Ethical Web Hacking for Fun and (maybe) Profit

whoami

Aditya Saligrama

https://saligrama.io

- Stanford ‘24, MS ‘25 (Computer Science)
- Cybersecurity nerd since ‘21
- I help startups with their security issues
- I’m a course assistant for CS 155 on security
- I taught a course on cloud computing! (CS 40)

CYBER @ SECURITY

STANFORD SECURITY CLINIC

Why care about security?

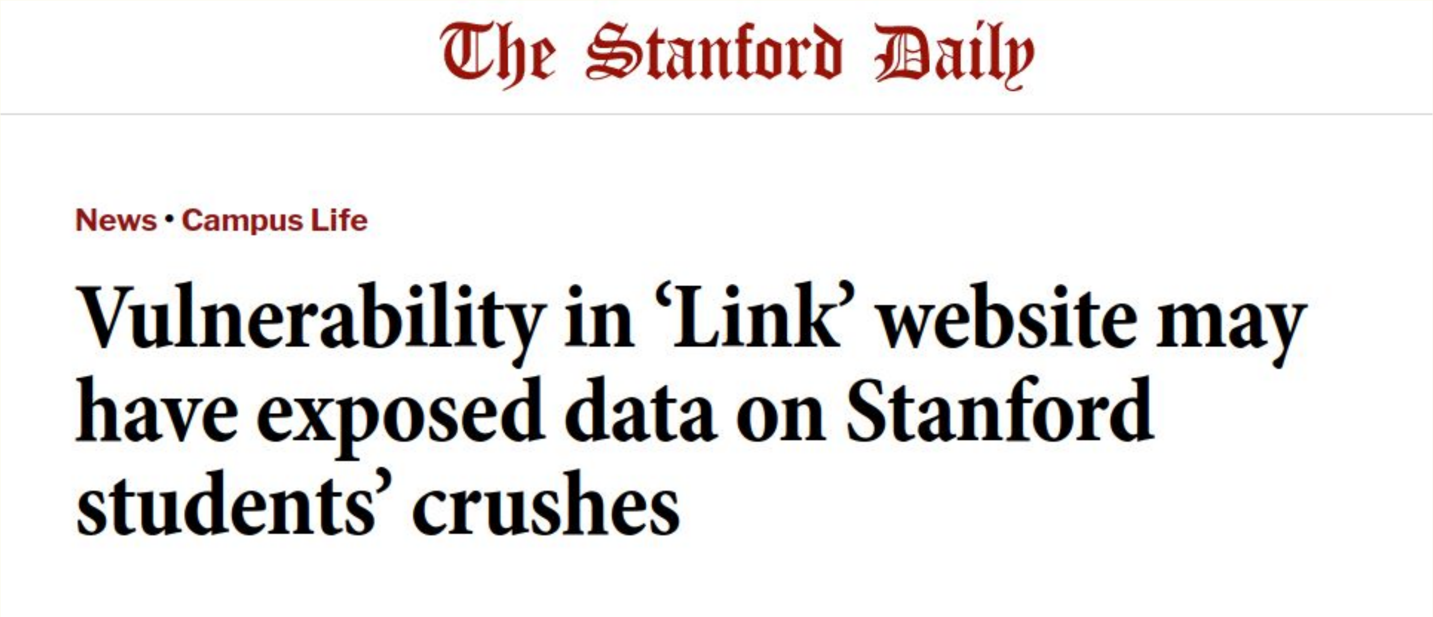
Case study: Stanford Link (2020)

- *Match with your crush if they like you back*
- *Website keeps you anonymous if they don’t*

Case study: Stanford Link (2020)

- *Match with your crush if they like you back*
- *Website keeps you anonymous if they don’t*
- ***What could go wrong?***

Case study: Stanford Link (2020)

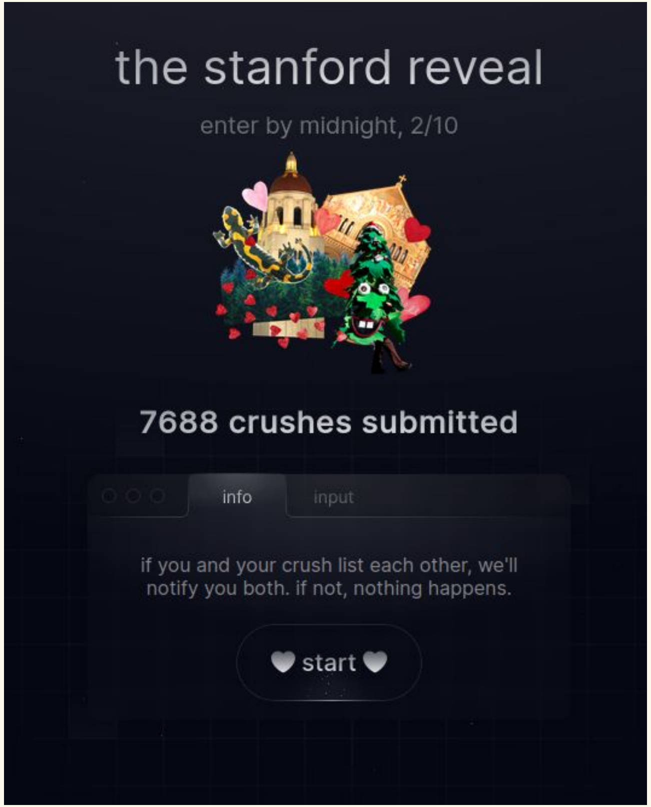


The Stanford Daily

News • Campus Life

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

What’s old is new again: Stanford Reveal (2023)

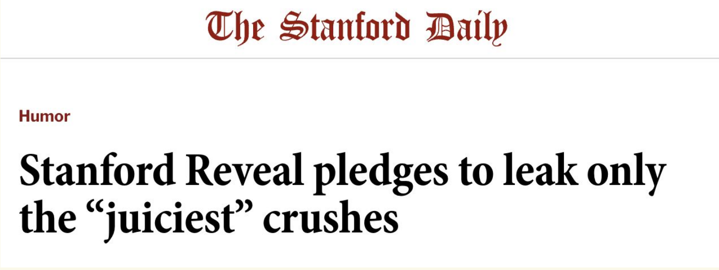


the stanford reveal

enter by midnight, 2/10

7688 crushes submitted

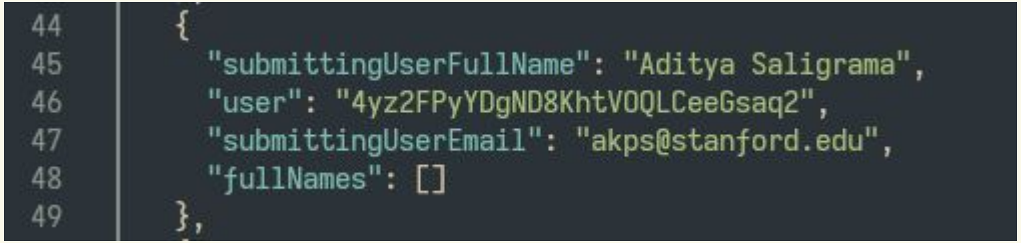
if you and your crush list each other, we'll notify you both. if not, nothing happens.



