Web Application Security Testing -> **Report for the 20231211 lesson 1**

STATEMENT OF CONFIDENTIALITY

The contents of this document were developed by Selivonchik S. I believe that the contents of this document are not proprietary or business confidential information. This information should be used for educational purposes only. This document may be transferred to any other person without my prior consent. In addition, any part of this document may be transmitted, reproduced, copied or distributed without prior consent.

The contents of this document do not constitute legal advice and should not be construed as such. This is the result of my own educational process. The assessment detailed here is conducted on a fictitious company for training and testing purposes, and the vulnerabilities do not impact external or internal infrastructure in any way.

Introduction

Black Box Penetration Testing

For IT Academy WAST Course Lesson 1 V1.0

December 21th, 2023

By: Selivonchyk S

Document Properties

Title	Black Box Penetration Testing Report	Contacts
Version	V1.2	
Author	Selivonchyk S.	
Pen-testers	Selivonchyk S.	
Reviewed By	Kutaisov M.	
Approved By	Kutaisov M.	
Classification	Not confidential	

Version control

Version	Date	Author	Description
V1.0	Dec 21th, 2023	Selivonchyk Sergey	CTF

Table of Content

List Of Illustrations

- List of Tables

- List of Figures

1. EXECUTIVE SUMMARY

The IT Academy (*hereis "edu"*) provided Selivonchik S. with a special resource for training in conducting penetration testing of web applications in order to identify security weaknesses, capture the flag (*CTF*) and determine the degree of influence on them. As well as developing skills in documenting all research results in an understandable and reproducible form and developing skills in providing recommendations for correcting situations.

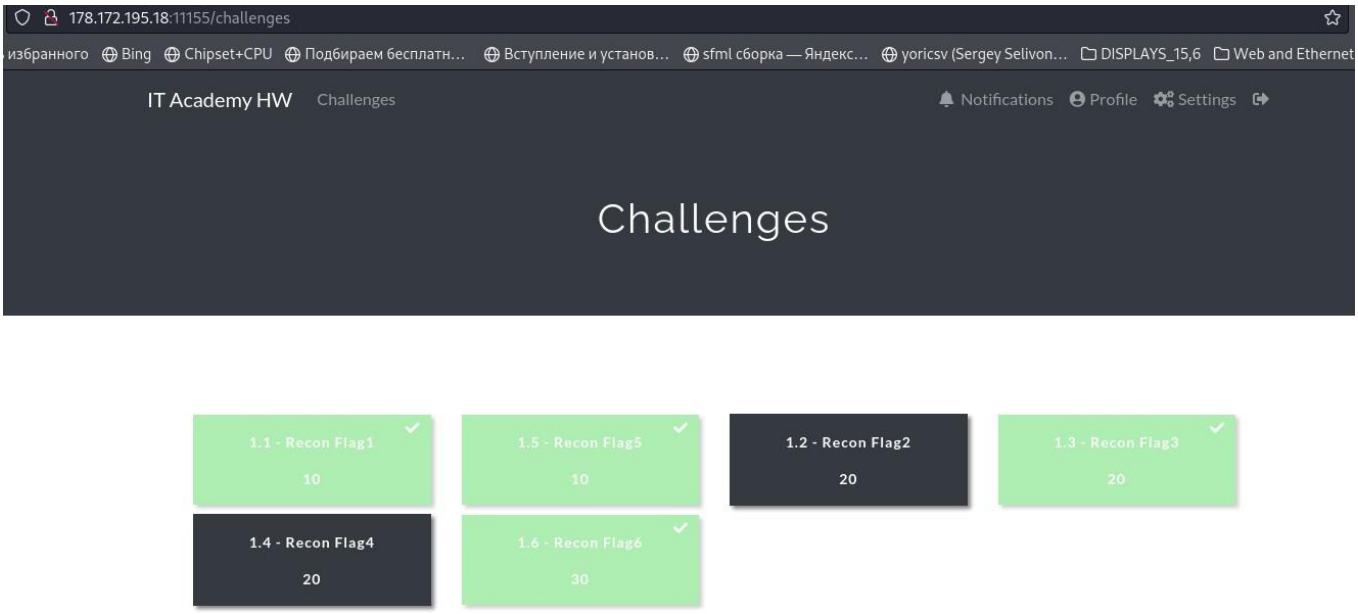


Figure 1 *Challenges*

Scope of work

This security assessment involves remote penetration testing of 1 available server located at *178.172.195.18 and port 11166*.

