

Hack@UCF

Collegiate Cyber Defense Club

irc.freenode.net #hackucf Slack hackersofucf.slack.com

Stay informed!

- Join our mailing list
 - <https://hackucf.org/blog/mailing-list/>
- Join the CECS Slack
 - <https://hackersofucf.slack.com/>
 - Knights mail required
 - Once registered, chat with us in the #hackucf channel
- Twitter: @HackUCF
- Facebook
 - <https://www.facebook.com/HackUCF/>



Today's Topics

- Announcements
- Current Events
- Tool Time
- Featured Content
- Closing

Mentorship

- Mentorship program is live!
- Join #hackucf_mentors to see mentor bios, and for updates
- If you're interested in being a mentor, dm @dmaria

Shirts and Membership

We have our shirt design for this year!



Insomnihack CTF

- Saturday (1/19/2018)
- HEC 101
- All skill levels welcome!
- Beginners are encouraged!
- Starts at NOON

The screenshot shows a debugger window for a binary named 'dungeon'. The assembly view displays the following code:

```
main
00400041 push rbp
00400042 mov rbp, rsp (var_8)
00400043 sub rsp, 010
00400046 mov dword [rbp-04] (var_cj), esi
00400049 mov word [rbp-010] (var_l0), rs!
00400052 call init
00400057 test eax, eax
00400059 je 00400109

00400109 call exit
(Does not return.)

0040020b mov edi, 041a524 (" rept/dungeon")
0040020d mov eax, 0x0
00400210 call chrout
0040021a test eax, eax
0040021c je 0040020d

0040021c mov edi, 0x1a531 ("chroot")
0040021d mov eax, 0x0
0040021f call perror

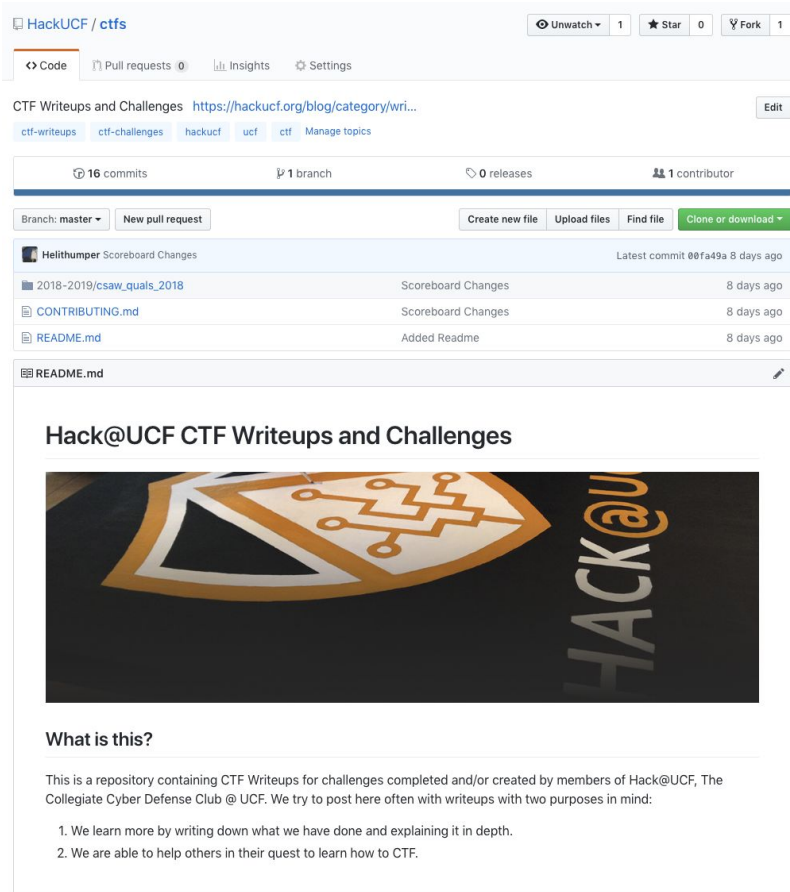
0040021f mov edi, 0x2e
00400221 mov eax, 0x0
00400223 call write
00400225 mov edi, 0x2e
00400227 mov eax, 0x0
00400229 call write
0040022b call _close
(Does not return.)
```

The control flow graph shows the execution path starting from the `main` function, through the `init` function, and then to the `chrout` and `perror` functions. The graph also shows a branch to `exit` based on the result of the `test eax, eax` instruction.



CTF Writeups

- github.com/hackucf/ctfs
- Read CONTRIBUTING.md
- [Make a Pull Request](#) with your write up!
- **Raffle for 100\$ for completed, quality writeups**
- Questions? Need Help? #knightsec on Slack, or email pduncan@hackucf.org



HackUCF / ctfs

Unwatch 1 Star 0 Fork 1

Code Pull requests 0 Insights Settings

CTF Writeups and Challenges <https://hackucf.org/blog/category/wri...> Edit

ctf-writeups ctf-challenges hackucf ucf ctf Manage topics


16 commits 1 branch 0 releases 1 contributor

Branch: master New pull request Create new file Upload files Find file Clone or download

Helthumper Scoreboard Changes	Latest commit 00fa49a 8 days ago
2018-2019/csaw_qualz_2018	Scoreboard Changes 8 days ago
CONTRIBUTING.md	Scoreboard Changes 8 days ago
README.md	Added Readme 8 days ago

README.md

Hack@UCF CTF Writeups and Challenges



What is this?

This is a repository containing CTF Writeups for challenges completed and/or created by members of Hack@UCF, The Collegiate Cyber Defense Club @ UCF. We try to post here often with writeups with two purposes in mind:

1. We learn more by writing down what we have done and explaining it in depth.
2. We are able to help others in their quest to learn how to CTF.