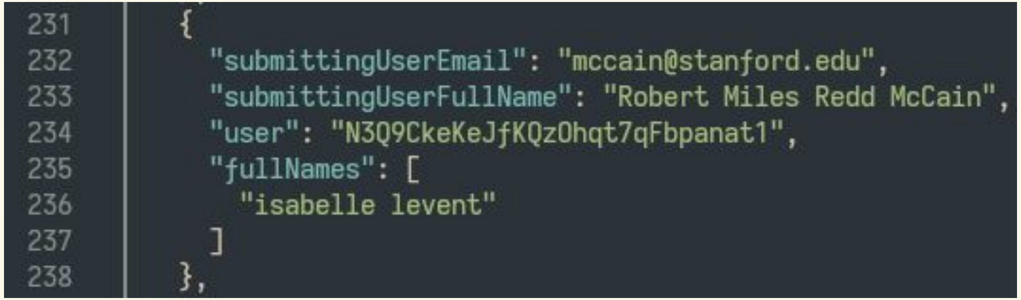
The Stanford Daily

Humor

Stanford Reveal pledges to leak only the “juiciest” crushes



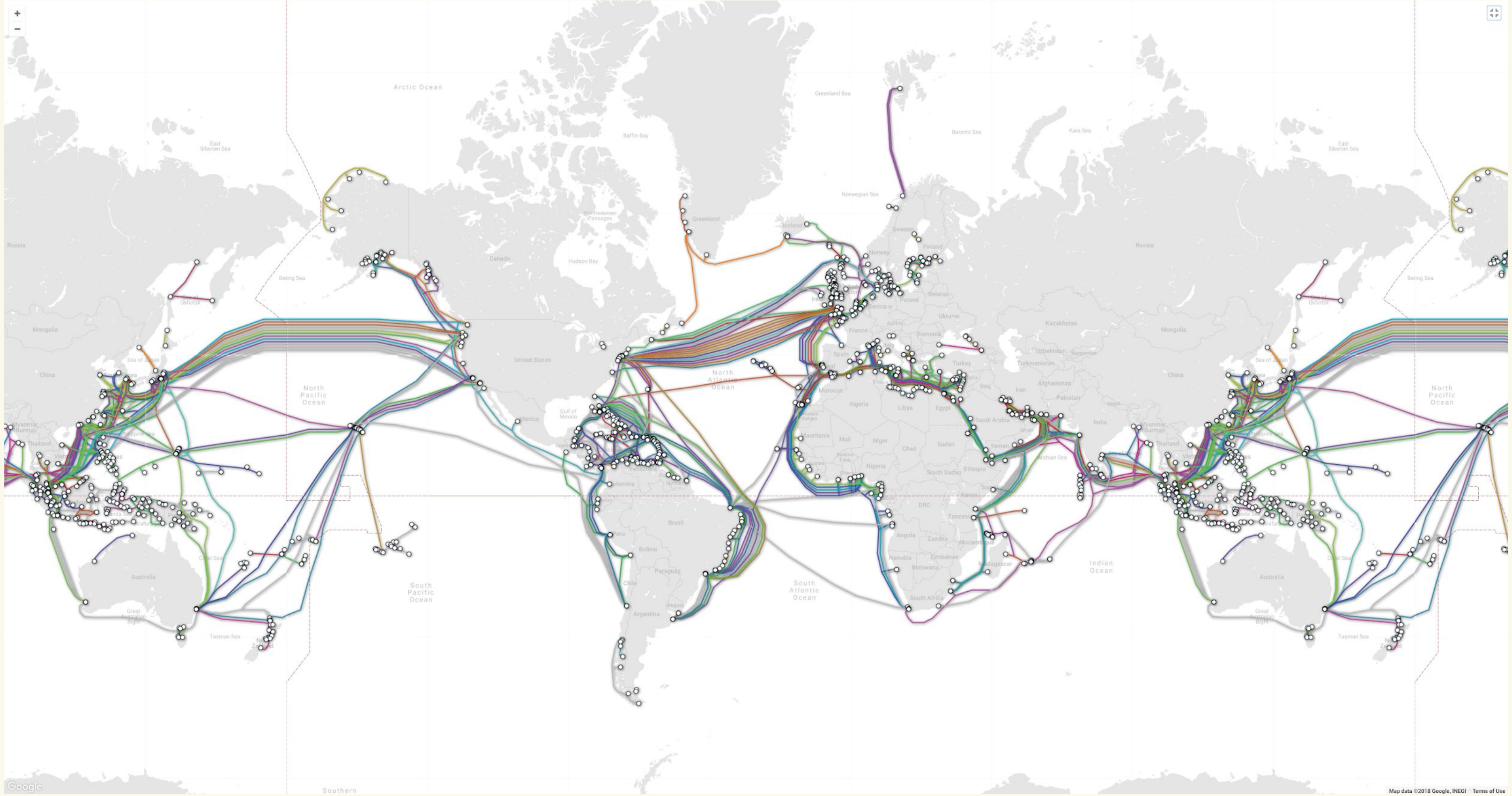
```
  {
    "submittingUserFullName": "Aditya Saligrama",
    "user": "4yz2FPyYDgND8KhtVOQLCeeGsaq2",
    "submittingUserEmail": "akps@stanford.edu",
    "fullNames": []
  },
```



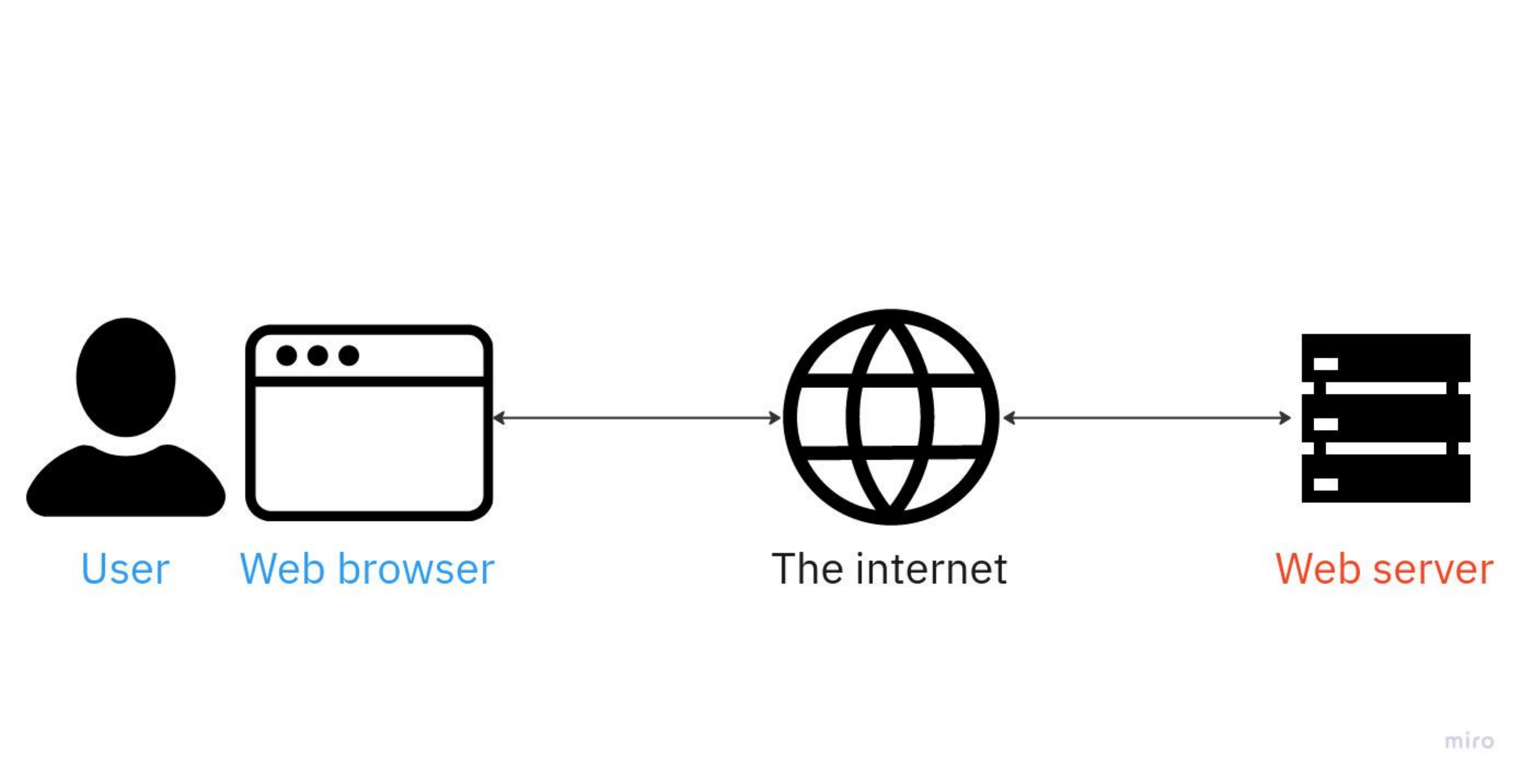
```
  {
    "submittingUserEmail": "mccain@stanford.edu",
    "submittingUserFullName": "Robert Miles Redd McCain",
    "user": "N3Q9CkeKeJfKQzOhqt7qFbpanat1",
    "fullNames": [
      "isabelle levent"
    ]
  },
```

The fastest web crash course ever

How does the Internet work?



