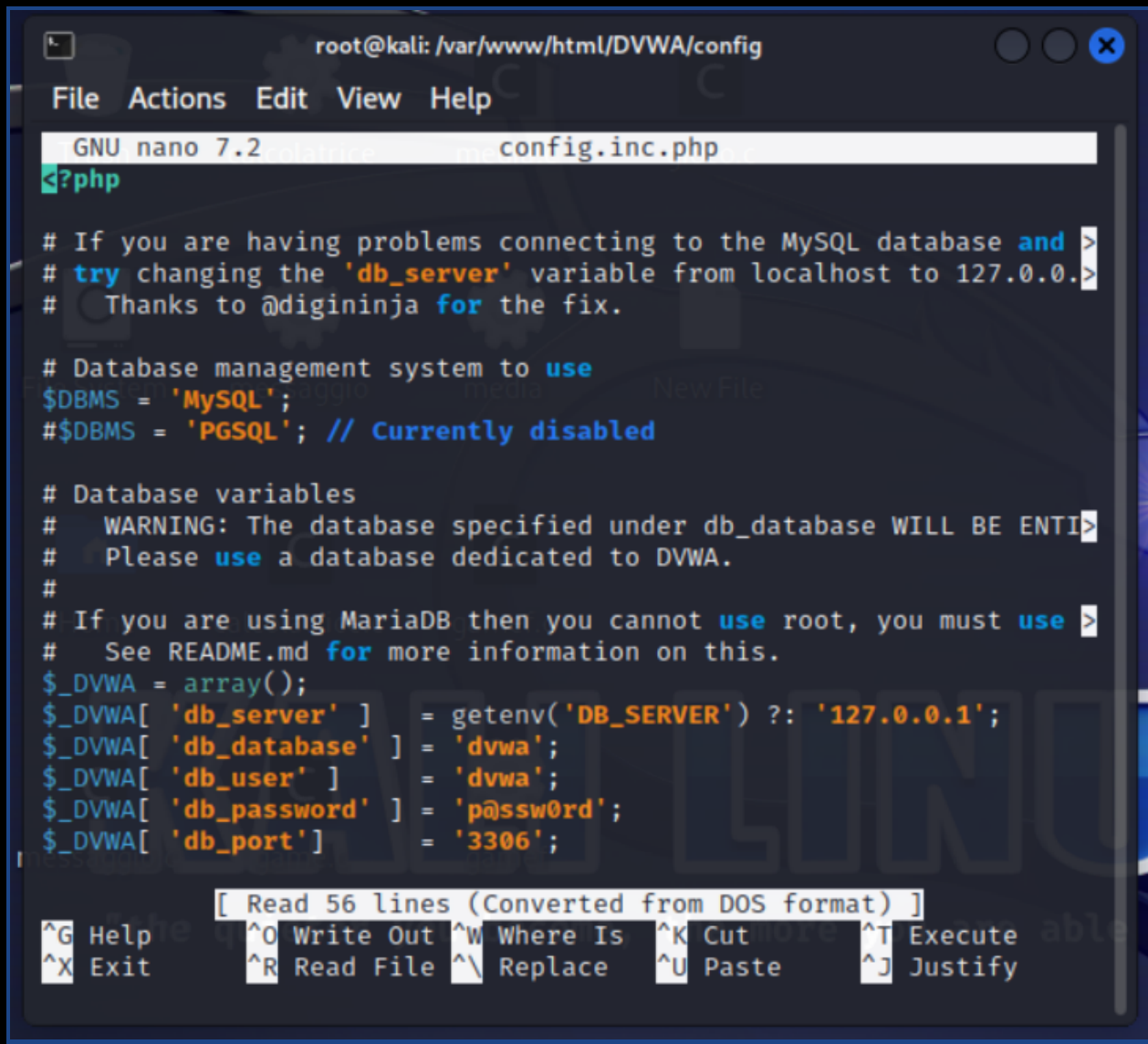


Pratica S3L2

Configurazione DVWA e utilizzo pratico del tool Burpsuite.

