CS 106S Week 5

👾 Ethical Hacking & Web Security

Ben Yan, Winter 2025 ☃️

Based on materials by Stanford Applied Cyber, all credit to **Aditya Saligrama & Cooper de Nicola**

Student
Benjamin Yan

Total Points
450 / 45 pts

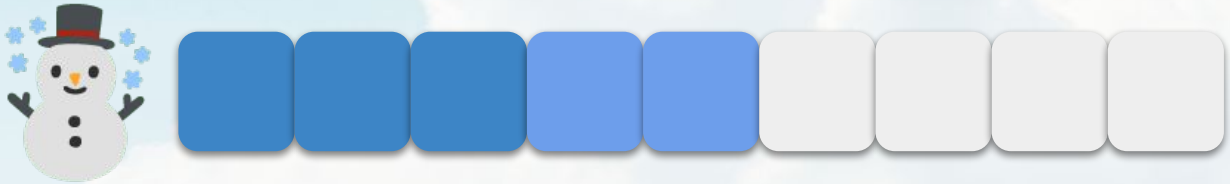
Question 1
Download Materials and Honor Code Acknowledgement

cs106s.stanford.edu

Stanford | ENGINEERING
Computer Science

Welcome back!
Great to see you :)

It’s Week 5 wow



Winter Break

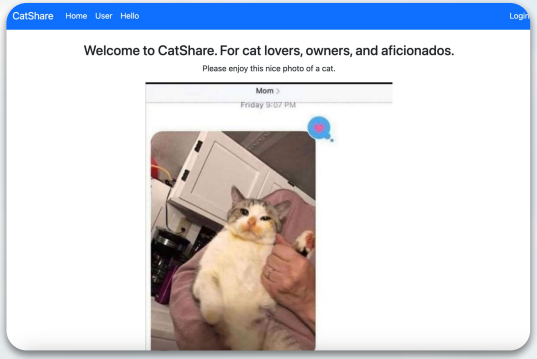
Spring Break

Agenda for Today

1. Brief overview of cybersecurity, relevant & modern case studies

2. Crash course of the web & web hacking, typical insecure designs

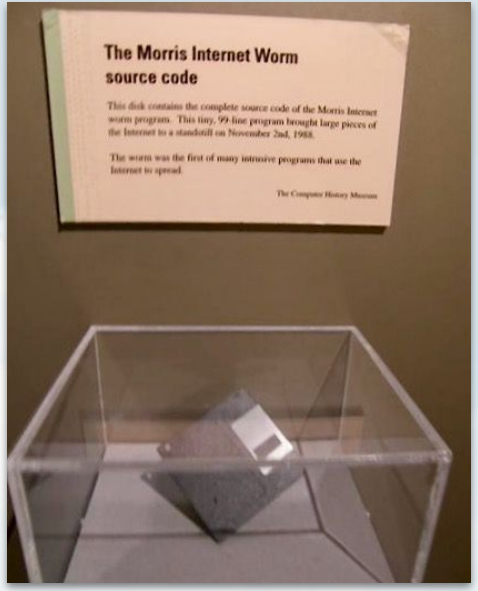
3. project: hacking a public cat photosharing website



4. Reflections & check-off form!

1988: Morris Worm

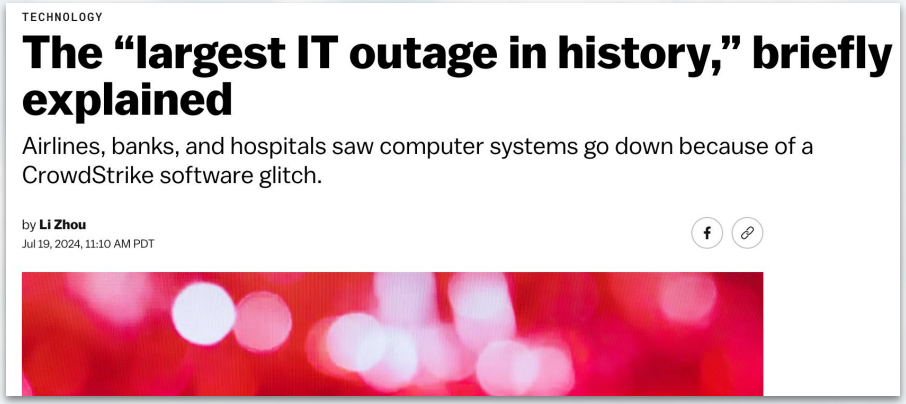
- **First computer worm on the Internet**
- Nov. 1988 – A Cornell grad student (Robert Morris) released a worm from MIT, exploiting computers with certain UNIX and network security flaws.
- The worm could replicate itself repeatedly, leading to some computers crashing over and over again.
- **Est. 10% of all machines at the time were infected.**
- Morris was caught and convicted, in 1989, under the brand new **Computer Fraud and Abuse Act.**
- He then went on to become a tenured professor in EECS at MIT ✨, with research on computer networks.



for ethical reasons, this is a joke

2024: Crowdstrike Outage

- **~8.5 million system crashed** (endless blue screens of death)
- Though the bug was found within hours, many computers had to be fixed manually → persisting outages



TECHNOLOGY

The "largest IT outage in history," briefly explained

Airlines, banks, and hospitals saw computer systems go down because of a CrowdStrike software glitch.

by **Li Zhou**
Jul 19, 2024, 11:10 AM PDT

https://www.vox.com/technology/361740/crowdstrike-outage-windows

Why should we care about security?

Basically everything out there is secure by now right?

Stanford Link (2020)

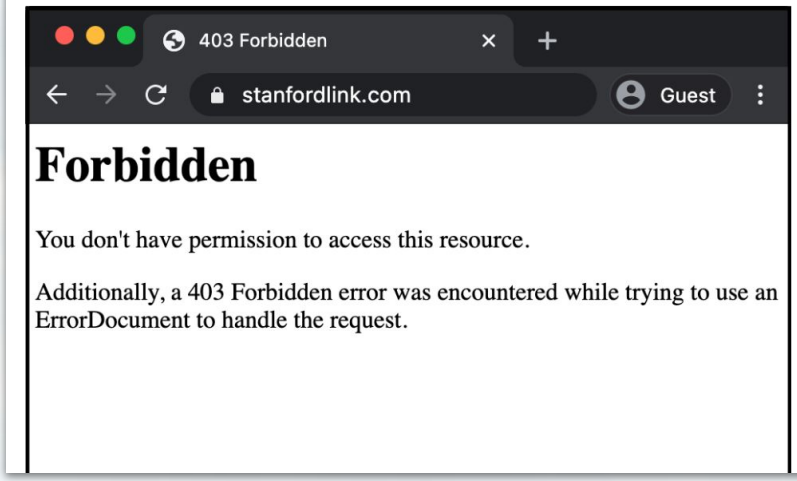
News • Campus Life

New Stanford Link website connects students with mutual crushes

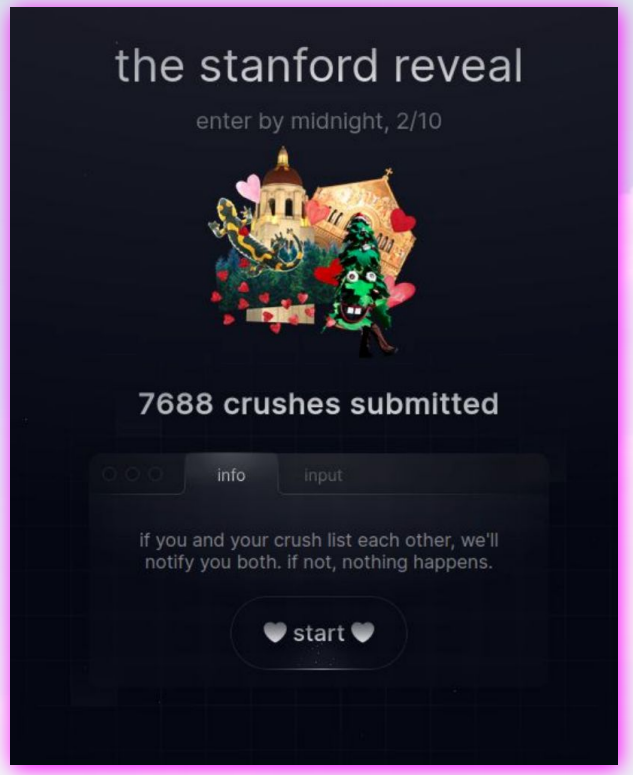
Stanford Link's logo. (Photo: stanfordlink.com)

