Cyber@UC Meeting 101

// Vulnerability and Exploit Basics //

If You’re New!

- Join our Slack: cyberatuc.slack.com
- Join our gitlab: gitlab.com/cyberatuc
- **SIGN IN!** *(Slackbot will post the link in slack)*
- Feel free to get involved with one of our committees:

  Content Finance Public Affairs Outreach Recruitment Lab

- **Elections will be held at the first November meeting**

Announcements / Upcoming Events

- 10.5 Hack Ohio (OSU Hackathon) Registration Closes
- 10.11 GE Aviation SOC visit
- 10.16 NSA Visit
- 10.30 Rockwell Automation Visit

Cyber@UC tours

October 11th, from 9:00am - 3:30pm

GE Security Operations Center Visit
20 spots open

Itinerary:

- Learning Center Tour to overview jet engine technologies
- Individual Team Walk-throughs:
  - Data Protection
  - Intel
  - Detect
  - Vulnerability Management
  - Application and Data Services
- Security Operations Center in-depth tour

Bring Resumes and sign up as soon as possible!
https://forms.gle/Wqf26pCi1591pPSPA

GE Aviation Security

Weekly News

Comodo Breach

- Remote code execution through vBulletin vulnerability
- Dumped 170,000 users data
  - usernames/passwords/salts
  - emails
  - most recent IP
- Happened four days after patch was released
- Second breach this year

COMODO

https://www.scmagazine.com/website-web-server-security/attacker-breaches-comodo-forums-by-exploiting-vbulletin-flaw/

Open Document Malware

- AVs are treating OD files as standard archives
- Majority was MS Office with some OpenOffice and LibreOffice
- Used Object Linking and Embedding to drop binaries on the system
  - Spotify.exe (.NET binary)
  - Filled with packers
- End payload was “AZORult”

https://threatpost.com/hackers-turn-to-opendocument/148817/

Hospital Ransomware

- Hospitals in US and Australia were hit
- Undisclosed amount of money
- Had to turn away new patients and cancel surgeries
- Adds more to the ransomware scare
- DHS Cyber Hunt and Incident Response Teams Act

https://threatpost.com/ransomware-attacks-leave-u-s-hospitals-turning-away-patients/148823/

Vulnerabilities and Exploits

Agenda

- I wasn’t here last week!
- Forewarning
- Vulnerabilities
  - CVE’s
  - Detecting Vulnerabilities
- Exploits
  - Off the Shelf Exploits
- Metasploit / Armitage
- Training Environment

I wasn’t here last week!

- Shame on you
- Previously, we went over the core docker basics
- Today works much nicer with docker or a full Kali machine
- You can do this on Windows but it would literally be faster to setup a Kali VM and use that

Forewarning

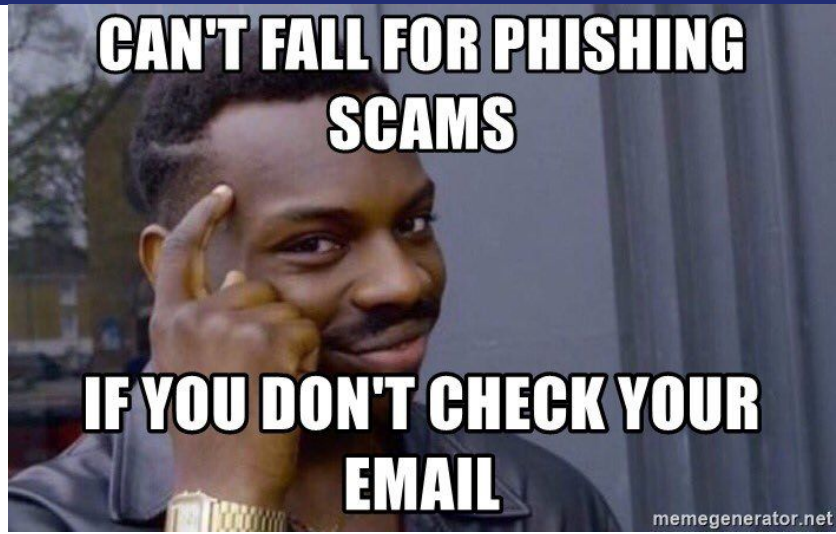
- Today’s tools are meant to demonstrate how dumb easy it can be to use canned exploits

- Metasploit can be used to do malicious things so don’t be fucking stupid

- We do not condone using either of these tools on devices you do not own or have permission to modify

Vulnerabilities

- Parts in a system that could potentially cause damage
- Typically caused by incorrect or unsafe handling of data by a program
- Some Examples
  - Not sanitizing user data
  - Misconfigured deployments
  - Incorrectly handling pointers
  - Not watching for potential attacks
  - Not training employees about spam
- These vulnerabilities can lead to potential exploitation of systems



Common Vulnerabilities and Exposures (CVE's)

- Vulnerability researchers can publish public documentation on vulnerabilities in the form of CVE's, although not all do
- Typically released after the company has had a chance to fix this issue
- CVE's typically cover what is affected and how dangerous the the vulnerability is
- This information is public so both defenders and attackers know at the same time, this is why security updates are very important

Search Results

There are **1085** CVE entries that match your search.

