Lessons from Web3 Security

World’s Fastest Intro

I’m engn33r and I do (did??) security

yAudit

yAcademy

Today’s Presentation

Security landscape today

Security misconceptions

Why security is hard

What you see of security

Cream Finance Exploited in Flash Loan Attack Netting Over $100M

What you see of security

Cream Finance Exploited in Flash Loan Attack Netting Over $100M

Binance Smart Chain hackers made $167M with flash loans, exploits in May

What you see of security

Cream Finance Exploited in Flash Loan Attack Netting Over $100M

Binance Smart Chain hackers made $167M with flash loans, exploits in May

Euler Finance hacked for over $195M in a flash loan attack

DeFi protocol Platypus suffers $8.5M flash loan attack, suspect identified

What you see of security

Cream Finance Exploited in Flash Loan Attack Netting Over $100M

Binance Smart Chain hackers made $167M with flash loans, exploits in May

Value DeFi Suffers $6M Flash Loan Attack

$182 million stolen from stablecoin provider Beanstalk Farms in 'flash loan' attack

Euler Finance hacked for over $195M in a flash loan attack

DeFi protocol Platypus suffers $8.5M flash loan attack, suspect identified


FLIP!

Web3 security history

2020: https://rekt.news/ starts highlighting hacks, DeFi summer begins

2021: code4rena begins, samczsun publishes a lot, security awareness grows

2022: security space growing quickly, long audit backlogs

2023: many new security people onboarded and learn fast

2024: security space is getting crowded, many audit firms, short audit backlogs

2025: ???

Today’s Security Characters

Auditor in a company or DAO

Security engineer (internal to a company or protocol, not auditing)

Solo auditor

Bounty hunter

Honorable Mention - seal911

- @seal_911_bot on Telegram

Why is security needed?

- Every line of code needs review
- The stakes are high
- Many incentivized blackhats

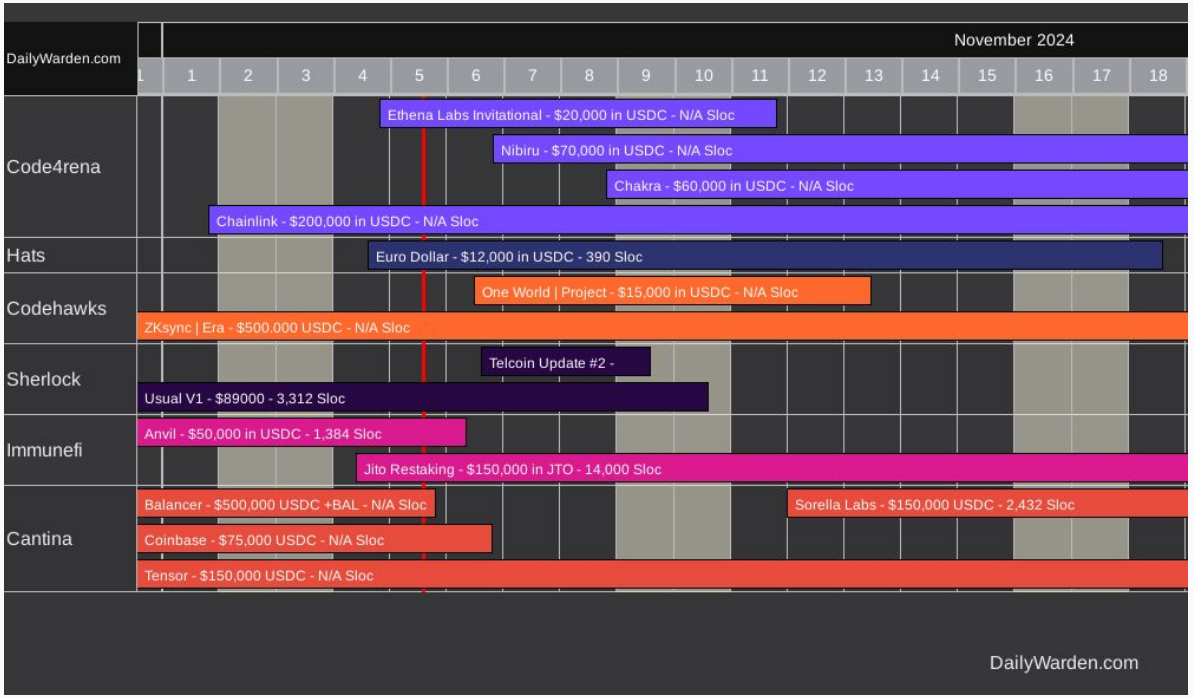
Many Misconceptions

Common Misconceptions

1. It’s too hard for me to learn web3 security because of _____
2. You have to know about all the hacks ever
3. It’s a high stress job
4. North Korea in unstoppable
5. Protocol developers are idiots if they get hacked
6. Security is the best job EVER!!

