S3 L3

Svolgimento esercizio del 06/12/23

Giulia Salani

Consegna

Traccia:

Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux.

La DVWA ci sarà molto utile per i nostri test sia durante la build week 1 che durante lo sviluppo del modulo 2, dove vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

Svolgimento

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 10:24

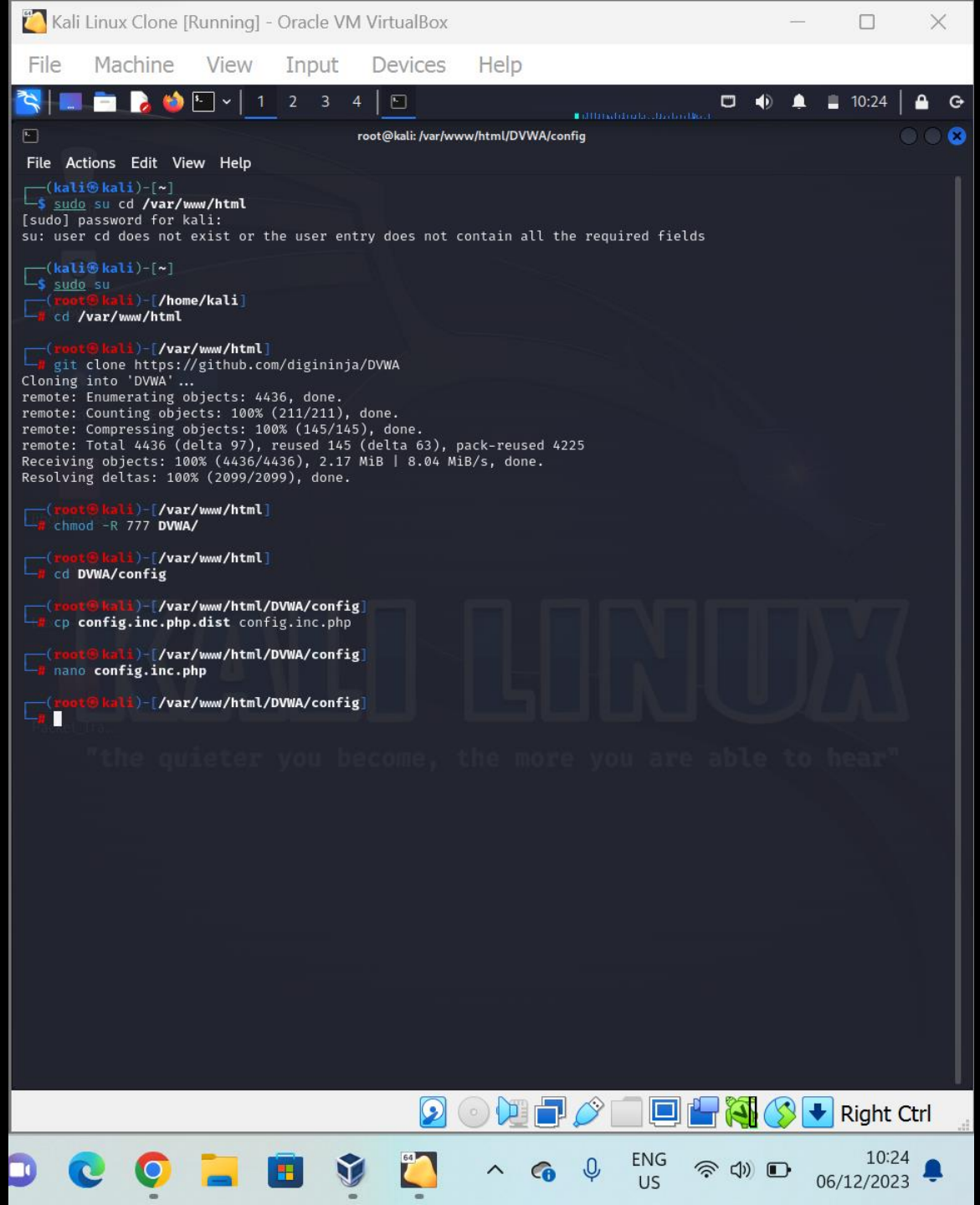
root@kali: /var/www/html/DVWA/config

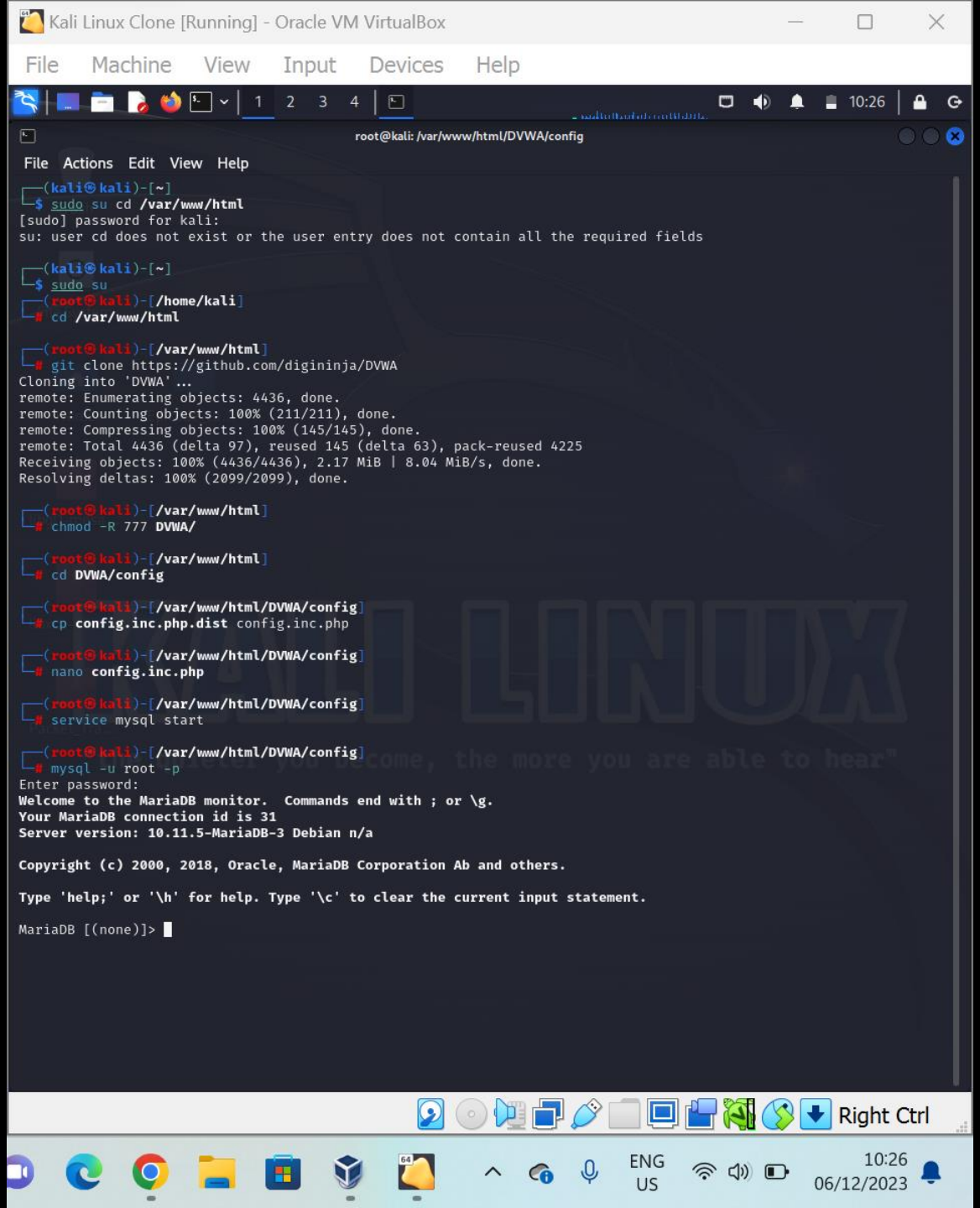
File Actions Edit View Help

```
  GNU nano 7.2                                  config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   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 setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   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
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = 'en';

# Disable authentication
#   Some tools don't like working with authentication and passing cookies around
#   so this setting lets you turn off authentication.
$_DVWA[ 'disable_authentication' ] = false;

define ('MYSQL', 'mysql');
define ('SQLITE', 'sqlite');

