# 6COSC019W – Cyber Security

**BussinessReadyFinance.com**

**Student: Shanmugaratnam Mohanaranjan**
**(W1870584/18705841)**

**Module Leader : Dr Ayman EI Hajjar**

## BSc (Hons) Computer Science degree

## BEng Software Engineering degree

## at the University of Westminster.

**School of Computer Science & Engineering**
**University of Westminster**

**Date : Thursday 09 May 2024 at 1.00 pm**

# Scenario:

My group has been asked to carry out a complete penetration test for BusinessReadyFinance.com, a recently launched website that offers small and medium-sized businesses (SMEs) all-inclusive financial solutions. With over 150 workers, this fictitious business serves both private and corporate clients worldwide on a medium-sized basis. To provide customized financial services, BusinessReadyFinance.com gathers a variety of data, including sensitive financial information and internal personnel data for administrative needs. The platform provides services including financial planning, budgeting, investment guidance, and business loan facilitation to a wide range of SMEs. The platform's secure systems handle all money transactions and data processing.

Client-side exploits like Man-in-the-Middle attacks and social engineering must consider the risk of compromising user credentials and financial information. Finally, strategies to reduce denial of service attacks and guarantee the deployment of robust security measures, including intrusion detection and prevention systems, are examined. A comprehensive penetration testing report specific to BusinessReadyFinance.com's operations and potential vulnerabilities is ensured with this customised technique.

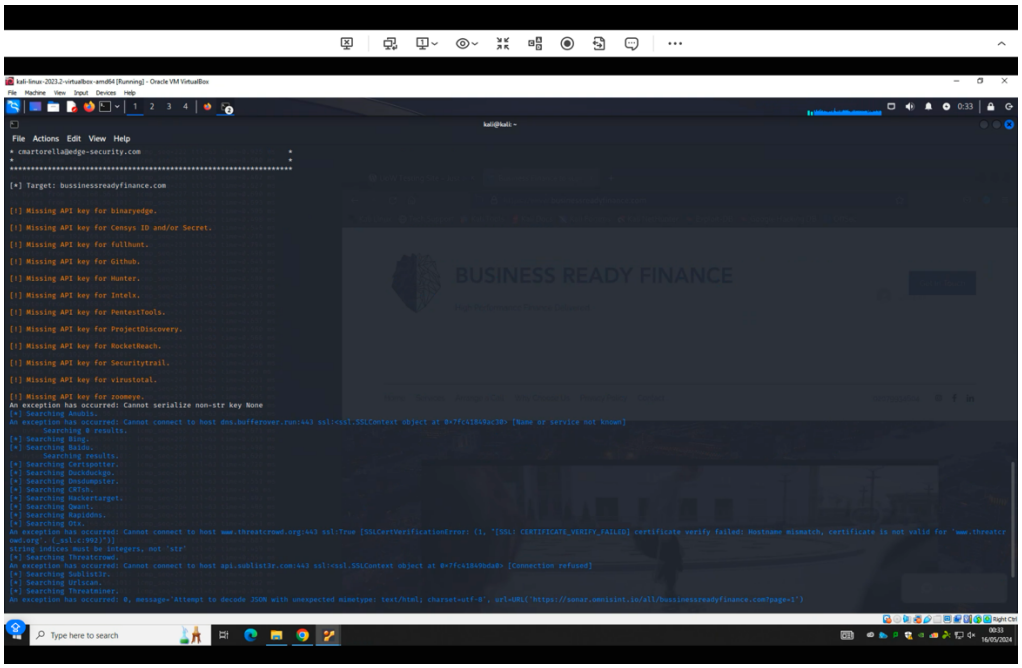
One of the most important factors to consider while using client-side exploits like social engineering and Man in the Middle attacks is the possibility of compromising user credentials and financial data. To sum up, strategies to prevent denial of service attacks and make sure that robust security measures, including intrusion detection and prevention systems, are put in place are examined. A comprehensive penetration testing report specific to the operations of BusinessReadyFinance.com and its possible vulnerabilities is ensured with this tailored technique.

# Findings of different penetration testing:

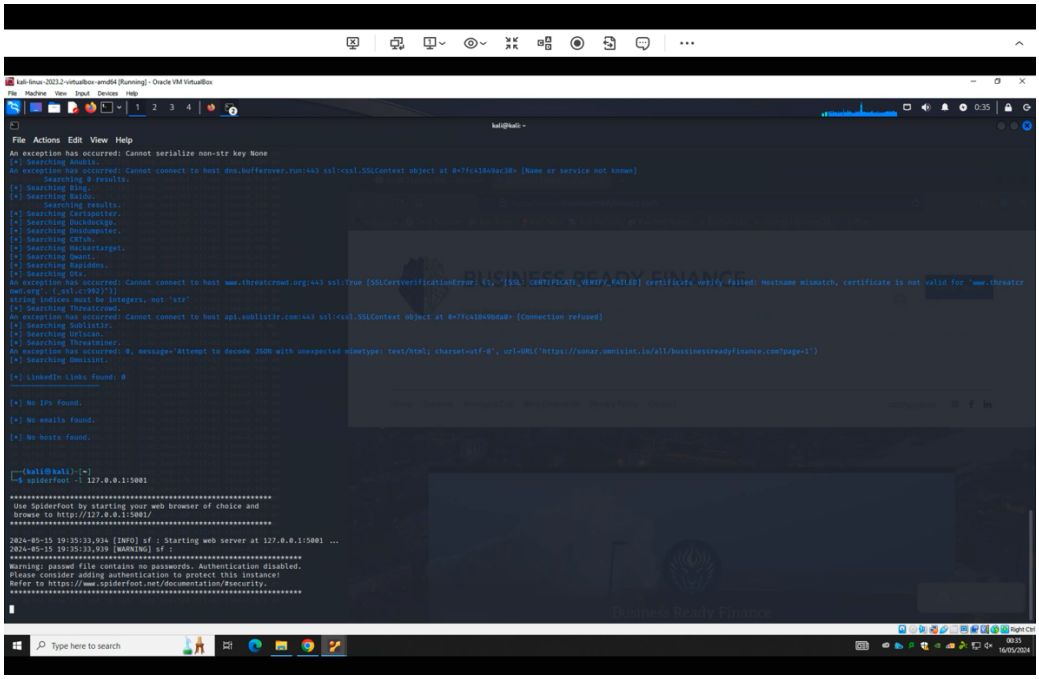
## A) Information gathering and scanning:

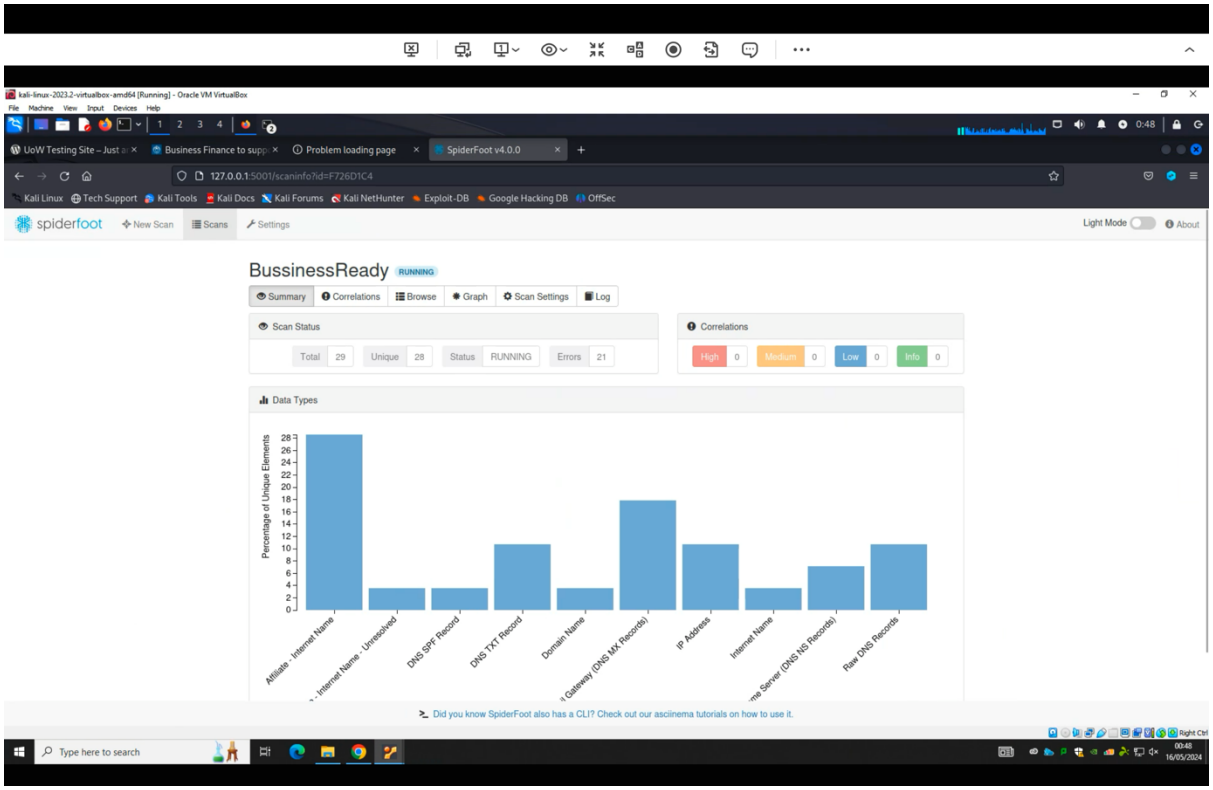
**OSNIT Activities:** GadgetSphere.at is the web application's address. I'll be utilising the following resources to collect information:

