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

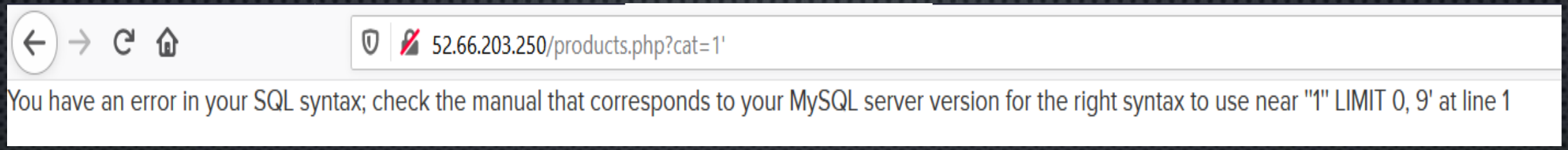
SQL INJECTION (CRITICAL)	Here are other similar SQLi in the web application **AFFECTED URL**: • http://52.66.203.250/products.php?cat=2' • http://52.66.203.250/products.php?cat=3'

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.

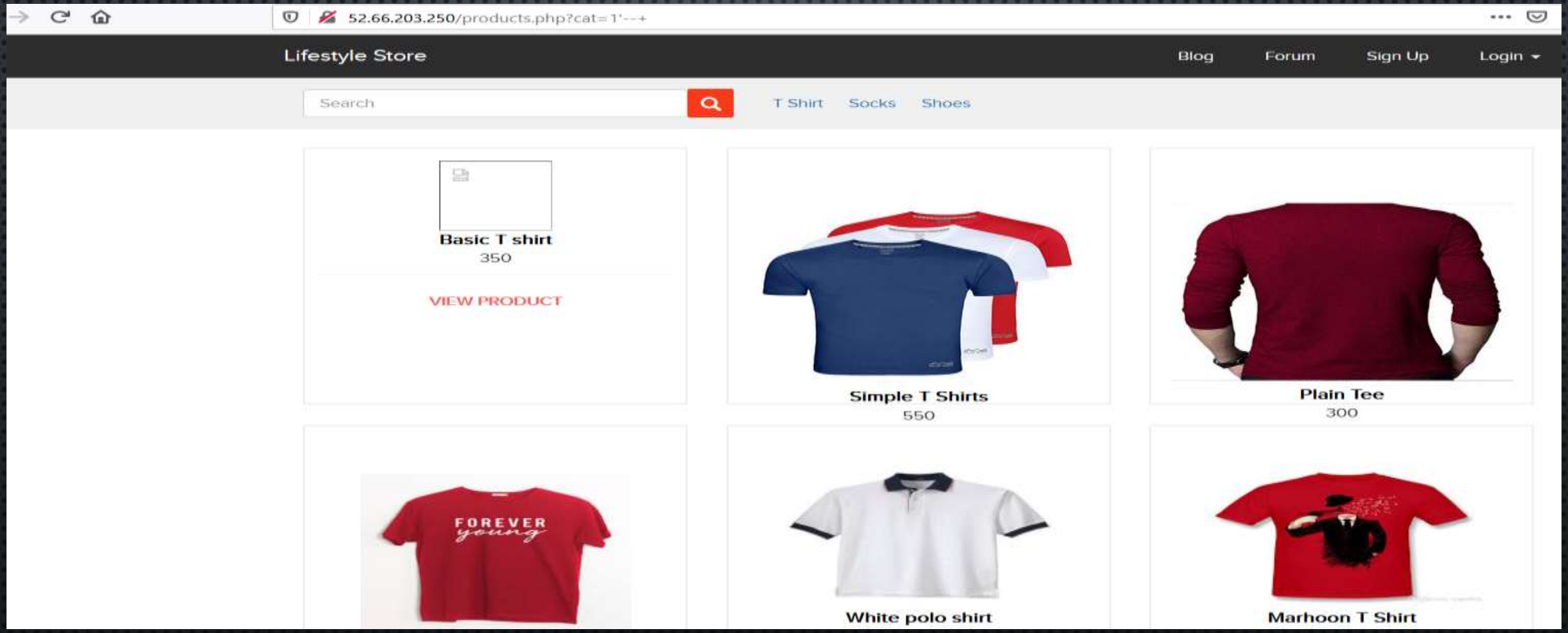
OBSERVATION

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



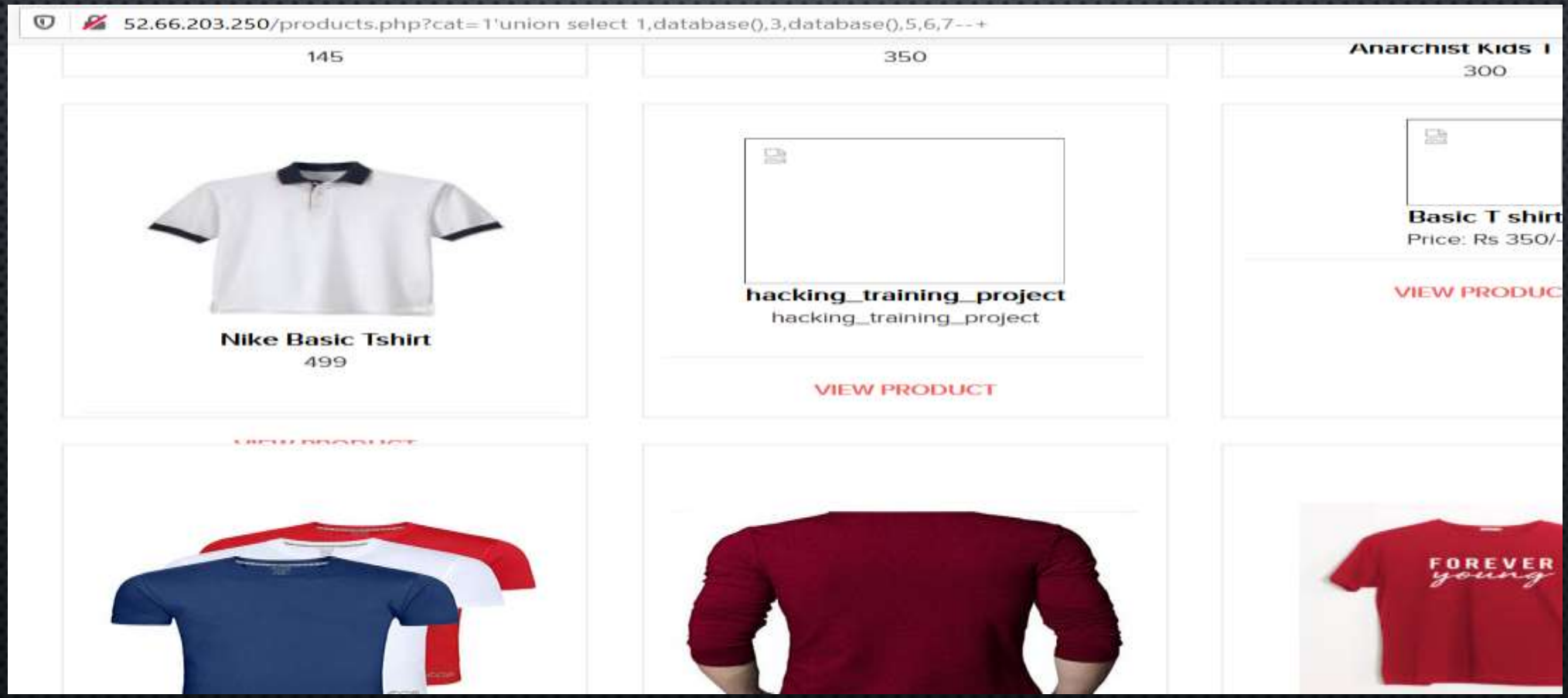
OBSERVATION

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



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.

```
atabase: hacking_training_project
able: users
15 entries]
+--------------------------+--------------------------------------------------------------+
| name                     | password                                                     |
+--------------------------+--------------------------------------------------------------+
| admin                    | $2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki |
| Donald Duck              | $2y$10$PM.7nBSP5FMa1dXiM/S3s./p5xR6GTKvjry7ysJtxOkBqOJURAHsO |
| Brutus                   | $2y$10$xkmdvrxSCxqdyWSrDx5YSe1NAwX.7pQ2nQmaTCovH4CFssxgyJTki |
| Chandan                  | $2y$10$4cZBEIrgthXdvT1hwUlivuFELe03rR.GIcdpO3NjrlS0VeiOKLVDa |
| Popeye the sailor man    | $2y$10$FkvlRfwYTioWOw2CaZtAQuXVnhGAUjt/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$10$pB3U9iFxwBgSb12AkBpiEeIBdhiYfwy9y.xV23q12gGbMCyn7N3g2 |
| asd                      | $2y$10$At5pFZnRWpjCD/yNnJWDL.L3Cc4Cv0W8Q/wEHmWzBFqVIkBQFpcF2 |
| acdc                     | $2y$10$J50B78.gpucuLTwpHwbcPedYcain.Yi.tsTLyQtK17FzdSpmIRRbi |
+--------------------------+--------------------------------------------------------------+
```

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

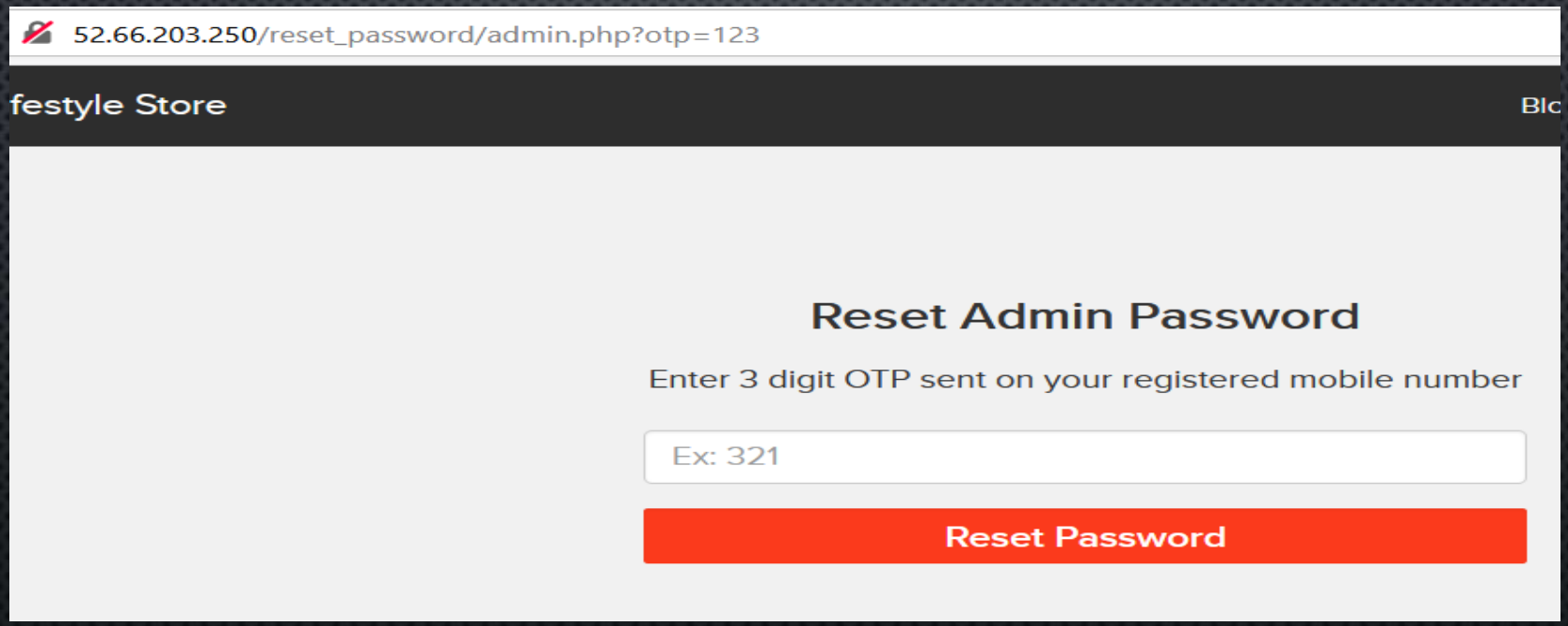
- https://www.owasp.org/index.php/SQL_Injection
- https://en.wikipedia.org/wiki/SQL_injection

2.ACCOUNT 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.



