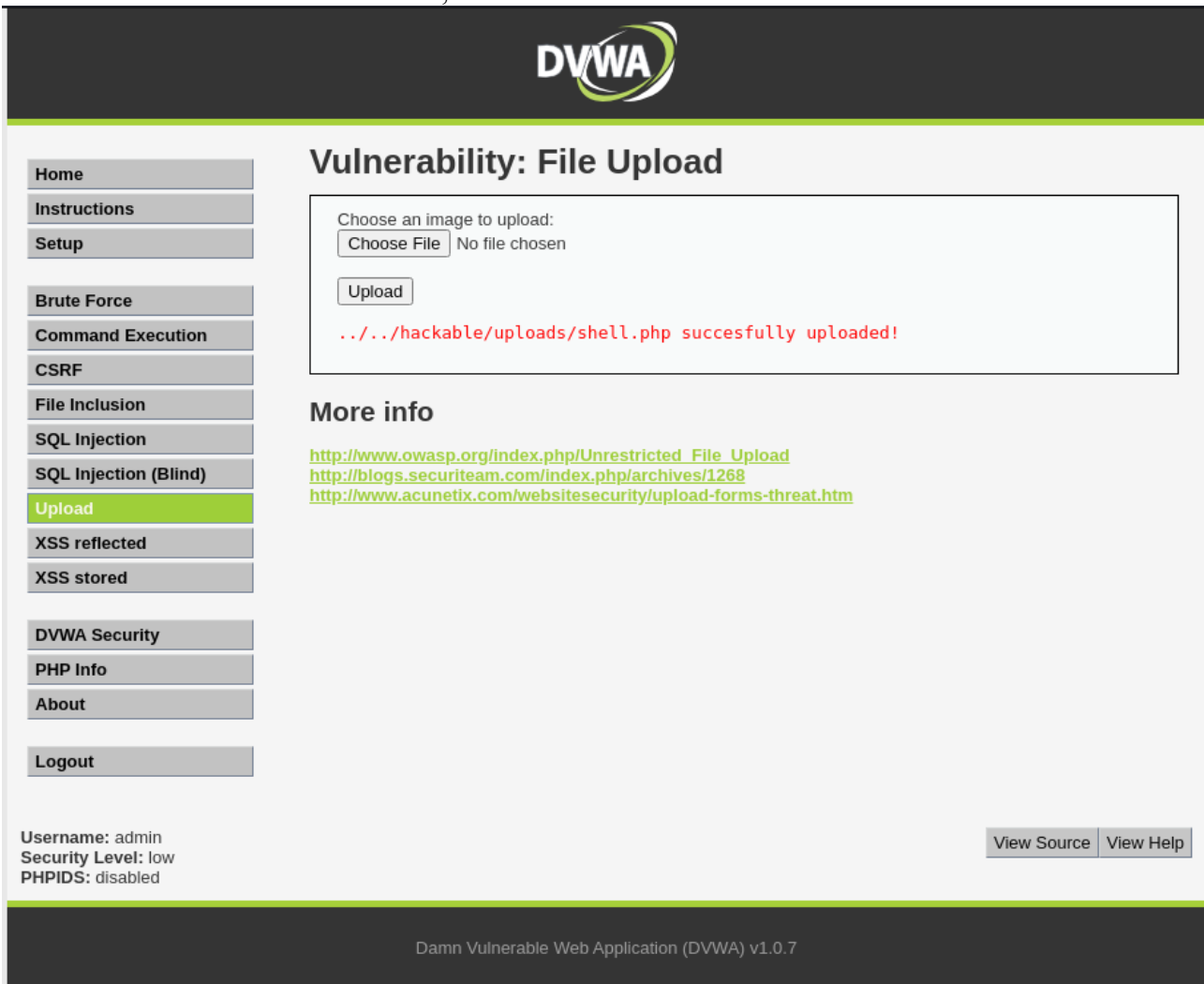


L'obiettivo di oggi è immettere una shell di comando sulla dvwa di metasploitable. Per farlo una volta ottenuto l'accesso alla dvwa impostiamo il livello di difficoltà su low e andiamo a inserirla nella sezione di download, sfruttando la vulnerabilità del caricare i file



DVWA

Vulnerability: File Upload

Choose an image to upload:
 No file chosen

..<../hackable/uploads/shell.php succesfully uploaded!