News • Campus Life

Vulnerability in 'Link' website may have exposed data on Stanford students' crushes



Stanford Reveal (2023)




```
{
  "submittingUserEmail": "bbyan@stanford.edu"
  "submittingUserFullName": "Benjamin Yan",
  "user": "YmVuamFtaW4geWFu",
  "fullNames": ["Squid Game Recruiter"]
},
```

Gradescope (2023) 😭😭

A student's dream: hacking (then fixing) Gradescope's autograder

February 28, 2023
2630 words

Ever since I started exploring security more deeply, I've been asked countless times by people if I could hack into grading systems to change my (or, more often, their) grades. With Gradescope being the most ubiquitous platform for grading STEM classes at Stanford, my standard response was always that I couldn't, imagining that a well-established EdTech company would secure their platform well enough.

As it turns out, Gradescope's autograders have been vulnerable to various types of attack since 2016. Gradescope has known about the issues since at least 2020, yet has indicated it cannot distribute a general fix.

This post covers my exploration of Gradescope's autograder vulnerabilities, an analysis of the potential impact on courses, and how I created Securescope, my attempt at a more secure autograder configuration.

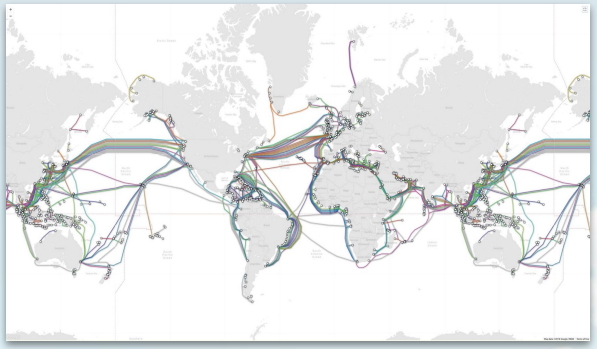
https://saligrama.io/blog/gradescope-autograder-security/

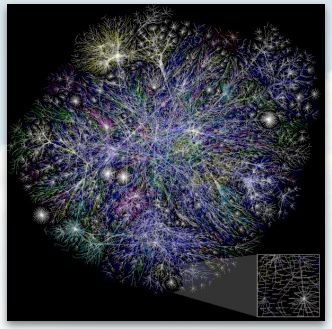
Why should we hack stuff?

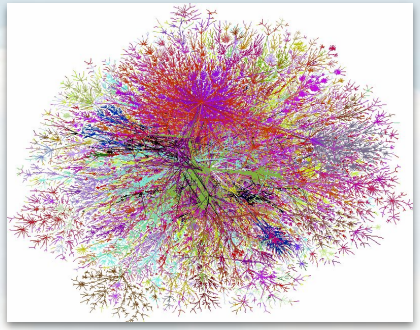
Hear me out...

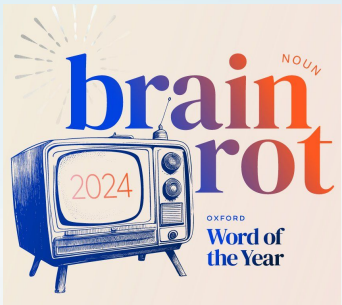
The Internet in a nutshell

What being chronically / terminally online has taught me









"The supposed deterioration of a person's mental or intellectual state, especially viewed as a result of overconsumption of material (now particularly online content) considered to be trivial or unchallenging." – *Oxford Dictionary*

Shams Charania ✓
@ShamsCharania

Follow

BREAKING: The Dallas Mavericks are trading Luka Doncic, Maxi Kleber and Markieff Morris to the Los Angeles Lakers for Anthony Davis, Max Christie and a 2029 first-round pick, sources tell ESPN. Three-team deal that includes Utah.

Internet: Client-Server Model

A conventional abstraction

HTTPS Request for
`cs106s.stanford.edu`

Internet

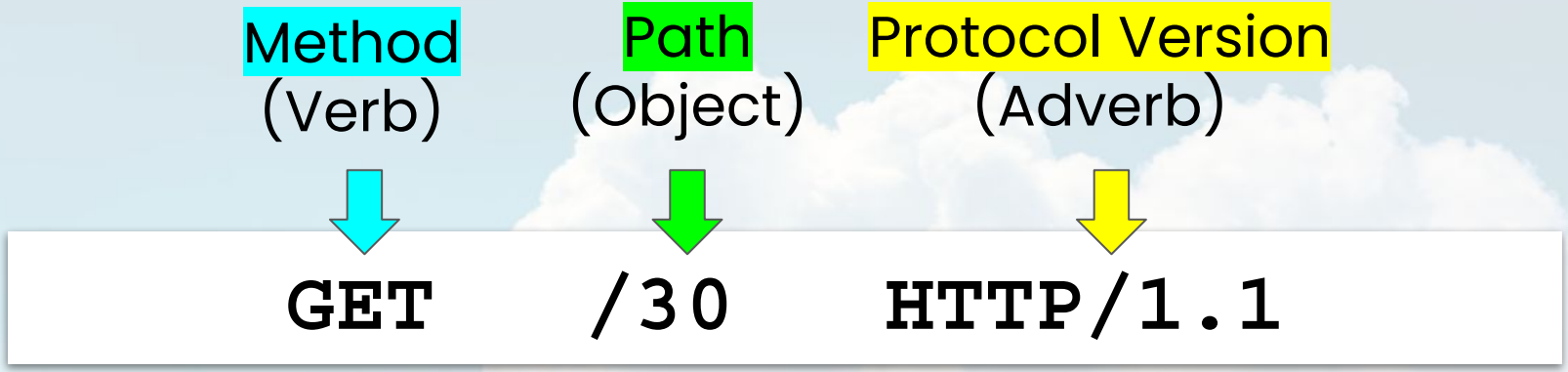
HTTPS Response of
`index.html`

User **Client Browser** **Web Server**

The client (who initiates requests for resources) and server communicate over a computer network, e.g., the Internet

HTTP: Hypertext Transfer Protocol

Request-response communication with web server



Headers
(Modifiers)

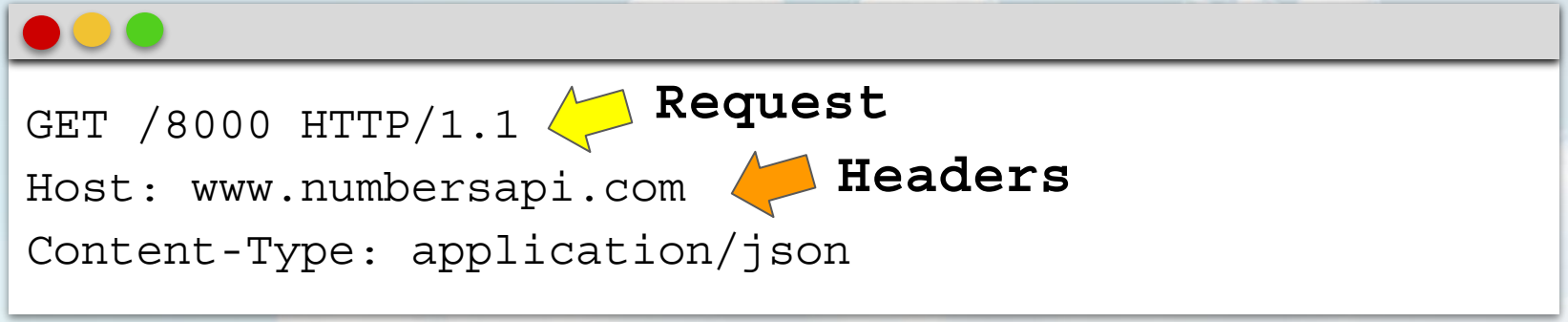
```
Host: www.numbersapi.com
Content-Type: application/json
```