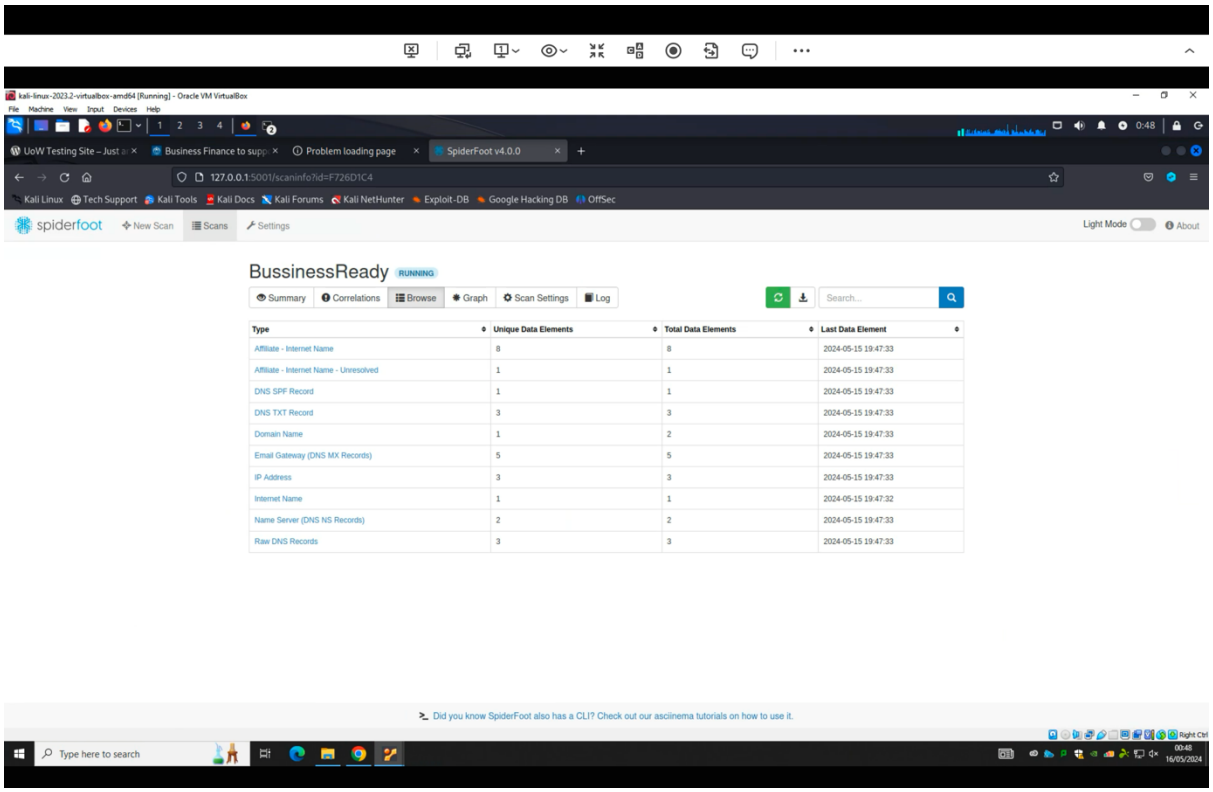
### The Harvester:




### Spiderfoot:




kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
SpiderFoot v4.0.0
127.0.0.1:5001/scaninfo?id=F726D1C4
spiderfoot
New Scan
Scans
Settings
Light Mode
About
BussinessReady
RUNNING
Summary
Correlations
Browse
Graph
Scan Settings
Log
Scan Status
Total 29
Unique 28
Status RUNNING
Errors 21
Correlations
High 0
Medium 0
Low 0
Info 0
Data Types
Percentage of Unique Elements
Affiliate - Internet Name
Affiliate - Internet Name - Unresolved
DNS SPF Record
DNS TXT Record
Domain Name
Email Gateway (DNS MX Records)
IP Address
Internet Name
Name Server (DNS NS Records)
Raw DNS Records
Did you know SpiderFoot also has a CLI? Check out our asciinema tutorials on how to use it.
Type here to search


kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
SpiderFoot v4.0.0
127.0.0.1:5001/scaninfo?id=F726D1C4
spiderfoot
New Scan
Scans
Settings
Light Mode
About
BussinessReady
RUNNING
Summary
Correlations
Browse
Graph
Scan Settings
Log
Search...
Type
Unique Data Elements
Total Data Elements
Last Data Element
Affiliate - Internet Name 8 8 2024-05-15 19:47:33
Affiliate - Internet Name - Unresolved 1 1 2024-05-15 19:47:33
DNS SPF Record 1 1 2024-05-15 19:47:33
DNS TXT Record 3 3 2024-05-15 19:47:33
Domain Name 1 2 2024-05-15 19:47:33
Email Gateway (DNS MX Records) 5 5 2024-05-15 19:47:33
IP Address 3 3 2024-05-15 19:47:33
Internet Name 1 1 2024-05-15 19:47:32
Name Server (DNS NS Records) 2 2 2024-05-15 19:47:33
Raw DNS Records 3 3 2024-05-15 19:47:33
Did you know SpiderFoot also has a CLI? Check out our asciinema tutorials on how to use it.
Type here to search

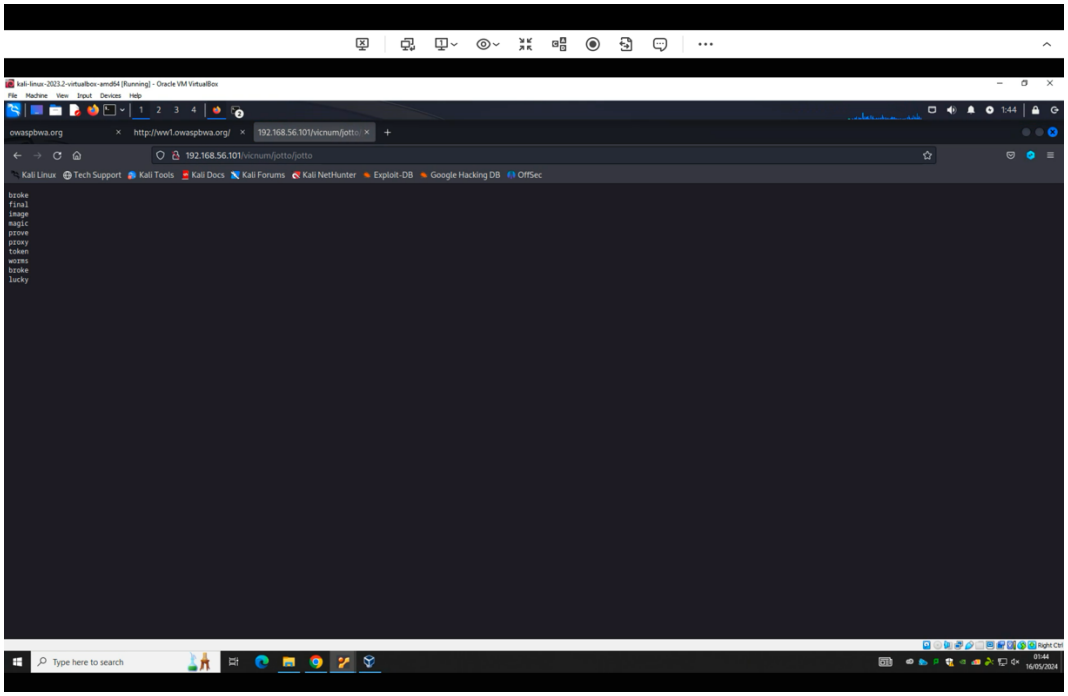
## OSINT for Penetration Testing:

