ETHICAL HACKING

PROJECT REPORT

Submitted in partial fulfillment of the requirements for the award of the degree

Of

-BACHELOR OF TECHNOLOGY-

In

ECE

By

ANJALI VIDYA SAGAR

13001022020

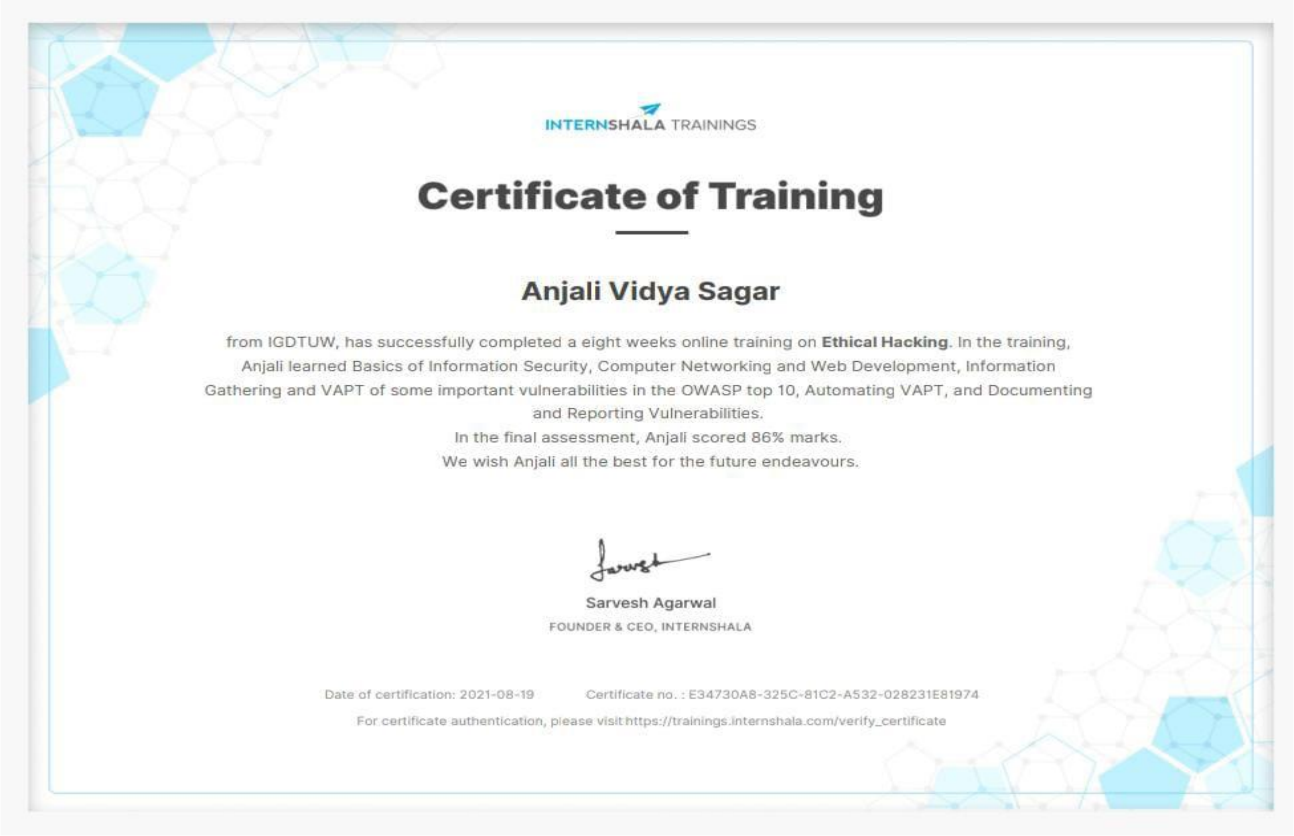
Guided by

Mr. Aman Sachdev
INTERNSHALA

INDIRA GANDHI DELHI TECHNICAL UNIVERSITY FOR WOMEN
NEW DELHI – 110006

JULY 2021

Certificate of training



INTERNSHALA TRAININGS

Certificate of Training

Anjali Vidya Sagar

from IGDTUW, has successfully completed a eight weeks online training on **Ethical Hacking**. In the training, Anjali learned Basics of Information Security, Computer Networking and Web Development, Information Gathering and VAPT of some important vulnerabilities in the OWASP top 10, Automating VAPT, and Documenting and Reporting Vulnerabilities.

In the final assessment, Anjali scored 86% marks.

We wish Anjali all the best for the future endeavours.

Sarvesh Agarwal
FOUNDER & CEO, INTERNSHALA

Date of certification: 2021-08-19   Certificate no. : E34730A8-325C-81C2-A532-028231E81974

For certificate authentication, please visit https://trainings.internshala.com/verify_certificate

.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to Mr. Aman Sachdev who is the virtual mentor at Internshala, and helped me learn Ethical Hacking from the scratch and encouraged me to do the project for the same, which also helped me in doing a lot of Research and I came to know about so many new things related to Ethical Hacking.

Secondly, I would also like to thank my teachers, parents and friends who helped me a lot during this internship.

DECLARATION

I, ANJALI VIDYA SAGAR, solemnly declare that the project report, is based on my own work carried out during the course of our study under the supervision of **Mr. Aman Sachdev through Internshala**. I assert the statements made and conclusions drawn are an outcome of my research work. I further certify that:

I. The work contained in the report is original and has been done by me under the supervision of my supervisor.

II. The work has not been submitted to any other Institution for any other degree/diploma/certificate in this university or any other University of India or abroad.

III. I have followed the guidelines provided by the university in writing thereport.

IV. Whenever I have used materials (text, data, theoretical analysis/equations, codes/program, figures, tables, pictures, text etc.) from other sources, we have given due credit to them in the report and have also given their details in the references.

ABSTRACT

Corporations and other entities are faced with the unenviable task of trying to defend their networks against various types of intrusive attacks. Although traditional methods of deterrence,(i.e. firewalls, intrusion detection devices, etc.) have their place in this battle, there has arisen the need to utilize specialists who are adopt at exploiting both known and unknown vulnerabilities in networks in order to determine the security posture of an organization. These "Ethical Hackers" have created a niche for themselves in the "Defense in-Depth" spectrum. This article seeks to various kinds of Ethical Hackers, and its process involved in the Ethical Hacking systems. Finally Ethical Hacker's qualification will be discussed

INDEX

INTRODUCTION

As the computer technology advances, it has its darker side also; HACKERS. In today world the size of the internet is growing at a very fast rate, a large amount of data is moving online, therefore, data security is the major issue. The internet has led to the increase in the digitization of various processes like banking, online transaction, online money transfer, online sending and receiving of various forms of data, thus increasing the risk of the data security. Nowadays a large number of companies, organizations, banks, and websites are targeted by the various types of hacking attacks by the hackers. Generally, after hearing the term hacker we all think of the bad guys who are computers experts with bad intensions, who tries to steal, leak or destroy someone's confidential or valuable data without their knowledge. They are the persons with very high computer skills who tries to break into someone else security for gaining access to their personal information, but all the times it is not like that. To overcome the risk of being hacked by the hackers we have Ethical Hackers in the industry, who are also computer experts just like the hackers but with good intensions or bounded by some set of rule and regulations by the various organizations. These are the persons who try to protect the online moving data by the various attacks of the hackers and keeping it safe with the owner. Further, this paper tells you more about hackers, ethical hackers and Linux operating system (kali Linux) and aware you about some attacks performed by the hackers on the interne

MODULE 1:
Basics of Information Security and Computer Networking

In this module we learned:

- What is hacking?
  It is an attempt to exploit a computer system or a private network inside a computer.
- Types of hacking
  - Ethical hacking
  - Unethical hacking
- Types of hackers
  - White Hat hackers
  - Black Hat hackers
  - Grey Hat hackers
- Classification of computer networks
  - Internal Network
  - External Network
- IP Address, Domain names and DNS, Ports, Protocols TCP/IP Model and concept of proxy and VPNs.

