

Act. 3.3 Practica WAF AL DVWA INTALAR CERTIFICADO DE HTTP A HTTPS.- 50%

Configuración del WAF.

```
sudo apt install libapache2-mod-security2
sudo a2enmod security2
sudo nano /etc/modsecurity/modsecurity.conf-recommended
sudo nano /etc/modsecurity/modsecurity.conf
cd /etc/modsecurity
sudo git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git
sudo mv owasp-modsecurity-crs/crs-setup.conf.example owasp-modsecurity-crs/crs-setup.conf
sudo nano etc/modsecurity/modsecurity.conf
sudo service apache2 restart
```

Nota: Por defecto no te aparecera modsecurity.conf, por lo cual tendras que hacer una copia de modsecurity.conf-recommended y luego renombrarlo a modsecurity.conf

Configuración del HTTPS.

```
sudo apt update
sudo ufw allow "Apache Full"
sudo a2enmod ssl
sudo systemctl restart apache2
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
cd /etc/apache2/sites-available
sudo nano apache2.conf
```

Aquí, actualizaremos esta información:

```
DocumentRoot /var/www/html

SSLEngine on

SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
```

Y luego testaremos y reiniciaremos el servidor para reflejar los cambios.

```
sudo apachectl configtest
sudo a2ensite default-ssl.conf
sudo systemctl reload apache2
```

Protección de rutas.

```
cd /etc/apache2
sudo nano apache2.conf
```

Aquí, actualizaremos esta información:

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>

<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/html>
    AllowOverride ALL
    Require all granted
</Directory>

<Directory /var/www/html/images>
    Options Indexes
</Directory>
```

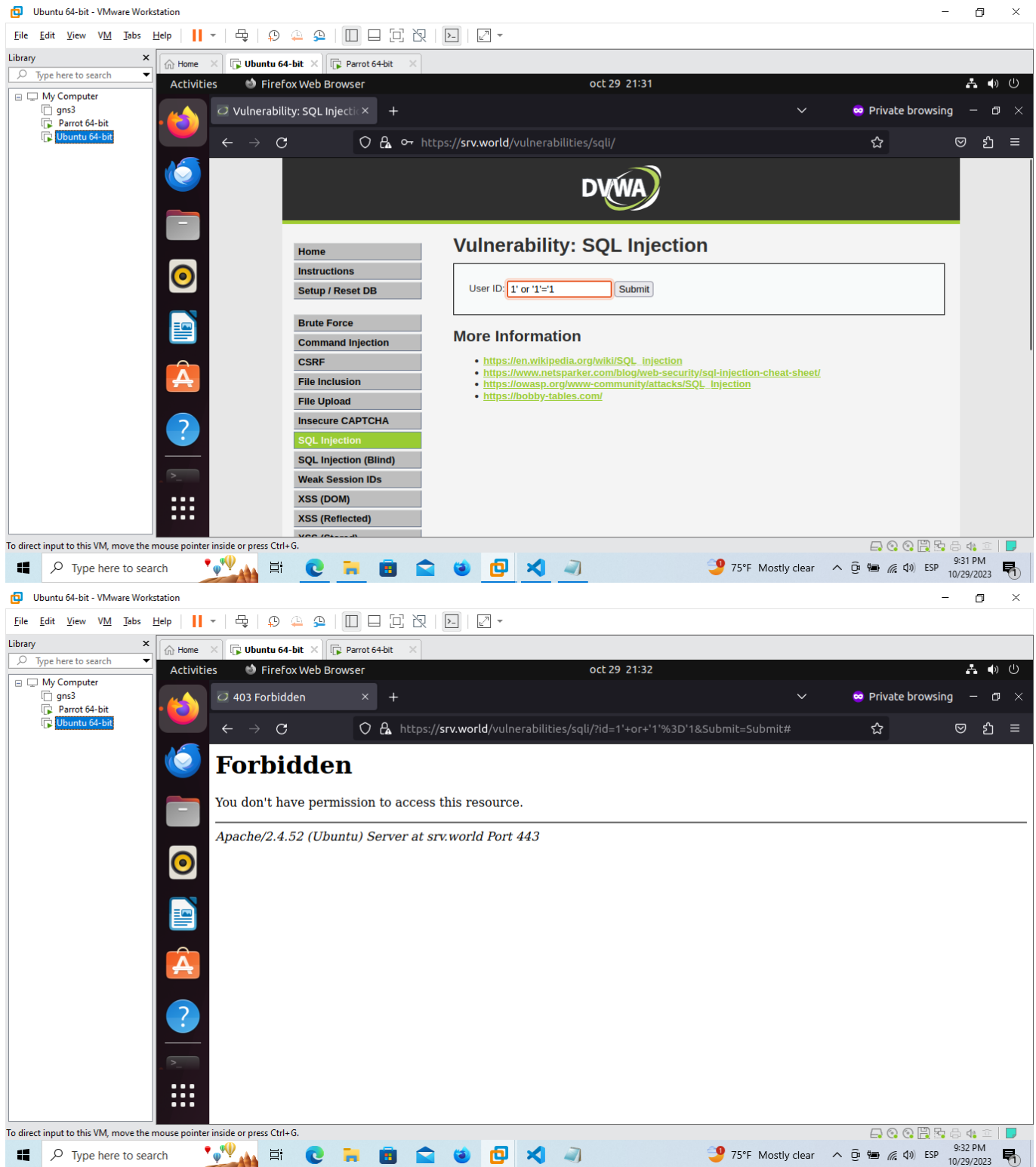
Y luego reiniciaremos el servidor para reflejar los cambios.

