



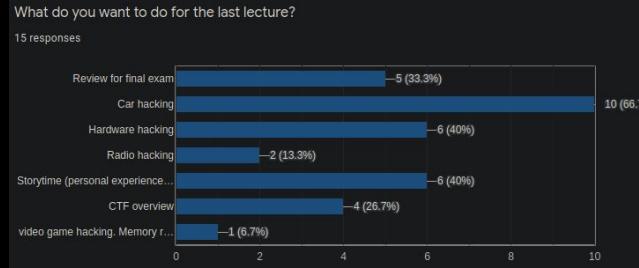
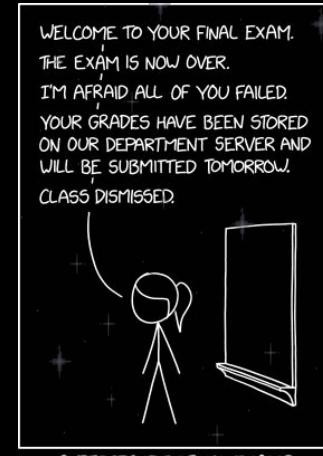
CMSC388U

Web I & II



Announcements

- Web I and Web II are combined - today!
- HW 10 (this week's) will be due by next lecture
 - This is the final write-up!
- Topics for 4/30 and 5/7 are up for discussion
 - Keep an eye for new poll on Piazza/ELMS
- Final Exam!
 - Will be CTF-like, with an overview of the concepts covered in the class
 - Specifics will be announced soon
 - Will be open for a week (will not take that long!)
 - 5/7 @ 3:30pm ET to 5/14 @ 3:30pm ET



Homework #9 Review

- **Question 1A**
 - Y21zYzM4OHV7ZW5jb2RpbmchPWVuY3J5cHRpb24tcmlnaHQ/fQ==
 - Base64 decode
 - echo Y21zYzM4OHV7ZW5jb2RpbmchPWVuY3J5cHRpb24tcmlnaHQ/fQ== | base64 -d cmsc388u{encoding!=encryption-right?}
- **Question 1B**
 - pzpf388h{prnfre_jnfa'g_gung_fzneg}
 - ROT13 decode!
 - cmcs388u{ceaser_wasn't_that_smart}

Homework #9 cont.

- Question 2
 - Issue with how original fake breach was generated

```
for line in $(shuf -n 50 rockyou.txt) do
    pw_hash=$(cat rockyou.txt | shuf -n 1 | tr -d "\n" | md5sum | awk '{print $1}')
    echo "$line@sna.pp:$pw_hash"
done
```



- “Raw-MD5” should have taken seconds to crack
 - Unsalted MD5 is not a strong algorithm against brute forcing

```
(kali㉿kali)-[~/HW9]
$ wget -q https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
(kali㉿kali)-[~/HW9]
$ wget http://supersecure.store:9901/hash.txt
--2021-04-23 00:10:06-- http://supersecure.store:9901/hash.txt
Resolving supersecure.store (supersecure.store) ... 18.191.224.93
Connecting to supersecure.store (supersecure.store)|18.191.224.93|:9901 ...
HTTP request sent, awaiting response ... 200 OK
Length: 2485 (2.4K) [text/plain]
Saving to: 'hash.txt'

hash.txt          100%[=====]  2.43K --+--KB/s   in 0s

2021-04-23 00:10:06 (237 MB/s) - 'hash.txt' saved [2485/2485]
```

