



CSC 405

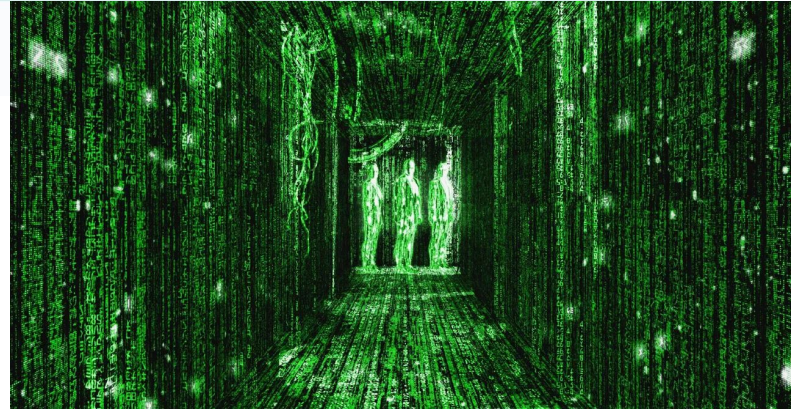
Computer Security

Alexandros Kapravelos
akaprav@ncsu.edu

**Why take a course in
computer security?**

The computer security problem

- Security is everywhere (like the Matrix)
- Developers are not aware of security (we should fix this!)
 - Buggy software
 - Legacy software
 - Social engineering
- Vulnerabilities can be very damaging (and expensive)
- There is financial incentive in finding and exploiting vulnerable systems



Hacking used to be cool

But now everything is done for profit!

Listed for \$200,000



[source](#)

Twitter - DB/Scrape Leak 200+Mill Lines

by StayMad - Wednesday January 4, 2023 at 12:04 AM

Today, 12:04 AM (This post was last modified: 11 hours ago by pompompurin.)

#1

StayMad



GOD User



Posts: 2
Threads: 1

Twitter 200+ m DB/Scrape



Sample Format

Quote:

Email: [REDACTED] - Name: [REDACTED] - ScreenName: [REDACTED] - Followers: [REDACTED] - Created At: [REDACTED] 2013
Email: [REDACTED] - Name: [REDACTED] - ScreenName: [REDACTED] - Followers: [REDACTED] - Created At: [REDACTED]
Email: [REDACTED] - Name: [REDACTED] - ScreenName: [REDACTED] - Followers: [REDACTED] - Created At: [REDACTED]

