



SECURITY TESTING AND REPORT

Irish Bank Company



MAY 5, 2021

SURENDRA DURA
2020436@student.cct.ie

Table of Contents

Introduction:	2
TASK 1 Scanning:	2
TASK 2 Monitoring:	5
TASK 3 Gain Access:	6
TASK 4 Monitoring Distribution Systems:	12
TASK 5 Data Security:	15
References	16

Introduction:

The Irish bank want to make a security system in their bank and assign me as a project manager for this role. The security which we need for the company to be secure from the attacks are going to be listed in this document and I am also going to show the examples of the vulnerability system so that the IT manager and other newly hired developers and technical support staff get an idea to secure the system.

TASK 1 Scanning:

For the Scanning process, I am going to use a Kali Linux as a working system and the vulnerable system as a Metasploitable device. With the help of the ifconfig command in the Metasploitable(Metasploitable 2 Exploitability Guide | Metasploit Documentation, 2021) device, I can see the IP address of Metasploitable device which is 192.168.56.102. It helps us to scanning the Metasploitable device using the Nmap in the Kali Linux.

The three different options/switches to show differing results against Metasploitable are as follows:

1. -sS (TCP SYN scan):

From this -sS (*nmap(1) - Linux man page, 2021*) scanning, we can scan all the possible port and it give us details of all the open port in the Metasploitable device with the MAC address. With the help of the open port, we can attack the device. For example, HTTP is running in port 80 and MySQL is running in port 3306 which is shown below diagram.

```
suren@kali:~$ sudo nmap -sS 192.168.56.102
[sudo] password for suren:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 18:03 IST
Nmap scan report for 192.168.56.102
Host is up (0.0015s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D9:86:D2 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```

2. -O:

This scanner helps us to find out the Operating System details of the Metasploitable so that using google we can find out the weakness of that OS and attack the device easily. For example, in the below diagram we can see the OS details is Linux _kernel:2.6.

```
surenakali:~$ sudo nmap -O 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 19:28 IST
Nmap scan report for 192.168.56.102
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D9:86:D2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
```

3. -A -T4:

With the help of this command, we can scan the all the details of the Metasploitable device. Usually, -A help us to enable the OS and version detection, script scanning and traceroute and -T4 for the faster execution. This is a powerful command of the Nmap because it help us to find out almost all the details of the target device which was shown in the below diagrams.

```

arenekali:~$ nmap -A -i4 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 19:18 IST
Nmap scan report for 192.168.56.102
Host is up (0.0095s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.56.101
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-05-06T18:19:15+00:00; -2s from scanner time.
sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
53/tcp    open  domain         ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - linux
111/tcp   open  rpcbind        2 (RPC #100000)
|_rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 57478/tcp mountd
|_100005 1,2,3 60227/udp mountd
|_100021 1,3,4 44450/tcp nlockmgr
|_100021 1,3,4 57359/udp nlockmgr
|_100024 1 33635/tcp status
|_100024 1 54835/udp status
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login          Netkit rshd
514/tcp   open  shell          Netkit rshd
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
|_mysql-info:
|_Protocol: 10
|_Version: 5.0.51a-3ubuntu5
|_Thread ID: 13
|_Capabilities flags: 43564
|_Some Capabilities: Support41Auth, ConnectWithDatabase, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, LongColumn
Flag, SupportsCompression
|_Status: Autocommit
|_Salt: -Bn6kma-w[Ar=tU,x=bU
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2021-05-06T18:19:15+00:00; -2s from scanner time.
5900/tcp  open  vnc            VNC (protocol 3.3)
5900/tcp  open  vnc            VNC (protocol 3.3)
|_vnc-info:
|_Protocol version: 3.3
|_Security types:
|_VNC Authentication (2)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_clock-skew: mean: 59m58s, deviation: 2h00m01s, median: -2s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|_OS: Unix (Samba 3.0.20-Debian)
|_Computer name: metasploitable
|_NetBIOS computer name:
|_Domain name: localdomain
|_FQDN: metasploitable.localdomain
|_System time: 2021-05-06T14:19:07-04:00
|_smb-security-mode:
|_account-used: <blank>
|_authentication level: user
|_challenge response: supported
|_message signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.90 seconds

