Class Notes

September 16th, 2021

**Basic Auth**

Sends username & password on every HTTP Request

Base64 string includes the username and password

**Cookie Auth**

Cookie: Session Token sent on each HTTP Request

Session cookies do not contain username and password

Cookie Attributes control what they can/cant do

Webserver sends the cookie

IsAuth = 1 to access, 0 not

Set scope to domain or the path of the website

**Cookie Attribute - Domain:**

example.com or foo.example.com

**Cookie Attribute – Path:**

Path = /blue/index/html

**Cookie Attribute – Secure:**

Send over Https ONLY

HTTPS packet information is encrypted unlike HTTP

**Cookie Attribute – HTTPOnly:**

No JavaScript with be accessed by the website

Protects against cookie stealing because no JavaScript can't access the webpage

**HTTP Script Transport Security (HSTS):**

A website can tell your browser to always send requests over HTTPS

For HSTS to work you first need to visit the website but browsers can load a list from Google

**Research Paper to see if Secure & HTTOnly are even useful:**

* Make account
* Log in
* Automate the process for more webpages
* Examine cookie headers
* Test website with any cookie to see if it’s a valid authentication cookie, if not the server will respond with a valid one
* Logged into 167k of 1.6 million websites
* Were able to log in to about 24k of them
* They concluded that websites were vulnerable to eavesdropping if it did not include HTTPonly and Secure tags on.
* 12k were vulnerable to ease dropping
* 5k were vulnerable to cross site injection
* 1.8k website were misconfigured and still allowed it