MODULE 2:
Information Gathering and Basics of Web Development

In this module we learned:

- Concept of Digital Footprinting
- Information Gathering
- Reconnaissance
- What is Whols?
- Reverse IP Lookup
- Search engines and dorks
- Google Dorks
- GHDB (Google Hacking Database)
- Basics of Web Architecture
- What is HTML?
- Web Servers
- Common Security Misconceptions
- Basics of HTML
- Fundamentals of PHP

MODULE 3:
Introduction to Web VAPT, OWASP and SQL Injections

In this module we learned:

- Vulnerability assessment
- Penetration testing
- Introduction to OWASP
- Introduction to SQL and Databases
- How to write basic SQL queries
- SQL injection
- Introduction to Burp Suit

MODULE 4:
Advanced Web Application Attacks

In this module we learned:

- Web application filters
- Steps to bypass client side filters
- Understanding IDOR
- Rate limiting flaws
- Basic file uploading vulnerabilities
- Uploading shells

MODULE 5:
Client Side Attacks

In this module we learned:

- Understanding Response headers
- Sessions and cookies
- DOM – Document Object Model
- Basics of JS
- JavaScript Elements
- Event listeners
- Cross Site Scripting (XSS)
    - Temporary XSS
    - Permanent XSS
- HTML Injection
- Exploiting temporary XSS
- Exploiting permanent XSS
- Authentication and Authorisation
- Forced Browsing
- Session – Cookie flaws
- CSRF – Cross Site Request Forgery
- Understanding open redirection

- Brute forcing and its types
- PII(Personally Identifiable Information) Leakage
- Sensitive Information Disclosure

MODULE 6:
Identifying Security Misconfiguration and Exploiting Outdated Web Applications

In this module we learned:

- Common Security Misconfigurations
- Descriptive Error messages
- Default debug files
- Default debug pages
- Guess weak passwords
- Components with known vulnerability
    - Fingerprinting components
    - Finding exploits
- CMS – Content Management Systems
- Ways to Fingerprint third party components
    - Manual
    - Automated
- Scanning WordPress CMS for known vulnerabilities
- Exploiting Vulnerable Components

MODULE 7:
Automating VAPT and Secure Code Development

In this module we learned:

- Techniques of Advanced information gathering
- Tools used for Advanced information gathering
    - Dirbuster
- N-map – Network Mapper
- N-map Scans
- Tools for Automating VAPT
- Nikto
- Configuration flaws captured by Nikto

MODULE 8:
Documenting and Reporting Vulnerabilities

In this module we learned:

- Importance of Documentation

- Fundamental concepts of documenting a vulnerability
- Steps for PoC for Nikto scan
- Tools used for preparing a PoC
- Tips for PoC
- Kinds for VAPT Reports
    - For developers – Detailed developer report
    - For security in-charges – High level management summary
- Improper input and output sanitization
- Recommendations for OWASP Top 10 Vulnerabilities
- Concepts of code patching
- Components of a VAPT report
- Categorization of vulnerabilities
- Tips for writing a report

Benefits or advantages of Ethical Hacking

Following are the benefits or advantages of Ethical Hacking:

➡It helps to fight against cyber terrorism and to fight against national security breaches.

It helps to fight against cyber terrorism and to fight against national security breaches.

➡It helps to take preventive action against hackers.

➡It helps to build a system which prevents any kinds of penetration by hackers.

➡Ethical hacking offers security to banking and financial establishments.

➡It helps to identify and close the open holes in a computer system or network.

Drawbacks or disadvantages of Ethical Hacking

Following are the drawbacks or disadvantages of Ethical Hacking:

➡This may corrupt the files of an organization.

➡Ethical hacker might use information gained for malicious use. Hence trustful hackers are needed to have success in this system.

➡Hiring such professionals will increase cost to the company.

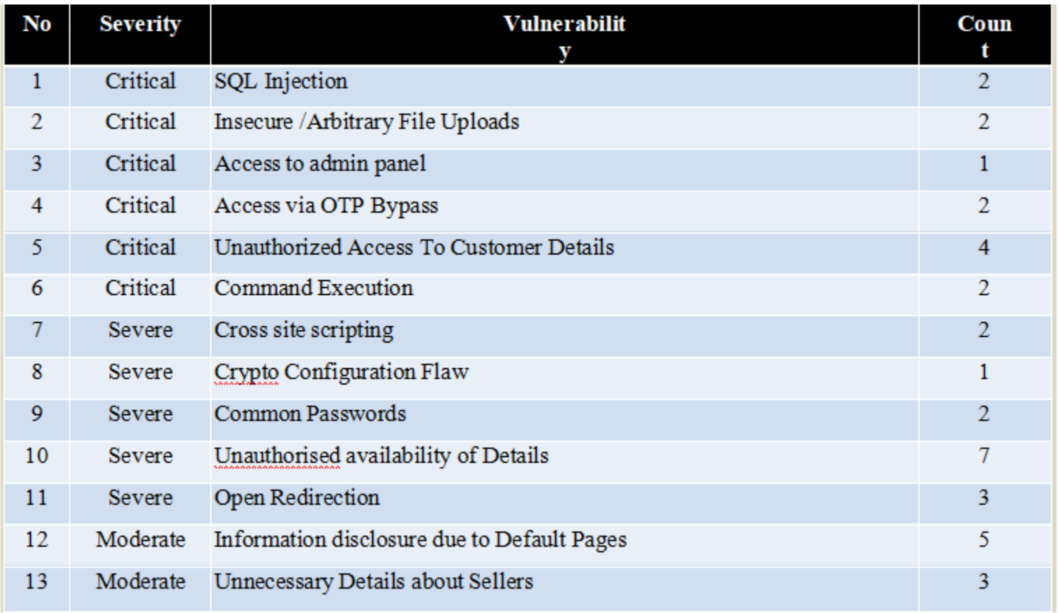
➡The technique can harm someone's privacy.

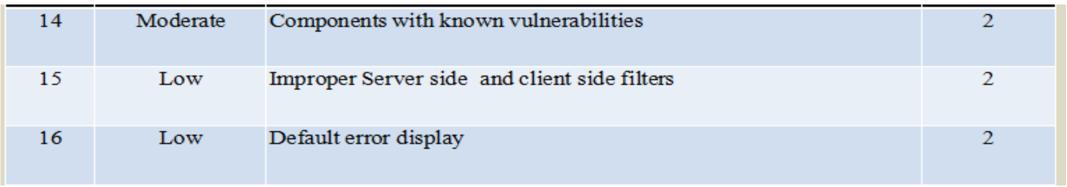
➡The system is illegal.

ABOUT PROJECT AND 16 VULNERABILITIES :

In the final project, I performed ethical hacking on a dummy website provided by Internshala. It was a real life-like web application in the form of an online e-commerce portal. I prepared a detailed developer report of all the vulnerabilities and loopholes (including the PoCs) that I found in the dummy website.

Number of vulnerabilities that I found on the life store dummy websites are





No	Severity	Vulnerability	Count
1	Critical	SQL Injection	2
2	Critical	Insecure /Arbitrary File Uploads	2
3	Critical	Access to admin panel	1
4	Critical	Access via OTP Bypass	2
5	Critical	Unauthorized Access To Customer Details	4
6	Critical	Command Execution	2
7	Severe	Cross site scripting	2
8	Severe	Crypto Configuration Flaw	1
9	Severe	Common Passwords	2
10	Severe	Unauthorised availability of Details	7
11	Severe	Open Redirection	3
12	Moderate	Information disclosure due to Default Pages	5
13	Moderate	Unnecessary Details about Sellers	3
14	Moderate	Components with known vulnerabilities	2
15	Low	Improper Server side and client side filters	2
16	Low	Default error display	2

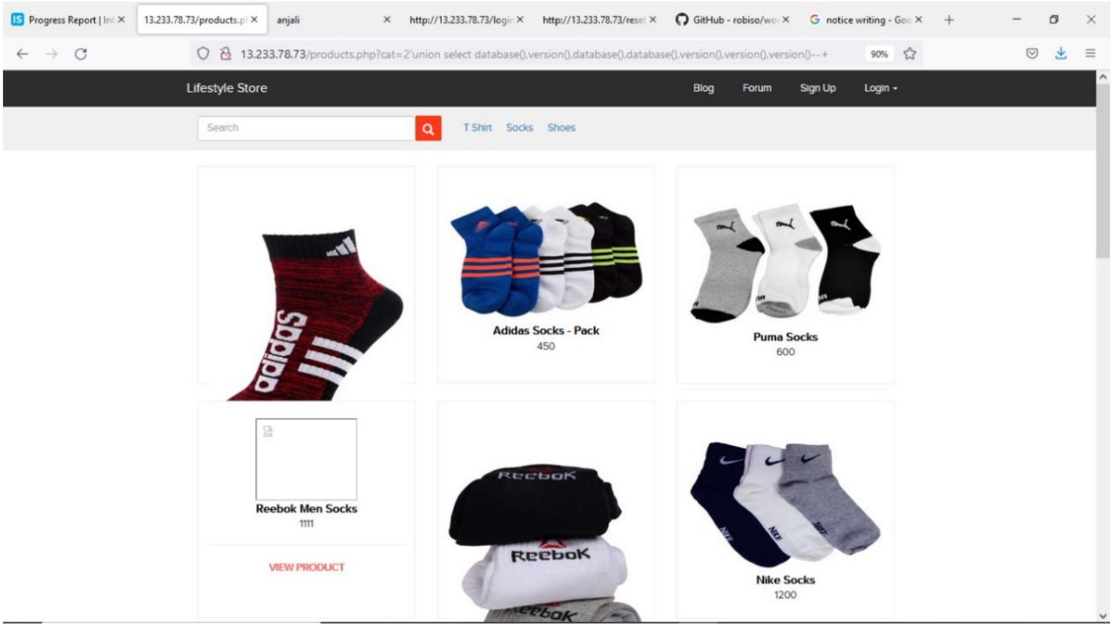
1.SQL Injection

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.