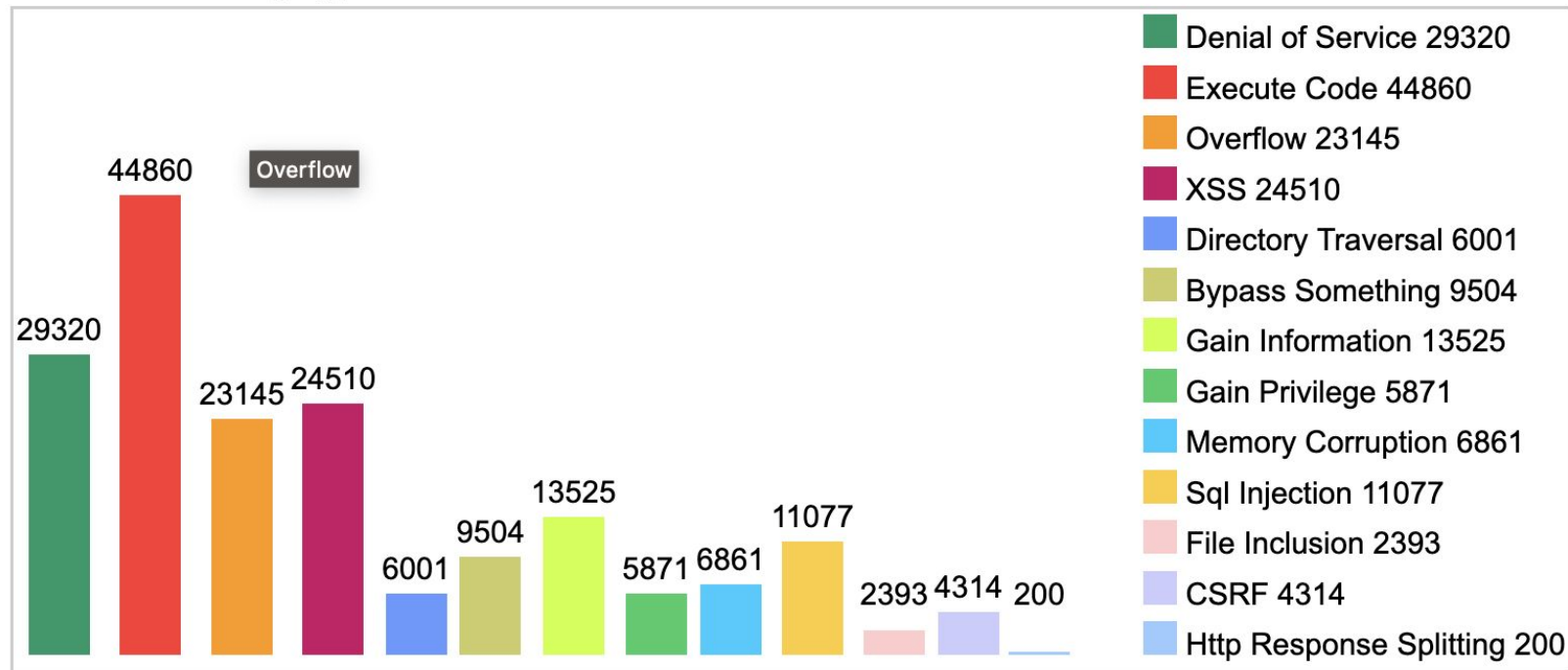
List of 100k Verified Accounts

Vulnerabilities per product - 2022

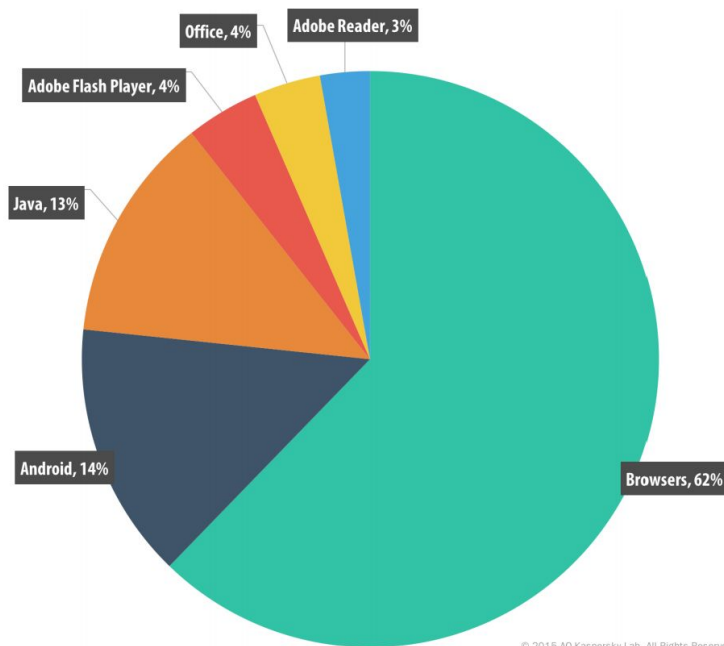
	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	7528
2	Android	Google	OS	4902
3	Fedora	Fedoraproject	OS	4115
4	Ubuntu Linux	Canonical	OS	3709
5	Mac Os X	Apple	OS	3101
6	Linux Kernel	Linux	OS	3034
7	Windows 10	Microsoft	OS	3016
8	Iphone Os	Apple	OS	2864
9	Windows Server 2016	Microsoft	OS	2786
10	Chrome	Google	Application	2586