```
service apache2 restart
```

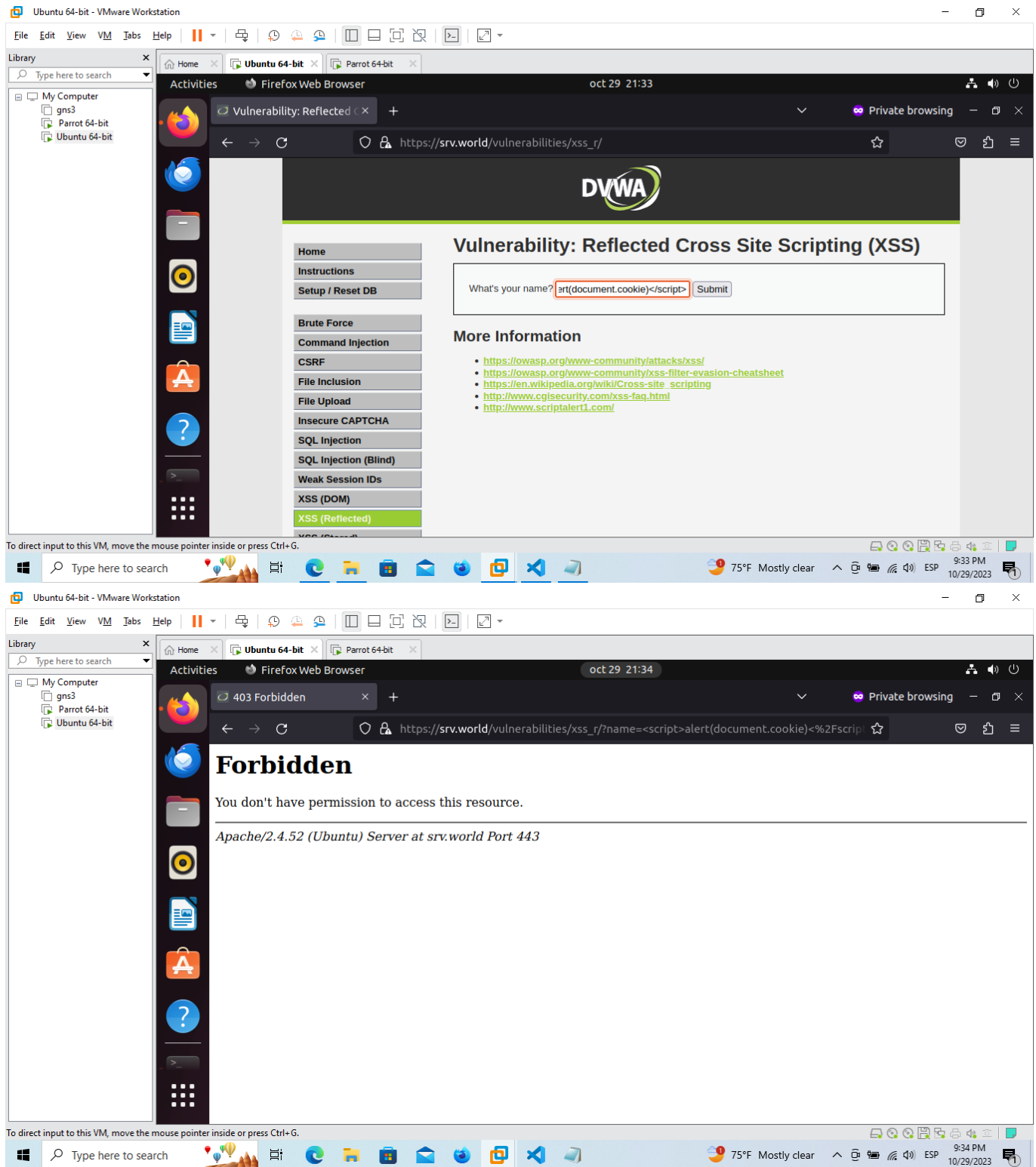
Testeando Parametros de Seguridad.

Waf.