# SQLi DB Backend
#   Use this to switch the backend database used in the SQLi and Blind SQLi labs.
#   This does not affect the backend for any other services, just these two labs.
#   If you do not understand what this means, do not change it.
$_DVWA['SQLI_DB'] = MYSQL;

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```

Right Ctrl

ENG US 10:24 06/12/2023


Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:24
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su cd /var/www/html
[sudo] password for kali:
su: user cd does not exist or the user entry does not contain all the required fields
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]
cd /var/www/html
(root㉿kali)-[/var/www/html]
git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4436, done.
remote: Counting objects: 100% (211/211), done.
remote: Compressing objects: 100% (145/145), done.
remote: Total 4436 (delta 97), reused 145 (delta 63), pack-reused 4225
Receiving objects: 100% (4436/4436), 2.17 MiB | 8.04 MiB/s, done.
Resolving deltas: 100% (2099/2099), done.
(root㉿kali)-[/var/www/html]
chmod -R 777 DVWA/
(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]
#
"the quieter you become, the more you are able to hear"
Right Ctrl
ENG US
10:24
06/12/2023


Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:26
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su cd /var/www/html
[sudo] password for kali:
su: user cd does not exist or the user entry does not contain all the required fields
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]
cd /var/www/html
(root㉿kali)-[/var/www/html]
git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4436, done.
remote: Counting objects: 100% (211/211), done.
remote: Compressing objects: 100% (145/145), done.
remote: Total 4436 (delta 97), reused 145 (delta 63), pack-reused 4225
Receiving objects: 100% (4436/4436), 2.17 MiB | 8.04 MiB/s, done.
Resolving deltas: 100% (2099/2099), done.
(root㉿kali)-[/var/www/html]
chmod -R 777 DVWA/
(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: 10.11.5-MariaDB-3 Debian n/a
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)]>
Right Ctrl
ENG US
10:26 06/12/2023

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 10:30

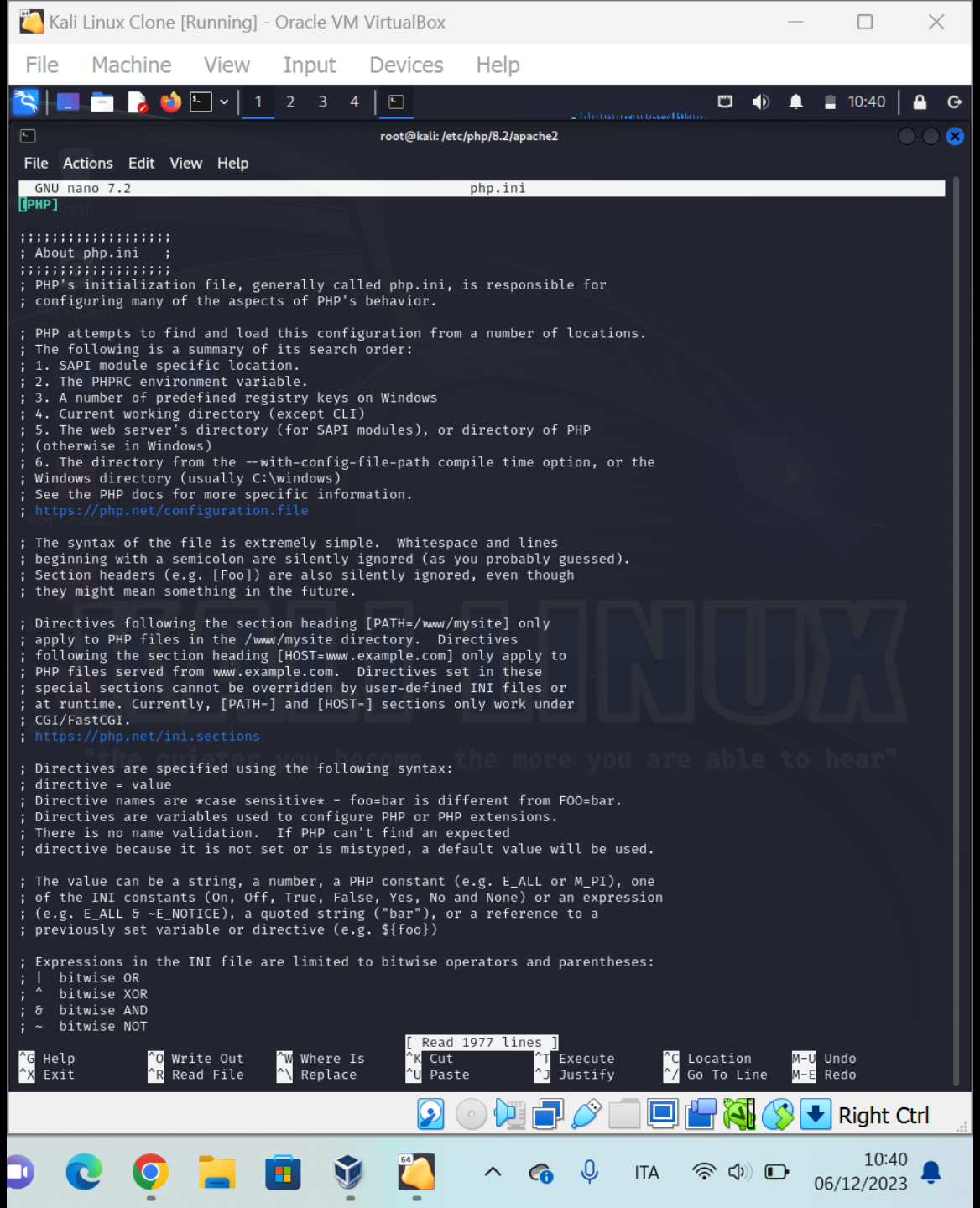
root@kali: /var/www/html/DVWA/config

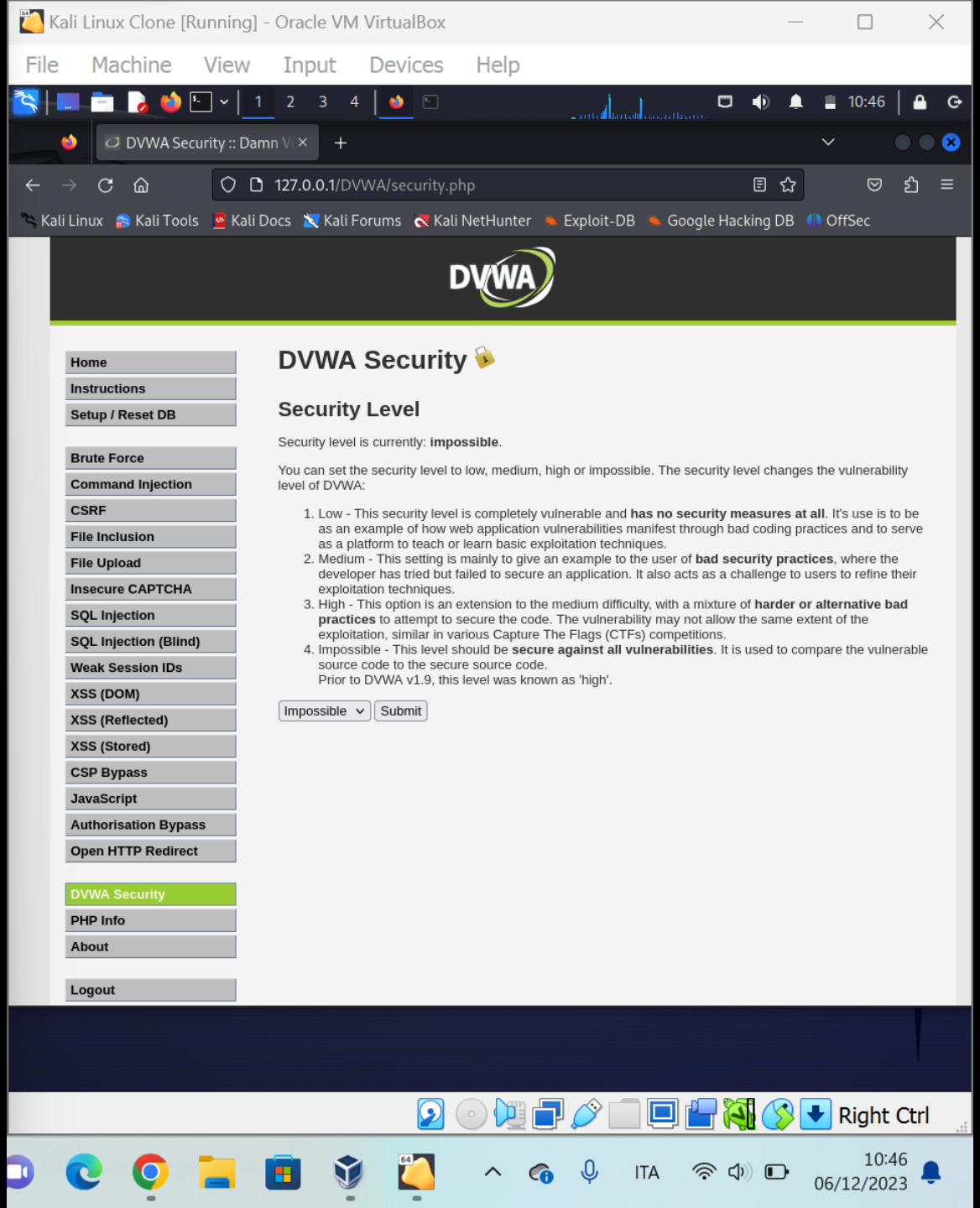
File Actions Edit View Help