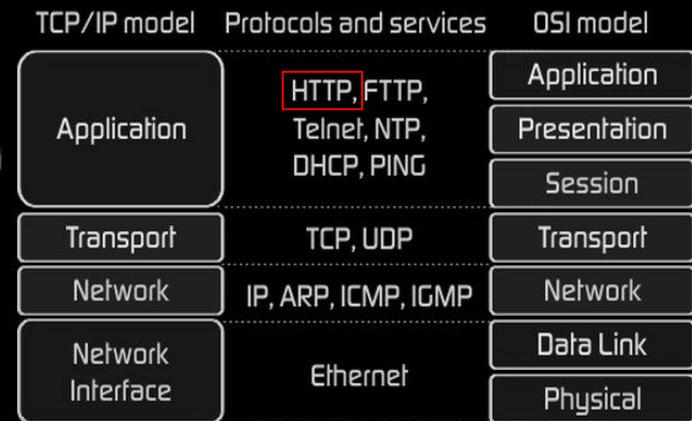
```
(kali㉿kali)-[~/HW9]
$ john --wordlist=./rockyou.txt --format="Raw-MD5" ./hash.txt
Using default input encoding: UTF-8
Loaded 50 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
```

```
(kali㉿kali)-[~/HW9]
$ john --format="Raw-MD5" --show ./hash.txt
0843089856@sna.pp:3655848
0926548151@sna.pp:lysabug17
camilaniky@sna.pp:330084
60985bucaneros15@sna.pp:canoramos
iloveang@sna.pp:0851902709
va40ni@sna.pp:muephy
nayeliscarlett@sna.pp:5261192
P0ReLmundo8@sna.pp:mindy
thanos@sna.pp:decieann07
```

This would have a different output if it wasn't run before

HTTP

- HyperText Transfer Protocol
- What is it?
 - Protocol that is used to interact with web applications
 - Interfaces between web browser and internet
- OSI Model?
 - Open Systems interconnection model
 - Demonstrates modern internet/network abstraction
 - Modern CS mostly stays from Network up
 - Lots of fun to be had lower!



HTTP Response Codes

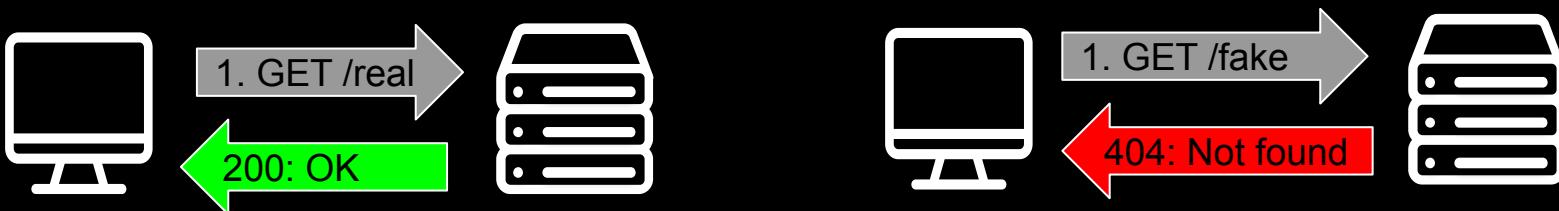
- When you send a request to a web server you'll get a response
- Depending on the status of the request the corresponding resp code will be sent back to you
- Example: 404 not found pages!



- **100: Informational Responses**
- **200: Successful**
 - Success/Ok
- **300: Redirecting**
 - 301: Permanent Redirect
 - 302: Temporary Redirect
 - 304: Not Modified
- **400: Client Errors (your fault)**
 - 401: Unauthorized
 - 403: Forbidden
 - 404: Not found
- **500: Server Errors (not your fault)**
 - 502: Bad gateway
 - 503: Service unavailable

HTTP Request Methods

- Within HTTP there are multiple types of requests you can make to webservers
- When you want to receive content - browser sends a GET request
- When you want to send content - browser uses a POST request
- There is also - PUT, OPTION, HEAD, DELETE, CONNECT, TRACE, PATCH



HTTP Cookies

- “Small piece of data stored in the web browser that is used to remember stateful information (settings, username, password, logged in, etc)
- Stored client side
 - Can be modified by user!
- Persistent, server can set expiry time
- Used to track users across websites
- Secure - specifies that they can be transferred with only HTTPS
- Extra reading: <https://samy.pl/evercookie/>