1. It’s Too Hard to Learn

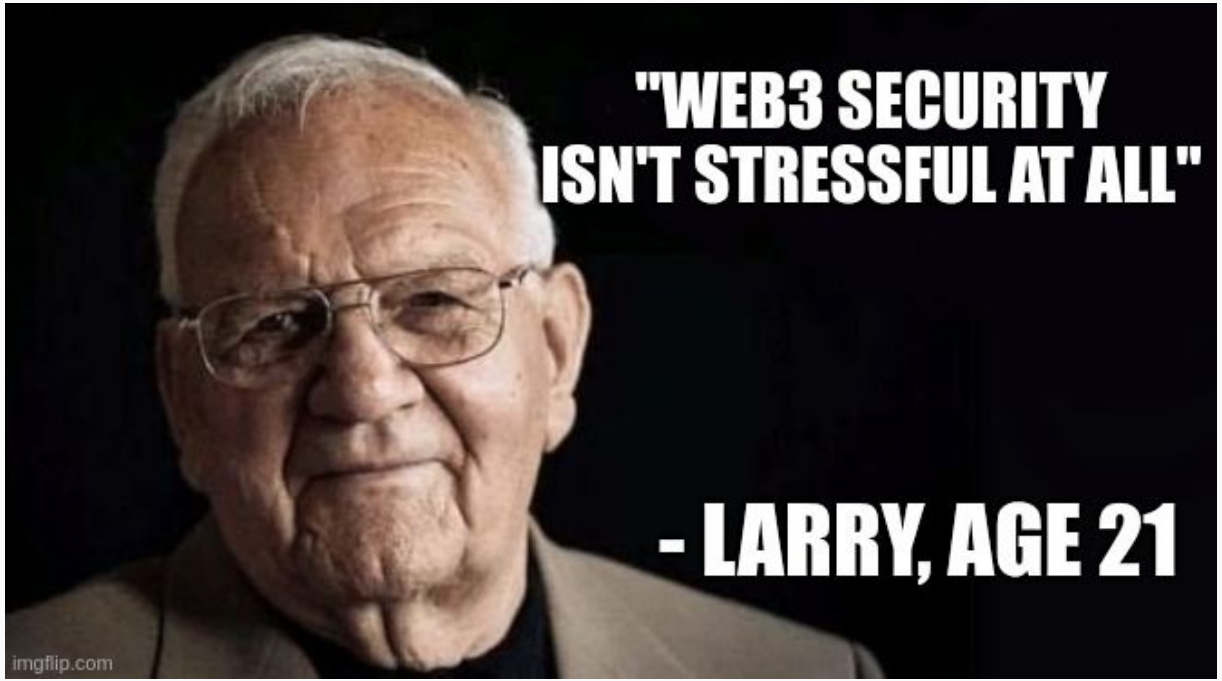
- Contests = incentive
- Learning takes time
- Solidity is easy
- yAcademy and Secureum hold trainings



2. Knowing all Hacks Ever

- You can focus on very specific bugs and still succeed
- Auditors should find all bugs, bug bounties or contests don’t require this
- Many hacks are known vulnerabilities (duplicates of past hacks)
- Great list of past hacks: https://github.com/SunWeb3Sec/DeFiHackLabs