```
└─$ sudo su cd /var/www/html
[sudo] password for kali:
su: user cd does not exist or the user entry does not contain all the required fields

┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4436, done.
remote: Counting objects: 100% (211/211), done.
remote: Compressing objects: 100% (145/145), done.
remote: Total 4436 (delta 97), reused 145 (delta 63), pack-reused 4225
Receiving objects: 100% (4436/4436), 2.17 MiB | 8.04 MiB/s, done.
Resolving deltas: 100% (2099/2099), done.

┌──(root㉿kali)-[/var/www/html]
└─# chmod -R 777 DVWA/

┌──(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: 10.11.5-MariaDB-3 Debian n/a

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)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.018 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> exit
Bye

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

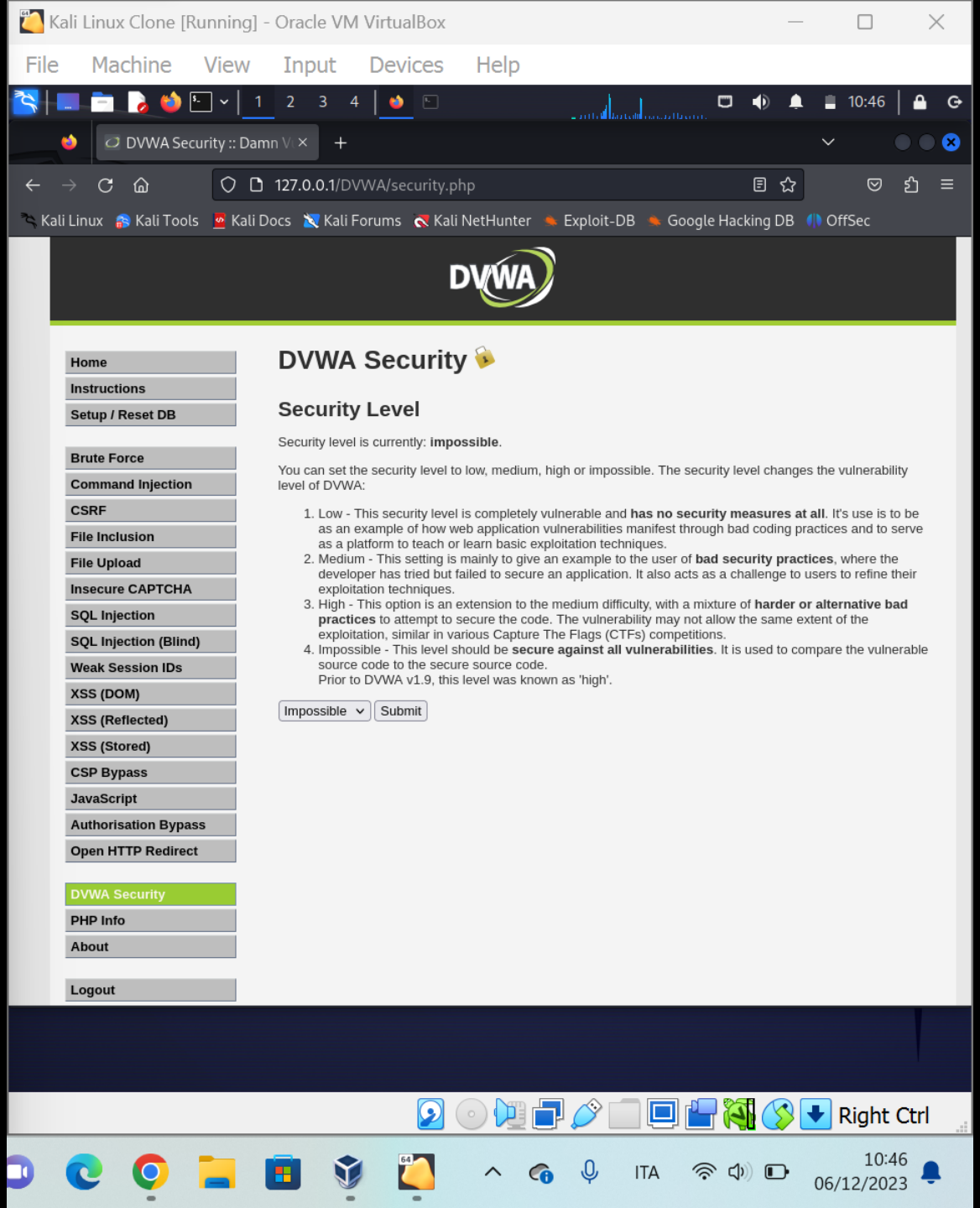
Right Ctrl

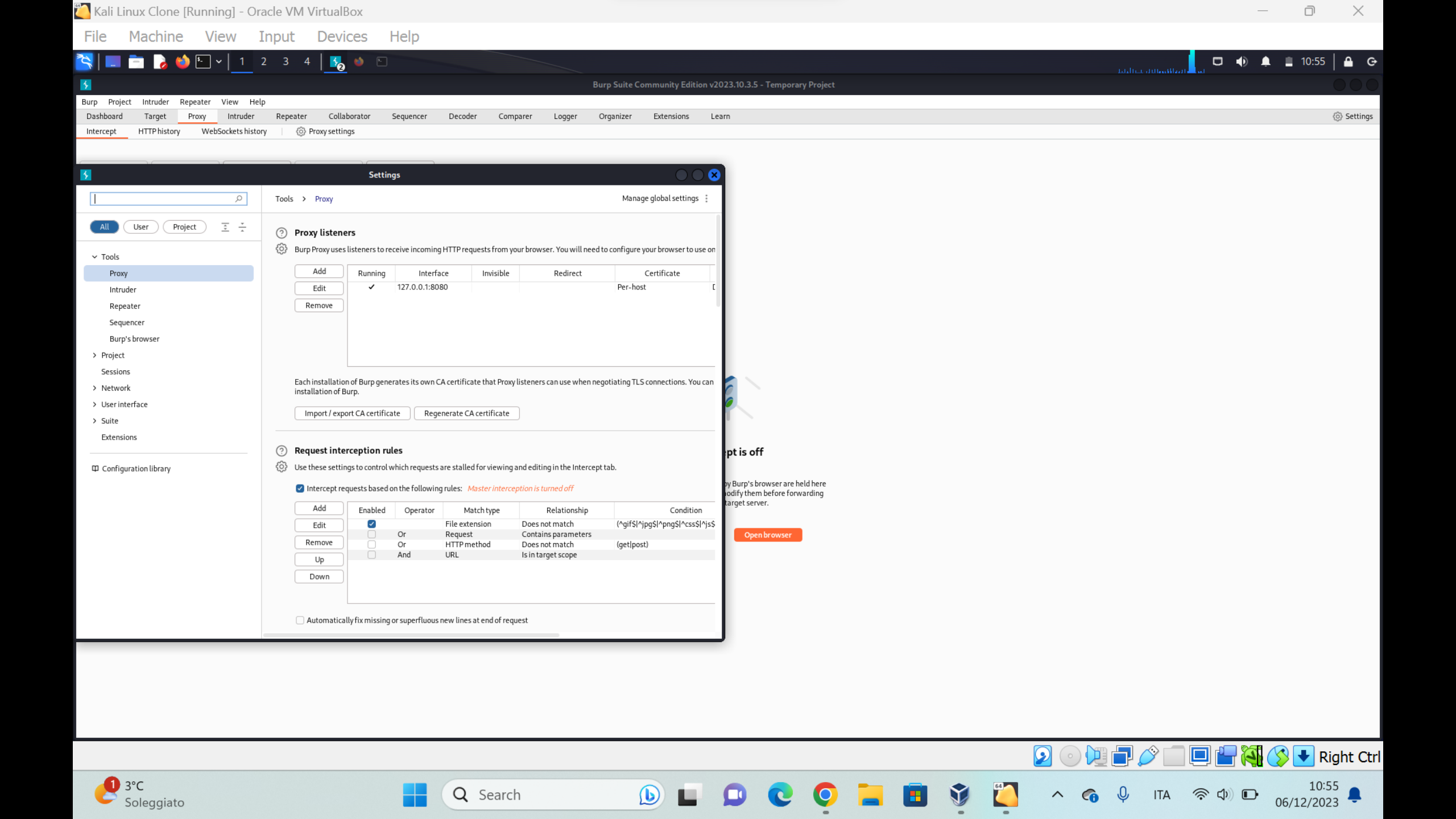
ITA 10:30 06/12/2023

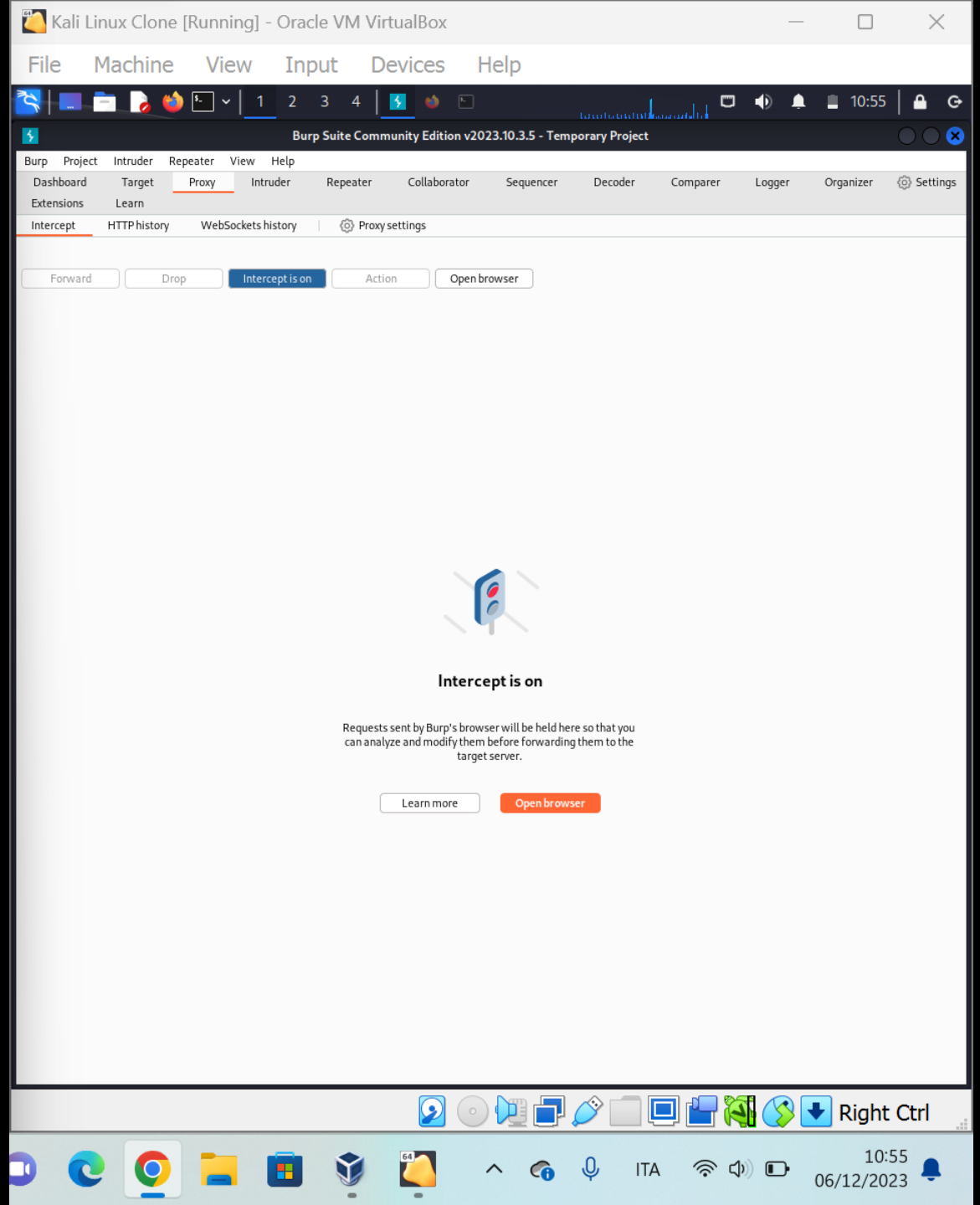

Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:40
root@kali: /etc/php/8.2/apache2
File Actions Edit View Help
GNU nano 7.2 php.ini
[PHP]
;;;;;;;;;;;;;;;;;;;
; About php.ini ;
;;;;;;;;;;;;;;;;;;;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.
; PHP attempts to find and load this configuration from a number of locations.
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable.
; 3. A number of predefined registry keys on Windows
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or the
; Windows directory (usually C:\windows)
; See the PHP docs for more specific information.
; https://php.net/configuration.file
; The syntax of the file is extremely simple. Whitespace and lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
; they might mean something in the future.
; Directives following the section heading [PATH=/www/mysite] only
; apply to PHP files in the /www/mysite directory. Directives
; following the section heading [HOST=www.example.com] only apply to
; PHP files served from www.example.com. Directives set in these
; special sections cannot be overridden by user-defined INI files or
; at runtime. Currently, [PATH=] and [HOST=] sections only work under
; CGI/FastCGI.
; https://php.net/ini.sections
; Directives are specified using the following syntax:
; directive = value
; Directive names are *case sensitive* - foo=bar is different from FOO=bar.
; Directives are variables used to configure PHP or PHP extensions.
; There is no name validation. If PHP can't find an expected
; directive because it is not set or is mistyped, a default value will be used.
; The value can be a string, a number, a PHP constant (e.g. E_ALL or M_PI), one
; of the INI constants (On, Off, True, False, Yes, No and None) or an expression
; (e.g. E_ALL & ~E_NOTICE), a quoted string ("bar"), or a reference to a
; previously set variable or directive (e.g. ${foo})
; Expressions in the INI file are limited to bitwise operators and parentheses:
; | bitwise OR
; ^ bitwise XOR
; & bitwise AND
; ~ bitwise NOT
[Read 1977 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Right Ctrl
ITA
10:40
06/12/2023