Our Internet Abstraction



What language does the web speak?

```
<body style="
<div i
<h
```

```
<link rel="stylesheet" href="http://localhost/css.css" type="text/css" />
<script type="text/javascript" src="http://localhost/javascript.js"></script>
<script type="text/javascript">
  (function(){
    onLoaded: function(request) {
      if (request.name == 'log_error') return;
      log.trace("Ajax.Request: " + (request.name || request.url.substr(0, 30
        )) + "...");
    },
    onComplete: function(request) {
      if (request.name == 'log_error') return;
    },
    onException: function(request, e) {
      if (request.name == 'log_error') return;
      log.fatal(request.url + ' : ' + e.name + ' | ' + e.message + ' | ' +
        .stack);
```

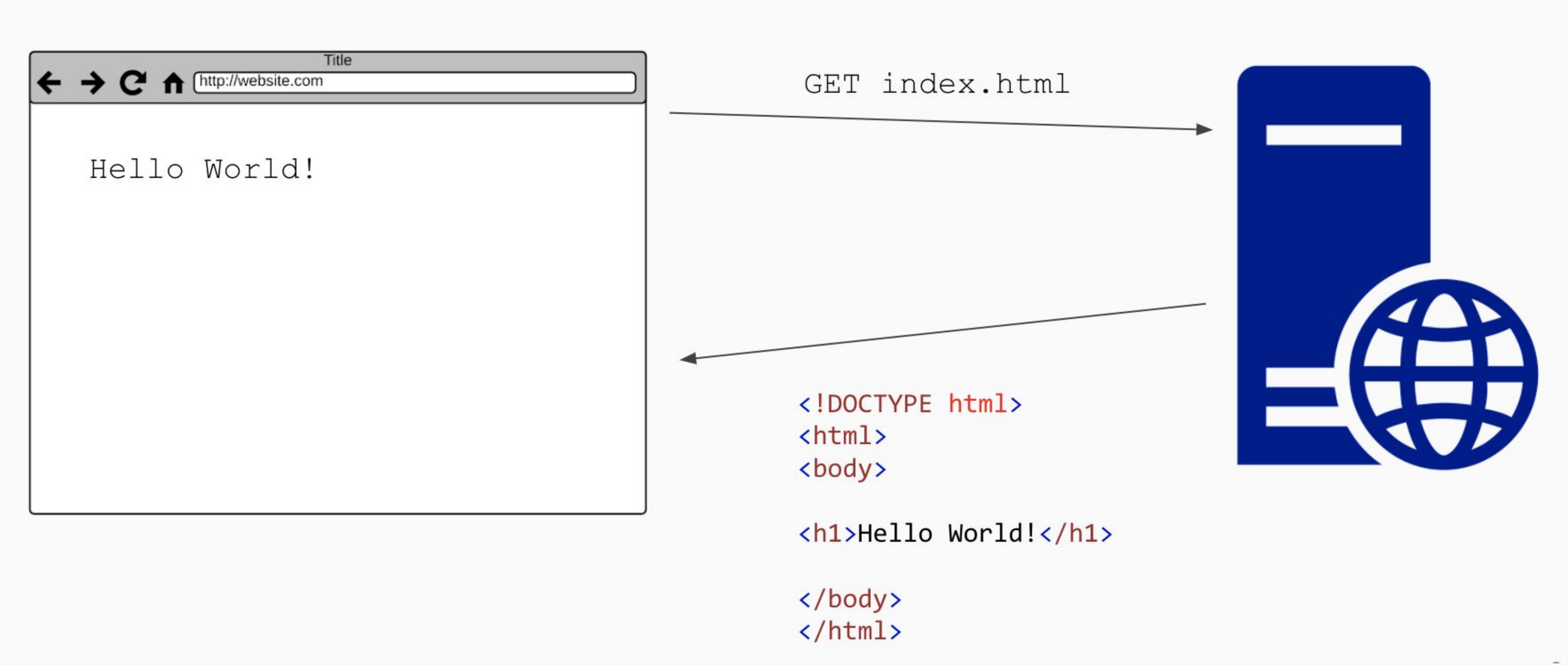
```
.screen-reader-text:hover,
.screen-reader-text:active,
.screen-reader-text:focus {
    background-color: #f1f1f1;
0, 0, 0.6);
lbar. */
```

How do we communicate with a web server?

HTTP

Hypertext Transport Protocol

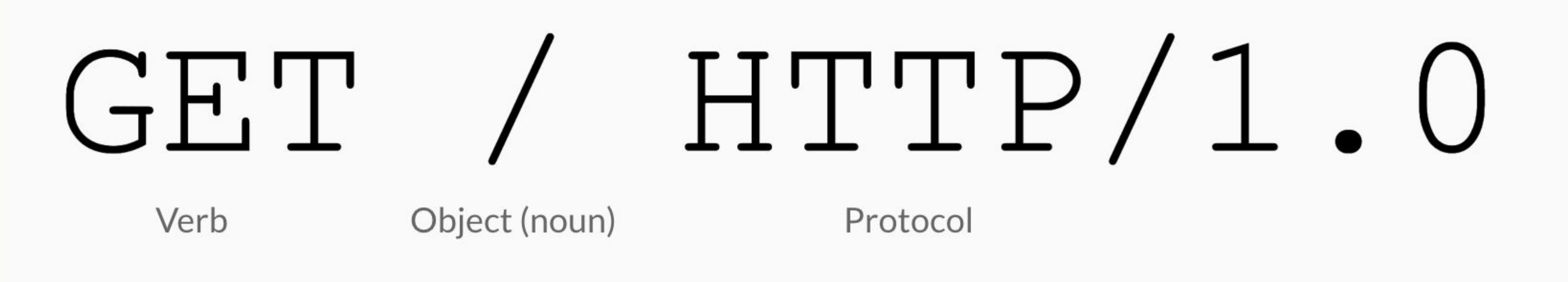
HTTP: the missing language of the web



```
GET index.html
```