1°



```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 7.2 config.inc.php
<?php

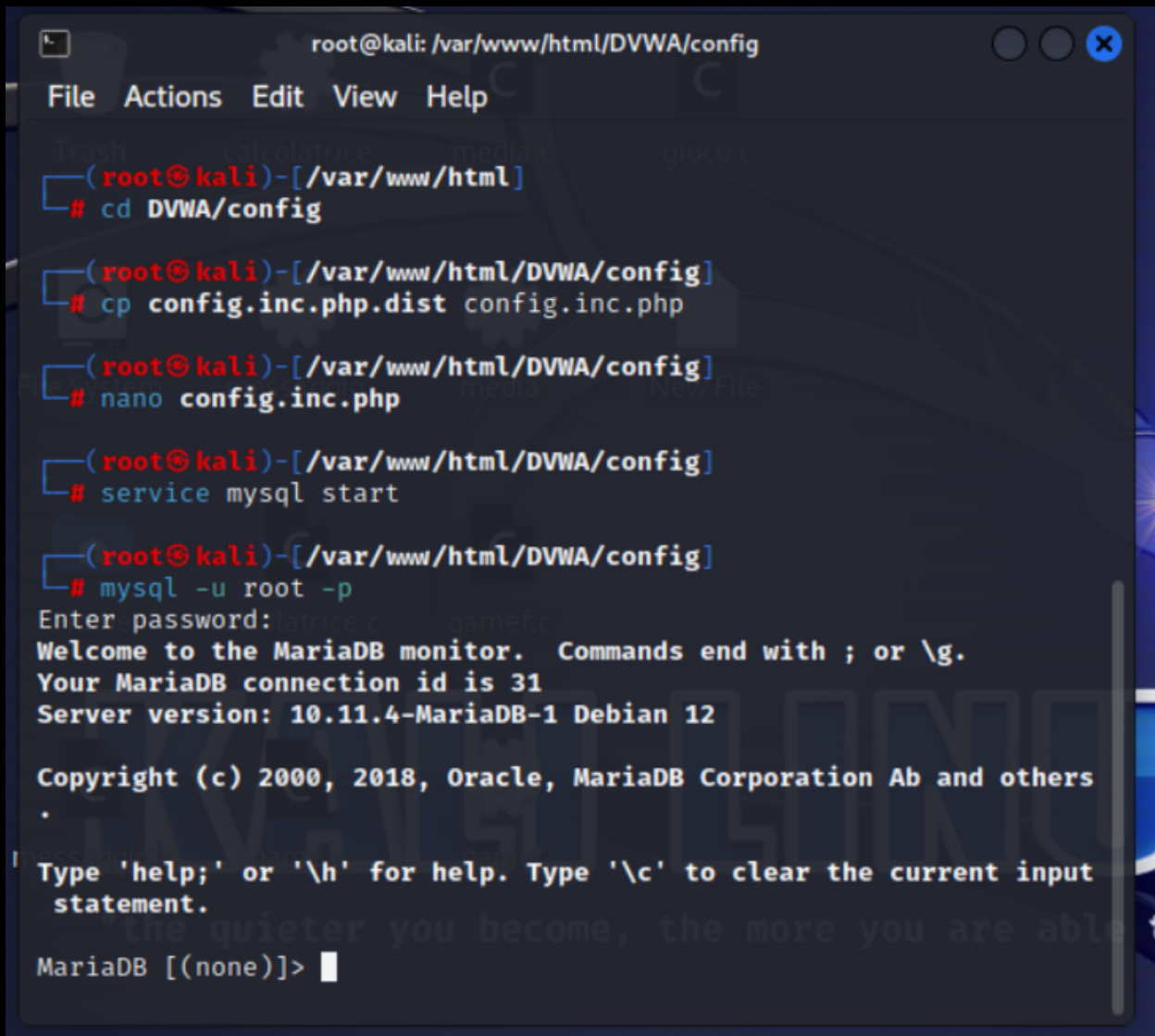
# If you are having problems connecting to the MySQL database and >
# try changing the 'db_server' variable from localhost to 127.0.0.1 >
# Thanks to @digininja for the fix.

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

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY >
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use >
# 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' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port' ] = '3306';

[ Read 56 lines (Converted from DOS format) ]
^G Help ^O Write Out ^W Where Is ^K Cut more ^T Execute able
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

2°

A terminal window titled 'root@kali: /var/www/html/DVWA/config' with standard window controls. The terminal shows a series of commands being executed to set up DVWA. The commands are: 'cd DVWA/config', 'cp config.inc.php.dist config.inc.php', 'nano config.inc.php', 'service mysql start', and 'mysql -u root -p'. After the last command, the MySQL/MariaDB monitor interface is shown, including a password prompt, a welcome message, connection ID, server version, copyright notice, and help instructions. The prompt 'MariaDB [(none)]>' is at the bottom with a cursor.

