

Mason Competitive Cyber

**Profiling & Dissecting a Web App:
Recon to Scanning**





Media Recording Notice

This meeting is more than likely recorded. Got a problem with that? Emit a sharp screech at the nearest exec now.



CC in a nutshell

- Established (**yes we're sanctioned**) in 2016, maxing out meetings our first year at about 6 people, then in Fall '17 30 or 40 across both rooms
- Established with a heavy CTF/cyber competition focus
 - Since expanded to accommodate PH gap
- Focus on hands-on work
- Chat on Slack a lot, makes almost everything available in pretty much every medium (slides, videos, VMs, etc)
- Socializes **sometimes**
- Sponsored by Battelle, possible sponsorship by The Crypsis Group
 - Due to the people that work there

How can I stay posted/involved?



- **Speak up**
 - Speak at club
 - Communicate in the Slack, stay active
 - Offer advice and constructive criticism
- **Compete**
 - 9/10 times there's no barrier to entry and we'll say when there is
 - If you aren't qualified to be on a team, rest assured we'll privately tell you to get off of it
 - You learn a lot in a small period of time, get real practice
- **Make friends**
 - We have nice people
 - A lot of them like to have fun
 - A lot of them are also a great resource



What will I learn at meetings?

What you may learn	What you probably won't
Methodologies Certain tools Techniques used in CTF or at work Exploitation tactics	How TCP/IP works How Linux works (TBD) 99% of things that can easily be described in a list in a book High prereq knowledge things (i.e. not “what's a stack”, but stack smashing exploits may be covered)



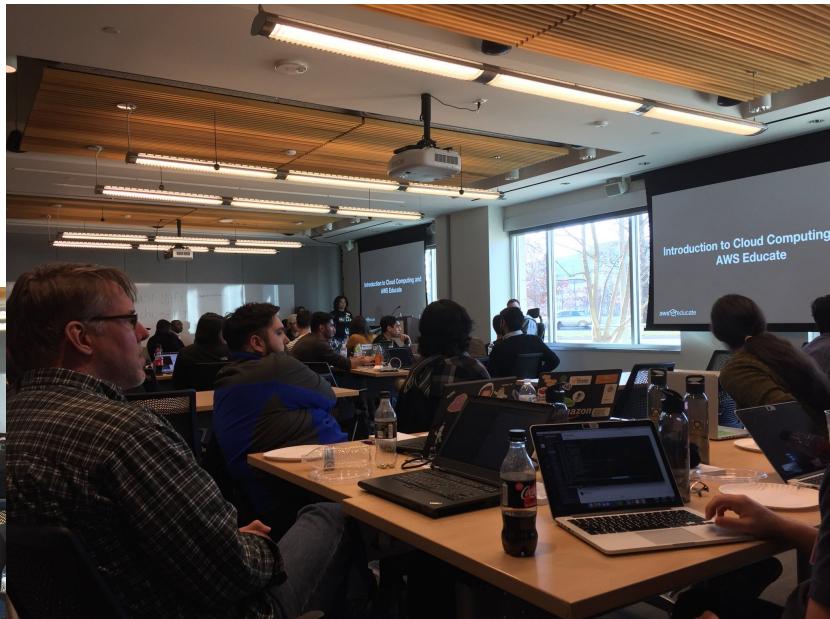
News since last meeting

- Our last meeting was months ago
 - So... Plenty?
 - But we're going to skip over that because I always skip over that
 - Some people were confused by that



Recent Competitions

- AWS Security Coding Challenge
 - 21st of December
 - We didn't organize at all, 4 of us just happened to show up
 - Teams of 5, 5 challenges, we got $\frac{4}{5}$, was a 3 way tie
 - Matt and I won Echos when they raffled off



Fall 2017 in Pictures



Upcoming Competitions & Events



- SharifCTF #sharifctf channel
- Cyber Fusion
 - All day, Feb 23
 - At VMI, Invite Only
 - Each college sends one team
- BSidesNOVA
 - Team of 8, \$20 registration fee
- CryptoParty
 - March 3 10:30am to 6:00pm
 - Includes food, a little swag, a CTF w/ prizes, etc
 - Register and see schedule at cryptoparty.gmu.io
- VT Summit, UMDCTF

Know of other competitions? *Tell us**



Recon and Scanning

- Recon and Scanning
 - Recon - Gathering information about a target
 - Scanning - Somewhat subjective
- How does it relate to real world work?
 - Any non-shit app requires more than 3 slides and random tools to hack
 - *study on your own as well*
 - There's no reason to run attacks that aren't applicable