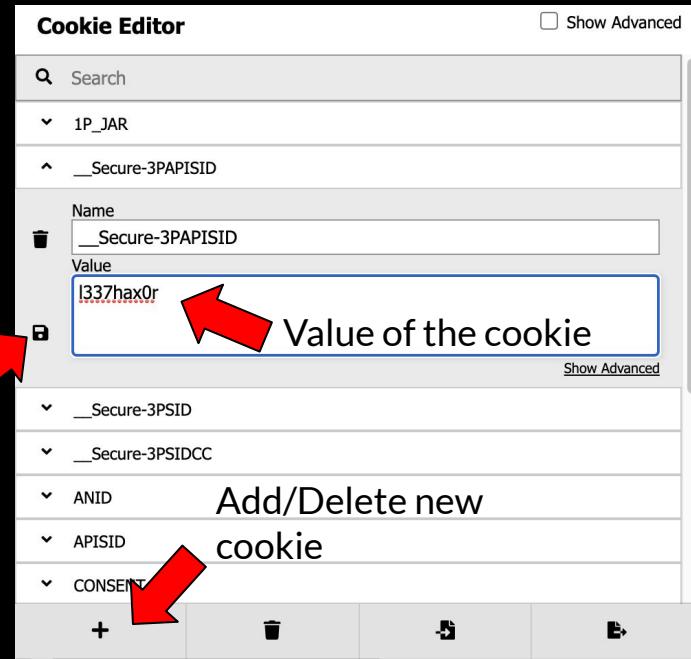
A screenshot of a browser's developer tools showing the cookie list. The list includes various cookies such as _gid, _rdt_uid, fpestd, has_js, mp_dfdc461caa5b279eab322a99fcc0762_mixpanel, nmstat, and UUID. The UUID cookie is selected, showing its name, value (b8ac6ea7-a4a5-15a4-8 [REDACTED]), and a 'Show Advanced' button.

Name	Value
UUID	b8ac6ea7-a4a5-15a4-8 [REDACTED]

Modifying Cookies

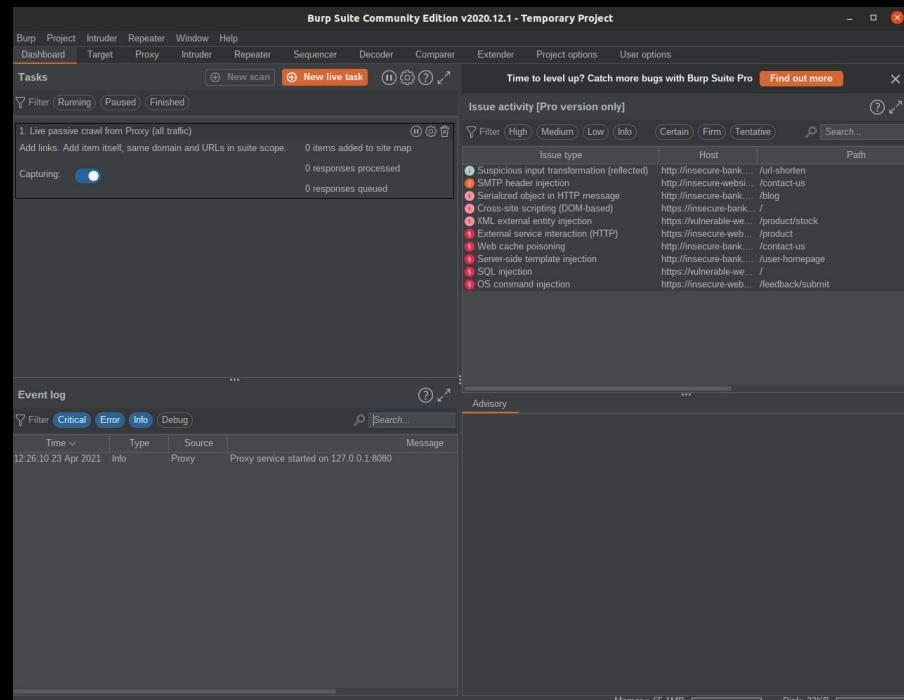
- Tons of browser plugins for this
 - EditThisCookie
 - Cookie-Editor
 - Natively in Chrome/Firefox Dev tools
- Important values:
 - Name (what js looks for)
 - Value
 - State
 - Expiry
 - Secure