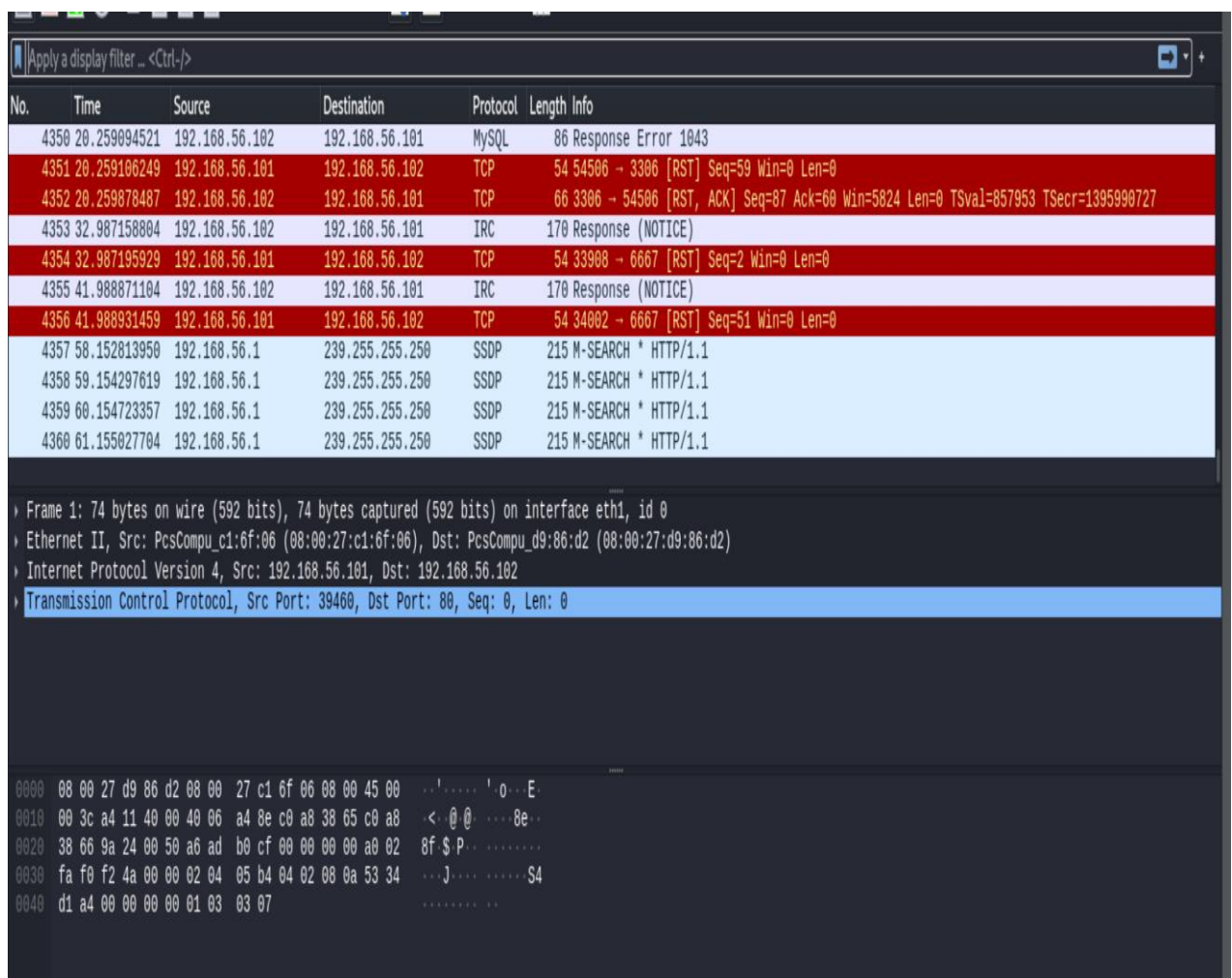
```

TASK 2 Monitoring:

For the monitoring process, I am using the Wireshark tool which is already found in the kali Linux. The below picture shows the scanner shot of Wireshark. For this I am using the third scanning process of Task 1. Wireshark is the tool help me to network troubleshooting.

When I select the TCP protocol in the top section of Wireshark then I can see the TCP/IP layer in the second section. In the TCP/IP, there are five layers which are Physical, Data link, Internet layer, transport, and application layer, respectively.

In the figure below, the first layer is Physical layer which have 528 bits on wire, and it will transfer to the second layer called Data link layer. The second layer is data link layer where I can see the MAC address of the layers. The third layer is Internet layer where I can see the Internet Protocol version 4 and it also shows that source and the destination address to send. The fourth layer is Transport layer where TCP is transferring from the port 3306 to the port 54506. It does not have the application layer because it does not have application to show on the internet using HTTP or HTTPS protocol.



TASK 3 Gain Access:

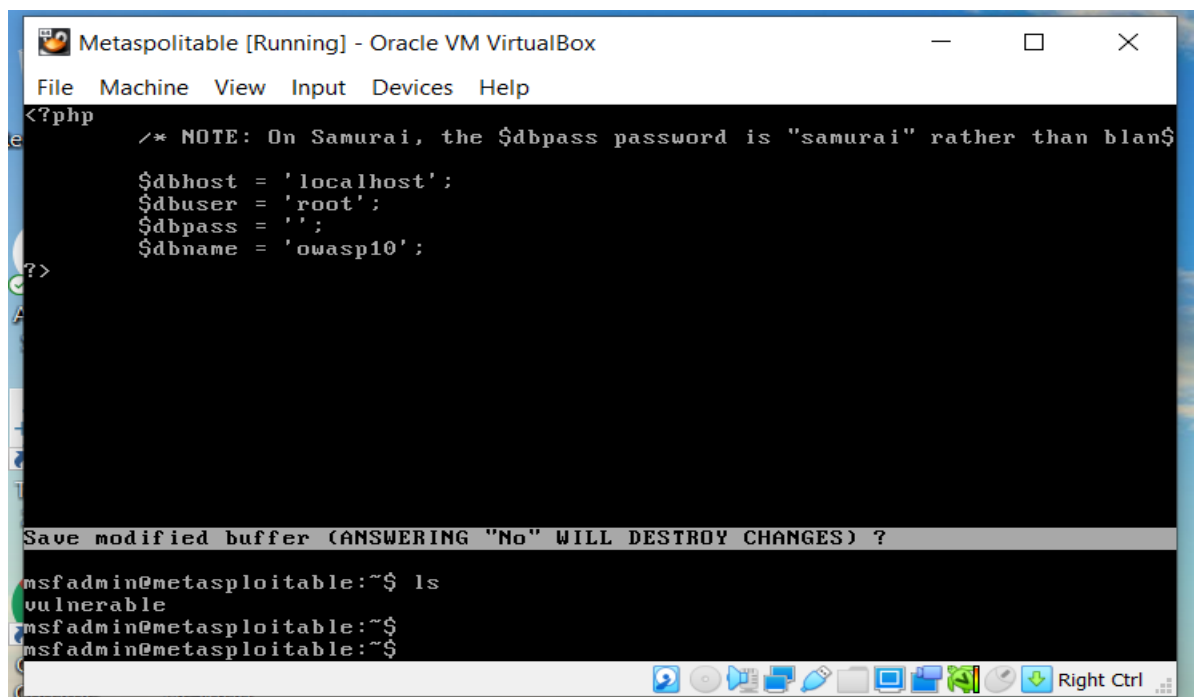
The three different attacks against Metasploitable 2 using the Kali Linux are as follows:

1. SQL Injection:

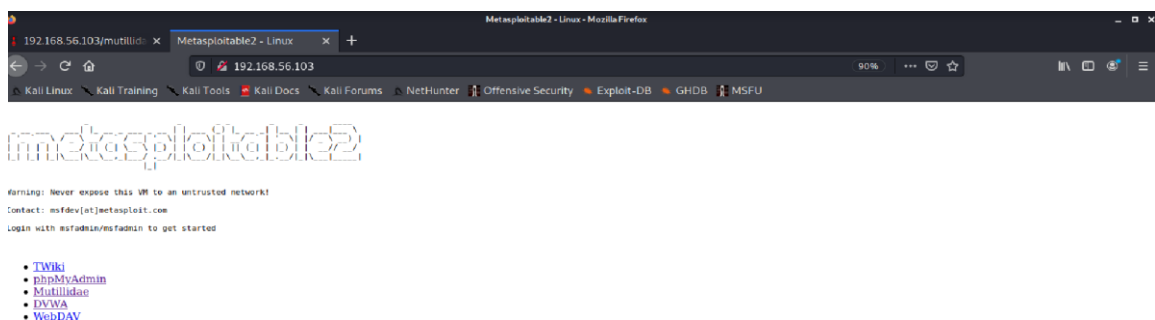