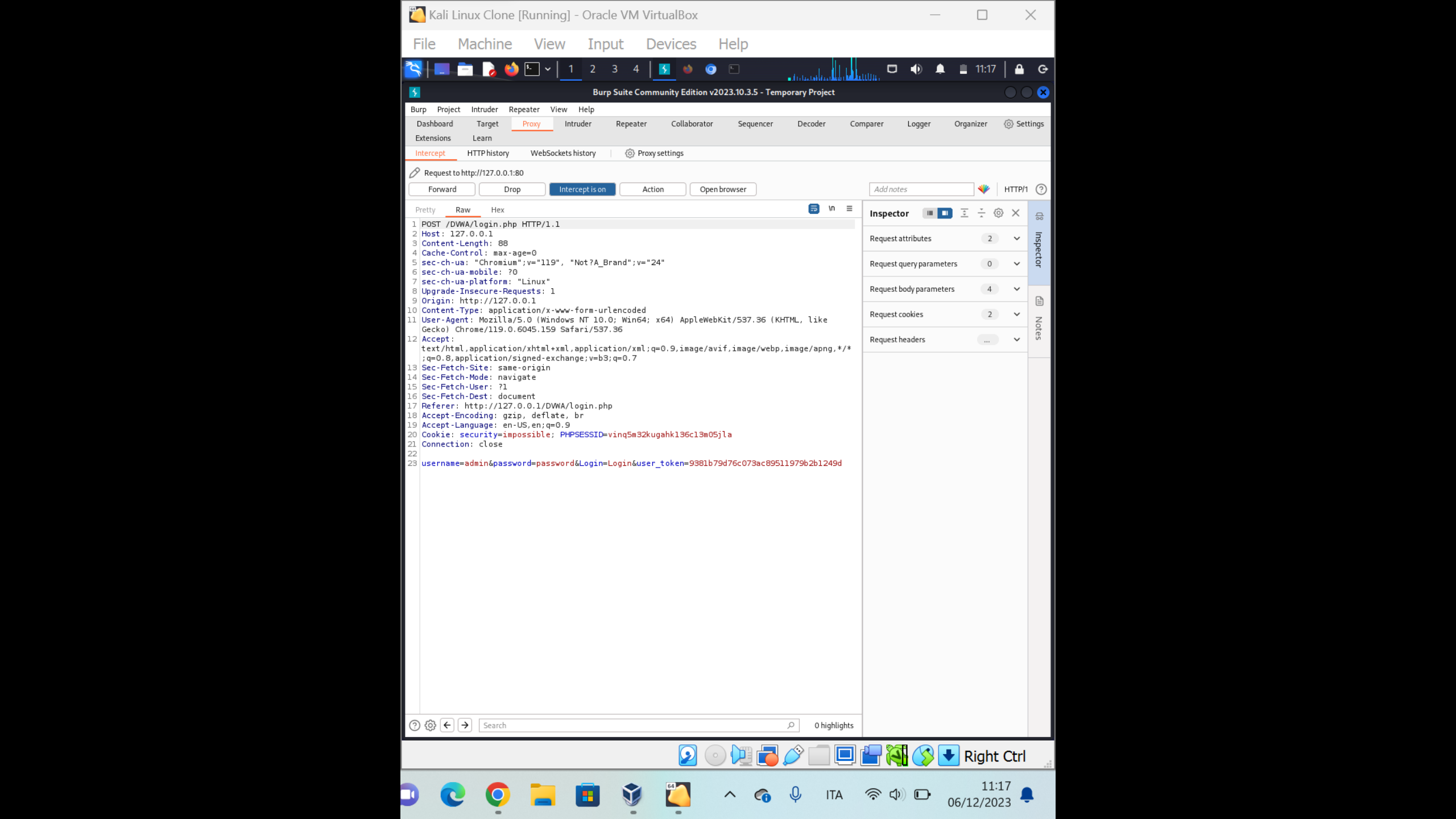

Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:46
DVWA Security :: Damn V
127.0.0.1/DVWA/security.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
DVWA Security
Security Level
Security level is currently: impossible.
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'.
Impossible
Submit
Right Ctrl
ITA
10:46
06/12/2023

