Mark Seliternikov

TryHackMe - Web Fundamentals [Easy]

HTTP

The purpose of this writup is reference for myself for future CTFs which I'll need to use 'curl'.

This isn't a challenging CTF but I found it very interesting and useful for future CTFs. The main point here is that I can do web-based CTFs without relying on a browser but rather use the terminal with **'crul**'.

Here are the 4 flags I had to achieve by using the 'curl' command differently:

First, send a regular http get request to the web-server on port 8081 at the /ctf/get page.

```
┌──(root💀 kali)-[/home/kali]
└─# curl http://10.10.82.43:8081/ctf/get

thm{162520bec925bd7979e9ae65a725f99f}
```

Well that one was more of a sanity check that I'm actually connected and can communicate with the right web-server. Anyway… Now using post! I usually had to rely on pre-made forms on previous CTF's and had to change the action to post and such. This time I'm attempting to do it manually from the terminal!

```
┌──(root💀 kali)-[/home/kali]
└─# curl -X POST --data flag_please http://10.10.82.43:8081/ctf/post
thm{3517c902e22def9c6e09b99a9040ba09}
```

Because that was a post request, one must include data to be passed because it cannot be passed via the URL. Now lets try getting a cookie from the web-server.

```
┌──(root💀 kali)-[/home/kali]
└─# curl -vv http://10.10.82.43:8081/ctf/getcookie
*   Trying 10.10.82.43:8081 ...
* Connected to 10.10.82.43 (10.10.82.43) port 8081 (#0)
> GET /ctf/getcookie HTTP/1.1
> Host: 10.10.82.43:8081
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Set-Cookie: flag=thm{91b1ac2606f36b935f465558213d7ebd}; Path=/
< Date: Thu, 13 May 2021 12:53:32 GMT
< Content-Length: 19
< Content-Type: text/plain; charset=utf-8
<
* Connection #0 to host 10.10.82.43 left intact
Check your cookies!
```

We can see the flag in the cookies! (-vv, makes it very verbose which allows me to see the whole request)

Now lets try create and send a custom cookie!

```
┌──(root💀kali)-[/home/kali]
└─# curl --cookie flagpls=flagpls http://10.10.82.43:8081/ctf/sendcookie
thm{c10b5cb7546f359d19c747db2d0f47b3}
```

That’s it! This is going to be useful in web-based CTFs.