SQL injection(*What is SQL Injection? Tutorial & Examples | Web Security Academy, 2021*) is a web security vulnerability which allows us to attack the website database using the queries. This is a most popular vulnerabilities in the world because all the websites have the database.

As we know that Metasploitable have the Mutillidae web application which have web vulnerabilities so for this process I am going to use this web page.

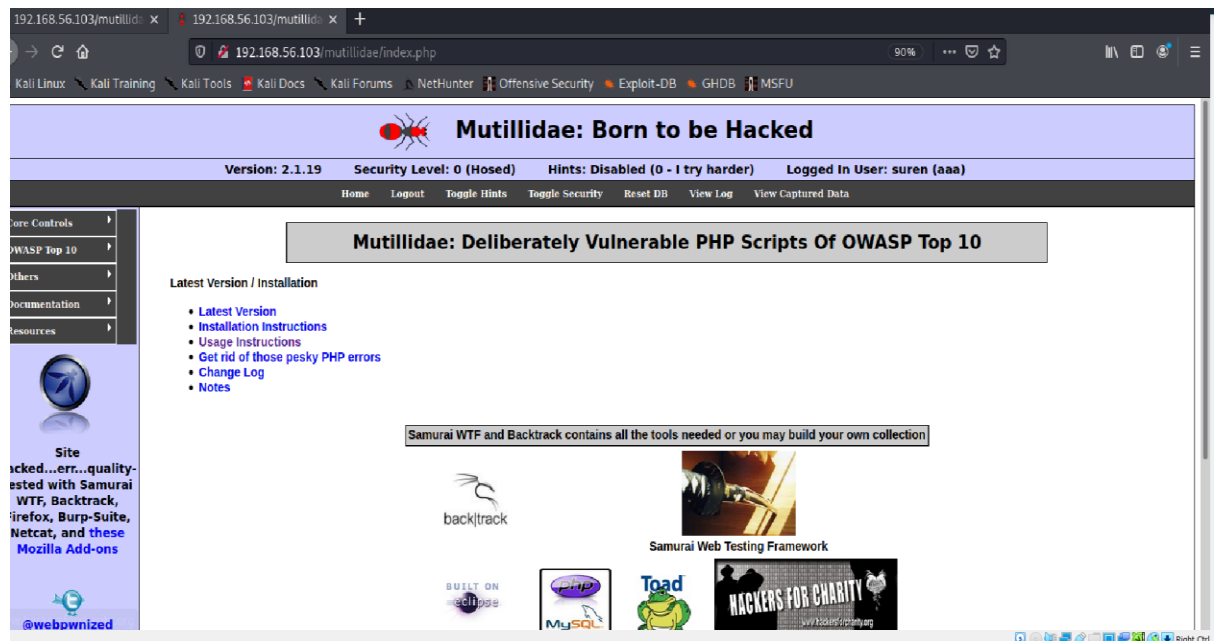
First, I change the database name to the owasp10 inside the Metasploitable which is show in the below picture.



Then, I went to the Firefox and run the IP address of the Metasploitable inside the Kali Linux which is show in the below picture.

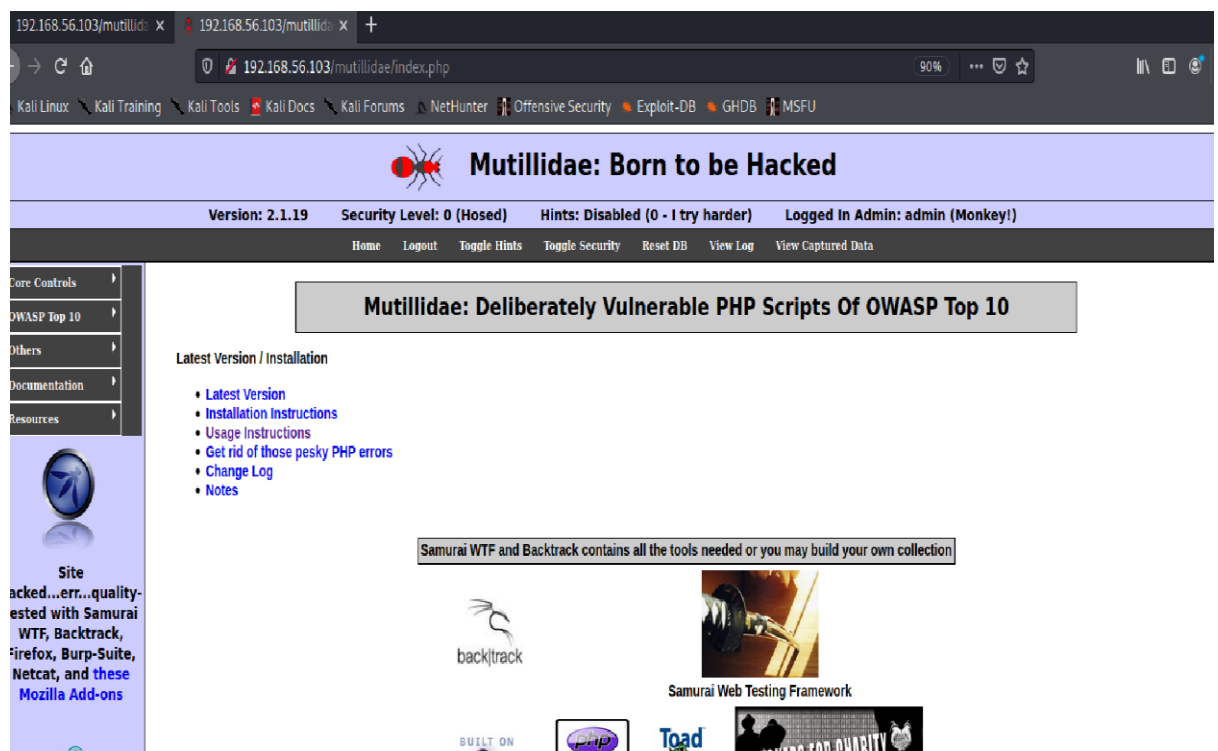


Then, I went to the Mutillidae web page and click on the login/register button in the navigation bar and made the username=suren and password=1234 which is show in the below picture.



After that I logout from the web page and try to hack the web page with the wrong username and the password.

At first, I used the same username but in the password field I put aaa' or 1=1 # which help me to log in, in the web page with the admin user show below figure.



After that, I logout from the system and used username as an admin' # and any password or without password I got the same result as above figure.

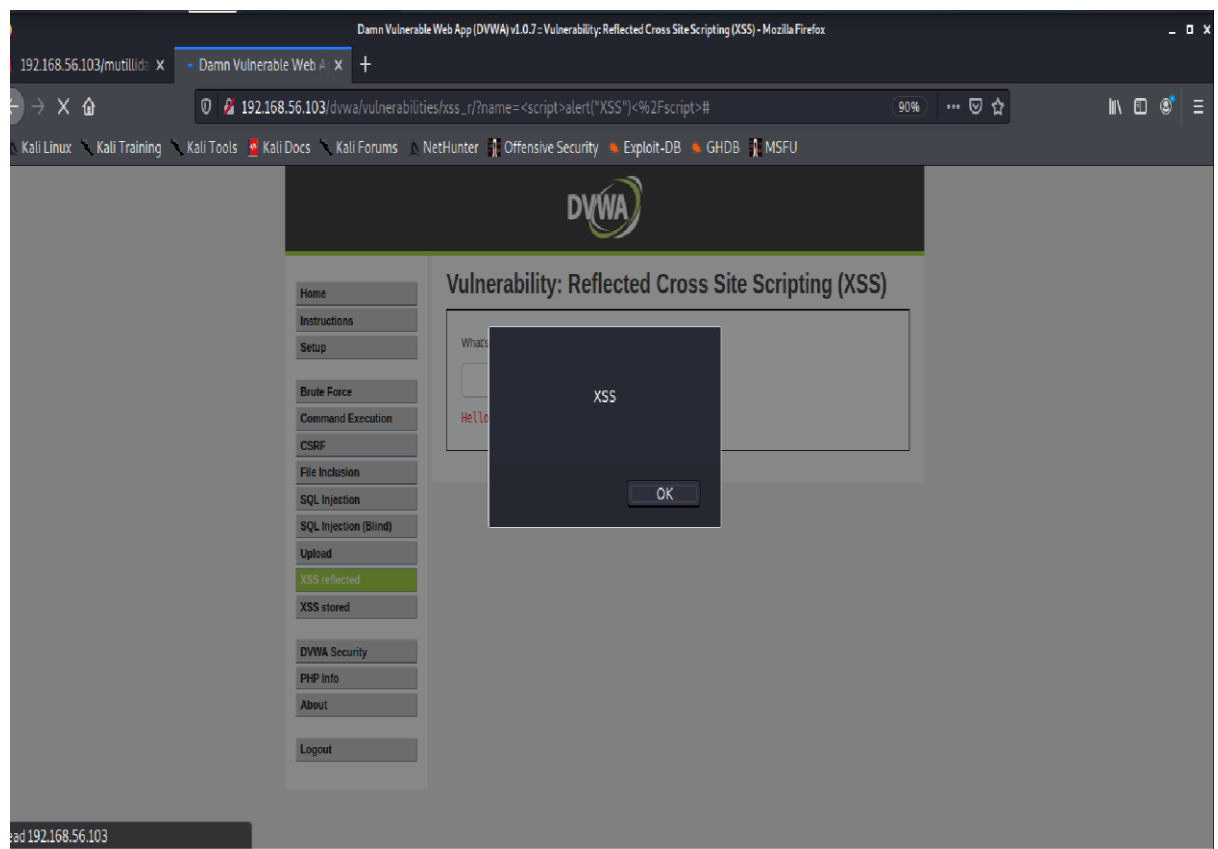
So, from the above task I can see that the web page can be injected by the sql query.