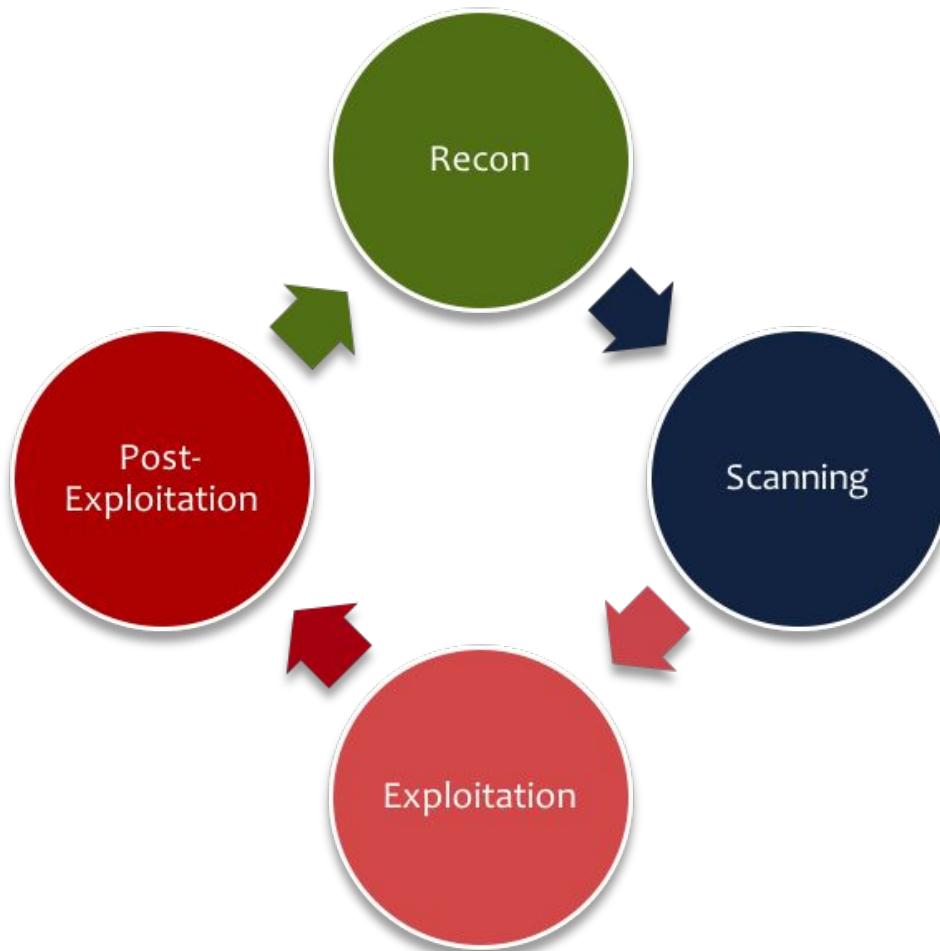


Web: Different Levels of Impact

- What is your ultimate goal?
 - Are you on a bug bounty?
 - What's in scope? Is chaining authorized?
 - CTF?
 - What are they hinting at? What is the competition's context?
 - Pентest?
 - Impact they care about? Rules of engagement? (I guess?)
- This only follows a **subset** of the ways to recon and scan a website
- Templating bugs vs content injection vs domain takeover vs command injection
 - All varying levels of impact

Understanding Cycle

- Where does web fit in the exploitation cycle?





(Chrome) Extensions To Use

- BuiltWith - Discover technologies a site is built with
- EditThisCookie or CookieInspector - Manage cookies
- ModHeader - Modify headers you send to a server
- XSS Radar or comparable scanners (I don't personally use this)

BuiltWith

Home Relationships Advanced Sign Up Log In

tctf.competitivecyber.club/

JavaScript Libraries and Functions

Moment JS	Usage Statistics · Websites using Moment JS	moment.js is a date library for parsing, validating, manipulating, and formatting dates.
Nunjucks	Usage Statistics · Websites using Nunjucks	A templating language for JavaScript from Mozilla.
jQuery	Usage Statistics · Websites using jQuery	jQuery is a fast, concise, JavaScript Library that simplifies how you traverse HTML documents, handle events, perform animations, and add Ajax interactions to your web pages. jQuery is designed to change the way that you write JavaScript.