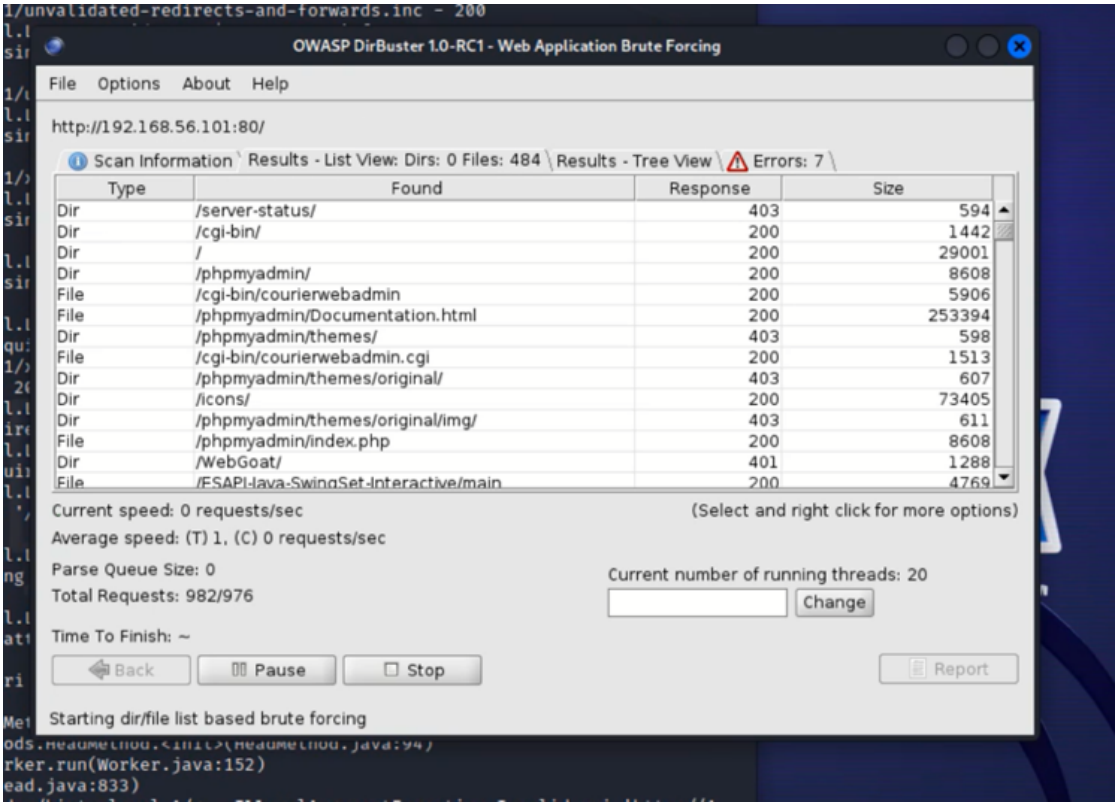
Because it is inexpensive, easy to use, and offers a wealth of information, Open Source Intelligence (OSINT) is a crucial first step in penetration testing. Investigations using open-source intelligence (OSINT) may yield important details about possible cyberthreats, including threat actors' possible tactics, methods, and approaches. This can help businesses thwart attacks by identifying vulnerabilities and implementing customised security measures. This easy process helps find potential access points and weaknesses, which facilitates the construction of more targeted attacks. Additionally, by enabling testers to move quickly and effectively to additional analysis and exploitation based on trustworthy intelligence, OSINT aids in the strategic design of social engineering methods and compliance checks, which speeds up the penetration process.

## Scenario

The Harvester and Spiderfoot may reveal sensitive information that could result in significant harm, according to data gathered from penetration testing with the use of OSINT tools. I discovered 3 IP addresses that might reveal network infrastructure, like weaker security zones or exposed access points. An exposed email address, like escape@bussinessreadyfinance.com, could lead to focused phishing attempts that could jeopardise customer and employee information. The thorough indexing of related URLs and in-depth web content suggests a substantial digital footprint that could be misused if vulnerabilities in out-of-date content or third-party scripts are found. Moreover, facts about DNS configurations, including TXT and SPF records, may allow for communication eavesdropping or domain hijacking, and SSL certificate information may expose encryption vulnerabilities that could be exploited to compromise security and data integrity.