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) Gec
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag
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.

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

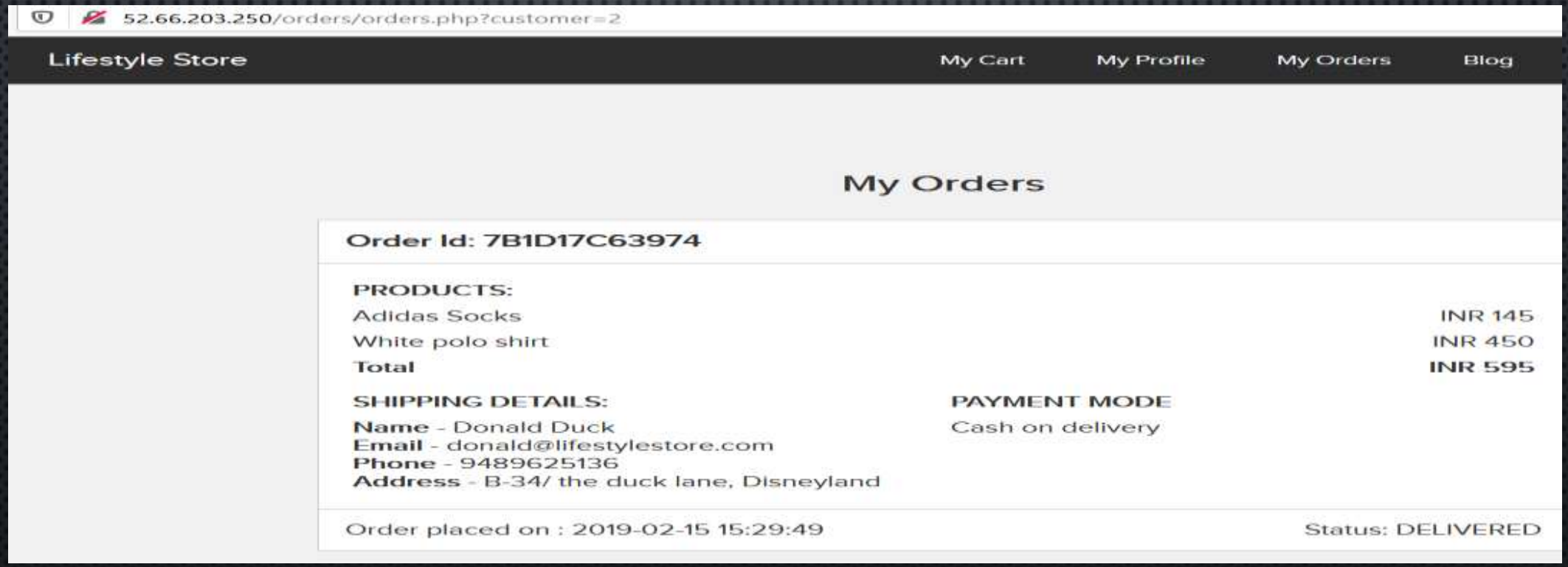
Unauthorized Access to Customer Details (critical)	The My Orders section of the website suffers from an Insecure direct Object Reference(IDOR), THAT Allows Hackers to get access to any other customers order details and more. **AFFECTED URL:** http://52.66.203.250/orders/orders.php?customer=2 **AFFECTED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

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 **AFFECTED PARAMETERS**:P_ID (GET)

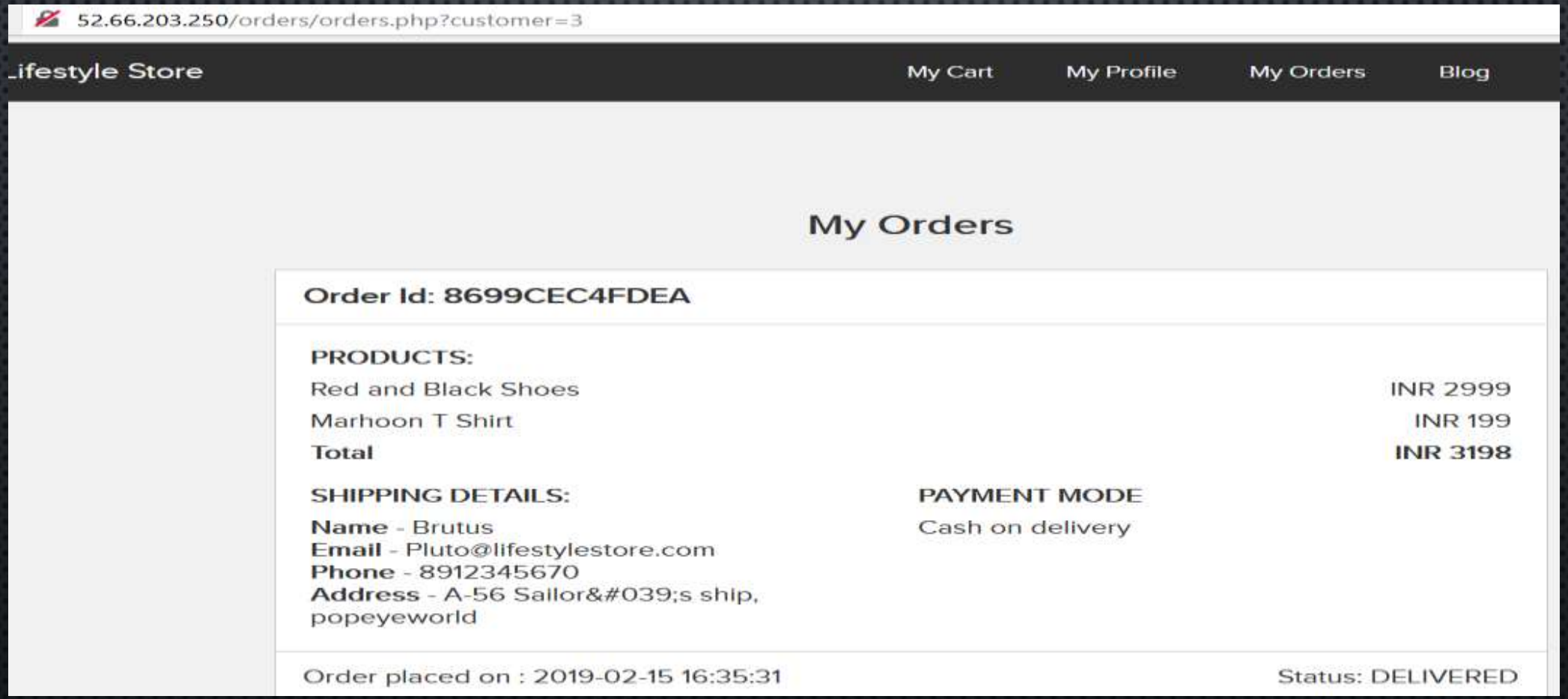
OBSERVATION

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



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.



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/blackmarket.
- 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)

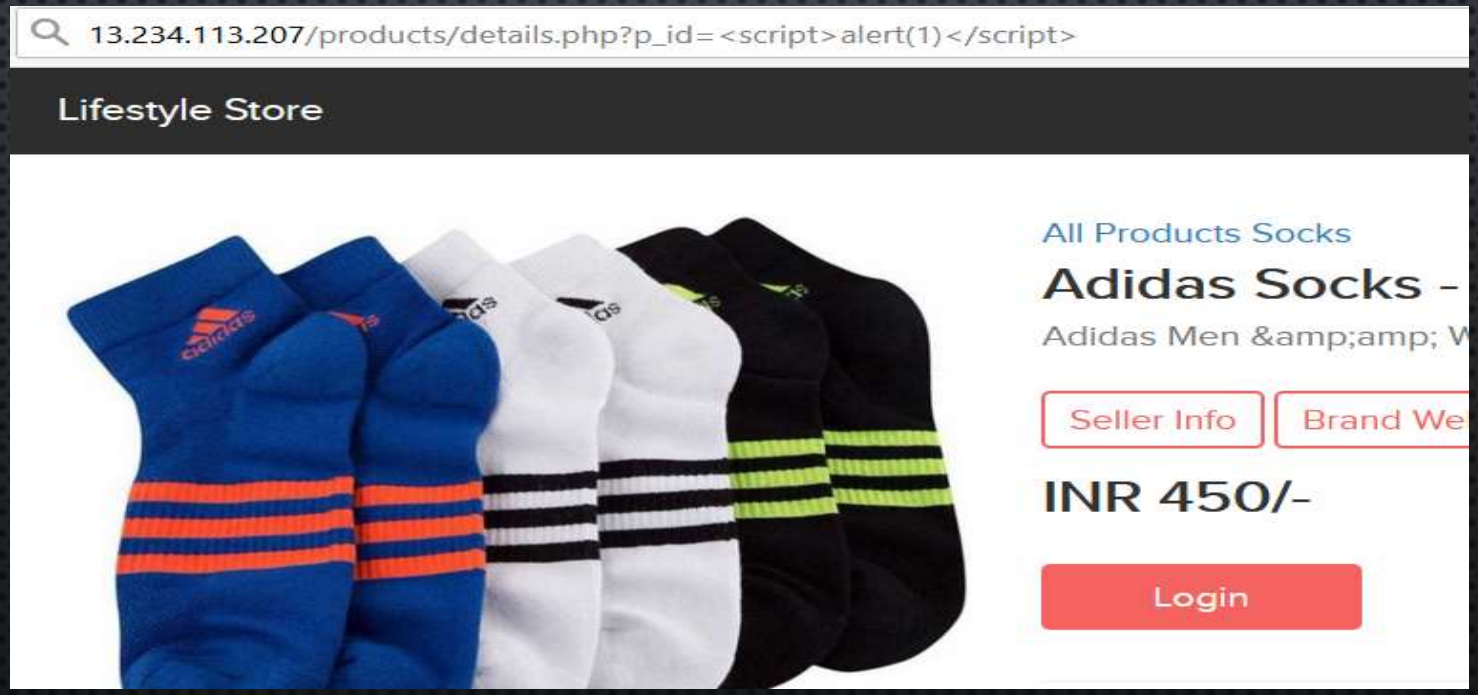
REFLECTED CROSS-SITE-SCRIPTING(XSS) (SEVERE)	Below mentioned parameters are affected to XSS. **Affected URL**:13.234.113.207/products/details.php?p_id=2 **AFFECTED PARAMETER**: URL(any thing after p_id) **PAYLOAD**: • <script>alert(1)</script>