```
1' or '1'='1
```



```
<script>alert(document.cookie)</script>
```



```
sqlmap -u "https://192.168.18.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" -  
-cookie="PHPSESSID=36tr0lmnmhdt7jqpq1u2cijvn;security=low"
```

The image shows two virtual machines in a VMware Workstation environment.

Top VM: Ubuntu 64-bit

- Running Firefox Web Browser.
- Tab: Vulnerability: SQL Injection.
- Address bar: `https://srv.world/vulnerabilities/sql/`
- Page title: DVWA Vulnerability: SQL Injection.
- Form: User ID: Submit
- Inspector: Cookies table.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure
PHPSESSID	36tr0lmnmhdt7/kpq1u2cijnv	srv.world	/	Tue, 31 Oct 2023 03:30:51 GMT	35	true	false
security	low	srv.world	/	Session	11	false	false

Bottom VM: Parrot 64-bit

 - Running Parrot Terminal.
 - Terminal output:

```
{1.6.12#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

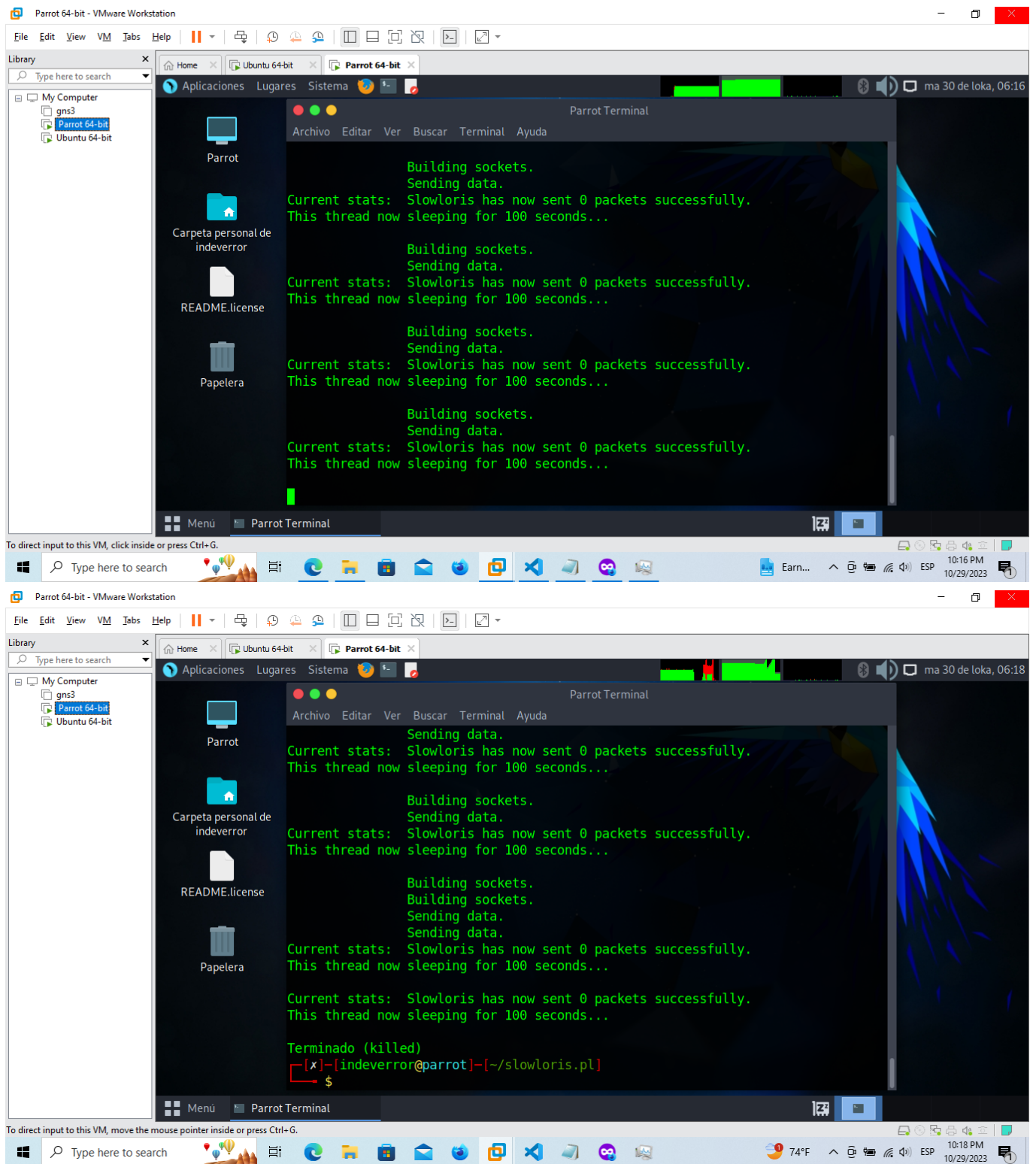
[*] starting @ 05:53:50 /2023-10-30/

[05:53:50] [INFO] testing connection to the target URL
[05:55:20] [CRITICAL] can't establish SSL connection
[05:55:20] [WARNING] your sqlmap version is outdated