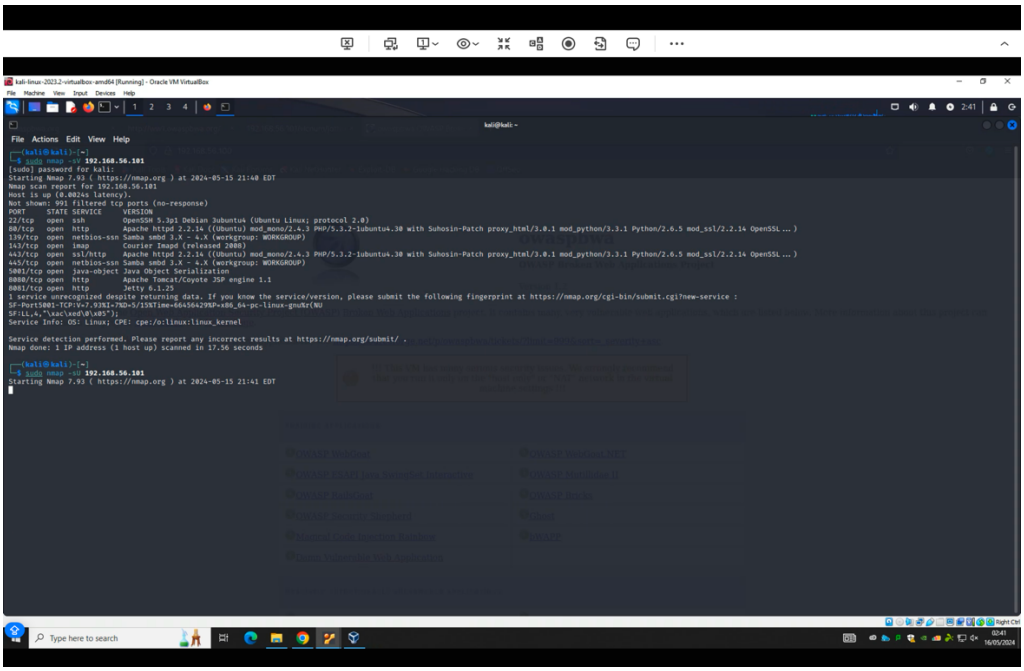
## Website Reconnaissance

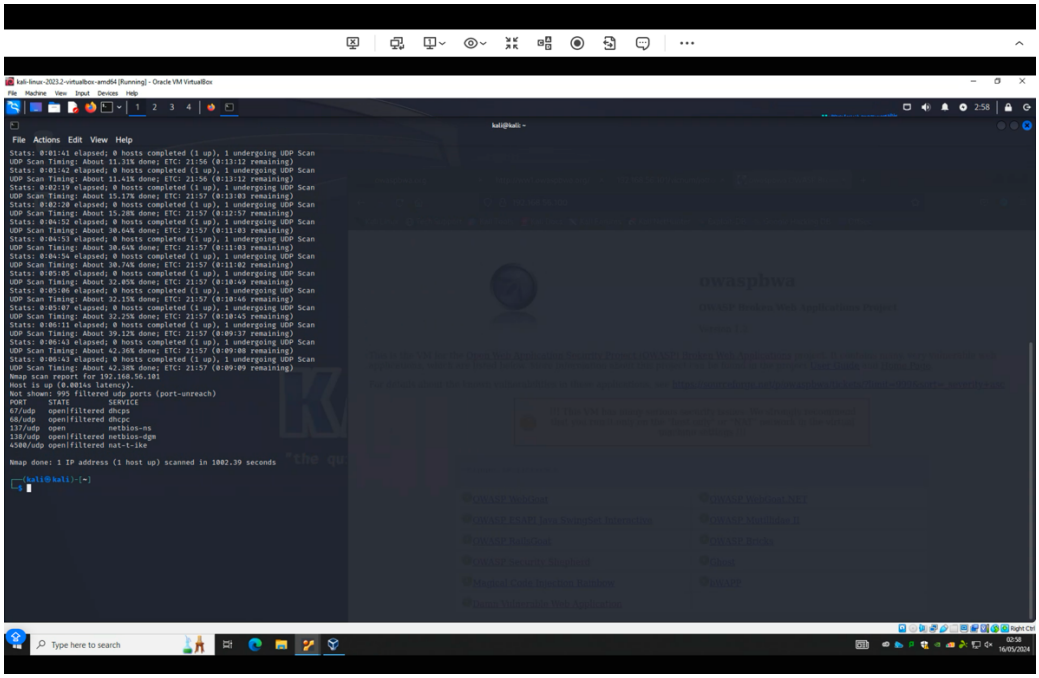





In my case, finding these directories may reveal administrator interface keys, user credentials, or API keys. An attacker may attempt to alter the website's content or reroute transactions using this sensitive data, which could lead to data breaches or financial losses.

**Port Scaning and Enumeration:**






Open Port and threats it can cause:

A network port that is open allows communication with the underlying server technology and accepts traffic via TCP or UDP. To host remote services that end users can access, open ports are necessary. Open ports don't always mean there's a security issue. It is contingent upon port setup, configuration, and security, nevertheless. Hackers could get access to your computer or network, take advantage of software flaws, and take control of the system if ports are not configured correctly.

**Scenario**

Secure Shell (SSH):

Open SSH can compromise system security by increasing attack surface and allowing brute force attacks. In an e-commerce website, attackers can access the server without authentication, potentially compromising customer and business data or disrupting operations. A brute force attack on the open port could lead to personal information, vehicle information, and website activity data.

HTTP:

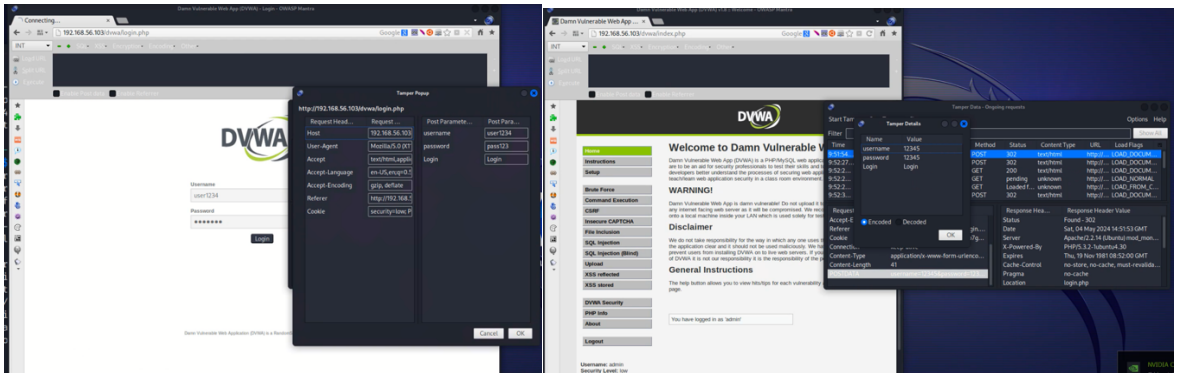
An outdated port poses a high security risk due to potential DOS attacks, affecting user access and content updates. Threats include cross-site scripting, DDoS attacks, SQL injection, and cross-site request forgeries. Attackers could exploit vulnerabilities to gain consumer information or disrupt website functionality.

HTTPS :

Exposure to open ports vulnerable to DDoS attacks, SQL injection, or cross-site scripting can lead to fraudulent transactions or client data breaches, affecting a business's standing and financial stability. The Dos vulnerability can cause unexpected traffic to the web server, causing poor performance for users.

## B) Server-Side Exploit:

### Data Tempering:



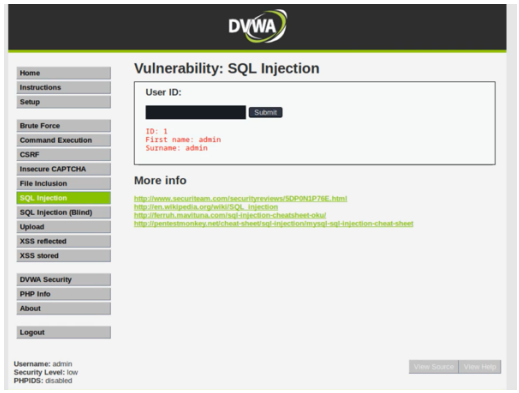
### Data Tampering Vulnerabilities:

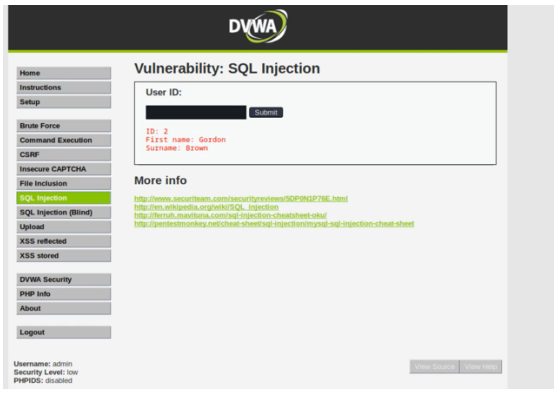
Data tampering is the deliberate or inadvertent insertion, modification, or alteration of data without authorization or proper validation. This affects all digital storage devices, databases, network connections, and software systems. Data tampering is also possible on systems that permit antiquated or insufficient security mechanisms, such as shared credentials or open network ports, weak passwords, and unencrypted data. The CIA trinity—confidentiality, user integrity, and availability—is broken by data tampering. User privacy and confidentiality are crucial to guard against unwanted access attempts. The availability of information refers to its regular and easy accessibility for authorised users, whereas integrity refers to the requirement that user data not be changed by unauthorised parties, such as in a data breach.

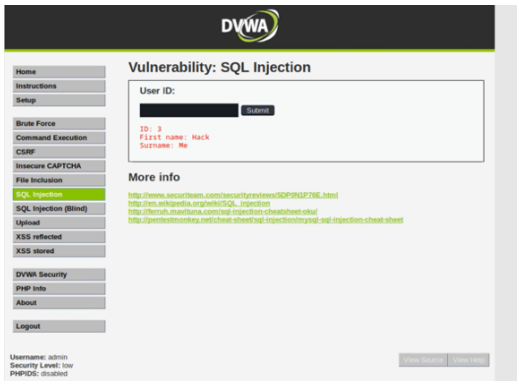
### Scenario

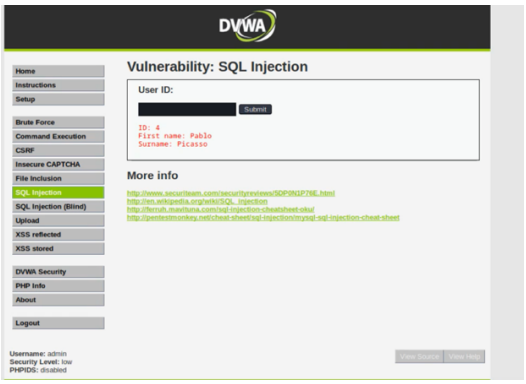
Given the nature of data, data tampering could be hazardous for BusinessReady Finance. Sensitive information that can be obtained by attackers includes login passwords, order history, and client information. They can alter or remove product descriptions, prices, or stock details, which could lead to prospective customers seeing erroneous specs. If customers make purchases based on false information, the company can be in trouble financially and legally. Attackers can alter consumer reviews, harming businesses' reputations. Attackers can also alter customer information or steal login credentials to meddle with user accounts. This may result in unauthorised access to accounts, which may then cause fraud, data theft, or alterations to client profiles. Such lapses could erode customer confidence and harm the company's reputation. Attackers might also alter company documents.