Demo: Sending HTTP Requests in the Terminal via `telnet`

HTTP: Hypertext Transfer Protocol

Request-response communication with web server

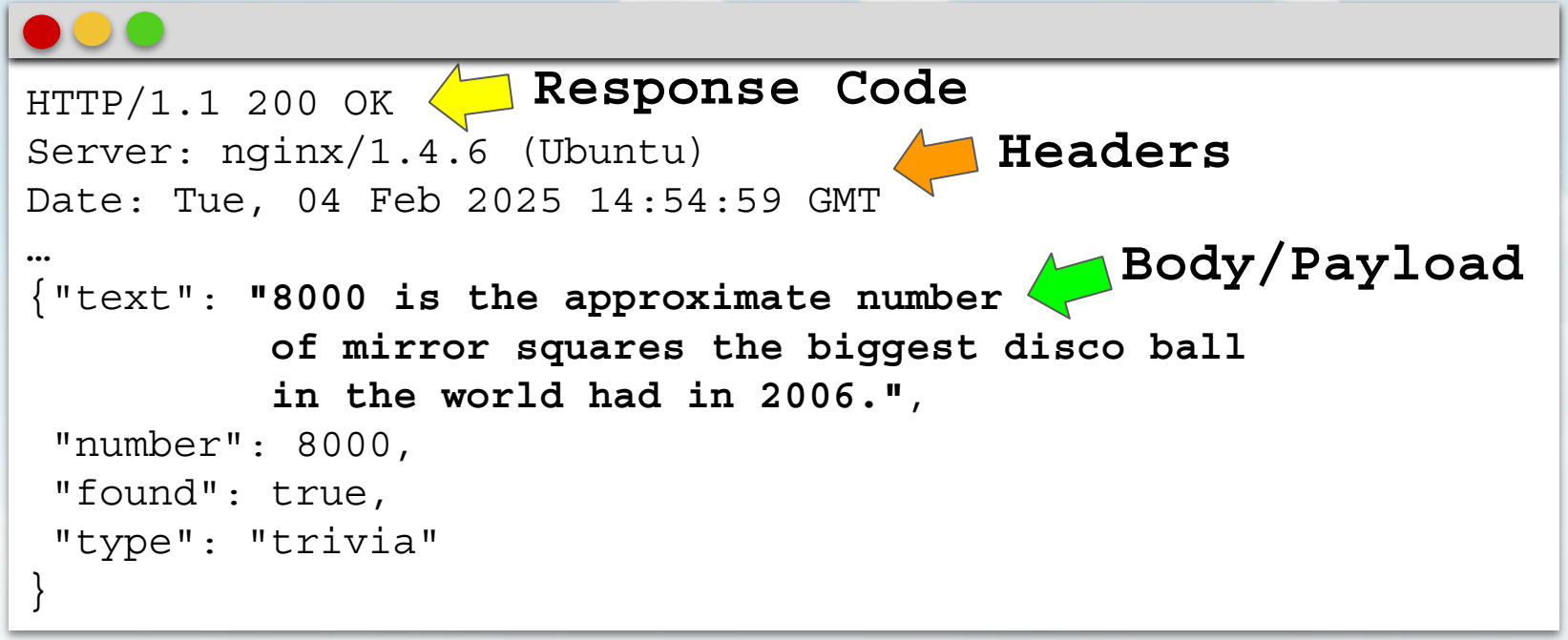
Say we want some fun facts about the number `8000`...



HTTP: Hypertext Transfer Protocol

Request-response communication with web server

We got a fun fact I guess



HTTP Requests: GET vs POST

- A **`GET`** request **only extracts** data from a server.
- A **`POST`** request **modifies or updates resources** on the server side, like making changes within a database.

HTTP Requests: GET vs POST

- A **GET** request **only extracts** data from a server.
- A **POST** request **modifies or updates resources** on the server side, like making changes within a database.

```
GET /api/images
```

Client (JavaScript)


```
['img1.jpg',
 'img2.jpg',
 ...]
```

Web Server / Database

E.g., a **GET** request may fetch one's Instagram feed from an internal database, with the payload (**server→ client**) being a collection of images.

HTTP Requests: GET vs POST

- A **GET** request **only extracts** data from a server.
- A **POST** request **modifies or updates resources** on the server side, like making changes within a database.

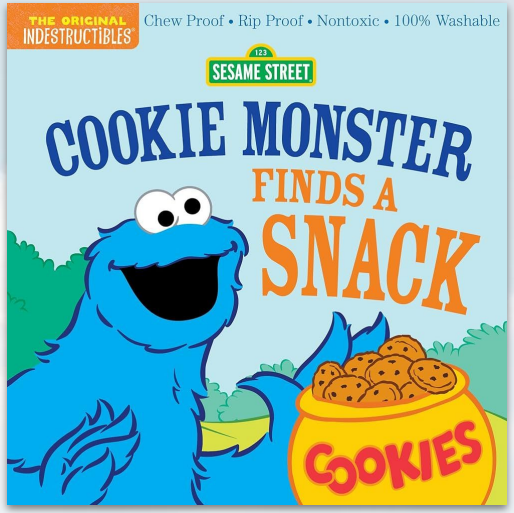
```
POST /api/images
```

E.g., a **POST** request may add a newly posted image to the Instagram database, with the payload (**client**→ **server**) being the new image.

Session Handling

How does a website remember user sessions / logins?

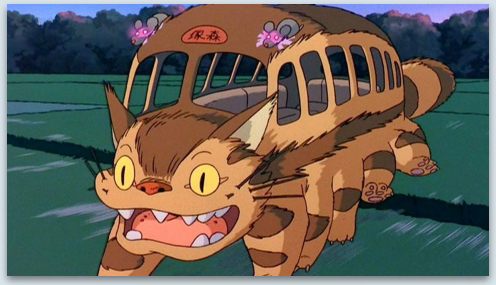
- **Cookies!** 🍪🍪🤌
- Cookies allow websites to store **stateful information** (e.g., classes added to a SimpleEnroll planner), or to track browsing activity.
- **Authentication Cookies:** Used to authenticate that a user is currently logged in & with which account



website = cookie monster

When logging in: `Set-Cookie: session=session_id`
After first login: `Cookie: session=session_id` 🍪