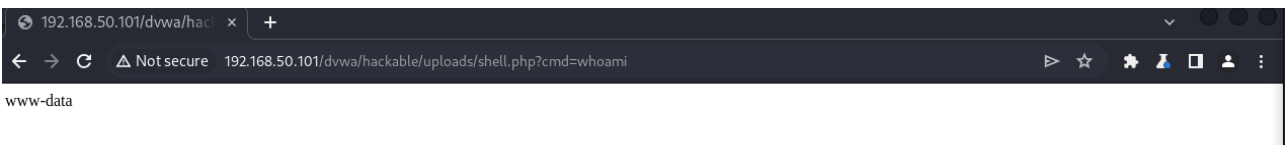
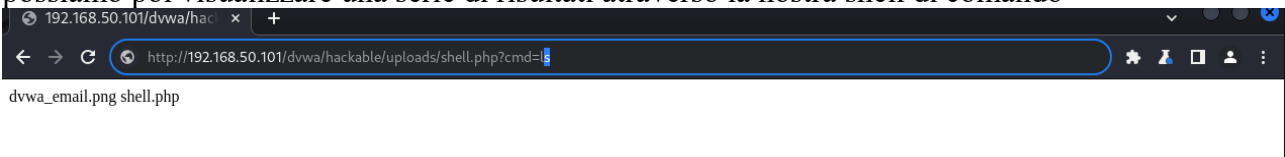
More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>

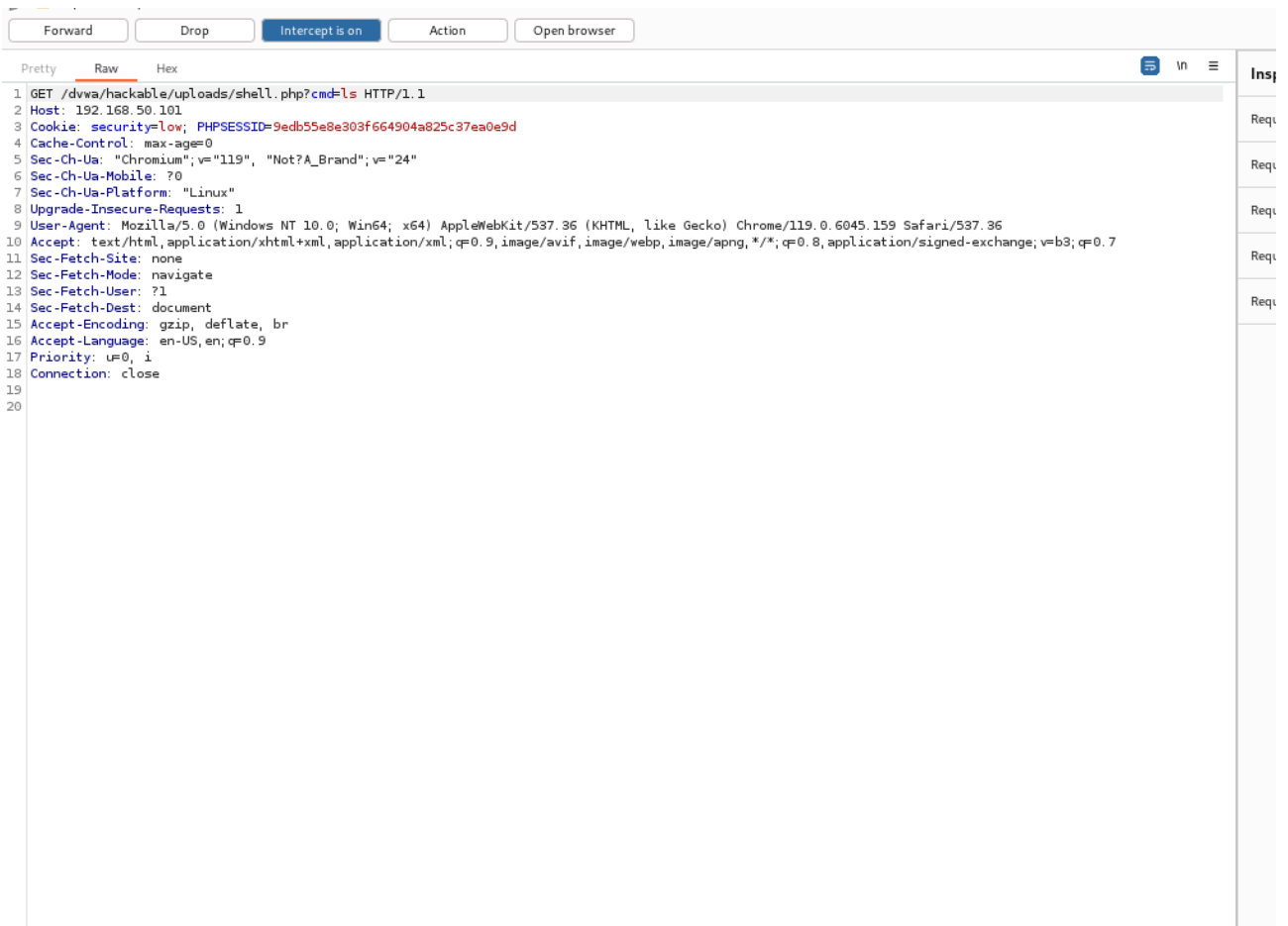
Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

possiamo poi visualizzare una serie di risultati attraverso la nostra shell di comando



qui possiamo vedere un esempio di come viene mandato un pacchetto attraverso burp



all'interno del sito abbiamo trovato anche una mail

