Batman’s Kitchen Hacker Mindset

2024 Meeting 1

INTRO

Why do we teach people to hack?

- Hacking is a very important skillset to have if you can put it to use **ethically and responsibly**
  - Everything we teach in this club is something that people in the cybersecurity industry use at their day jobs all the time
- The only way to stop (evil) hackers is to find vulnerabilities before they can
- Cybersecurity is a massive industry with a lot of job openings
- Also hacking is super fun

What is a hacker?

What is a hacker?

- Someone who exploits the gaps between assumptions and designs
- Not just computer systems!
  - Social systems (people and organizations)
  - Physical security systems
  - Public information systems

How does a hacker think?

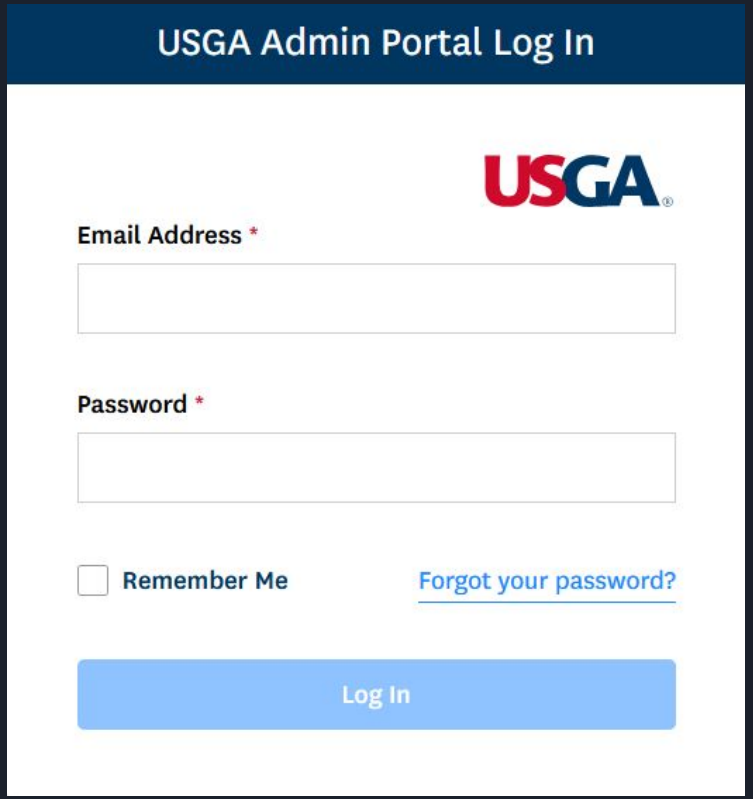
- Interested in seemingly mundane systems
- Figures out how systems work, and what weird edge cases can cause them to not work correctly
- Goes down deep rabbitholes about random things

Part 1: Hack the Internet

Case Study: Admin Login Page

Things a hacker might try:

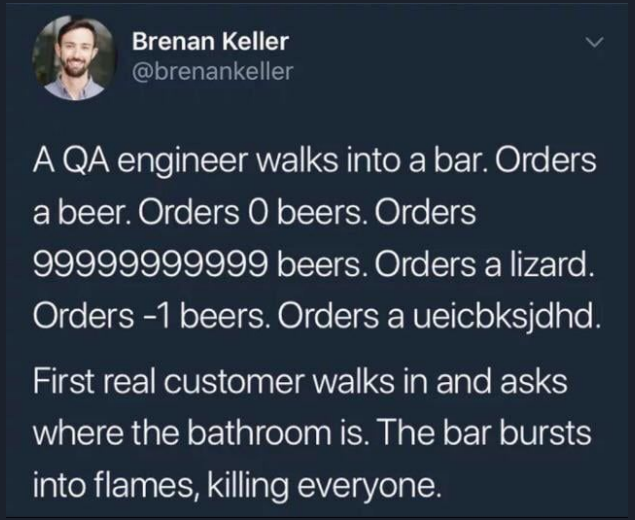
- “admin / password” or “admin / admin”
- Weird Characters (‘:;_-=**&^!#$%
  L⁝˙- ㅠ⁝⁝)
  □□▄□ʒ—□- ◦Ⓗ✲ □≵↜↘÷ⓒ□□□〆⏬)
- Usernames without passwords
- Submitting passwords from a data breach
- Forgor password 💀



Case Study - Shopping Application

What a hacker might try on a shopping website:

- Intercept web request and submit a negative price
- Edit a coupon code to be 100% off
- Submit a refund for something you didn't buy
- Try to buy 1000000000 of an item. Try to buy -1 of an item
- Mess with other people's carts
- Brute force coupon codes



Case Study: UW’s network

- Did you know that you can scan every publicly visible device on UW’s network in like 10 seconds?
  - https://www.shodan.io/search?query=org%3A%22University+of+Washington%22
  - http.html:"admin”
  - http.html:"camera"
  - http.html:"index of"
- Did you know that you can find every UW website that exists in like 10 seconds?
  - https://crt.sh/
  - https://ui.ctsearch.entrust.com/ui/ctsearchui

Part 2: Hack The People

The human is usually the weakest link

- You don’t need a PhD in cryptography to guess the password to the work payroll portal is ‘ILoveMoney$’
- People make mistakes, they make assumptions, and they are too nice
- Sometimes you can just ask nicely and people will give you sensitive information for free
- This is a whole field of security called **social engineering**

