CSSS 3510 Writing Secure Code

Spring 2 2020

Author: Jose Pablo Murillo

Hands-on lab report

Annex 2 – Sample code

Web page with simple form.

****

Index.html

****

```
<!doctype html>
<html>
   <head>
      <title>File creation</title>
   </head>

   <body>
      <form action="unsafeResponse.php" method="post">
         <label for="fileName">Enter the name of the file</label>
         <input type="text" name="fileName" id="fileName">
         <input type="submit" name="submit" value="Create file">
      </form>
   </body>
</html>
```

****

unsafe.php

****

```
<?php
   $fileName = $_POST['fileName'];
```

```
   system("touch $fileName", $retval);
   if ($retval == 0) {
      echo("$fileName created");
   } else {
      echo ("Whoops, something is not right");
   }
?>
```

****

Safe.php

****

```
<?php
   $fileName = $_POST['fileName'];
   $escapedFileName = escapeshellcmd($fileName);
   system("touch $escapedFileName", $retval);
   if ($retval == 0) {
      echo("$fileName created");
   } else {
      echo ("Whoops, something is not right");
   }
?>
```