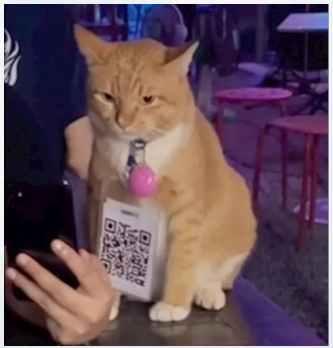



🐈 Catshare Website

https://catshare.saligrama.io

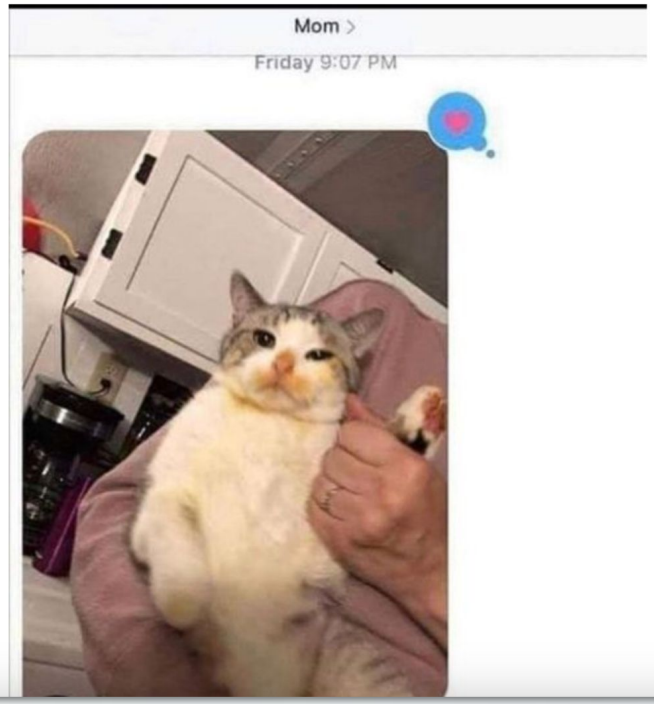



CatShare Home User Hello Login

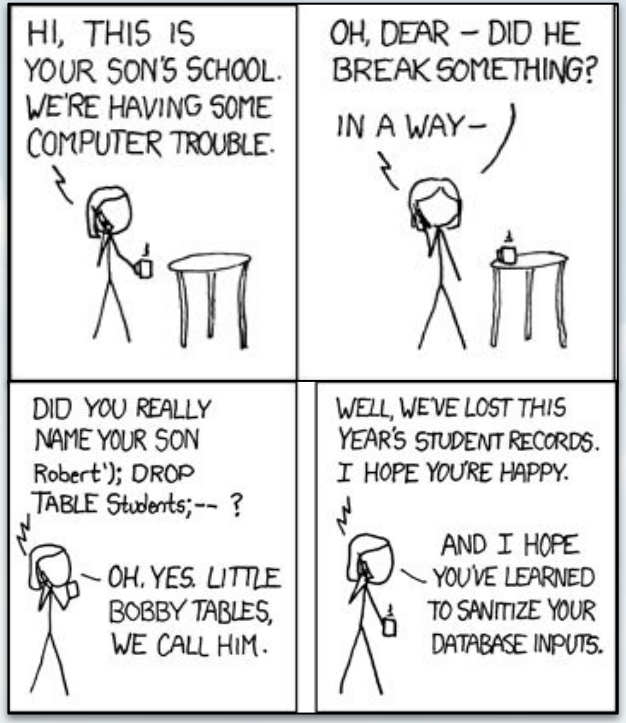
Welcome to CatShare. For cat lovers, owners, and aficionados.

Please enjoy this nice photo of a cat.



Common Website Vulnerabilities

1. Insecure Direct Object Reference (IDOR)
2. Cross Site Scripting (XSS)
3. Improper Session Handling
4. Database vulnerabilities, e.g., SQL injection

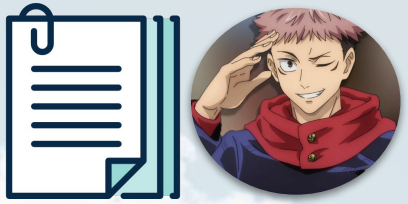


IDOR (Insecure Direct Object Reference)

Requesting resources directly from the server

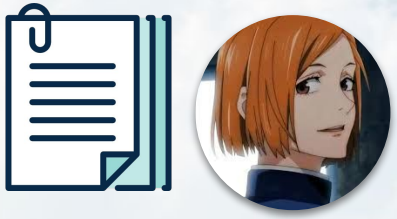
get me the records of **student 1** plz!

ofc boss, here's **Yuji Itadori**'s file



get me the records of **student 2** plz!

ofc boss, here's **Nobara Kugisaki's** file



get me the records of **my fav student** plz!

who's that again?

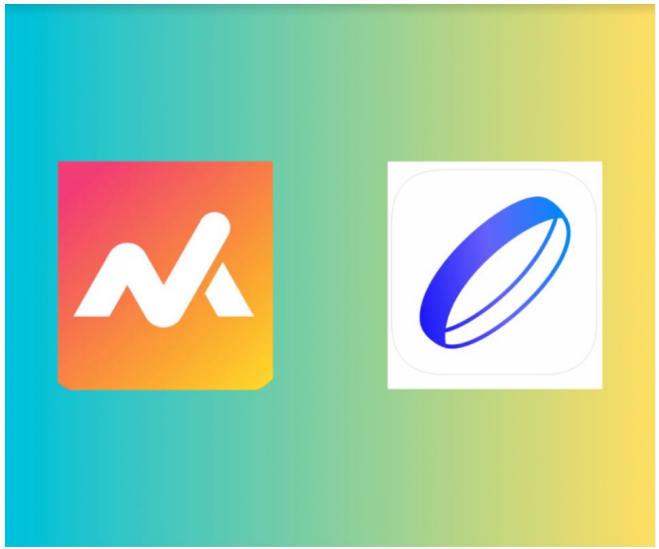
HTTP 404 Error

IDOR: Wristband (2023)

The Stanford Daily

News • Campus Life

Stanford party apps hit the scene



Mixer and Wristband both launched this year at Stanford. (Graphic: ANANYA UDAYGIRI/The Stanford Daily)

Wristband: a startup app for discovering and getting into public & private events on campus 🌲

Vulnerability disclosure, unauthorized read and write to sensitive data -- Wristband

Aditya Saligrama <saligrama@stanford.edu> Thursday, October 26, 2023 at 4:49 PM

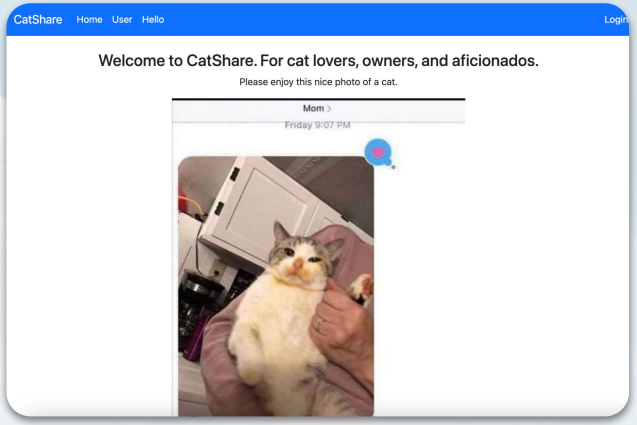
To: contact@wristband.events; +1 more

Moreover, since your event IDs are sequentially ordered, anyone can use the share URL functionality to access private events; this is an issue even if row-level security is enabled. For example, https://wristband.events/event/269 is a private event that can be accessed by enumerating event IDs starting from 1.

🎬 Hack Catshare! Round 1

- The Catshare startup has developed a website that stores personal information!

https://catshare.saligrama.io/



- There's a **new endpoint** to access this info:

https://catshare.saligrama.io/**user**

An example use case:
https://catshare.saligrama.io/**user?id=0**

- The Catshare team claims that this endpoint is secure and only accessible to admins. **Prove them wrong.**

IDOR: Stanford Marriage Pact (2020)

We told you we couldn't leave you empty handed tonight. Well, here's a gift from to thank you for your patience. A token of our gratitude, to let you know *just* how special you are.

👇 Check it out 👇

Gimme my 🔥Hot Takes🔥

Two more days until the end of Week 10—and one more day until the matches come out. When that happens, we want to help make sure as many people get matched as possible, so...