Case Study: Shopping Application Part 2

- Circa 2010, you could submit a password reset to your Amazon account if you could confirm a credit card associated with it
- You could also call Amazon Customer Support to add a credit card to your account
- How to hack any Amazon account (100% real) (you have to time travel to 2010)
  - Add a credit card to someone else's account
  - Use that credit card to reset their password
  - ???????
- Skills required: Being able to call customer support (difficulty: impossible)

Case Study: Shopping Application Part 2

- What changed between how the hacker approached this vs. the previous shopping application case study?
- Dealing with a human element and not just computers
  - Nondeterministic
  - Need to be good at talking to people, not just writing code
  - Much more directly connected to the “real world”

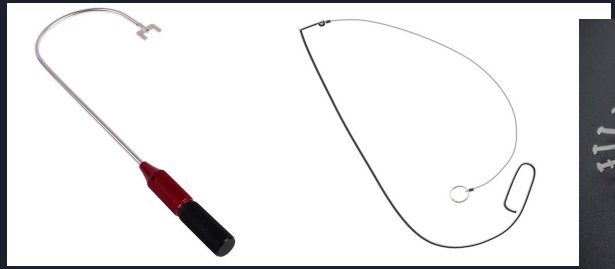
Case Study: Breaking into a corporate office

- Now what if we take this real world connection to the next level?
- The hacker's goal is now to break into Amazon HQ
- What they might try:
  - Just walk in behind someone
    - What if they try to check your badge?
  - Go to a coffee shop across the street and clone an employee's badge
  - Pretend to be an elevator repair tech, pizza delivery guy, IT person, etc.
    - How do you figure out what their IT people, badges, etc. look like?

Case Study: Breaking into a corporate office

Other stuff they could try:

- Weird burglary tools
- Find an RFID reader and wiretap it
- Try to hack a WiFi security camera
- Abuse other weird devices and panels nobody ever thinks about
- I’m gonna shut up about physical security before the other admins kick me off stage



Case Study: Breaking into a corporate office

So we've gone from just hacking websites, to hacking people, to hacking physical access control systems. Now what?

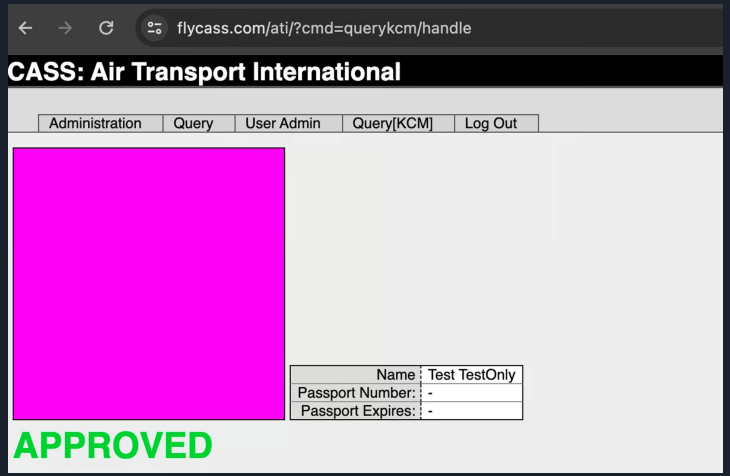
Part 3: Hack the Planet

Case Study: Hacking the transit system

- How do transit cards work? Nobody knows
- …or at least that's what transit organizations think
- Turns out that with many transit cards you can crack the encryption they use and just change how much money is on the card if you know how they work
  - (some of them might not even use encryption!)
- If you're interested in the technical details:
  https://medium.com/@bobbyrsec/operation-charlie-hacking-the-mbta-charliecard-from-2008-to-present-24ea9f0aaa38

Case Study: Hacking the airport

- This year, security researchers discovered that you can just… get full control of the database which controls airport security
- This would allow anyone to skip TSA checks **and also the security system for airliner cockpits**
- Really simple technique (we'll be demoing it next week lmao)
- Didn't get found earlier just because **nobody thought to look for it**



https://ian.sh/tsa

Other wild hacks

The State of log4shell in Minecraft Months Later

66K views • 2 years ago

LiveOverflow

Laws are complicated and internet wide scan...

CC

7 chapters Intro | Let's...

DEF CON 18 - Barnaby Jack - Jackpotting Automated Teller...

87K views • 10 years ago

DEFCONConference

Barnaby Jack - Jackpotting **Automated Teller** Machines Redux T...

21 chapters Intro | Goal | Current Attacks ...

PromptArmor Blog

Data Exfiltration from Slack AI via indirect prompt injection

Authors: PromptArmor

PROMPTARMOR
AUG 20, 2024

20 Share

This vulnerability can allow attackers to steal anything a user puts in a private Slack channel by manipulating the language model used for content generation. This was responsibly disclosed to Slack (more details in Responsible Disclosure section at the end).

DEF CON 22 - Deviant Ollam & Howard Payne - Elevator Hacking -...

803K views • 9 years ago

Hacking Millions of Modems (and Investigating Who Hacked My Modem)

Mon Jun 03 2024

Tying it all back together

- Being a hacker isn’t just about typing stuff into a computer terminal
- Anyone can be a hacker - you just have to think like one
  - Look for weird systems nobody pays attention to
  - Go in rabbit holes
  - Challenge assumptions people make
  - Try weird shit, experiment, break stuff (responsibly)

Tying it all back together

- What are some systems you encounter in your lives which might be interesting to hack?