Operations

- Come help run the club!
 - Mondays at 6:00 PM in HEC 356
 - Open to anyone

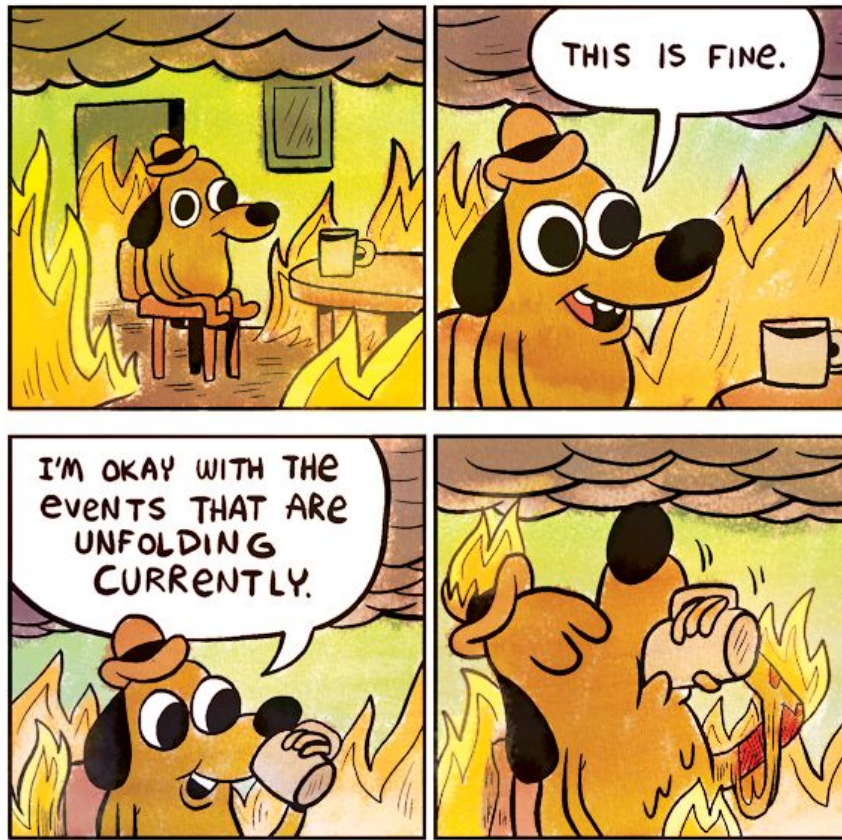
LMCO thing



Stick Around After!

- Come chat and get some food with us after the meeting

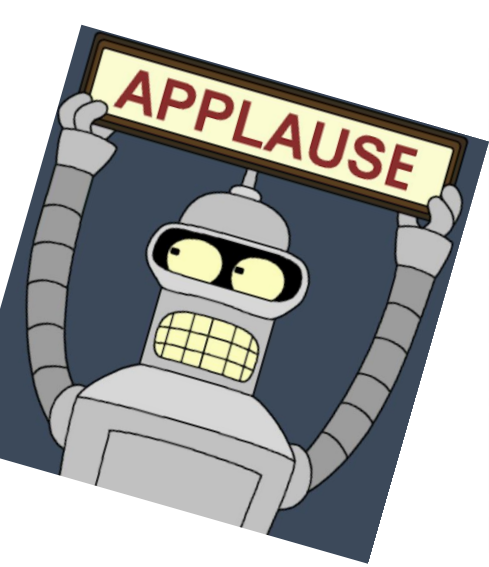




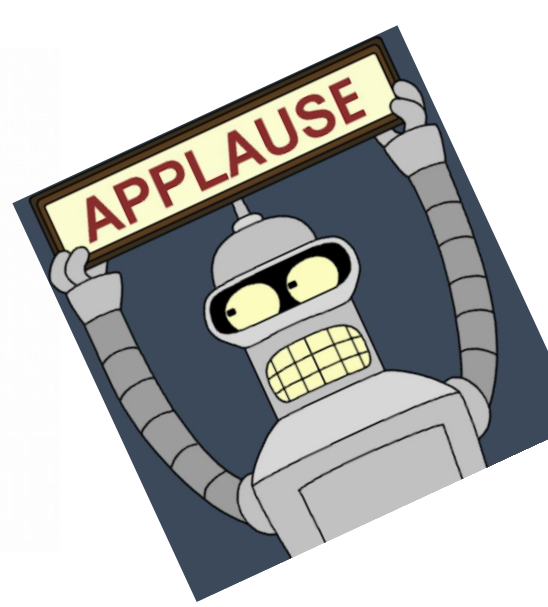
Current Events (<http://gunshowcomic.com/648>)

IMPORTANT

This is the most important news this week



slack



New Slack Logo

JK



Our holiday gift to you!

Rates starting from \$89

Pack your bags and take a few days off from the hectic holiday season. Or invite family and friends to stay a little longer. Either way, the Marriott family of hotels has an offer that's sure to bring joy to everyone.



Marriott Recap

- 500 Million People Affected
- Encrypted Credit Card numbers leaked (Don't know status of encryption keys)
- Passport Numbers included
- Only press was one friday about a month ago
 - On "Take out the trash" day





The merged **Marriott**, Starwood, Ritz-Carlton rewards program has a ...
 Washington Business Journal - 14 hours ago
 Last August, **Marriott** International launched a rewards program with unified benefits for its three major brands — **Marriott**, Starwood and ...

Marriott looks to reboot loyalty plan after cyberattack
 CNBC - Jan 16, 2019

Marriott unveils name for its new unified loyalty program: **Marriott** Bonvoy
 USA TODAY - Jan 16, 2019

Marriott streamlines loyalty programs after data breach
 Marketing Dive - 12 hours ago

Marriott Bonvoy Reflects Hospitality Loyalty Evolution
 TravelPulse - 10 hours ago

[View all](#)



More **Marriott** hotels planned for oceanfront
 Hometown News (press release) (blog) - 8 hours ago
 Daytona Beach City Commissioners voted unanimously Jan. 9 to rezone 2.176 acres at 41 S. Ocean Ave. to a planned development for ...