4.REFLECTED CROSS-SITE-SCRIPTING(XSS)

REFLECTED CROSS-SITE-SCRIPTING(XSS) (SEVERE)	Below mentioned parameters are also affected to XSS. **AFFECTED URL:**13.234.113.207/products/details.php?p_id=2 **Affected Parameter**:comment(review box) **PAYLOAD**: • In review comment box <script>alert(1)</script>

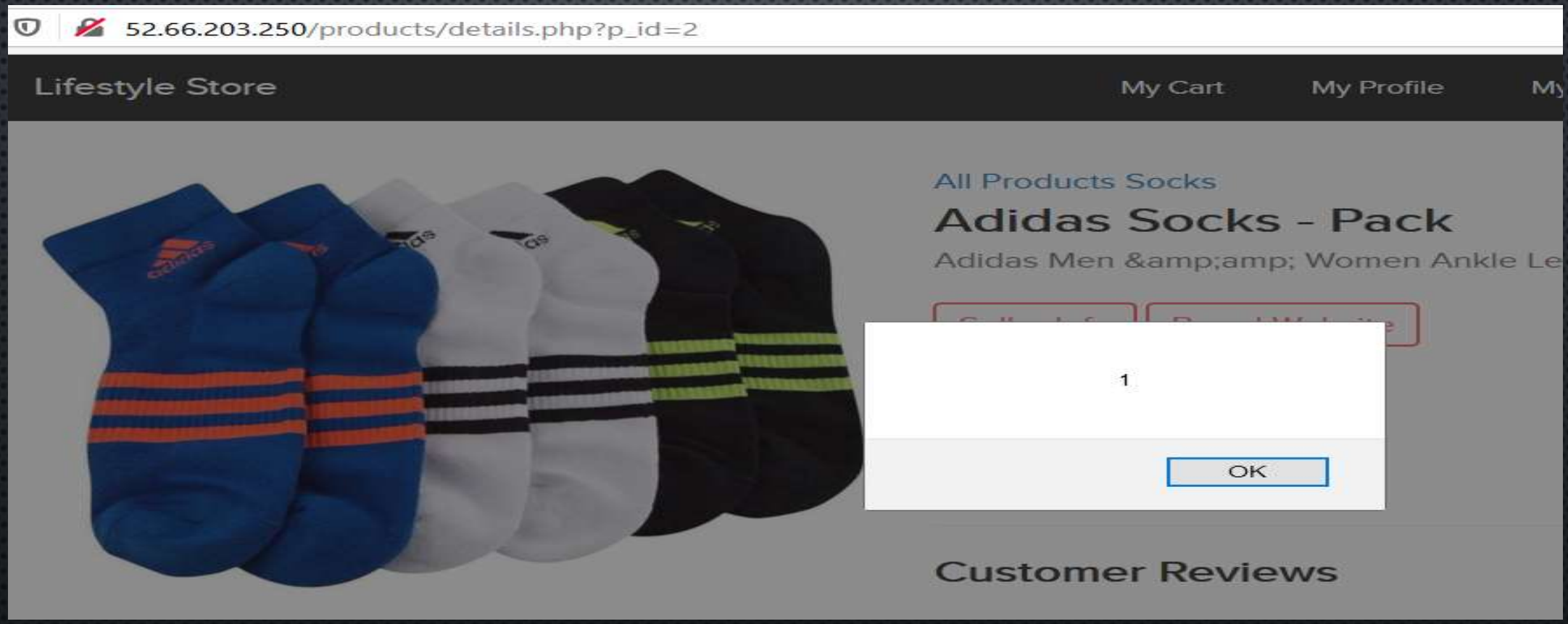
OBSERVATION

- 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.



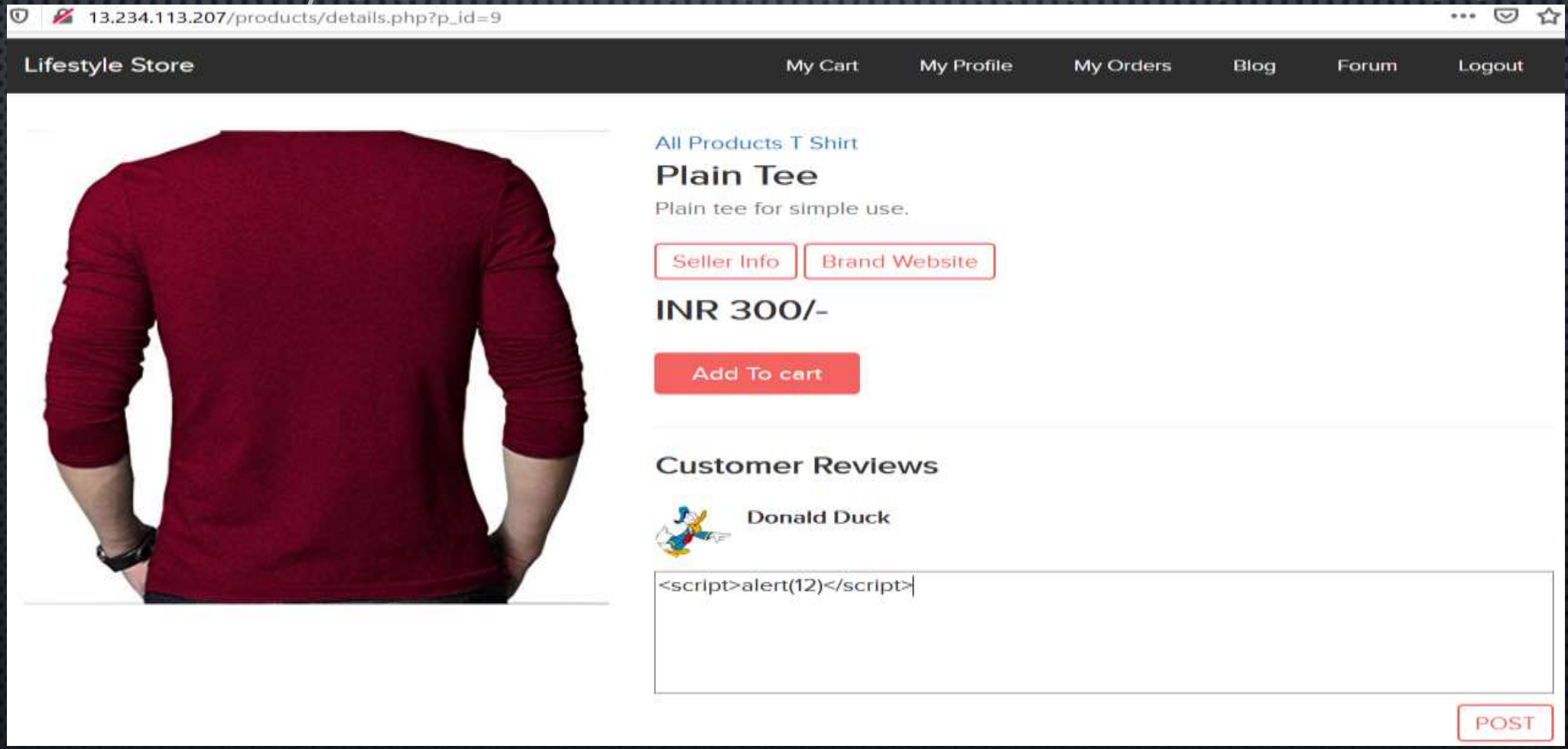
OBSERVATION

- 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.

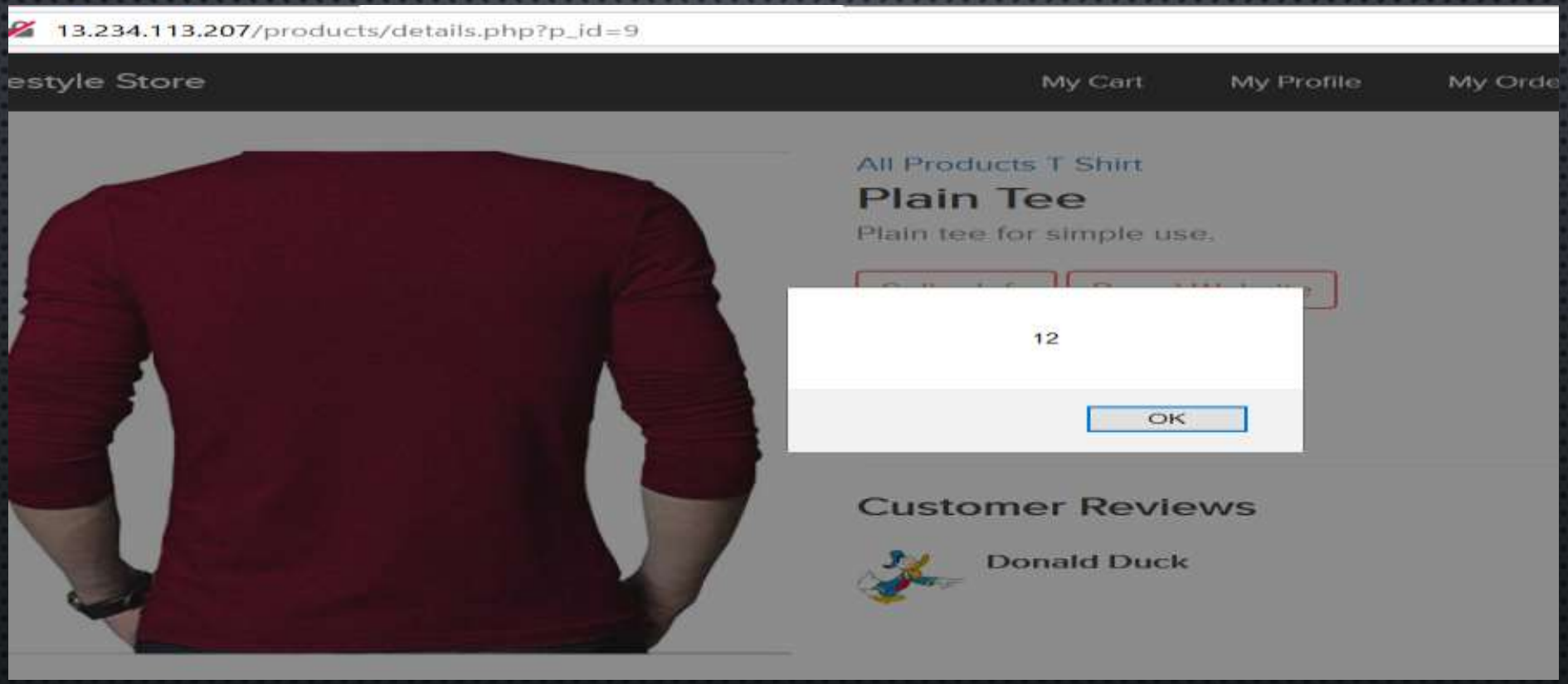


POC

IN REVIEW/COMMENT SECTION XSS IS PRESENT ALSO.