```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
Trash calculatrice media.c groco.c
(root@kali)-[/var/www/html]
# cd DVWA/config
(root@kali)-[/var/www/html/DVWA/config]
# cp config.inc.php.dist config.inc.php
(root@kali)-[/var/www/html/DVWA/config]
# nano config.inc.php
(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)]>
```

3°

```
root@kali: /home/kali
File Actions Edit View Help
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)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
'> Ctrl-C -- exit!
Aborted

(kali@kali)-[/home/kali]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 46
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)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
Query OK, 0 rows affected (0.059 sec)

MariaDB [(none)]> exit
Bye

(kali@kali)-[/home/kali]
#
```

4°

```
root@kali: /etc/php/8.2/apache2
File Actions Edit View Help
chmod: changing permissions of 'php.ini': Operation not permitted

(kali@kali)-[/etc/php/8.2/apache2]
$ sudo su
[sudo] password for kali:
(kali@kali)-[/etc/php/8.2/apache2]
# edit php.ini
Warning: unknown mime-type for "php.ini" -- using "application/octet-stream"
Error: no "edit" mailcap rules found for type "application/octet-stream"

(kali@kali)-[/etc/php/8.2/apache2]
# chmod +rx php.ini

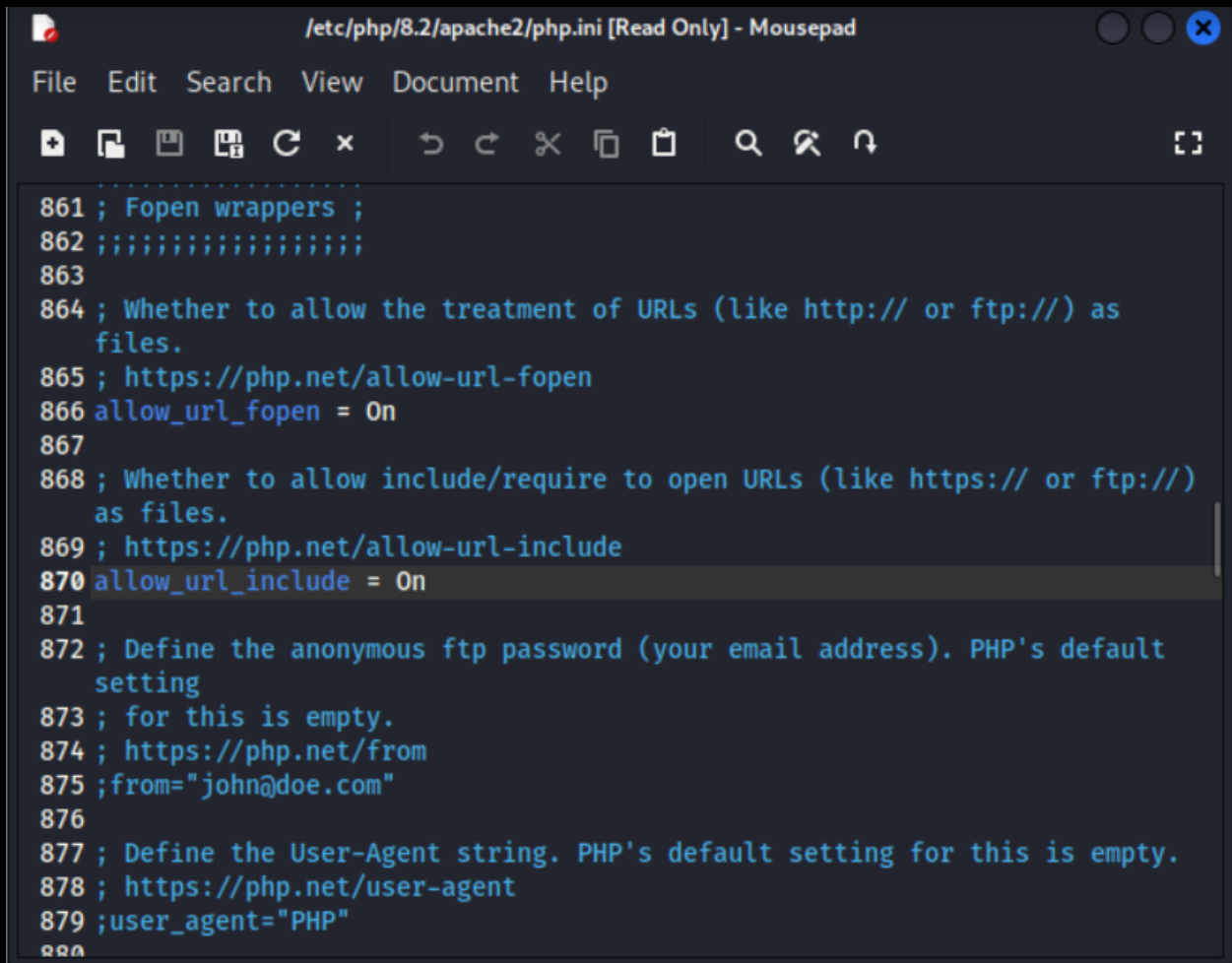
(kali@kali)-[/etc/php/8.2/apache2]
# edit php.ini
Warning: unknown mime-type for "php.ini" -- using "application/octet-stream"
Error: no "edit" mailcap rules found for type "application/octet-stream"

(kali@kali)-[/etc/php/8.2/apache2]
# open php.ini

(kali@kali)-[/etc/php/8.2/apache2]
#
(mousepad:39547): dconf-WARNING **: 10:25:11.645: failed to commit changes to dconf: Fa
iled to execute child process "dbus-launch" (No such file or directory)

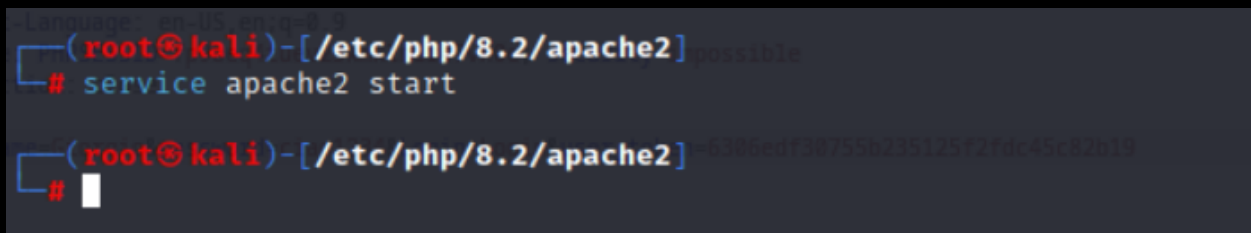
(mousepad:39547): dconf-WARNING **: 10:25:11.645: failed to commit changes to dconf: Fa
```

5°



