CSCI 3403

Introduction to Cybersecurity

CSCI 3403

Attend from afar

Lectures are streamed and recorded

- Zoom link and recordings are posted on Canvas
- This is **just lectures!** Recitations are not recorded

Class logistics

CSCI 3403

Alex Curtiss (he/him)

Senior Security Engineer

Render

leviathan security group

CSCI 3043

The other wonderful people who make this class happen:

TAs:

- Madeleine Wade
- Dorothea French
- Jackson Sippe
- Qinrun Dai
- Sriranga Ramaswamy
- Kirby Linvill
- Nicolas Ammann

CAs:

- Sonia Purisai
- Kaile Suoo
- Dorjee Zhang

Grader:

- Rhea Nair

Raise your hand if…

You already have security experience

Raise your hand if…

Have some background but no formal training

Raise your hand if…

You are brand new to security!

Prereqs

This is an intro class: no security background required

The only prereq is computer Systems (CSCI 2400)

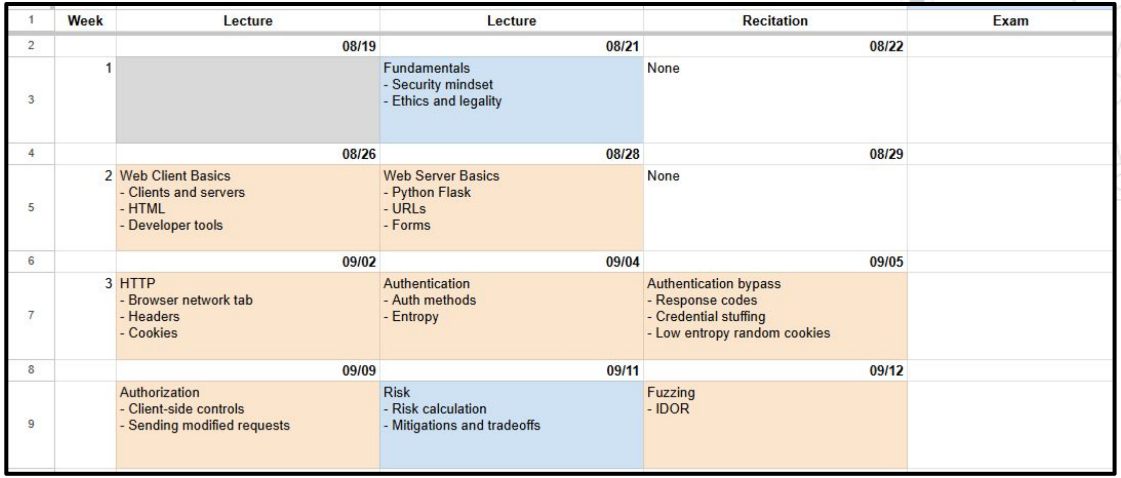
This class covers a wide range of languages and tools.

We expect that you can learn to read and write short code snippets in an unfamiliar programming language without too much difficulty.

Core Topics

Topics covered

- Web security
- Linux security
- Cryptography
- Network security



Week	Lecture	Lecture	Recitation	Exam
	08/19	08/21	08/22	
1		Fundamentals - Security mindset - Ethics and legality	None	
	08/26	08/28	08/29	
2	Web Client Basics - Clients and servers - HTML - Developer tools	Web Server Basics - Python Flask - URLs - Forms	None	
	09/02	09/04	09/05	
3	HTTP - Browser network tab - Headers - Cookies	Authentication - Auth methods - Entropy	Authentication bypass - Response codes - Credential stuffing - Low entropy random cookies	
	09/09	09/11	09/12	
	Authorization - Client-side controls - Sending modified requests	Risk - Risk calculation - Mitigations and tradeoffs	Fuzzing - IDOR	

A full day-by-day breakdown is listed in the syllabus

Class Format

- **Lectures (2 per week):**
  Discuss and demo new material
- **Recitation exercises (1 per week):**
  Get hands-on with new tools
- **Exams (5 total):**
  Take-home exercises which apply skills you acquired

Recitations

Recitations cover hands-on material. They are not streamed or recorded.

- You can attend other recitations if needed, just ask the other TA if they have room.
- There is no recitation tomorrow (Aug 22) or next week (Aug 29). The first recitation is Sept 05.

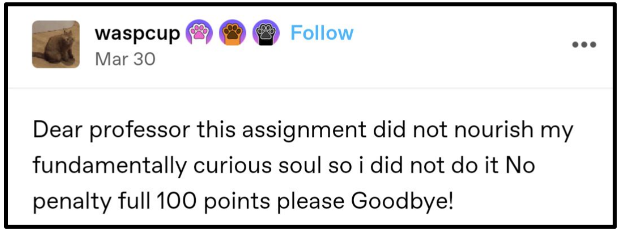
Grading

Grade breakdown:

Weekly exercises **25%**	**Exams (5 total)** **75%**

Late policy:

- Exercises can be turned in late with no penalty
- Exams cannot be turned in late



Dear professor this assignment did not nourish my fundamentally curious soul so i did not do it No penalty full 100 points please Goodbye!

Resources

Resources:

- **Canvas** (assignments, materials, slides)
  https://canvas.colorado.edu
- **Discord** (announcements, Q&A, office hours)
  https://discord.gg/SuXJjgpB (also in syllabus)

No textbook, but I can recommend additional resources

Honor Code Policy

Honor code:

- You may work with classmates on weekly exercises, but not on exams.
- Assignments which are partially or entirely plagiarized will receive a 0%.

The full policy is in the syllabus.

Honor Code Policy

While completing all classwork:

- Provide all answers in your own words

Do not copy other student’s answers or AI tools directly.