POC


13.234.113.207/products/details.php?p_id=9
estyle Store
My Cart
My Profile
My Orde
All Products T Shirt
Plain Tee
Plain tee for simple use.
12
OK
Customer Reviews
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

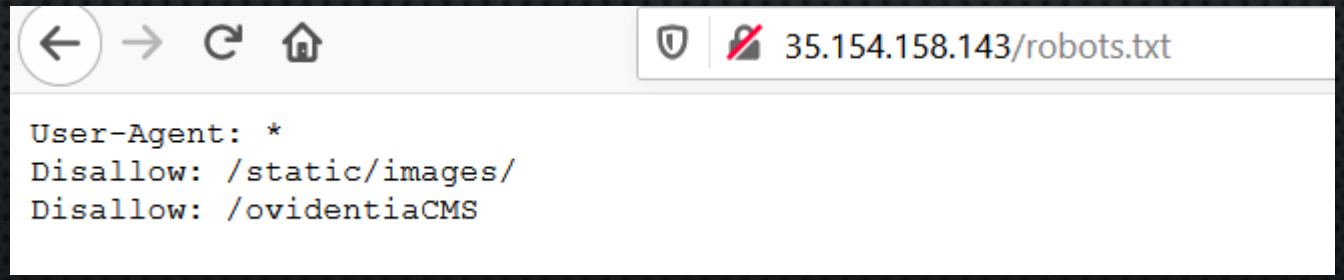
- *https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)*
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.w3schools.com/html/html_entities.asp

5.DIRECTORY LISTINGS

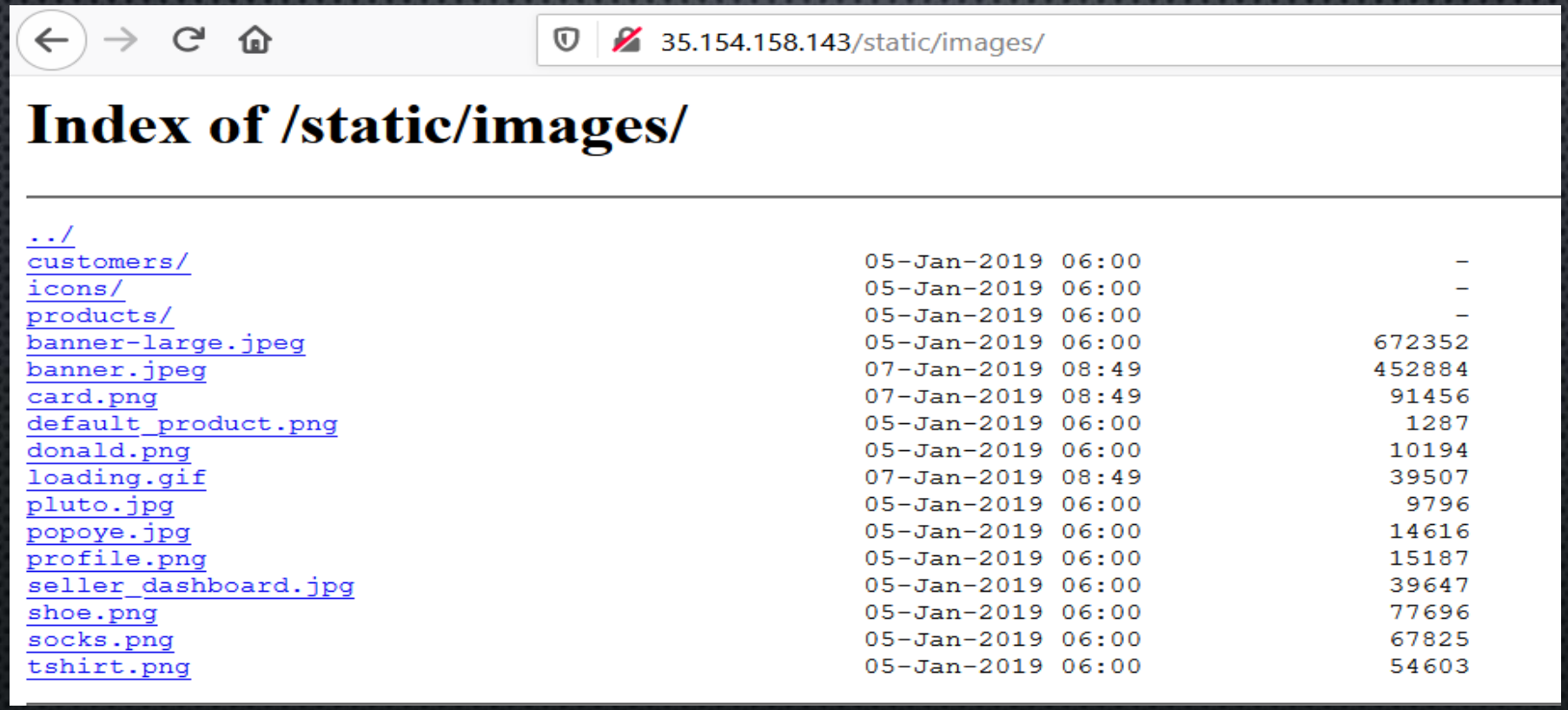
DIRECTORY LISTINGS (Severe)	Below affected URL are vulnerable to reflected XSS. **Affected URL**: http://35.154.158.143/robots.txt

OBSERVATION

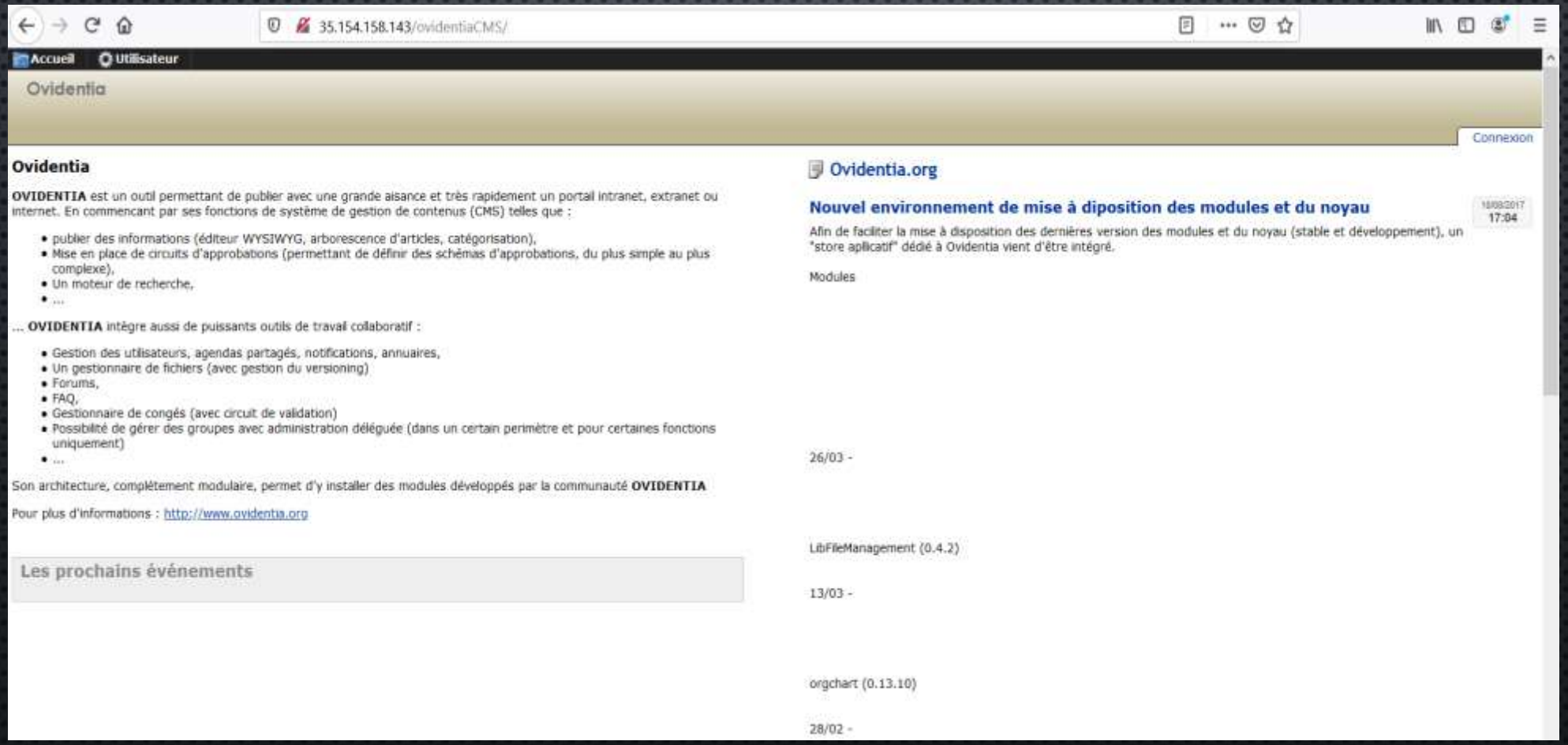
- GO TO HTTP://35.154.158.143/ROBOTS.TXT
- COMPLETE LIST AND DIRECTORIES OF THE CUSTOMER AND IMAGES OF PRODUCTS AND ALL THE PRODUCTS PAGE INFO AND ALSO THE ADMINISTRATOR DIRECTORY IS ALSO SHOWN.
- ALSO THIS SUFFERS WITH WEAK PASSWORD FLAW IN OVEDENTIACMS, WHICH LETS AN ATTACKER GET INSIDE THE ADMINISTRATOR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