[*] ending @ 05:55:20 /2023-10-30/

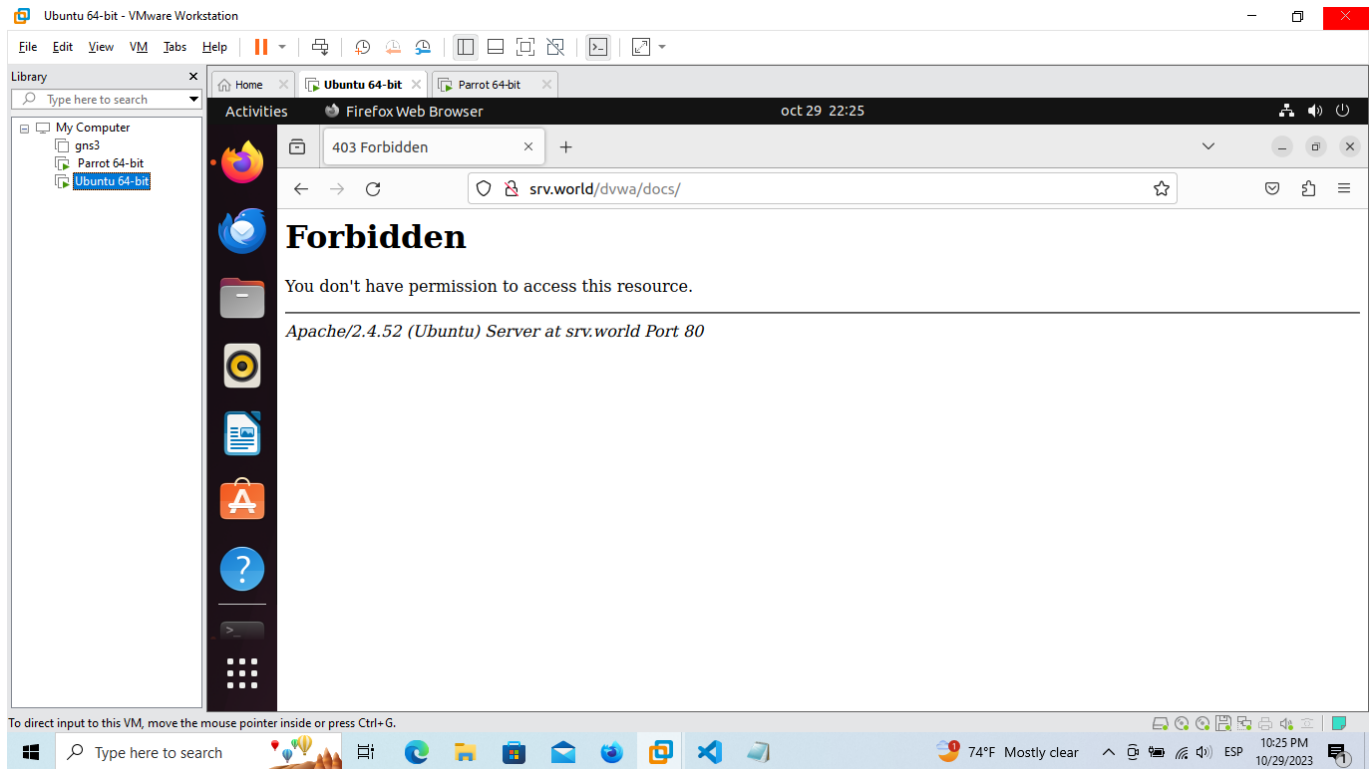
[inderror@parrot]~$
```

```
cd slowloris.pl
perl slowloris.pl -dns https://192.168.18.129 -num 100000