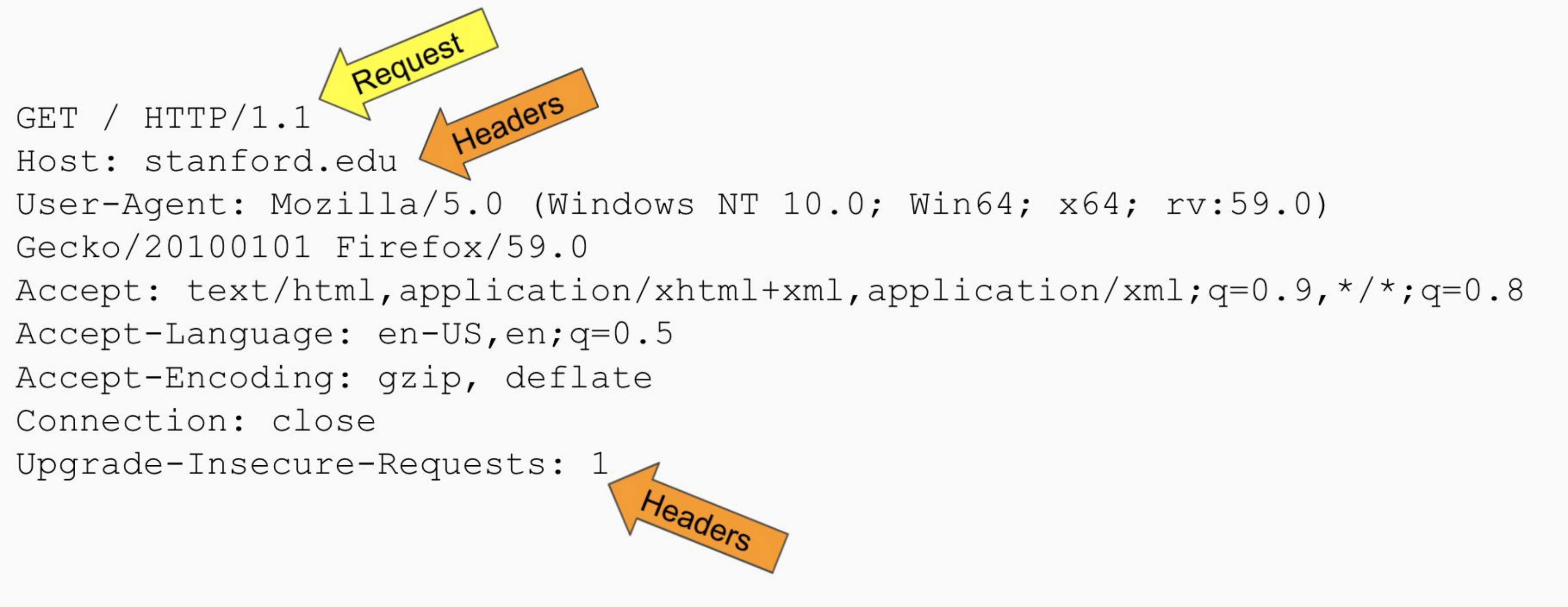
```
<!DOCTYPE html>
<html>
<body>

<h1>Hello World!</h1>

</body>
</html>
```

