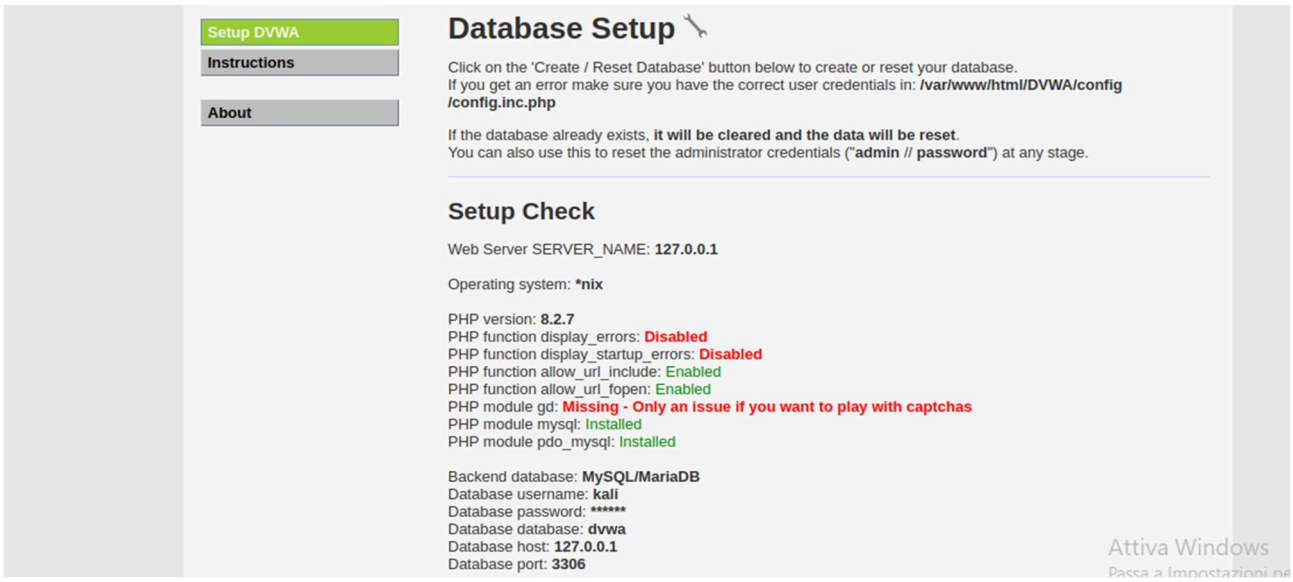
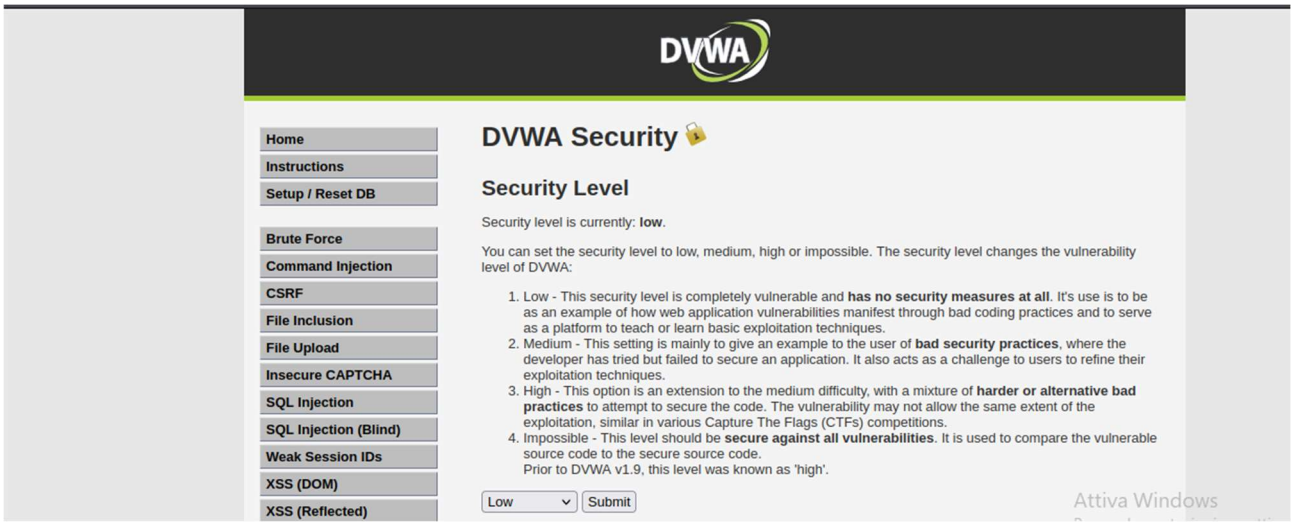
```
 GNU nano 7.2                                                    config.in
<?php
# If you are having problems connecting to the MySQL database and all of the variables
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem du
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during s
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DV
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_DVWA[ 'db_port']      = '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
```