```

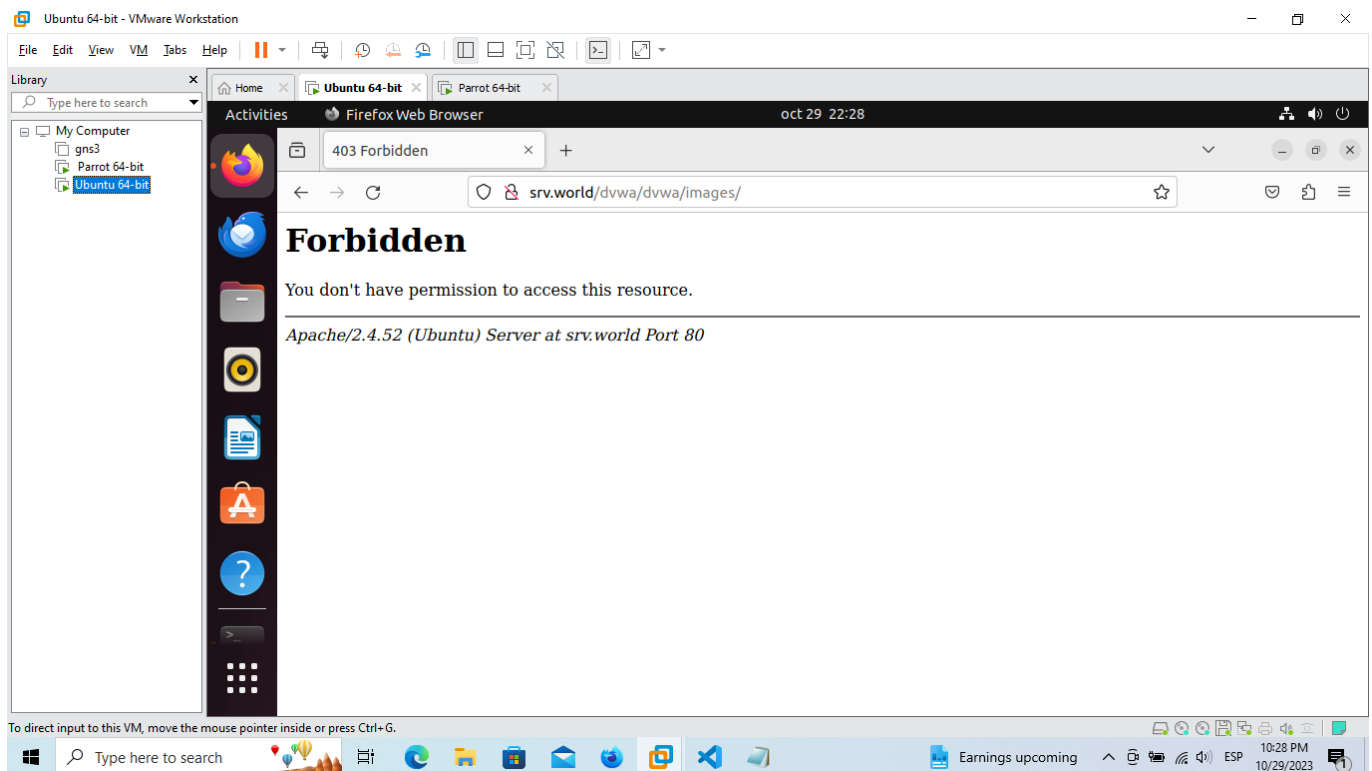


Rutas.

<http://srv.world/dvwa/docs/>

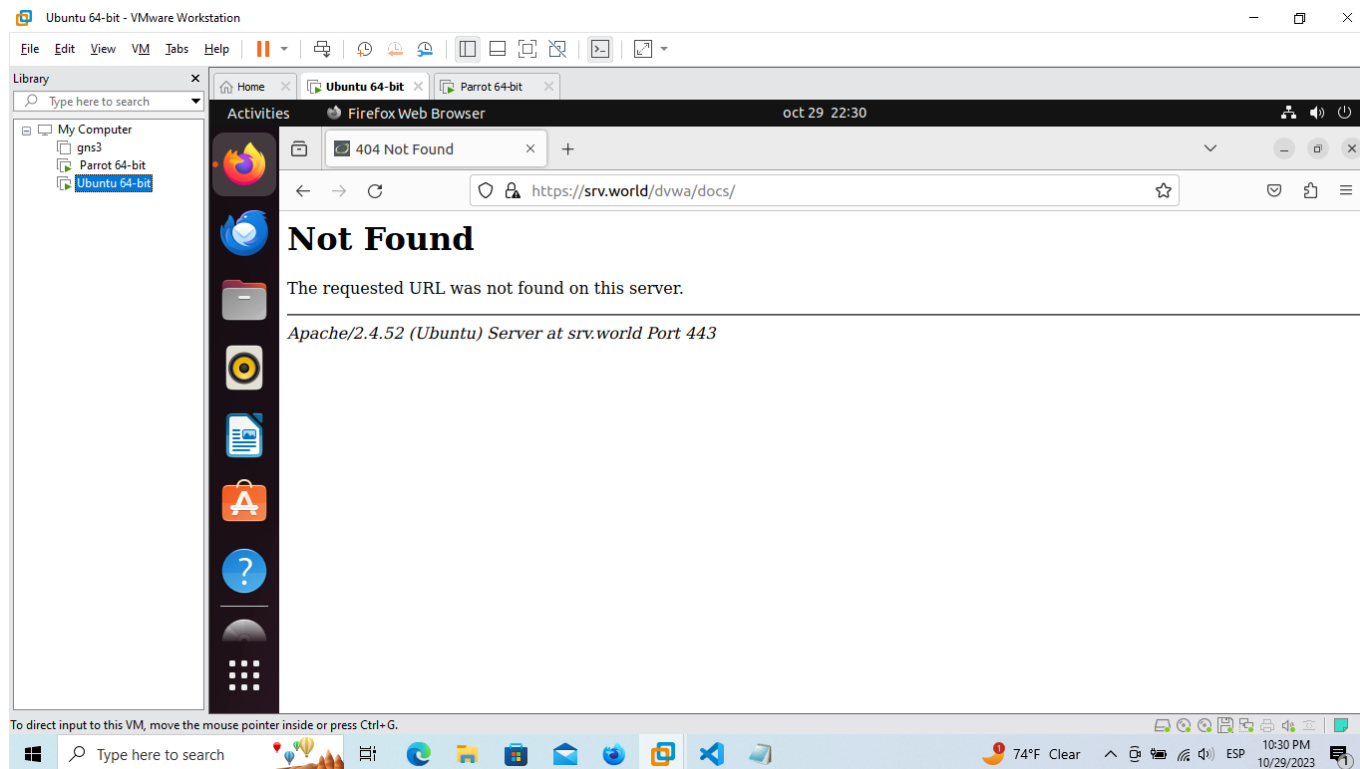