Exclusive: Leidos to lease **Marriott** office space
 Washington Business Journal - Jan 16, 2019
 Leidos Holdings Inc. plans to lease about 300,000 square feet of Gaithersburg office space currently occupied by **Marriott** International Inc. as ...



Dual-Brand Now Open in Atlanta; More **Marriott** Openings...
 Hotel Business - 10 hours ago
 NATIONAL REPORT— **Marriott's** family of brands is charting growth across the U.S. with openings in big cities in the South and out West.



Marriott hotel on Pine Grove Road moves forward in Steamboat ...
 Steamboat Pilot & Today - Jan 16, 2019
 STEAMBOAT SPRINGS — Developers hoping to build a four-story, 110-suite Residence Inn by **Marriott** are eyeing a 2.79-acre lot at 1480 Pine ...



Marriott's data breach may be the biggest in history. Now it's facing ...
 Vox - Jan 11, 2019
 More than 150 people who previously stayed in **Marriott** properties are suing the hotel chain in a federal class-action lawsuit, claiming that ...
 Class-action lawsuit filed over **Marriott** data breach
 KOMO News - Jan 11, 2019
[View all](#)



New TownePlace Suites by **Marriott** opens directly across from Salt ...
 KUTV 2News - Jan 15, 2019
 This exciting **Marriott** extended-stay hotel is in an ideal location and has wonderful amenities. Whether it's for a one-night stay or a month-long ...
 Planning Commission approves site plan for new **Marriott** Towneplace ...
 Tehachapi News - Jan 15, 2019
[View all](#)

“Even more egregious is the fact that Marriott did not discover this breach for **nearly four years**, and then for months after that discovery **failed to tell its customers what had occurred**. This conduct constitutes a significant **breach of trust and confidence** unparalleled in the hospitality industry.”

But cybersecurity experts say that **the hospitality industry is often targeted by hackers precisely because of lax security policies.** - Vox

(<https://www.vox.com/the-goods/2019/1/11/18178733/marriott-starwood-hack-lawsuit>)

What's New?

- \$100 to replace passport num if effected
- Class Action Lawsuits
- Investigation still underway





EMERGENCY ALERTS



Emergency Alert

This is CRESA 911. 911 lines are down in our area. call [360-693-3111](tel:360-693-3111) for emergencies

Settings



0118 999 881 999 119 7253

CenturyLink

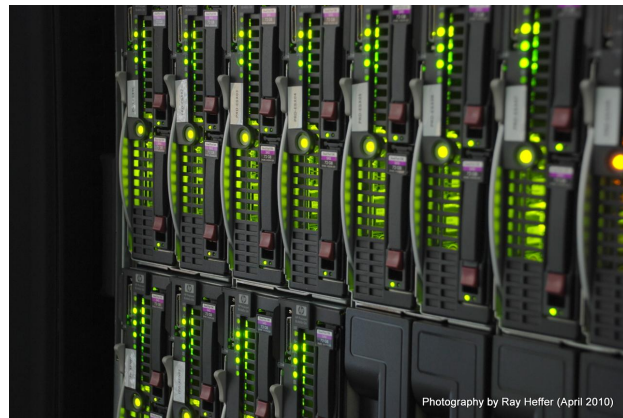
- Malfunctioning NIC
- Lost access to Out of Band management network
- 911 Service outage nationwide



CenturyLink®

WTF Is CenturyLink doing!?!

- Over a **DAY** to restore service
- One Bad NIC.
 - 1 Blade => 2 NICs
 - 1U Rackspace => 1 Blade
 - 42U Racks => 84 NICs per Rack
 - 10,000 Racks in a Datacenter => 840,000 NICs
 - IT TOOK ONE!



What is a bad NIC?

- NICs - Network Interface Card
- Deals with the low end of the TCP/IP stack and conversion to electrical signals (OSI Layer 1)
- What if it forgets to send Source, Destination, or TTL (time to live) information?
- Large Data Centers ***should*** be monitoring for hardware failures such as this. Most Do...

Why so long to fix?

- Out of Band Management
- Control your network infrastructure from a different network than normal traffic.
- Isolating management interfaces.
- CenturyLink lost their ability to use their Out of Band Management network (somehow?)

What does this have to do with 911?

- CenturyLink's Brilliant Idea!
- Let's run Emergency Phone traffic over VOIP
 - Probably not a great idea...
- CenturyLink causes 911 service to drop when their Data Centers have issues

CenturyLink:



Even Mr. Reese's Mug is in on the investigation

“When an emergency strikes, it’s critical that Americans are able to use 911 to reach those who can help,”

said FCC Chairman Ajit Pai.

"The CenturyLink service outage is therefore completely unacceptable, and its breadth and duration are particularly."



Depressing Warning

This was an accident. Imagine what could happen if someone actually was trying to take down 911 services....

New from CenturyLink!

THE CI DUO!



CenturyLink®



Insert Smooth Segue Here





ethereum

Quick note

I am no blockchain expert, nor do I claim to be one. All work here is cypypasta-ed from someone who i'm guessing is kinda-sorta truthful, right, or humored me. If you want actual blockchain advice, please help my startup's ICO coming soon™ or chat in #hackucf on slack (heh, smooth slack advertisement)

Movie Time (Totally relevant..)



51% Attack on Ethereum Classic

“The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. **To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.**”

- Satoshi Nakamoto (<https://bitcoin.org/bitcoin.pdf>)

Results

*“Updated Jan. 7, 10:27pm PT: At time of writing, we have identified a total of 15 reorganizations, 12 of which contained double spends, **totaling 219,500 ETC (~\$1.1M)**. No Coinbase accounts have been impacted by the attack.” - Coinbase*

SCP Vulns

- 30+ Year old vulns
- SCP doesn't actually check if it's receiving what it asked for...

<https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt>

CVE-2019-6111: missing received object name validation

Due to the scp implementation being derived from 1983 rcp [1], **the server chooses which files/directories are sent to the client.** However, scp client only perform cursory validation of the object name returned (only directory traversal attacks are prevented). **A malicious scp server can overwrite arbitrary files in the scp client target directory.** If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example overwrite .ssh/authorized_keys).