- Complete each step of the assignments yourself

For example: Some assignments involve stealing passwords. Getting advice on how to crack passwords is allowed. Being told the password without ever cracking it yourself is not.

Questions?

Security Fundamentals

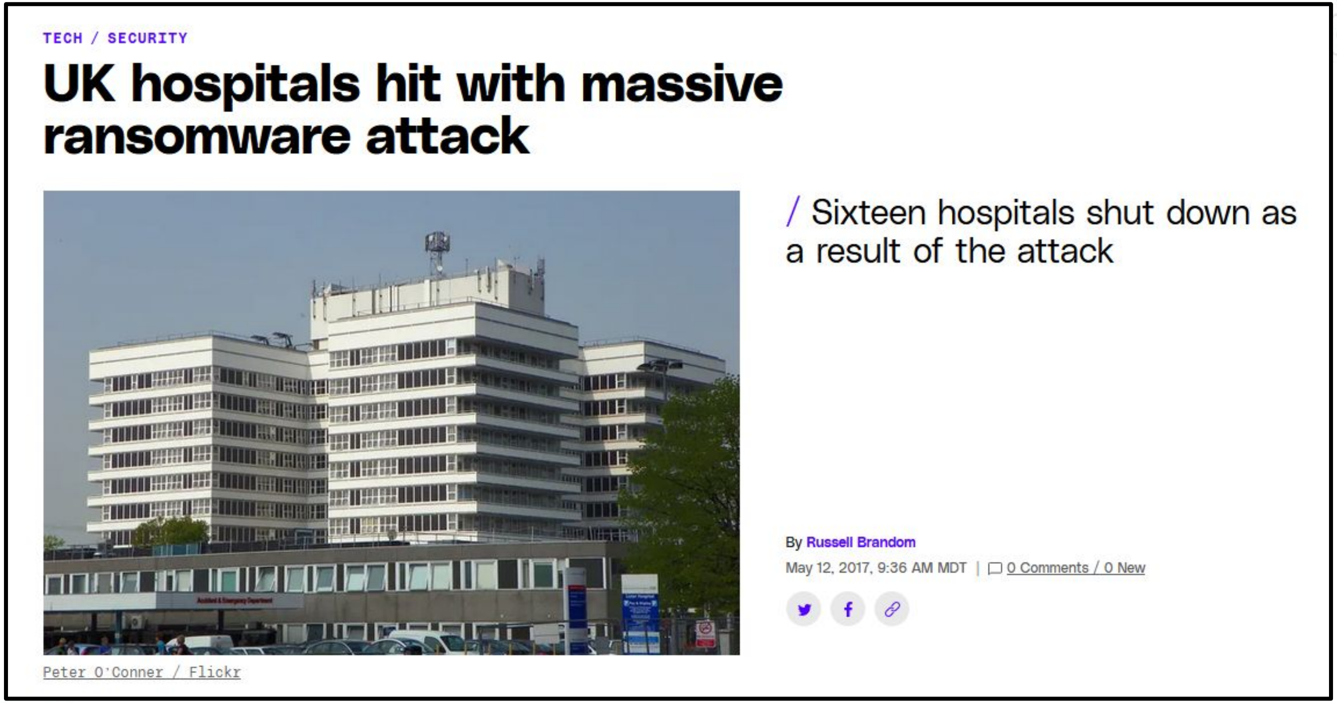
What is security?

Security Fundamentals

Security:

Protecting ***things we care about*** *from* ***harm.***

Security Fundamentals



TECH / SECURITY

UK hospitals hit with massive ransomware attack

/ Sixteen hospitals shut down as a result of the attack

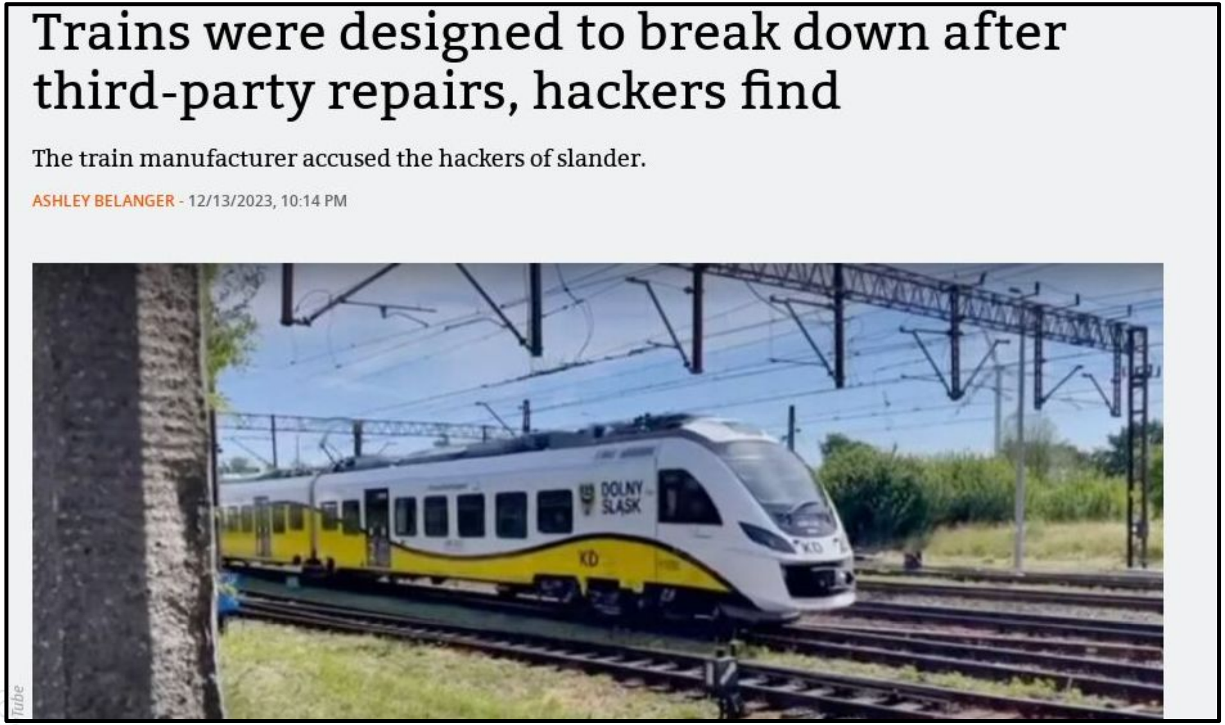
By Russell Brandom

May 12, 2017, 9:36 AM MDT | 0 Comments / 0 New

Peter O'Conner / Flickr

https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

Security Fundamentals



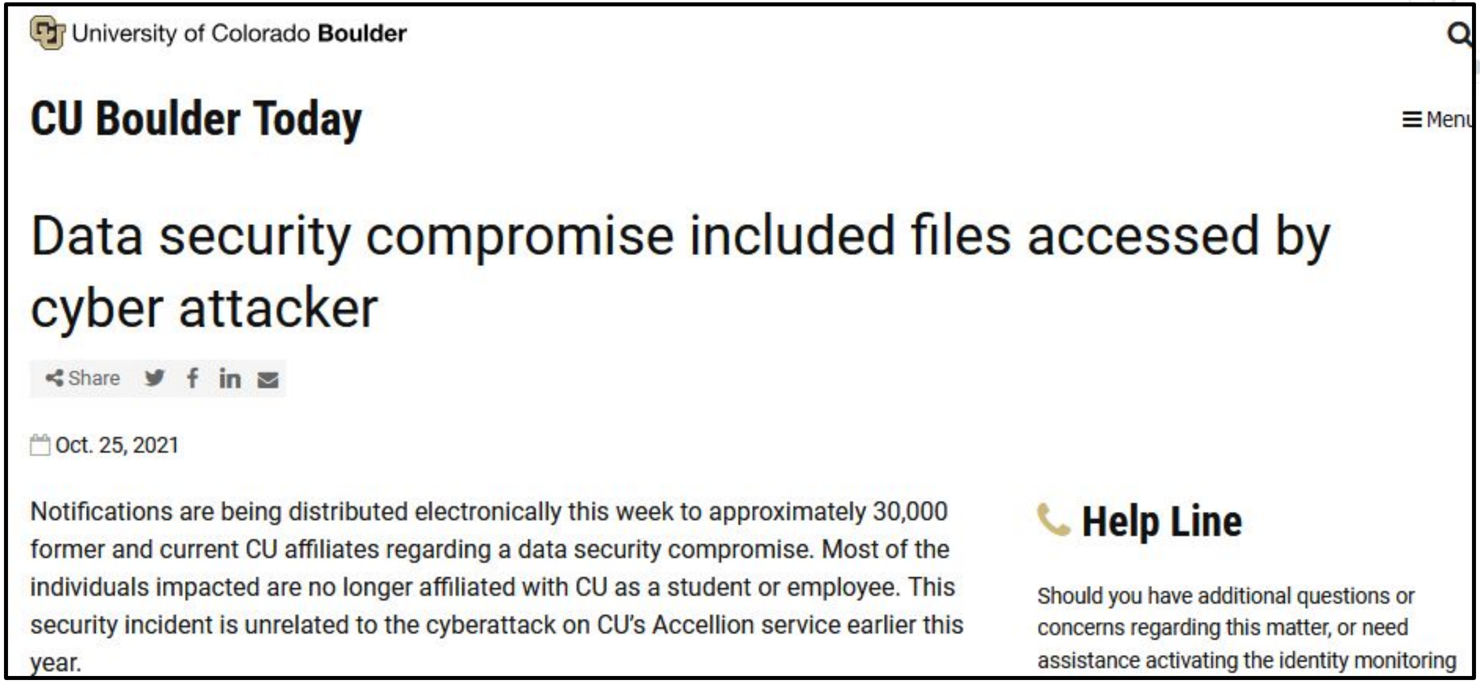
Trains were designed to break down after third-party repairs, hackers find

The train manufacturer accused the hackers of slander.

ASHLEY BELANGER - 12/13/2023, 10:14 PM

https://arstechnica.com/tech-policy/2023/12/manufacturer-deliberately-bricked-trains-repaired-by-competitors-hackers-find/

