POST Practice

ctflearn.com

Jakub Kazimierski February 2023

1 Introduction

This sheet meant to be a walkthrough of CTF challenge from ctf [6]. Here I try to explain step by step what metodology for solving this problem was taken along with actions which were needed. Some of steps will be showed on screenshots and some just explained along with commands used.

OS which was used for this presentation is Kali Linux in version 2022.4

2 Problem overview

Description of this task is short, we should exploit site: [7]. When we open link we get home page:

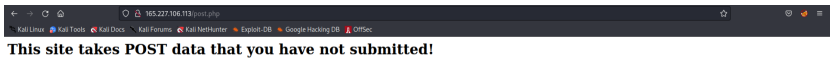

Figure 1: Site home page

There are no much information on this execpt that we missed to request POST some data. Let's try to inspect it, maybe there will be some more informations.

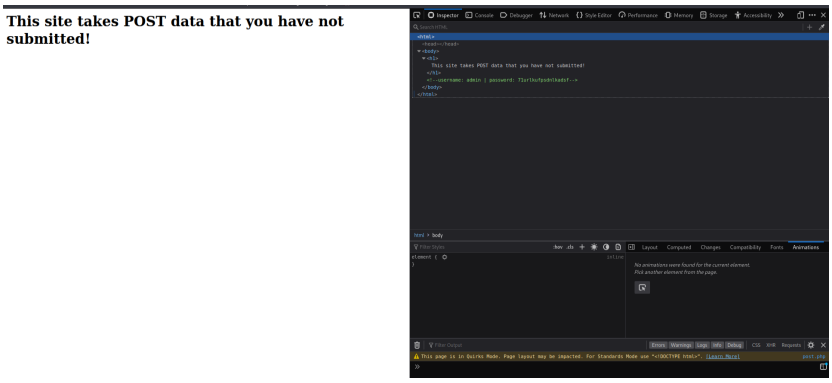

Figure 2: Inspecting page

In html code there is interesting commend with login and password. **Username: admin** and **password: 71urlkufpsdnlkadsf** as that may be useful, so lets save it somewhere.

At this point it may also be useful to enumerate directories of this site, it is possible that we will find something useful. To achieve that we can use Gobuster [4] tool which is installed on Kali. To start enumeration I used command:

```
linux@linux-$ gobuster dir -u http://165.227.106.113/ -w
    /usr/share/wordlists/dirb/common.txt -x php,txt,jpg
```

Listing 1: Gobuster syntax

Where:

- dir - uses directory/file enumeration mode
- -u - uses given url
- -w - uses given wordlist (wordlists used to enumerations are preinstalled on Kali by default)
- -x - uses wordlist to check for files with specified extension in searched directory

Ok so output which I get looks like this:

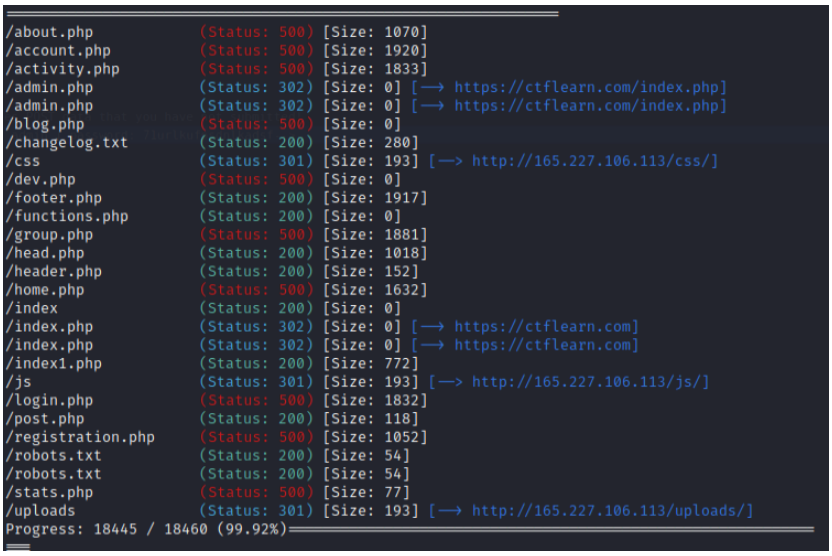

Figure 3: Gobuster output

There seems to be some adressess which we can access, I tried with **/index1.php**:

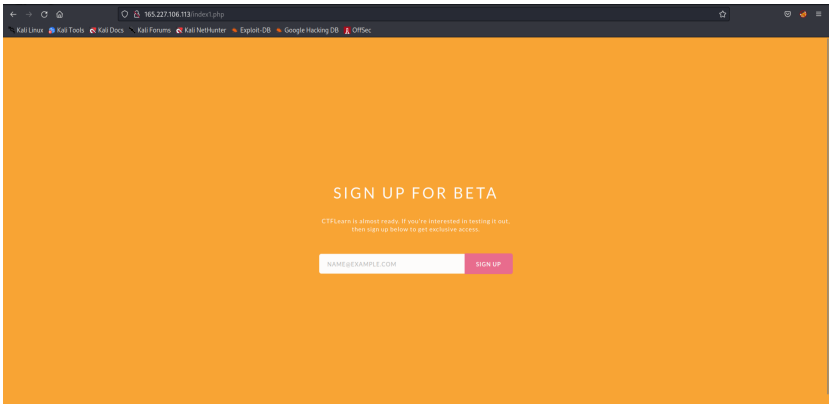

Figure 4: Redirected

Well it seems that page where we was redirected may be not connected to this challenge, it is possible that this IP address was used for some other challenges too. At this point We have credentials for admin account and description on home page says that we need to request POST header with some data. I suggest to use Burpsuite [1] (and FoxyProxy [3] to configure proxy in browser), and by

using proxy, edit and send POST header with these credentials, at address of home page.

