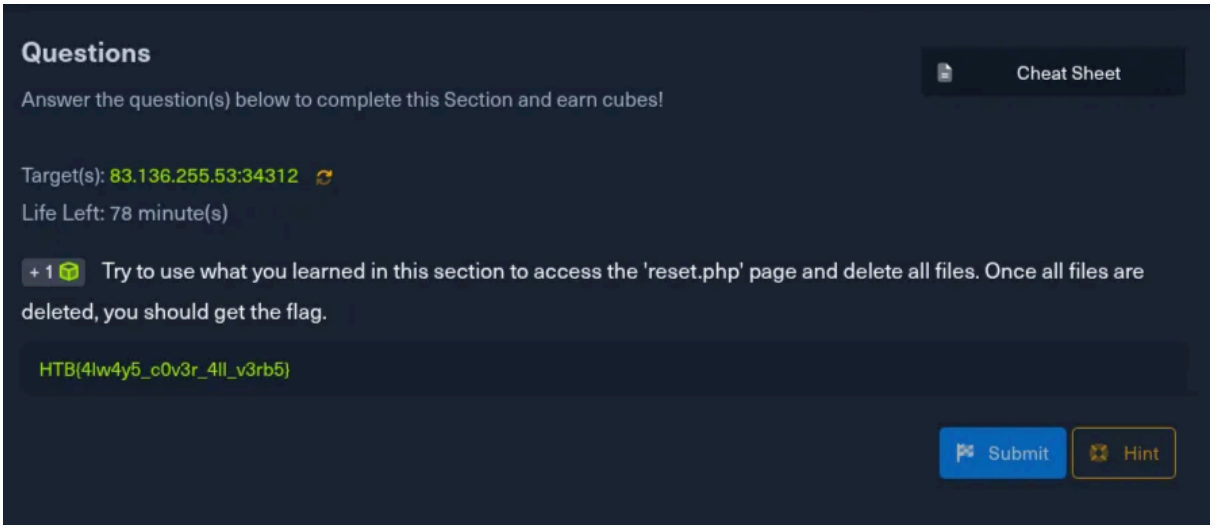
Web Attacks-HTTP Verb Tampering

Web Attacks-HTTP Verb Tampering Writeup

Written By: Alexander Sapo

Bypassing Basic Authentication



Question

Try to use what you learned in this section to access the 'reset.php' page and delete all files. Once all files are deleted, you should get the flag.