Elements Console Sources Cookies > 13 3

Name	Value	...	S...	...	Expires (G...)
player	sequenceId=-1&paused=true...	/	Sun Feb 1...		
beacons_enabled	true	/	Fri Jan 19 ...		
visit_id	677fe299-f08d-452d-b1f6-6...	/	Fri Jan 19	
persistent_id	pid%3D4ece4b2a-b341-4290...	/	Fri Jan 01	

CookieInspector

Name	Value	...	S...	...	Expires (G...)
player	sequenceId=-1&paused=true...	/	Sun Feb 1...		
beacons_enabled	true	/	Fri Jan 19 ...		
visit_id	677fe299-f08d-452d-b1f6-6...	/	Fri Jan 19	
persistent_id	pid%3D4ece4b2a-b341-4290...	/	Fri Jan 01	

Mobile

Viewport Meta

Usage Statistics · Websites using Viewport Meta

This page uses the viewport meta tag which means the content may be optimized for mobile content.



Using Said Extensions

- Builtwith is self-explanatory, install, click on it, it tells you technologies
- Any cookie reader if you don't have Chrome suffices
 - Run **document.cookie** in Console if that's not even an option to dump them
- CTF Challenge: **Nom Nom Nom**

		Elements	Console	Sources	Network	Performance	Memory	Cookies	»	⋮	X
Name	Value									H...	Se...
session	.ejwtj01rwzAQRP9K2bMPqpJeDD0U_IELWiGQEL...	tctf.com...	31...	/		Session		True			
	masoncc{ }	tctf.com...	24 B	/		Session					
_ga	GA1.2.515893691.1504830702	.competi...	29 B	/		Sat Dec 14 201...					
_cfduid	d28d16e28ed11a6f3c683760d4be01bf615041...	.competi...	51 B	/		Fri Aug 31 201...		True			

CookieInspector at TCTF



Using What You Have

- **Actually visit the site**
 - Get application version, it may not broadcast it in a technical format
 - Related challenge: A few...
- Google/research often and carefully
- **Use built in developer tab**, we'll be using it a few times here
 - Safari: Require you go to advanced preferences, enable **Develop**, then select it from the top nav menu
 - Chrome: Dots to top right -> More tools -> Developer Tools
 - Firefox: Similar to chrome, 3 tabs -> Developer -> Select Option like Web Console
 - **Each looks very similar once you get to it**



Console Deep Dive

- **Related CTF Challenge: Heads Up**
- There are a variety of tabs available, many self explanatory, we'll focus on three

Console - Run Javascript

Elements - Breakdown of “DOM tree”, or the page’s design (similar to Right Clicking and hitting View Source/View Page Source, but more visual)

Network - My personal favorite, records requests/responses related to the page

The screenshot shows the Network tab of the browser developer tools. At the top, there's a banner for 'MASON COMPETITIVE CYBER' with the subtext 'GMU'S CYBERSECURITY ORGANIZATION'. Below the banner, a photo shows several people working at desks with laptops. A callout box highlights the text 'Solving Silly Little Puzzles Since 2016'. The Network tab has a toolbar with various filters and settings. The main area displays a timeline of network requests. One request is highlighted: 'competitivecyber.club' with a status of 304, type document, initiator 'Other', size 16.9 KB, time 287 ms, and a waterfall chart. Other requests listed include 'css?family=Open+Sans' (status 200, type stylesheet, initiator '(index)', size 0 ms), 'inuvr.min.js' (status 200, type script, initiator '(index)', size 1 ms), and 'index.html' (status 200, type document, initiator '(index)', size 0 ms). The bottom of the screenshot shows the footer with the text '23 requests | 22.0 KB transferred | Finish: 1.33 s | DOMContentLoaded: 852 ms | Load: 1.22 s'.



More on Network Tab

- Click on interactions to view details about them, both their request and response
 - In Chrome, **Headers** and **Response**
- Good for determining higher level versions of what the sites running, such as language, web server, HTTP version, any sort of caching, etc
- Pay special attention to Headers in TCTF when you load it.

The screenshot shows the Chrome DevTools Network tab. At the top, there's a toolbar with icons for zoom, refresh, and various tabs: Elements, Console, Sources, Network (which is underlined in blue), Performance, Memory, Application, Security, Audits, and Cookies. Below the toolbar is a control bar with a red dot, a circular icon, and several buttons for View (grid, list, group by frame), Preserve log, Disable cache, Offline, and Online. A timeline below the controls shows time markers at 200 ms, 400 ms, 600 ms, 800 ms, 1000 ms, and 1200 ms. Underneath the timeline, a list of network requests is shown. The first request, 'tctf.co...', has its 'Headers' tab selected. The Headers panel displays the following:

Name	Value
Server	gunicorn/19.7.1
Server-Version	
Vary	Accept-Encoding

Below the Headers panel, there are tabs for Preview, Response, Cookies, and Timing. At the bottom of the request row, there's a 'Request Headers' button and a 'view source' link.