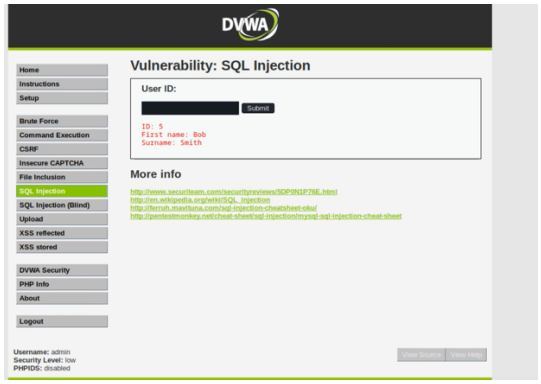
## SQL Injection:





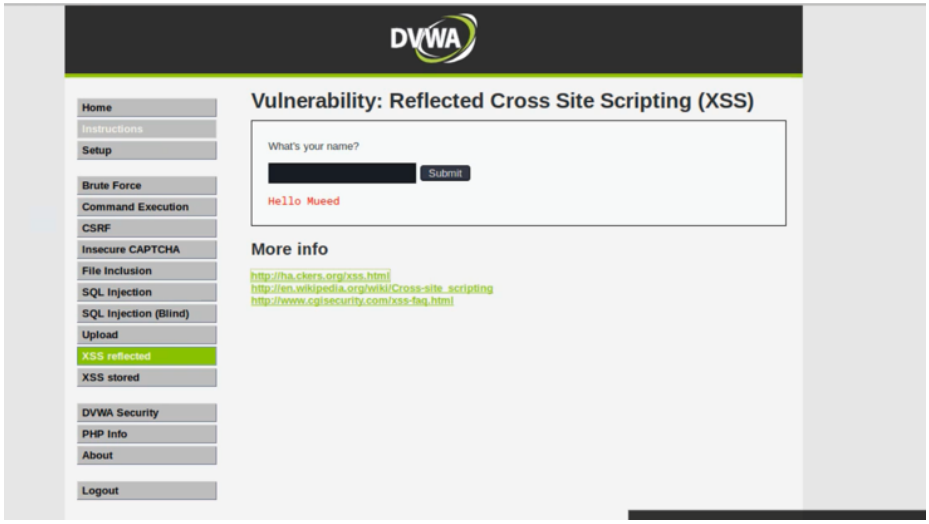
## SQL Injection Vulnerability:

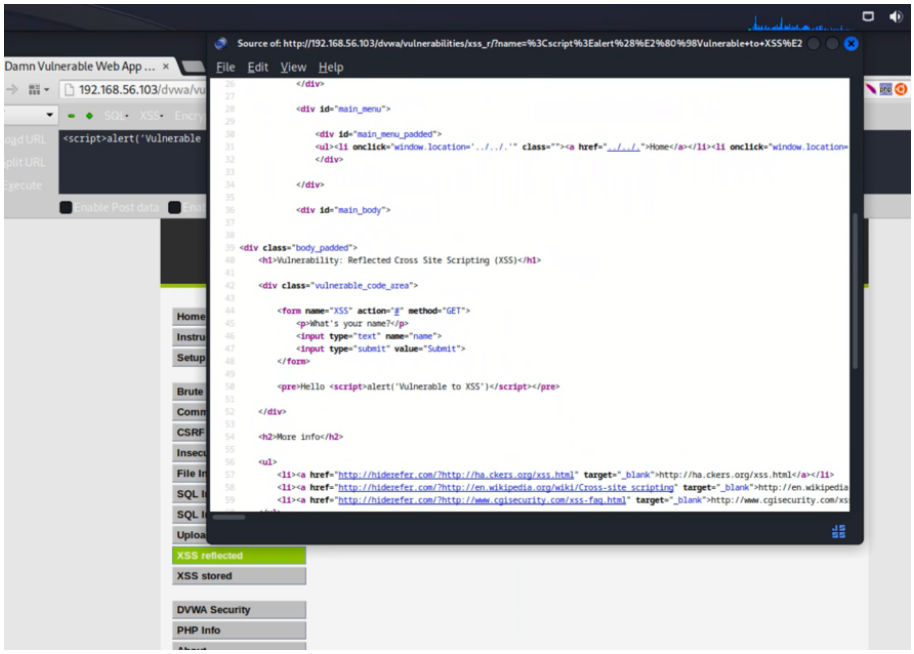
A online security flaw known as SQL injection (SQLi) enables an attacker to tamper with database queries made by an application. This gives an attacker access to data that they otherwise wouldn't have the ability to study. This could include any other data that the programme has access to or data that belongs to other users. The majority of the time, an attacker can alter or erase this data, changing the behaviour or content of the programme over time. The CIA trinity of secrecy, integrity, and availability is likewise broken by SQL injection.

## Scenario

Attackers may be able to access sensitive data in the company's database using a SQL injection on the BusinessReady Finance website. In addition to login passwords for staff members, administrators, and customers, this data may include customer names, addresses, payment information, and order details. By utilising SQL injection to get administrator account access, attackers can take over the website's back-end systems, alter or remove data, and steal important user and corporate data. For BusinessReady Finance, this would be exceedingly risky and could lead to financial loss, legal issues, and harm to the company and its clients.

## XSS Scripting:



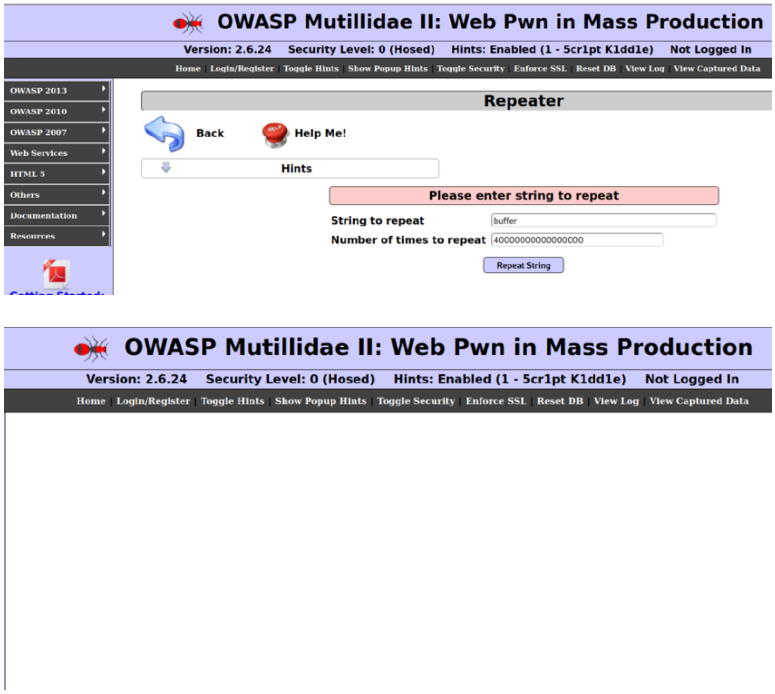
**Cross Site Scripting (XSS) vulnerability:**

Cross-Site Scripting (XSS) attacks are a sort of injection in which malicious scripts are inserted into otherwise legitimate and reliable websites. XSS attacks occur when an attacker uses a web application to transmit malicious code, typically in the form of a browser-side script, to a separate end user. Cross-Site Scripting violates the first two (and maybe all three) of security's fundamental CIA triad: confidentiality, integrity, and availability.