After enabling proxy and with Burpsuite option **Intercept is on** after refreshing page we will get intercepted GET request:

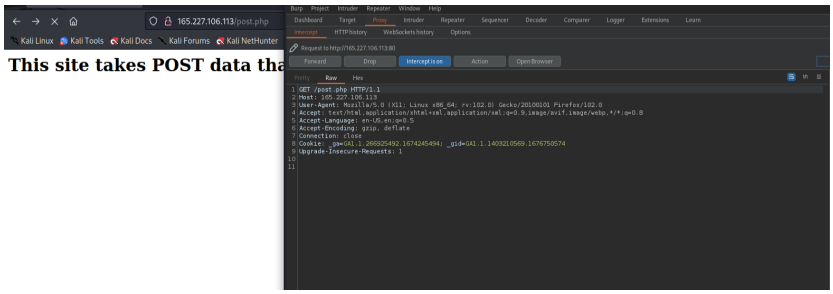

Figure 5: Get home page

Let's try to edit it to POST and include admin credentials, option 'send to repeater' may be helpful:

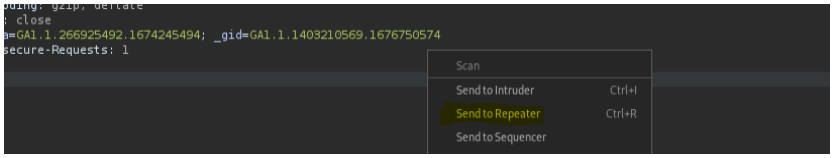

Figure 6: Send to repeater

And in repeater view edited POST request should look like:

Figure 7: POST request

If You would like to copy paste it below is syntax:

```
POST /post.php HTTP/1.1

Host: 165.227.106.113

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
    Gecko/20100101 Firefox/102.0

Accept: text/html,application/xhtml+xml,application/xml;q
    =0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

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

Content-Length: 42



username=admin&password=71urlkufpsdnlkadsf
```

Listing 2: Name of file to upload

To check syntax of web headers You can use site [5]. I mentioned syntax because without two elements:

- Content-Type: application/x-www-form-urlencoded
- Content-Length: 42

This request was not passing. But after is prepared correctly we get response:

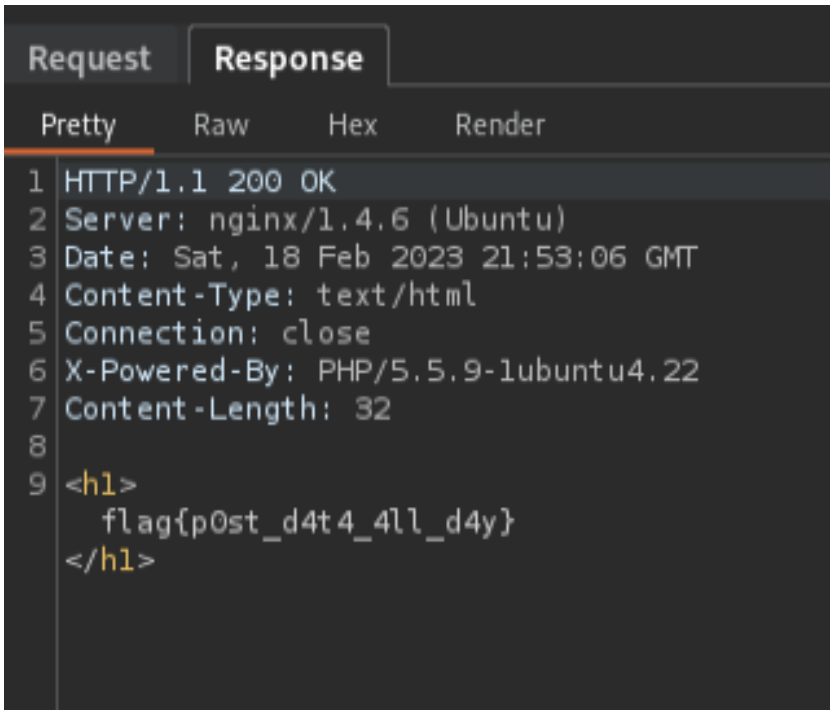

Figure 8: Flag

And the flag is **flag{p0st_d4t4_4ll_d4y}**

There is one more way to achieve this flag which I'd like to mention due to fact that preparing syntax proper POST request in Burp may be annoying after many unsuccessfull tries. We can use **curl** [2] command with POST request including credentials. Syntax would be:

```
curl -X POST -d 'username=admin&password=71
    urlkufpsdnlkadsf' http://165.227.106.113/post.php
```

Listing 3: Curl syntax

And as an output in your terminal you would get:

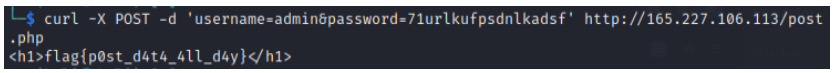

Figure 9: Edit page

References

[1] Burp suite. https://portswigger.net/burp/communitydownload.

[2] Curl command. https://linuxize.com/post/curl-post-request/.

[3] Foxyproxy configuration. https://null-byte.wonderhowto.com/how-to/use-burp-foxyproxy-easily-switch-between-proxy-settings-0196630/.

[4] Gobuster. https://www.kali.org/tools/gobuster/.

[5] Post syntax. https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST.

[6] Reference to site with this challenge. https://ctflearn.com/.

[7] Site to exploit. http://165.227.106.113/post.php.