell.php>

AFFECTED PARAMETER: SHELL UPLOAD

# OBSERVATION

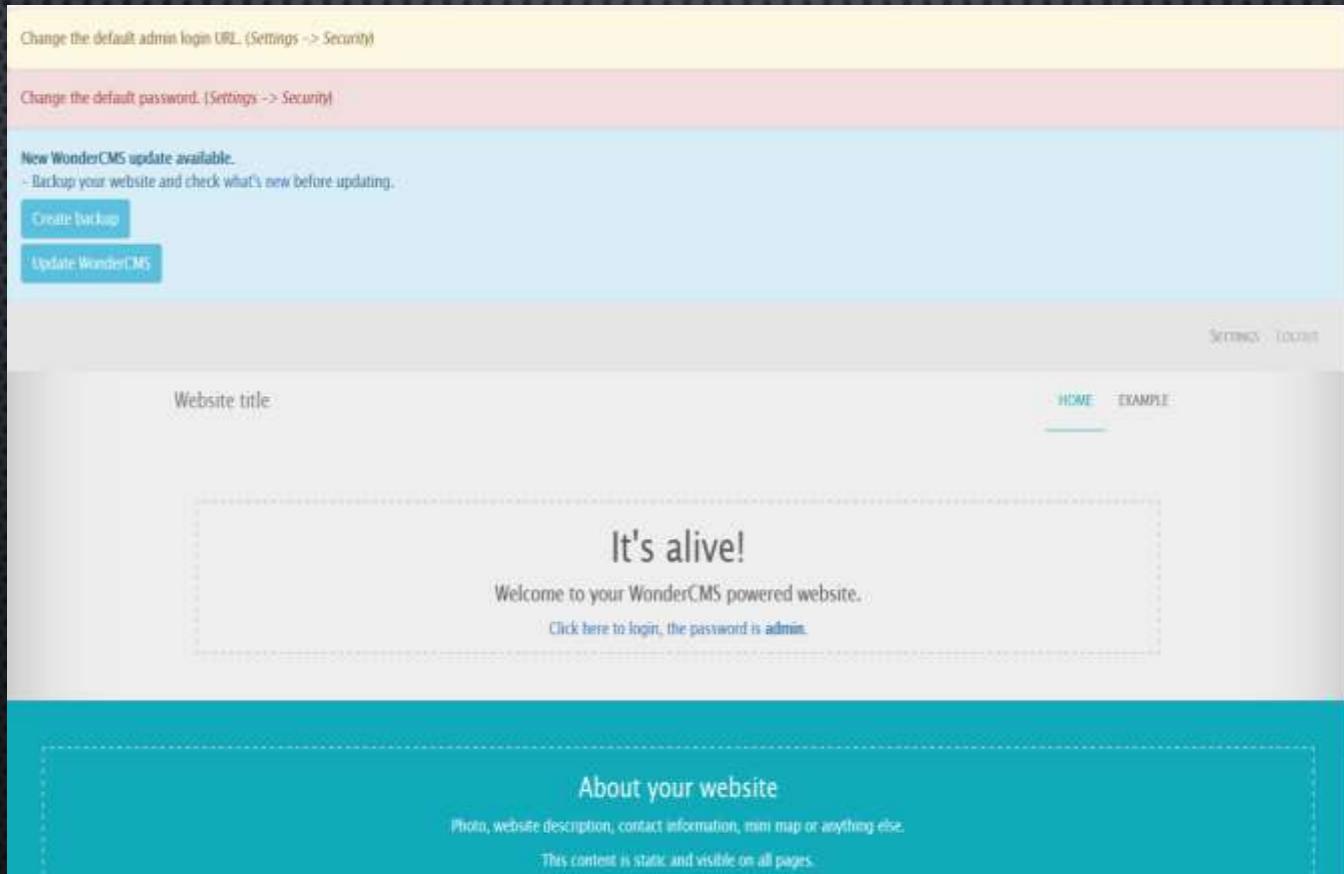
AT THE FRONT PAGE OF THE BLOG SITE WE CAN DIRECTLY FIND THE LOGIN OPTION , THAT SAYS “CLICK HERE TO LOGIN, THE PASSWORD IS ADMIN” BY CLICKING ON IT , IT WILL REDIRECTS TO THE LOGIN PAGE WHERE JUST BY ENTERING ‘ADMIN’ AS PASSWORD ONE CAN GET ACCESS TO THE ADMIN ACCOUNT OF THIS SITE. THIS IS A PROPER EXAMPLES OF SERVER SIDE MISCONFIGURATION.