POC


35.154.158.143/static/images/
Index of /static/images/
../
customers/ 05-Jan-2019 06:00 -
icons/ 05-Jan-2019 06:00 -
products/ 05-Jan-2019 06:00 -
banner-large.jpeg 05-Jan-2019 06:00 672352
banner.jpeg 07-Jan-2019 08:49 452884
card.png 07-Jan-2019 08:49 91456
default_product.png 05-Jan-2019 06:00 1287
donald.png 05-Jan-2019 06:00 10194
loading.gif 07-Jan-2019 08:49 39507
pluto.jpg 05-Jan-2019 06:00 9796
popoye.jpg 05-Jan-2019 06:00 14616
profile.png 05-Jan-2019 06:00 15187
seller_dashboard.jpg 05-Jan-2019 06:00 39647
shoe.png 05-Jan-2019 06:00 77696
socks.png 05-Jan-2019 06:00 67825
tshirt.png 05-Jan-2019 06:00 54603

POC


35.154.158.143/ovidentiaCMS/
Accueil
Utilisateur
Ovidentia
Connexion
Ovidentia
OVIDENTIA est un outil permettant de publier avec une grande aisance et très rapidement un portail intranet, extranet ou internet. En commencant 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 perimètre 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
Nouvel environnement de mise à diposition des modules et du noyau
17:04
Afin de faciliter la mise à disposition des dernières version des modules et du noyau (stable et développement), un "store applicatif" dédié à Ovidentia vient d'être intégré.
Modules
26/03 -
LibFileManagement (0.4.2)
13/03 -
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

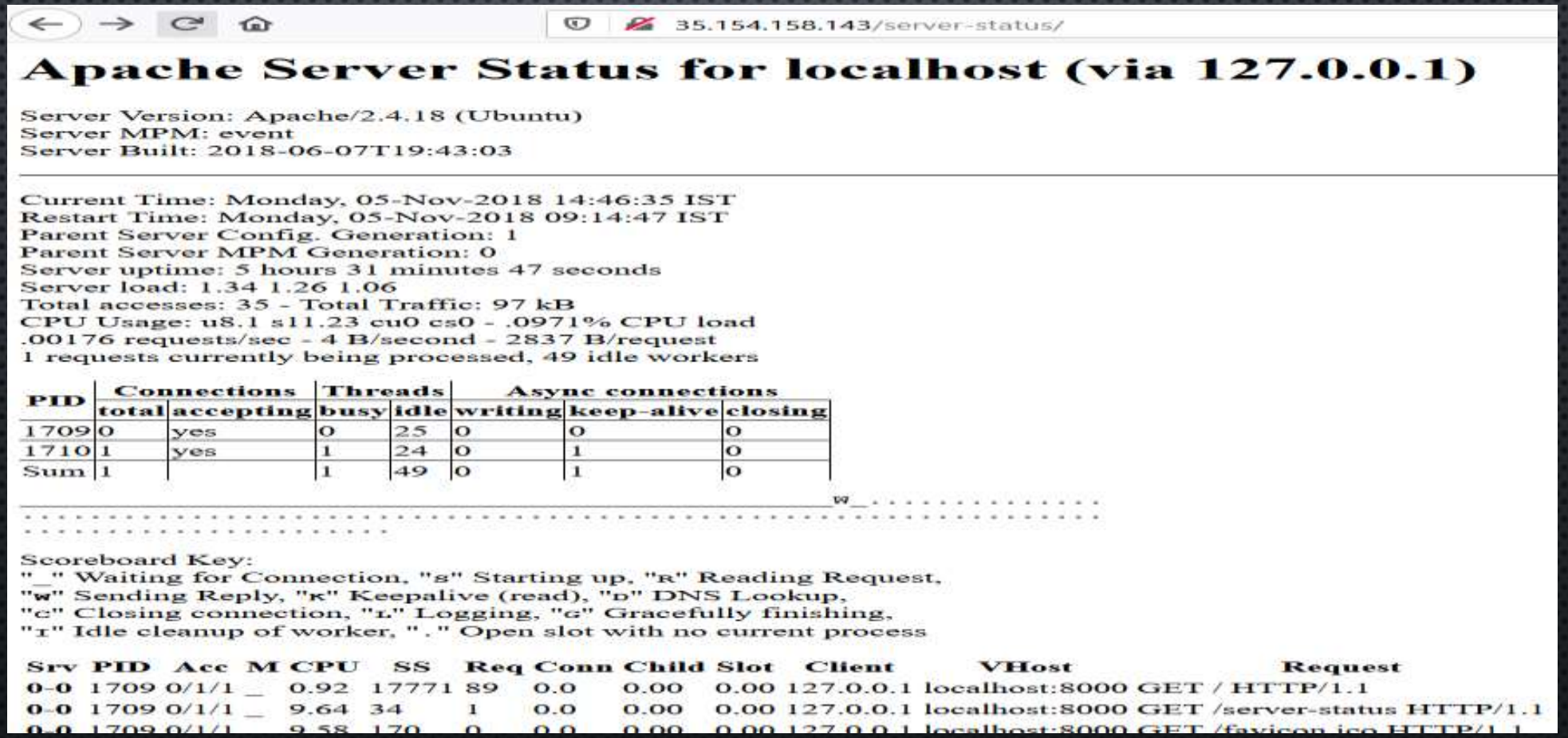
- Disable all the directory listings.
- Include a index.html in all folders with default messages.
- Remove all the default passwords and add your own new strong passwords which must have a special character and a number and must be greater or equal to 8 digits for maximum security.

6.INFORMATION DISCLOSURE

INFORMATION DISCLOSURE (LOW)	Below affected URL are vulnerable to reflected XSS. **Affected URL**: http://35.154.158.143/Server-status

OBSERVATION

GO TO HTTP://35.154.158.143/SERVER-STATUS AND INFORMATION WILL BE SHOWN LIKE BELOW.



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.

- RFERENCES:
- *HTTPS://VULDB.COM/?ID.88482*
- *HTTPS://HTTPD.APACHE.ORG/DOCS/CURRENT/MOD/MOD_STATUS.HTML*

7.PII LEAKAGE

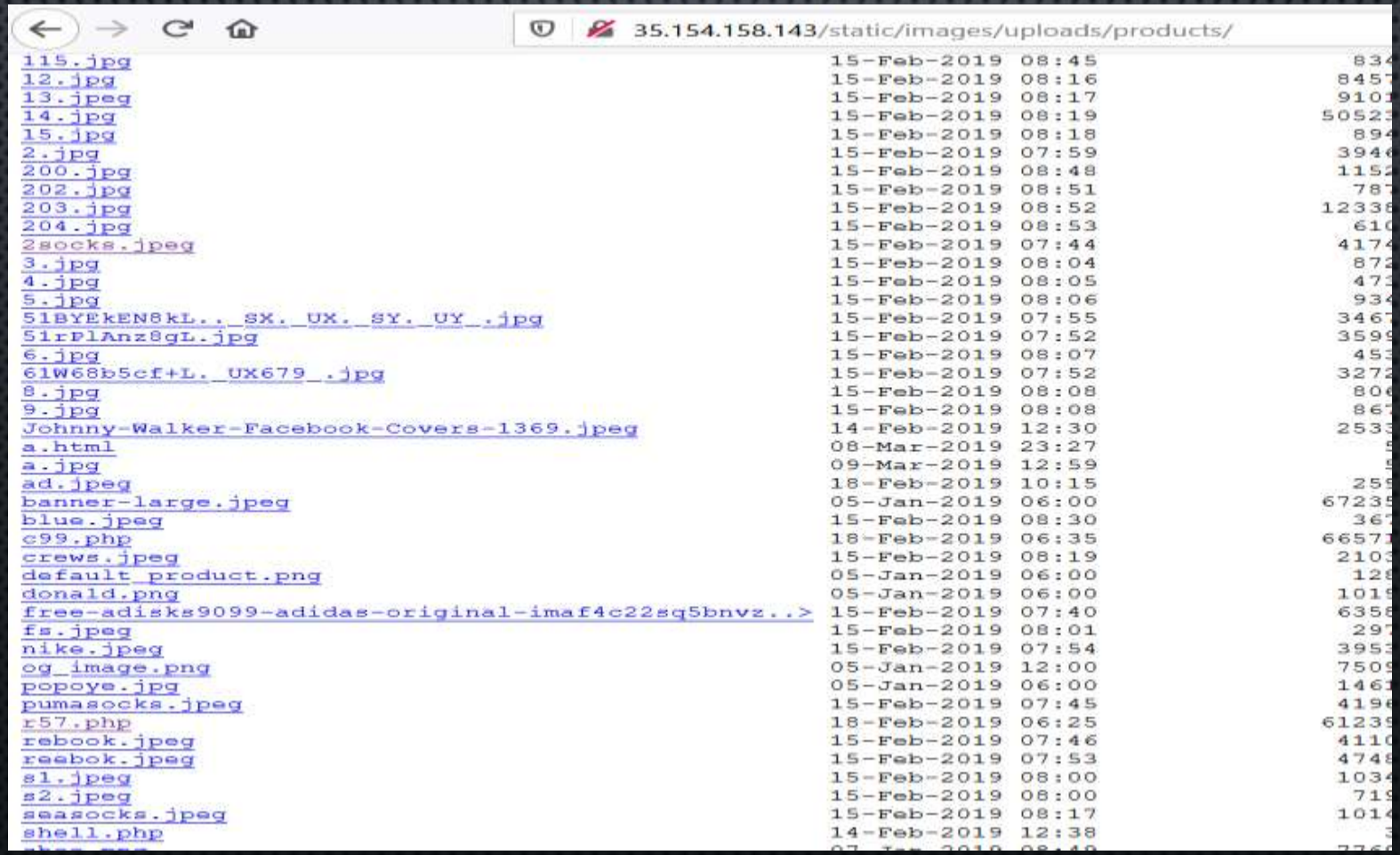
PII LEAKAGE (CRITICAL)	Below mentioned URL LEAKS Critical information via PII leakage. **Affected URL**: http://35.154.158.143/static/images/uploads/products/2socks.jpeg **Affected parameters**: IMAGE(every image after "products/")

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.JPEG" IN OUR CASE AND HIT ENTER, THE FOLLOWING PAGE WITH DETAILS WILL BE SHOWN,