The questionnaire is open for another 7.2 hours, until 4pm PST later today. Text your friends, bug your enemies. They may not be *your* perfect match, but they could be someone else's. The bigger the pool, the better everyone's matches become.

Thanks again for your patience. We'll see you this evening for the match announcement.

Love,
The Stanford Marriage Pact

Dear Benjamin,

Matches are here! Before you slide into their DMs, a few things are worth noting:

1) Remember, this is an algorithm

An algorithm is not the hand of god. All sorts of funky things can happen with algorithms. You could get someone you know. You could get someone you don't. You could get someone you wish you didn't.

The point is, it's entirely possible to get an ex-flame, current RA, or sibling (rip, lmfao). Remember: We're talking backup plans here. Sometimes the universe has a real sense of humor.

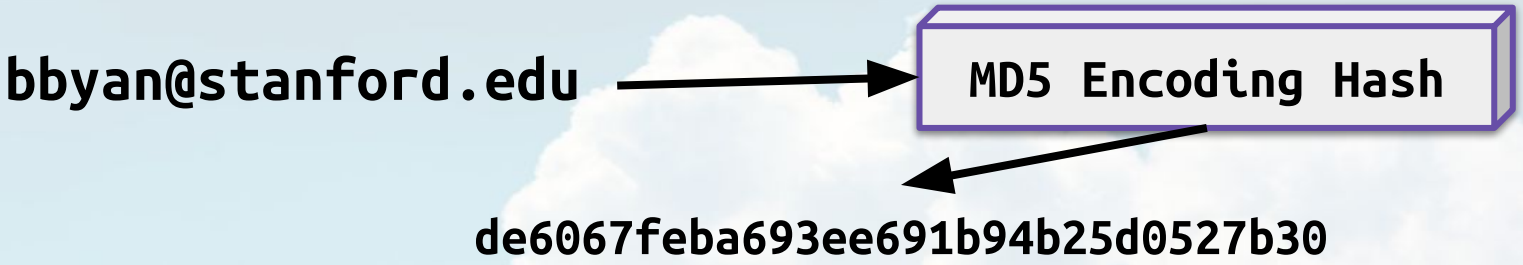
Sample Question: I believe in star signs ♐

1	2	3	4	5	6	7

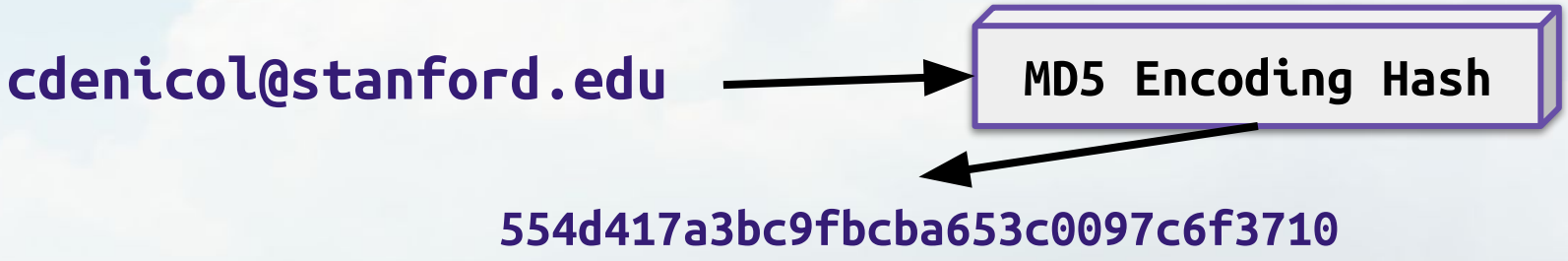
Strongly disagree — Neutral — Strongly agree

IDOR: Stanford Marriage Pact (2020)

Ben Yan https://mp.com/**de6067feba693ee691b94b25d0527b30**



Cooper de Nicola https://mp.com/**554d417a3bc9fbcba653c0097c6f3710**



Avoiding IDOR Attacks

- Ensure that a user is **allowed to access a resource** before returning it
- When this isn't possible (e.g., cloud storage buckets), **make resource URIs random and unpredictable.** Avoid:
  - Automatically incrementing resource IDs (e.g., Wristband)
  - Hashing a **guessable property** like name, phone number, username, email (e.g., Marriage Pact)

Use **random identifiers** such as globally unique 128-bit UUIDs

XSS Attacks

- XSS stands for **Cross Site Scripting**
- XSS is a potentially dangerous attack that enables hackers to take over your website to **run JavaScript code** on other users' browsers
- This typically occurs when **user input is not properly sanitized and displayed**, allowing it to execute as code

```
https://innocent.website/myfeed?id=<script>alert("you got hacked!")</script>
```

XSS Diagram

Heyo click on this reel I just sent you :)

https://website.com

Your Explore Page:

You got hacked!

GET /myfeed

```
<html>
<body>

<b>Your Explore Page:</b>
<script>
     alert("you got hacked!")
</script>

</body>
</html>
```

Reflected XSS

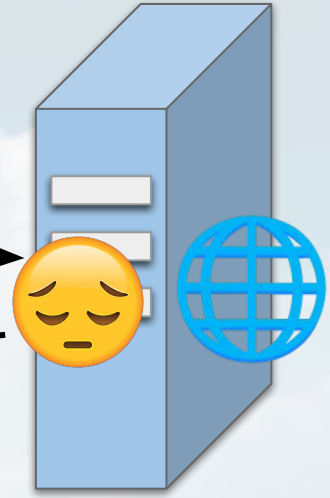
Heyo click on this reel I just sent you :)

https://website.com

Bad code sent as text

Bad code runs in the browser

The malicious code gets **reflected by the server** back to the user



https://vulnerable.website/search?q=<script>alert(“get rekt!”)</script>

Stored XSS

imma troll the database

website.com

Bad code sent as text

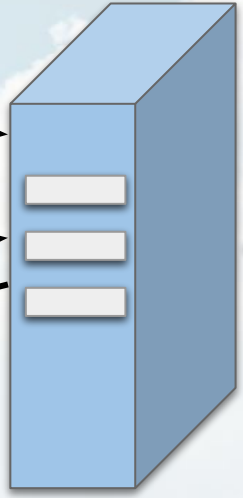
The malicious code gets sent and **stored in the database**

website.com

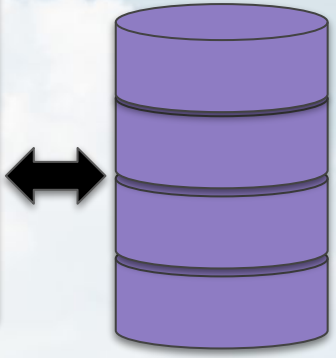
Just a regular request…

Bad code runs in browser

The server gets things from the database, and it'll **send over the malicious code**



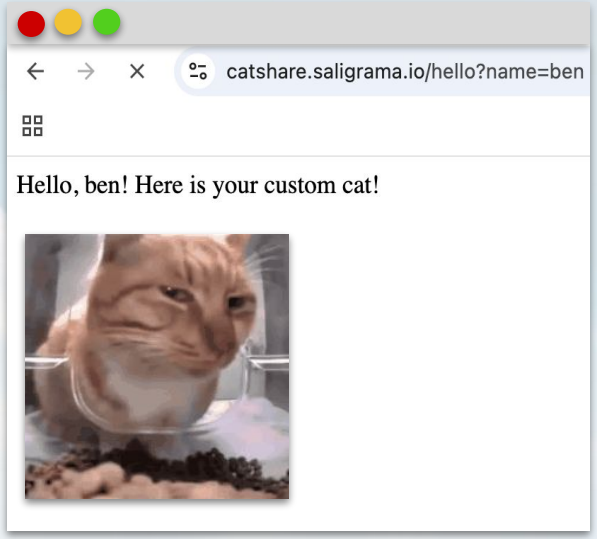
Server



Database

🎬 Hack Catshare! Round 2

- After the previous data breach, Catshare's valuation fell by 400 meows. Not good.
- As recompense, the Catshare startup wants to make its customers feel welcome again. They've added a **new endpoint** that takes a user's name and greets them :)