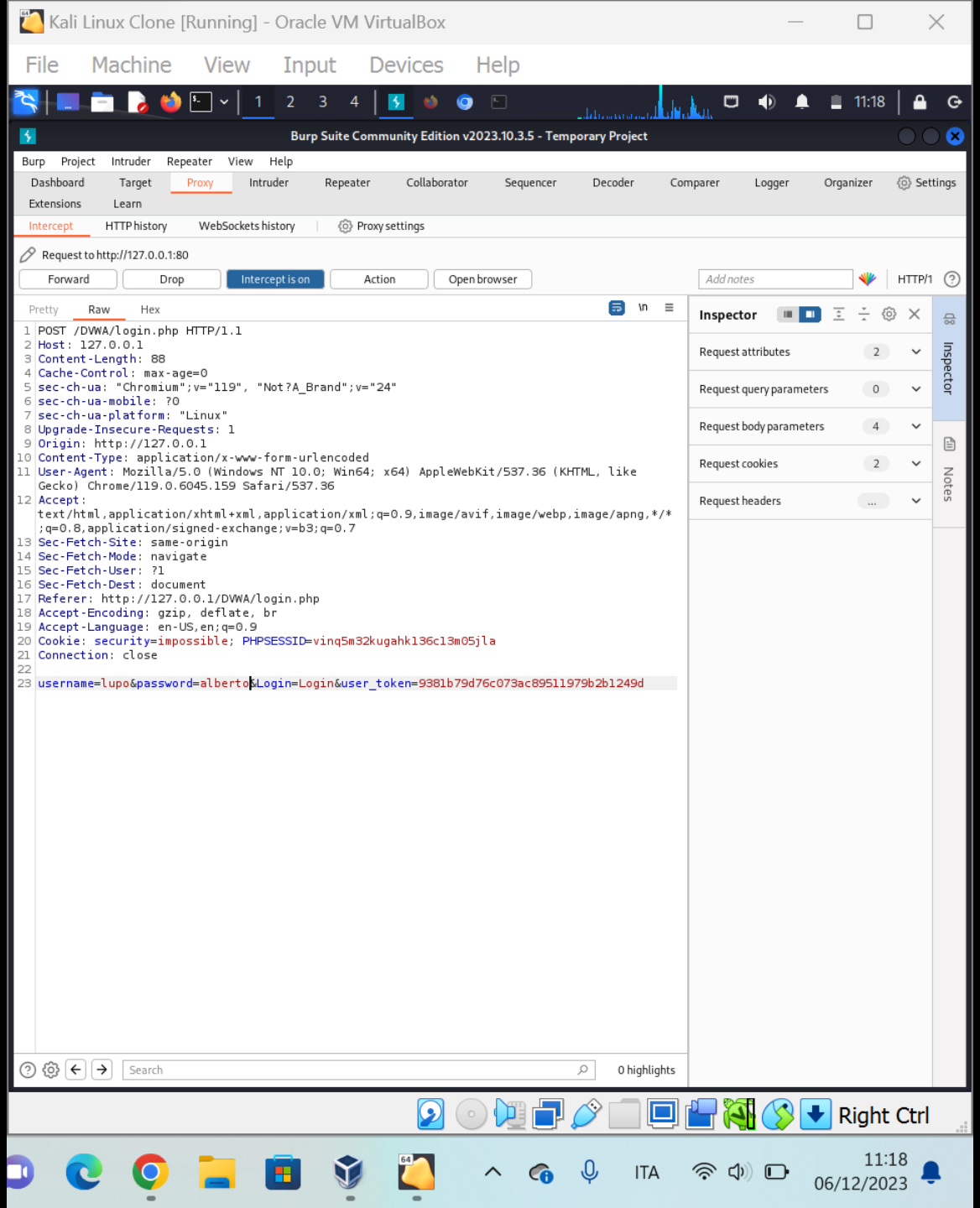

Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:49
root@kali: /etc/php/8.2/apache2
File Actions Edit View Help
└─# cd DVWA/config
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# 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: 10.11.5-MariaDB-3 Debian n/a
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)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.018 sec)
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.004 sec)
MariaDB [(none)]> exit
Bye
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php
┌──(root㉿kali)-[/etc/php]
└─# ls
8.2
┌──(root㉿kali)-[/etc/php]
└─# service apache2 start
┌──(root㉿kali)-[/etc/php]
└─# cd /etc/php/8.2/apache2
┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# ls
conf.d 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]
└─#
Right Ctrl
ITA
10:49
06/12/2023


Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:46
DVWA Security :: Damn V
127.0.0.1/DVWA/security.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
DVWA Security
Security Level
Security level is currently: impossible.
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'.
Impossible
Submit
Right Ctrl
ITA
10:46
06/12/2023


Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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
Settings
Tools > Proxy
Manage global settings
All User Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Suite
Extensions
Configuration library
Proxy listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use on
Add
Edit
Remove
Running Interface Invisible Redirect Certificate
127.0.0.1:8080 Per-host
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can
installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Request interception rules
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules: Master interception is turned off
Add
Edit
Remove
Up
Down
Enabled Operator Match type Relationship Condition
File extension Does not match (^gif$|^jpg$|^png$|^css$|^js$
Or Request Contains parameters
Or HTTP method Does not match (get|post)
And URL Is in target scope
Automatically fix missing or superfluous new lines at end of request
pt is off
by Burp's browser are held here
odify them before forwarding
target server.
Open browser
Right Ctrl
3°C
Soleggiato
Search
ITA
10:55
06/12/2023


Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:55
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 Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser
Right Ctrl
ITA
10:55
06/12/2023


Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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 Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/1
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: "Chromium";v="119", "Not?A_Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
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/119.0.6045.159 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, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=vinq5m32kugahk136c13m05jla
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=9381b79d76c073ac89511979b2b1249d
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers ...
Search
0 highlights
Right Ctrl
ITA
11:17
06/12/2023


Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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 Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/1
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: "Chromium";v="119", "Not?A_Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
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/119.0.6045.159 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, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=vinq5m32kugahk136c13m05jla
21 Connection: close
22
23 username=lupo&password=alberto&Login=Login&user_token=9381b79d76c073ac89511979b2b1249d
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers ...
Search
0 highlights
Right Ctrl
ITA
11:18
06/12/2023

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

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 Settings

Extensions Learn

Send Cancel

Target: http://127.0.0.1 HTTP/1

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: "Chromium";v="119",
   "Not?A_Brand";v="24"
5  sec-ch-ua-mobile: ?0
6  sec-ch-ua-platform: "Linux"
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/119.0.6045.159
   Safari/537.36
10 Accept:
   text/html,application/xhtml+xml,applicatio
   n/xml;q=0.9,image/avif,image/webp,image/ap
   ng,*/*;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, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=
   vinq5m32kugahk136cl3m05jla
19 Connection: close
20
21
```

Search 0 highlights

Response

ty Raw Hex Render

```
54
55          </fieldset>
56
57          <input type='hidden' name='
            user_token' value='
            78f848ca9ba10b4b28ef8c95e885e7c1
            ' />
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">-->
75
76      <div id="footer">
77
78        <p>
            <a href="
            https://github.com/digininja/DVW
            A/" target="_blank">
              Damn Vulnerable Web
              Application (DVWA)
            </a>
          </p>
79
80      </div>
          <!--<div id="footer"> -->
81
82    </div>
        <!--<div id="wrapper"> -->
83
84  </body>
85
86 </html>
```

Search 0 highlights

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 18

Response headers 9

Inspector Notes

Done 1,672 bytes | 0 millis

Right Ctrl

ITA 11:20 06/12/2023