**Scenario**

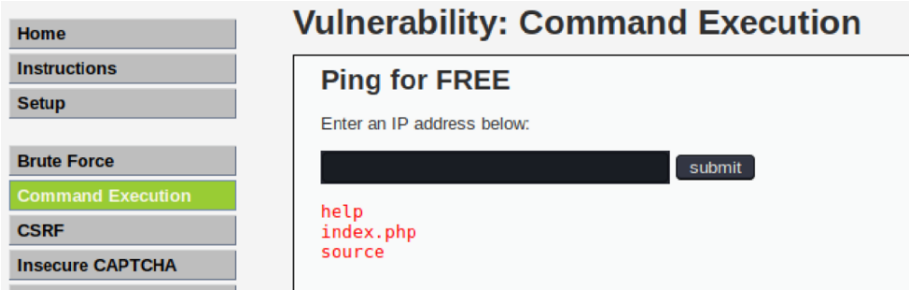
In my scenario, businessreadyfinance, attackers might be able to obtain sensitive customer data, including names, email addresses, shipping addresses, and payment details, by exploiting Cross-Site Scripting (XSS) vulnerabilities. This could result in identity theft, phishing scams, or financial fraud. In addition, they might steal login credentials and session tokens, giving unauthorised users access to user accounts and possibly leading to fraudulent transactions or data manipulation. Furthermore, vital firm information, including sales figures, inventory records, or internal communications, could be compromised by attackers, disrupting business operations.

**Other vulnerabilities:**





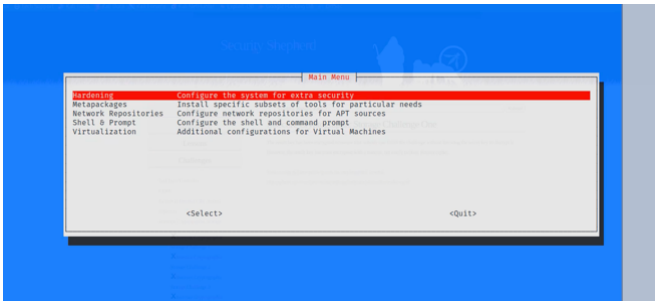


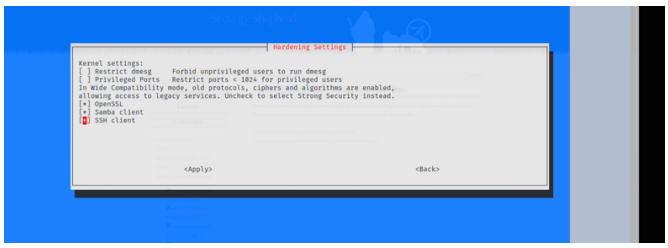


**Scenario**

The Repeater function in my example, an e-commerce website, puts integrity and availability at risk from possible buffer overflows that could contaminate data or cause a system crash. The vulnerability related to Command Execution poses a threat to confidentiality as it may reveal sensitive data, integrity as it permits unauthorised manipulation of data, and availability as it permits disruptive instructions that have the potential to take the system offline.

## Cryptanalysis attack




```
┌──(kali㉿kali)-[~]
└─$ hydra 192.168.56.101 ssh -L user.txt -P pass.txt -t 4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-06 09:10:22
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.56.101:22/
[22][ssh] host: 192.168.56.101   login: root   password: owaspbwa
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-06 09:10:22
```

```
┌──(kali㉿kali)-[~]
└─$ hydra 192.168.56.101 http-form-post "/dvwa/login.php:username=^USER^&passwrod=^
PASS^&Login=Login:login.php" -L users.txt -P pass.txt -e ns -u -t 2 -w 30 -o myresu
lts.txt
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in milit
ary or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-06 09:27:43
[DATA] max 2 tasks per 1 server, overall 2 tasks, 3 login tries (l:1/p:3), ~2 tries
 per task
[DATA] attacking http-post-form://192.168.56.101:80/dvwa/login.php:username=^USER^&
passwrod=^PASS^&Login=Login:login.php

1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-06 09:27:44
```

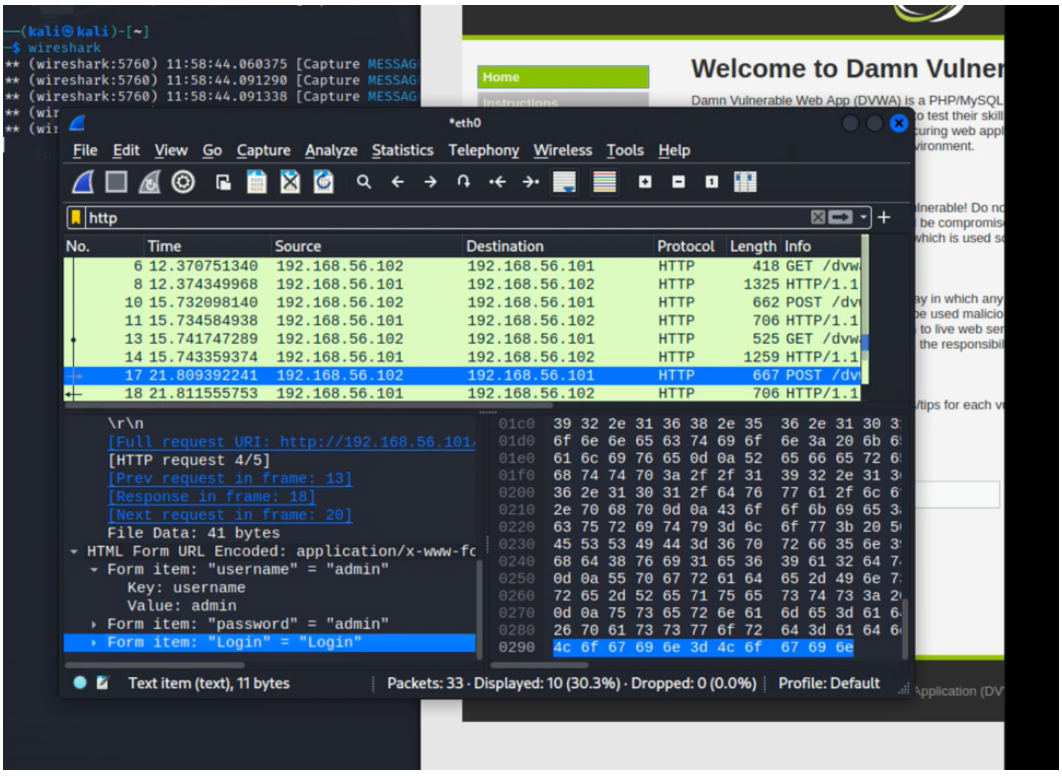
A cryptanalysis attack attempts to decipher or gain unauthorized access to encrypted data, compromising the secrecy of the information.