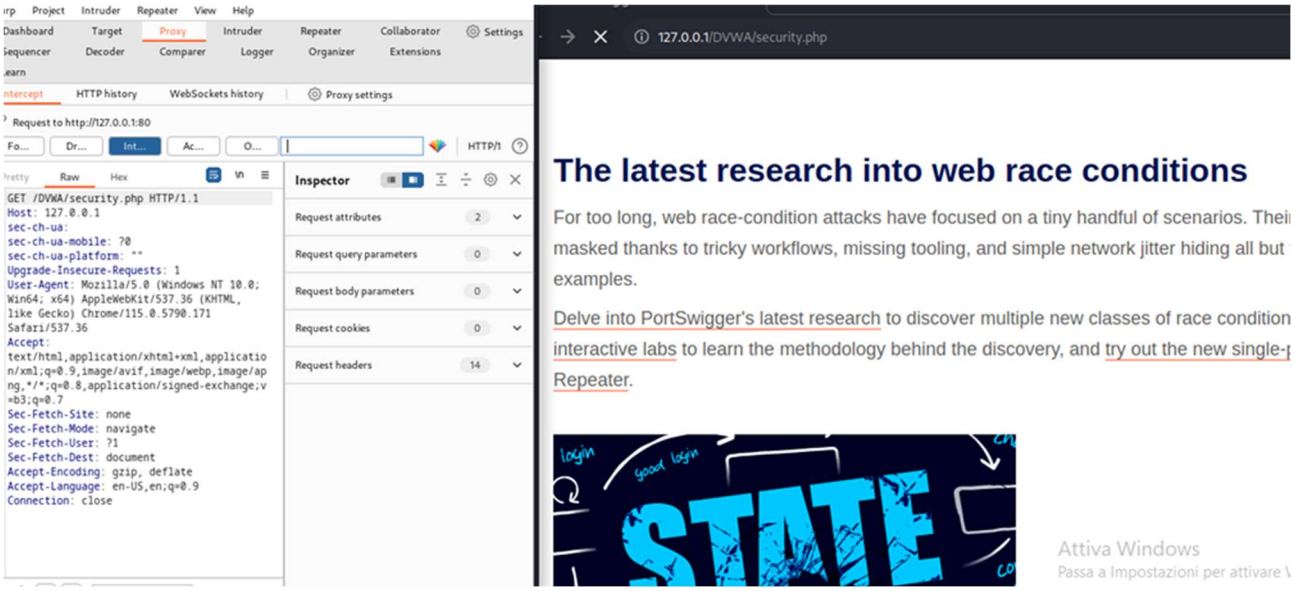
```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service mysql start

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.4-MariaDB-1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service apache2 start

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2

┌──(root㉿kali)-[/etc/php]
└─# cd /etc/php/8.2/apache2

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─#
```

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2

┌──(root㉿kali)-[/etc/php]
└─# cd /etc/php/8.2/apache2

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# nano php.ini

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# nano php.ini

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# service apache2 start

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─#
```


Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/DVWA/config/config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.
Setup Check
Web Server SERVER_NAME: 127.0.0.1
Operating system: *nix
PHP version: 8.2.7
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Backend database: MySQL/MariaDB
Database username: kali
Database password: ******
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
Attiva Windows


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
DVWA Security
Security Level
Security level is currently: low.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Low
Submit
Attiva Windows



Pretty Raw Hex