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

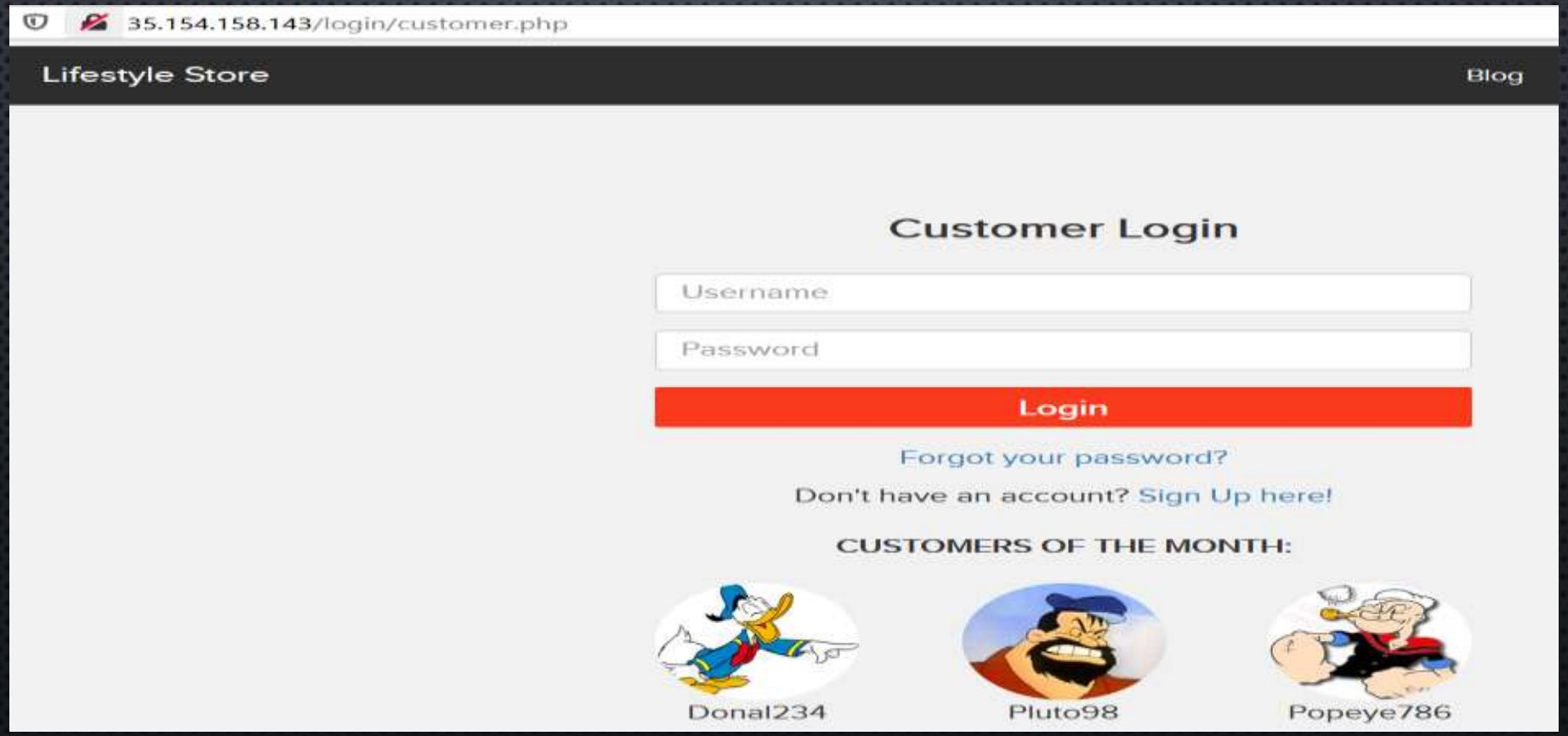
- 2- FACTOR AUTHENTICATIONS FOR SENSITIVE DATA SHOULD BE ADDED WITH STRONG PASSWORDS.
- FIND ALL PII STORED AND ENCRYPT THEM WITH VARIOUS TECHNIQUES AND ALSO DISABLE ALL THE LISTINGS.

8.SELF REDIRECTION/HTML/DEVELOPER FLAW

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

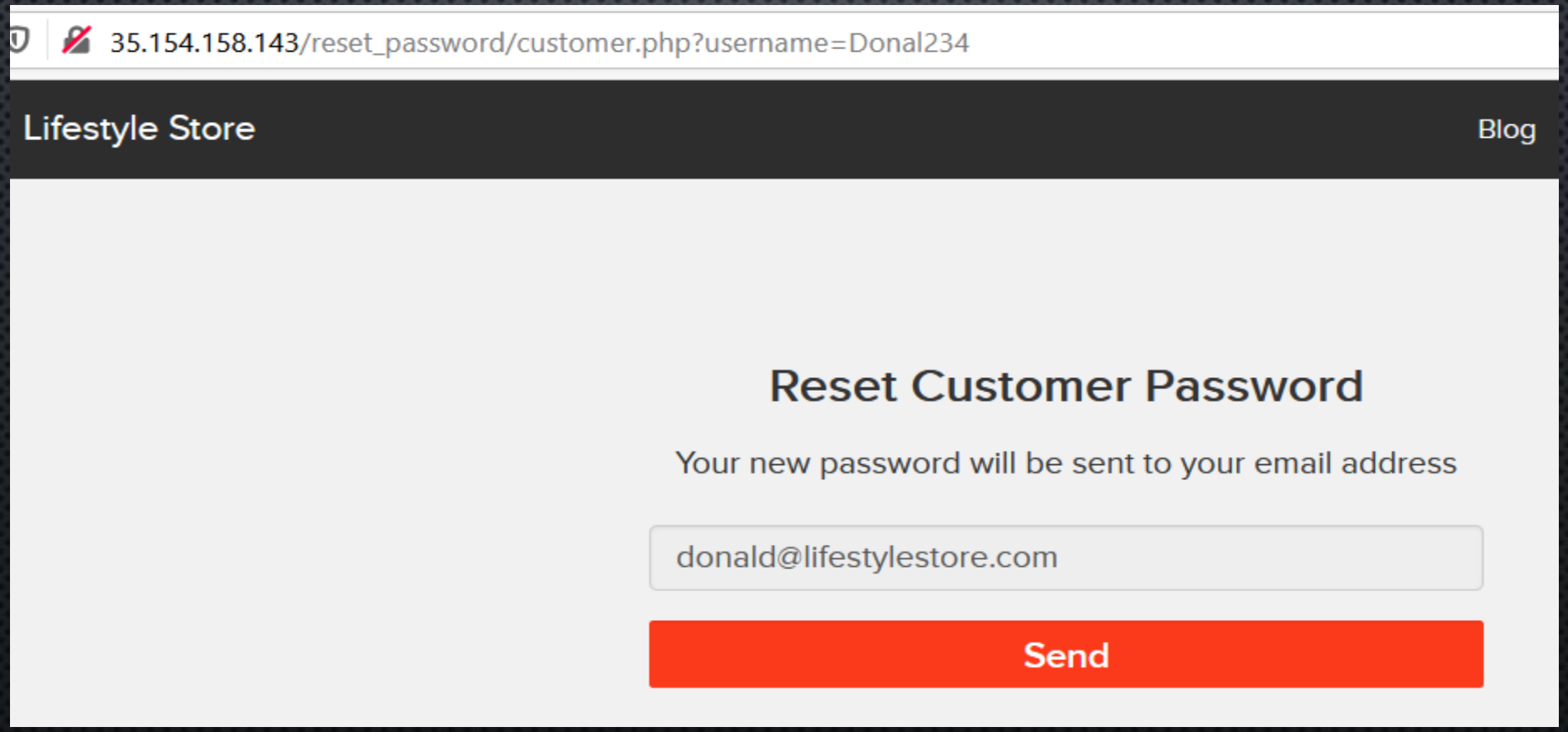
OBSERVATION

- GO TO 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,

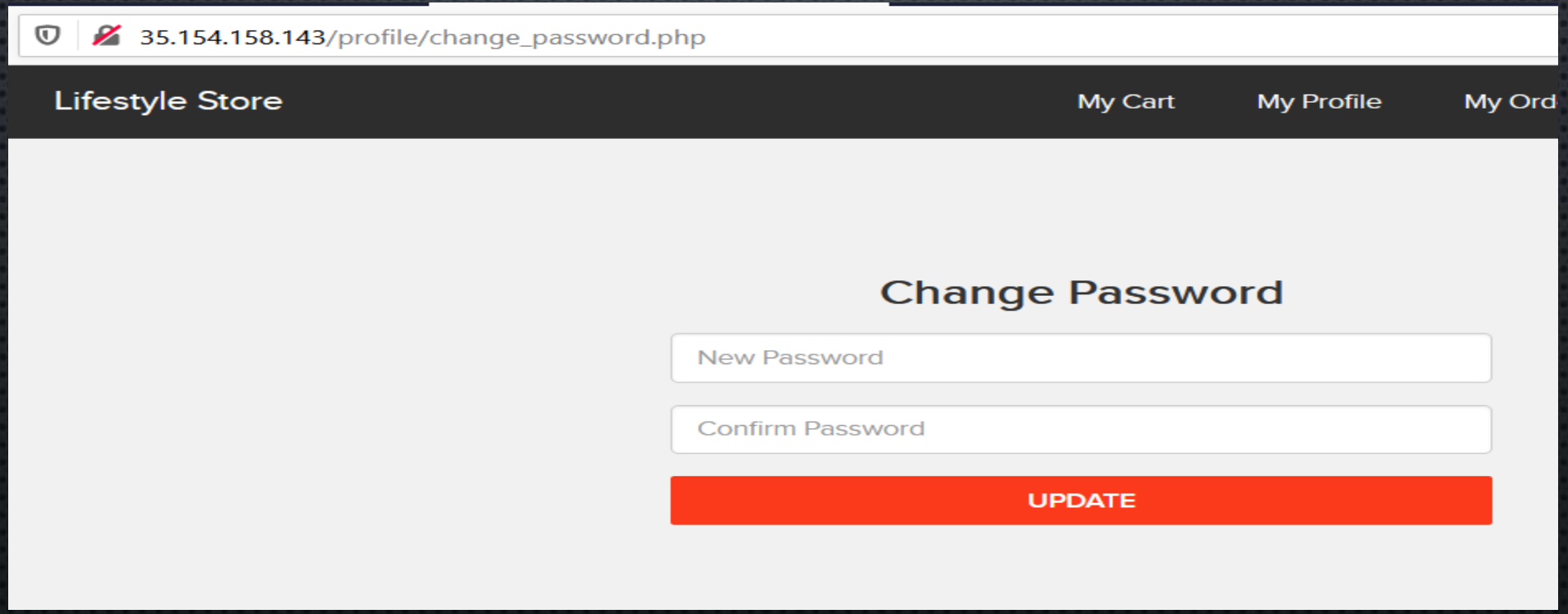


OBSERVATION

- 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.