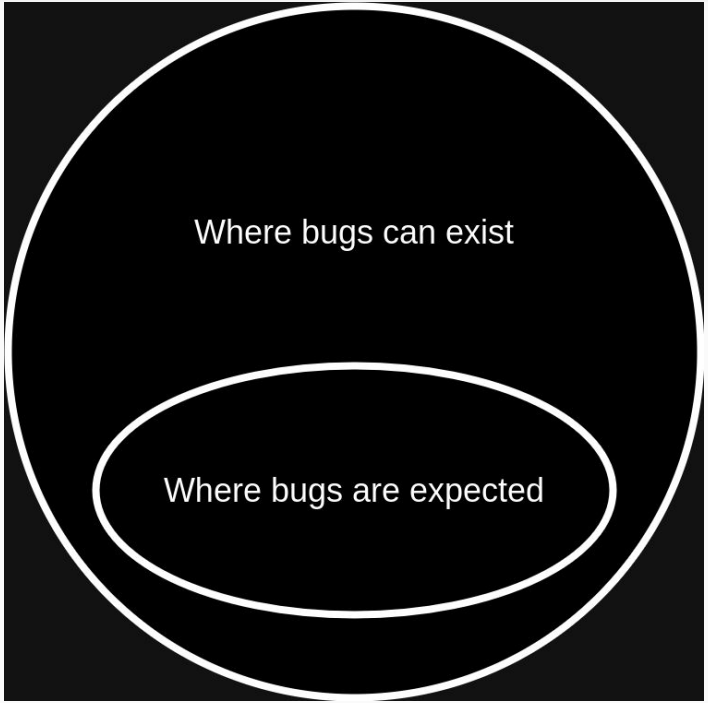
3. Stressful Job



3. Stressful Job

- **Auditors:** constant fear of missing findings (FOMF)
- **Security engineers:** constant fear of deploying and getting “u up?”
- **Solo auditors:** where are my next clients
- **Bounty hunter:** will I ever find anything

3. Stressful Job



4. North Korea is Unstoppable

- Very few hacks use novel types of attacks
- There’s SO MANY ways a protocol can be hacked that having all defenses activated 100% of the time is hard
- Web3 teams forget about web2 security 🤡

4. North Korea is Unstoppable

Attack Vectors by Incident Count

1	Price Oracle Manipulation	29	6	Reentrancy	11
2	Function Access Control	19	7	Logic Error	8
3	Reward Manipulation	18	8	Incorrect Reward Calculation	7
4	Stolen Private Keys	16	9	Weak Private Keys	5
5	Function Parameter Validation	13	10	DNS Hijacking	5

5. Devs of hacked protocols are idiots

- Some yes, some no
- Depends on the vulnerability. Novel vulnerabilities are hard to see

6. Security Jobs are the BEST

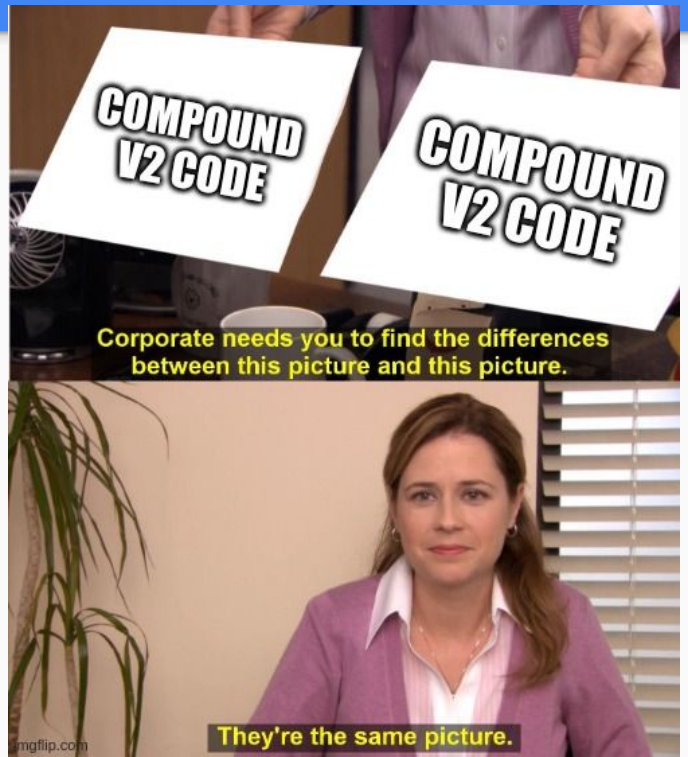
- If you’re paranoid, it’s a great fit
- If you’re not paranoid, you will become paranoid

- Devs will always argue whether something is a legit issue

- After a while, you expect code to always have bugs…
- Expecting all code to have bugs is not a positive view of tech 🥲