THE LOGGED IN PAGE LOOKS LIKE BELOW,



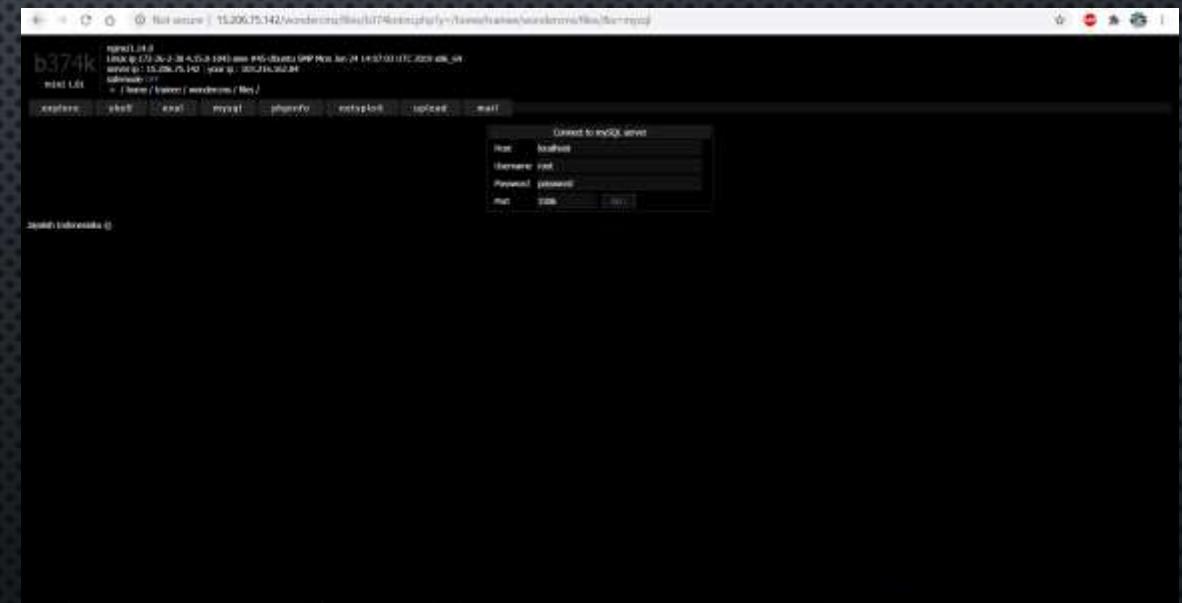
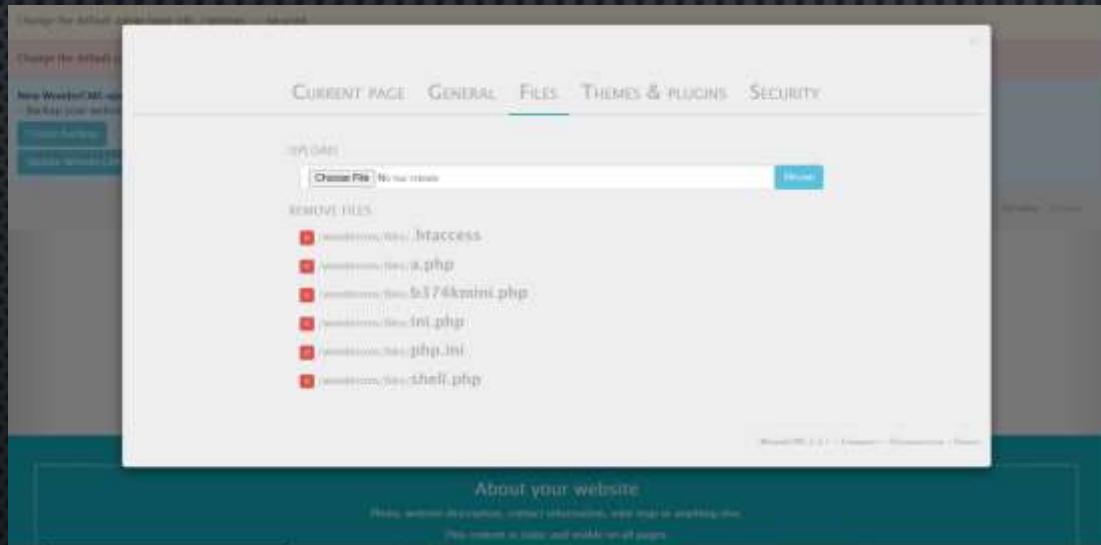
# OBSERVATION