Vulnerabilities per type - 1999-2022

Vulnerabilities By Type

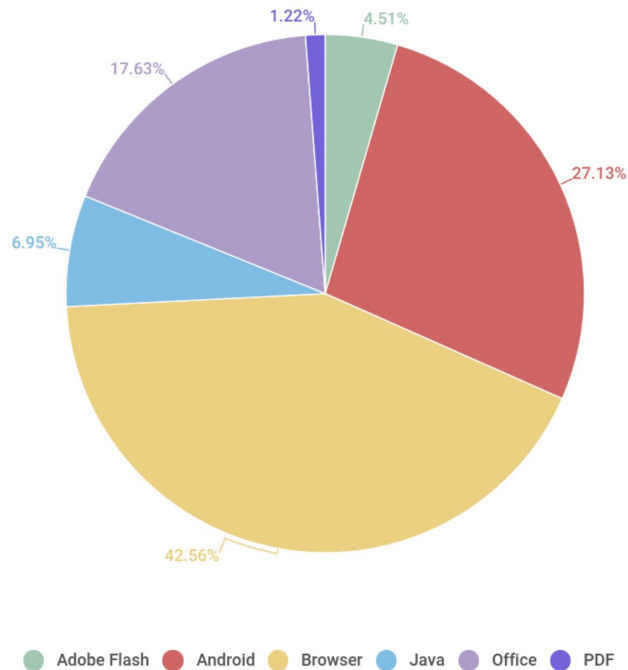


Distribution of exploits per application 2015

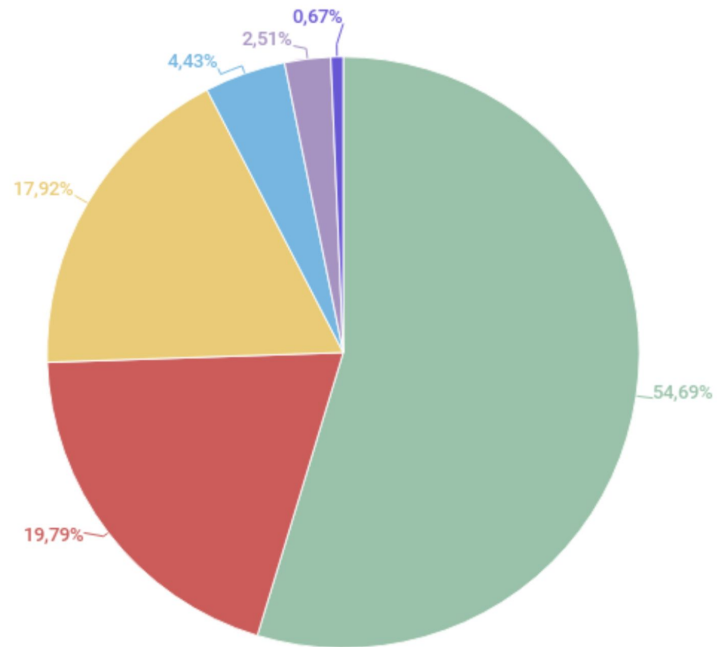


© 2015 AO Kaspersky Lab. All Rights Reserved.