Security Fundamentals



University of Colorado **Boulder**

CU Boulder Today

☰ Menu

Data security compromise included files accessed by cyber attacker

Oct. 25, 2021

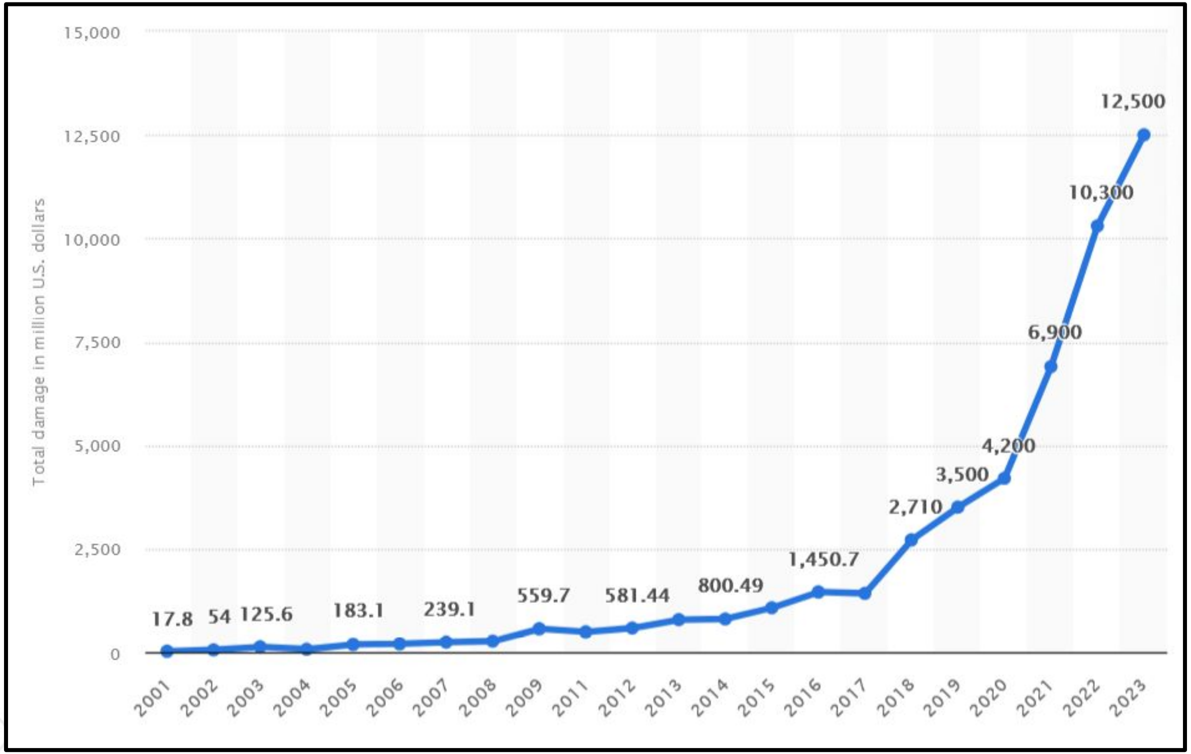
Notifications are being distributed electronically this week to approximately 30,000 former and current CU affiliates regarding a data security compromise. Most of the individuals impacted are no longer affiliated with CU as a student or employee. This security incident is unrelated to the cyberattack on CU's Accellion service earlier this year.

☎ Help Line

Should you have additional questions or concerns regarding this matter, or need assistance activating the identity monitoring

https://www.colorado.edu/today/2021/10/25/data-security-compromise-included-files-accessed-cyber-attacker

Security Fundamentals



https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/

Security Fundamentals

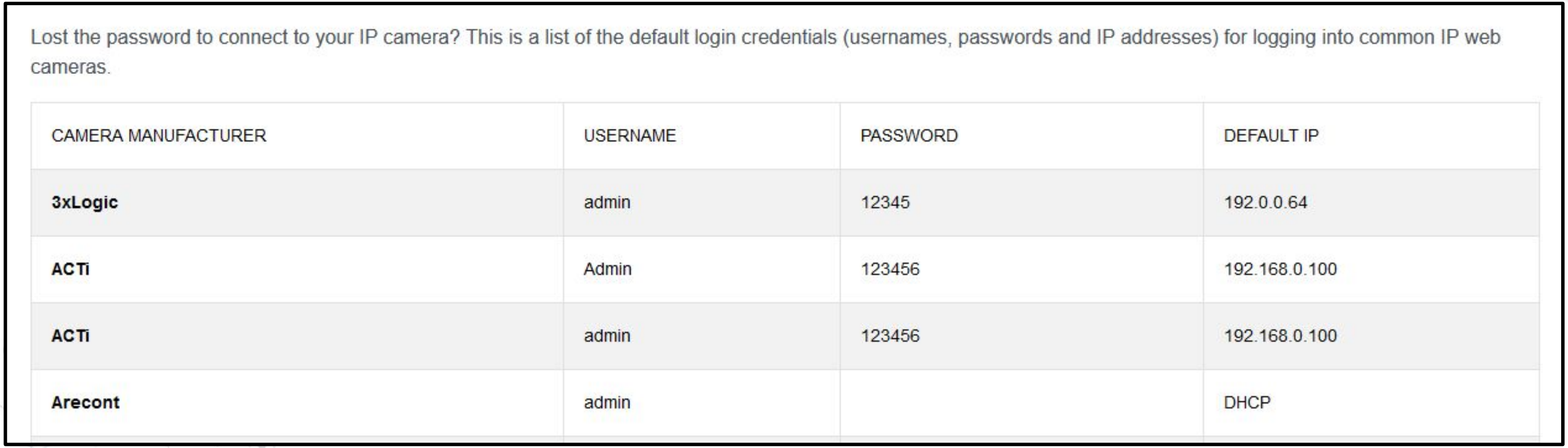
Software engineers often do not consider how somebody could abuse their code to cause harm.

Have you ever thought about it?

Hopefully after this class, you will!

Security Fundamentals

Many smart devices are given a default password. This approach is simple to code and easy to set up.



Lost the password to connect to your IP camera? This is a list of the default login credentials (usernames, passwords and IP addresses) for logging into common IP web cameras.

CAMERA MANUFACTURER	USERNAME	PASSWORD	DEFAULT IP
3xLogic	admin	12345	192.0.0.64
ACTi	Admin	123456	192.168.0.100
ACTi	admin	123456	192.168.0.100
Arecont	admin		DHCP

How can this be abused?