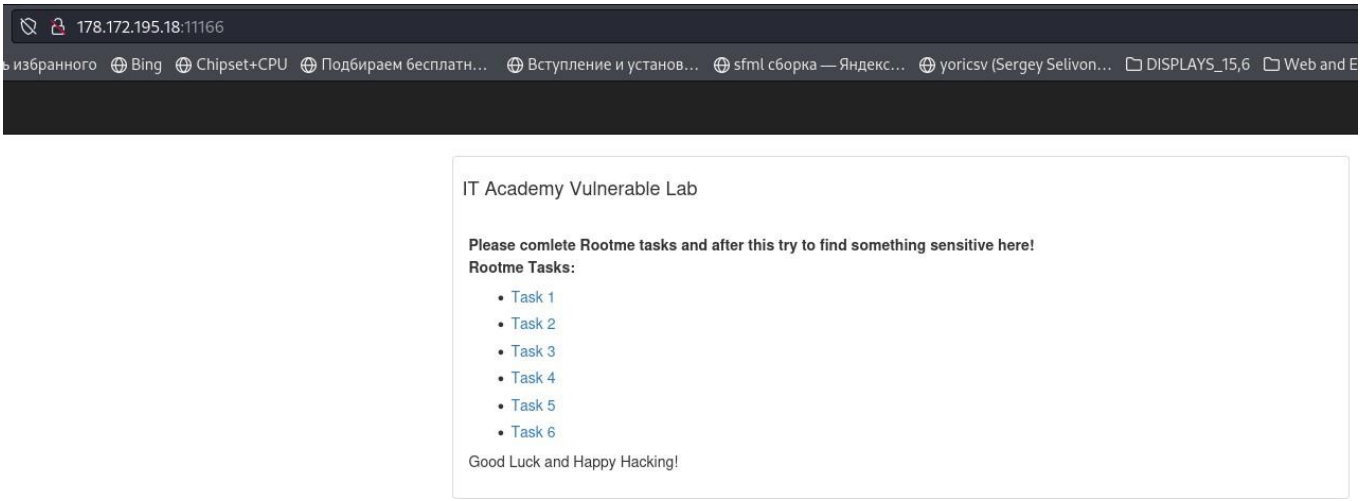


Figure 2 *Target*

The assessment was conducted from a "black box" perspective, without credentials or any advance knowledge of internally facing environment with the goal of identifying unknown weaknesses, with the only information provided being the IP address and port of the server being tested. No other information was assumed at the start of the assessment.

In-Scope Assets

Host/URL/IP Address/Port	Description
178.172.195.18:11166	IT Academy external resource

Table 1: *Scope details*

1.1 Project Objectives

posture, identify vulnerabilities and potential flaws in its design in order to capture as many flags (*CTF*) as possible. Testing was conducted remotely via a host dedicated to this evaluation. Each identified vulnerability is assigned a threat-based risk rating and manually reviewed to determine its potential for exploitation and escalation.

1.2 Assumption

When writing the report, we assume that a special resource will be in the public domain for a short period of time and signing a non-disclosure agreement (*NDA*) and rules of interaction with it does not make sense.

1.3 Timeline

The timeline of the test is as below:

Penetration Testing	Start Date/Time	End Date/Time
Pen Test 1	12/11/2023	12/20/2023

Table 2: *Penetration Testing Time Line*

1.4 Summary of Findings

This table shows the number of alerts for each **risk** and **confidence level** included in the report.

Confidence:	High	Medium	Low	TOTAL
Risk Level **High**	0	0	0	0
Risk Level **Medium**	1	2	0	3
Risk Level **Low**	1	1	0	2
Risk Level **Info**	0	1	0	1

Table 3: *Total Risk and Confidence Rating*

This table shows the number of vulnerabilities found by type, as well as their risk level.

Vulnerability	Severity	Quantity
Content Security Policy (*CSP*) Header Not Set	Medium	4
Missing Anti-clickjacking Header	Medium	3
Vulnerable JS Library	Medium	1
Server Leaks Information via "X-Powered-By" HTTP Response Header	Low	3
Server Leaks Version Information via "Server" HTTP Response Header	Low	9
User Agent Fuzzer	Info	24
Total	**6**	

Table 4: *Risk Analysis*

1.5 Summary of Recommendation

1. Ensure that the web server, application server, load balancer, etc. is configured to set the *Content-Security-Policy* header. Set a **non-permissive** *Content-Security-Policy frame-ancestors* header for all requested resources.

2. Modern web browsers support the *Content-Security-Policy* and `X-Frame-Options` HTTP headers. Make sure one of these is set on all web pages returned by the site or application. If the page is to be generated only by pages on the server (*eg it is part of a* `FRAMESET`) then `SAMEORIGIN` should be used, otherwise if the page will never be generated in a frame then `DENY` should be used. As an alternative, consider implementing the Content Security Policy's "*frame-ancestors*" directive.

3. Upgrade to the latest version of Bootstrap library.

4. Ensure that the application server sets the Content-Type header appropriately, and that it sets the *X-Content-Type-Options* header to `nosniff` for all web pages.