Save the cookie



BURP

- Great multi tool for web security analysis
- General workflow:
 - Proxy traffic through burp
 - Either make your browser/device proxy through or use burp's embedded browser
 - Intercept/examine/modify/etc the traffic burp gets



Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
134	https://umd.edu	GET	/			200	53268	HTML		The University of Mar...	✓	99.84.176.5	
141	https://www.youtube.com	GET	/embed/sN4ynr6QbtA?rel=0		✓	200	52382	HTML		YouTube	✓	142.250.73.238	
142	https://umd.edu	GET	/js/user-alert/get-message			200	963	JSON			✓	99.84.176.5	
143	https://content-autofill.goog...	GET	/Nl/pages/Chc2LjEuMTcxNS4xN...		✓	400	652	script			✓	172.217.164.138	
144	https://googleleads.g.double...	GET	/pagead/id			200	991	JSON			✓	142.251.33.194	
146	https://www.youtube.com	GET	/iframe/api			200	1675	script			✓	142.250.73.238	
147	https://www.youtube.com	GET	/embed/sN4ynr6QbtA?rel=0&ena...		✓	200	52426	HTML		YouTube	✓	142.250.73.238	
149	https://www.youtube.com	GET	/generate/2047Dn.9Mg		✓	204	280				✓	142.250.73.238	
150	https://insight.adsvr.org	GET	/track/tp/Advertiser=dasvnm&ref=https%...		✓	200	284	HTML			✓	3.220.172.21	
151	https://googleleads.g.double...	GET	/pagead/id			200	991	JSON			✓	142.251.33.194	
153	https://www.youtube.com	GET	/generate/2047MuuJg		✓	204	280				✓	142.250.73.238	
154	https://www.youtube.com	GET	/csi/2047=&youtube&action...		✓	204	531	HTML			✓	142.250.73.238	
155	https://google-analytics.com	POST	/collect?v=2&id=G-GYM82268...		✓	204	562	text			✓	172.217.7.174	
156	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json&...		✓	200	513	JSON			✓	142.250.73.238	

Request Response

Pretty Raw In Actions ▾

```
1 GET / HTTP/1.1
2 Host: umd.edu
3 Connection: close
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Sec-Fetch-Site: none
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Cookie: has_js=1; nmstat=c6ba9db-643a-635f-2d30-ae09e6c0adid; _gid=GA1.2.1405413829.1619145723; UUID=d9ccb756-123d-0594-fd6f-18a4dd5409a5; _gat_UA_49344270_2=; _ga_GYM822681N=GS1.1.1619145722.1.1.1619145895; _ga=GA1.2.1540893784.1619145723
```