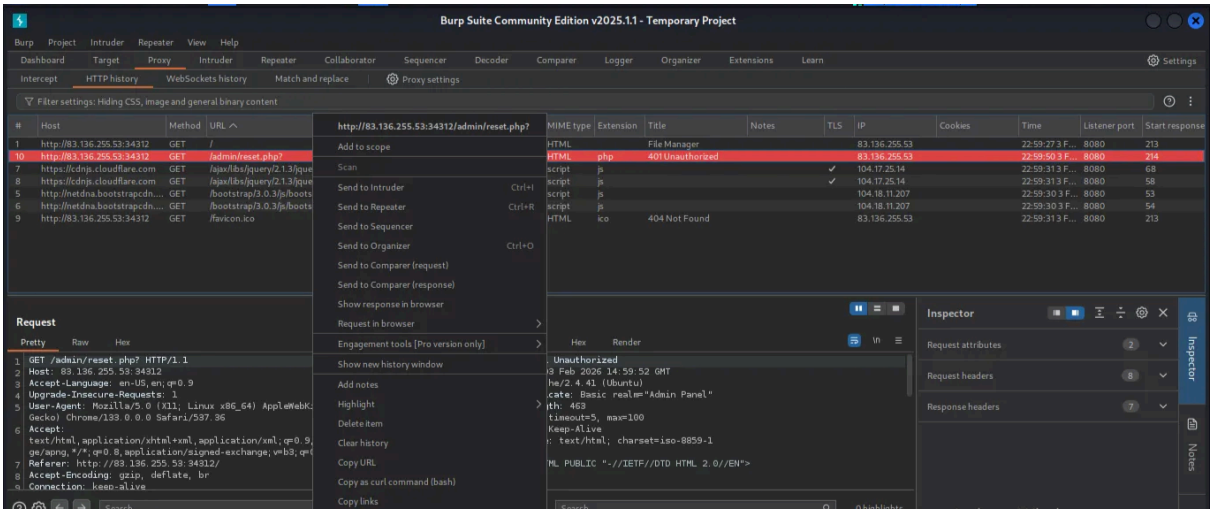
flag: HTB{4lw4y5_c0v3r_4ll_v3rb5}

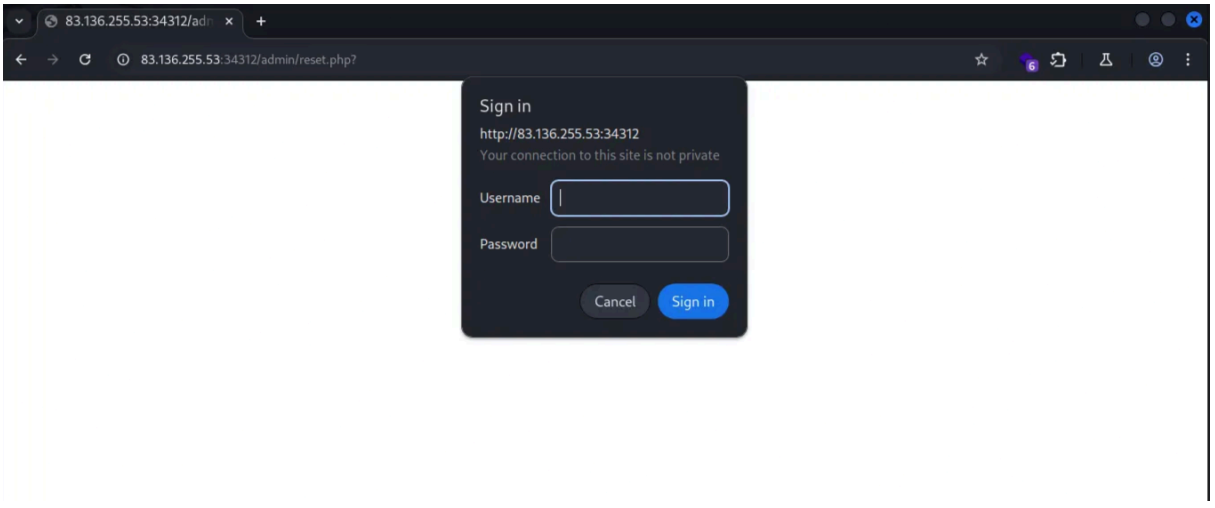
process:

As mentioned in the task, the goal is to access reset.php and delete all the files in it.

Since this is an HTTP Verb Tampering challenge and it is assumed that the target is vulnerable, we try what we learned by changing the HTTP method in Burp Suite.