`http://srv.world/dvwa/dvwa/images/`

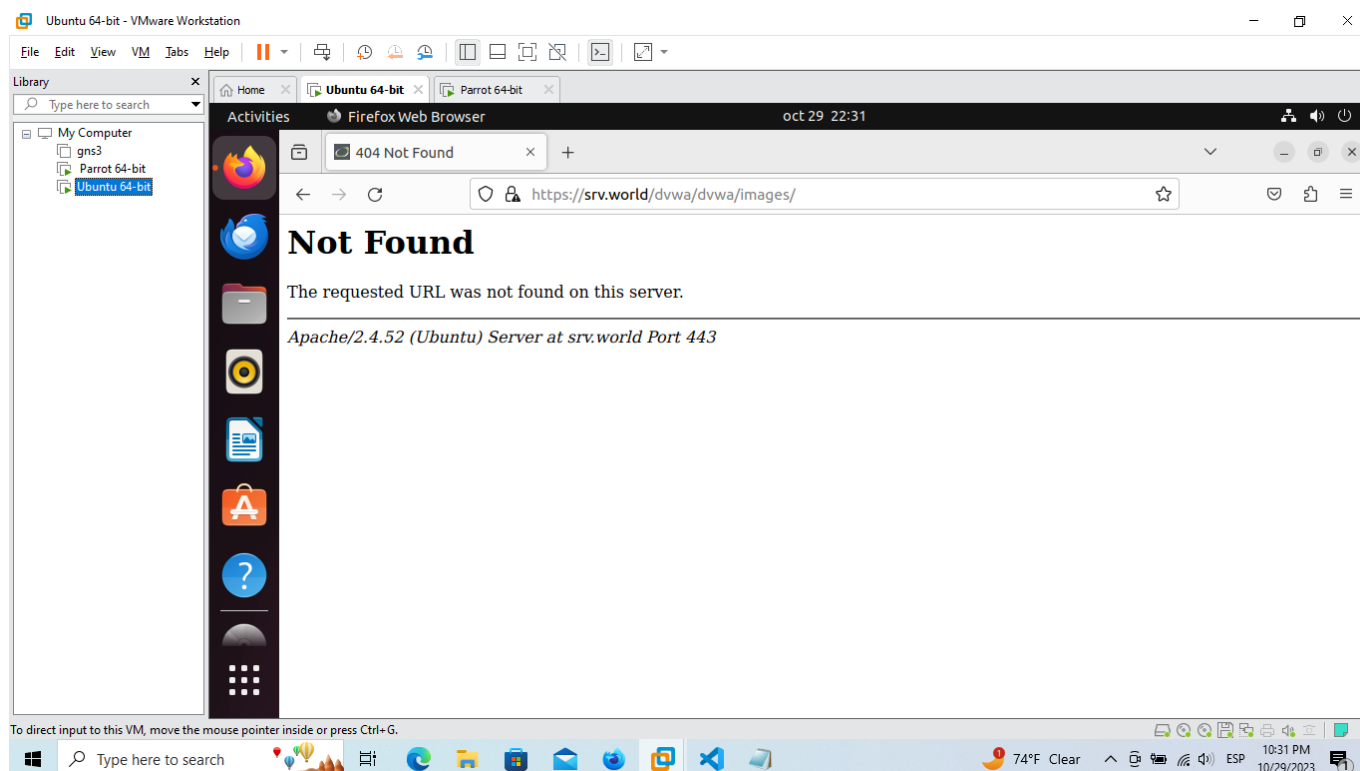


Dato curioso, si habilitamos https, ni si quiera menciona que el contenido existe.