HTTP protocol



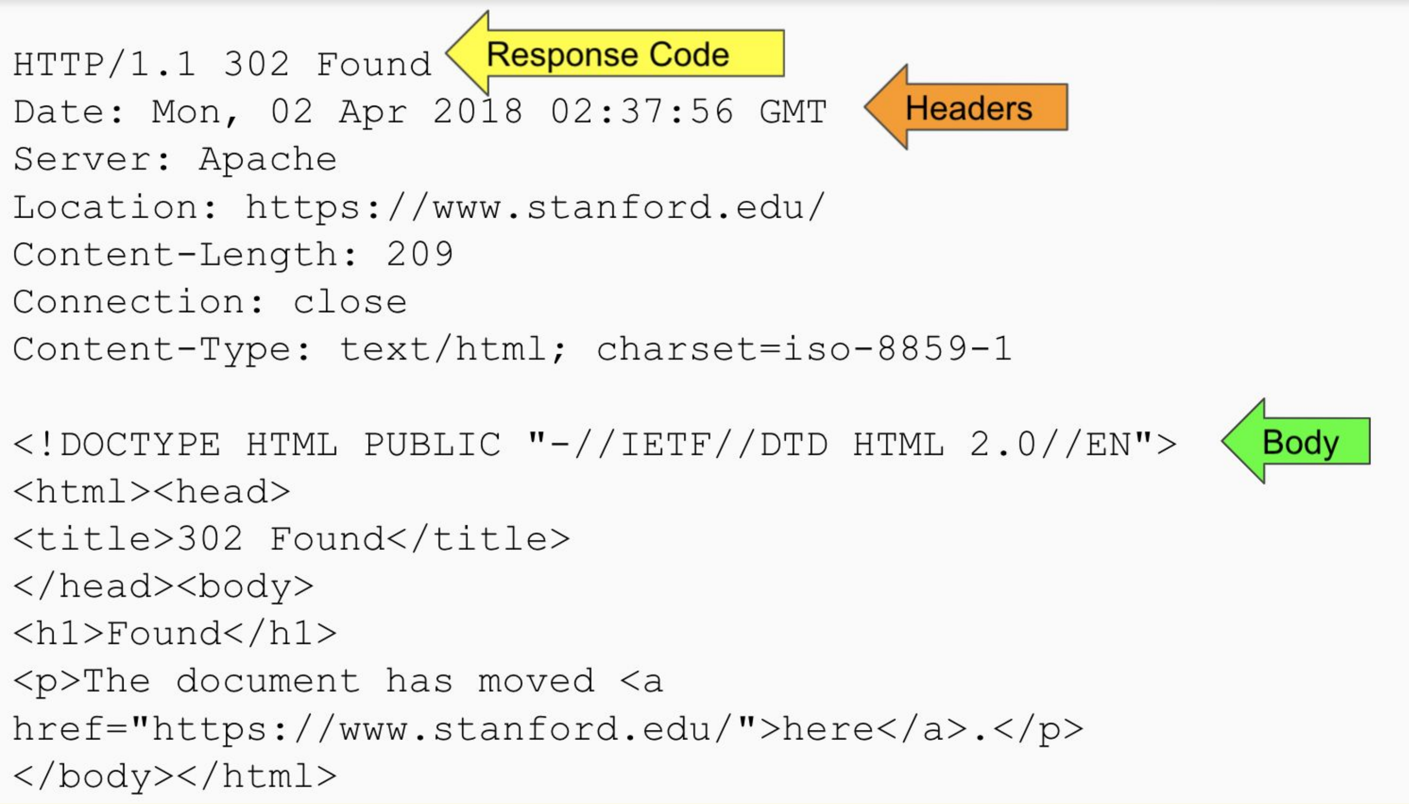
```
GET / HTTP/1.0
```

HTTP requests



```
GET / HTTP/1.1
Host: stanford.edu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

HTTP responses



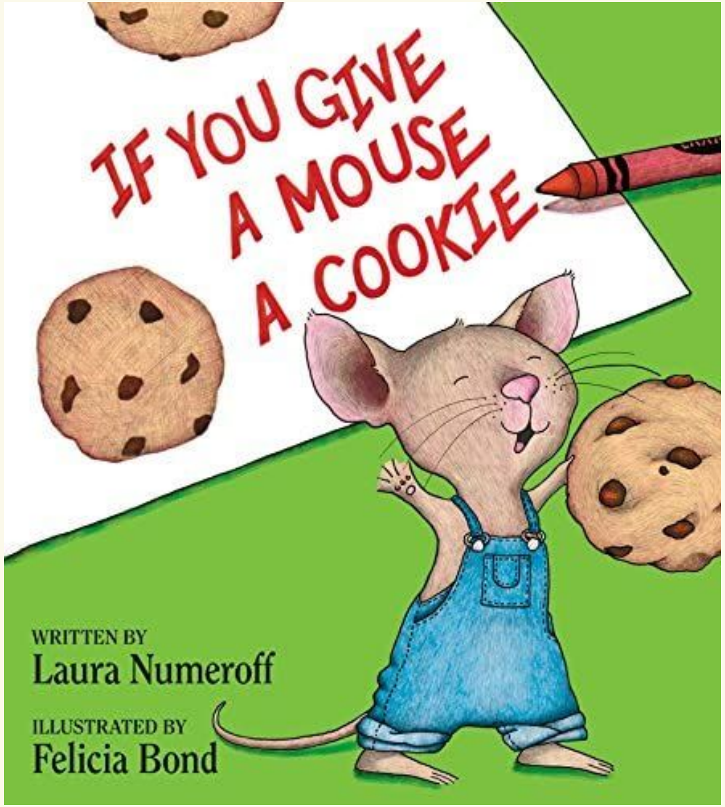
```
HTTP/1.1 302 Found
Date: Mon, 02 Apr 2018 02:37:56 GMT
Server: Apache
Location: https://www.stanford.edu/
Content-Length: 209
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a
href="https://www.stanford.edu/">here</a>.</p>
</body></html>
```

HTTP requests: GET and POST

- **GET**: Requests a specified resource
    - Should only retrieve data, without changing server state

- **POST**: Submits data to the specified resource
    - Often causes changes in state or side effects on the server

Session handling: how does a website remember?



- **Cookies** enable web servers to store stateful information in your browser

- *Authentication cookies* are used to authenticate that a user is logged in, and with which account
  - On login: **`Set-Cookie: session=session-id`**
  - Future requests: **`Cookie: session=session-id`**

Demo: browser developer tools

Common insecure design patterns

CatShare

https://catshare.saligrama.io

We're a real startup!

October 14, 2022