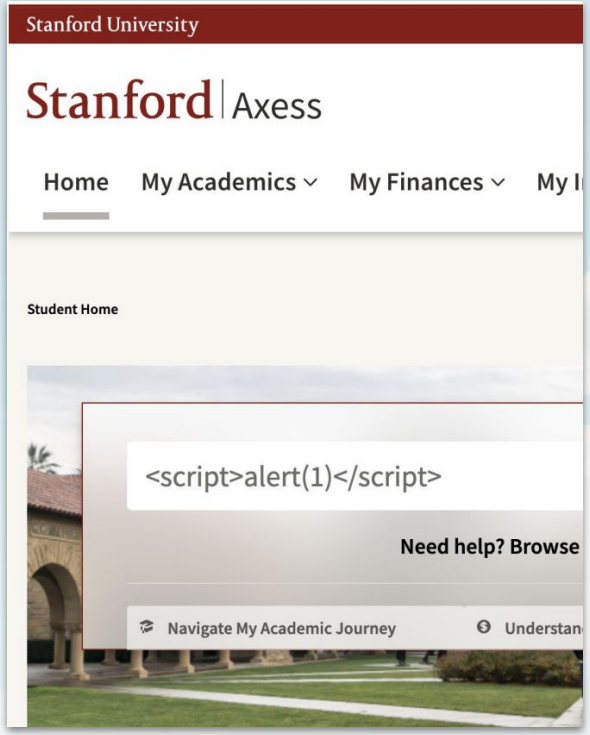


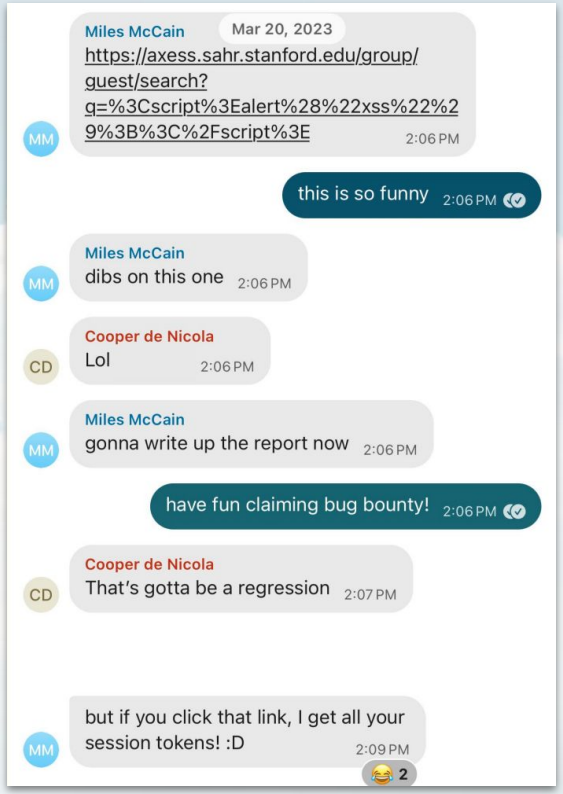
https://catshare.saligrama.io/**hello**

An example use case:
https://catshare.saligrama.io/**hello?name=ben**

- The Catshare team thinks this is harmless cheer and will restore customer faith in their business. **Prove them wrong :(**

XSS: Stanford Axess (2023)





Miles & company found and disclosed an XSS vulnerability in Axess (March 2023)

Awarded **$1000** by the **Stanford Bug Bounty**

Remediated Jan. 2024

The possibilities could be nightmarish

When your friend has the last spot in Social Dance 💃:

```
www.axess.stanford.edu/<?unenroll-in-social-dance-muahaha.js>/
```

Yeah this is kinda bad:

```
www.myfinances.stanford.edu/<?steal-all-the-money.js>/
```

for legal reasons, Stanford, this is a joke

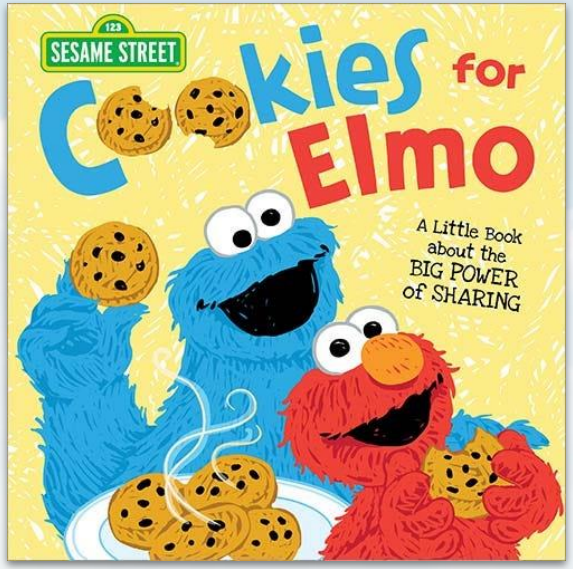
Cookies: Improper Session Handling

Cookie itself is insecure

- Can **modify cookie** to access another's account, e.g., become admin

Cookie not checked for authorization

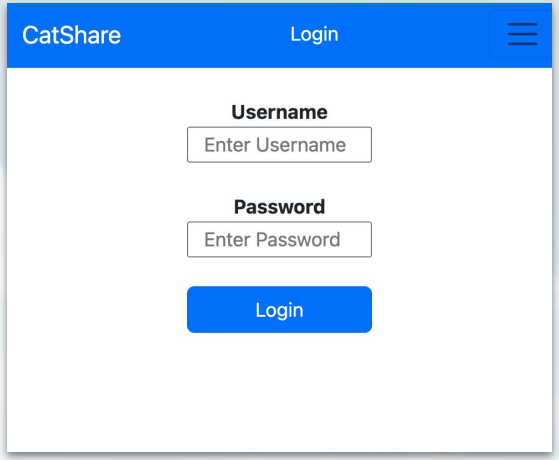
- Use **your own account** to:
  - Impersonate someone else
  - Ascend privileges to admin



Hack Catshare! Final Round

- Seeking to rectify the user data privacy issue, Catshare has built an **admin-only view** to look at user data, at the new endpoint below.

`https://catshare.saligrama.io/login`

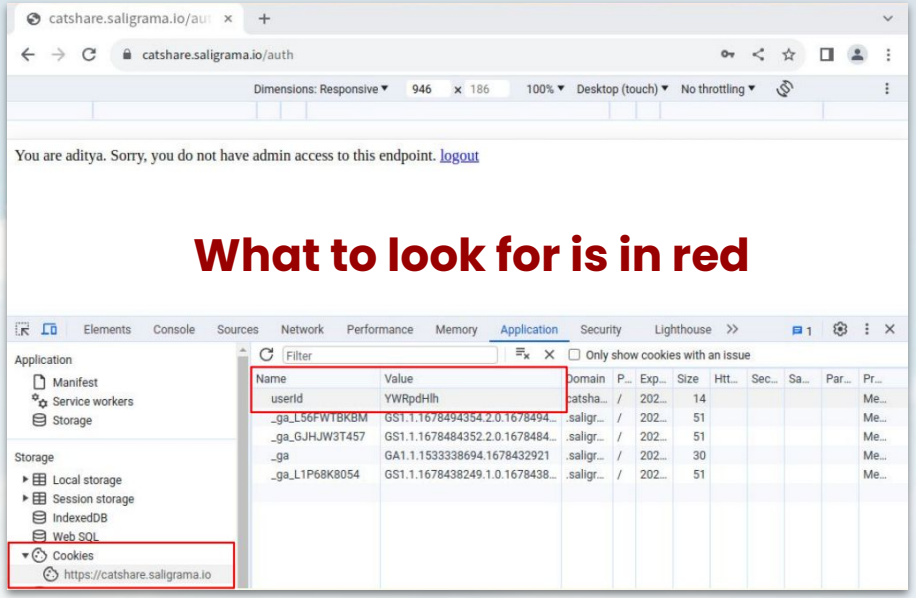


- First, log in using:
  - *Username*: **stanford**
  - *Password*: **stanford**

- **Can you become admin** and view the user data?

