VotD: Cross-Site Request Forgery (CSRF)

Attack Pattern: See CAPEC-62 (https://capec.mitre.org/data/definitions/62.html)

Weakness/Vulnerability: See CWE-352 (http://cwe.mitre.org/data/definitions/352.html) . Another good description (http://www.cgisecurity.com/csrf-faq.html) .

Description: When you log in to websites, they often will send a browser cookie that helps preserve your session on the website. For example, an e-commerce site might write a 'token' to the cookie that identifies you, and also write a list of the items in your 'cart' in case you browse away and then come back to site. The idea behind CSRF is to get you to unknowingly send a request to a website to do something by taking advantage of the fact that you have already authenticated to the site.

DVWA and Fuzzer:

- Make sure the DVWA Security level is set to Low.
- Go to the CSRF page and change the admin password to 'seahawk'
- Take note of the resulting URL at the top. This URL suggests that an HTTP GET (https://www.w3schools.com/tags/ref_httpmethods.asp) request is used to send data to the web server and persistently change the password. Bad idea!
- Now log out of DVWA. The login info is now admin/seahawk.
- An attack would be getting a user to load an HTML page with a malicious request. Download and unzip csrf.zip (https://uncw.instructure.com/courses/16302/files/470575/download?wrap=1) . Open the html file in a web browser and you will see a web page with a broken image. Edit the .html file with a text editor and you will see this image tag: `<img src="http://127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=12345&password_conf=12345&Change=Change#">` that is attempting the CSRF.
- The CSRF will FAIL if you are logged out of DVWA. Remember, the dstinguishing feature of CSRF is that is leverages the trust a website places in a user's cookies/session after logging in.
- So, go login to DVWA with admin/seahawk. Now refresh the csrf.html file you have open in the web browser. The attack will change the admin password to 12345.
- Log out of DVWA and try logging in with admin/seahawk. You will be locked out. The new password, set without your knowledge, is admin/12345

Mitigations:

- As a rule, don't allow HTTP GET requests to perform persistent modifications to the website or website data
- If a GET does still need to make a modification, then require authentication within that HTTP request (see DVWA as an example).
- Session tokens should not be allowed in URLs, only in cookies.
- Many web application frameworks will produce a CSRF token with forms. These are random numbers that the server provides to presented forms, and expect before processing any POST requests.

However, these can be circumvented when other situations such as XSS are possible.

Notes

- Technically, this is not cross-site scripting as no script is being executed on user's browser. However, CSRFs allow attackers to fool victims into sending GET requests to malicious sites or by modifying something in the app itself.
- CSRF is one reason that many email clients don't show images upon initially showing an email.