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)



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)*

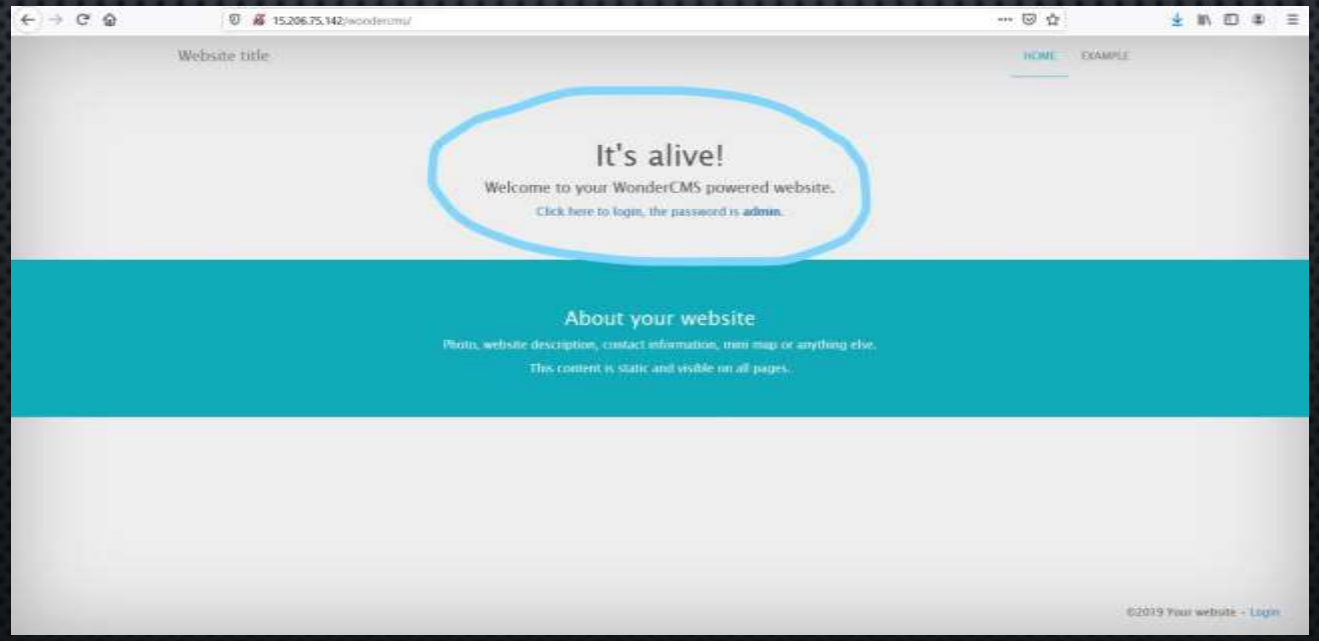
9.MULTIPLE VULNERABILITIES FOUND IN BLOG SITE(PII LEAKAGE , TEMPORARY XSS AND MORE)

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

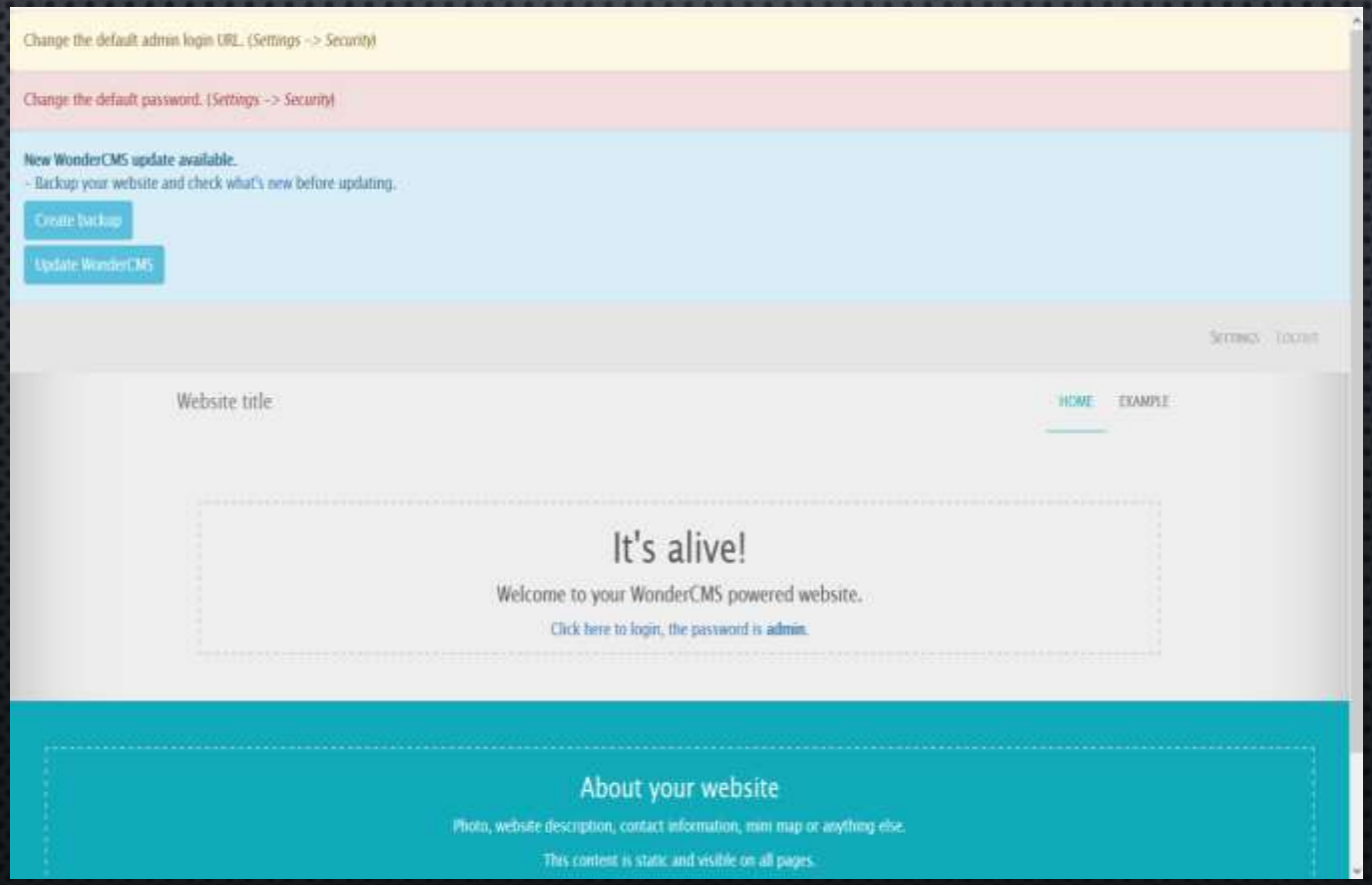
AT THE FRONT PAGE OF THE BLOG SITE WE CAN DIRECTLY FIND THE LOGIN OPTION , THAT SAYS "CLICK HERE TO LOGIN, THE PASSWORD IS ADMIN" BY CLICKING ON IT , IT WILL REDIRECTS TO THE LOGIN PAGE WHERE JUST BY ENTERING 'ADMIN' AS PASSWORD ONE CAN GET ACCESS TO THE ADMIN ACCOUNT OF THIS SITE. THIS IS A PROPER EXAMPLES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

THE LOGGED IN PAGE LOOKS LIKE BELOW,



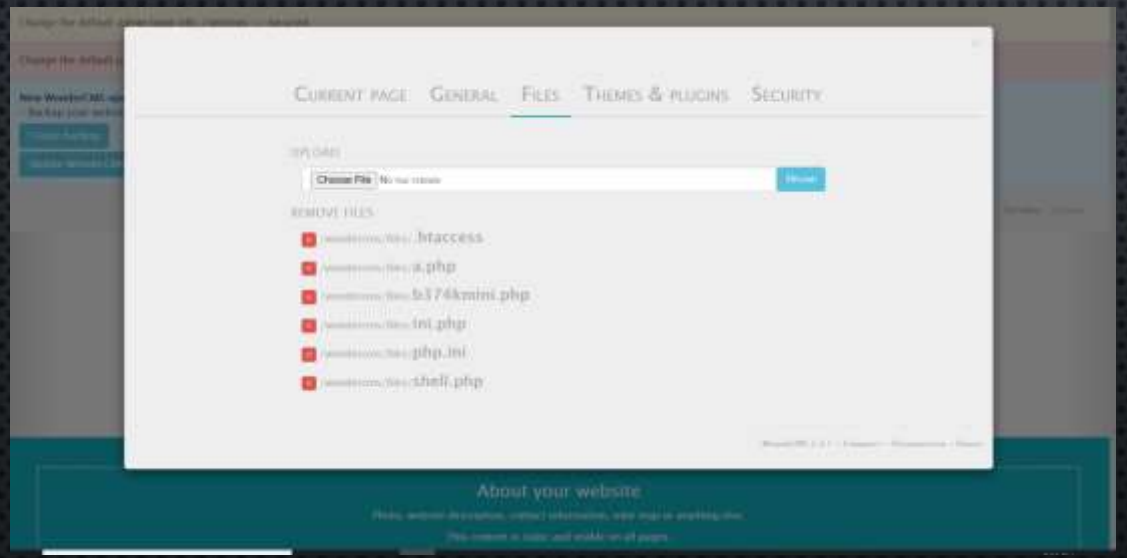
OBSERVATION

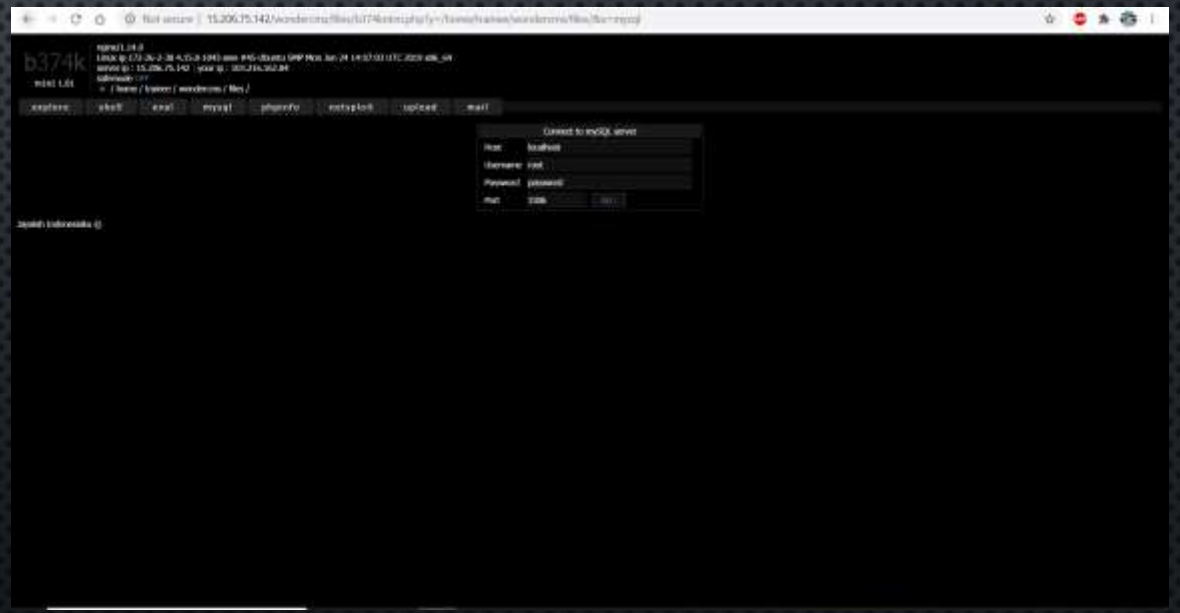
- WHEN WE LOG-IN AS THE ADMIN ,AT THE FIRST PAGE OF THE SITE WE CAN SEE SOME TEXT WRITTEN AS "IT'S ALIVE !_ _ _ _" IF WE CLICK ON IT , THE HTML CODES JUST STARTS RUNNING AND ONE MALICIOUS HACKER CAN EASILY MAKE CHANGES AND CAN USE THE PAGE AS HIS/HER PHISHING PORTAL . THIS IS A CLASSIC EXAMPLE OF TEMPORARY XSS.