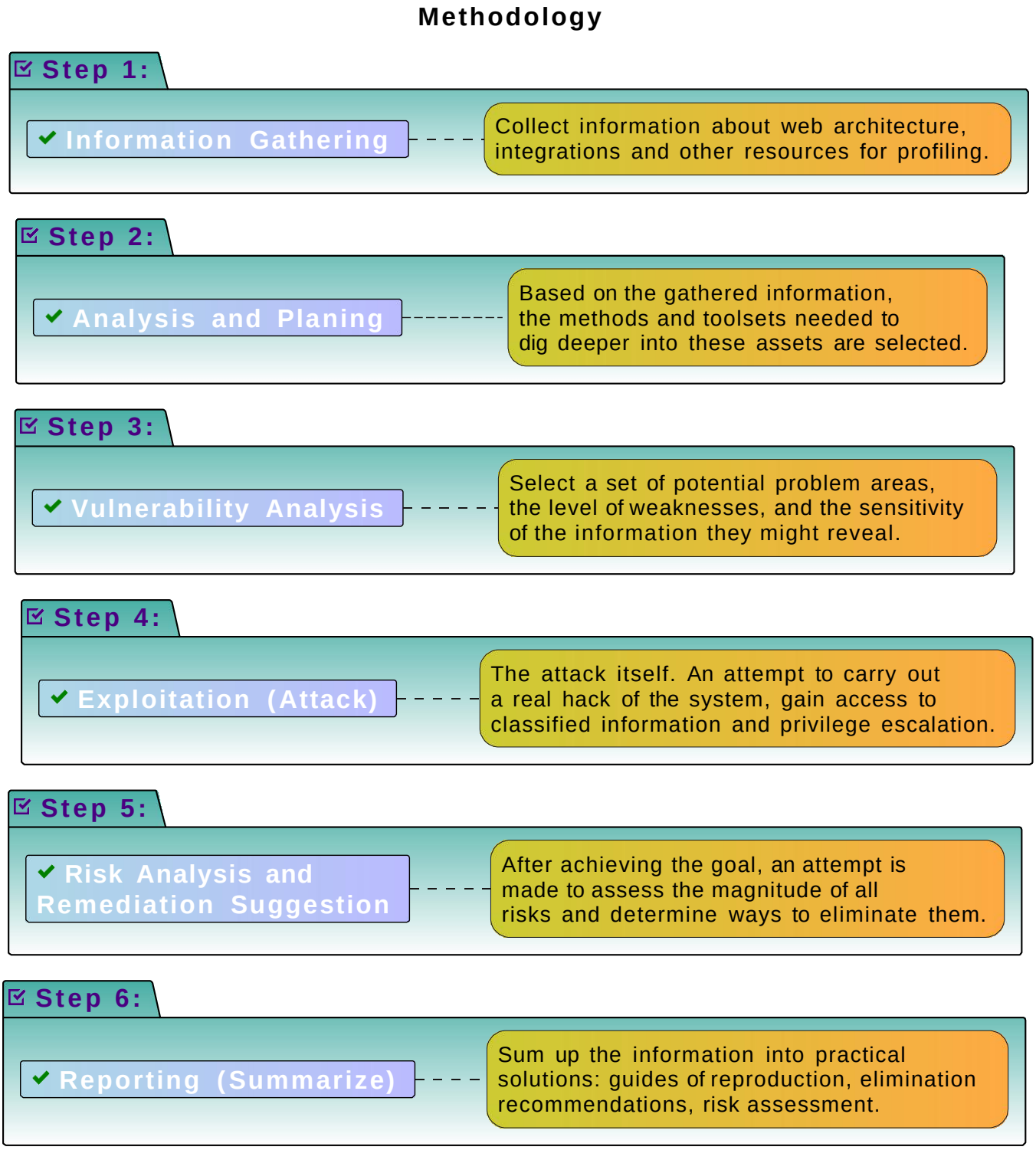
   If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not

perform MIME-sniffing.

5. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "*Server*" header or provide generic details.

6. It is necessary to develop special handler rules for the user agent (*firewall, application, etc.*). Depends on implementation.