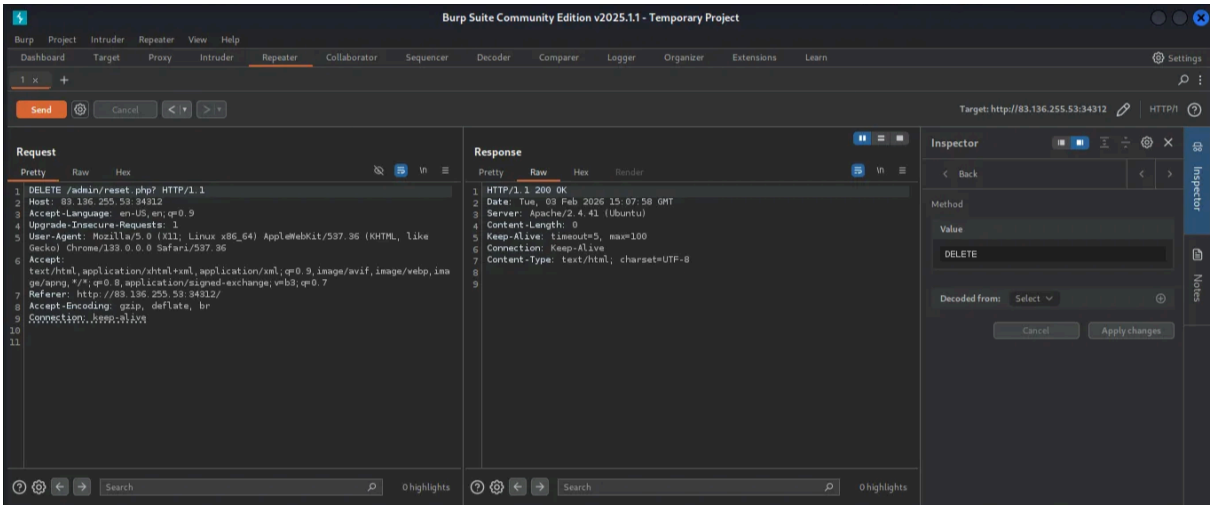
First, fire up Burp and analyze the web application. During the initial analysis, we find /admin/reset.php. That is the endpoint we are looking for.



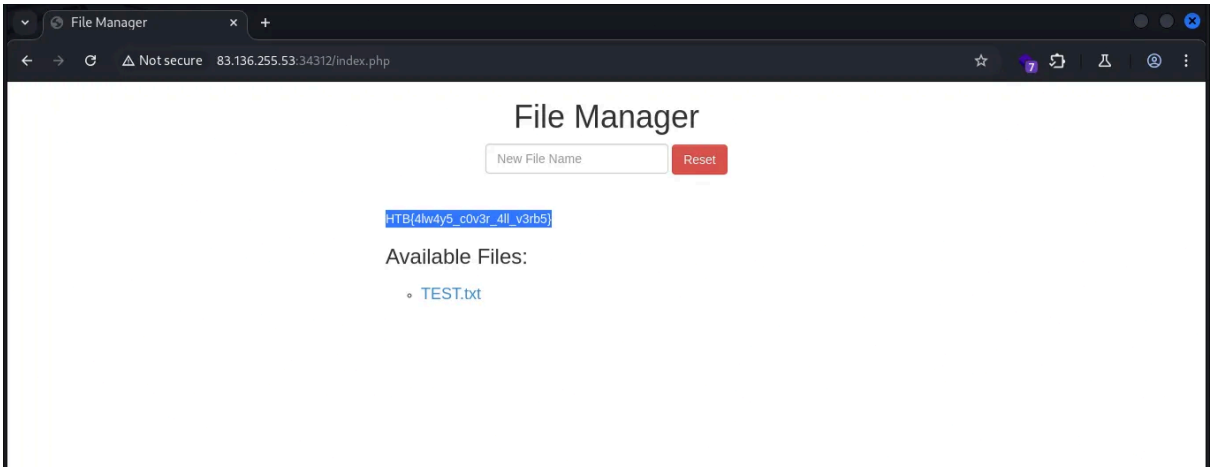


Next, we attempt to access it, and it appears that authentication is required.