- 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 AND ONE MALICIOUS HACKER CAN EASILY MAKE CHANGES AND CAN USE THE PAGE AS HIS/HER PHISHING PORTAL . THIS IS A CLASSIC EXAMPLE OF TEMPORARY XSS.



# OBSERVATION

- AS WE ARE INSIDE THE ADMIN ACCOUNT IF WE SELECT THE SETTINGS OPTION AND GO TO ‘FILES’ MENU WE CAN SEE SOME FILES WITH EXTENTION ‘.PHP’ WHICH CAN GIVE INFORMATION ABOUT THE SITE AND ALSO VERY MUCH CAPABLE OF TAKING OVER THE SITE. HERE, IF WE SELECT THE ‘[/WONDERCMS/FILES/B374KMINI.PHP](#)’ OPTION IT WILL REDIRECT US TO A PAGE WHICH WILL GIVE US MANY CRUCIAL INFORMATION LIKE SERVER IP ADDRESS, LINUX IP ADDRESS , THE SERVER TYPE , THE DATABASE , SHELL , THE PHP INFO , UPLOADS ALSO ONE CAN MAIL SOMEONE WITH THE ADMINS ACCOUNT WHICH CAN BE TERMED AS PHISHING (SOCIAL ENGINEERING) .



# OBSERVATION

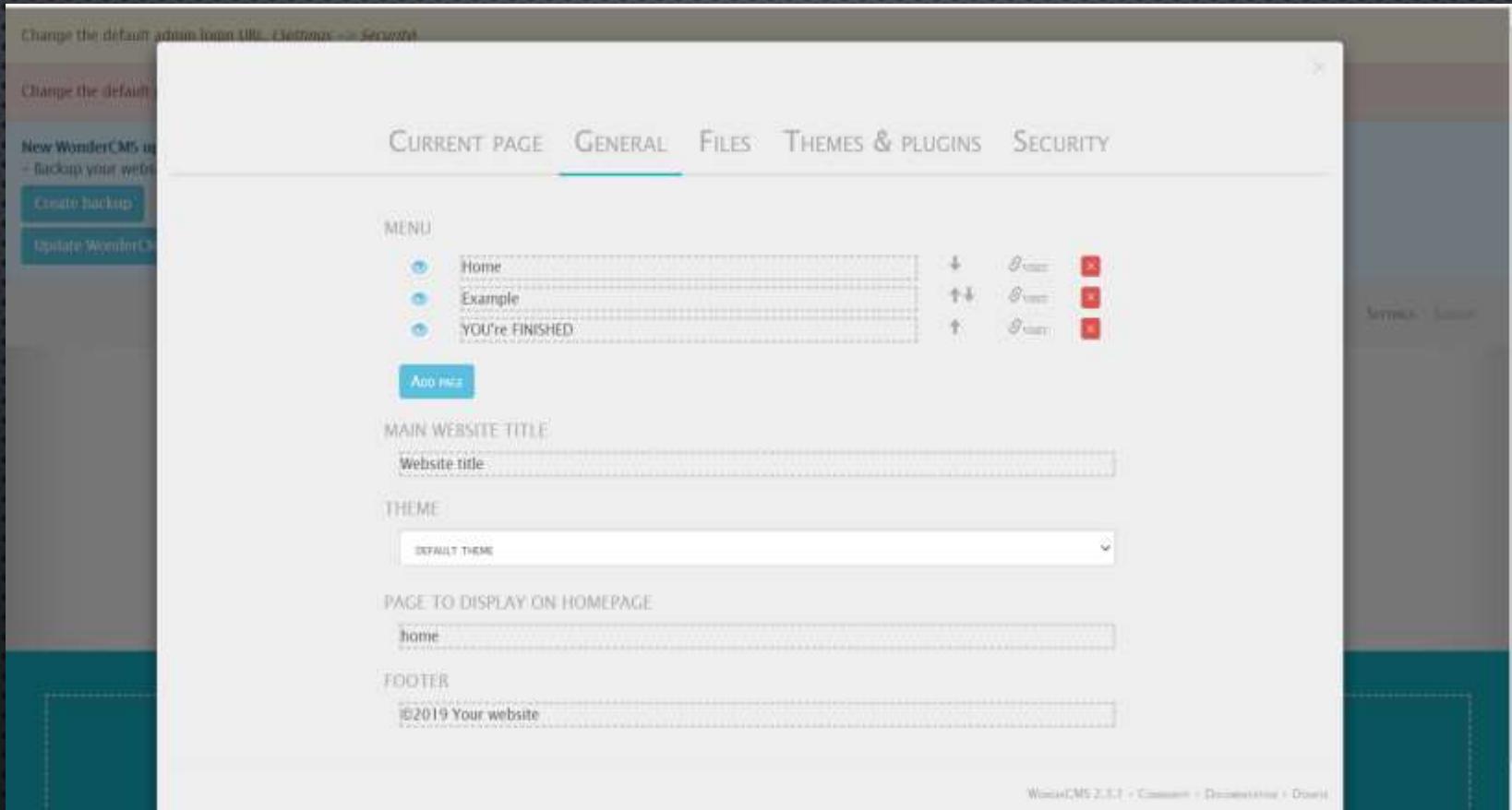
The screenshot shows a web browser window with the URL `Not secure | 15.206.75.142/wondercms/files/b374kmini.php?y=/home/trainee/wondercms/files/8or=phpinfo`. The page displays detailed information about the PHP environment, including the PHP version (5.6.39-1+ubuntu18.04.1+deb.sury.org+1), the operating system (Ubuntu 18.04.1 LTS), and various configuration settings. A prominent red banner at the top of the page reads "b374k mini 1.01". Below the banner, there is a navigation bar with links: explore, shell, eval, mysql, phpinfo, netsploit, upload, mail. A large "php" logo is centered above the main content area.