NSA GHIDRA

- NSA's Christmas Present to Sec Peeps
- Sadly no upload yet due to shutdown



Speaking of Shutdown!

SSL Certs

- Turns out they need to be renewed
- They Expire!
- Periodically, they need to be replaced with newly signed certs
- But nobody's being paid to do it

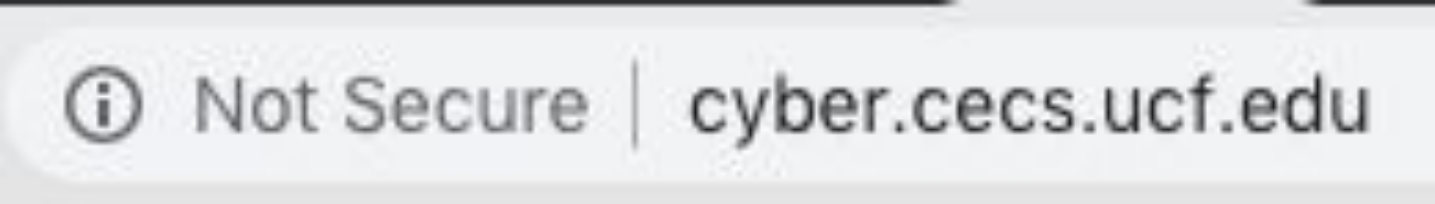


https://

I would show some examples

But they've already been taken down...

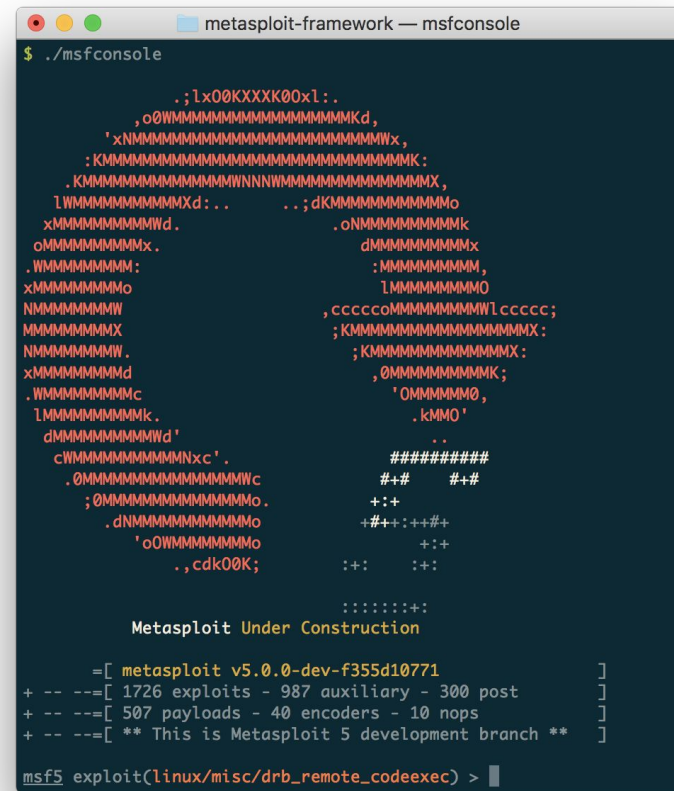
So here's some other SSL Irony in its place



ⓘ Not Secure | cyber.cecs.ucf.edu

Metasploit 5.0 Release

- Announced at Derbycon 2018
- Automation APIs (RESTful DB)
- Evasion Modules
- Python + GoLang support
- And lots of other fun stuffs



```
metasploit-framework — msfconsole
$ ./msfconsole

      ;l×00K××××K00×l:
      ,o0WMMMMMMMMMMMMMMMMKd,
      'xNMMMMMMMMMMMMMMMMMMMMWx,
      ;KMMMMMMMMMMMMMMMMMMMMMMMMMK:
      .KMMMMMMMMMMMMMMMMNNNMMMMMMMMMX,
      lWMMMMMMMMMXd:.. ..;dKMMMMMMMMMo
      xMMMMMMMMWd. .oNMMMMMMMMK
      oMMMMMMMMx. dMMMMMMMMx
      .WMMMMMMMM: :MMMMMMMM,
      xMMMMMMMMo lMMMMMMMMO
      NMMMMMMMMW ,cccccOMMMMMMMMWlcccc;
      MMMMMMMMMX ;KMMMMMMMMMMMMMMMMX:
      NMMMMMMMMW . ;KMMMMMMMMMMMMMMMMX;
      xMMMMMMMMd ,0MMMMMMMMMK;
      .WMMMMMMMMc 'OMMMMMMO,
      lMMMMMMMMMk. .kMMO'
      dMMMMMMMMWd' ..
      cMMMMMMMMNxc'. #####
      .0MMMMMMMMMMMMMWc #+# #+#
      ;0MMMMMMMMMMMMMo. ++
      .dNMMMMMMMMMMMMo. +#+:++
      'oOMMMMMMMMMo. ++
      .,cdk00K; :+ :+

      :::::++
      Metasploit Under Construction

      =[ metasploit v5.0.0-dev-f355d10771 ]
+ -- --[ 1726 exploits - 987 auxiliary - 300 post ]
+ -- --[ 507 payloads - 40 encoders - 10 nops ]
+ -- --[ ** This is Metasploit 5 development branch ** ]

msf5 exploit(linux/misc/dr_b_remote_codeexec) >
```

TOOL TIME

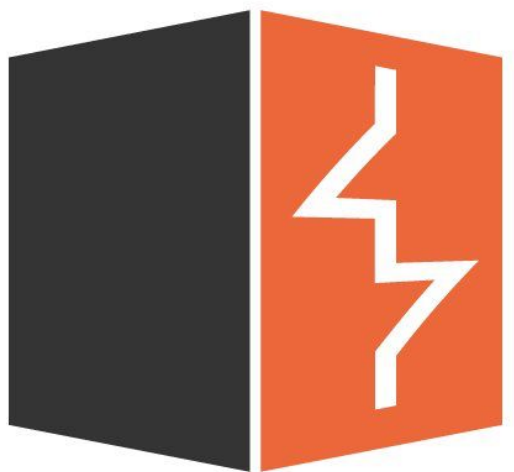


Tool Time is back!