Proof of Concept (PoC)

•Attacker can execute SQL commands as shown below. Here we have used the payload below to extract the database name and MySQL version information:

http://13.233.148.87/products.php?cat=1' union select database(),version(),database(),database(),version(),version(),version() --+



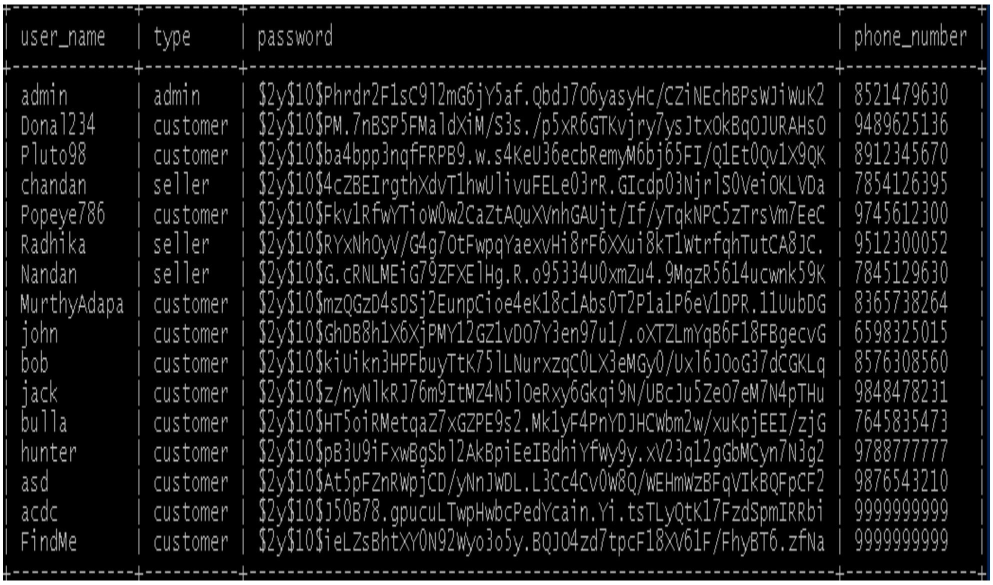
13.233.78.73/products.php?cat=2'union select database(),version(),database(),database(),version(),version(),version()--+

Proof of Concept (PoC)

•No of databases: 2
•information_schema
•hacking_training_project

•No of tables in SQL_Injection_V3: 10
•brands
•cart_items
•categories
•customers
•order_items
•orders

- product_reviews
- products
- sellers
- users



```
+-------------+----------+--------------------------------------------------------------+--------------+
| user_name   | type     | password                                                     | phone_number |
+-------------+----------+--------------------------------------------------------------+--------------+
| admin       | admin    | $2y$10$Phrdr2F1sC912mG6jY5af.QbdJ7O6yasyHc/CZiNEchBPsWJiWuK2 | 8521479630   |
| Donal234    | customer | $2y$10$PM.7nBSP5FMaldXiM/S3s./p5xR6GTKvjry7ysJtxOkBqOJURAHsO | 9489625136   |
| Pluto98     | customer | $2y$10$ba4bpp3nqfFRPB9.w.s4KeU36ecbRemyM6bj65FI/Q1Et0Qv1X9QK | 8912345670   |
| chandan     | seller   | $2y$10$4cZBEIrgthXdvT1hwUlivuFELe03rR.GIcdp03Njrl S0VeiOKLVDa | 7854126395   |
| Popeye786   | customer | $2y$10$Fkv1RfwYTioW0w2CaZtAQuXVnhGAUjt/If/yTqkNPC5zTrsVm7EeC | 9745612300   |
| Radhika     | seller   | $2y$10$RYxNhOyV/G4g7OtFwpqYaexvHi8rF6XXui8kT1wtrfqhTutCA8JC. | 9512300052   |
| Nandan      | seller   | $2y$10$G.cRNLMEiG79ZFXElHg.R.o95334U0xmZu4.9MqzR5614ucwnk59K | 7845129630   |
| MurthyAdapa | customer | $2y$10$mzQGzD4sDSj2EunpCioe4eK18c1Abs0T2P1a1P6eV1DPR.11UubDG | 8365738264   |
| john        | customer | $2y$10$GhDB8h1X6XjPMY12GZ1vDO7Y3en97u1/.oXTZLmYqB6F18FBgecvG | 6598325015   |
| bob         | customer | $2y$10$kiUikn3HPFbuyTtK75lLNurxzqC0LX3eMGy0/Ux16JOoG37dCGKLq | 8576308560   |
| jack        | customer | $2y$10$z/nyNlkRJ76m9ItMZ4N5lOeRxy6Gkqi9N/UBcJu5ZeO7eM7N4pTHu | 9848478231   |
| bulla       | customer | $2y$10$HT5oiRMetqaZ7xGZPE9s2.Mk1yF4PnYDJHCWbm2w/xuKpjEEI/zjG | 7645835473   |
| hunter      | customer | $2y$10$pB3U9iFxwBgSbl2AkBpiEeIBdhiYfWy9y.xV23q12gGbMCyn7N3g2 | 9788777777   |
| asd         | customer | $2y$10$At5pFZnRWpjCD/yNnJWDL.L3Cc4Cv0W8Q/WEHmWzBFqVIkBQFpCF2 | 9876543210   |
| acdc        | customer | $2y$10$J50B78.gpucuLTwpHwbcPedYcain.Yi.tsTLyQtK17FzdSpmIRRbi | 9999999999   |
| FindMe      | customer | $2y$10$ieLZsBhtXY0N92Wyo3o5y.BQJO4zd7tpcF18XV61F/FhyBT6.zfNa | 9999999999   |
+-------------+----------+--------------------------------------------------------------+--------------+
```

2.Insecure /Arbitrary File Uploads

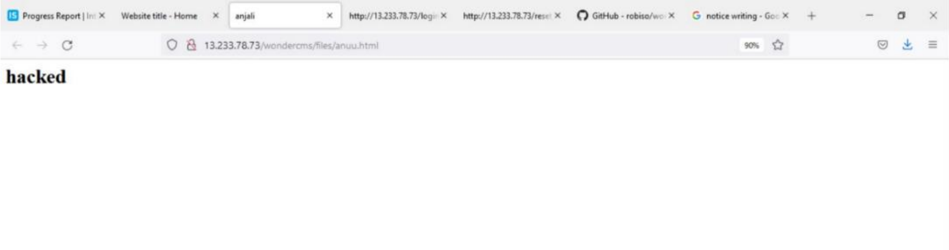
This happens when applications do not implement proper file type checking and allow uploading of files of different file formats. For example, a PHP file instead of a jpeg profile picture

Proof of Concept (PoC)

- Weak password - admin.

- Arbitrary File Inclusion.

Below is the result of the uploded file in the previous slide likewise some malicious shell can be uploaded as well.

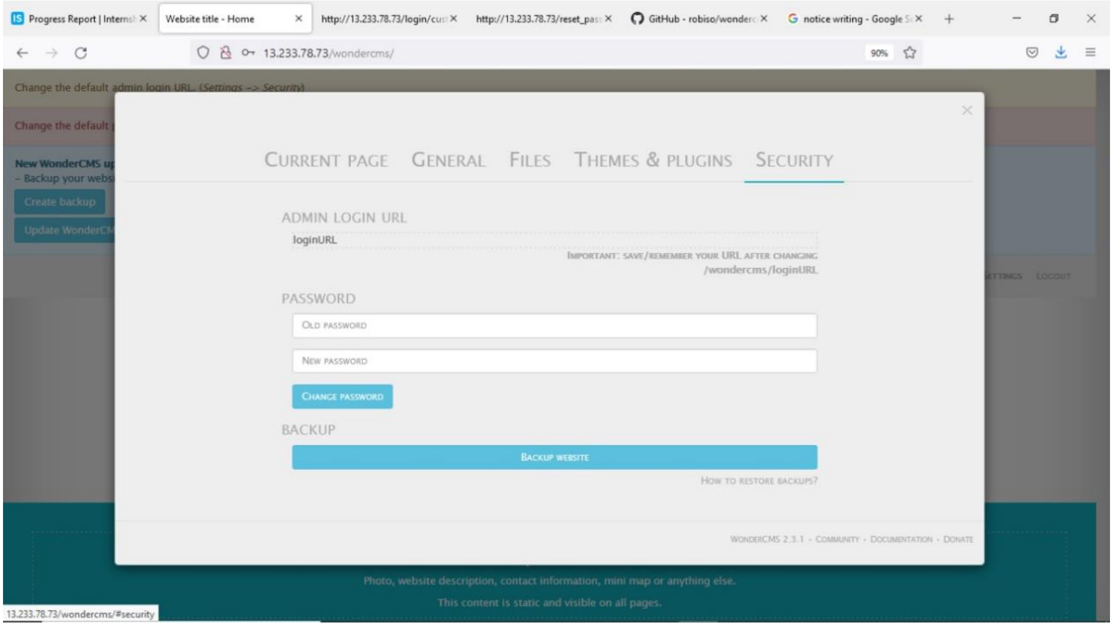


hacked

3. Access to admin panel

Proof of Concept (PoC)

Hacker can change the admin login password making the actual admin unable to login the next time.Hacker can also add and delete anything



