Infosec Institute CTF level 5 Write Up

Chris Issing

Nov. 18, 2015

1 Read the challenge Description

The challenge starts off by telling us that we need to have visited the `login` page before we can viewing the challenge [age. This makes it seem like you have to login before you can access the other page, but in reality, we can just trick the website to think we logged in before.

2 About the exploit

First we have to determine what the actual login page is. We can do that by reading the HTML code of the website. In browsers like chrome or firefox, we can use the inspect element tool. If we wanted to do it through the command line on a unix based system like a Linux OS or Mac OS X, we would open the Terminal Application and use the `curl` command. `curl` is a to that can be used to transfer data to and from a server. You can read more up on what `curl` does by reading the manpage with the command `man curl`. In the HTML, we notice that there is a disabled link to `login.html`. Now that we know the url that we need to go to before we can access the challenge page (`http://ctf.infosecinstitute.com/ctf2/exercises/ex5.php`). We can use one of `curl`'s features, that will allow use to forge the `Referer` header. Using the command `curl --refer [LOGIN URL] [CHALLENGE URL]` we can pretend that we visited the login page right before the challenge page.

3 Final Exploit

The final command that would solve this challenge would be

```
curl --refer http://ctf.infosecinstitute.com/ctf2/exercises/login.html
http://ctf.infosecinstitute.com/ctf2/exercises/ex5.php
```

We know we solved it because we will see

```
<p class="lead">Gosh, you were fast.  You completed Level 5.  You will be redirected
to level 6 in 10 seconds.</p>
```

We can go even further and check to see all the HTTP Headers by adding the verbose option `-v`

```
* Connected to ctf.infosecinstitute.com (52.27.151.103) port 80 (#0)
> GET /ctf2/exercises/ex5.php HTTP/1.1
> Host: ctf.infosecinstitute.com
> User-Agent: curl/7.43.0
> Accept: */*
> Referer: http://ctf.infosecinstitute.com/ctf2/exercises/login.html
>
```