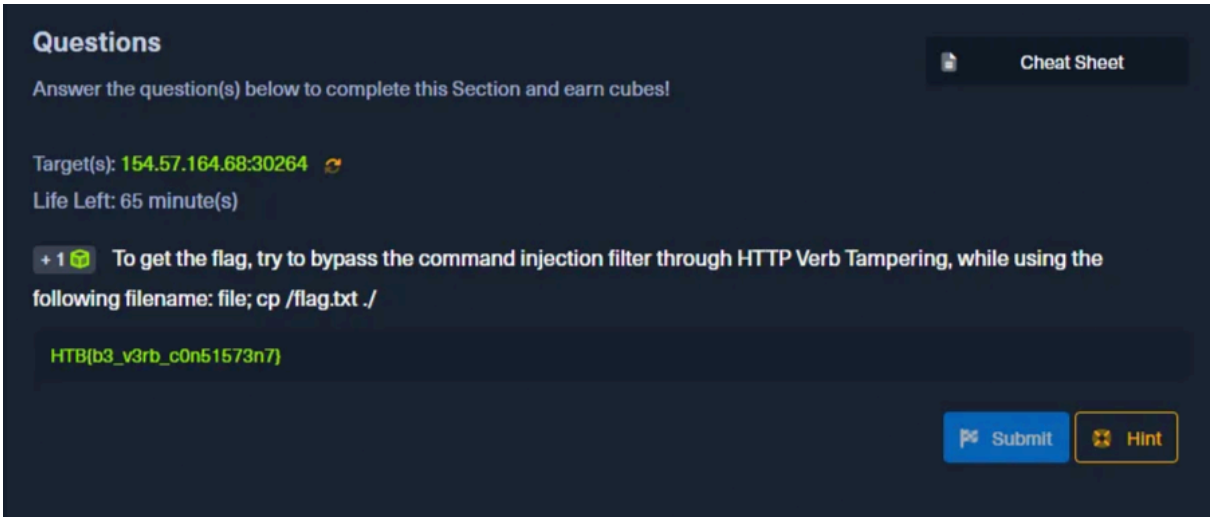
We then go back to Burp, right-click the request for /admin/reset.php, and send it to Repeater. In Repeater, we change the HTTP method to DELETE and send the request.



After sending the modified request, we check the web application, and the flag appears.



Bypassing Security Filters



Question

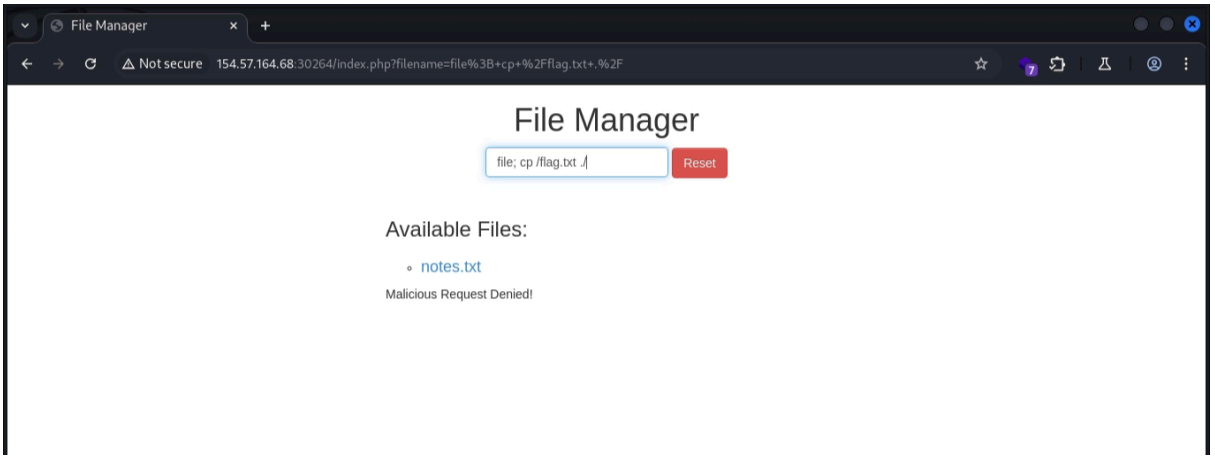
To get the flag, try to bypass the command injection filter through HTTP Verb Tampering, while using the following filename: file; cp /flag.txt ./