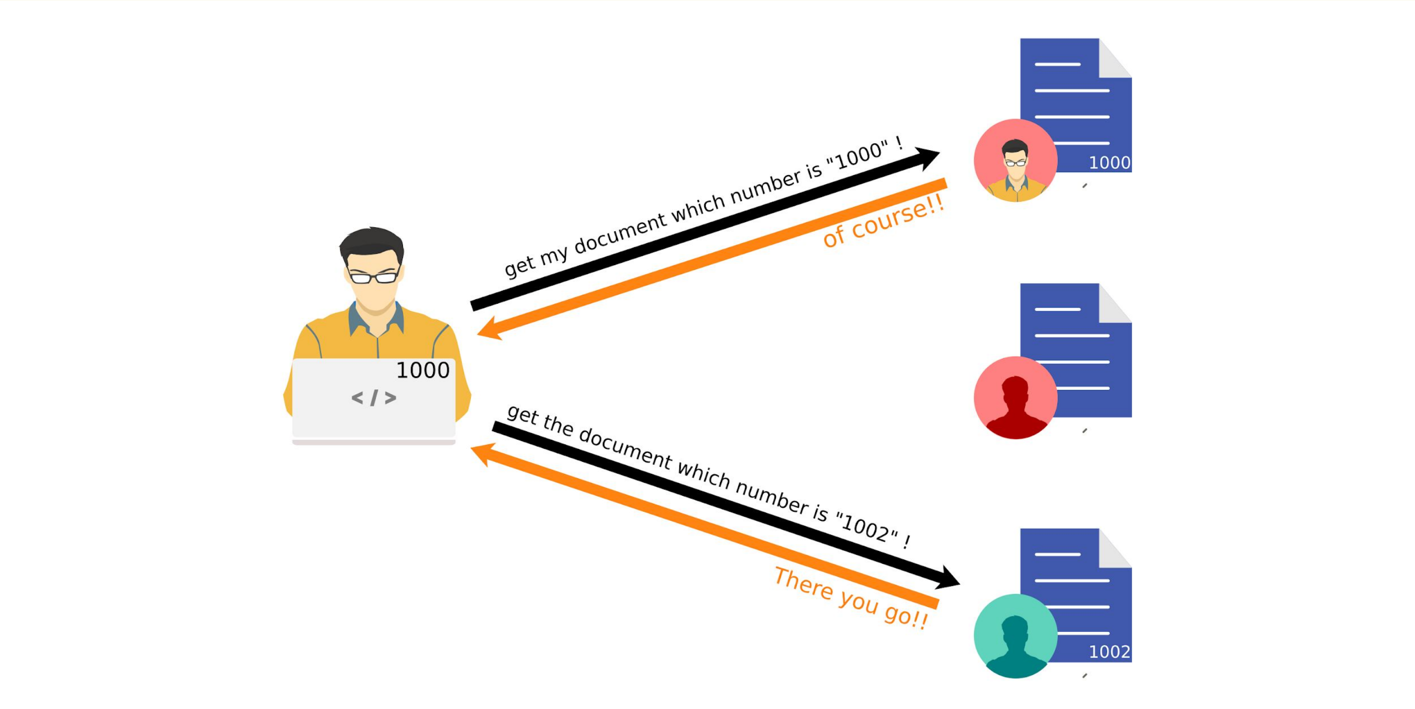
Vulnerabilities

- Insecure Direct Object Reference (IDOR)
- Cross Site Scripting (XSS)
- Improper Session Handling
- Database vulnerabilities: Firebase and SQL Injection

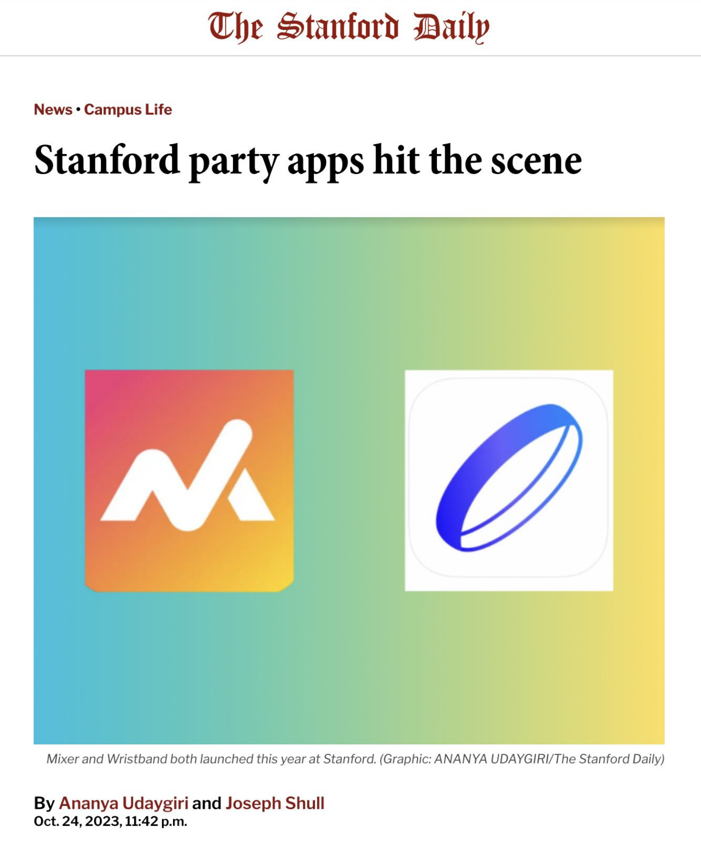
Insecure Direct Object Reference

Insecure Direct Object Reference (IDOR)

Or: asking the server for the resources you want


get my document which number is "1000" !
of course!!
1000
1000
get the document which number is "1002" !
There you go!!
1002

IDOR case study I: Wristband (2023)



The Stanford Daily

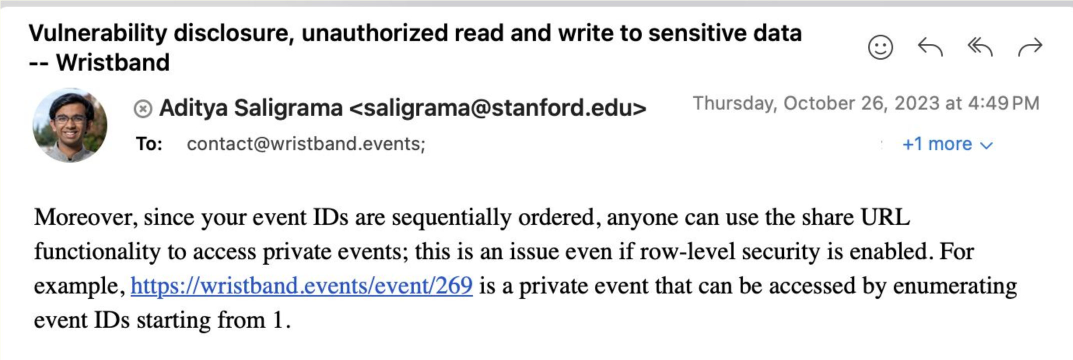
News • Campus Life

Stanford party apps hit the scene

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

By Ananya Udaygiri and Joseph Shull
Oct. 24, 2023, 11:42 p.m.

Wristband: an app for finding and getting into public and private events



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.

TRY IT!

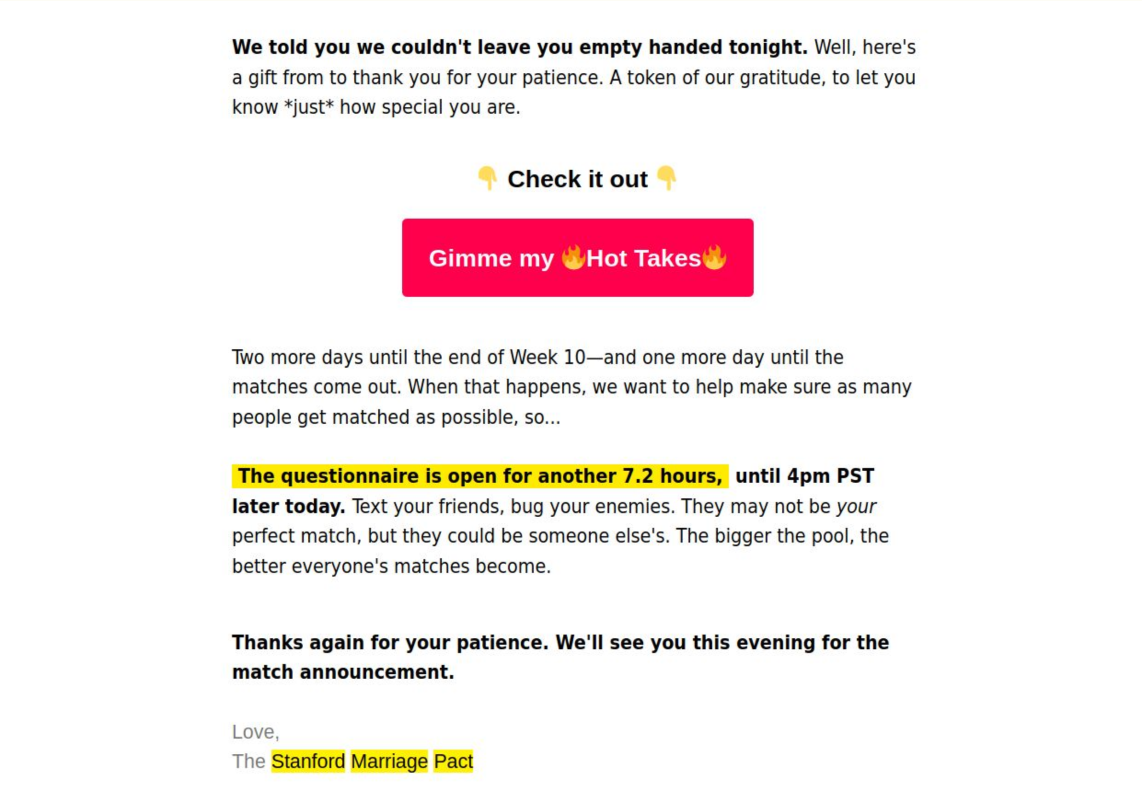
- The CatShare team has a website https://catshare.saligrama.io/ that **stores personal information**

- There's an endpoint https://catshare.saligrama.io/user to access this info
    - e.g. https://catshare.saligrama.io/user?id=0