13.233.78.73/wondercms/

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

ADMIN LOGIN URL

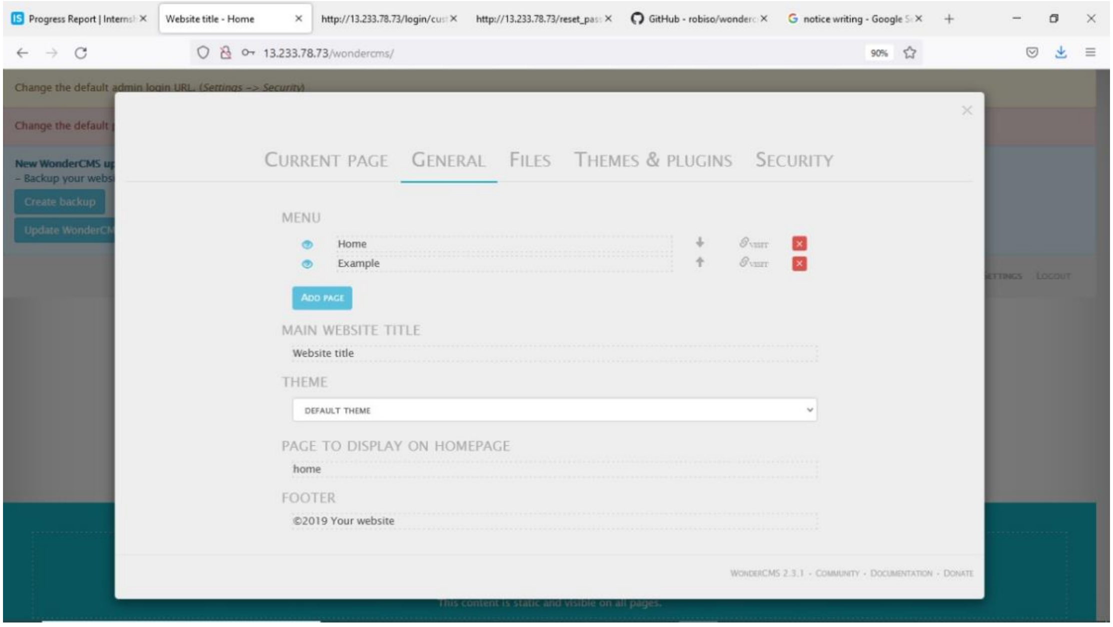
loginURL

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

PASSWORD

13.233.78.73/wondercms/#security

Progress Report | Interns
Website title - Home
http://13.233.78.73/login/cu
http://13.233.78.73/reset_pas
GitHub - robiso/wonder
notice writing - Google S
90%
Change the default
New WonderCMS u
– Backup your webs
Create backup
Update WonderCM
CURRENT PAGE
GENERAL
FILES
THEMES & PLUGINS
SECURITY
OLD PASSWORD
NEW PASSWORD
CHANGE PASSWORD
BACKUP
BACKUP WEBSITE
HOW TO RESTORE BACKUPS?
SETTINGS
LOGOUT
WONDERCMS 2.3.1 · COMMUNITY · DOCUMENTATION · DONATE
Photo, website description, contact information, mini map or anything else.
This content is static and visible on all pages.



13.233.78.73/wondercms/

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

MENU

Home

Example

MAIN WEBSITE TITLE

Website title

THEME

DEFAULT THEME

PAGE TO DISPLAY ON HOMEPAGE

home

FOOTER

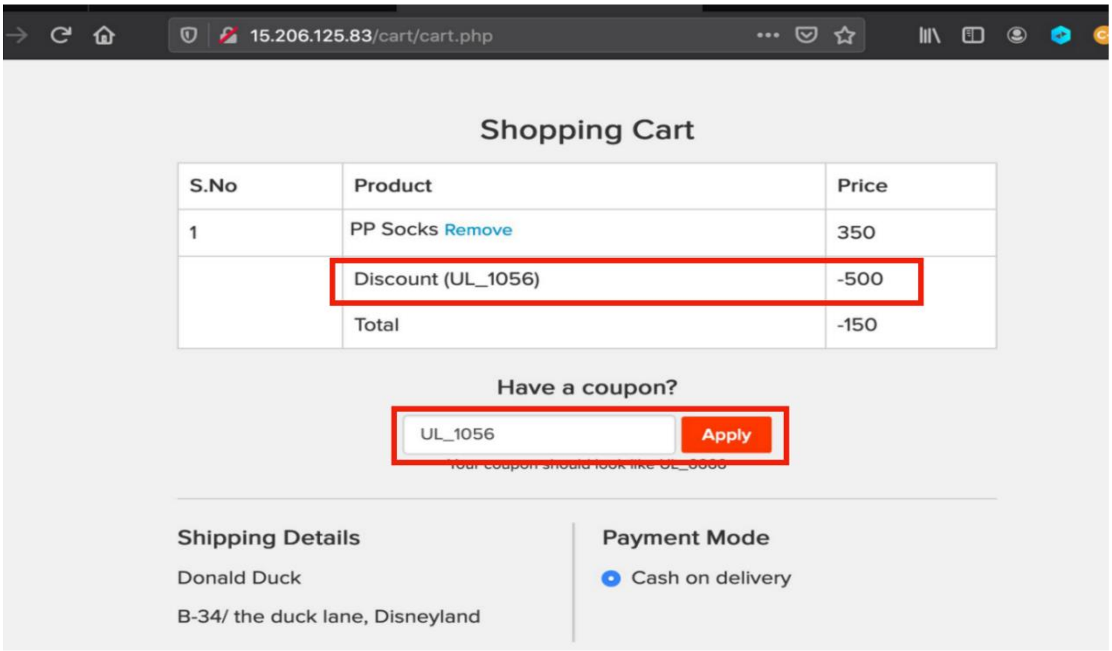
©2019 Your website

Progress Report | Interns
Website title - Home
http://13.233.78.73/login/cu
http://13.233.78.73/reset_pas
GitHub - robiso/wonder
notice writing - Google S
90%
Change the default
New WonderCMS u
– Backup your webs
Create backup
Update WonderCM
CURRENT PAGE
GENERAL
FILES
THEMES & PLUGINS
SECURITY
VISIT
VISIT
ADD PAGE
SETTINGS
LOGOUT
WONDERCMS 2.3.1 · COMMUNITY · DOCUMENTATION · DONATE
This content is static and visible on all pages.

4.Access via OTP Bypass

Proof of Concept (PoC)

At url http://13.233.78.73/cart/cart.php coupon code - UL-1056 is applied.


15.206.125.83/cart/cart.php

Shopping Cart

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

Have a coupon?

UL_1056
Apply
Your coupon should look like UL_0000

Shipping Details

Donald Duck

B-34/ the duck lane, Disneyland

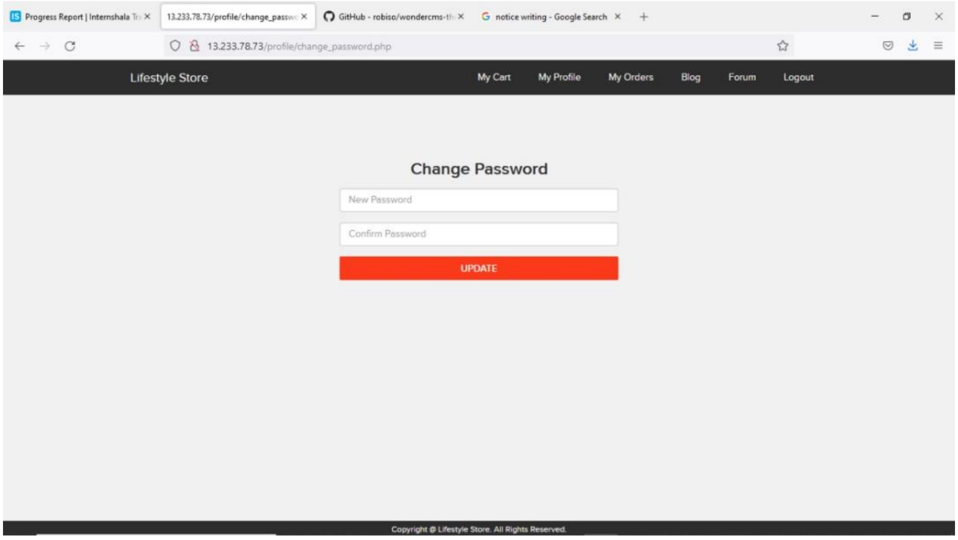
Payment Mode

● Cash on delivery

5.Unauthorised Access To Customer Details

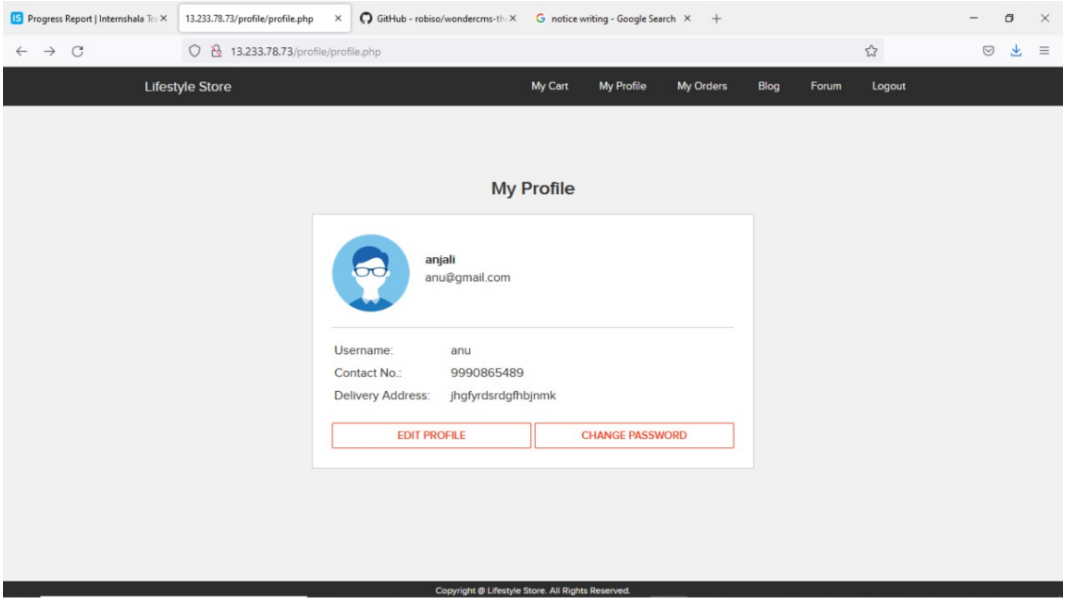
Proof of Concept (PoC)

•Attacker can change the details and password of the customer easily and can place orders on user’s behalf.