2. Cross Site Scripting:

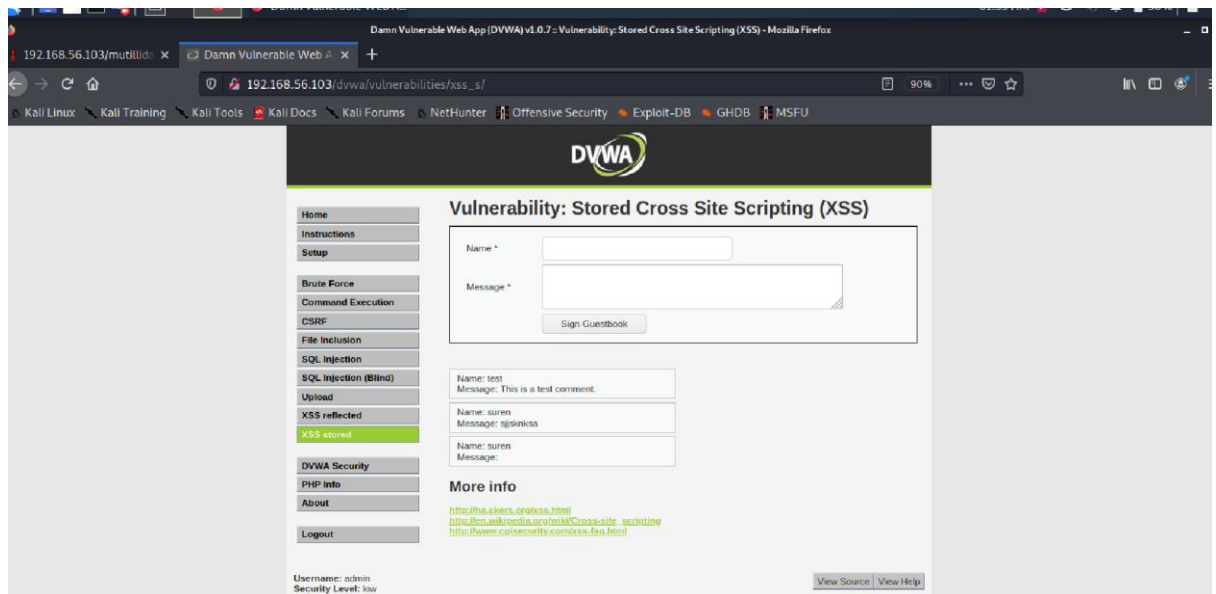
Cross Site Scripting is the scripting done by the attacker to inject the JavaScript code into the page. So, the user going to get the JavaScript code if the website is vulnerable.

As we know that DVWA is also another web app in the Metasploitable which is vulnerable.

So, When I log in to the DVWA web app using admin username and password as a password then I went to the data security and change to the low. Then, I went to the XSS reflected then I type my name then I get Hello suren but when I put the simple JavaScript script like `<script>alert("XSS") </script>` which prompts in the web page and gives me XSS which is shown below. On the other hand, I found that inside URL of web page, the name is equal to script so that I can change the script and got the new value.



After that I went to the XSS stored and use the name and the same script then I go the XSS as a prompt but in the site, it is empty which I can see in the figure below.



3. Sensitive data Exposure:

On the website, we have the sensitive data which should not be shown to the public, so we must hide our data. But today I am going to use a dirb command to use identify the sensitive data of the Mutillidae web app which is show in the below figure. The figure shows the link of the sensitive data pages by using the link I can see the sensitive data of the web page.