Distribution of exploits per application 2017

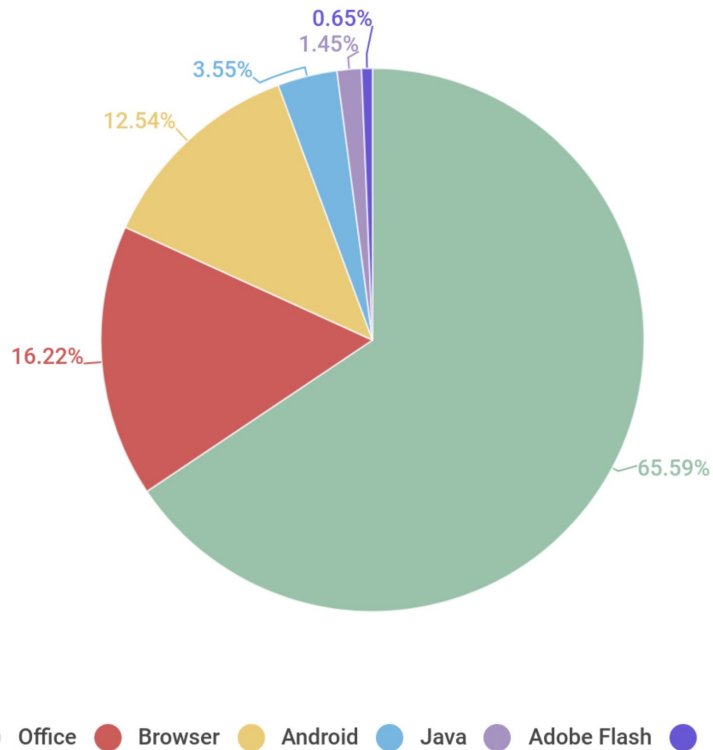


Distribution of exploits per application 2018

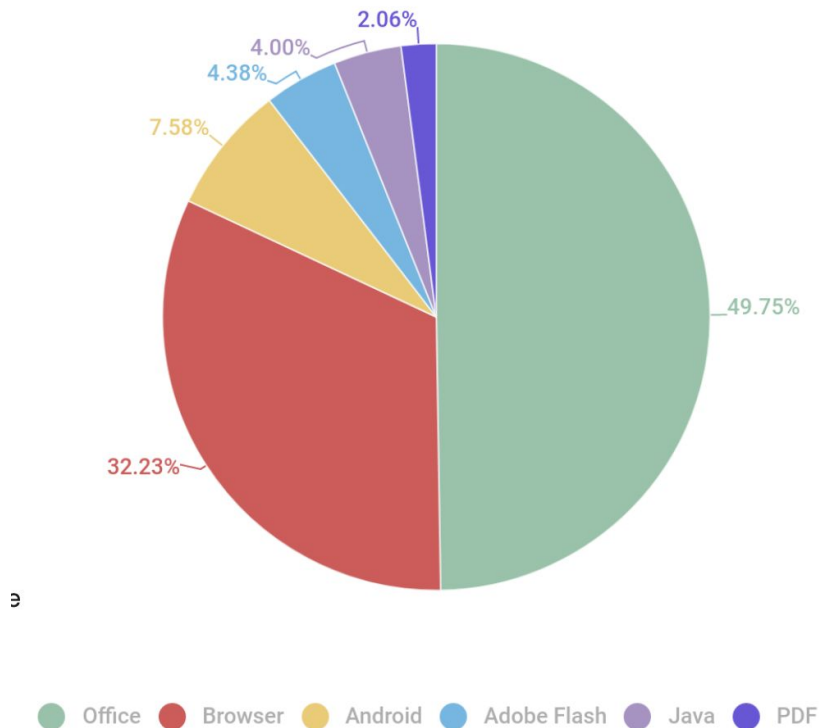


● Office ● Browser ● Android ● Java ● Adobe Flash ● PDF

Distribution of exploits per application 2019



Distribution of exploits per application 2021



Bug bounty programs

- Companies will pay you money to report vulnerabilities
- Certain conditions and rules per program
 - No Denial-of-service attacks
 - Spam
 - ... (depends on the program)
- Hackerone
 - <https://hackerone.com/hacktivity>