This week we will be going over...

Burp Suite!

Burp Suite by PortSwigger



- GUI to test web app security
- Free community edition
- Use for CTFs and penetration testing

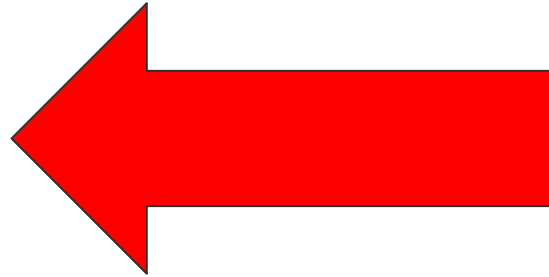
DEMO

Additional Features

- Scanner [pro only] - automatically scans for web vulnerabilities
- Sequencer - analyzes randomness
- Decoder - encode/decode values
- Comparer - points out differences between files (even binary ones)

Get the triangular foods!

Sponsored by:

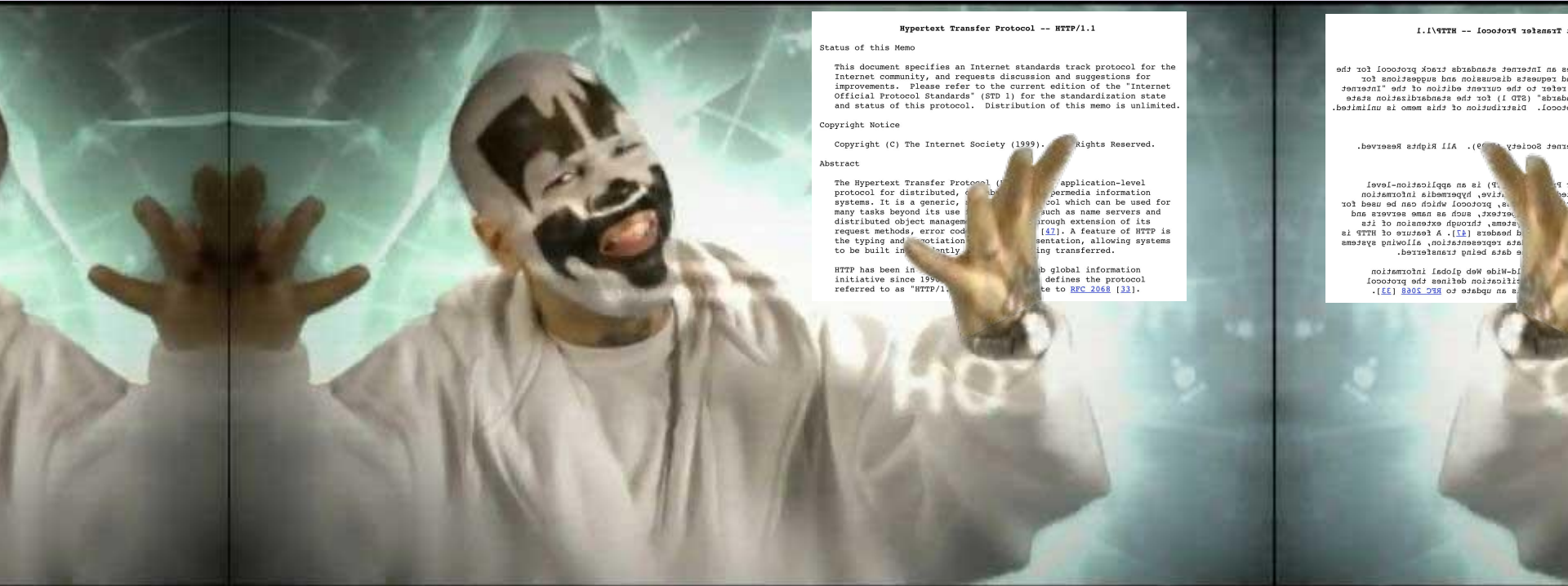


Line up down the left aisle

Web Application Insecurity

By Charlton Trezevant & David Maria





Hypertext Transfer Protocol -- HTTP/1.1

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypertext information systems. It is a generic, distributed object management environment, through extension of its request methods, error codes, and negotiation capabilities. A feature of HTTP is the typing and negotiation of data being transferred.

HTTP has been in use since 1990. This document defines the protocol referred to as "HTTP/1.1" in RFC 2068 [3].

1.1 HTTP -- Internet Standard

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypertext information systems. It is a generic, distributed object management environment, through extension of its request methods, error codes, and negotiation capabilities. A feature of HTTP is the typing and negotiation of data being transferred.

HTTP has been in use since 1990. This document defines the protocol referred to as "HTTP/1.1" in RFC 2068 [3].

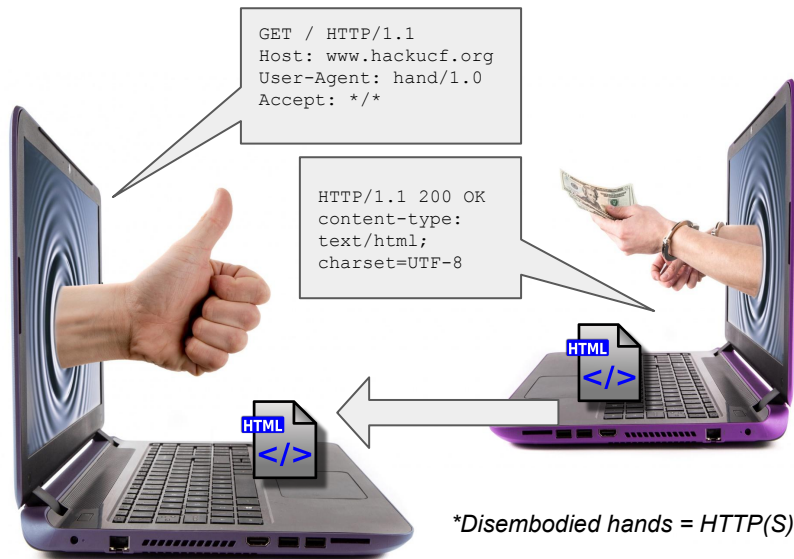
How do Websites *Work*?