- CatShare claims this is secure and only accessible to admins

- **Prove CatShare wrong**

IDOR case study II: 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** 👇

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...

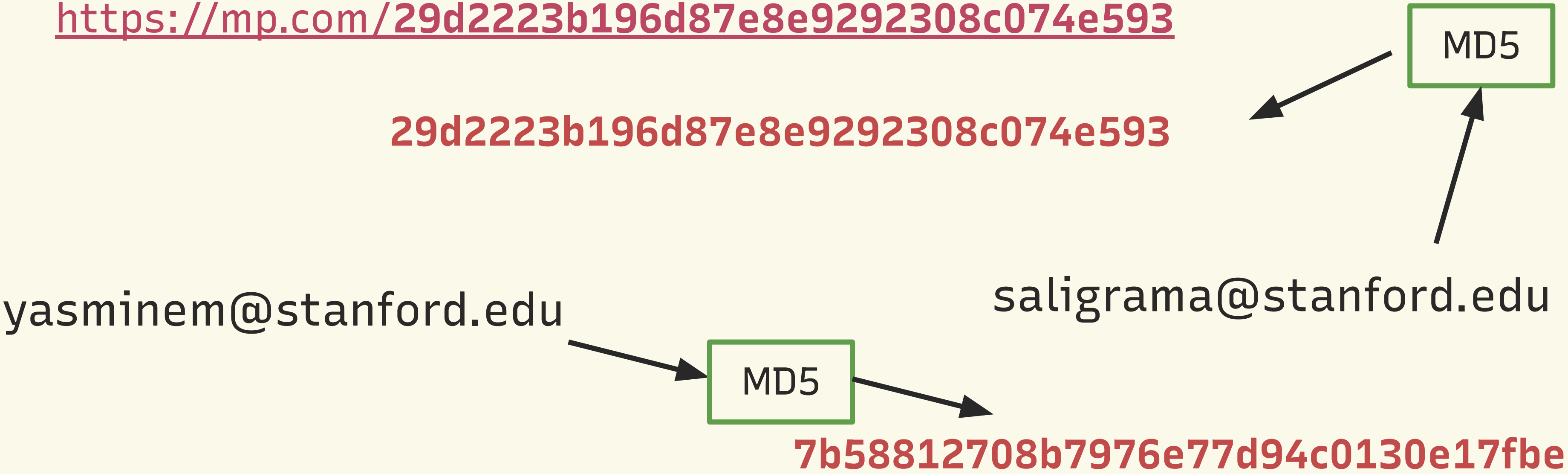
The questionnaire is open for another 7.2 hours, until 4pm PST later today. Text your friends, bug your enemies. They may not be *your* perfect match, but they could be someone else's. The bigger the pool, the better everyone's matches become.

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

Love,
The Stanford Marriage Pact

IDOR case study II: Stanford Marriage Pact (2020)

https://mp.com/**29d2223b196d87e8e9292308c074e593**



MD5

29d2223b196d87e8e9292308c074e593

saligrama@stanford.edu

yasminem@stanford.edu

MD5

7b58812708b7976e77d94c0130e17fbe

https://mp.com/7b58812708b7976e77d94c0130e17fbe

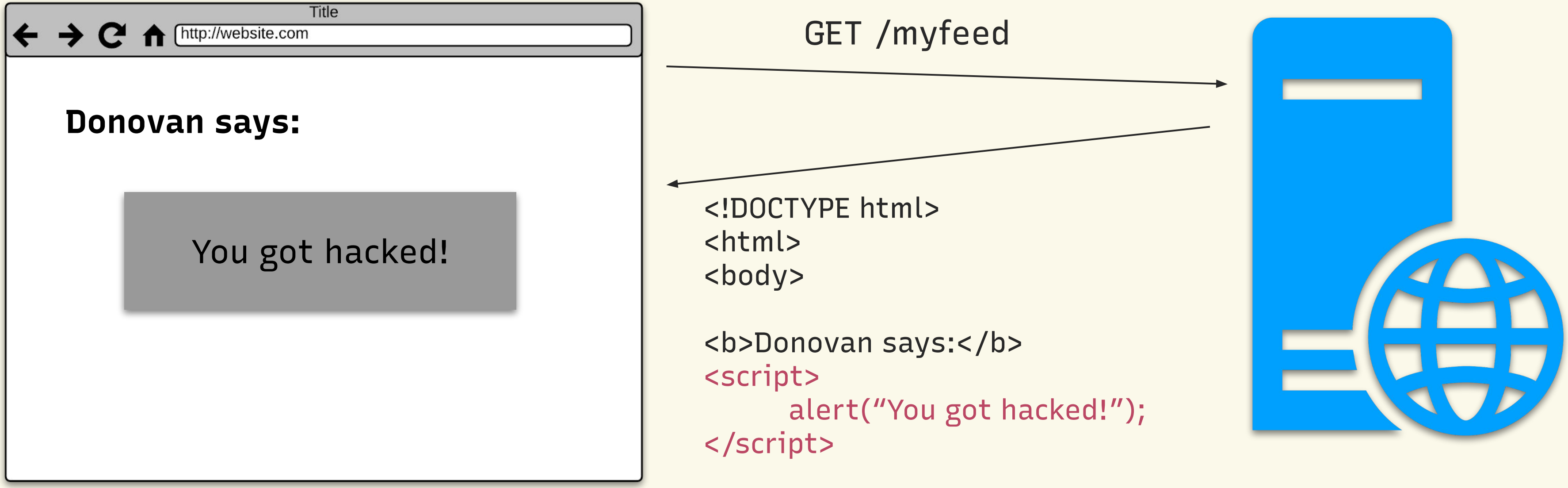
Cross-Site Scripting

Cross-Site Scripting (XSS)

- XSS attacks enable attackers to hijack your website to **run JavaScript code** on other users' browsers

- They occur when **user input is not properly sanitized and displayed**, allowing it to execute as code

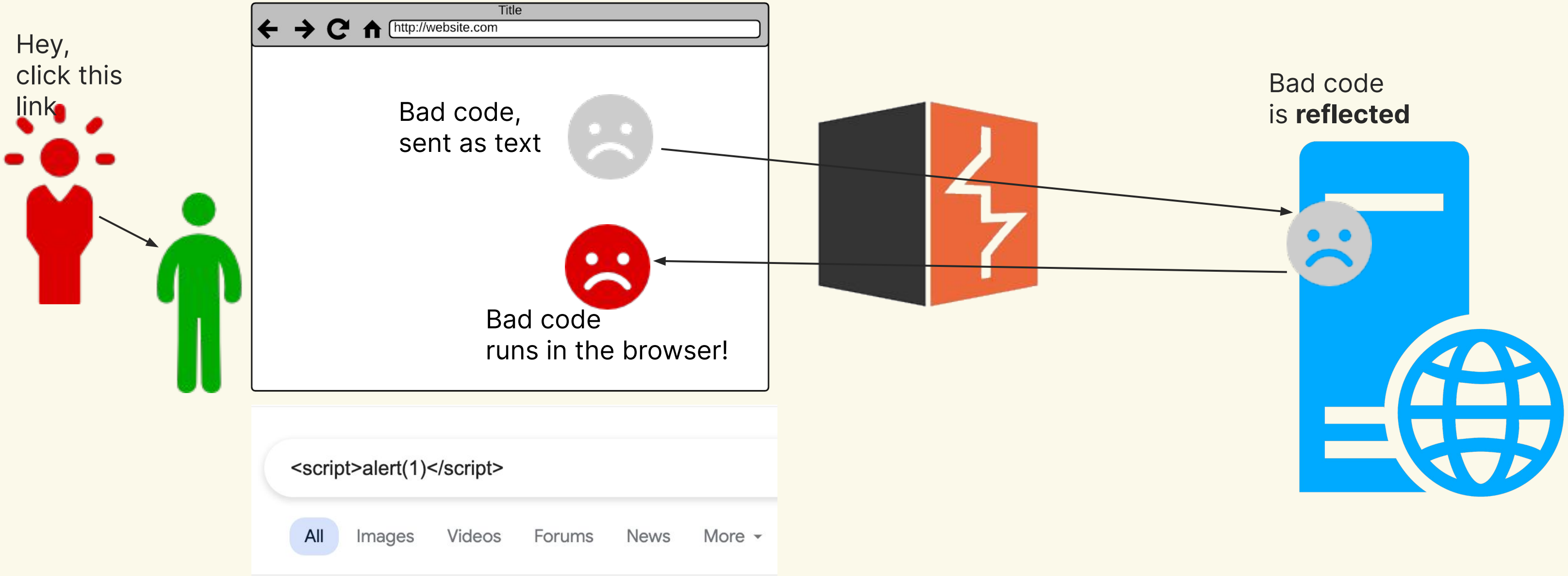
Cross-Site Scripting (XSS)