2. METHODOLOGY



> **Figure 2:** *Penetration Testing Methodology*

2.1 Information Gathering

To find existing (*and/or hidden*) web objects, I used the DIRB web content scanner (*comes with Kali*).

```
dirb http://178.172.195.18:11166/ /home/vagrant/Downloads/fuzz.txt
```

> **NOTE:**
>
> - **fuzz.txt** - additional dictionary

```
-----------------------------------------------------
DIRB v2.22
By The Dark Raver

URL_BASE: http://178.172.195.18:11166/
WORDLIST_FILES: /home/vagrant/Downloads/fuzz.txt

FOUND: 75
-----------------------------------------------------

-------------------------------------------------------------------------------
-------------
http://178.172.195.18:11166/config.php
(CODE:200|SIZE:0)
http://178.172.195.18:11166/credentials.txt
(CODE:200|SIZE:113)          <- FLAG + (PMA: Login + Password)
http://178.172.195.18:11166/home
(CODE:200|SIZE:1399)
http://178.172.195.18:11166/index.php
(CODE:200|SIZE:2392)
http://178.172.195.18:11166/php.ini
(CODE:200|SIZE:64)
http://178.172.195.18:11166/robots
(CODE:200|SIZE:77)
http://178.172.195.18:11166/robots.txt
(CODE:200|SIZE:77)           <- FLAG
http://178.172.195.18:11166/admin/index.php
(CODE:200|SIZE:514)
http://178.172.195.18:11166/cgi-bin/
(CODE:403|SIZE:292)
http://178.172.195.18:11166/css/custom
(CODE:200|SIZE:527)
http://178.172.195.18:11166/js/main
(CODE:200|SIZE:379)          <- FLAG
http://178.172.195.18:11166/server-status
(CODE:403|SIZE:297)
-------------------------------------------------------------------------------
-------------
http://178.172.195.18:11166/phpmyadmin/ChangeLog
(CODE:200|SIZE:12219)
http://178.172.195.18:11166/phpmyadmin/composer
(CODE:200|SIZE:3189)
```

```
http://178.172.195.18:11166/phpmyadmin/favicon.ico
(CODE:200|SIZE:22486)
http://178.172.195.18:11166/phpmyadmin/index.php
(CODE:200|SIZE:14457)       <- FLAG (DB: Acad; Table: Flag)
http://178.172.195.18:11166/phpmyadmin/doc/html/_images/chart
(CODE:200|SIZE:35466)
http://178.172.195.18:11166/phpmyadmin/doc/html/bookmarks
(CODE:200|SIZE:10088)
http://178.172.195.18:11166/phpmyadmin/doc/html/charts
(CODE:200|SIZE:15016)
http://178.172.195.18:11166/phpmyadmin/doc/html/config
(CODE:200|SIZE:359162)
http://178.172.195.18:11166/phpmyadmin/doc/html/copyright
(CODE:200|SIZE:6572)
http://178.172.195.18:11166/phpmyadmin/doc/html/credits
(CODE:200|SIZE:45625)
http://178.172.195.18:11166/phpmyadmin/doc/html/developers
(CODE:200|SIZE:4877)
http://178.172.195.18:11166/phpmyadmin/doc/html/faq
(CODE:200|SIZE:202201)
http://178.172.195.18:11166/phpmyadmin/doc/html/glossary
(CODE:200|SIZE:33723)
http://178.172.195.18:11166/phpmyadmin/doc/html/index
(CODE:200|SIZE:14976)
http://178.172.195.18:11166/phpmyadmin/doc/html/index.html
(CODE:200|SIZE:14976)
http://178.172.195.18:11166/phpmyadmin/doc/html/intro
(CODE:200|SIZE:11055)
http://178.172.195.18:11166/phpmyadmin/doc/html/other
(CODE:200|SIZE:7013)
http://178.172.195.18:11166/phpmyadmin/doc/html/require
(CODE:200|SIZE:8462)
http://178.172.195.18:11166/phpmyadmin/doc/html/search
(CODE:200|SIZE:3662)
http://178.172.195.18:11166/phpmyadmin/doc/html/security
(CODE:200|SIZE:12017)
http://178.172.195.18:11166/phpmyadmin/doc/html/settings
(CODE:200|SIZE:6266)
http://178.172.195.18:11166/phpmyadmin/doc/html/setup
(CODE:200|SIZE:121361)
http://178.172.195.18:11166/phpmyadmin/doc/html/themes