`https://srv.world/dvwa/docs/`



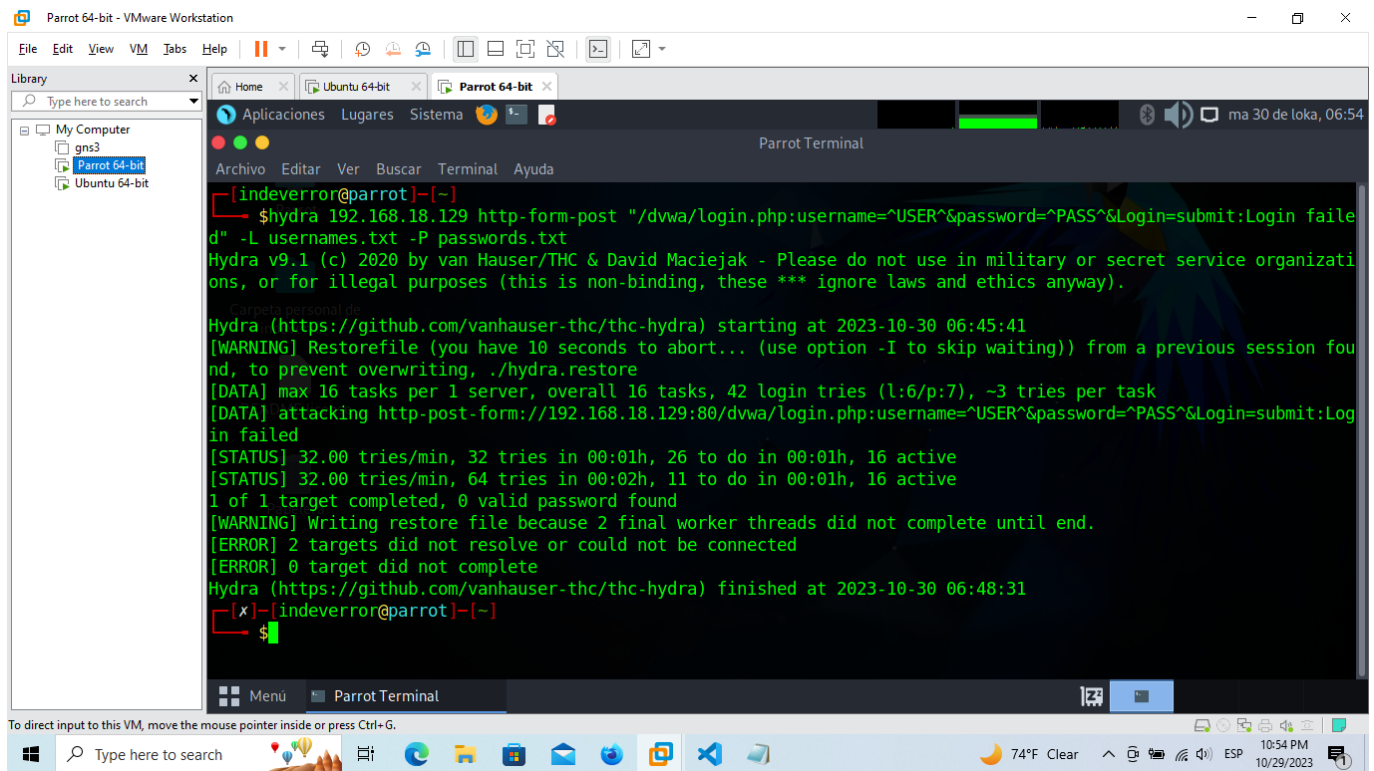
`https://srv.world/dvwa/dvwa/images/`



Extras.

hydra

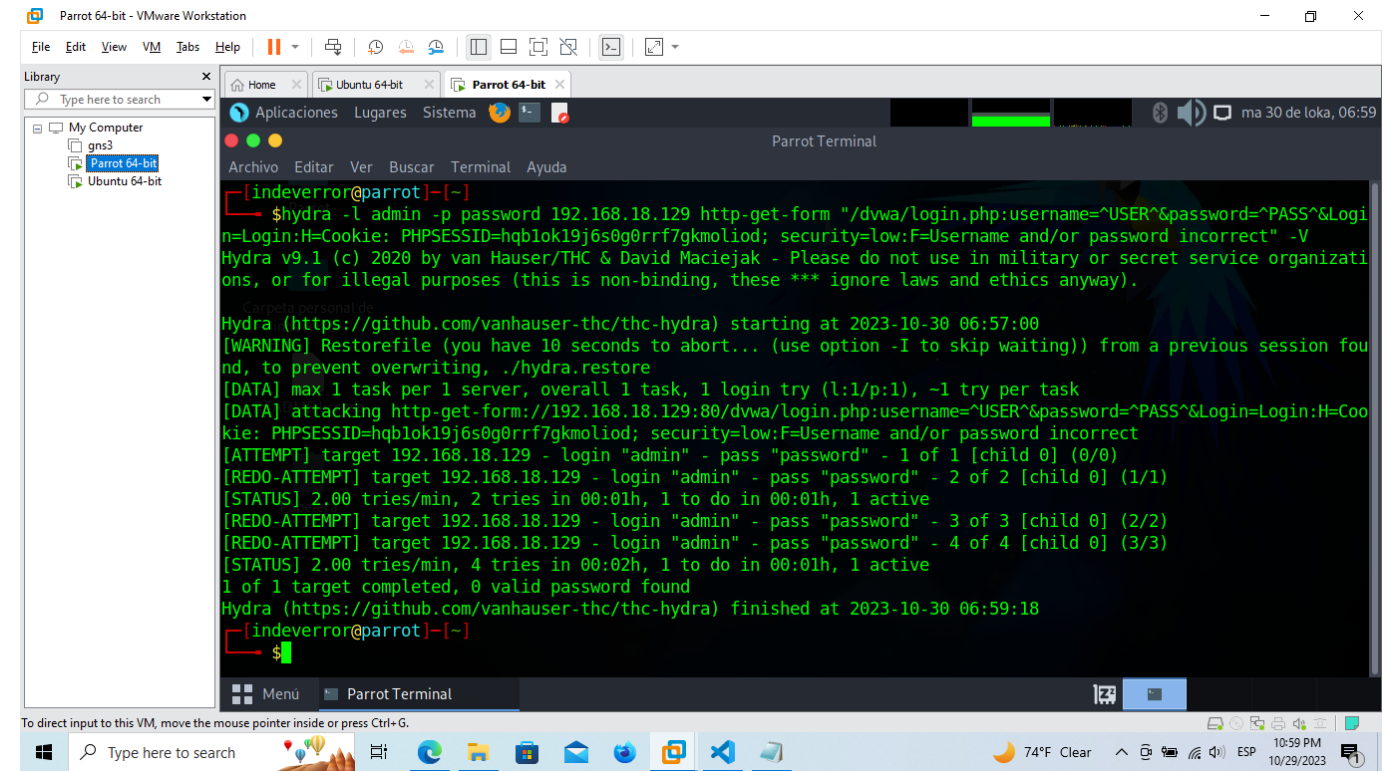