Progress Report | Internshala Tr
13.233.78.73/profile/change_passw
GitHub - robiso/wondercms-th
notice writing - Google Search
13.233.78.73/profile/change_password.php
Lifestyle Store
My Cart
My Profile
My Orders
Blog
Forum
Logout

Change Password

New Password
Confirm Password
UPDATE
Copyright @ Lifestyle Store. All Rights Reserved.


Progress Report | Internshala Tr
13.233.78.73/profile/profile.php
GitHub - robiso/wondercms-th
notice writing - Google Search
13.233.78.73/profile/profile.php
Lifestyle Store
My Cart
My Profile
My Orders
Blog
Forum
Logout
EDIT PROFILE
CHANGE PASSWORD
Copyright @ Lifestyle Store. All Rights Reserved.

My Profile

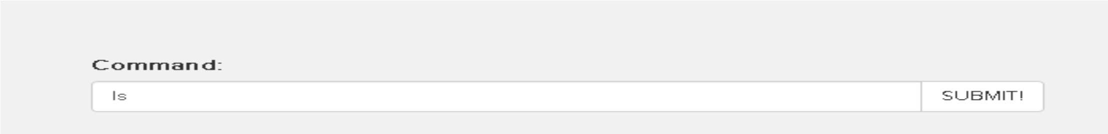
anjali
anu@gmail.com

Username: anu
Contact No.: 9990865489
Delivery Address: jhgfyrdsrdgfhbjnmk

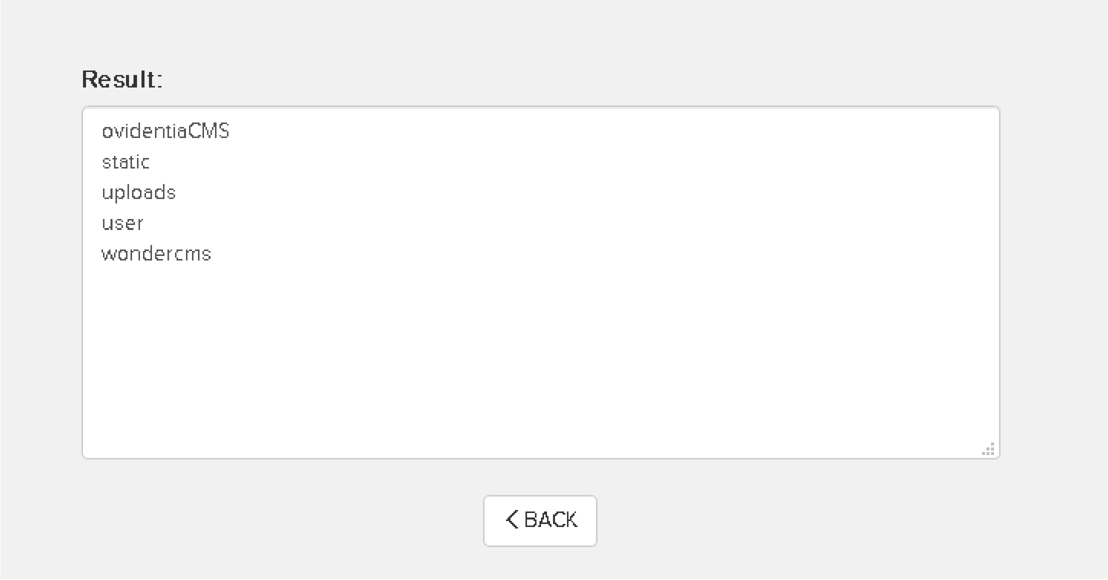
6.Command Execution Vulnerability

Proof of Concept (PoC)

When command ls is entered the following output is visible.



Command: ls



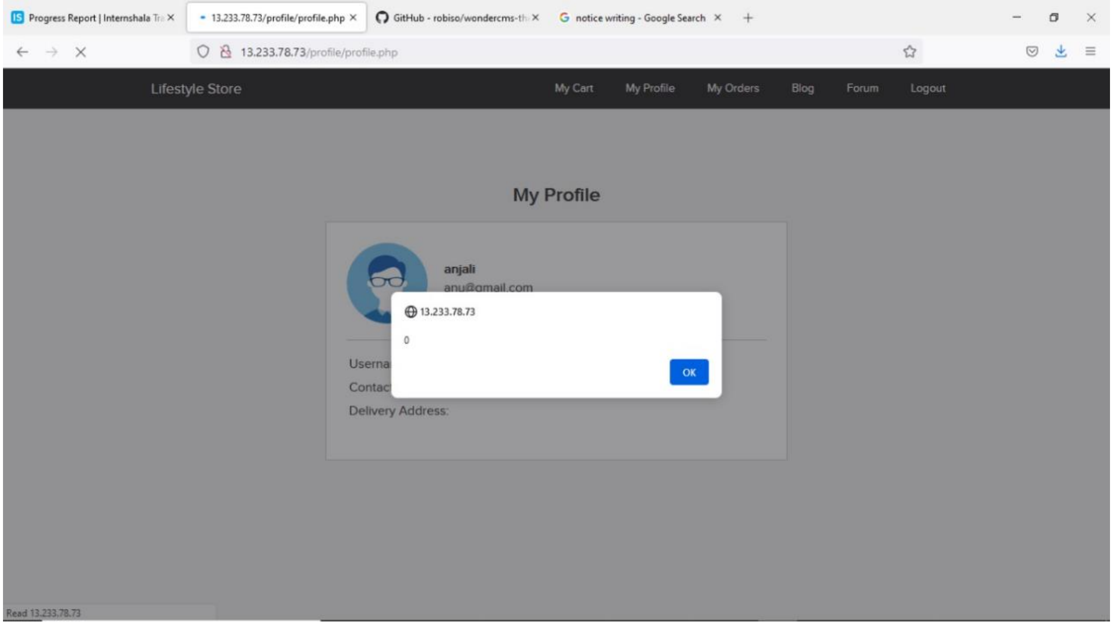
Result:

```
ovidentiaCMS
static
uploads
user
wondercms
```

7.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.

Proof of Concept (PoC)


Progress Report | Internshala Tr
13.233.78.73/profile/profile.php
GitHub - robiso/wondercms-th
notice writing - Google Search
13.233.78.73/profile/profile.php
Lifestyle Store
My Cart
My Profile
My Orders
Blog
Forum
Logout
OK
Read 13.233.78.73

My Profile

anjali
anu@gmail.com

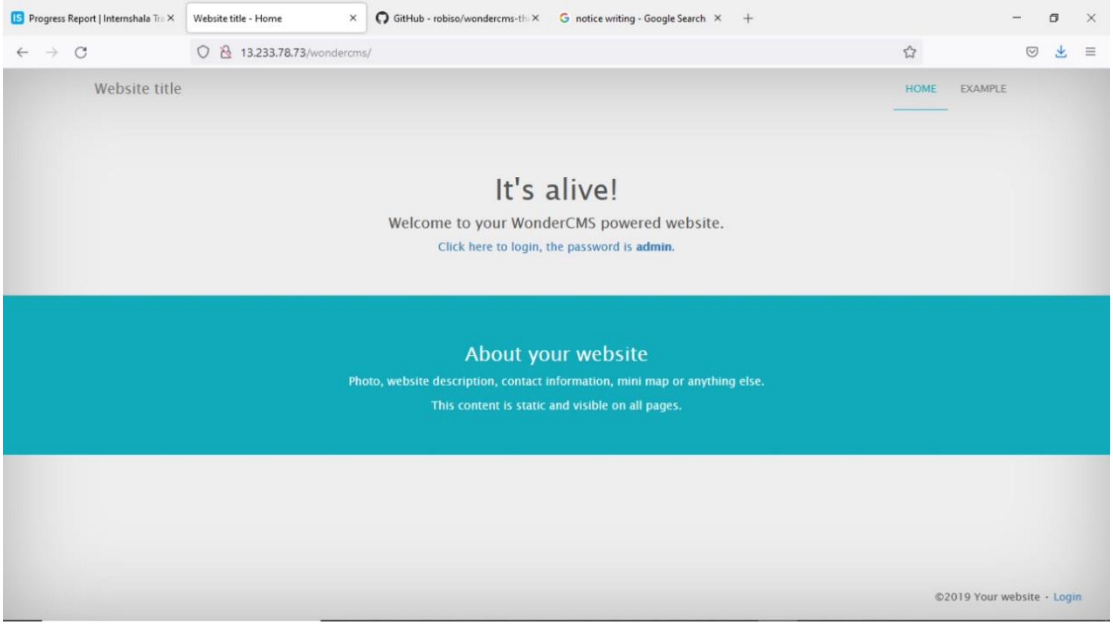
13.233.78.73

0

Userna
Contac
Delivery Address:

8.Crypto Configuration Flaws

Proof of Concept (PoC)


Progress Report | Internshala Tr
Website title - Home
GitHub - robiso/wondercms-th
notice writing - Google Search
13.233.78.73/wondercms/
Website title
HOME
EXAMPLE
Login

It's alive!

