bob

daven farnham

March 2017

1 Finding the PIN

I wasn't able to get all the way to the flag; I was able to log onto the router's homepage after finding the PIN. However, trying to inject an attack into the GET request in the

```
?action=view
```

field sometimes would cause my system to crash, so I never quite got all the way. Still! A very fun assignment!

The way I attacked this was by uploading multiple files in the 'grades' section of Foo's website. Although the files take .pdfs, if you use the extension .pdf.php you can upload code onto the server.

The three main files I used in this attack were:

- **handle.pdf.php**
- **index.pdf.php**
- **inject.pdf.php**

index.pdf.php rewrites the code in index.tpl in the templates folder. It adds javascript: a loop that'll make numerous XMLHttpRequests to Bob's router.local. When you open inject.pdf.php (another file you've uploaded), it'll copy the code you've written in index.pdf.php into index.tpl. Now, whenever Bob visits index.php, he'll unknowingly be making numerous requests to his router, trying different pin numbers.

When I was trying to brute force the pin, I noticed I could only make about 150 requests before Bob refreshed the page. The responses from Bob's router I then sent, through another XMLHttpRequest, to handle.pdf.php which would write the content out to a file with the PIN number appended to the end of the file. This way I could check the files and once one returned with me logged in, I would know the pin from the file name.

To make this a bit easier, I used a number of helper files:

- **cleanup.pdf.php**
- **diff.pdf.php**

cleanup.pdf.php would delete files that accumulated in the /handins directory, while diff.pdf.php would run the shell command 'diff' to find the response from bob's router that was different from the usual "incorrect password or username". This was actually important, since the first time I tried brute forcing this I just looked at the file sizes, assuming the correct PIN would return a file that was of a different size. For some reason, the first time I tried, though, this didn't happen and it wasn't until I ran diff.pdf.php that I found the correct file. The correct PIN for my VM is **9210**.

2 The Flag

Once logged onto Bob's router's homepage, I tried messing with the GET action variable. From the handout it mentioned RCE, so I tried a couple things:

1. check to see if php might be calling eval()
2. see if I could do straight shell injection
3. try to inject javascript into the GET variable

A number of my attempts are in **action.pdf.php**. What kept happening to me, though, is I think some of these attempts were working, but the syntax was slightly off, which would cause the system to freeze up, resulting in a 403 error when I tried resetting everything. If I could've gotten a shell command to run, I couldn't checked out the files on the system using 'ls' and then basically done whatever I wanted.