```
/etc/php/8.2/apache2/php.ini [Read Only] - Mousepad
File Edit Search View Document Help
+ [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
861 ; Fopen wrappers ;
862 ;;;;;;;;;;;;;;;;;;;;;;;;;
863
864 ; Whether to allow the treatment of URLs (like http:// or ftp://) as
    files.
865 ; https://php.net/allow-url-fopen
866 allow_url_fopen = On
867
868 ; Whether to allow include/require to open URLs (like https:// or ftp://)
    as files.
869 ; https://php.net/allow-url-include
870 allow_url_include = On
871
872 ; Define the anonymous ftp password (your email address). PHP's default
    setting
873 ; for this is empty.
874 ; https://php.net/from
875 ;from="john@doe.com"
876
877 ; Define the User-Agent string. PHP's default setting for this is empty.
878 ; https://php.net/user-agent
879 ;user_agent="PHP"
880
```

6°



```
Language: en-US en-US.UTF-8
[ (root@kali)-[/etc/php/8.2/apache2] possible
# service apache2 start

[ (root@kali)-[/etc/php/8.2/apache2] -6386edf38755b235125f2fdc45c82b19
# ]
```

7°

The screenshot displays the Burp Suite Community Edition v2023.9.1 interface. The top menu bar includes File, Macchina, Visualizza, Inserimento, Dispositivi, and Aiuto. The main toolbar shows various icons for navigation and analysis. The interface is divided into several panels:

- Top Panel:** Contains tabs for Dashboard, Target, Proxy (selected), Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, and Settings.
- Left Panel:** Includes tabs for Intercept (selected), HTTP history, WebSockets history, and Proxy settings.
- Request Details:** Shows a request to http://127.0.0.1:80. The request is a POST to /DVWA/login.php. The raw data is displayed in the main pane, showing headers and a body with login credentials.
- Inspector Panel:** Located on the right, it shows details for the selected request, including Request attributes (2), Request query parameters (0), Request body parameters (4), Request cookies (2), and Request headers (20).

The raw request data is as follows:

```
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
12 Gecko) Chrome/115.0.5790.171 Safari/537.36
13 Accept:
14 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
15 */*;q=0.8,application/signed-exchange;v=b3;q=0.7
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Sec-Fetch-Dest: document
20 Referer: http://127.0.0.1/DVWA/login.php
21 Accept-Encoding: gzip, deflate
22 Accept-Language: en-US,en;q=0.9
23 Cookie: security=impossible; PHPSESSID=fp9beq4tuev25kmln1r47vh0e
24 Connection: close
25
26 username=admin&password=password&Login=Login&user_token=
27 a6a6ba857c8775a5ae8af5c9ba0b147a
```

8°

```
Cookie: PHPSESSID=fp9beq4tuev25kmln1r47vh0e; security=impossible
Connection: close

username=Giorgio&password=ciao1234&Login=Login&user_token=6306edf30755b235125f2fdc45c82b19
```

9°

The screenshot displays the Burp Suite Community Edition v2023.9.1 interface. The 'Repeater' tab is active, showing a single request and its corresponding response.

Request:

```
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/apn
  g,*/*;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=fp9beq4tuev25kmln1r47vh0e
19 Connection: close
20
21
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Tue, 12 Dec 2023 15:44:31 GMT
3 Server: Apache/2.4.57 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 1381
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12 <!DOCTYPE html>
13
14 <html lang="en-GB">
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
19
20 <title>
  Login :: Damn Vulnerable Web Application (DVWA)
  </title>
21
22 <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />
23
24 </head>
25
26 <body>
27
28 <div id="wrapper">
29
30 <div id="header">
```

The 'Inspector' panel on the right shows the following details:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 18
- Response headers: 9

The status bar at the bottom indicates 'Done' and '1,672 bytes | 77 millis'.

10°



Username

Password

Login

Login failed