Mirai Botnet

1

Find online devices

Mirai Botnet

1

Find online devices

2

Try common credentials

```
root admin
admin admin
root default
admin password
root root
root 12345
user user
...
```

Mirai Botnet

1

Find online devices

2

Try common credentials

```
root admin
admin admin
root default
admin password
root root
root 12345
user user
...
```

3

Build a botnet with thousands of devices

Mirai Botnet

1

Find online devices

2

Try common credentials

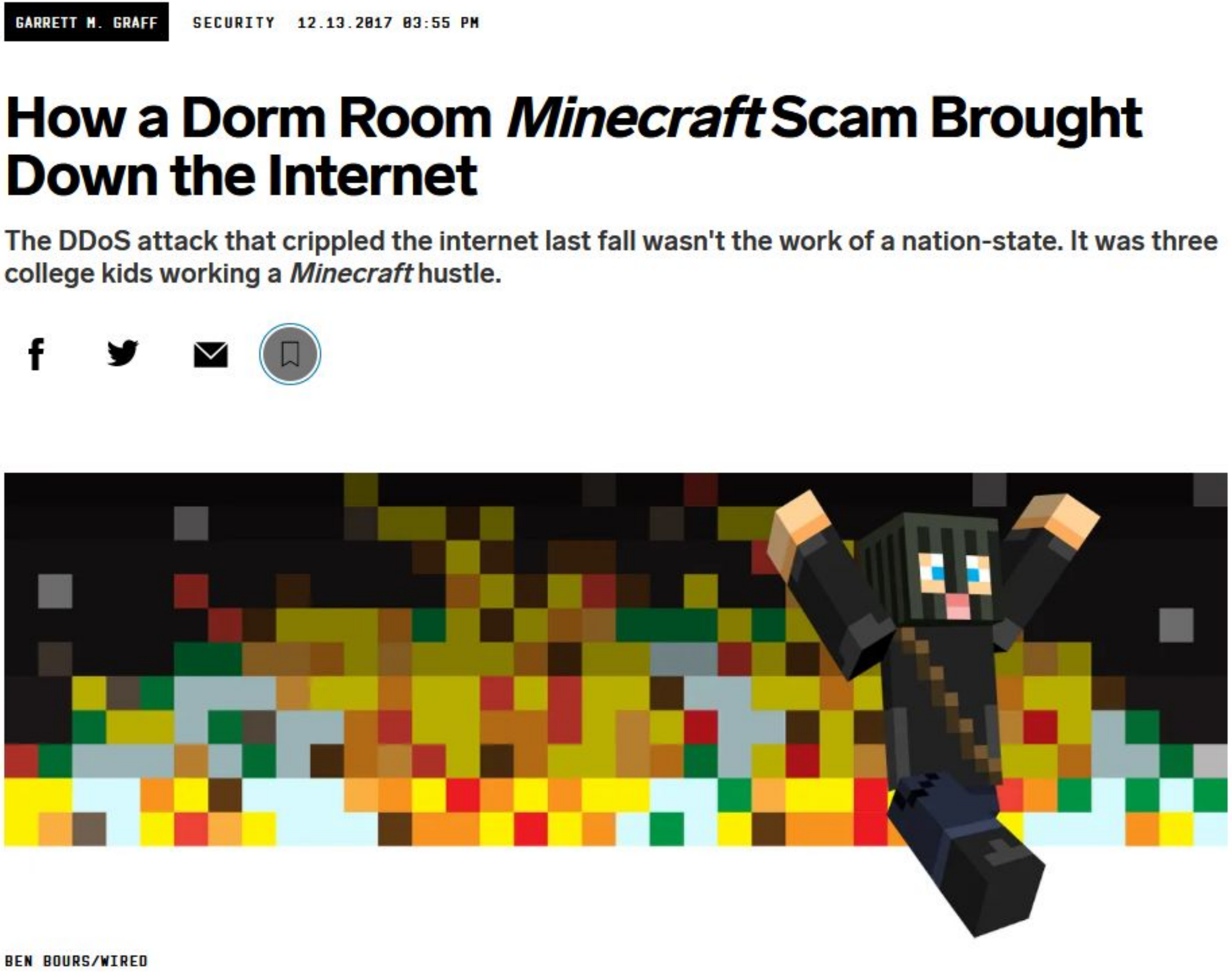
```
root admin
admin admin
root default
admin password
root root
root 12345
user user
...
```

3

Build a botnet with thousands of devices

4

???



GARRETT M. GRAFF SECURITY 12.13.2017 03:55 PM

How a Dorm Room *Minecraft* Scam Brought Down the Internet

The DDoS attack that crippled the internet last fall wasn't the work of a nation-state. It was three college kids working a *Minecraft* hustle.

BEN BOURS/WIRED

https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

GARRETT M. GRAFF SECURITY 12.13.2017 03:55 PM

Ho Dorm Room *Minecraft* Scam Brought I e Internet

d the internet last fall wasn't t

aft hustle.

BEN BO

om/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

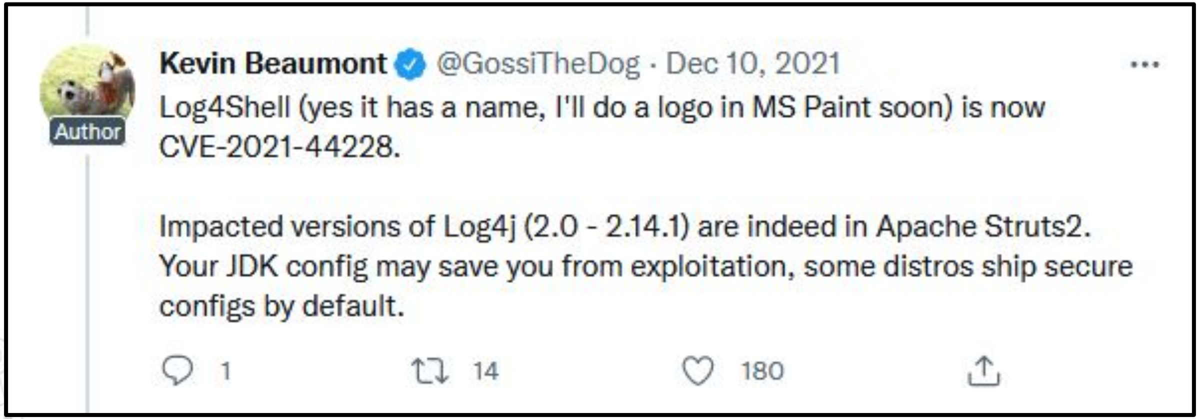
Security Fundamentals

Fun aside: Vulnerabilities like “Mirai” typically get their name from the first person who Tweets about it.