Welcome to your WonderCMS powered website.

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

About your website

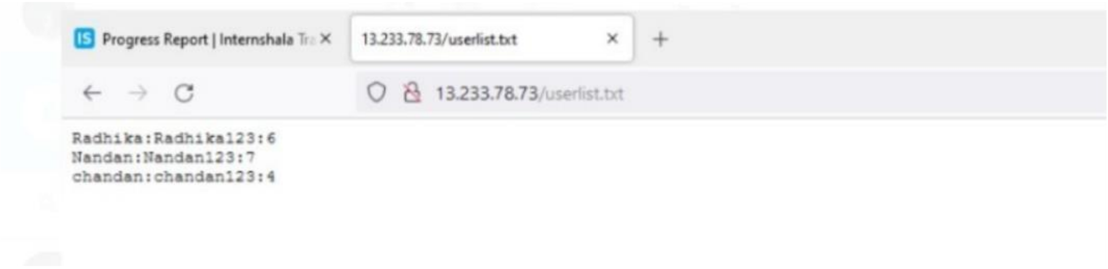
Photo, website description, contact information, mini map or anything else.

This content is static and visible on all pages.

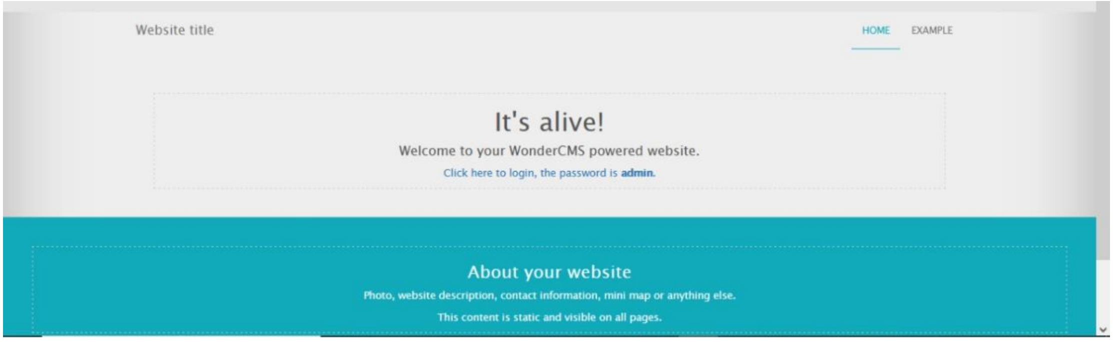
©2019 Your website · Login

9. Common Passwords

Proof of Concept (PoC)


Progress Report | Internshala Tr
13.233.78.73/userlist.txt
13.233.78.73/userlist.txt

```
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**.

About your website

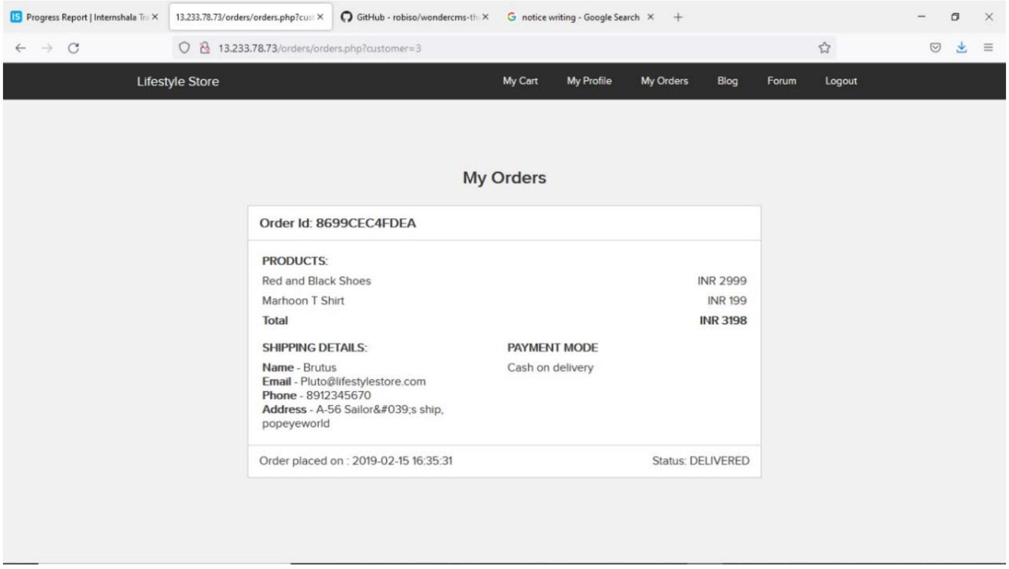
Photo, website description, contact information, mini map or anything else.

This content is static and visible on all pages.

10.Unauthorised availability of Details

Proof of Concept (PoC)

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


Progress Report | Internshala Tr
13.233.78.73/orders/orders.php?cus
GitHub - robiso/wondercms-th
notice writing - Google Search
13.233.78.73/orders/orders.php?customer=3
Lifestyle Store
My Cart
My Profile
My Orders
Blog
Forum
Logout

My Orders

Order Id: 8699CEC4FDEA

PRODUCTS:	
Red and Black Shoes	INR 2999
Marhoon T Shirt	INR 199
Total	**INR 3198**

SHIPPING DETAILS:

Name - Brutus
Email - Pluto@lifestylestore.com
Phone - 8912345670
Address - A-56 Sailor&#039;s ship, popeyeworld

PAYMENT MODE

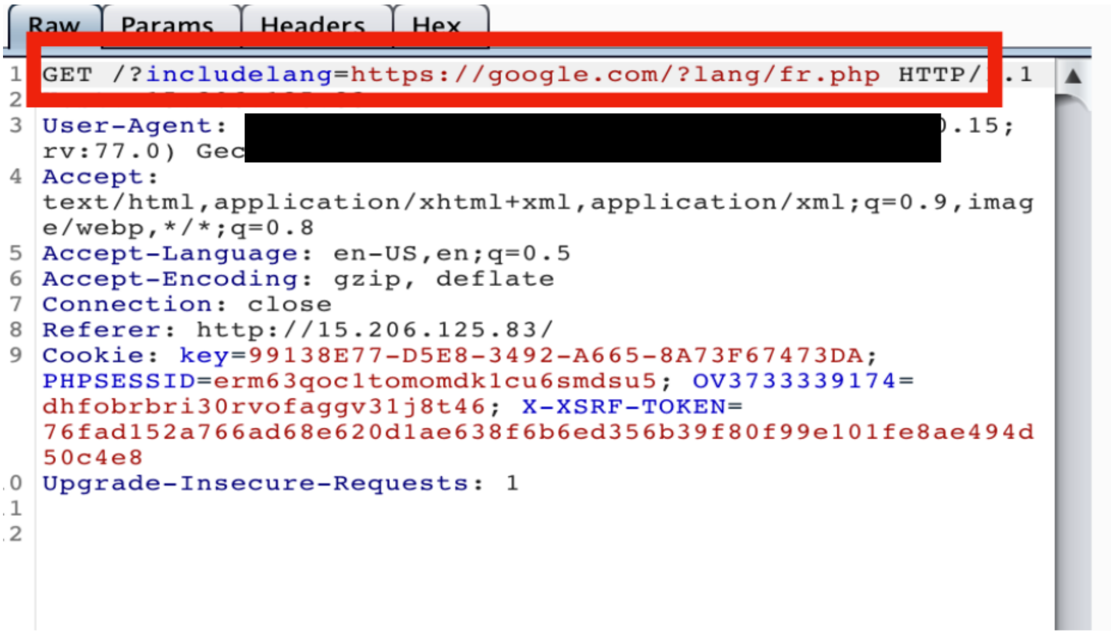
Cash on delivery

Order placed on : 2019-02-15 16:35:31

Status: DELIVERED

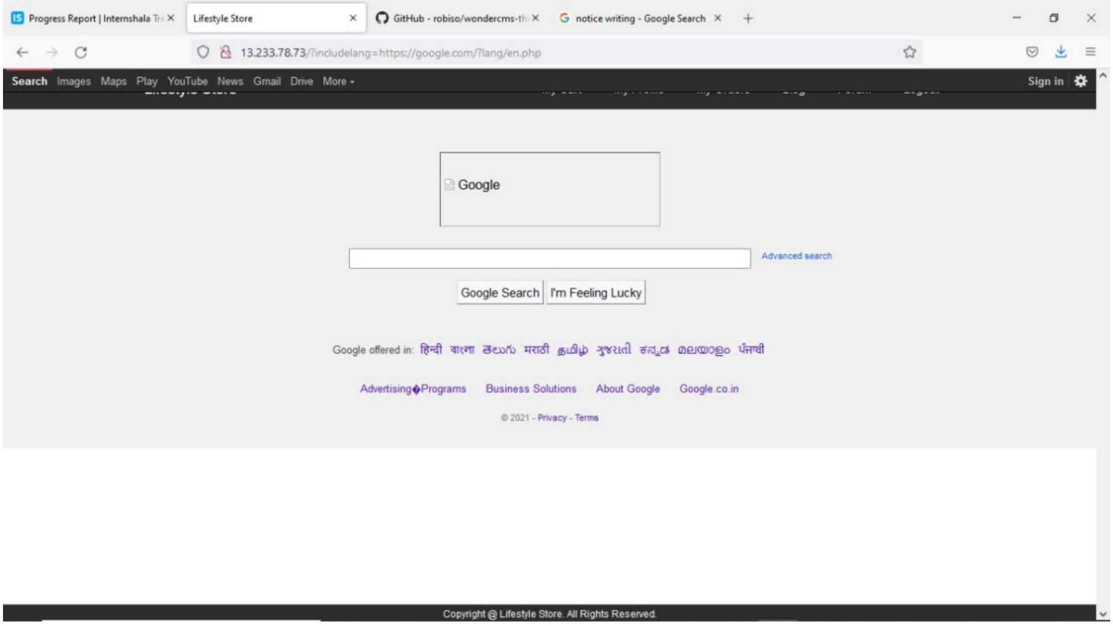
11.Open Redirection

Proof of Concept (PoC)



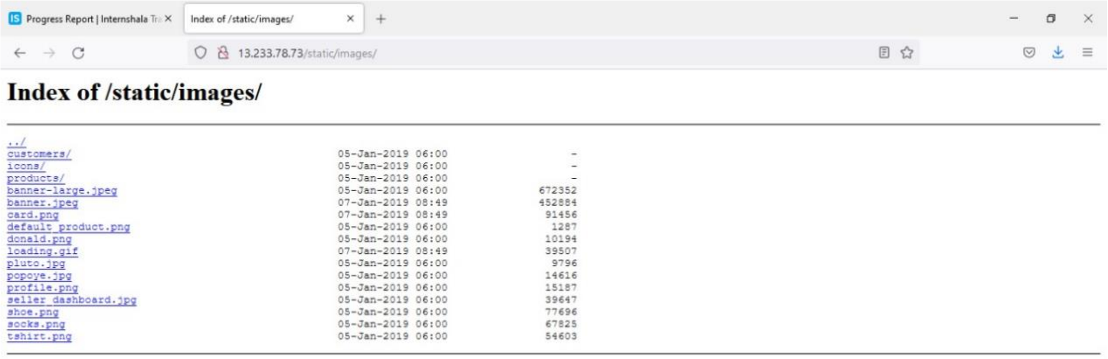
```
GET /?includelang=https://google.com/?lang/fr.php HTTP/1.1