```

suren@kali:~$ dirb http://192.168.56.103/mutillidae/
_____
DIRB v2.22
By The Dark Raver

START_TIME: Sun May 16 02:41:30 2021
URL_BASE: http://192.168.56.103/mutillidae/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____

GENERATED WORDS: 4612

_____ Scanning URL: http://192.168.56.103/mutillidae/ _____
=> DIRECTORY: http://192.168.56.103/mutillidae/classes/
+ http://192.168.56.103/mutillidae/credits (CODE:200|SIZE:509)
=> DIRECTORY: http://192.168.56.103/mutillidae/documentation/
+ http://192.168.56.103/mutillidae/favicon.ico (CODE:200|SIZE:1150)
+ http://192.168.56.103/mutillidae/footer (CODE:200|SIZE:450)
+ http://192.168.56.103/mutillidae/header (CODE:200|SIZE:19879)
+ http://192.168.56.103/mutillidae/home (CODE:200|SIZE:2930)
=> DIRECTORY: http://192.168.56.103/mutillidae/images/
+ http://192.168.56.103/mutillidae/inc (CODE:200|SIZE:386260)
=> DIRECTORY: http://192.168.56.103/mutillidae/includes/
+ http://192.168.56.103/mutillidae/index (CODE:200|SIZE:24237)
+ http://192.168.56.103/mutillidae/index.php (CODE:200|SIZE:24237)
+ http://192.168.56.103/mutillidae/installation (CODE:200|SIZE:8138)
=> DIRECTORY: http://192.168.56.103/mutillidae/javascript/
+ http://192.168.56.103/mutillidae/login (CODE:200|SIZE:4102)
+ http://192.168.56.103/mutillidae/notes (CODE:200|SIZE:1721)
+ http://192.168.56.103/mutillidae/page-not-found (CODE:200|SIZE:705)
=> DIRECTORY: http://192.168.56.103/mutillidae/passwords/
+ http://192.168.56.103/mutillidae/phpinfo (CODE:200|SIZE:48903)
+ http://192.168.56.103/mutillidae/phpinfo.php (CODE:200|SIZE:48915)
+ http://192.168.56.103/mutillidae/phpMyAdmin (CODE:200|SIZE:174)
+ http://192.168.56.103/mutillidae/register (CODE:200|SIZE:1823)
+ http://192.168.56.103/mutillidae/robots (CODE:200|SIZE:160)
+ http://192.168.56.103/mutillidae/robots.txt (CODE:200|SIZE:160)
=> DIRECTORY: http://192.168.56.103/mutillidae/styles/