Security Fundamentals

Fun aside: Vulnerabilities like “Mirai” typically get their name from the first person who Tweets about it.

Yes, really:



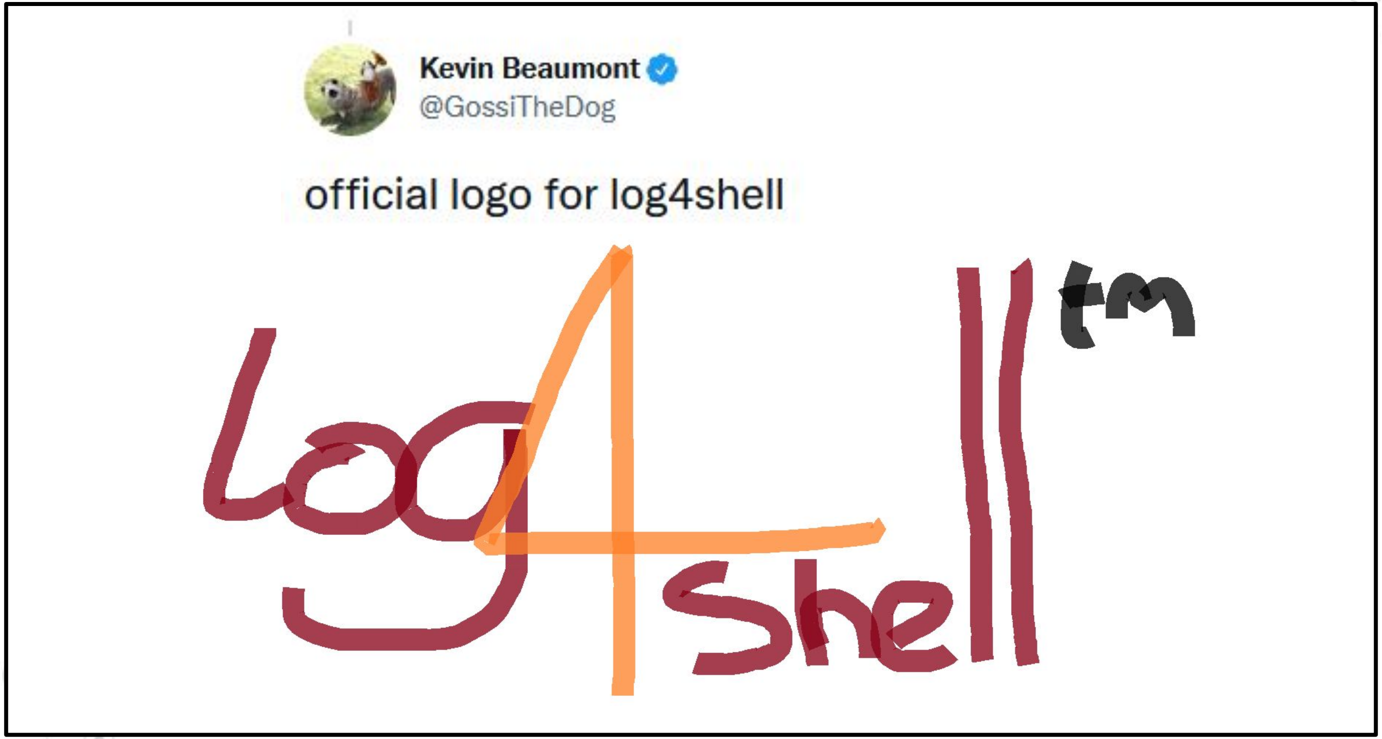
Author

Kevin Beaumont @GossiTheDog · Dec 10, 2021

Log4Shell (yes it has a name, I'll do a logo in MS Paint soon) is now CVE-2021-44228.

Impacted versions of Log4j (2.0 - 2.14.1) are indeed in Apache Struts2. Your JDK config may save you from exploitation, some distros ship secure configs by default.