Pretty Raw Render In Actions ▾

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Date: Fri, 23 Apr 2021 02:44:23 GMT
5 Server: Apache/2.4.6 (Red Hat Enterprise Linux)
6 X-Powered-By: PHP/5.6.25
7 X-Drupal-Cache: HIT
8 Content-Language: en
9 X-Frame-Options: SAMEORIGIN
10 X-Generator: Drupal 7 (http://drupal.org)
11 Link: <https://umd.edu/>; rel="canonical",<https://um...
```

INSPECTOR

Request Cookies (7)

NAME	VALUE
has_js	1
nmstat	cb6
_gid	GA1
UUID	d90
_gat_UA-48344270-2	1
_ga_GYM822681N	GS1
_ga	GA

Request Headers (13)

NAME	VALUE
Host	umd.edu
Connection	close
Cache-Control	max-age=0
Upgrade-Insecure-Req...	1
User-Agent	Mozilla/5.0 (Windows ...
Accept	text/html,application/x...
Sec-Fetch-Site	none
Sec-Fetch-Mode	navigate



Burp Suite Community Edition v2020.12.1 - Temporary Project

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general content

#	A	Host	Method	URL	Params	Edited	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	
1		https://accounts.google.com	POST	/ListAccounts?gtcc=1&source=...		✓	200	1203	JSON			✓	142.251.33.205		12:30:01	
2		https://www.google.com	GET	/asyncnewtab_promos			200	540	JSON			✓	172.253.62.147		12:30:01	
3		https://www.google.com	GET	/asyncnewtab_ogb?hl=en-US&a...		✓	200	166715	JSON			✓	172.253.62.147		12:30:01	
6		https://www.gstatic.com	GET	/og/_js/k=eg_qtm_en_US_3gGou...			200	119954	script			✓	172.217.7.227		12:30:05	
7		https://apis.google.com	GET	/_scs/abc-static/_js/k=qapn_gap...			200	103612	script			✓	172.217.7.206		12:30:05	
8		https://logs.google.com	GET	/widget/app/so/bc=1&ongin=chr...		✓	200	51131	HTML		301 Moved Perman...		✓	142.251.33.206	NID=214=rHKv...	12:30:05
10		http://umd.edu	ET	/			301	568	HTML					99.84.176.5		12:30:21
11		https://umd.edu	GET	/sites/umd.edu/files/jsp/xKaMc...			200	9471	HTML		The University of Mar...		✓	99.84.176.5		12:30:21
16		https://umd.edu	GET	/sites/umd.edu/files/jsp/xKaMc...			200	963	script	js			✓	99.84.176.5		12:30:21
17		https://umd.edu	GET	/sites/umd.edu/files/jsp/38VW...			200	4035	script	js			✓	99.84.176.5		12:30:21
19		https://ajax.googleapis.com	GET	/sites/lib/jquery/1.10.2/jQuery.m...			200	33805	script	js			✓	172.217.164.138		12:30:21
20		https://umd.edu	GET	/sites/umd.edu/files/jsp/9tQmVA...			200	240	script	js			✓	99.84.176.5		12:30:21
21		https://umd.edu/bootstrap...	GET	/bootstrap/3.3.7/js/bootstrap.min.js			200	38314	script	js			✓	104.18.176.207	ctid=rf5de...	12:30:21
22		https://umd.edu	GET	/sites/umd.edu/files/jsp/khWAY...			200	10015	script	js			✓	99.84.176.5		12:30:21
23		https://umd.edu	GET	/sites/umd.edu/themes/umt/build...			200	13357	XML	svg			✓	13.32.206.122		12:30:21
29		https://www.googletagmanager...	GET	/gtm_js?id=GTM-KKOTNDW			✓	200	112324	script	js			142.250.73.232		12:30:21
30		https://www.youtube.com	GET	/embed/dNyn6CjwNa?rel=0			✓	200	56332	HTML		YouTube		172.217.9.206	YS=CQzCzI3J4...	12:30:21
31		https://adsnr.org	GET	/ua_bader_1.1.0			✓	200	5066	script	js			172.217.9.206		12:30:21
35		https://www.youtube.com	GET	/s/player/f2244af1www/embed-p...			✓	200	191313	script	js			172.217.9.206		12:30:21
37		https://umd.edu	GET	/sites/umd.edu/themes/umt/build...			✓	27768	woff2					99.84.176.5		12:30:21
									...							

Request Headers (10)

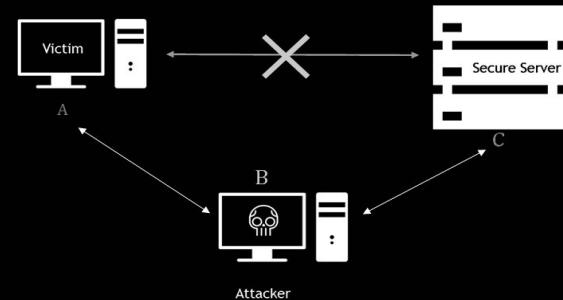
NAME	VALUE
Host	umd.edu
Connection	close
User-Agent	Mozilla/5.0 (Windows ...
Accept	*/*
Sec-Fetch-Site	same-origin
Sec-Fetch-Mode	no-cors
Sec-Fetch-Dest	script
Referer	https://umd.edu/
Accept-Encoding	gzip, deflate

Response Headers (16)

NAME	VALUE
Content-Type	application/javascript

SSLstrip & HSTS, a story

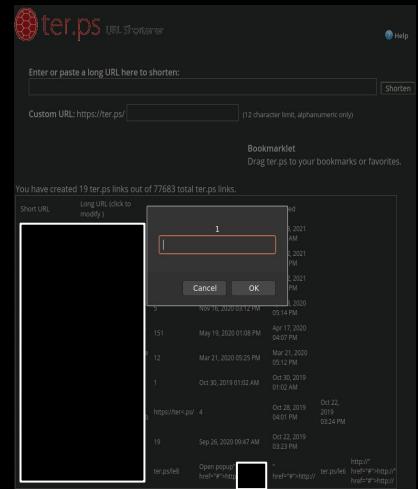
- Example of a downgrade attack
- Evil access point that redirects HTTPS queries to HTTP, which can be intercepted
- Fixed with “HTTP Strict Transport Security” (HSTS)
- Timeframe:
 - SSLstrip (10 years ago)
 - HSTS
 - SSLstrip+/SSLstrip2 (7 years ago)
 - HSTS updated



<https://arnavtripathy98.medium.com/sslstrip-tool-for-fighting-https-e917d76b0d45>

XSS

- “Cross Site Scripting”
 - Occurs when unsanitized user input is stored/printed back out
 - User input can contain valid HTML/Javascript/etc.
 - <script><alert>("XSS")</alert></script>
- Different types:
 - Reflected (aka “Self-XSS”)
 - Only shown against user who inputs the XSS
 - Stored
 - Becomes stored on the site, affects all users
 - DOM
 - [https://example.com/page.html?variable=<script>alert\('XSS'\)</script>](https://example.com/page.html?variable=<script>alert('XSS')</script>)
 - Blind
 - Hope that the input will be appropriately rendered somewhere
- Lots of possibilities!
 - <https://github.com/payloadbox/xss-payload-list>



^ Great video on the subject!

XSS: Electron

- ElectronJS is effectively a chromium based browser