User-Agent: [redacted].15;
rv:77.0) Gec
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://15.206.125.83/
Cookie: key=99138E77-D5E8-3492-A665-8A73F67473DA;
PHPSESSID=erm63qoc1tomomdk1cu6smdsu5; OV3733339174=
dhfobrbri30rvofaggv31j8t46; X-XSRF-TOKEN=
76fad152a766ad68e620d1ae638f6b6ed356b39f80f99e101fe8ae494d
50c4e8
Upgrade-Insecure-Requests: 1
```


Progress Report | Internshala Tr
Lifestyle Store
GitHub - robiso/wondercms-th
notice writing - Google Search
13.233.78.73/?includelang=https://google.com/?lang/en.php
Search
Images
Maps
Play
YouTube
News
Gmail
Drive
More
Sign in
Google
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
Copyright @ Lifestyle Store. All Rights Reserved.

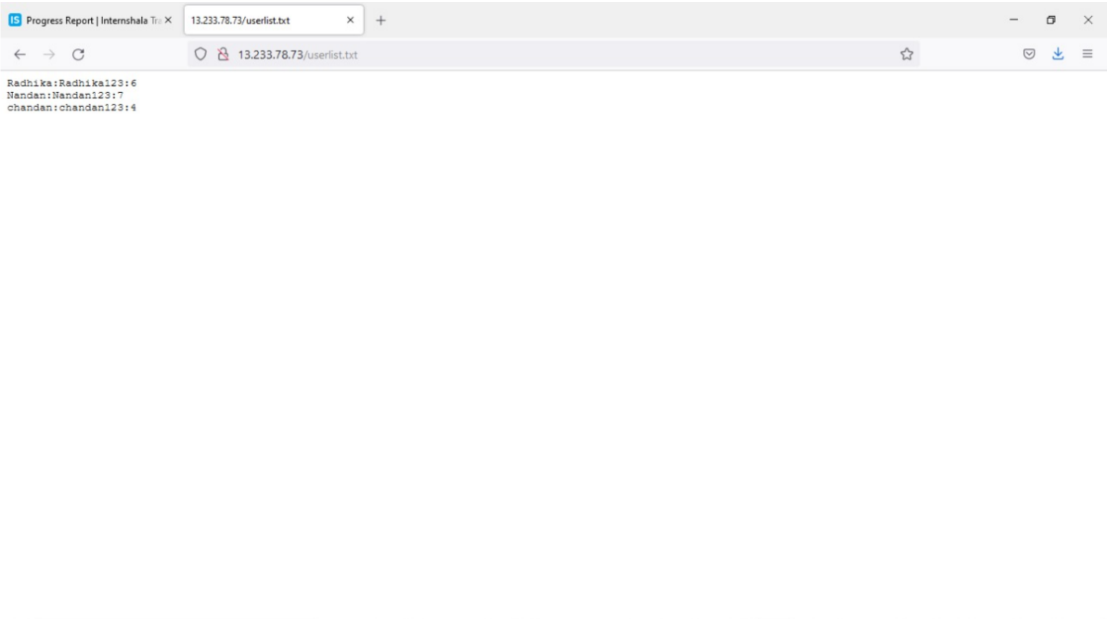
12.Information disclosure due to Default Pages

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
```

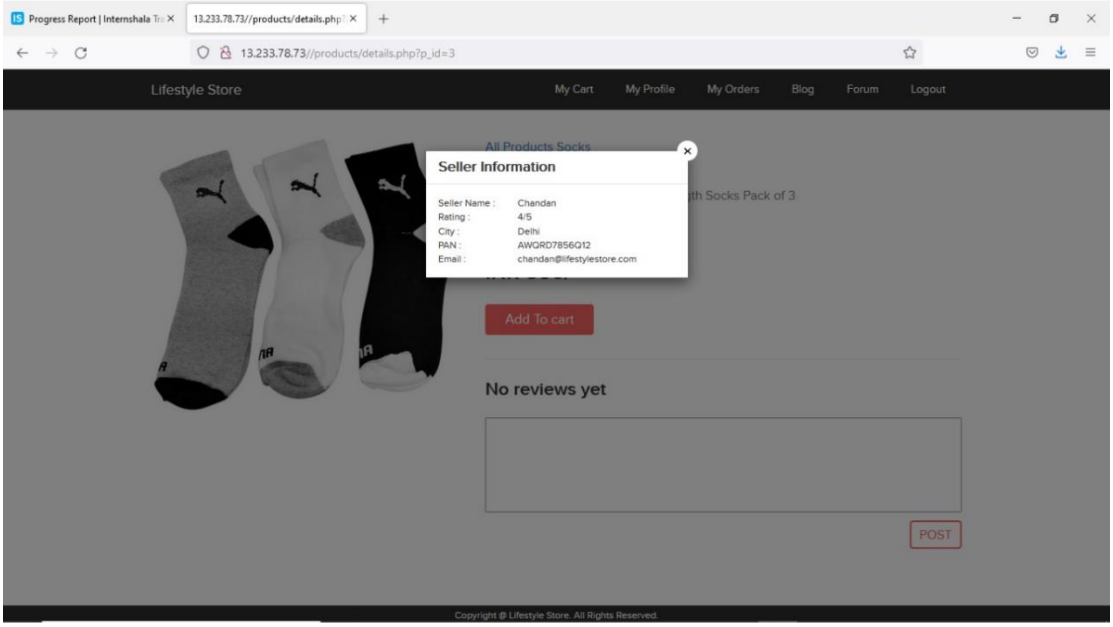

Progress Report | Internshala Tr
13.233.78.73/userlist.txt
13.233.78.73/userlist.txt

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

13. Unnecessary Details about Sellers

Proof of Concept (PoC)

•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.



Progress Report | Internshala Tr
13.233.78.73//products/details.php
13.233.78.73//products/details.php?p_id=3
Lifestyle Store
My Cart
My Profile
My Orders
Blog
Forum
Logout
All Products Socks
th Socks Pack of 3
Add To cart
POST
Copyright @ Lifestyle Store. All Rights Reserved.