PHP Version 5.6.39-1+ubuntu18.04.1+deb.sury.org+1	
System	Linux ip-172-26-2-38 4.15.0-1043-aws #45-Ubuntu SMP Mon Jun 24 14:07:03 UTC 2019 x86_64
Server API	PPM/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-calculator.ini, /etc/php/5.6/fpm/conf.d/20-crypt.ini, /etc/php/5.6/fpm/conf.d/20-dom.ini, /etc/php/5.6/fpm/conf.d/20-ext.ini, /etc/php/5.6/fpm/conf.d/20-finfo.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-javascript.ini, /etc/php/5.6/fpm/conf.d/20-mbstring.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-system.ini, /etc/php/5.6/fpm/conf.d/20-tokenizer.ini, /etc/php/5.6/fpm/conf.d/20-wddc.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/70-xslini
PHP API	20131106
PHP Extension	20131229
Zend Extension	220131226
Zend Extension Build	API20131226NTS

- THE PAGE LOOKS LIKE ABOVE, FROM WHICH A ATTACKER CAN KNOW ALL INSIDE DETAILS LIKE VERSIONS, AND MORE.,

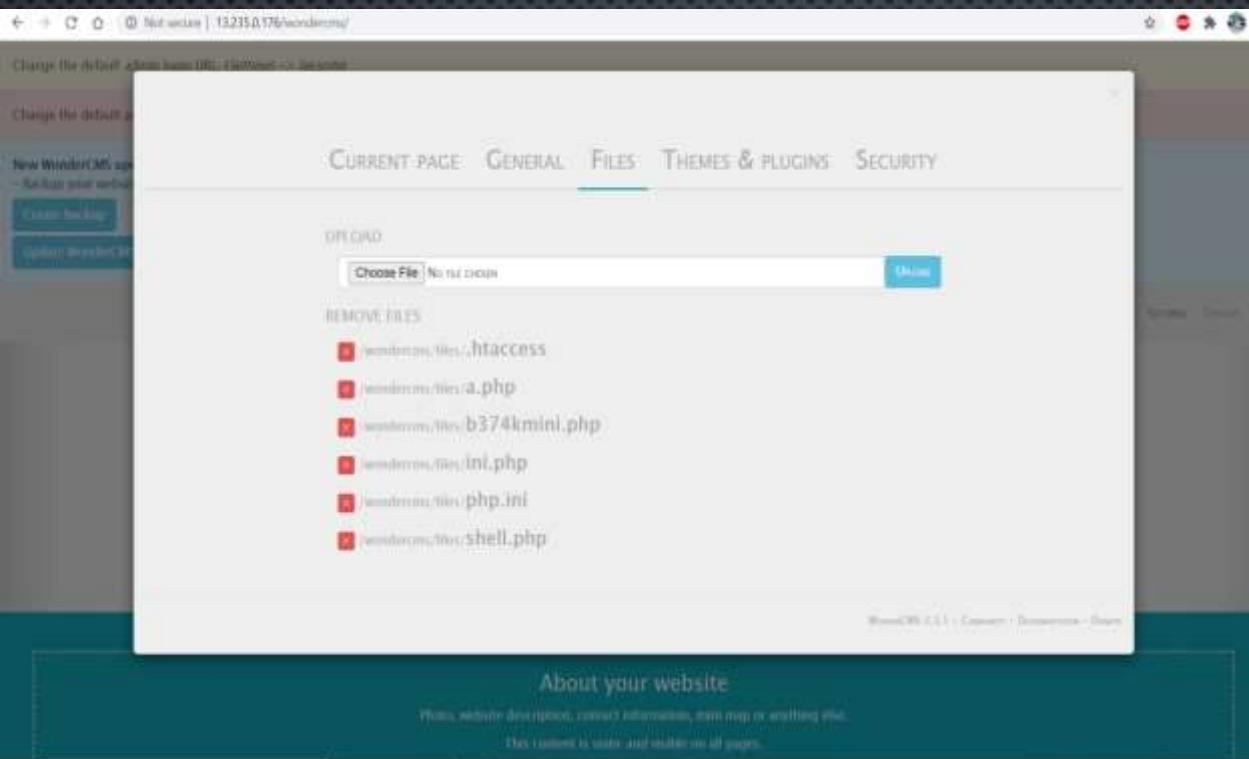
# OBSERVATION

- WHEN WE ARE IN THE ADMIN ACCOUNT AND IF WE GO TO THE SETTINGS->GENERAL OPTIONS , WE CAN SEE THAT A MALICIOUS HACKER CAN INJECTS AND EXECUTE MALICIOUS CLIENT SIDE SCRIPTS THROUGH IT WHICH GETS PERMANENTLY STORED IN THE DATABASE.



