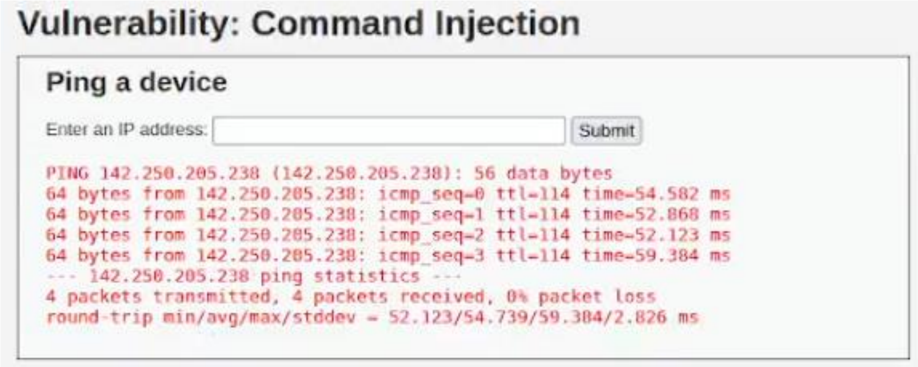
Command Injection

DVWA

Procedure:

1.Enter the Ip address



Vulnerability: Command Injection

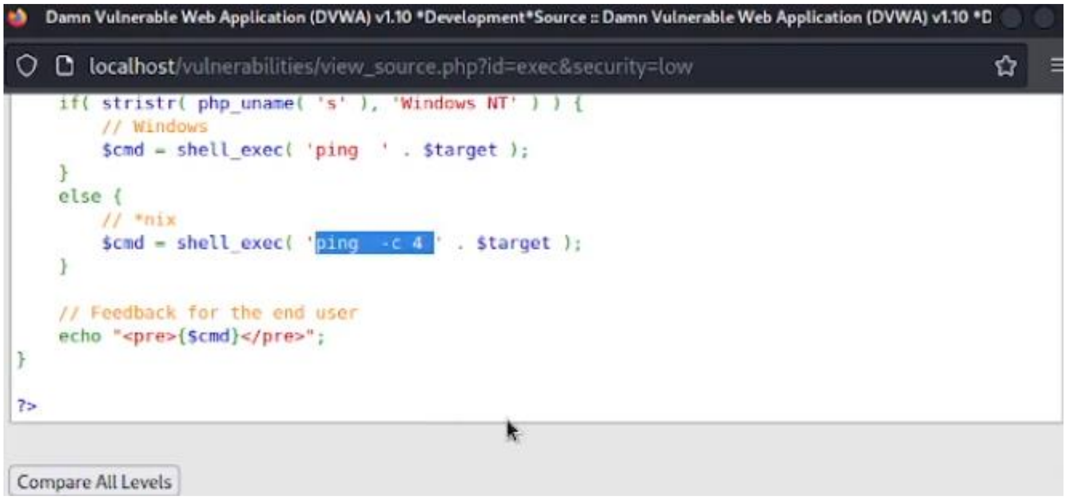
Ping a device

Enter an IP address: Submit

```
PING 142.250.205.238 (142.250.205.238): 56 data bytes
64 bytes from 142.250.205.238: icmp_seq=0 ttl=114 time=54.582 ms
64 bytes from 142.250.205.238: icmp_seq=1 ttl=114 time=52.868 ms
64 bytes from 142.250.205.238: icmp_seq=2 ttl=114 time=52.123 ms
64 bytes from 142.250.205.238: icmp_seq=3 ttl=114 time=59.384 ms
--- 142.250.205.238 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 52.123/54.739/59.384/2.826 ms
```

It will return 4 responses. The ping command is used here.

2.Check bottom of the page there is a php code let analyze that code



Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) v1.10 *D

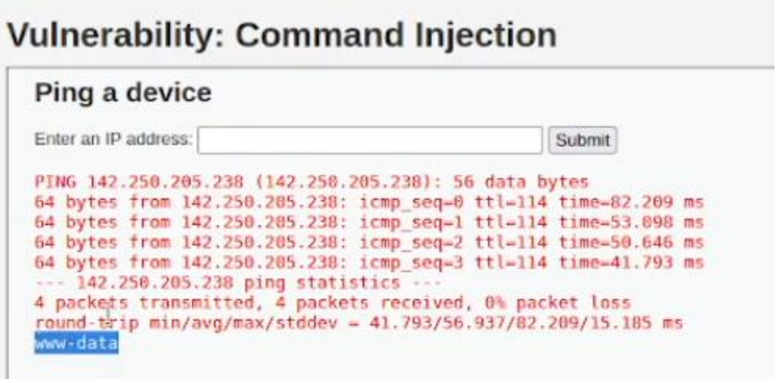
localhost/vulnerabilities/view_source.php?id=exec&security=low

```
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

3.use whoami command to check who is the user?



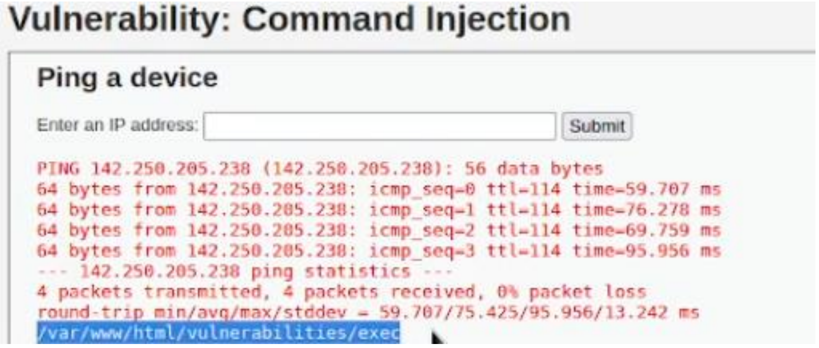
Vulnerability: Command Injection

Ping a device

```
PING 142.250.205.238 (142.250.205.238): 56 data bytes
64 bytes from 142.250.205.238: icmp_seq=0 ttl=114 time=82.209 ms
64 bytes from 142.250.205.238: icmp_seq=1 ttl=114 time=53.898 ms
64 bytes from 142.250.205.238: icmp_seq=2 ttl=114 time=50.646 ms
64 bytes from 142.250.205.238: icmp_seq=3 ttl=114 time=41.793 ms
--- 142.250.205.238 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 41.793/56.937/82.209/15.185 ms
www-data
```

www.data is shown. We clearly understand that this machine is vulnerable to command injection.

4. I used pwd command to print the current working directory.



Vulnerability: Command Injection

Ping a device

```
PING 142.250.205.238 (142.250.205.238): 56 data bytes
64 bytes from 142.250.205.238: icmp_seq=0 ttl=114 time=59.707 ms
64 bytes from 142.250.205.238: icmp_seq=1 ttl=114 time=76.278 ms
64 bytes from 142.250.205.238: icmp_seq=2 ttl=114 time=69.759 ms
64 bytes from 142.250.205.238: icmp_seq=3 ttl=114 time=95.956 ms
--- 142.250.205.238 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 59.707/75.425/95.956/13.242 ms
/var/www/html/vulnerabilities/exec
```

It will print the current directory.