

POST Practice CTF Writeup

This document is a walkthrough on one way to solve the **POST Practice CTF** on **CTFLearn**. The objective is to explain how I was able to solve this CTF to my future self.

General Information

- *Difficulty:* **Easy**
- *Category:* **Web**
- *Link:* [POST Practice - CTFLearn](#)

Solution

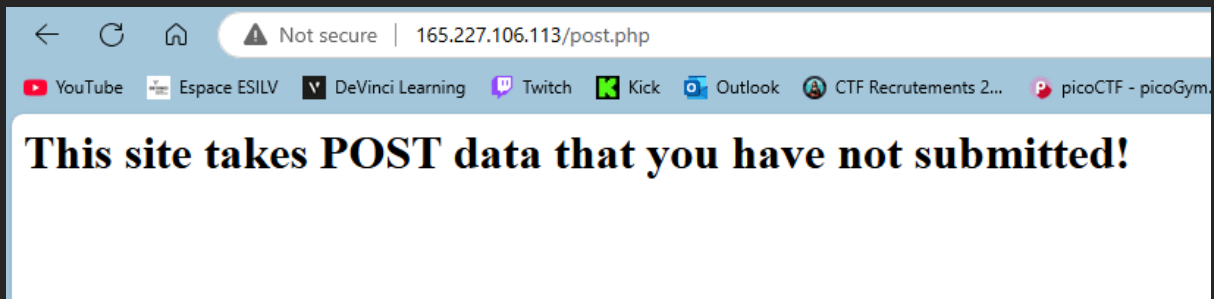
POST Practice

40 points

Medium

This website requires authentication, via POST. However, it seems as if someone has defaced our site. Maybe there is still some way to authenticate?
<http://165.227.106.113/post.php>

The URL takes us to an empty website.



Since we're not able to interact with the website, and given the clue that it's waiting for "**POST data**" to be sent, it looks like we're going to have to use a tool to do this.

First, the source code gives us a clue.

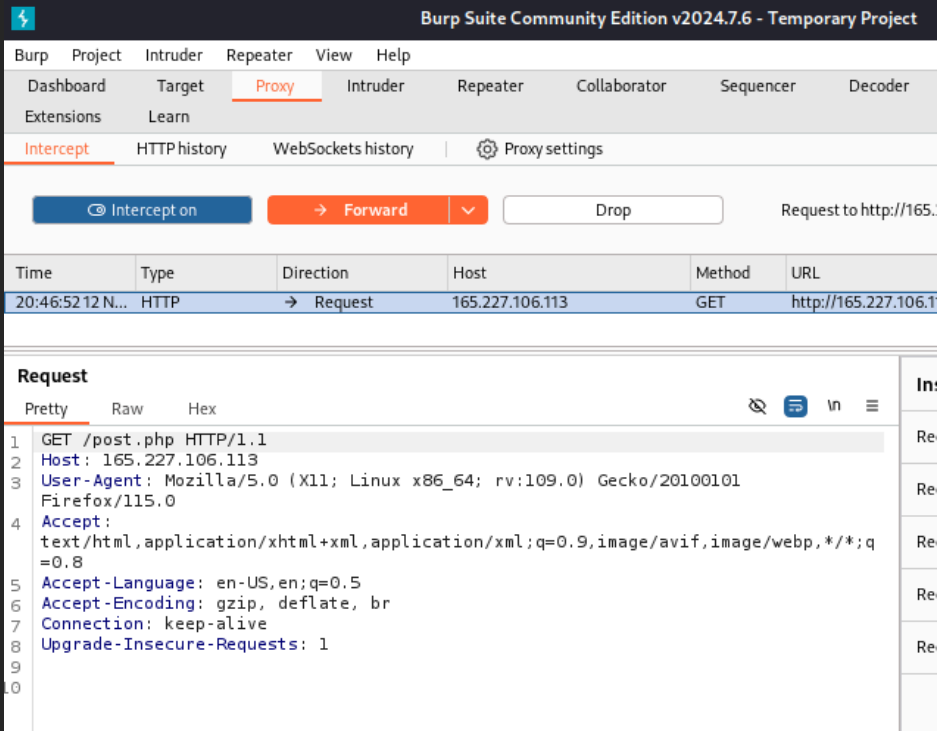
```
Line wrap ☐
1 <h1>This site takes POST data that you have not submitted!</h1><!-- username: admin | password: 71urlkufpsdnlkadsf -->
```

username: admin | password: 71urlkufpsdnlkadsf

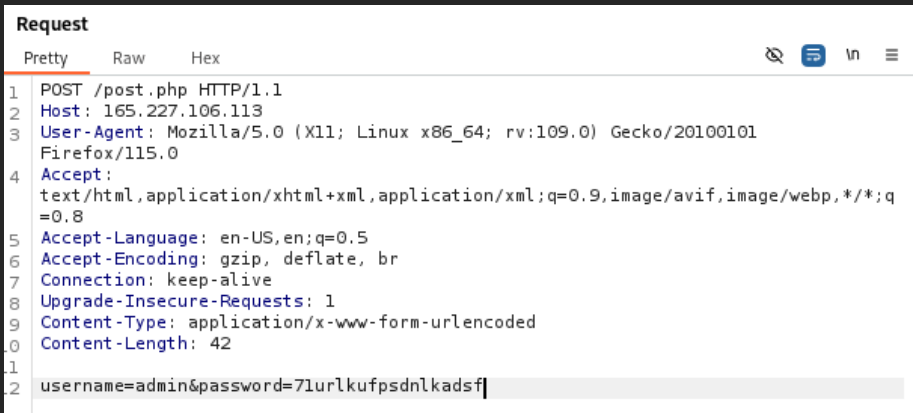
This looks like the data we'll have to put in the **POST request**

We can do this using **Burp Suite**, a tool that's useful for penetration testing of web applications.

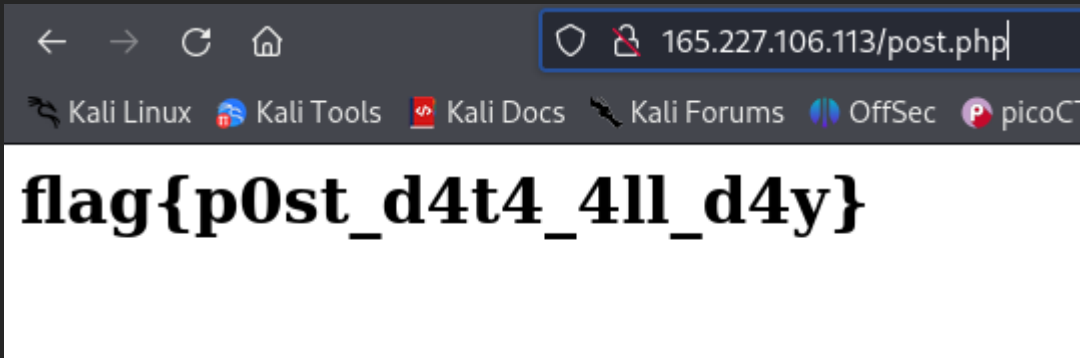
Opening up Burp Suite, we've intercepted the **GET request** made by our browser, before it's sent to the server.



Let's modify it to a POST request, which is what we want here.



Forwarding the request, the web server sends us new HTML code, which contains the flag:



flag{p0st_d4t4_4ll_d4y}