Client-Side vs. Server-Side

What's a *Client*?



What's a *Server*?



Web 2.0



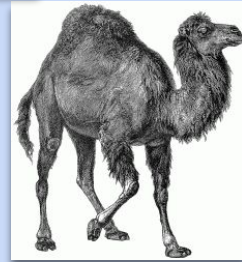
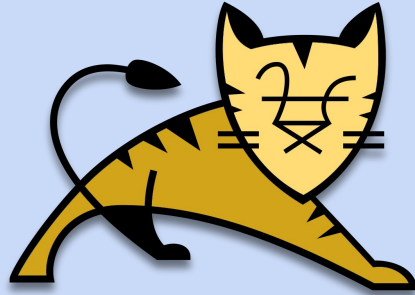
Interactive Websites

django

Microsoft
ASP.net

cf

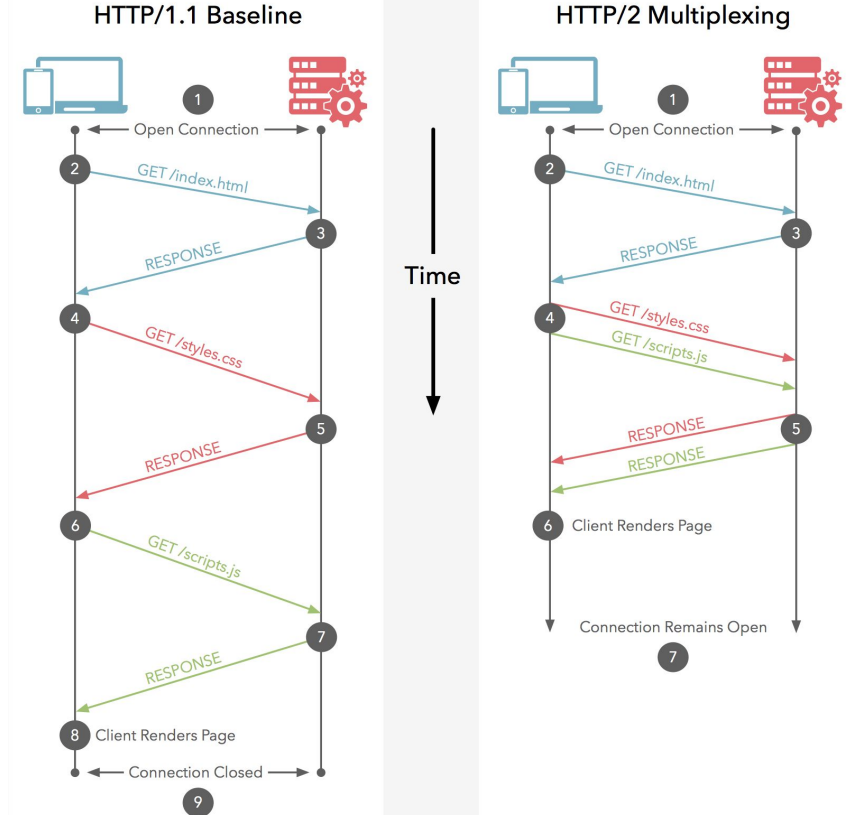
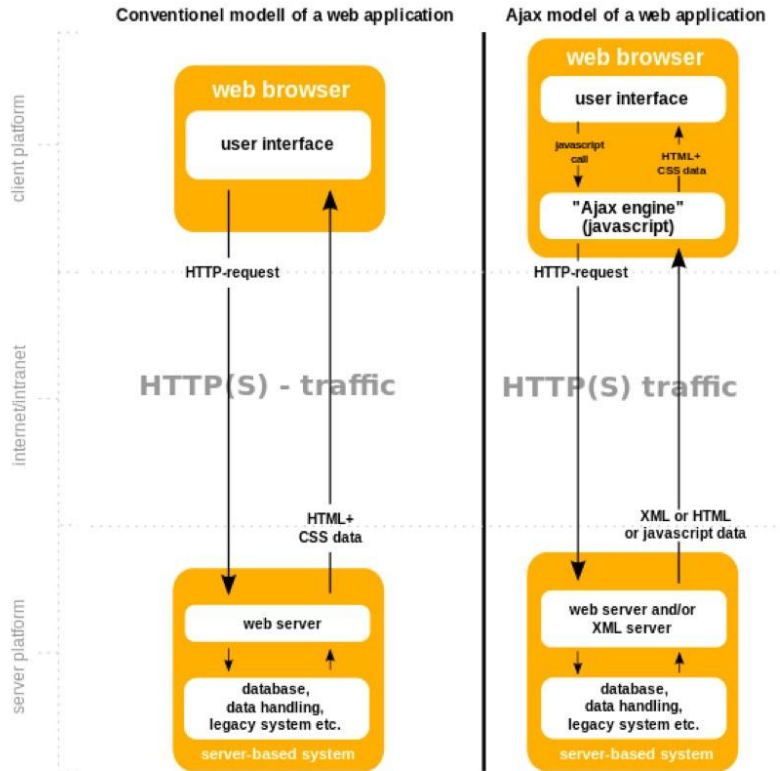
php