(CODE:200|SIZE:11438)
http://178.172.195.18:11166/phpmyadmin/doc/html/transformations
(CODE:200|SIZE:13570)
http://178.172.195.18:11166/phpmyadmin/doc/html/user
(CODE:200|SIZE:8667)
http://178.172.195.18:11166/phpmyadmin/doc/html/vendors
(CODE:200|SIZE:6222)
http://178.172.195.18:11166/phpmyadmin/js/ajax
(CODE:200|SIZE:31246)
http://178.172.195.18:11166/phpmyadmin/js/chart
(CODE:200|SIZE:18509)
http://178.172.195.18:11166/phpmyadmin/js/common
(CODE:200|SIZE:19196)
```

```
http://178.172.195.18:11166/phpmyadmin/js/config
(CODE:200|SIZE:27526)
http://178.172.195.18:11166/phpmyadmin/js/console
(CODE:200|SIZE:57280)
http://178.172.195.18:11166/phpmyadmin/js/export
(CODE:200|SIZE:35062)
http://178.172.195.18:11166/phpmyadmin/js/functions
(CODE:200|SIZE:175177)
http://178.172.195.18:11166/phpmyadmin/js/import
(CODE:200|SIZE:5640)
http://178.172.195.18:11166/phpmyadmin/js/indexes
(CODE:200|SIZE:27654)
http://178.172.195.18:11166/phpmyadmin/js/navigation
(CODE:200|SIZE:60012)
http://178.172.195.18:11166/phpmyadmin/js/replication
(CODE:200|SIZE:3201)
http://178.172.195.18:11166/phpmyadmin/js/rte
(CODE:200|SIZE:47688)
http://178.172.195.18:11166/phpmyadmin/js/sql
(CODE:200|SIZE:38441)
http://178.172.195.18:11166/phpmyadmin/js/transformations/json
(CODE:200|SIZE:670)
http://178.172.195.18:11166/phpmyadmin/js/transformations/xml
(CODE:200|SIZE:665)
http://178.172.195.18:11166/phpmyadmin/js/vendor/jquery/jquery
(CODE:200|SIZE:9574)
http://178.172.195.18:11166/phpmyadmin/LICENSE
(CODE:200|SIZE:18092)
http://178.172.195.18:11166/phpmyadmin/package
(CODE:200|SIZE:729)
http://178.172.195.18:11166/phpmyadmin/phpinfo.php
(CODE:200|SIZE:14459)
http://178.172.195.18:11166/phpmyadmin/print
(CODE:200|SIZE:1213)
http://178.172.195.18:11166/phpmyadmin/README
(CODE:200|SIZE:1520)
http://178.172.195.18:11166/phpmyadmin/robots
(CODE:200|SIZE:26)
http://178.172.195.18:11166/phpmyadmin/robots.txt
(CODE:200|SIZE:26)
http://178.172.195.18:11166/phpmyadmin/setup/ajax
(CODE:200|SIZE:248)
http://178.172.195.18:11166/phpmyadmin/setup/index.php
(CODE:200|SIZE:10518)
http://178.172.195.18:11166/phpmyadmin/setup/scripts
(CODE:200|SIZE:6086)
http://178.172.195.18:11166/phpmyadmin/setup/styles
(CODE:200|SIZE:10563)
http://178.172.195.18:11166/phpmyadmin/themes/dot
(CODE:200|SIZE:43)
http://178.172.195.18:11166/phpmyadmin/themes/original/css/printview
(CODE:200|SIZE:2746)
http://178.172.195.18:11166/phpmyadmin/themes/original/img/console
(CODE:200|SIZE:295)
```

```
http://178.172.195.18:11166/phpmyadmin/themes/original/img/error
(CODE:200|SIZE:1150)
http://178.172.195.18:11166/phpmyadmin/themes/original/img/hide
(CODE:200|SIZE:284)
http://178.172.195.18:11166/phpmyadmin/themes/original/img/more
(CODE:200|SIZE:85)
http://178.172.195.18:11166/phpmyadmin/themes/original/img/play
(CODE:200|SIZE:329)
http://178.172.195.18:11166/phpmyadmin/themes/original/img/show
(CODE:200|SIZE:263)
http://178.172.195.18:11166/phpmyadmin/themes/original/img/spacer
(CODE:200|SIZE:68)
http://178.172.195.18:11166/phpmyadmin/themes/original/screen
(CODE:200|SIZE:22511)
http://178.172.195.18:11166/phpmyadmin/themes/original/theme
(CODE:200|SIZE:209)
http://178.172.195.18:11166/phpmyadmin/vendor/composer/LICENSE
(CODE:200|SIZE:1070)
-----------------------------------------------------------------------------
-------------
```