_____ Entering directory: http://192.168.56.103/mutillidae/classes/ _____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

_____ Entering directory: http://192.168.56.103/mutillidae/documentation/ _____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

_____ Entering directory: http://192.168.56.103/mutillidae/images/ _____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

_____ Entering directory: http://192.168.56.103/mutillidae/includes/ _____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

_____ Entering directory: http://192.168.56.103/mutillidae/javascript/ _____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

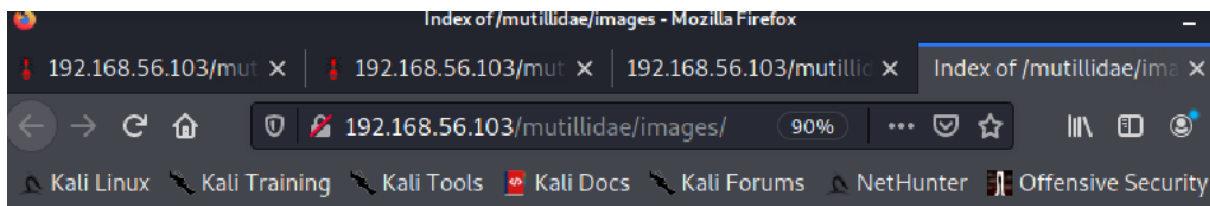
_____ Entering directory: http://192.168.56.103/mutillidae/passwords/ _____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

_____ Entering directory: http://192.168.56.103/mutillidae/styles/ _____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)









_____

END_TIME: Sun May 16 02:41:37 2021
DOWNLOADED: 4612 - FOUND: 18

```



Index of /mutillidae/images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	-	-	-
 ThackBanner2x_final_print.jpg	29-Aug-2008 16:15	100K	
 add_icon.png	13-Mar-2012 21:56	6.9K	
 back-button-128px-by-128px.png	08-Jul-2011 21:21	12K	
 backtrack-4-r2-logo-90-69.png	11-Apr-2011 20:14	1.4K	
 bui_eclipse_pos_logo_fc_med.jpg	11-Apr-2011 20:14	50K	
 coykillericon.png	11-Apr-2011 20:14	5.4K	
 coykillericonfaceup.png	11-Apr-2011 20:14	5.3K	

The Recommendations to Irish bank technical teams to help mitigate each of the attacks which I demonstrated are as follows:

1. For the SQL injection(*What is SQL Injection? Tutorial & Examples | Web Security Academy*, 2021), they can use the prepared statement instead of the concatenation query which is showing below.