6. Security Jobs are the BEST

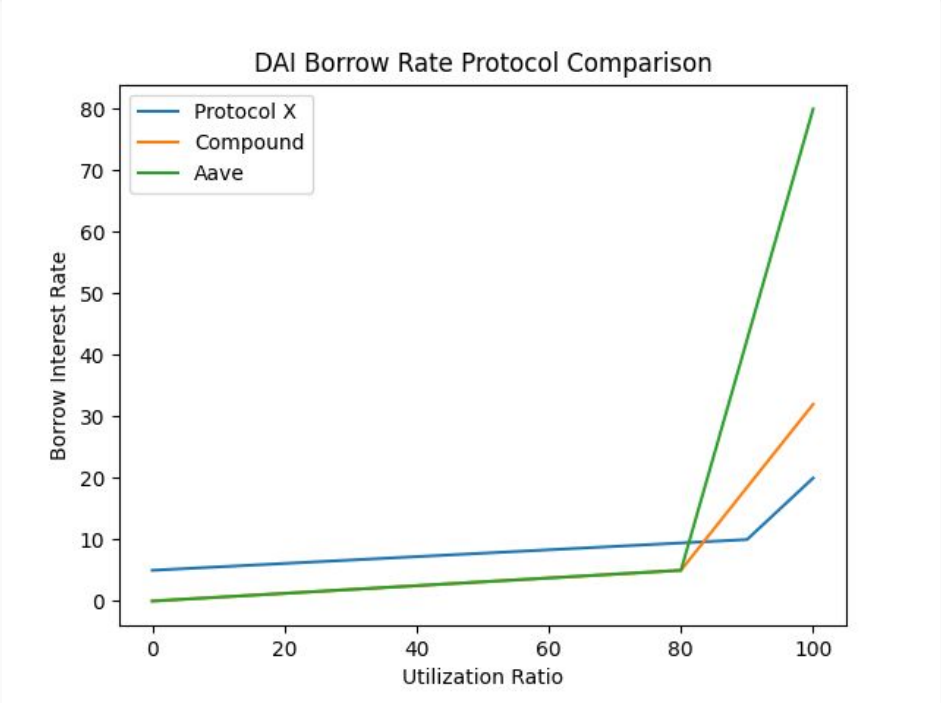
Why Security is Hard



Why Security is Hard

- CREAM: flashloan attack & reentrancy with ERC777-like token (no checks-effects-interaction protection) Postmortem POC
- CREAM: Price manipulation Postmortem POC
- Lendf.me: Flashloan and reentrancy (no checks-effects-interaction protection) Postmortem
- Compound: Double-entry point token issue Retrospective POC
- Lodestar Finance: Exchange rate manipulation Thread POC
- Hundred Finance: Flashloan and reentrancy on gnosis, where native token has callback hook (no checks-effects-interaction protection) Postmortem
- Ola Finance: Flashloan and reentrancy (no checks-effects-interaction protection) Postmortem
- Rari Capital: Flashloan and reentrancy (no checks-effects-interaction protection) POC
- Venus: Chainlink LUNA oracle became inaccurate during the Terra collapse, which cause a similar result as oracle manipulation and led to draining of protocols writeup
- Hundred Finance: Exploit of empty markets Postmortem POC
- 0VIX: price oracle vulnerability allowed donation-based price maniulation Thread POC
- Midas Capital: Exploit of empty markets writeup
- Onyx Finance: Exploit of empty markets Postmortem POC
- Sonne Finance: Exploit of empty markets Postmortem

Why Security is Hard



Why Security is Hard

Block	Age	Txn	Fee Recipient
19904531	3 mins ago	123	beaverbuild
19904530	3 mins ago	134	beaverbuild
19904529	3 mins ago	137	beaverbuild
19904528	3 mins ago	177	beaverbuild
19904527	4 mins ago	141	beaverbuild

Why Security is Hard

EIP implementation is not synchronized between chains

- EIP-1559 (gas fee pricing change)
  - Mainnet Ethereum: August 5 2021
  - Polygon: January 18 2022
  - Optimism: June 6 2023
  - BNB: August 30 2023

Undiscovered Web3 Security jobs?

- Web3 wallet penetration tester
- Web3 frontend penetration tester
- L1/L2 networking security expert
- DeFi protocol specialist (lending protocols, options protocols, etc.)
- Post-deployment monitoring specialist
- Blockchain-specific specialization
- Security tool expert (fuzzing, etc.)
- Post-hack recovery experts

Summary

Web3 security landscape keeps changing

Many misconceptions exist

Security is hard, but more and more learning avenues exist

The End

Slides QR Code