

CTF LEARN: POST PRACTICE

1. Story:

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>

2. Website View:

When you first visit the website, you see this message

This site takes POST data that you have not submitted!

3. Solution

If you view page source, it will show you the required data to be sent

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

The required data: "username: admin | password: 71urlkufpsdnlkadsf"

Then you can send the data using curl command

```
C:\Users\Luka>curl -X POST http://165.227.106.113/post.php -d "username=admin&password=71urlkufpsdnlkadsf"
<h1>flag{p0st_d4t4_4ll_d4y}</h1>
```

The Flag is **flag{p0st_d4t4_4ll_d4y}**