```
hydra 192.168.18.129 http-form-post  
"/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L  
usernames.txt -P passwords.txt
```



The screenshot shows a Parrot 64-bit VM running a terminal window. The terminal displays the execution of a Hydra brute-force attack. The command used is: `hydra 192.168.18.129 http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L usernames.txt -P passwords.txt`. The output shows the attack starting at 2023-10-30 06:45:41, with a warning to restore a previous session. The attack is running with 16 tasks and 42 login tries. The status shows 32.00 tries/min, 32 tries in 00:01h, 26 to do in 00:01h, 16 active. The data shows attacking http-post-form://192.168.18.129:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed. The attack finished at 2023-10-30 06:48:31, with 0 valid password found and 0 target did not complete.

```
Parrot 64-bit - VMware Workstation  
File Edit View VM Tabs Help  
Library  
Type here to search  
My Computer  
gns3  
Parrot 64-bit  
Ubuntu 64-bit  
Home x Ubuntu 64-bit x Parrot 64-bit x  
Aplicaciones Lugares Sistema  
Parrot Terminal  
ma 30 de loka, 06:54  
Archivo Editar Ver Buscar Terminal Ayuda  
[indeverror@parrot]~  
$ hydra 192.168.18.129 http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L usernames.txt -P passwords.txt  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Carpetas personal de  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-30 06:45:41  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (l:6/p:7), ~3 tries per task  
[DATA] attacking http-post-form://192.168.18.129:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed  
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 26 to do in 00:01h, 16 active  
[STATUS] 32.00 tries/min, 64 tries in 00:02h, 11 to do in 00:01h, 16 active  
1 of 1 target completed, 0 valid password found  
[WARNING] Writing restore file because 2 final worker threads did not complete until end.  
[ERROR] 2 targets did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-30 06:48:31  
[x]-[indeverror@parrot]~  
$
```

```
hydra -l admin -p password 192.168.18.129 http-get-form  
"/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie:  
PHPSESSID=hqb1ok19j6s0g0rrf7gkmlod; security=low:F=Username and/or password  
incorrect" -V
```



file uploads