```
String query = "SELECT * FROM products WHERE category = '" + input+"'";
```

```
Statement statement = connection.createStatement();
```

```
ResultSet resultSet = statement.executeQuery(query);
```

2. For the XSS vulnerabilities(*Cross Site Scripting Prevention - OWASP Cheat Sheet Series*, 2021), we must use the form validation for the user input, and we can also escape any untrusted input in the web page. For example: email address should be validated and then the user should have to verify their email address.
3. For the sensitive data exposure(*A3:2017-Sensitive Data Exposure | OWASP*, 2021), we have to provide an extra layer of security for the sensitive data like using the tokenization. And also, we have to encrypt our all-sensitive data and store in the web page with the layer of strong algorithms, protocols and the keys or passwords.

TASK 4 Monitoring Distribution Systems:

According to the Google's SRE(Ewaschuk, 2017), Monitoring is the process of collecting, processing, aggregating and displaying the real time data of the system in a dashboard so that we can find the error, latency and traffic of the system. For the Irish bank, I would suggest using the white box monitoring, black box monitoring and the dashboard because as the follow's reasons:

1. Black box monitoring('Distributed Monitoring 101', 2021) help us to monitoring that our service or the nodes which one is failure in the system but it does not help us to solve the problem For example, Black box monitoring give us alter when the system disk cross the exceeds of the certain threshold.
2. White box monitoring ('Distributed Monitoring 101', 2021) help us to monitoring the entire system like logs, metrics and traces. So, it helps us to fix the problem because it provides us the control and visibility of the system like showing the works and expectation of the system in the result. For example, White box monitoring help us to find out the rate at which the disk will fill up in the system.
3. Dashboard(Ewaschuk, 2017) is another useful monitoring technique which help us to find out the summary of the system so that we can filter and select each system and find out the error and the problem in the system. It us help the team to make a ticket queue, listing of high-quality bugs and divides the team to fix the problem.

Finally, I would like to say that Irish bank should use all three system to do the best monitoring because each monitoring system have their own responsibility and advantages and disadvantages. All the three system help us to monitor our distribution system in an easy and the reliable way. For example, Irish bank can used black box monitoring to identify problem from the end user point of view. White box monitoring help them to find out the problem in the system and the application. Dashboard help them to see the issue in a single dashboard and managing the team members and the error and the bugs. On the other hand, Google('Distributed Monitoring 101', 2021) also using black box monitoring with heavy white box monitoring in their system. So, all three monitoring is required to do the best monitoring.

According to the Google SRE(Four Golden Signals for Monitoring Distributed Systems, 2018), three are four golden signals metrics of user-facing systems which are latency, traffic , errors, saturation so I will also recommended to use this four golden signals for Irish bank. The four golden signals are discussing below:

1. Latency:
It is a processing time between the request and the response in the application. For the application, low latency gives us the high performance so we must have to measure the latency in our system. In our system, we must have high response time when the system shows us the success or the error result. If the system run in the server than the client must get the success or error result within a second so latency help Irish bank to check their server within the seconds and solve the problem. For example, HTTP 200 is the success, and the HTTP 500 is the error in the database. By using the HTTP error, we can solve the issue, but the system should response fast so that we can know what going on inside the system.

SolarWinds AppOptics(*Four Golden Signals for Monitoring Distributed Systems*, 2018) is the monitoring tool for the server-side latency and SolarWinds Pingdom(*Four Golden*

Signals for Monitoring Distributed Systems, 2018) is the monitoring tool for the client-side latency which are showing below figures.

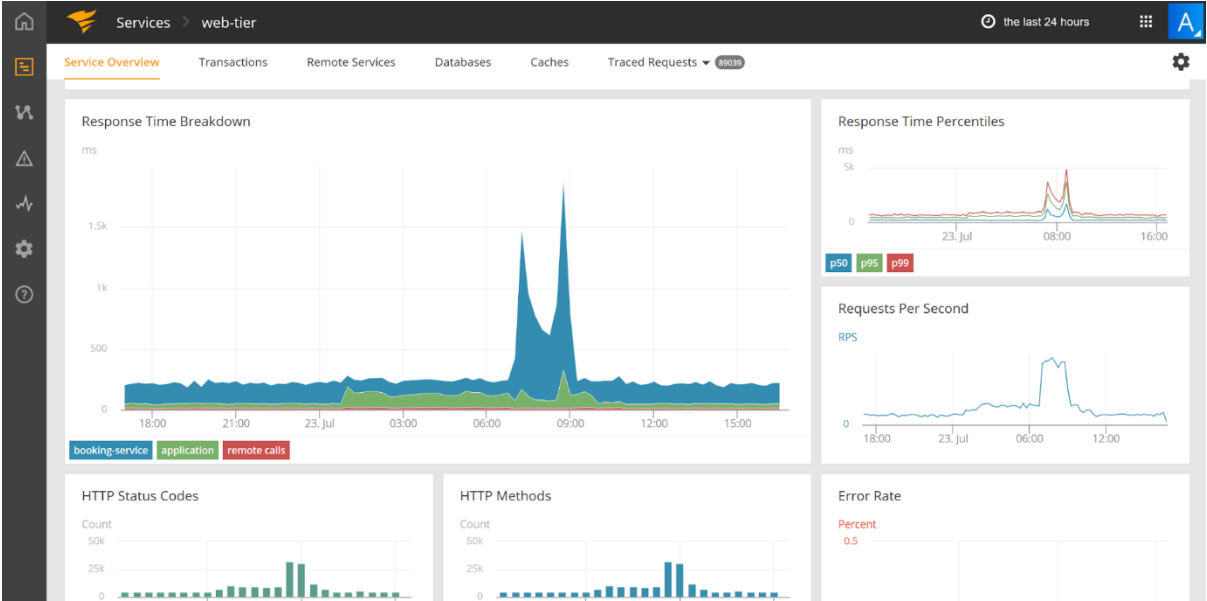


Fig: SolarWinds AppOptics(*Four Golden Signals for Monitoring Distributed Systems, 2018*)

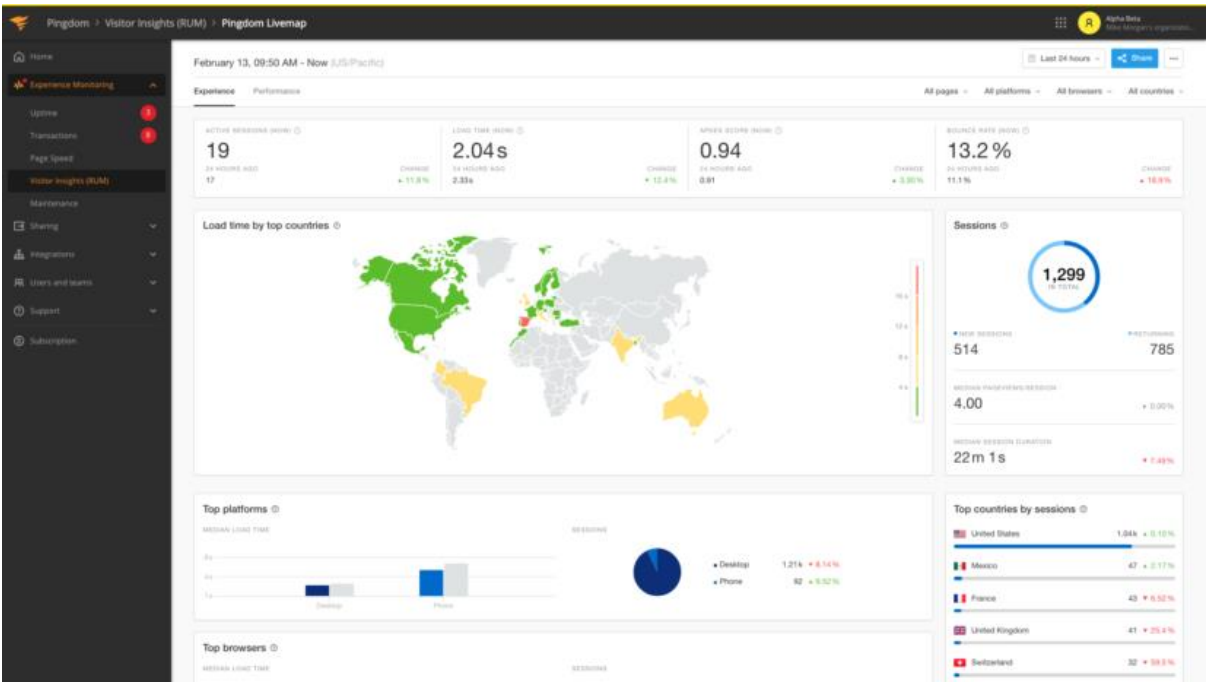


Fig: SolarWinds Pingdom(*Four Golden Signals for Monitoring Distributed Systems, 2018*)

2. Traffic:

Traffic is the requests flowing in the network using HTTP requests to the web server or API on the internet. So, we must measure the traffic flowing in the system per second so that we can make our system more reliable and easy flow on the internet. For example, if the more people want to access our website than we must provide more traffic flow to them so that additional people also can use our website smoothly.

3. Errors:

Errors help us to find out error and the problem in the system so that we can find out the bugs in the code, broken dependencies, and other system failure activities. In our system, we also must look the error so that our client would not get any problem while using our website. For example, we must see the error between the database and the frontend site so that our database should properly connect to frontend.

4. Saturation:

Saturation helps us to find out the load in our system and the network resources. For example, we must check our CPU utilization, memory usage, disk capacity and options per second on the internet. So, by watching this things we can find out that which system will be saturated first and what should we have to do in the future like if the memory is full then we must free the memory or add the hard drive to give the more memory in the system.

TASK 5 Data Security:

The three key risks and threats associated with data security in Irish Bank are follows:

1. Accidental sharing:
Accidental sharing(Council, 2019) means sharing the data in the internet by the employee accidentally. It was also found that most of the data breaches in the company is done by the accident of the employee. According to the 2018 Shred-It(July 23, 2018 and Pst, 2018) report it was found that 40% of the data was breaches by the employee negligence. So, for the Irish bank employee, they must have thought about this risk while working in the company to secure their system.
2. Employee Data Theft:
Employee Data Theft(Council, 2019) means the employee working in the company may share the data or information to the other people or other company. According to the Verizon's 2019 Insider Threat Report(*Verizon's 2019 Insider Threat Report*, 2021) it was found that 57% of data was breached by the insider threats within an organization and 61% of the data was breached by the employees who are not in the leader position. Some employees may sale the data for the money also. So, Irish bank employee should have to know about this risk factor.
3. Fraud:
Fraud(Council, 2019) means many black hacker will ask them about the data and the security system of their organization by using email or by using any link. For the Irish bank, the hacker will hack their system by using the different kinds of activities so the security system team should be aware of the fraud activities. Somebody will ask the email and password of the customers so on this case the security team should have to aware that how they will secure their data.

The three recommendations on how the relevant legislative and regulatory framework (such as General Data Protection Regulation) apply to Irish banks organization in the case of access control are as follows:

1. For the Protection of the Data of the Irish bank they should have to appoint a Data Protection Officer (DPO)(What is GDPR, the EU's new data protection law?, 2018) so that if the data breaches in the public then all the responsibilities should go to that person and he/she have to solve the problem. On the other hand, he/she must know the GDPR rule and regulation and then apply the GDPR rule and regulation inside the organization by conducting the data protection training for the staff.
2. According to the GDPR(*What is GDPR, the EU's new data protection law?*, 2018), people have a right to handle their data so whenever the Irish bank want the customer data then they should have to ask the customer about it. For example, if the customer wants credit card from the bank, then the detail of the customer goes to the credit card department so the company should have to inform them about it.
3. Irish banks have highly sensitive data of the customer so they must secure their system in such a way that the data will not breaches on the internet. For example, they must store their data in the encryption format so that when the data breaches happen, the data must be decrypted, otherwise the data cannot be readable. On the other hand, they must use two-factor authentication on the account of the customer to verify so that if the hacker hacks the system, then they need addition process to crack the system.

References

A3:2017-Sensitive Data Exposure | OWASP (2021). Available at: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html (Accessed: 16 May 2021).

Council, Y. E. (2019) *Council Post: 10 Data Security Risks That Could Impact Your Company In 2020*, *Forbes*. Available at: <https://www.forbes.com/sites/theyec/2019/10/01/10-data-security-risks-that-could-impact-your-company-in-2020/> (Accessed: 14 May 2021).

Cross Site Scripting Prevention - OWASP Cheat Sheet Series (2021). Available at: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html (Accessed: 16 May 2021).

'Distributed Monitoring 101' (2021) *IOD*, 12 January. Available at: <https://iamondemand.com/blog/distributed-monitoring-101/> (Accessed: 14 May 2021).

Ewaschuk, R. (2017) *Google - Site Reliability Engineering*. Available at: <https://sre.google/sre-book/monitoring-distributed-systems/> (Accessed: 13 May 2021).

Four Golden Signals for Monitoring Distributed Systems (2018) *AppOptics Blog*. Available at: <https://blog.appoptics.com/the-four-golden-signals-for-monitoring-distributed-systems/> (Accessed: 13 May 2021).

July 23, M. K. in S. on, 2018 and Pst, 10:58 Am (2018) *More than 40% of reported security breaches are caused by employee negligence*, *TechRepublic*. Available at: <https://www.techrepublic.com/article/over-40-of-reported-security-breaches-are-caused-by-employee-negligence/> (Accessed: 14 May 2021).

Metasploitable 2 Exploitability Guide | Metasploit Documentation (2021). Available at: <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/> (Accessed: 6 May 2021).

nmap (1) - Linux man page (2021). Available at: <https://linux.die.net/man/1/nmap> (Accessed: 6 May 2021).

Verizon's 2019 Insider Threat Report (2021) *Verizon Enterprise*. Available at: <https://enterprise.verizon.com/resources/reports/insider-threat-report/> (Accessed: 14 May 2021).

What is GDPR, the EU's new data protection law? (2018) *GDPR.eu*. Available at: <https://gdpr.eu/what-is-gdpr/> (Accessed: 15 May 2021).

What is SQL Injection? Tutorial & Examples | Web Security Academy (2021). Available at: <https://portswigger.net/web-security/sql-injection> (Accessed: 16 May 2021).