 - Popular electron apps include:
 - Discord
 - Slack
 - Atom
 - VSCode
 - And many more!
- Note: With ElectronJS XSS can be a big issue!
 - If “nodeIntegration” is set to true (used to be default in electron):
 - XSS becomes RCE!
 - <script> require('child_process').exec('whoami'); </script>

A screenshot of a search results page from a search engine. The query 'electron rce' is entered in the search bar. The results list several articles and links related to Electron security issues:

- [About 351,000 results \(0.33 seconds\)](https://medium.com/swlh/open-sesame-escalating-a-open-redir-to-rce-with-cve-2020-16608)
 - [Open Sesame: Escalating Open Redirect to RCE With ...](https://medium.com/swlh/open-sesame-escalating-a-open-redir-to-rce-with-cve-2020-16608)
Aug 14, 2020 — For better or worse, Node.js has rocketed up the developer popularity charts. Thanks to frameworks like React, React Native, and Electron, ...
 - [CVE-2020-16608. RCE using XSS in Electron applications ...](https://ghosh2402.medium.com/cve-2020-16608-rce-using-xss-in-electron-applications)
RCE using XSS in Electron applications. TLDR: Notable 1.8.4 allows XSS via crafted Markdown text, with resultant remote code execution (because ...)
 - [https://portswigger.net/daily-swig/discord-desktop-a... |](https://portswigger.net/daily-swig/discord-desktop-a...)
Discord desktop app vulnerable to RCE via chained exploit ...
Oct 19, 2020 — The exploit (demonstrated in this video) capitalized on the fact that Discord had disabled the RCE-blocking contextualization option in Electron.
 - [https://twitter.com/bcrypt/status yan](https://twitter.com/bcrypt/status/yan)
on Twitter: "yet another example of XSS -> full RCE using ...
Aug 23, 2020 — probably the funniest Electron app RCE was one we found in Brave soon after we launched: if you drag-and-drop a tab above the tab bar, the ...
 - [https://github.com/doyensec-awesome-electronjs-ha... |](https://github.com/doyensec-awesome-electronjs-ha...)
doyensec/awesome-electronjs-hacking: A curated list ... - GitHub
A curated list of awesome resources about Electron.js (Insecure ... | Signature Validation Bypass Leading to RCE In Electron Updater", Doyensec Blog ...
 - [https://gist.github.com/1rehj |](https://gist.github.com/1rehj)
RCE using XSS in Electron. GitHub Gist: instantly share code, notes, and snippets.
 - [https://blog.doyensec.com/electron-framework-security |](https://blog.doyensec.com/electron-framework-security)
Modern Alchemy: Turning XSS into RCE - Doyensec's Blog
Aug 3, 2017 — After a quick overview of Electron's security model, we discussed design weaknesses and implementation bugs that can be leveraged to ...
 - [https://infsecwriteups.com/remote-code-execution-in-electron |](https://infsecwriteups.com/remote-code-execution-in-electron)
Remote Code Execution Through Cross-Site Scripting In ...
How to execute a Remote Code Execution (RCE) attack through a Cross-Site Scripting (XSS) payload in Electron Apps that have Node.js integration enabled.
 - [https://book.hacktricks.xyz/pentesting-web/xss-to-rce-electron-desktop-apps-hacktricks |](https://book.hacktricks.xyz/pentesting-web/xss-to-rce-electron-desktop-apps-hacktricks)
XSS to RCE Electron Desktop Apps - HackTricks
XSS to RCE Electron Desktop Apps... When I test Electron app, first I always check the options of the BrowserWindow API, which is used to create a browser ...

The right side of the screenshot shows a dark-themed Electron application window with a menu bar and various icons for file operations, including a central atom-like icon.

Build cross-platform desktop apps with JavaScript, HTML, and CSS

Ess-queue-ehl / See-quill

- Databases, in web?
 - Just a place to store data! Usernames, passwords, settings, etc
 - **Main types:**
 - MySQL
 - Postgres
 - MongoDB
 - SQLite
- Structured Query Language (SQL)
 - Used to communicate with SQL databases
 - Websites will build queries from user input
 - If done wrong can allow for leaking of information from said database



SQLi

- SQL Injection
- When user input isn't "sanitized"
 - Dangerous characters such as ' " --)
- You can make queries you aren't supposed to!
- Ex: Information supplied by user - such as a username - is passed into a query that will do something with that info (login, sign up, etc)
- Example:
 - SELECT * FROM users WHERE username='admin' ... <- Vulnerable!
 - SELECT * FROM users WHERE username='admin'--' ...



SQL Comment

SQL Map

- Tool that automates the discovery of SQLi
- Powerful but you gotta know how to use it
- Usage: `python sqlmap.py -u "http://testsite/get_thing.php?id=1"`

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
```