node.js

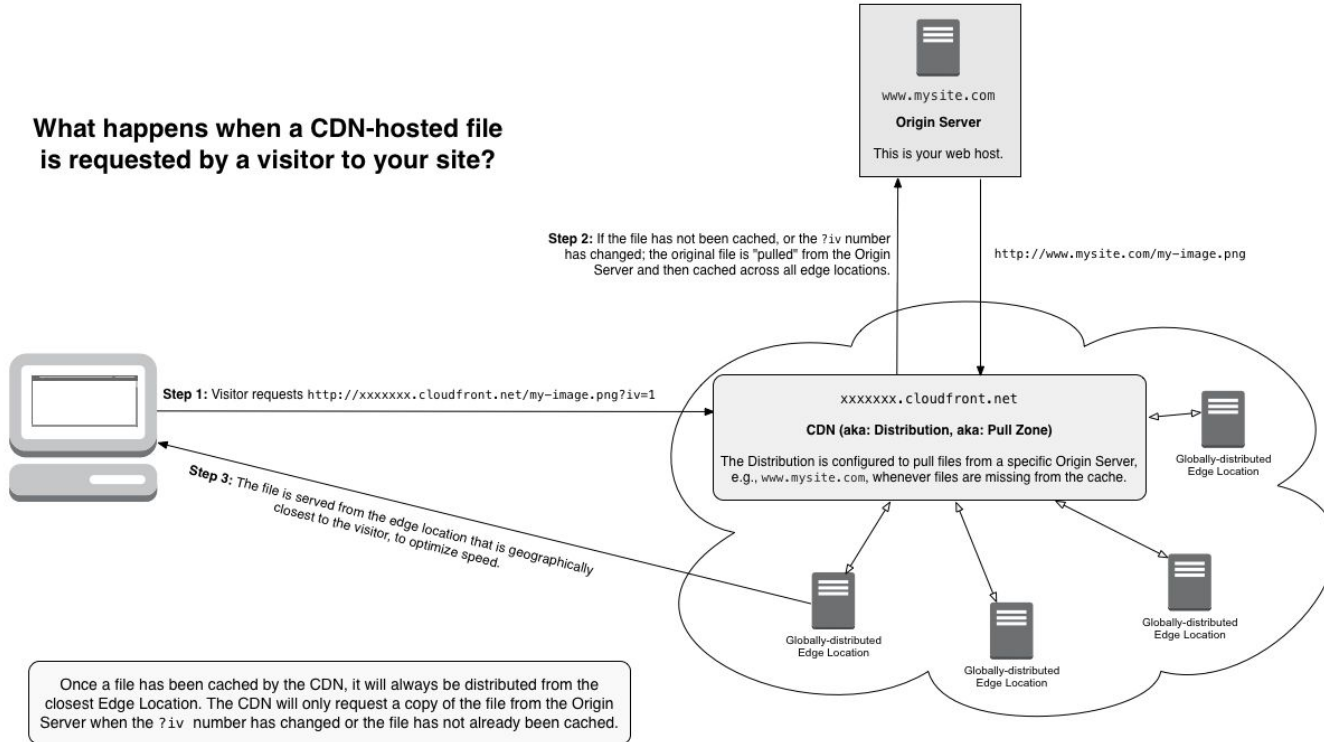


Complexity: HTTP(S), Ajax, and HTTP/2



More Complexity: CDNs and Caching

What happens when a CDN-hosted file is requested by a visitor to your site?



Once a file has been cached by the CDN, it will always be distributed from the closest Edge Location. The CDN will only request a copy of the file from the Origin Server when the `?iv` number has changed or the file has not already been cached.



Common Vulnerabilities

Information Disclosure

- What is it?
 - Your app unnecessarily discloses information that could be useful to an attacker
- Examples
 - Verbose error messages with code snippets / stack traces / file paths (think Django DEBUG mode)
- Mitigations
 - Always turn off debug modes, look up best practices for whatever framework you're using

Page not found (404)

Request Method: GET

Request URL: http://127.0.0.1:8000/kjh

Using the URLconf defined in `pollsite.urls`, Django tried these URL patterns, in this order:

1. `^accounts/`
2. `^admin/`
3. `^/?$` `{name: 'poll_home'}`
4. `^polls/(?P<catslug>[-\w]+)/$` `{name: 'category_polls'}`
5. `^polls/(\w+)/(?P<pid>[-\d]+)/` `{name: 'detail_poll'}`
6. `^add/` `{name: 'add_poll'}`



The current URL, `kjh`, didn't match any of these.

You're seeing this error because you have `DEBUG = True` in your Django settings file. Change that to `False`, and Django will display a standard 404 page.

Cross-Site Scripting (XSS)

- What is it?
 - Security vulnerability allowing an attacker to alter the code a web application delivers to the user, which is then executed in the context of that application.
- Types of XSS
 - Stored / Persistent
 - Reflected
 - DOM-Based

Cross-Site Scripting (XSS)

- Potential Attacks

- Stealing client's login session cookies
- Controlling what requests / actions are made by the client
- Changing the content displayed on the page

- Mitigations

- VALIDATE USER INPUT
- Encode all input that is added to a page as output

Demo Time!

SQL Injection (SQLi)

- What is it?
 - Injection attack that allows an attacker to modify SQL statements being executed on the server
- Potential Attacks
 - Bypass authentication
 - Dumping user credentials or other sensitive data from the database
 - Delete all data in a database

SQL Injection (SQLi)

- Mitigations
 - SANITIZE USER INPUT
 - SQL Prepared statements w/ parameterized queries
 - SQL Stored procedures
 - Escape user sanitized input
 - Use something like SQLAlchemy to abstract away database access and not have to write any SQL

Demo Time!