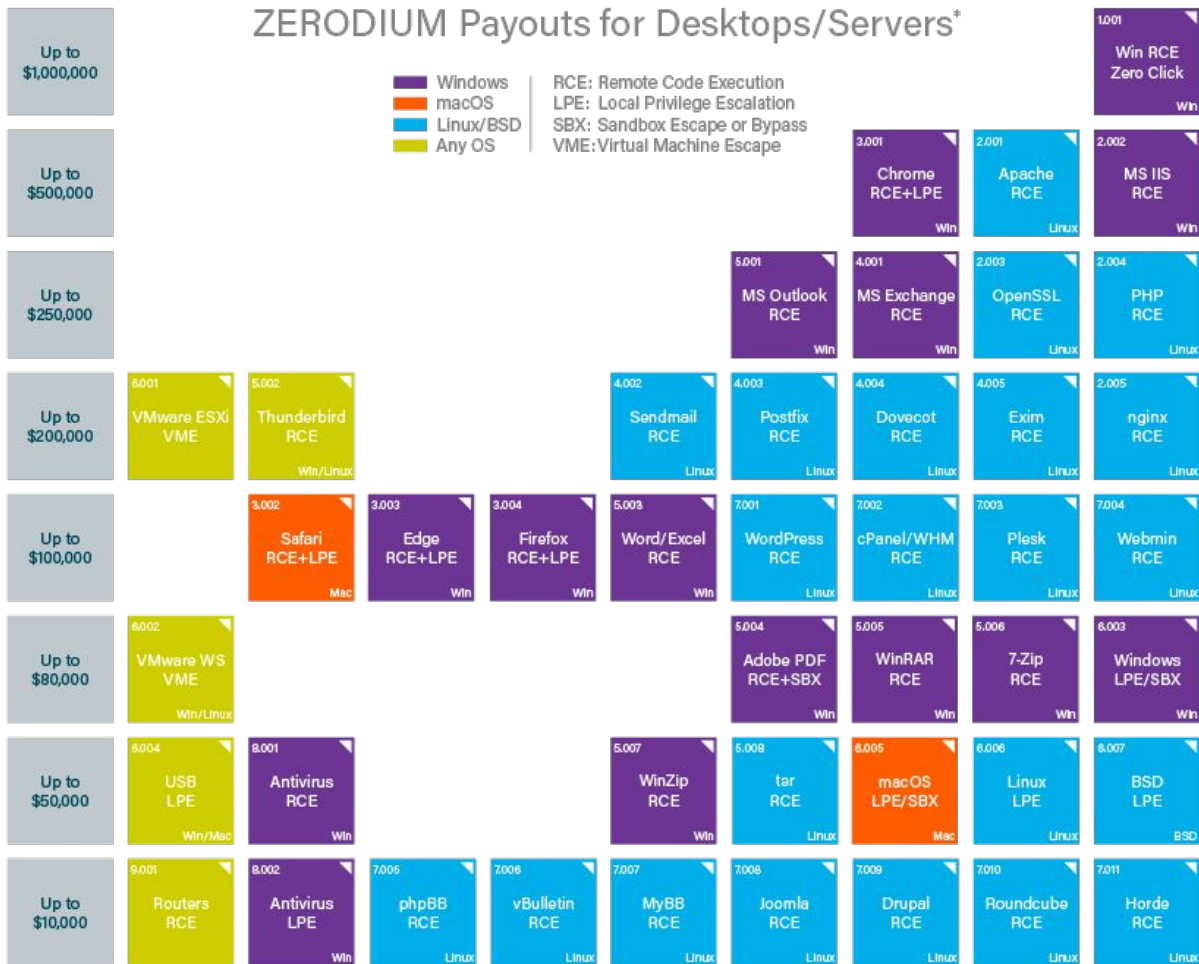
Black market for exploits

Last iOS exploit was sold for

more than 1 million dollars

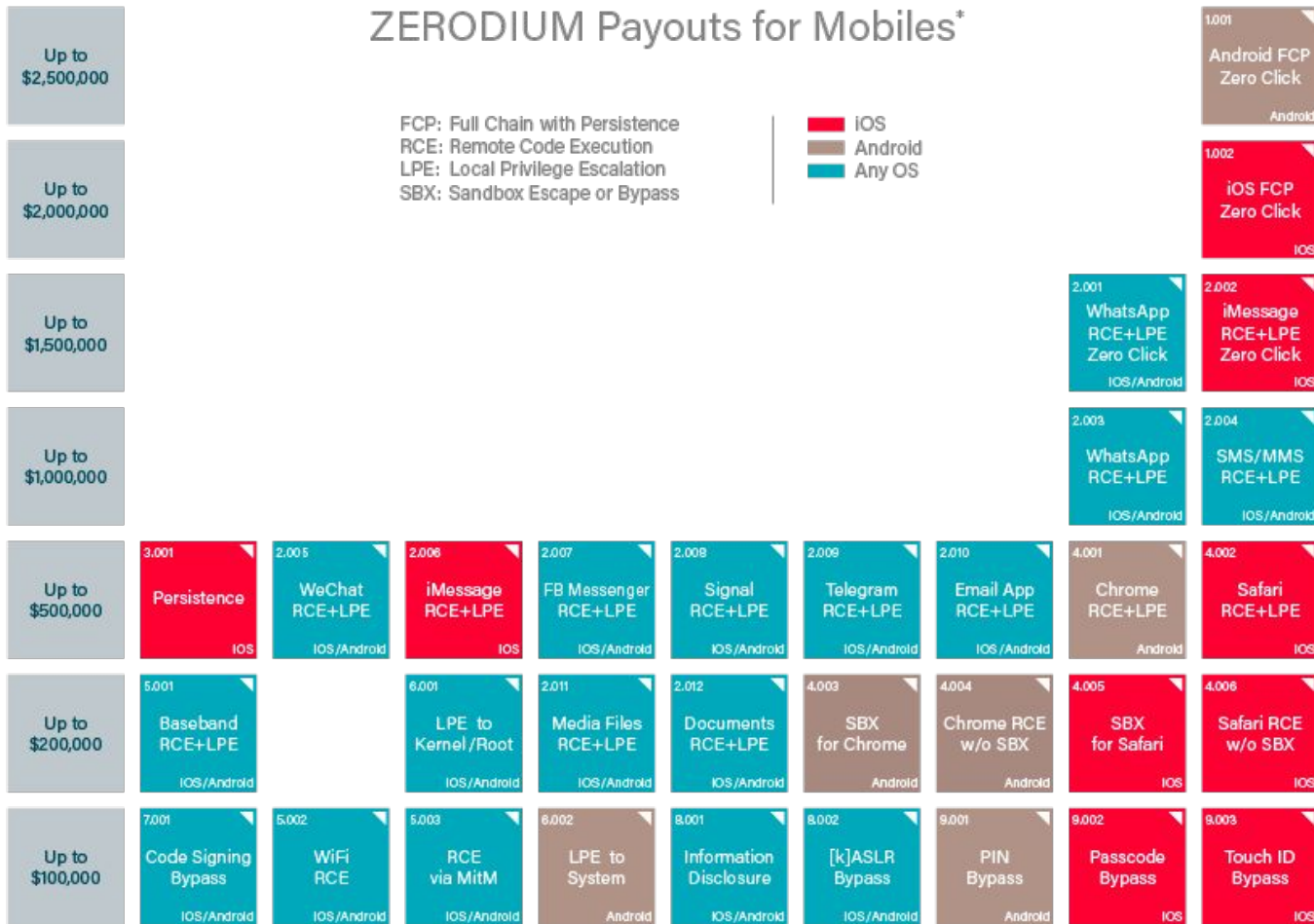


ZERODIUM Payouts for Desktops/Servers*



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

ZERODIUM Payouts for Mobiles*



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

Exploits for modern software are extremely
difficult to write!

Chrome exploit

- Bug 1: run Native Client from any website
- Bug 2: integer underflow bug in the GPU command decoding -> ROP chain in GPU process