2.2 Planning

Now we need to explore the resources found.

- http://178.172.195.18:11166/index.php
- http://178.172.195.18:11166/credentials.txt
- http://178.172.195.18:11166/config.php
- http://178.172.195.18:11166/php.ini
- http://178.172.195.18:11166/robots.txt
- http://178.172.195.18:11166/admin/index.php
- http://178.172.195.18:11166/js/main
- http://178.172.195.18:11166/css/custom
- http://178.172.195.18:11166/phpmyadmin/index.php

There are various tools for this. The choice of tool set depends on your goals. For web exploitation purposes I plan to use:

- Browser Developer Tools
- Perform a detour
- Basic SQL injection
- Swigger Port Resources

2.3 Exploitation

There are a few common places I can go to determine the current architecture:

- HTTP headers
- Cookie
- HTML, CSS and JS source code

- Specific files and folders.
- File extensions
- Error message

I can do all the research using standard browser development tools.

> **NOTE:**
>
> I think I may have to use **dirb** or **dirbuster** to search deeper for information about *Specific files and folders* and *File extensions*, but I've already done that in the information gathering phase.

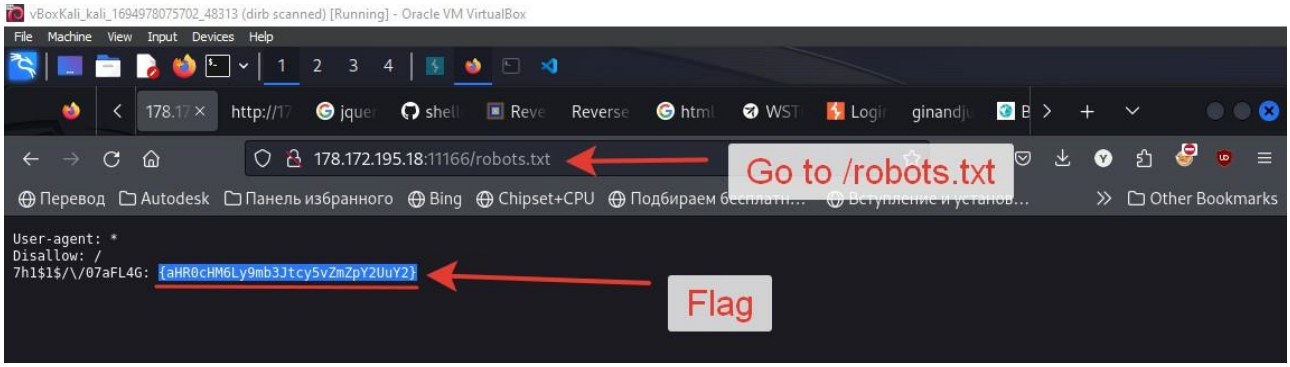
2.4 Reporting

I was able to find most of the flags using standard *browser development tools*.

1.1 - Recon Flag1

To find the first flag you need to do the following:

1. Open a browser and go to `http://178.172.195.18:11166/robots.txt`
2. The flag is here



> **Figure 3** *Task: 1.1 - Recon Flag1*

1.3 - Recon Flag3

To find the next flag you need to do the following:

1. Open a browser and go to `http://178.172.195.18:11166/admin/index.php`
2. Press [F12] to open *Developer Tools* (*for **Firefox** browser*)
3. Select the "*Debugger*" tab.
4. On the left side, expand the `js` folder.
5. Select the `main.js` file to display its contents.
6. On **line 4** you will find a flag.