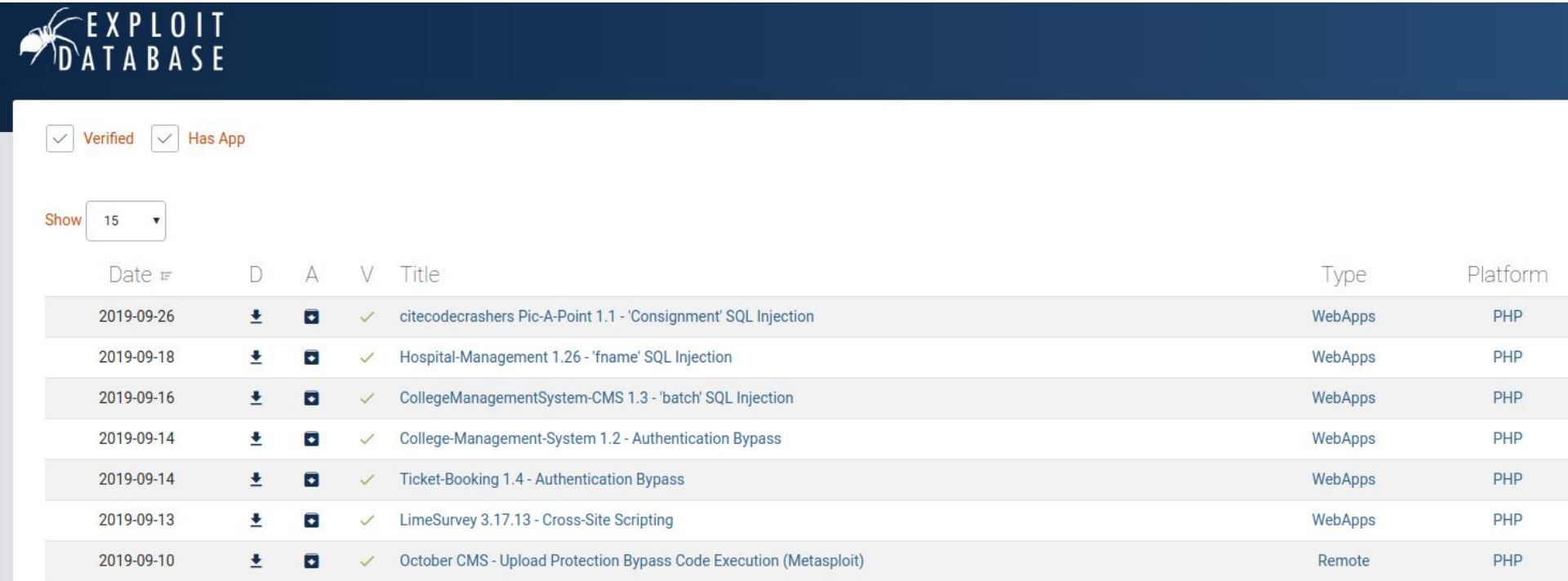
Name	Description
CVE-2019-7839	ColdFusion versions Update 3 and earlier, Update 10 and earlier, and Update 18 and earlier have a command injection vulnerability. Successful
CVE-2019-6517	BD FACSLyric Research Use Only, Windows 10 Professional Operating System, U.S. and Malaysian Releases, between November 2017 and N user access control to privileged accounts, which may allow for unauthorized access to administrative level functions.
CVE-2019-6165	A DLL search path vulnerability was reported in PaperDisplay Hotkey Service version 1.2.0.8 that could allow privilege escalation. Lenovo has e similar features.

Exploits

- Exploits use vulnerabilities to cause unexpected behaviours in a vulnerable system
- Exploits can cause:
  - Code execution
  - Information Disclosure
  - Escalating privileges
- Exploits can be reverse engineered from security updates
  - Again, why it’s important to update quickly

Off the shelf exploits

Just the same way there are public vulnerability notices, there are public exploits



Metasploit / Armitage

- Metasploit is a massive tool that can scan target machines for potential working exploits and then trivially launch attacks
  - Indexes and manages thousands of exploits and payloads
- Armitage is a GUI for metasploit that requires only basic knowledge of what you're trying to do