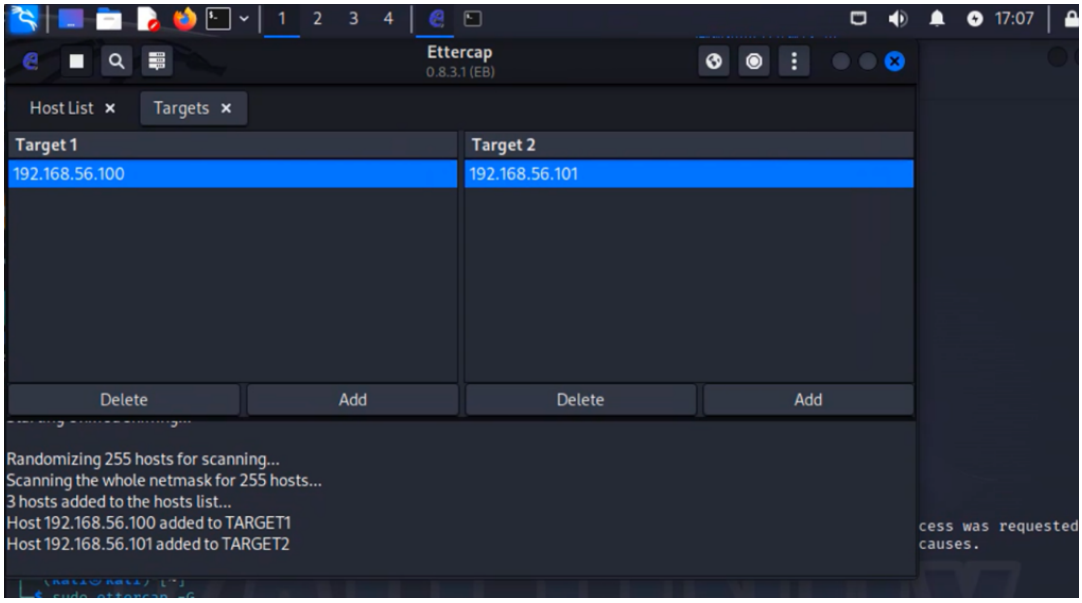
### Scenario

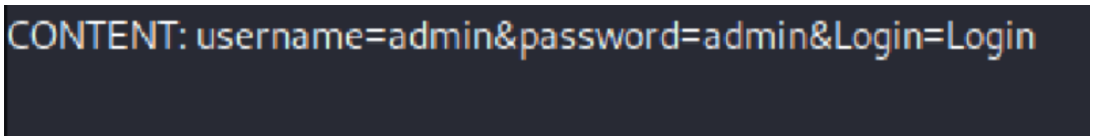
The primary goal of attackers employing brute force techniques with Hydra on my scene, the BusinessReady Finance website, is direct access via SSH and HTTP forms. However, consideration of cryptanalysis is also necessary. This technique, which focuses on decrypting encrypted data without the encryption key, has the potential to expose users' sensitive or private information if it is not well protected. For a thorough security evaluation, ensure that robust encryption methods like AES and RSA are utilised. You should also verify that installations are free of any vulnerabilities that could lead to cryptanalysis.

## C) Client-side exploit:

### Man in the Middle:



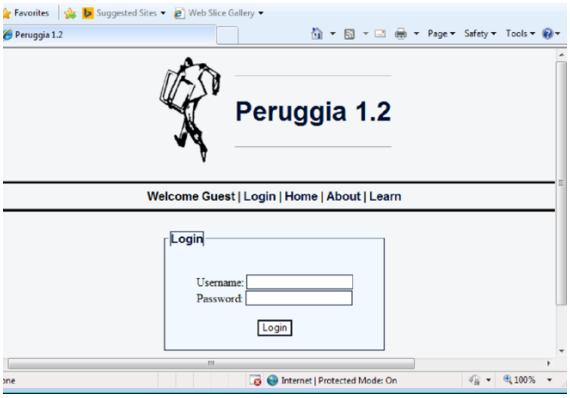


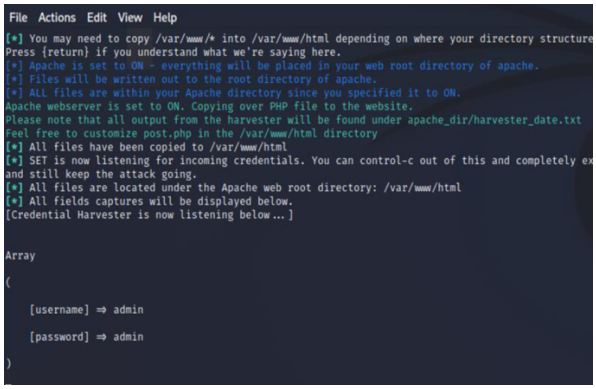




**Scenario**

A Man-in-the-Middle (MiTM) attack poses a significant risk since it gives hackers access to private information including customer login credentials, payment details, and internal conversations. The attackers may take advantage of weak apps to obtain usernames and passwords, which would enable them to access client accounts without authorization, steal identities, or carry out fraudulent transactions. All of these actions might seriously undermine customer confidence and result in financial loss or legal ramifications. Intercepted internal communications may also jeopardise important business information or cause operational disruptions, which could hurt the company's brand or put it at a competitive disadvantage. The confidentiality, integrity, and availability of the business's online services and communications are all at risk from MiTM attacks, which highlights the necessity of robust security measures to thwart these threats.

**Social Engineering:**

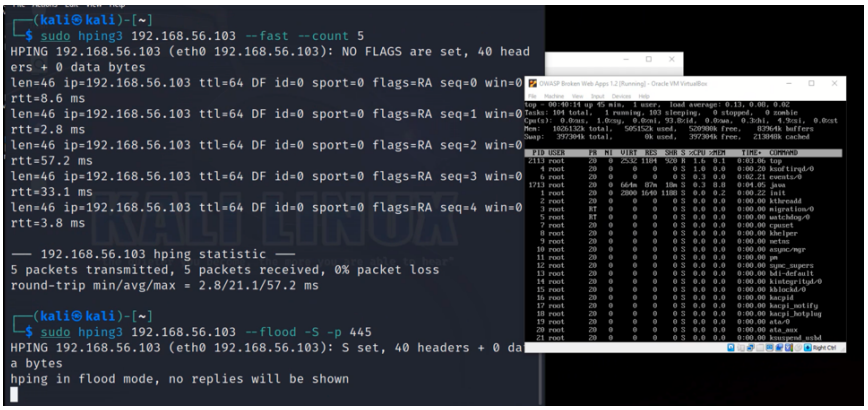


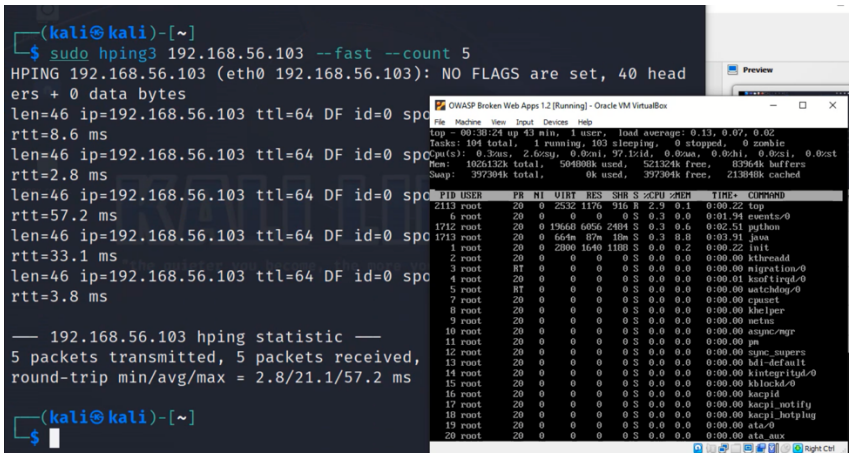



**Scenario**

Because social engineering assaults trick customers or staff into divulging private information or acting in an undesired way, they pose a serious risk. Similar strategies can be used by attackers to obtain customer data, staff passwords, and important company information. These attacks have the potential to cause financial losses or legal issues, as well as illicit access, identity theft, fraudulent transactions, or operational issues. They could also seriously damage the reputation of businessreadyfinance. The confidentiality, integrity, and availability of the organization's systems and data are generally threatened by social engineering assaults, underscoring the necessity of rigorous security awareness training and preventative measures.

## Denial of Service Attacks (DoS):




Denial of Service Attack violates availability tenet from CIA triad.

**Scenario**

It may significantly affect the reputation and operations of businesses ready to financing. The unavailability of the company's website, which enables visitors to peruse and buy environmentally friendly home design products, could depress prospective clients and lead to lost sales. Employees use the online programme to keep track of customer questions and product listings; a denial-of-service attack could disrupt these business operations, leading to decreased revenue and productivity. This kind of assault may also reveal vulnerabilities that expose customer data, including payment and personal information, resulting in data breaches and legal issues. It is imperative to employ robust security protocols, such as firewalls, intrusion detection systems, and redundancy plans, in order to mitigate potential risks and uphold operational resilience.