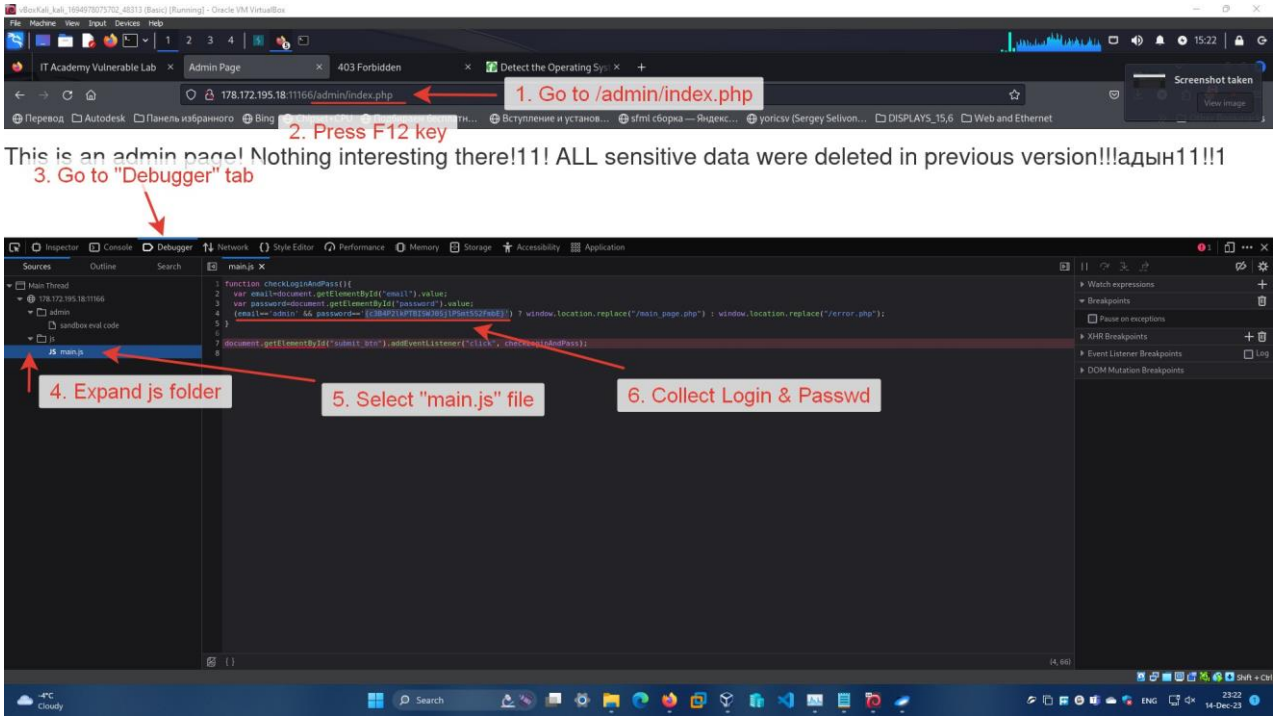


Figure 4 *Task: 1.3 - Recon Flag3*

1.5 - Recon Flag5

To find the next flag you need to do the following:

1. Open a browser and go to `http://178.172.195.18:11166/credentials.txt`
2. The flag is here

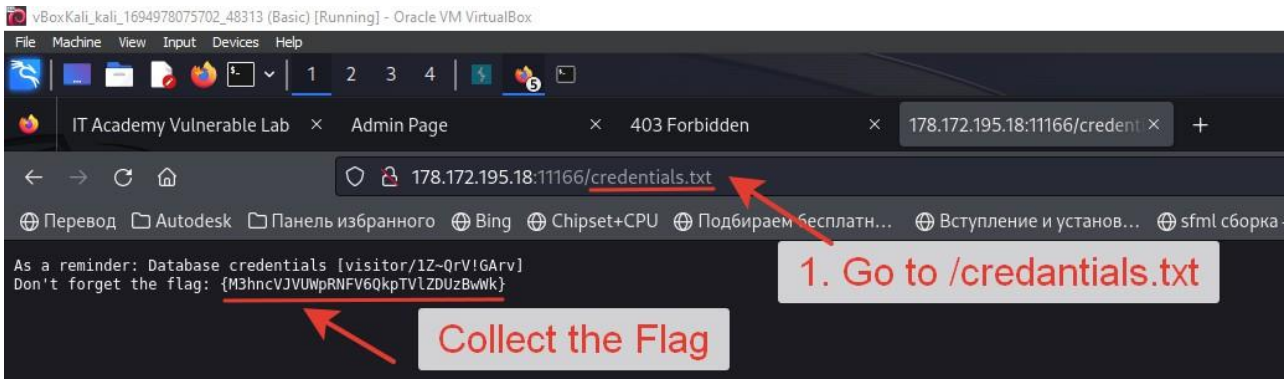


Figure 5 *Task: 1.5 - Recon Flag1*

1.6 - Recon Flag6

To find the first flag you need to do the following:

1. Open a browser and go to `http://178.172.195.18:11166/credentials.txt`
2. Here we can find **login** and **password** (*during the information gathering phase we found the **PhpMyAdmin** panel and these credentials are possibly used to login*)

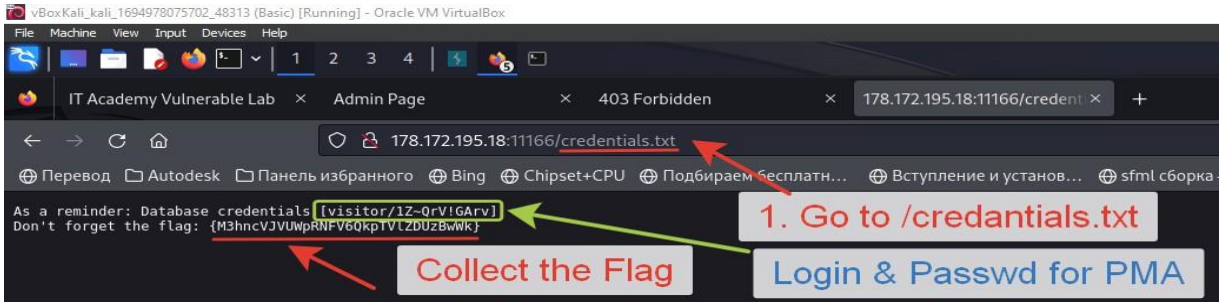


Figure 6 *Task: 1.6 - Recon Flag6 Step 1*

3. Go to `http://178.172.195.18:11166/phpmyadmin/index.php` to verify the credentials
4. Insert `visitor` into **User** and `1Z~QrV!GArv` into **Password** field
5. Click `Next` button