# OBSERVATION

- WHEN WE ARE INTO THE ADMINS ACCOUNT AND WE GO TO SETTINGS->FILES OPTION WE CAN FIND THAT FILES CAN BE UPLOADED THEIR WITH ANY FILE TYPE EXTENTION ONE WANTS , NOW IF WE CLICK ON CHOOSE FILE OPTION AND UPLOAD THE MINISHELL INTO THE SITE , IT WILL GIVE ACCESS TO TAKE OVER THE WHOLE WEBSITE.AND WILL BE A GREAT BREAKAGE ON THE SITE.



# BUSINESS IMPACT-EXTREMELY HIGH

AS THE BLOG SITE HAS MULTIPLE VULNERABILITIES AND LIMITATIONS AS THIS HAS TEMPORARY XSS , SERVER SIDE ERRORS AND DEVELOPMENT FLAWS THE SITE IS EXTREMELY VULNERABLE AS A MALICIOUS HACKER CAN INDULGE IN THE SITE AND CAN USE ALL THE VULNERABLE COMPONENTS TO DO PHISHING AND OTHER ATTACKS ON USER AND PERFORM MALICIOUS ACTIVITIES. THIS WILL RESULT IN DEFAMATION OF THE NAME OF THE COMPANY , MONEY LOSS AND CUSTOMERS NOT TRUSTING THE WEBSITE AGAIN.

# RECOMMENDATIONS

- TRY TO IMPLEMENT THE FOLLOWING:
  - 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 TECHNIQUES AT CHECKS OF THE WEBSITE

## REFERENCES:

- *[HTTPS://CWE.MITRE.ORG/DATA/DEFINITIONS/548.HTML](https://cwe.mitre.org/data/definitions/548.html)*
- *[HTTPS://WWW.W3SCHOOLS.COM](https://www.w3schools.com)*

# THANK YOU

CONTACT TO →BHAMARE2001@GMAIL.COM

FOR FURTHER DETAILS AND PATCH ASSISTANCE