- Bug 3: impersonate the renderer from the GPU in the IPC channel
- Bug 4: allowed an unprivileged renderer to trigger a navigation to one of the privileged renderers -> launch the extension manager

Chrome exploit

- Bug 5: specify a load path for an extension
- Bug 6: failure to prompt for confirmation prior to installing an unpacked NPAPI plug-in extension

Result: install and run a custom NPAPI plugin that executes outside the sandbox at full user privilege

Your Security Zen

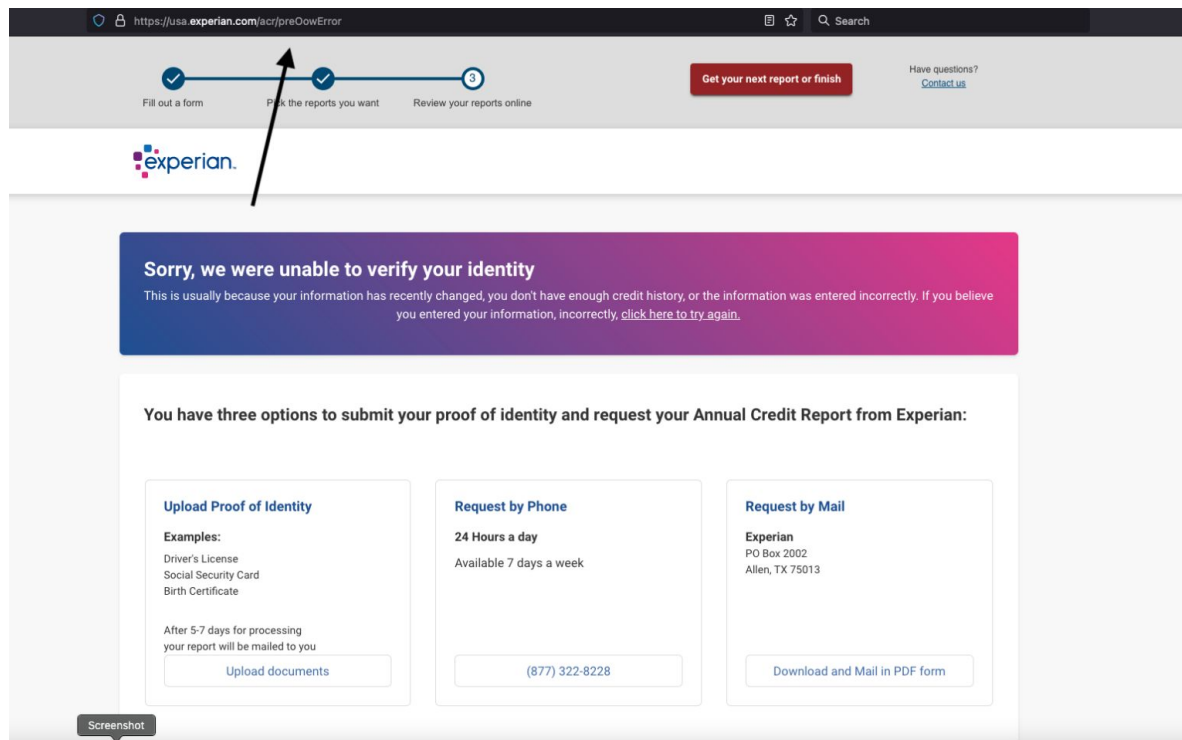
At the end of every lecture we will have a short discussion on a recent security topic