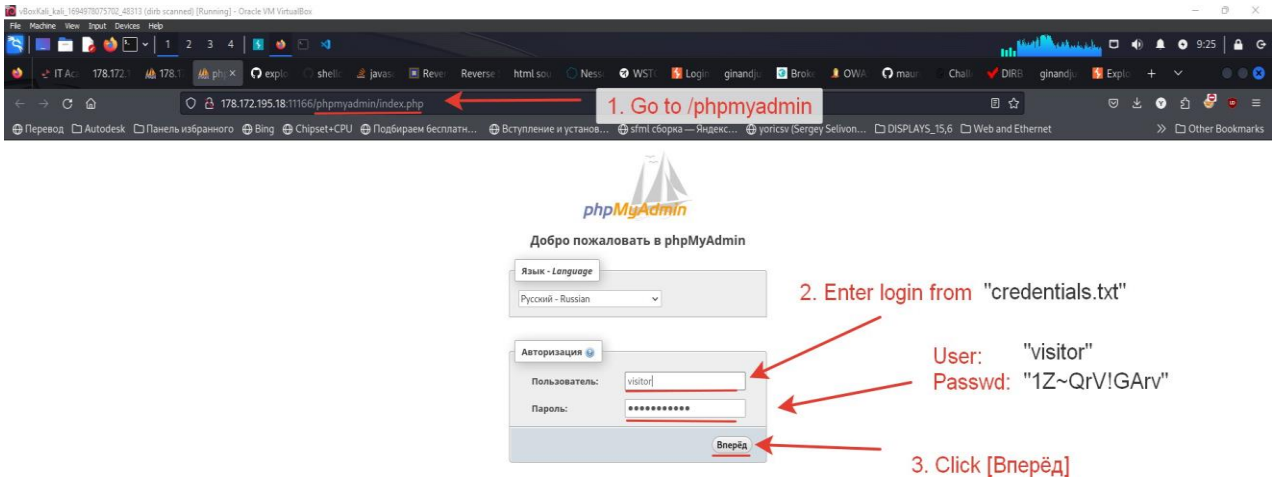


Figure 7 *Task: 1.6 - Recon Flag6 Step 2*

6. Digging deeper into the database structure, we found the `Acad` database and the `Flag` table.
7. By clicking on the `Flag` table, we found the following Flag.

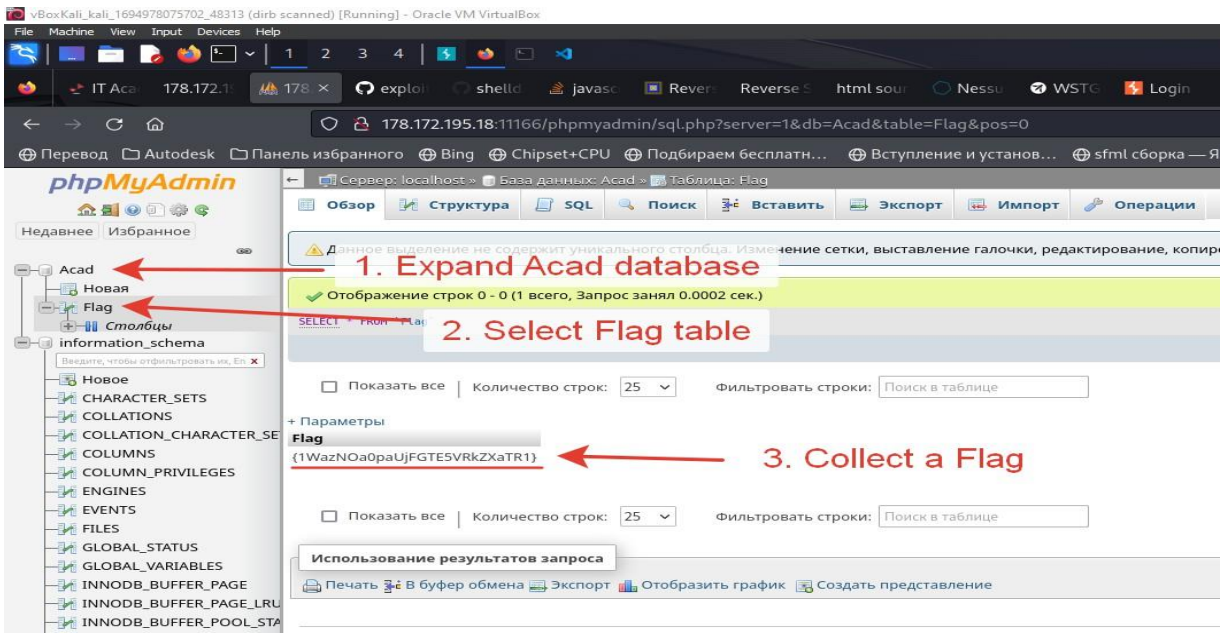


Figure 8 *Task: 1.6 - Recon Flag6 Step 3*