Hack Night

Week 4: Web Security (cont.)

But first...

Make sure you have signed in!

Grab some food :)

Hack Night chat: https://hn-chat.csaw.io

Sign up link: https://goo.gl/rSpeIO

Join our mailing list: https://goo.gl/wReOU5

Client-Server Relationship

Authorized actions should only be able to be performed by the user.

How does the server keep track of who you are?

- IP address
- Session cookie

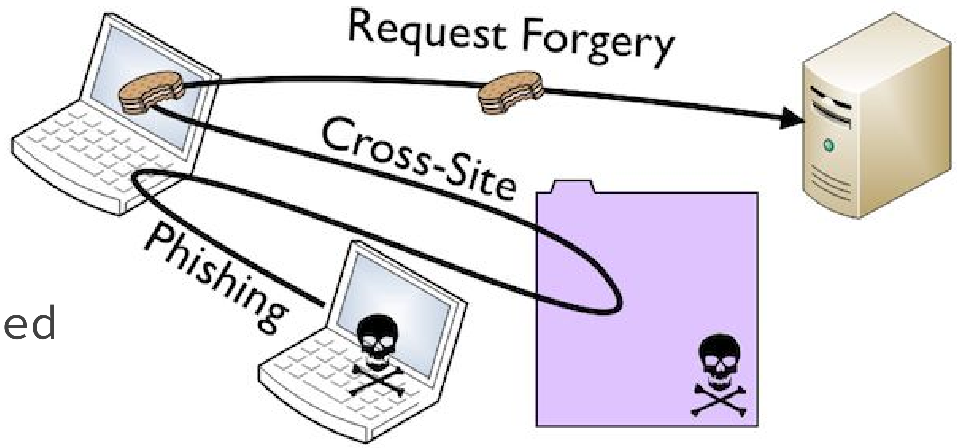
That should be enough to stop others from pretending to be that user right?

Cross Site Request Forgery

Wrong.

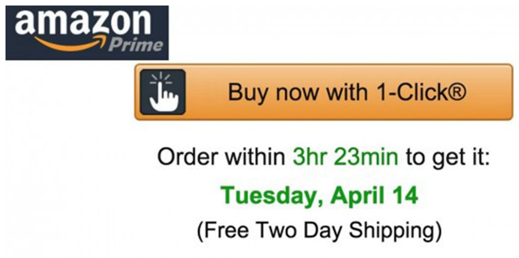
A CSRF attack is where an attacker gets the user to unknowingly perform authorized actions on the client side.

Some examples include: logging the user out, changing the user’s password, sending a message as a user.



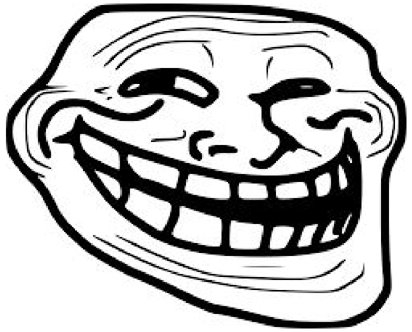
CSRF Example

URL: amazon.com



```
<form action=”buy.php” method=”post”>
     <input id=”product-id” type=”hidden”
value=”n” />
     <input id=”buy-now” type=”submit” />
</form>
```

URL: lulz.xyz



```
<form style=”display:none”
action=”http://amazon.com/buy.php”
method=”post” onload=”this.submit();”>
     <input id=”product-id” type=”hidden”
value=”n” />
     <input id=”buy-now” type=”submit” />
</form>
```

CSRF Mitigation

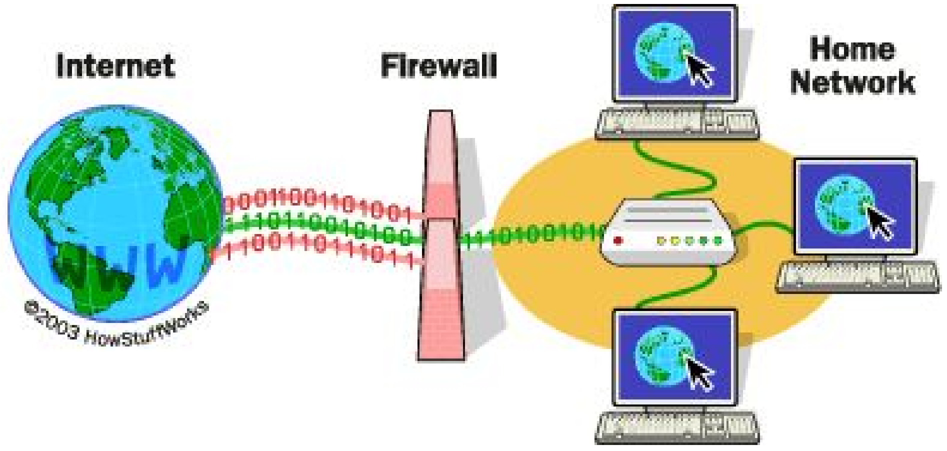
1) Check HTTP Origin and Referer headers to determine where the request was created

2) Use a CSRF Token (a random value injected into the form by the server) so the attacker will not have this value and so the server will reject the request

Server Side Request Forgery

Similar to CSRF, but instead you are tricking the server into making unintended requests rather than the client.

SSRF lets attackers access resources that would normally be unavailable or blocked



SSRF Example

Valid Client Requests

http://example.com

https://example.com

Invalid Client Requests

ftp://example.com

example.com:22

Valid Server Requests

http://example.com

https://example.com

ftp://localhost

mysql://127.0.0.1

file://127.0.0.1/../../etc/passwd

SSRF Mitigation

Sanitize input and check for dangerous ports, domains, and URI schemes

http://blog.includesecurity.com/2016/08/safeurl-server-side-request-forgery-protection-library.html

https://github.com/JordanMilne/Advocate

Path Traversal

When the user can provide the path of a file to fetch, it might be possible to fetch files from anywhere in the filesystem by using path traversal.

Ex:

http://example.com/get_file.php?file=info.txt

http://example.com/get_file.php?file=../../../etc/passwd

Useful Tools

Burp Suite: Web Pentesting tool

Wireshark: Network Traffic Analysis Tool

cURL: Swiss army knife of web requests