Use piazza or [HackPack's Discord server](#) #random channel if you see in the news interesting security incidents!



Your Security Zen

Identity Thieves Bypassed Experian Security to View Credit Reports



The screenshot shows the Experian website interface. At the top, there is a progress bar with three steps: 'Fill out a form' (checked), 'Pick the reports you want' (checked), and 'Review your reports online' (not checked). A red button labeled 'Get your next report or finish' is visible. Below the progress bar is the Experian logo. A large error message box states: 'Sorry, we were unable to verify your identity. This is usually because your information has recently changed, you don't have enough credit history, or the information was entered incorrectly. If you believe you entered your information, incorrectly, [click here to try again](#).' Below the error message, there are three options to submit proof of identity: 'Upload Proof of Identity', 'Request by Phone', and 'Request by Mail'. Each option includes details and a button to proceed.

https://usa.experian.com/acr/preOowError

Fill out a form ✓ Pick the reports you want ✓ Review your reports online ③

Get your next report or finish

Have questions? [Contact us](#)

experian.

Sorry, we were unable to verify your identity

This is usually because your information has recently changed, you don't have enough credit history, or the information was entered incorrectly. If you believe you entered your information, incorrectly, [click here to try again](#).

You have three options to submit your proof of identity and request your Annual Credit Report from Experian:

- Upload Proof of Identity**
Examples:
Driver's License
Social Security Card
Birth Certificate
After 5-7 days for processing your report will be mailed to you
[Upload documents](#)
- Request by Phone**
24 Hours a day
Available 7 days a week
[\(877\) 322-8228](#)
- Request by Mail**
Experian
PO Box 2002
Allen, TX 75013
[Download and Mail in PDF form](#)

Screenshot

SOUTHEAST CYBERSECURITY PITCH COMPETITION

ROUND 1 - NORTH CAROLINA

WHAT?

DO YOU HAVE A BUSINESS IDEA IN **CYBERSECURITY, DATA PROTECTION, PRIVACY, OR CYBER SAFETY**? SELECTED APPLICANTS WILL PITCH TO INVESTMENT EXPERTS.

PRIZES?

\$25,000 TOP PRIZE

ADVICE FROM JUDGES & VC FIRMS, STARTUP LEGAL SUPPORT,
EXPOSURE TO LEADING VC FIRMS

WHEN?

ROUND 1: FEBRUARY 11TH, 2023

FINAL ROUND (IF SELECTED):

MARCH 10, 2023 (WASHINGTON DC)

HOW?

SCAN THE QR CODE FOR
WEBSITE WITH SIGN-UP FORM
AND MORE INFORMATION



Venture Sponsor:



PALADIN
CAPITAL GROUP

Corporate Sponsors:



University Sponsors:



Supporting Partners



JupiterOne

FORGEPOINT