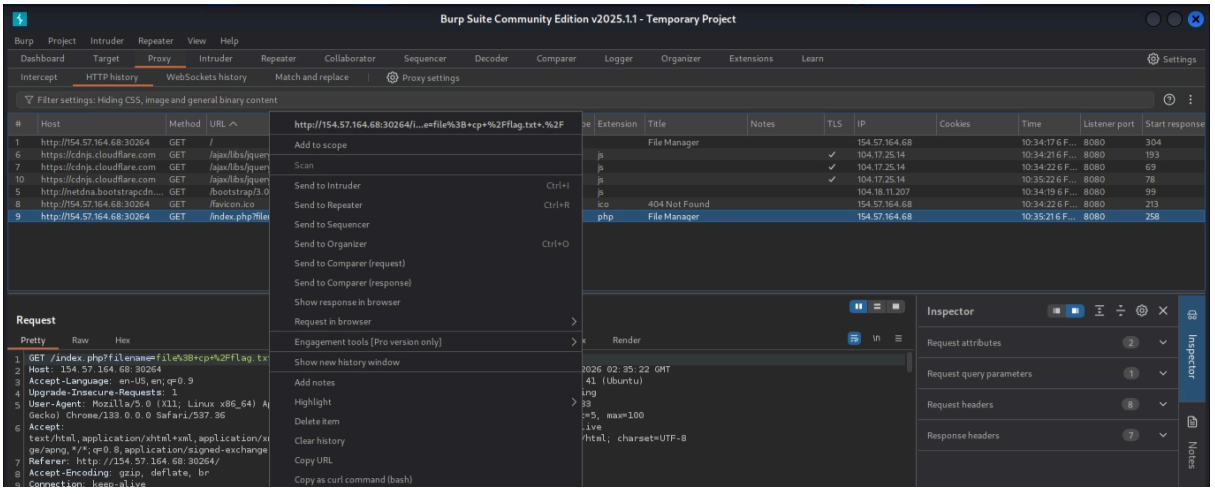
flag: HTB{b3_v3rb_c0n51573n7}

process:

First, fire up Burp Suite and look for /index.php?filename=. Send the request to Repeater.

It appears that certain commands are not allowed because they are filtered.

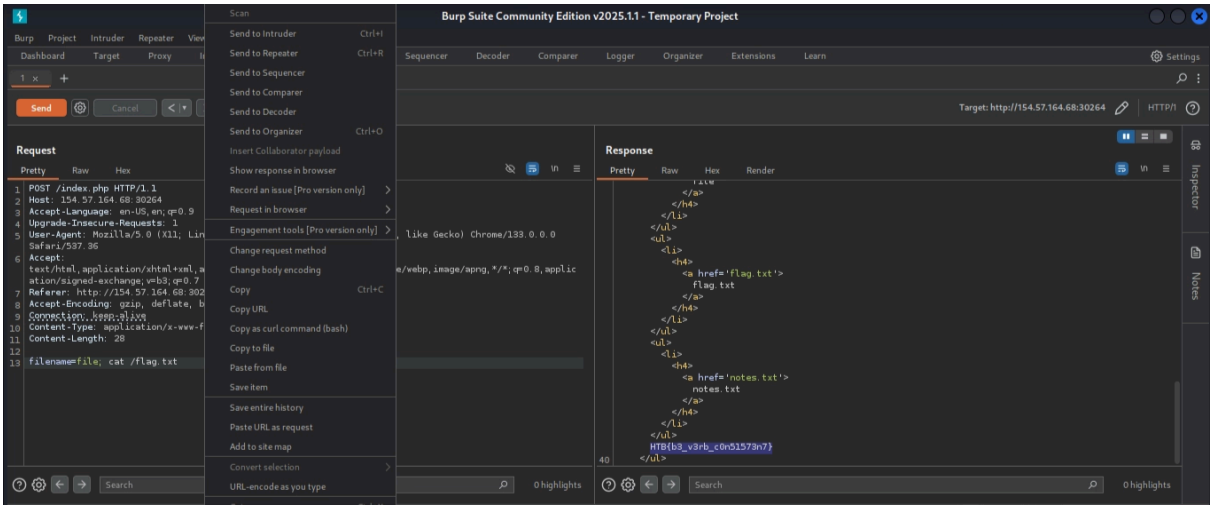




However, we test different commands, such as:

filename=file; cat /flag.txt

We then change the HTTP method from GET to POST, which allows the request to bypass the filter.

After sending the modified request, we can see the flag in the response.

So, we successfully obtained the flag.