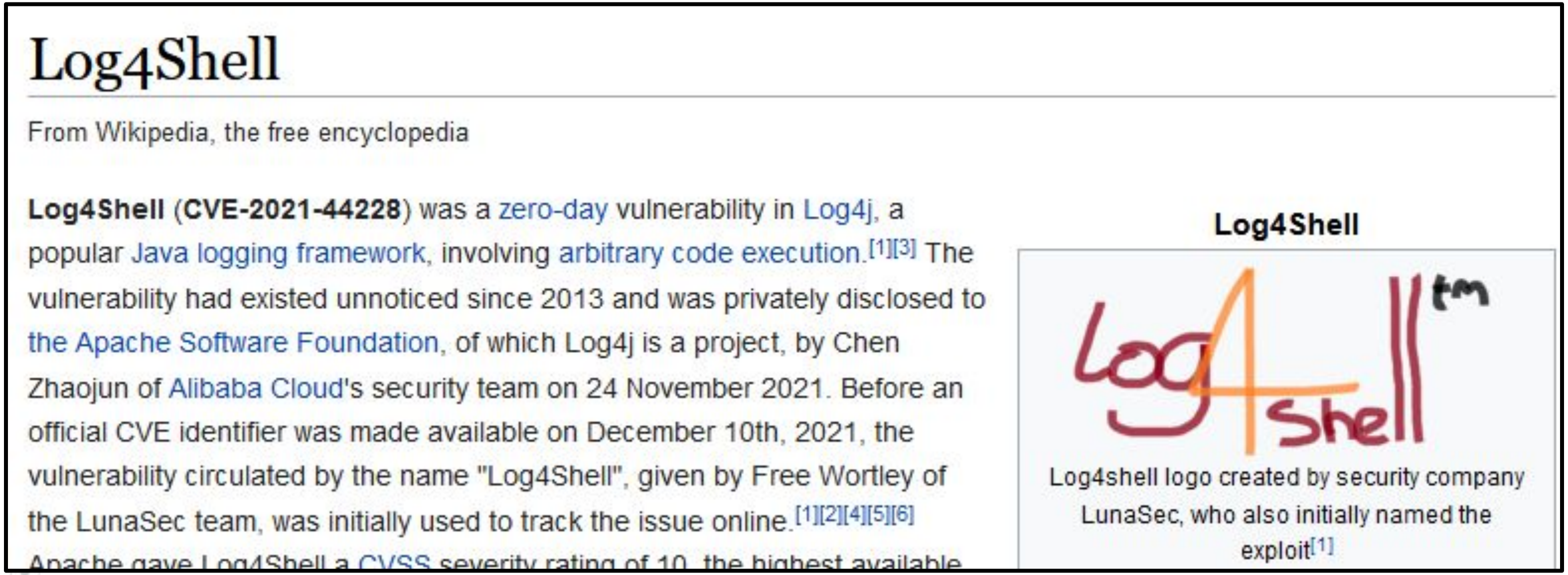
Security Fundamentals



Kevin Beaumont
@GossiTheDog

official logo for log4shell

Security Fundamentals



Log4Shell

From Wikipedia, the free encyclopedia

Log4Shell (**CVE-2021-44228**) was a zero-day vulnerability in Log4j, a popular Java logging framework, involving arbitrary code execution.[1][3] The vulnerability had existed unnoticed since 2013 and was privately disclosed to the Apache Software Foundation, of which Log4j is a project, by Chen Zhaojun of Alibaba Cloud's security team on 24 November 2021. Before an official CVE identifier was made available on December 10th, 2021, the vulnerability circulated by the name "Log4Shell", given by Free Wortley of the LunaSec team, was initially used to track the issue online.[1][2][4][5][6] Apache gave Log4Shell a CVSS severity rating of 10, the highest available

Log4Shell

Log4shell logo created by security company LunaSec, who also initially named the exploit[1]

Legality and Ethics

It is illegal to

“intentionally access a computer without authorization or exceed authorized access”

18 U.S.C. § 1030(a)(2)

Legality and Ethics

In plain terms: it is illegal to attack a system *unless you have been given permission first!*

During this class, you have permission to attack our class lab environment, **csci3403.com**.

Legality and Ethics

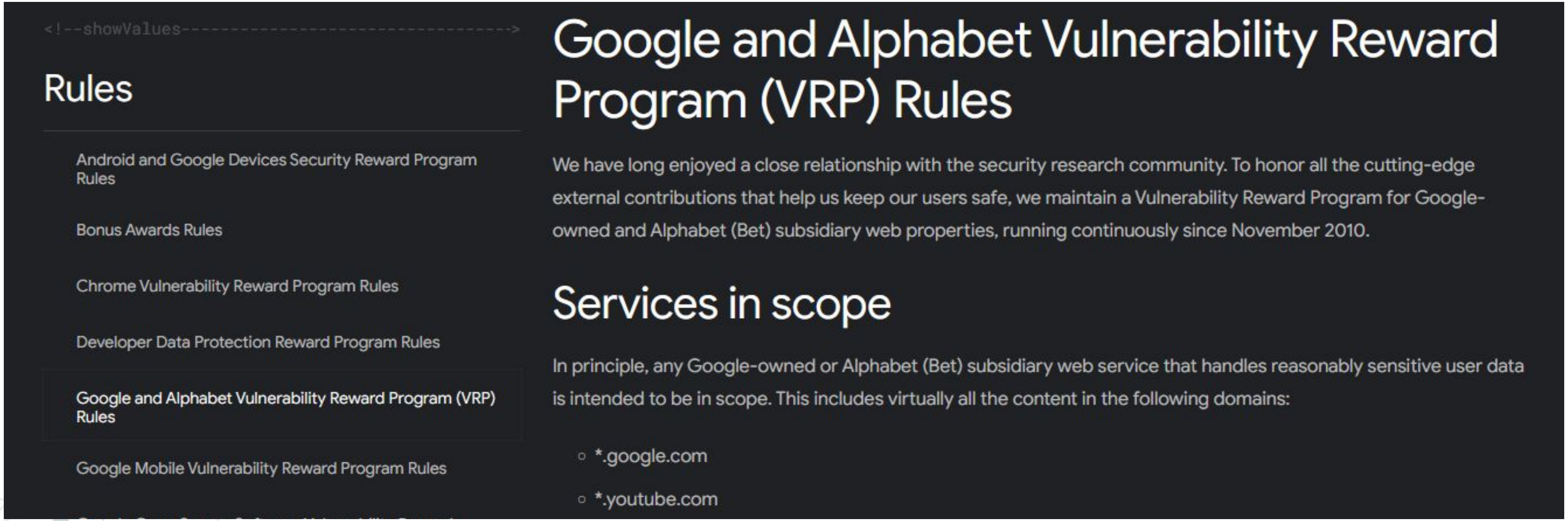
In plain terms: it is illegal to attack a system *unless you have been given permission first!*

During this class, you have permission to attack our class lab environment, **csci3403.com**.