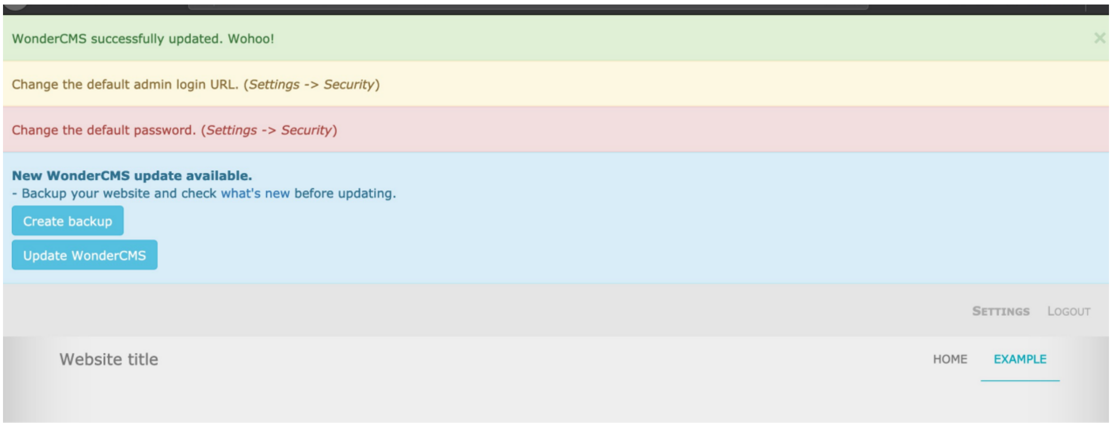
Seller Information

Seller Name :	Chandan
Rating :	4/5
City :	Delhi
PAN :	AWQRD7856Q12
Email :	chandan@lifestylestore.com

No reviews yet

14. Components with known vulnerabilities Proof of Concept (PoC)

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.



WonderCMS successfully updated. Wohoo!

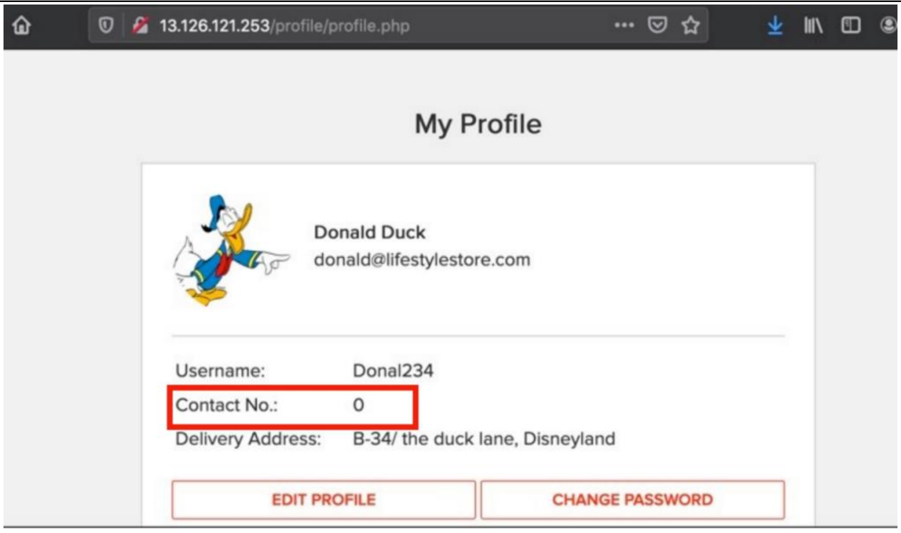
Change the default admin login URL. (*Settings -> Security*)

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

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

15.Improper Server Side and Client Side Filters Proof of Concept (PoC)

•But when we give a valid phone number on the client side, but intercept it through burpsuite and again give invalid number ,it gets accepted.



My Profile

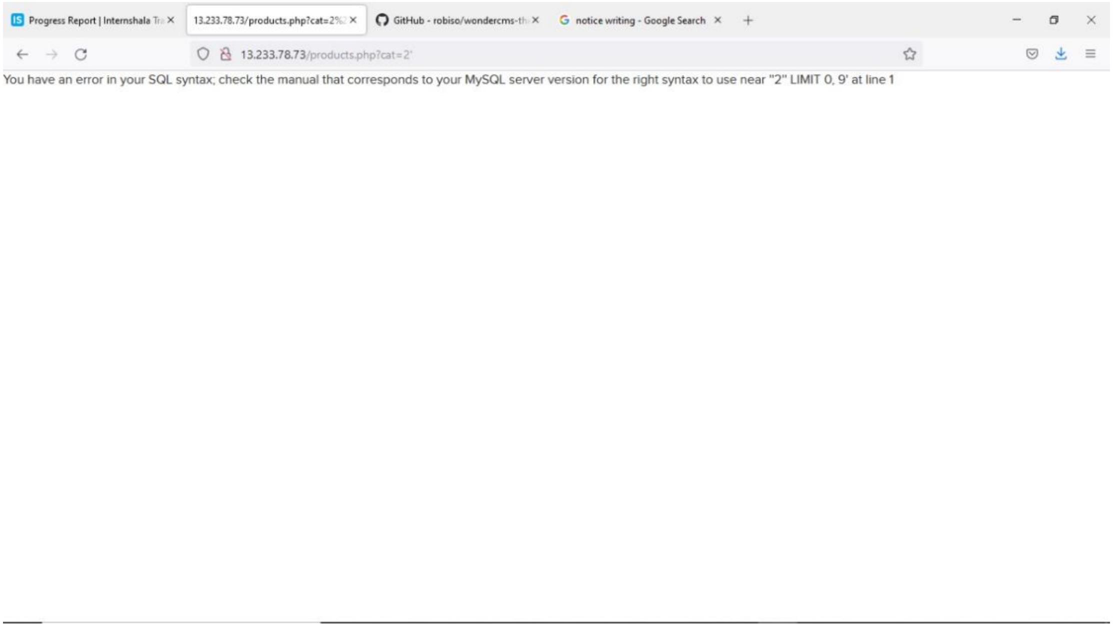
Donald Duck
donald@lifestylestore.com

Username: Donal234
Contact No.: 0
Delivery Address: B-34/ the duck lane, Disneyland

16.Default Error Display

Proof of Concept (PoC)

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


Progress Report | Internshala Tr
13.233.78.73/products.php?cat=2%
GitHub - robiso/wondercms-th
notice writing - Google Search
13.233.78.73/products.php?cat=2'

```
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 "2'' LIMIT 0, 9' at line 1
```

CONCLUSION

The whole world is moving towards the enhancement of technology, and more and more digitisation of the real world processes, with this the risk of security increases. This project and internship described the working of malicious hackers or crackers on one hand who tries to illegally break into the security and on the other hand white hat hackers or ethical hackers, who tries to maintain the security. As in the computer system, hacking plays a vital role as it deals with both sides of being good or bad.

Further, this tells about the types, working, and various attacks performed by the hackers. In conclusion, it must be said that
Ethical Hacking is a tool which when properly utilised can help in better understanding of the computer systems and improving the security techniques as well. By doing this internship and project I realised that no software is made with zero vulnerabilities

FUTURE SCOPES

Growing cases of computer hacking have forced renowned companies, financial institutions, and government organizations to recruit ethical hackers. Ethical hackers help these companies in finding out vulnerabilities and possible security leaks of their computer systems and also to protect them from any potential threat. So Ethical Hacking as a career has promising prospects in the near future.
According to a survey conducted by the International Data Corp, there is a demand for over 60,000 information security personnel worldwide. In India alone, the number is expected to grow by over 77,000 and 188,000 worldwide in the next few years.

Talented Ethical Hackers can look for making their career in some of the big names in the IT sector including Wipro, Dell, Reliance, Google, Accenture, IBM, and Infosys. In fact, business organisations need ethical hackers to keep their information protected. It is with this increasing demand that the ethical hacking salary in India is quite lucrative. But before taking up the profession, one must be aware that the position does not just require educational qualifications and technical skills but also honesty, strong ethics, and most importantly, a willingness to learn to combat challenges.

BIBLIOGRAPHY

REFERENCES

https://www.researchgate.net/publication/316431977_Ethical_Hacking_and_Hacking_Attacks

https://www.cromacampus.com/blogs/future-scope-of-ethical-hacking/

https://www.owasp.org/index.php/Unrestricted_File_Upload

https://www.opswat.com/blog/file-upload-protection-best-practices

https://owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-%20AUTHN-009)

https://www.owasp.org/index.php/Default_Passwords

https://www.us-cert.gov/ncas/alerts/TA13-175A

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

https://owasp.org/index.php/Improper_Error_Handling

https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/

https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/information-disclosure-phpinfo/

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

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

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)

BIO-DATA

NAME:	ANJALI VIDYA SAGAR
EDUCATION QUALIFICATION :	BTECH (ECE)
DATE OF BIRTH:	14/10/2001
LANGUAGE KNOWN:	ENGLISH/HINDI
CORRESPONDENCE ADDRESS:	HNO.50 SAVITRI NAGAR NEW DELHI 110017
MOBILE NO. :	9990865489
EMAIL ADDRESS:	anjalividyasagar9625@gmail.com

THANK YOU