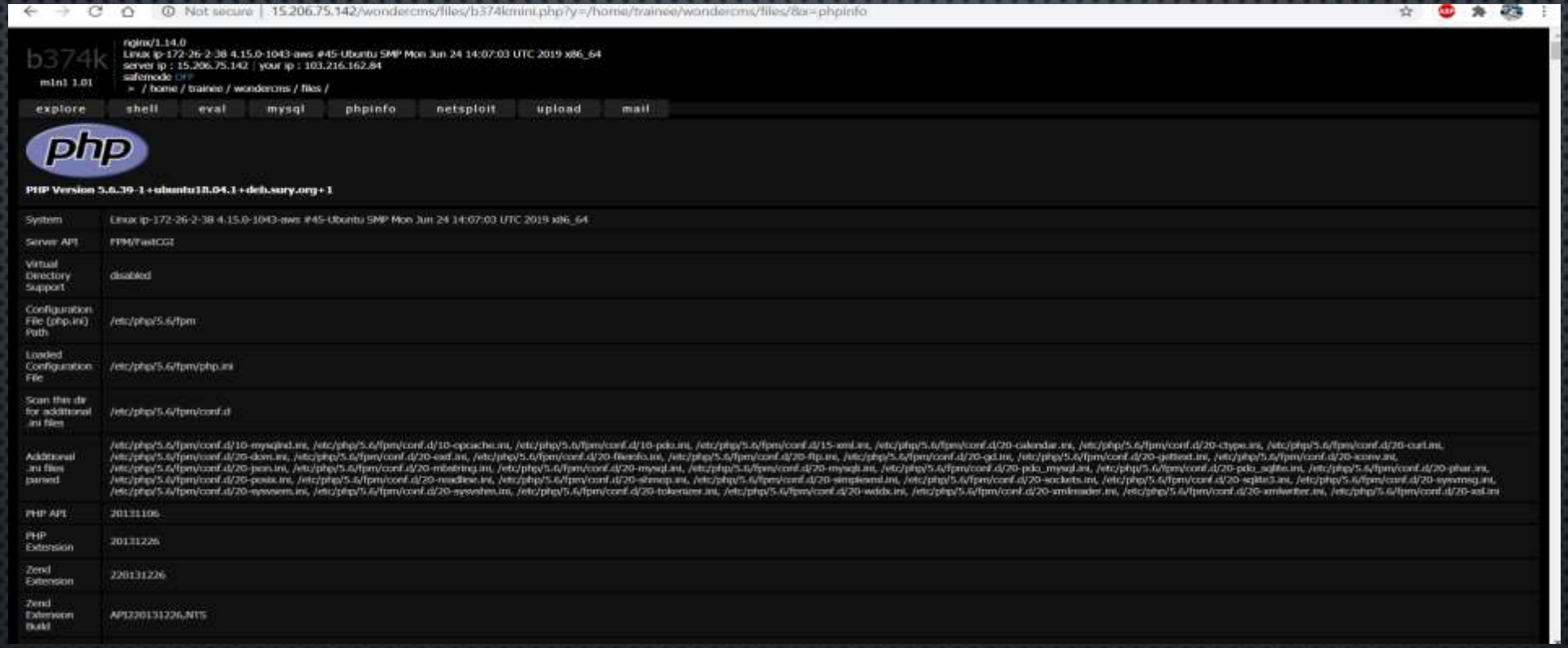
OBSERVATION

- 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) .





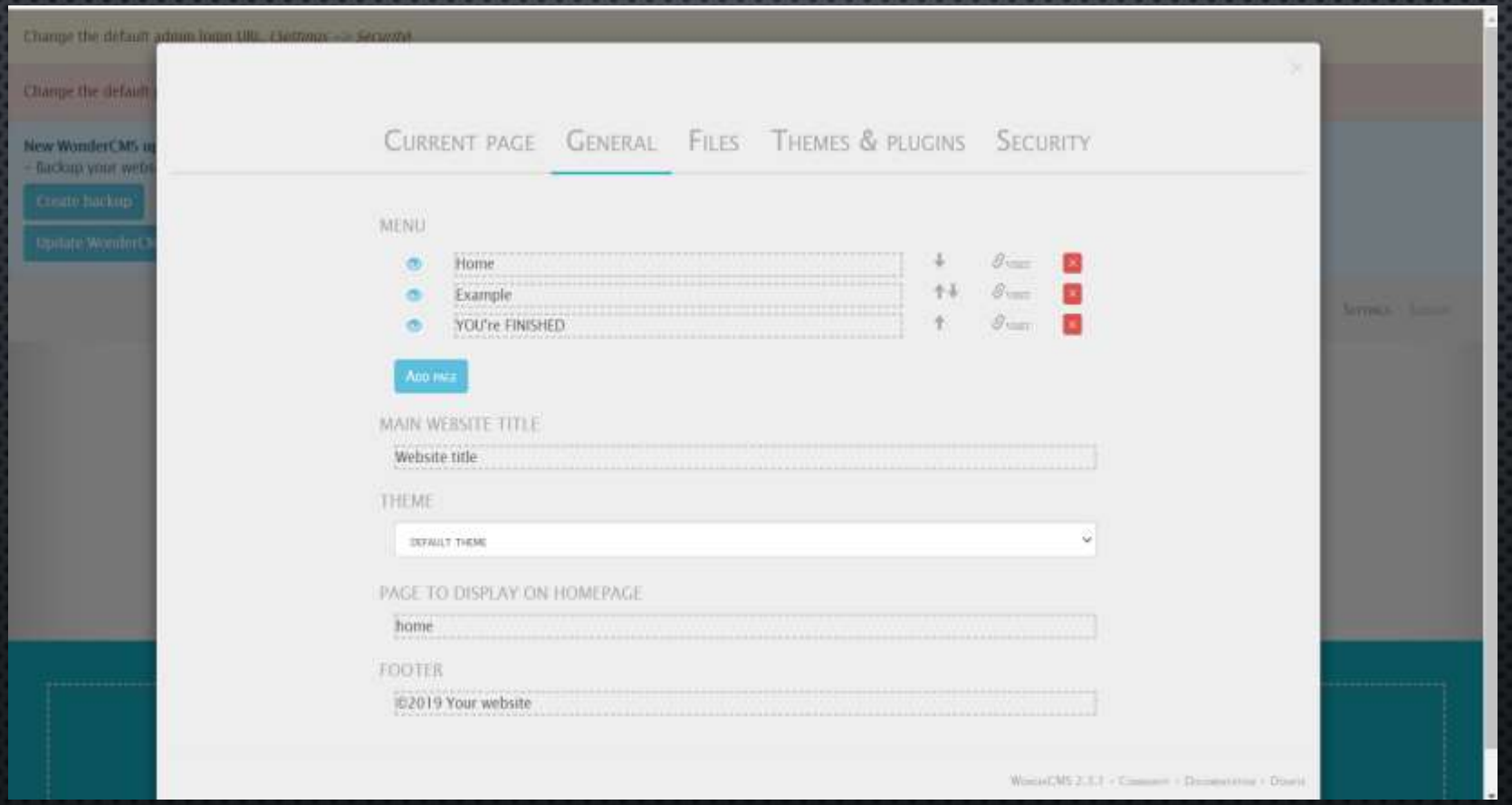
OBSERVATION



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

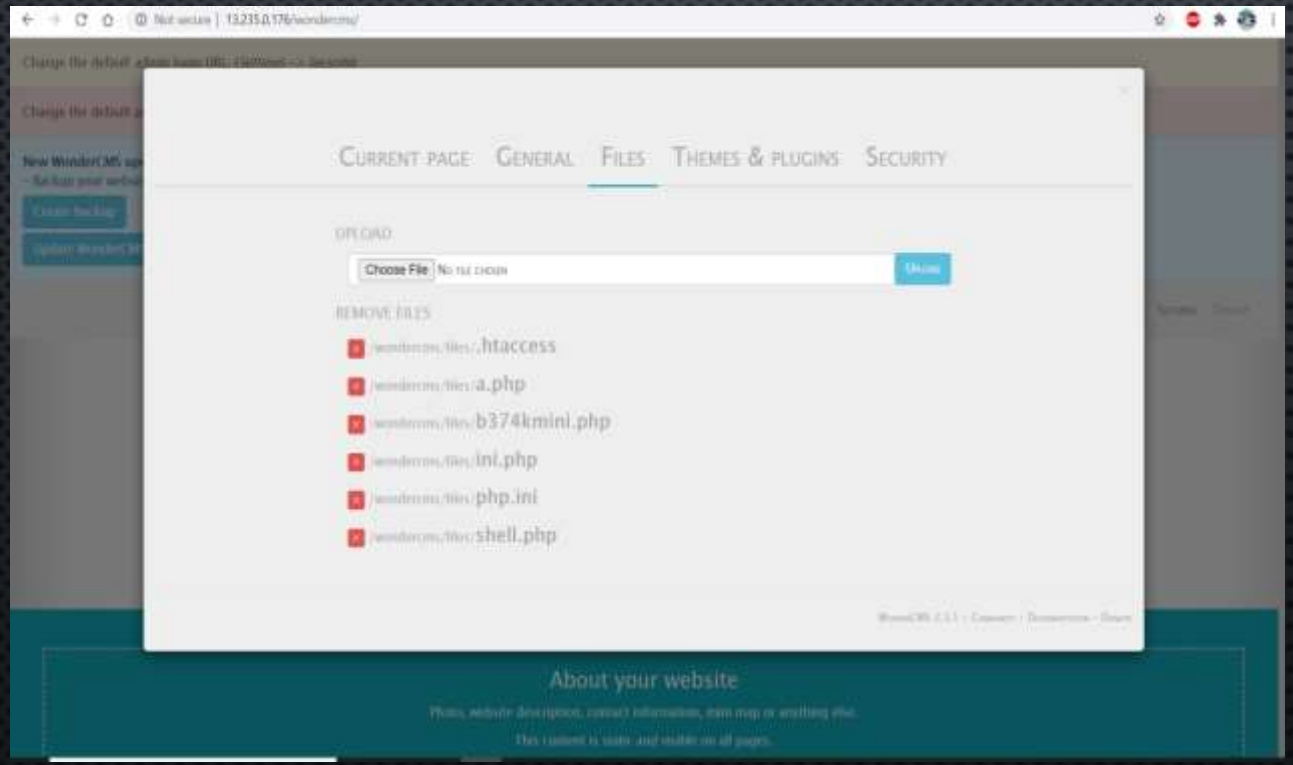
OBSERVATION

- 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://www.w3schools.com

THANK YOU

Contact to →bhamare2001@gmail.com

For further details and patch assistance