## E) Threats mitigation techniques & recommendations:

**Minimize the threats from Reconnaissance phase:**

We can limit information disclosure by deleting unnecessary data and using a properly configured robots.txt file, secure open ports by configuring firewalls and intrusion detection systems, and harden the web application by updating software and following best configuration practices in order to prevent or minimise the attacks caused by Web Reconnaissance. In addition, the company needs to protect input fields, use HTTPS to encrypt sensitive data, implement logging and monitoring, and have an incident response plan in place to handle any security breaches right away. These are the methods that could be applied to protect sensitive client information of Businessreadyfinance.

**Preventing information revealed during Port scanning and Enumeration:**

To stop Businessreadyfinance servers from providing excessive amounts of information during port scanning and enumeration, the organisation needs to implement many important security measures. These include setting up preventative systems to monitor for suspicious behaviour, blocking unused ports on firewalls, limiting access to trusted IP addresses, and disabling useless services to reduce attack surface. Companies should also use network address translation (NAT) to mask internal IP addresses, network segmentation to isolate essential systems, and banners and error messages to prevent data leaks. By keeping all ports closed until a specific sequence is "knocked," which hides crucial services and restricts access, port knocking can increase security.

**Protecting SQL Injection into Database:**

To safeguard a database from SQL injection attacks, system administrators, database administrators, and developers can implement several essential measures. It's critical that you maintain the most recent security patches installed on all online application components, such as web servers, database servers, plug-ins, frameworks, and libraries. When creating accounts that connect to SQL databases, it's also crucial to follow the least privilege principle. For example, if a website only needs to get content using SELECT queries, it shouldn't have access to INSERT, UPDATE, or DELETE functions. Database accounts shouldn't be shared between multiple web apps to lessen the impact of a potential compromise. It is essential to validate user-supplied data for expected data types, particularly for structured fields with drop-down options or radio buttons.

**Protecting Web application from Cross Scripting attacks:**

A web application should defend against cross-site scripting (XSS) assaults with a variety of strong security methods. Throughout development, a Security Development Lifecycle (SDL) can assist avoid coding errors and security vulnerabilities by treating all incoming data as untrusted. Since XSS can attack even authenticated users, this is crucial. Enforcing authenticated users to re-enter their login credentials before to accessing particular sites or services is one way that adopting a crossing boundaries policy stops XSS attackers from hijacking sessions. Additionally, a meta tag like prevents cross-site scripting assaults (XSS) by limiting the different types of script injection and specifying character encoding. Not to mention, employing a website vulnerability scanner could be useful in identifying security holes. particularly when using packages from third parties.

**Protecting Web application from Cryptanalysis attacks:**

Strong encryption methods, such RSA or ECC for asymmetric encryption and AES for symmetric encryption, are necessary to defend against cryptanalysis assaults. It is best to stay away from outdated or unreliable algorithms like DES and MD5. Proper key management requires using long enough keys and storing them securely in a hardware security module or key management service. Strong cypher suites combined with secure communication protocols like HTTPS are the best way to encrypt data while it's in transit.

**Preventing Man in the Middle Attack:**

Permit the use of virtual private networks (VPNs) by businesses. A virtual private network (VPN) can be used to secure sensitive data on a local area network. They create a subnet with key-based encryption to enable safe communication. In this manner, even if an attacker succeeds to connect to a shared network, he will be unable to decipher the conversation inside the VPN. HTTP can be used by security analysts to facilitate secure communication through the exchange of public-private keys. This stops any possible hacker from using the information they might be sniffing. Browser plugins can be installed to force searches to always utilise HTTPS.

**Preventing Social Engineering Attacks:**

Employers must place a high priority on threat identification, security policy enforcement, and employee training to stop social engineering attacks. Strong access control, two-factor authentication, and stringent password restrictions lessen the impact of compromised accounts. By safeguarding communication channels, verifying contact information, and guaranteeing timely action against potential assaults through intrusion detection system monitoring and incident response plans, sensitive information is secured.

**Preventing against DoS Attack:**

To defend their applications from Denial of Service (DoS) attacks, businesses can use firewalls to block traffic from specific IP addresses or ranges. Limiting traffic from IP addresses that are known to be harmful helps businesses defend their services from assaults. DDoS protection services are another option available to businesses; these services detect and thwart attacks before they reach the servers. By using sophisticated algorithms, these services identify and block fraudulent traffic, preventing unauthorised users from using the

application. Additionally, knowing the company's usual traffic patterns provides a baseline that helps identify anomalous activity that might be indicative of a denial-of-service assault.

**Difference Between Intrusion Detection System and Intrusion Prevention System: (IDS vs IPS):**

**Intrusion Detection System: (IDS)**

In order to identify security issues and possible threats, intrusion detection systems (IDS) monitor and analyse network traffic within the firm. Through proactive prevention of potential cybersecurity problems, these security solutions safeguard organisations. Host-based (HIDS) and network-based (NIDS) are the two main places for IDS network deployment. While NIDS systems monitor and safeguard entire company networks, HIDS is implemented at the endpoint level to protect individual devices from threats.

**Intrusion Detection System: (IPS)**

After identifying intrusions, intrusion prevention systems (IPS) take action to neutralise any threats they find.

**Differences:**

| IDS | IPS |
|---|---|
| IDS is a monitoring tool that looks at network packets and compares them to either a baseline created by machine learning or a database of known threat signatures. | Based on specified rule sets, IPS is a control-based solution that accepts or rejects network packets. |
| IDS notifies human security personnel when it finds evidence of a breach of the designated security policies, such as malware, ransomware, or port scanners. | IPS stops the flow of malicious communications when a threat is identified. |
| Adaptable | Less Adaptable |

**Scenario**

Because businessreadyfinance handles sensitive data, such as user personal information and payment details, I believe that intrusion prevention systems should be implemented in network architecture. My reasoning for this is that real-time protection is essential to preventing any breaches. The company's reputation and customer confidence would be safeguarded by an intrusion prevention system (IPS), which would offer proactive security against malicious activity by identifying threats before they may compromise critical data or disrupt operations.

**References and Bibliography:**


1. Chai, W. and Hashemi-Pour, C. (2023). *What is the CIA Triad? | Definition from TechTarget*. [online] WhatIs. Available at: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA#:~:text=The%20CIA%20triad%20refers%20to.

2. Einorytė, A. (2024). *What are open ports? Risks and security | NordVPN*. [online] nordvpn.com. Available at: https://nordvpn.com/blog/what-are-open-ports/#:~:text=effective%20data%20transmission.- [Accessed 4 May 2024].

3. Hernández, M. (2022). *Securing SSH on EC2: What are the real threats?* [online] Sysdig. Available at: https://sysdig.com/blog/aws-secure-ssh-ec2-threats/ [Accessed 4 May 2024].

4. OWASP (2020). *Cross Site Scripting (XSS) | OWASP*. [online] Owasp.org. Available at: https://owasp.org/www-community/attacks/xss/.

5. Palais, S. (2023). *OSINT 101: Understanding OSINT, its tools, benefits and risks*. [online] Yogosha. Available at: https://yogosha.com/blog/osint-open-source-intelligence/#:~:text=OSINT%20is%20generally%20used%20to [Accessed 5 May 2024].

6. portswigger.net. (n.d.). *What is SQL Injection? Tutorial & Examples | Web Security Academy*. [online] Available at: https://portswigger.net/web-security/sql-injection#:~:text=SQL%20injection%20(SQLi)%20is%20a.

7. Rapid7 (2023). *Man-in-the-Middle (MITM) Attacks: Techniques and Prevention*. [online] Rapid7. Available at: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/.

8. StickmanCyber Team (2021). *8 Ways Organisations Prevent Social Engineering Attacks*. [online] www.stickmancyber.com. Available at: https://www.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks.

9. UC Berkeley (2023). *How to Protect Against SQL Injection Attacks | Information Security Office*. [online] security.berkeley.edu. Available at:

https://security.berkeley.edu/education-awareness/how-protect-against-sql-injection-attacks.

10. Walkowski, D. (2020). *What Is Cross-Site Scripting?* [online] F5 Labs. Available at: https://www.f5.com/labs/learning-center/what-is-cross-site-scripting.