

Writeup by: **Danilo Nascimento | 1nv1ct4**

<https://github.com/ndanilo8/PositiveHackCamp2024>

---

## Description:

Follow task instructions and use `BurpSuite` to complete all challenges!

---

## Attack

- To solve the task we first have to change our request to **POST**
- then we have to add the new **header** `X-Cyber-ed=1`
- now its time to add the **POST Parameters** `?cyber-ed=hacker`
- And change the **POST format** to: `application/x-www-form-urlencoded`
- and add the **cookie**: `cookie: cyber-ed=1`
- and we must change the **user-agent to yandex browser**. For this we can google some random Yandex UA: for example <https://whatmyuseragent.com/browser/ya/yandex-browser/18>

```
Mozilla/5.0 (Linux; Android 4.2.2; PAP3400 DUO Build/JDQ39)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181
YaBrowser/18.6.0.683.00 Mobile Safari/537.36
```

## Payload for flag

```
POST /robots.txt?cyber-ed=hacker HTTP/1.1
Host: web.bn5rzokznmaxq595129u.labs.cyber-ed.space
User-Agent: Mozilla/5.0 (Linux; Android 4.2.2; PAP3400 DUO Build/JDQ39)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181
YaBrowser/18.6.0.683.00 Mobile Safari/537.36
Accept: application/x-www-form-urlencoded
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
```

Upgrade-Insecure-Requests: 1

Sec-GPC: 1

Content-Length: 8

X-Cyber-Ed: hacker

cookie: cyber-ed=1

AAAA

## Flag

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre>1 POST /robots.txt?cyber-ed=hacker HTTP/1.1 2 Host: web.bn5rzokznmqx595129u.labs.cyber-ed.space 3 User-Agent: Mozilla/5.0 (Linux; Android 4.2.2; PAP3400 DUO Build/JDQ39) AppleWebKit/537.36   (KHTML, like Gecko) Chrome/66.0.3359.181 YaBrowser/18.6.0.683.00 Mobile Safari/537.36 4 Accept: application/x-www-form-urlencoded 5 content-type: application/x-www-form-urlencoded 6 Accept-Language: en-US,en;q=0.5 7 X-Cyber-Ed: hacker 8 Accept-Encoding: gzip, deflate, br 9 DNT: 1 10 Connection: keep-alive 11 Upgrade-Insecure-Requests: 1 12 Sec-GPC: 1 13 Content-Length: 8 14 cookie: cyber-ed=1 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41</pre>			<pre>15 &lt;meta name= 16 17 &lt;title&gt;   Web Instructions &lt;/title&gt; 18 19 &lt;!-- Google font --&gt; 20 &lt;link href="https://fonts.googleapis.com/css?family=Montserrat:700,900" rel="stylesheet"&gt; 21 22 &lt;!-- Custom stylesheet --&gt; 23 &lt;link type="text/css" rel="stylesheet" href="style.css" /&gt; 24 25 &lt;/head&gt; 26 27 &lt;body&gt; 28 29 &lt;div id="notfound"&gt; 30   &lt;div class="notfound"&gt; 31     &lt;div class="notfound-404"&gt; 32       &lt;h1&gt;         CyberEd       &lt;/h1&gt; 33       &lt;h2&gt;         flag{c32637ded05ebacea89ee450a1fa3eca}       &lt;/h2&gt; 34     &lt;/div&gt; 35   &lt;/div&gt; 36 &lt;/div&gt; 37 38 &lt;/body&gt; 39 &lt;!-- This templates was made by Colorlib (https://colorlib.com) --&gt; 40 &lt;/html&gt; 41</pre>			

flag{c32637ded05ebacea89ee450a1fa3eca}