Tools & Reference Guide

- To access cookies, go to browser's Developer Tools (**Inspect Element** / Console -> **Application** tab -> then **Cookies** under Storage)
- Cookies are in **Base64** format
  - Transforms data into a mix of letters and numbers
  - Doesn't actually encrypt or secure the data, just a **different way to present it**
- Use **https://kk.lol** to encode and decode



https://catshare.saligrama.io/**login**

Try **stanford:stanford** first

Avoiding Improper Session Handling

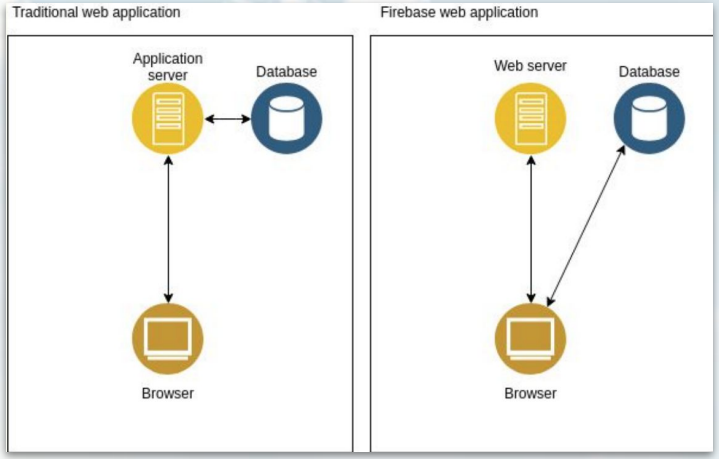
Before taking a sensitive action:

- Check the user **is who they say they are**
- And that they are **allowed to perform the action**

Database Vulnerabilities: Firebase

Clients can **directly access the database (including malicious clients!)**

- Database is in charge of validating user access to data
- Poor validation (e.g., misconfigured rules) → **unauthorized data access**



Firebase Vulnerabilities: Fizz (2021)

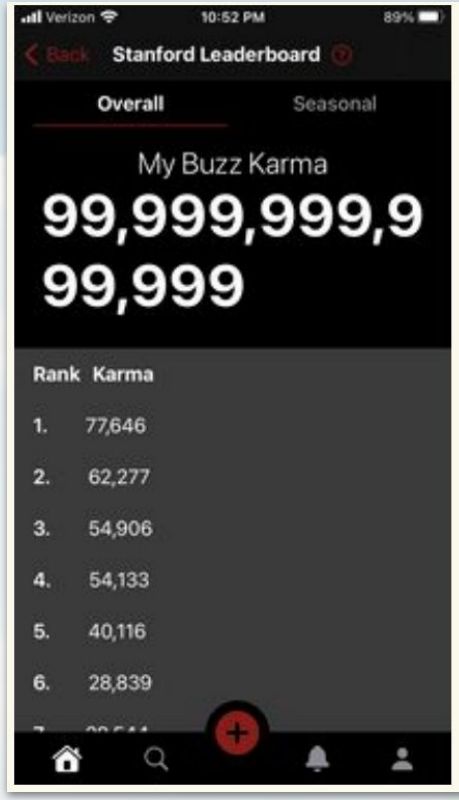
Opinions

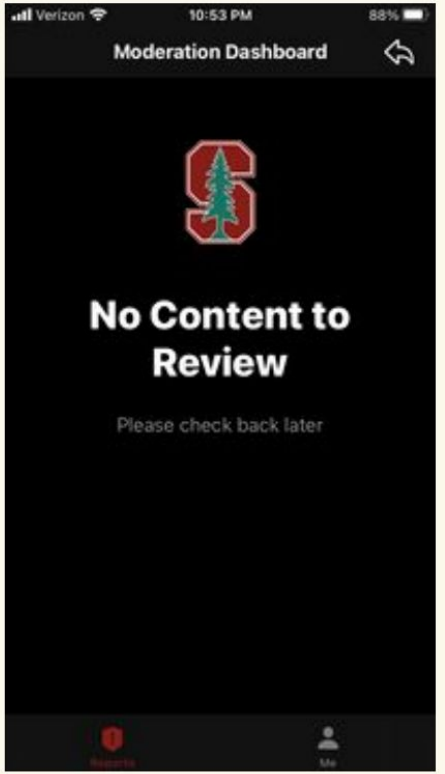
Opinion | Fizz previously compromised its users' privacy. It may do so again.

Fizz had a large data vulnerability discovered last fall. Their response raises questions about the app today.
(Graphic: JOYCE CHEN/The Stanford Daily)

Opinion by Joyce Chen
Nov. 1, 2022, 10:00 p.m.

Firebase Vulnerabilities: Fizz (2021)





Firebase Vulnerabilities: Fizz (2021)

"At the time, Fizz used Google's Firestore database product to store data including user information and posts. Firestore can be configured to use a set of security rules in order to prevent users from accessing data they should not have access to. However, **Fizz did not have the necessary security rules set up, making it possible for anyone to query the database directly and access a significant amount of sensitive user data.**

We found that **phone numbers and/or email addresses for all users were fully accessible**, and that posts and upvotes were directly linkable to this identifiable information. **It was possible to identify the author of any post on the platform.**

Moreover, the database was entirely editable — **it was possible for anyone to edit posts, karma values, moderator status**, and so on. Having moderator status granted access to a dashboard that provided the ability to delete arbitrary posts."

Potential Legal Consequences to Ethical Hacking

November 22, 2021

[redacted]

Via E-Mail

Cooper Barry deNicola [redacted]
Miles McCain [redacted]
Aditya Saligrama [redacted]

Re: Buzz Vulnerability Disclosure

To: Cooper de Nicola, Miles McCain and Aditya Saligrama

Hopkins & Carley represents The Buzz Media Corp. ("Buzz"). We write regarding your team of security researchers, both individually and collectively (referred to herein as the "Group") to make you aware of the Group's criminal and civil liability arising out of the Group's unauthorized access to Buzz's systems and databases.

Based on your own admissions in your email dated November 9, 2021 notifying Buzz of the security vulnerability, the Group explored "*…the vulnerability…*" and obtained unauthorized access to Buzz's "*…complete databases…*" and all information stored in Buzz's database. Your email further goes on to state that the Group edited user tables and created moderator and administrator accounts enabling the Group to access Buzz's systems without authorization.

The Group's actions in obtaining this unauthorized access to Buzz's databases violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030) (CFAA), the Digital Millennium Copyright Act (DMCA) and Buzz's Terms of Use.

The Group circumvented Buzz's technological measures designed to protect Buzz's databases, without any permission or authority in violation of the DMCA. For these violations of the DMCA the Group may be liable for fines, damages and each individual of the Group may be imprisoned. Further, the Computer Fraud and Abuse Act (18 U.S.C. § 1030) (CFAA) imposes additional criminal and civil liability for unauthorized access to a protected computer, including accessing files or databases to which one is not authorized to access. The CFAA prohibits intentionally accessing a protected computer, without authorization or by exceeding authorized access, and obtaining information from a protected computer. Criminal penalties under the CFAA can be up to 20 years depending on circumstances.