```
1  POST /DVWA/login.php HTTP/1.1
2  Host: 127.0.0.1
3  Content-Length: 88
4  Cache-Control: max-age=0
5  sec-ch-ua:
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: ""
8  Upgrade-Insecure-Requests: 1
9  Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=ag5v3hgrd5369o6ilc5hvkfc6u
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=88075c41c1c4addaf5d751c77c6446b8
```

Request

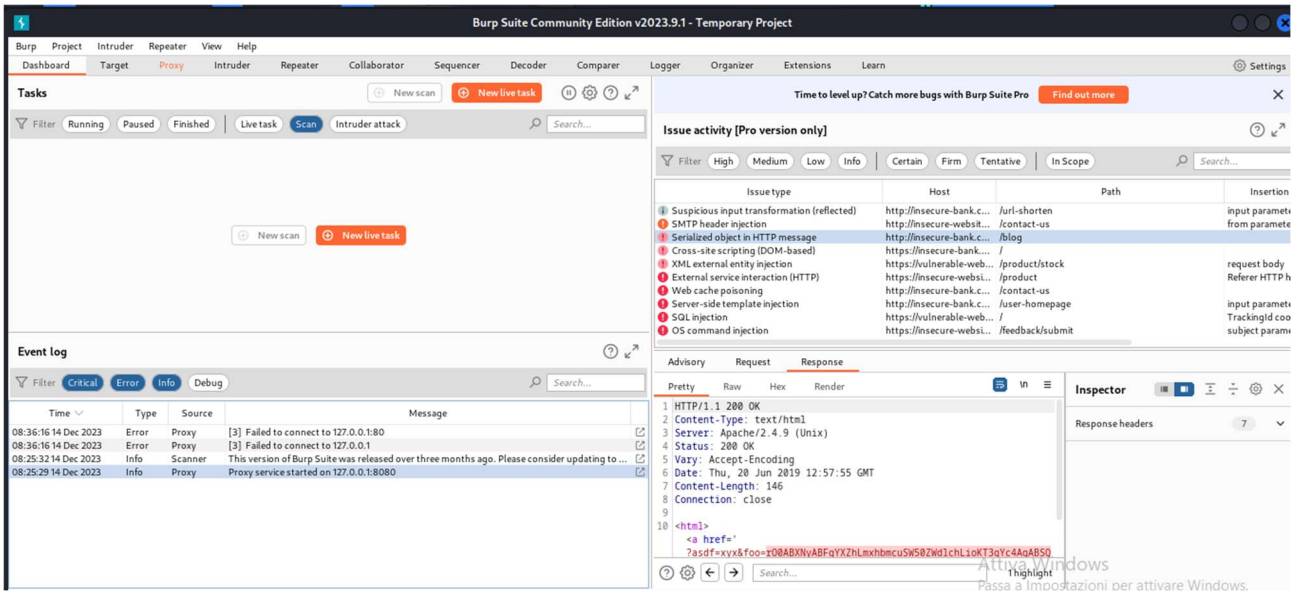
Pretty Raw Hex

```
1  GET /DVWA/login.php HTTP/1.1
2  Host: 127.0.0.1
3  Cache-Control: max-age=0
4  sec-ch-ua:
5  sec-ch-ua-mobile: ?0
6  sec-ch-ua-platform: ""
7  Upgrade-Insecure-Requests: 1
8  Origin: http://127.0.0.1
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=ag5v3hgrd5369o6ilc5hvkfc6u
19 Connection: close
20
21
```

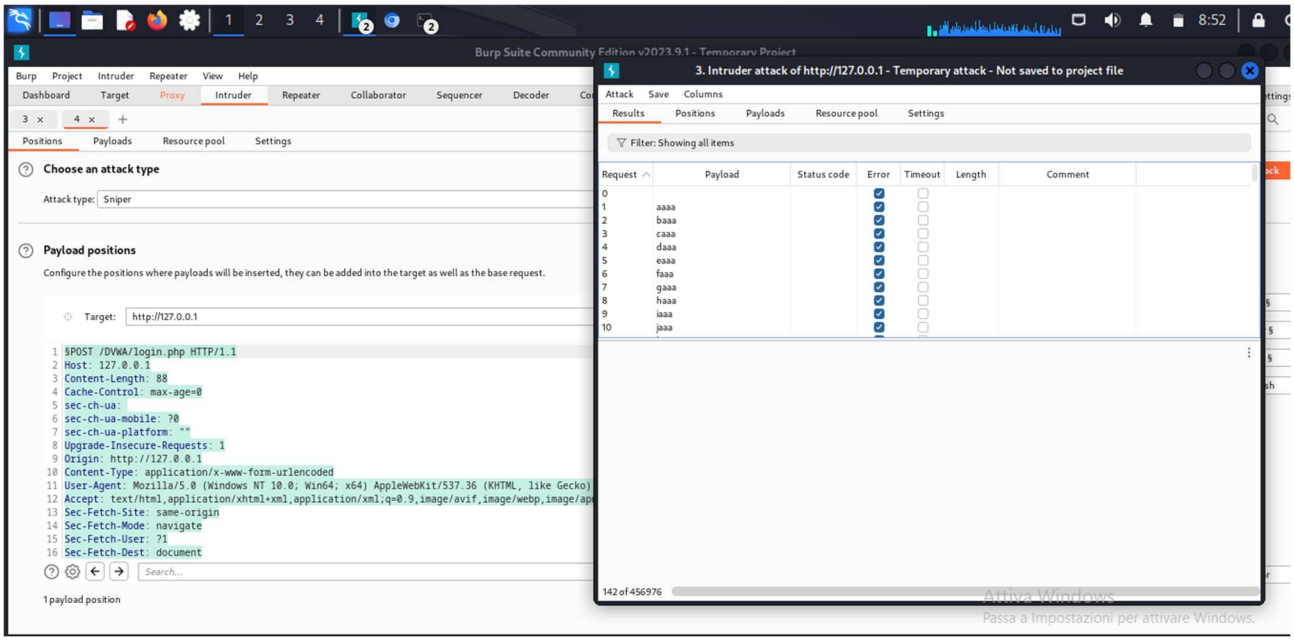
Response

Pretty Raw Hex Render