Arbitrary File Upload

- What is it?
 - A vulnerability which occurs in web applications if the file type uploaded is not checked, filtered or sanitized.
- Potential Attacks
 - Attacker can upload a malicious PHP , ASP etc. script and execute it.
 - Code execution on server

Arbitrary File Upload

- Mitigations
 - Thoroughly check file type to make sure users are only uploading file types that are needed
 - Make sure you're checking server side
 - Don't just look at file extension

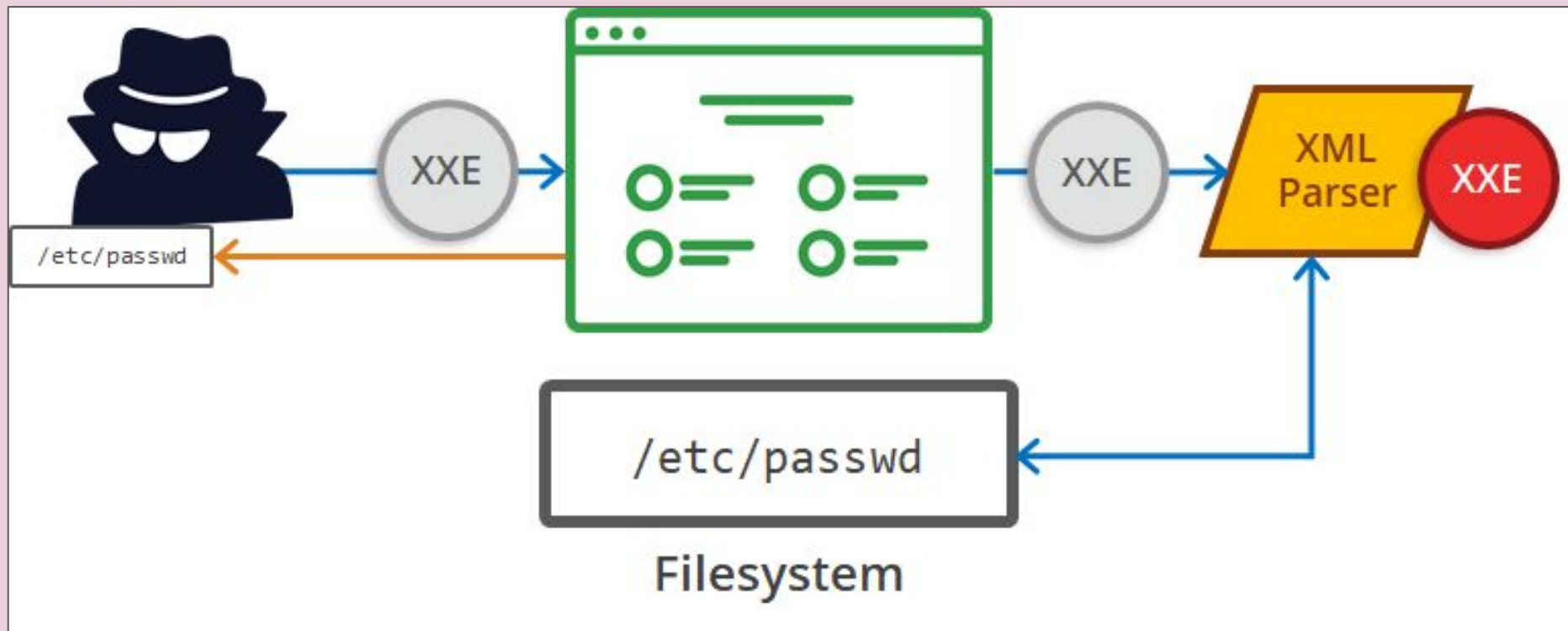
Demo Time!

XXE: XML eXternal Entity Injection

- What is it?
 - This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser
- Potential Attacks
 - Reading files on the server
 - Code Execution

XXE: XML eXternal Entity Injection

- Mitigations
 - Disable external entities in your XML parser if you're parsing XML that a user is inputting / contains user input
 - If external entities are a must, follow best practices for the parser you are using on how to properly configure it



```
<?xml version="1.0" encoding="utf-8"?>  
<!DOCTYPE rohit[  
  <!ENTITY entityex SYSTEM "file:///etc/passwd">  
>  
<abc>&entityex;</abc>
```

CSRF: Cross-Site Request Forgery

- What is it?
 - Attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.
- Potential Attacks
 - Transferring money, change users email address, etc.

CSRF: Cross-Site Request Forgery

- Mitigations
 - CSRF Token

1

www.fictitiousbank.com



Bob logs into his banks website

Cookie is set



Bob receives an image on email about fictitiousbank

2

Victim

Bob clicks on image



3

www.somesite.com



<html>

```

```

4

Bob submits request to transfer money to attacker's account



5

Bank's web application validates the session and then completes the transaction



Demo Time!

Deserialization Attacks

- What is it?
 - Common flaws in deserialization libraries allow for denial-of-service, and remote code execution attacks.
- Examples
 - Java deserialization
 - Python pickle
 - JSON Deserialization
 - PHP 'unserialize'

Deserialization Attacks

- Mitigations
 - Avoid deserializing user input at all costs
 - SANITIZE USER INPUT
 - Look up security of any deserialization libraries you're using

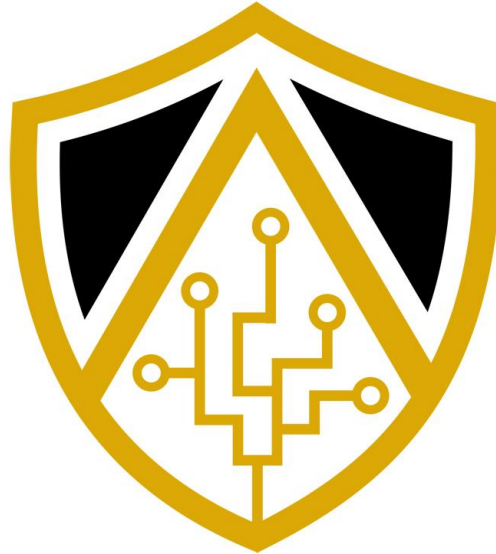
Resources!

[OWASP top ten](#)

ctf.hackucf.org

[Web app hackers handbook 2](#)

Thank you!



HACK@UCF

IRC Freenode: #hackucf, Slack: slack.hackucf.org

<https://hackucf.org> • <https://www.facebook.com/HackUCF>