Buzz's own Terms of Use expressly prohibits any of the following actions and clearly sets forth that the Group has no authorization to access Buzz's systems or databases "*…attempt to reverse engineer any aspect of the Services or do anything that might circumvent measures employed to prevent or limit access to any area, content or code of the Services (except as otherwise expressly permitted by law); Use or attempt to use another's account without authorization from such user and Buzz; Use any automated means or interface not provided by Buzz to access the Services;…*" Not only then are the Group's actions a violation of both the DMCA and the CFAA, as indicated above, the Group's actions are also a violation of Buzz's Terms of Use and constitute a breach of contract, entitling Buzz to compensatory damages and damages for lost revenue.

When your classmates threaten you with felony charges
Aug 28, 2023

Portfolio
Posts
Letter

A few weeks ago, I was part of a talk at DEF CON 31 called The Hackers, The Lawyers, and the Defense Fund. I was asked to share my experience receiving a legal threat for good-faith security research from my classmates.

This story has been told before (e.g., by my friend Aditya who was also involved and by the Stanford Daily), but I wanted to share my talk here for posterity.

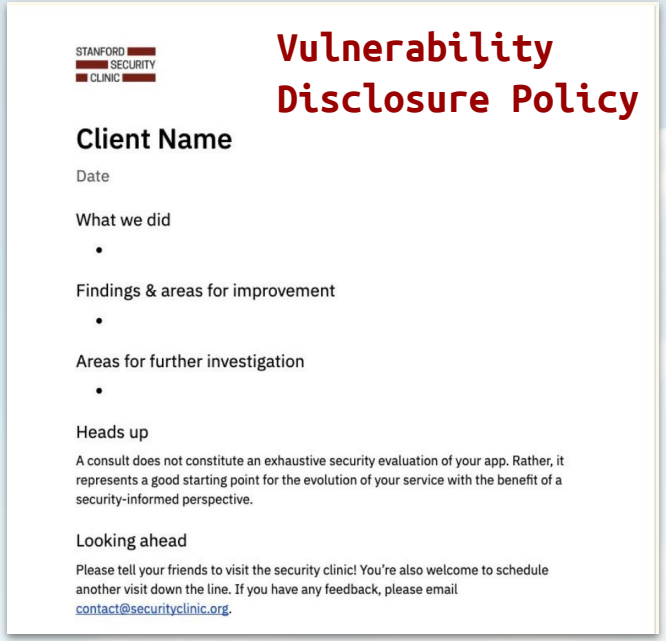
The following is an approximate transcript. (If the language feels terse, that's why.) I've added a few links and cleaned up some of the language for clarity.

https://miles.land/posts/classmates-legal-threat-fizz-defcon/

Nothing is 100% secure, but that isn't a reason not to build!

Vulnerabilities happen to the best

The community can help!



STANFORD SECURITY CLINIC

Vulnerability Disclosure Policy

Client Name

Date

What we did

•

Findings & areas for improvement

•

Areas for further investigation

•

Heads up

A consult does not constitute an exhaustive security evaluation of your app. Rather, it represents a good starting point for the evolution of your service with the benefit of a security-informed perspective.

Looking ahead

Please tell your friends to visit the security clinic! You're also welcome to schedule another visit down the line. If you have any feedback, please email contact@securityclinic.org.

Disclosing vulnerabilities ethically!

http://securityclinic.org

Bug Bounty programs incentivize responsible disclosures of security vulnerability (often with a monetary reward)

Further Resources

- 🐈📷 **CATSHARE** (Aditya Saligrama, Cooper de Nicola, George Hosono) & accompanying source code:
  - https://github.com/saligrama/catshare-serverless

- **Security / cybersecurity courses** at Stanford
  - INTLPOL 268: Hack Lab
  - CS 155: Computer & Network Security
  - CS 152: Trust & Safety Engineering
  - CS 255: Cryptography
  - CS 40: Cloud Infrastructure & Scalable App Deployment

- **Stanford Applied Cyber**, Stanford Security Clinic

Announcement from Haas Center to CS106S

Summer Undergraduate / Cardinal Quarter Fellowships

If you are interested in continuing your learning around your CS coursework consider a stipended Haas Center Undergraduate Fellowship this summer. There's a wide range of funding available, but some fellowships that might be of interest given your enrollment in this course are the Haas Center Undergraduate Fellowships, Public Service Projects Fellowship, CS+Social Good Fellowship, Social E Fellowship and the Roland Longevity Fellowship.

Each Cardinal Quarter Fellow receives a base stipend of $7000 to support travel and living expenses for a nine-week, full-time experience. Financial aid and supplemental funding, including a travel supplement and high cost of living supplement, is available to students who qualify. Cardinal Quarter programs are offered through 30+ campus partners, offering a wide range of service experiences.

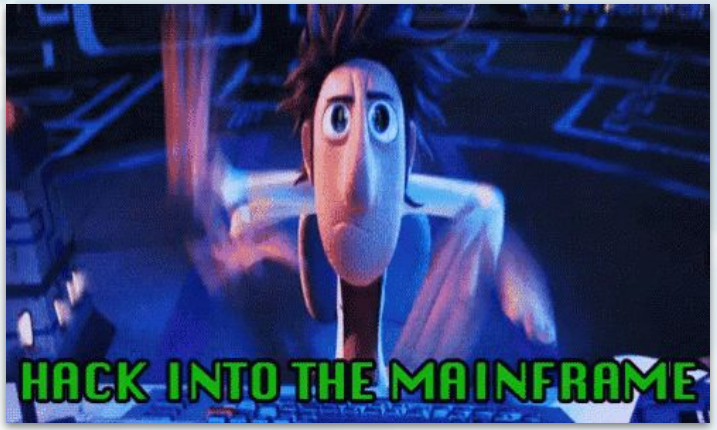
The application deadline for most fellowships is February 4, 11:59pm, PST. Please reach out to a Cardinal Quarter Peer Advisor or email cardinalquarter@stanford.edu with any questions.

Check-Off Form!

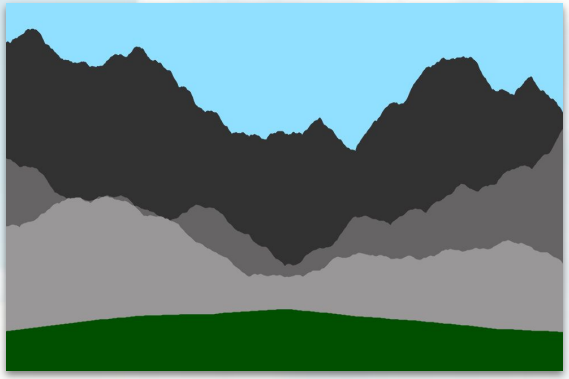
Another **brief check-off form** (<5 min to complete) for feedback and checking attendance!

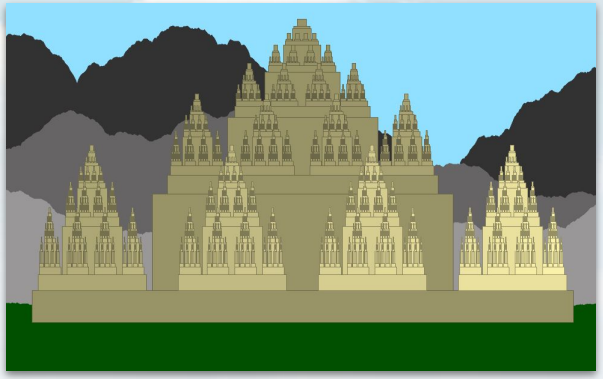
For today, click the "Check-Off Form" link in the **Week 5** section of **cs106s.stanford.edu.**

Thank you!



Have an awesome week, and good luck on any midterms! 🍀





You’re doing to do awesome by doing awesome