Do not attack other systems without **explicit permission**, or you could face consequences including failing the class or legal action.

Legality and Ethics

If you have permission though, that is fine.



```
<!--showValues------------------------------->
```

Rules

- Android and Google Devices Security Reward Program Rules
- Bonus Awards Rules
- Chrome Vulnerability Reward Program Rules
- Developer Data Protection Reward Program Rules
- Google and Alphabet Vulnerability Reward Program (VRP) Rules
- Google Mobile Vulnerability Reward Program Rules

Google and Alphabet Vulnerability Reward Program (VRP) Rules

We have long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help us keep our users safe, we maintain a Vulnerability Reward Program for Google-owned and Alphabet (Bet) subsidiary web properties, running continuously since November 2010.

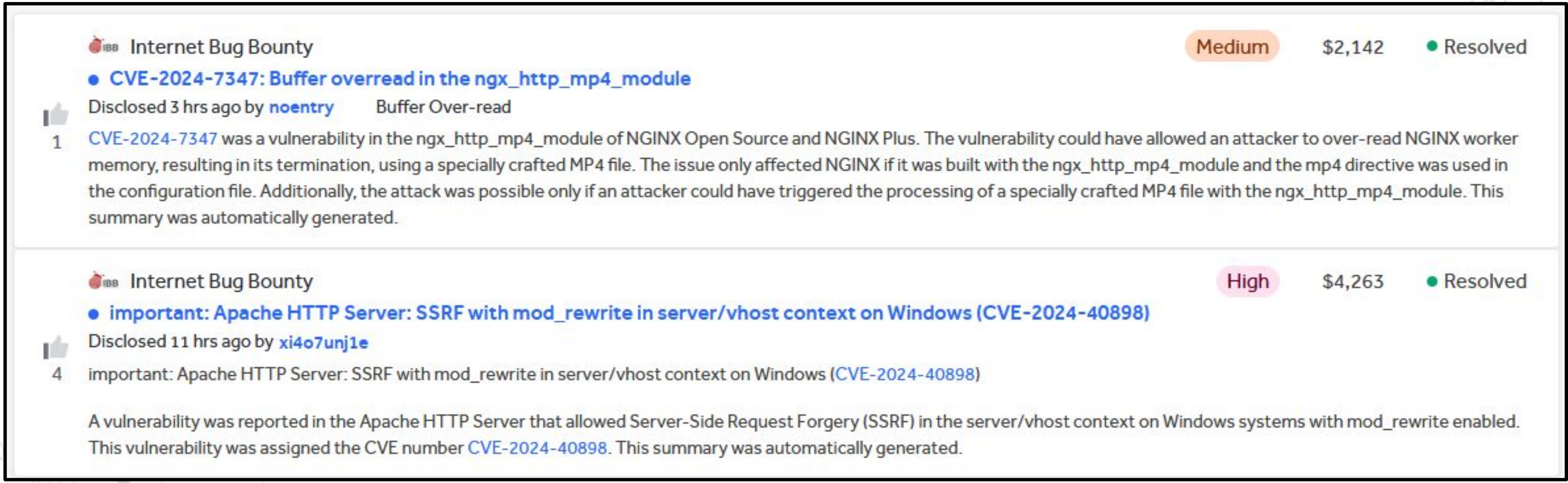
Services in scope

In principle, any Google-owned or Alphabet (Bet) subsidiary web service that handles reasonably sensitive user data is intended to be in scope. This includes virtually all the content in the following domains:

- *.google.com
- *.youtube.com

Legality and Ethics

Many companies even pay people who find vulnerabilities!



Internet Bug Bounty Medium $2,142 ● Resolved

- CVE-2024-7347: Buffer overread in the ngx_http_mp4_module

Disclosed 3 hrs ago by noentry Buffer Over-read

1

CVE-2024-7347 was a vulnerability in the ngx_http_mp4_module of NGINX Open Source and NGINX Plus. The vulnerability could have allowed an attacker to over-read NGINX worker memory, resulting in its termination, using a specially crafted MP4 file. The issue only affected NGINX if it was built with the ngx_http_mp4_module and the mp4 directive was used in the configuration file. Additionally, the attack was possible only if an attacker could have triggered the processing of a specially crafted MP4 file with the ngx_http_mp4_module. This summary was automatically generated.

Internet Bug Bounty High $4,263 ● Resolved

- important: Apache HTTP Server: SSRF with mod_rewrite in server/vhost context on Windows (CVE-2024-40898)

Disclosed 11 hrs ago by xi4o7unj1e

4

important: Apache HTTP Server: SSRF with mod_rewrite in server/vhost context on Windows (CVE-2024-40898)

A vulnerability was reported in the Apache HTTP Server that allowed Server-Side Request Forgery (SSRF) in the server/vhost context on Windows systems with mod_rewrite enabled. This vulnerability was assigned the CVE number CVE-2024-40898. This summary was automatically generated.

https://hackerone.com/hacktivity/overview

Optional Python Practice

This semester will involve some Python coding, starting next week.

We will cover all the basics, but if you have never seen Python before and want a head start:

- https://www.w3schools.com/python/python_getstarted.asp
- https://www.w3schools.com/python/python_syntax.asp
- https://www.w3schools.com/python/python_lists.asp
- https://www.w3schools.com/python/python_dictionaries.asp

Bye!