Getting briefly into Linux

- **Basically everyone should be familiar, especially if you're a STEM major and plan on going to a STEM career**
- If you have a Gmail, visit: <https://go.gmu.edu/linux>
 - This will wipe after a while
- If you don't but are a GMU student, visit:
<https://go.gmu.edu/gmuvcl>
 - New Reservation, Note the HTML5 RDP Session option when you wait a few seconds after you hit “Connect!”
 - For meeting purposes, pick any Ubuntu based VM
- Be prepared to install Docker at some point



Actually Using Linux

- Tools we're gonna use today in Linux:
 - dirb - Directory buster
 - dnsrecon - DNS reconnaissance tool

```
apt-get install dnsrecon -y  
wget go.gmu.edu/dnslist -O /tmp/dnslist
```

```
curl -L go.gmu.edu/dirb|sudo bash
```

when done, you should be able
to run **dirb** and **dnsrecon**



Dir Busting

- Appeared in a HackEd CTF challenge
- Brute forces files and directories in a website
- /uploads, /admin, etc among app-specific ones
- Uses a “wordlist”, a list of words to try, also used in our dnsrecon demo

Related TCTF problem: Busted Deer

Using Windows? Run DirBuster

Using Linux (or MacOS)? Run **dirb**

Usage: **dirb https://tctf.competitivecyber.club**



Dirb Run Example

```
root@cloudshell:~$ dirb https://tctf.competitivecyber.club  
-----  
DIRB v2.22  
By The Dark Raver  
-----  
  
START_TIME: Fri Jan 19 01:25:00 2018  
URL_BASE: https://tctf.competitivecyber.club/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----  
  
GENERATED WORDS: 4612  
  
---- Scanning URL: https://tctf.competitivecyber.club/ ----  
==> DIRECTORY: https://tctf.competitivecyber.club/[REDACTED]  
-> Testing: https://tctf.competitivecyber.club/25
```



DNS Brute Forcing

- In bug bounties and pentests, I recommend dnsdumpster.com in addition to this technique
- Simply run **dnsrecon** to expose options

```
root@cloudshell:~$ dnsrecon
Version: 0.8.10
Usage: dnsrecon.py <options>

Options:
  h, --help           Show this help message and exit.
  -d, --domain       <domain>          Target domain.
  i, --range          <range>           IP range for reverse lookup brute force in formats (first-last) or in (range/bitmask).
  n, --name_server   <name>           Domain server to use. If none is given, the SOA of the target will be used.
  -D, --dictionary   <file>           Dictionary file of subdomain and hostnames to use for brute force.
  f                  Filter out of brute force domain lookup, records that resolve to the wildcard defined
                      IP address when saving records.
  -t, --type          <types>          Type of enumeration to perform:
    std      SOA, NS, A, AAAA, MX and SRV if AXFR on the NS servers fail.
    rvl      Reverse lookup of a given CIDR or IP range.
    brt      Brute force domains and hosts using a given dictionary.
    srv      SRV records.
    axfr     Test all NS servers for a zone transfer.
    goo      Perform Google search for subdomains and hosts.
    snoop    Perform cache snooping against all NS servers for a given domain, testing
              all with file containing the domains, file given with -D option.
    tld      Remove the TLD of given domain and test against all TLDs registered in IANA.
    zonewalk Perform a DNSSEC zone walk using NSEC records.
  -a
  -s
  -g
  -w
  -z
  --threads         <number>        Performs a DNSSEC zone walk with standard enumeration.
  Number of threads to use in reverse lookups, forward lookups, brute force and SRV
  record enumeration.
  --lifetime        <number>        Time to wait for a server to response to a query.
  --db              <file>          SQLite 3 file to save found records.
  --xml             <file>          XML file to save found records.
  --iw              Continue brute forcing a domain even if a wildcard records are discovered.
  -c, --csv          <file>          Comma separated value file.
  -j, --json         <file>          JSON file.
  -v                  Show attempts in the brute force modes.
```



DNS Brute Forcing Command

- **Related CTF Challenge: A Record to Remember**
- dnsrecon -D /tmp/dnslist -d tctf.competitivecyber.club -t brt
- Should produce any records in the wordlist
- Some wordlists are much larger, and as such take longer to run
 - This one is *quite* small

```
-v                                     SHOW ATTEMPTS IN THE BRUTE FORCE MODES.  
root@cloudshell:~$ dnsrecon -D /tmp/dnslist -d tctf.competitivecyber.club -t brt  
[*] Performing host and subdomain brute force against tctf.competitivecyber.club  
[*]      A [REDACTED] 54.172.0.227  
[*] 1 Records Found  
root@cloudshell:~$
```



Proud Sponsors

Thank you to these organizations who give us their support:

BATTTELLE

It can be doneTM