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting @ 10:44:53 /2019-04-30/
```

```
[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
(possible DBMS: 'MySQL')
```

IDORs

- “InDirect Object Response”
 - If you login to example.com and see:
 - <https://example.com/?userID=155>
 - What would happen if you change the URL to say:
 - <https://example.com/?userID=156>?
- If no checks were placed (other forms of authentication), incrementing/decrementing the userID could cause you to be logged in as another user!
 - This example is simplified, but not far off!



^ Great video on the subject!

LFI

- Local File Inclusion:
 - Occur when the web application allows users to read files from victim machine
 - <http://192.168.80.134/dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd>  Directory traversal to root, read etc/passwd
 - PHP is usually culprit
- Exploiting LFI
 - If a user is able to upload file - upload some malicious script .php
 - Then you can access the file using LFI
 - File may be executed

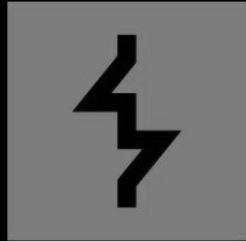
OWASP - Top X

- There are many categories of web based vulnerabilities, such as
 - XXE, CSRF, SSRF, etc.
- Open Web Application Security Project
 - List the top threats to web applications
 - <https://owasp.org/www-project-top-ten/>
 - Juice Shop: great place to practice web hacking stuff
 - <https://owasp.org/www-project-juice-shop/>



Burp Demo?

(Time permitting)



For next time

- Final HW writeup due by next lecture :)
- Keep an eye out for the ELMS+Piazza poll to vote on the topics for the next two lectures
- Don't be afraid to ask on Piazza or schedule office hours!