```
                <input type="submit" value="Login" name="Login">
              </p>
54
55          </fieldset>
56
57          <input type='hidden' name='user_token' value='
            37084ace5df6337ae2ed4b7de26af375' />
58
59        </form>
60
61        <br />
62
63        <div class="message">
            Login failed
          </div>
64
65        <br />
66        <br />
67        <br />
68        <br />
69        <br />
70        <br />
71        <br />
72        <br />
73
74      </div >
        <!--<div id="content">-->
```


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Search...
New scan
New live task
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative In Scope
Search...
Issue type Host Path Insertion
Suspicious input transformation (reflected) http://insecure-bank.c... /url-shorten input parameter
SMTP header injection http://insecure-websit... /contact-us from parameter
Serialized object in HTTP message http://insecure-bank.c... /blog
Cross-site scripting (DOM-based) https://insecure-bank.... /
XML external entity injection https://vulnerable-web... /product/stock request body
External service interaction (HTTP) https://insecure-websi... /product Referer HTTP h
Web cache poisoning http://insecure-bank.c... /contact-us
Server-side template injection http://insecure-bank.c... /user-homepage input parameter
SQL injection https://vulnerable-web... / TrackingId coo
OS command injection https://insecure-websi... /feedback/submit subject param
Event log
Filter Critical Error Info Debug
Search...
Time Type Source Message
08:36:16 14 Dec 2023 Error Proxy [3] Failed to connect to 127.0.0.1:80
08:36:16 14 Dec 2023 Error Proxy [3] Failed to connect to 127.0.0.1
08:25:32 14 Dec 2023 Info Scanner This version of Burp Suite was released over three months ago. Please consider updating to ...
08:25:29 14 Dec 2023 Info Proxy Proxy service started on 127.0.0.1:8080
Advisory Request Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Content-Type: text/html
3 Server: Apache/2.4.9 (Unix)
4 Status: 200 OK
5 Vary: Accept-Encoding
6 Date: Thu, 20 Jun 2019 12:57:55 GMT
7 Content-Length: 146
8 Connection: close
9
10 <html>
<a href='
?asdf=xyx&foo=rO0ABXNyABFqYXZhLmxhbmcuSW50ZWdlchLioKT3qYc4AqABSQ
Search...
1 highlight
Inspector
Response headers 7
Attiva Windows
Passa a Impostazioni per attivare Windows.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
3 × 4 ×
Positions Payloads Resource pool Settings
Choose an attack type
Attack type: Sniper
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://127.0.0.1
Update Host header to
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
Search...


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Positions Payloads Resource pool Settings
Choose an attack type
Attack type: Sniper
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://127.0.0.1
1 $POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
Search...
1 payload position
3. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status code Error Timeout Length Comment
0
1 aaaa
2 baaa
3 caaa
4 daaa
5 eaaa
6 faaa
7 gaaa
8 haaa
9 iaaa
10 jaaa
142 of 456976
Attiva Windows
Passa a Impostazioni per attivare Windows.