```
<!DOCTYPE html>
<html>
<body>

<b>Donovan says:</b>
<script>
        alert(“You got hacked!”);
</script>

</body>
</html>
```

www.yourwebsite.com/law/<?StealAllTheData.js>/supersecretdata

Reflected XSS



Hey, click this link

Bad code, sent as text

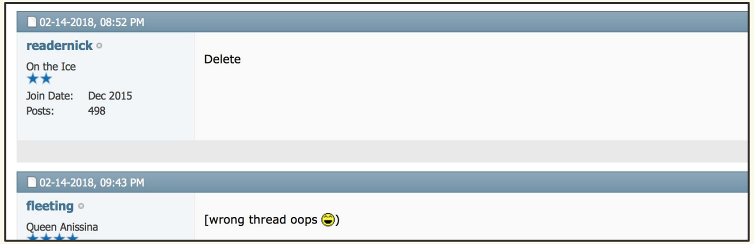
Bad code runs in the browser!

Bad code is **reflected**

<script>alert(1)</script>

https://vulnerable.website/search?query=<script>alert(“pwned”)</script>

Stored XSS



02-14-2018, 08:52 PM

readernick

On the Ice

Join Date: Dec 2015

Posts: 498

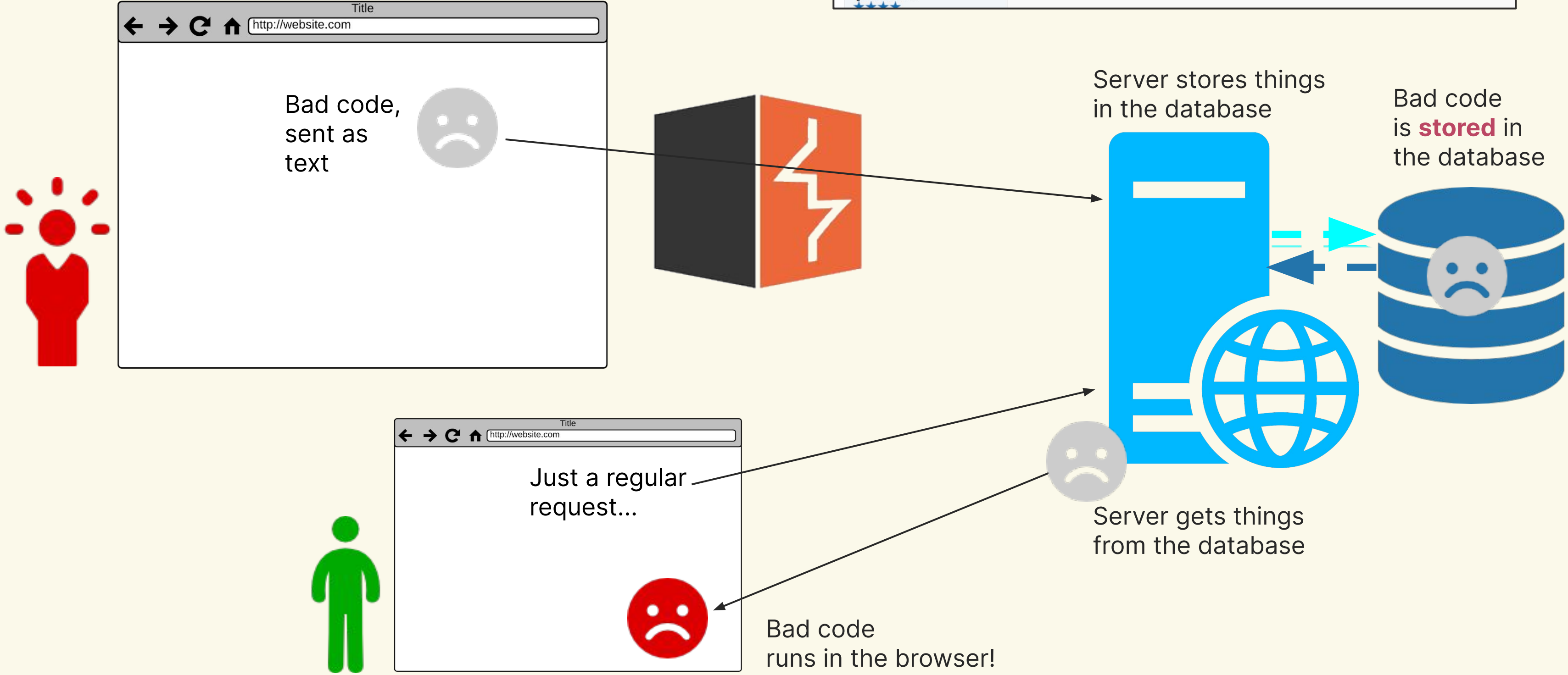
Delete

02-14-2018, 09:43 PM

fleeting

Queen Anissina

[wrong thread oops 😄)



Bad code, sent as text

Server stores things in the database

Bad code is **stored** in the database

Just a regular request...

Server gets things from the database

Bad code runs in the browser!

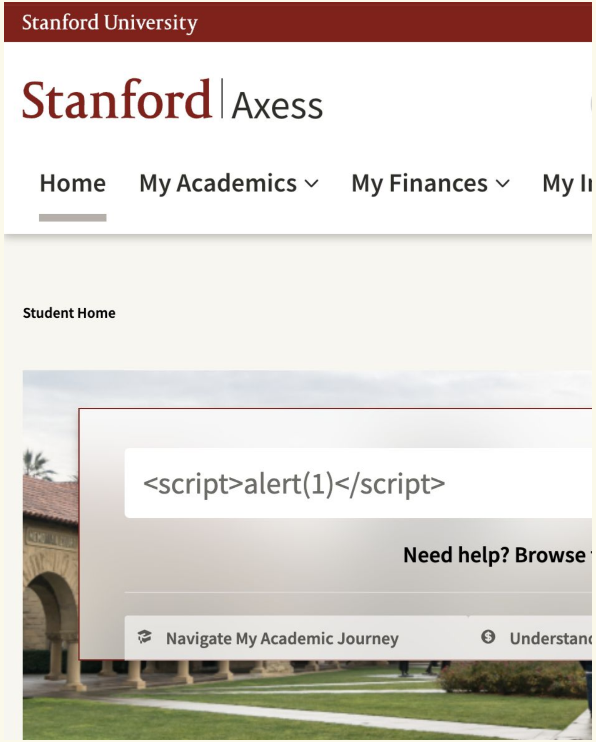
TRY IT!

- After our last data breach, we at CatShare want to make our customers feel like we care about them

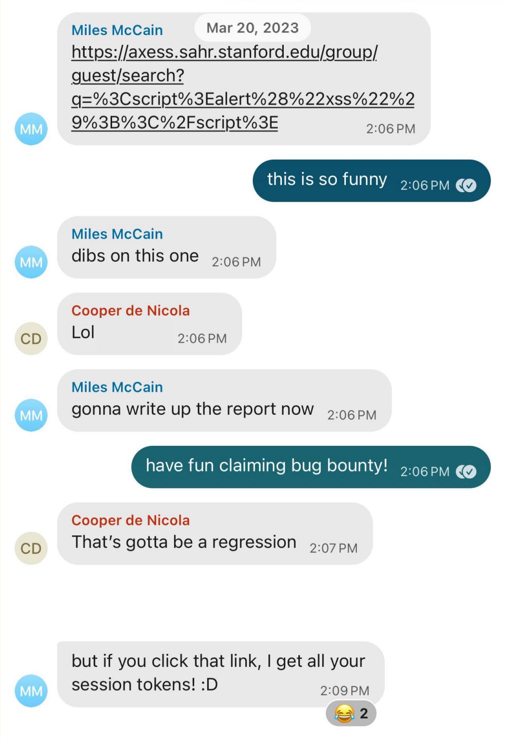
- We added an endpoint https://catshare.saligrama.io/hello that takes a user's name and greets them kindly. Ya know, to show we care
    - e.g. https://catshare.saligrama.io/hello?name=User1

- We think this is harmless and will only build customer trust. **Show us our mistake.**

XSS in Stanford Axess (2023)



<script>alert(1)</script>



Mar 20, 2023

Miles McCain
https://axess.sahr.stanford.edu/group/guest/search?q=%3Cscript%3Ealert%28%22xss%22%29%3B%3C%2Fscript%3E 2:06 PM

this is so funny 2:06 PM

Miles McCain
dibs on this one 2:06 PM

Cooper de Nicola
Lol 2:06 PM

Miles McCain
gonna write up the report now 2:06 PM

have fun claiming bug bounty! 2:06 PM

Cooper de Nicola
That's gotta be a regression 2:07 PM

but if you click that link, I get all your session tokens! :D 2:09 PM
😂 2

Found and disclosed in March 2023, awarded $1000 by the Stanford bug bounty.

Remediated January 2024.

Attacks on session handling

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
    - Escalate privileges to admin

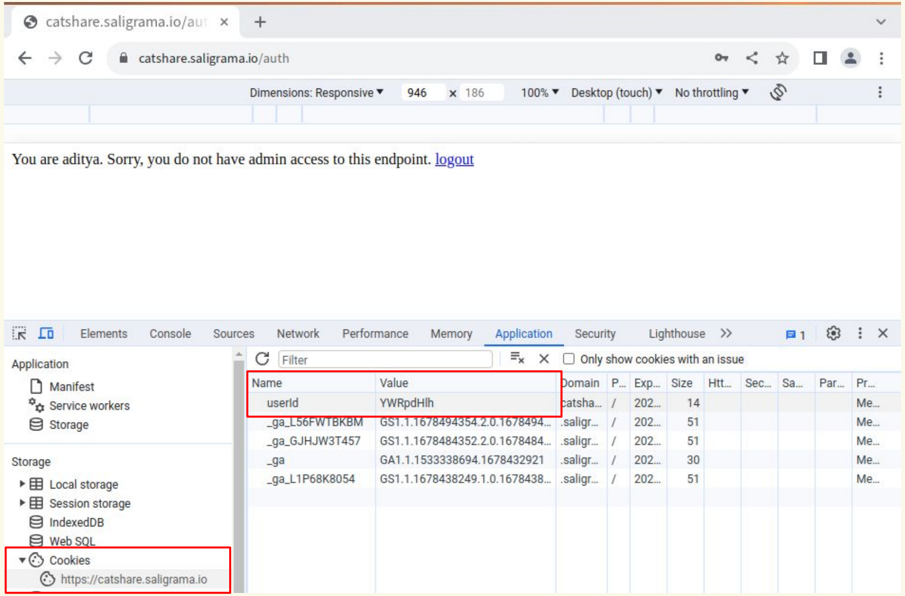
TRY IT!

- CatShare added an admin view to https://catshare.saligrama.io/login for admins to view user data
- Log in using `stanford:stanford`
- Can you become `admin` and view the user data?

TRY IT!

TOOLS/REFERENCE

- Cookie is in **Base64** format
  - Transforms data into a mix of letters and numbers.
  - Doesn't actually secure or encrypt data; it's just a **different way to show it**.
  - Use https://kk.lol to encode/decode
- Your browser's **Developer Tools**
  - Accessible from **Inspect Element**



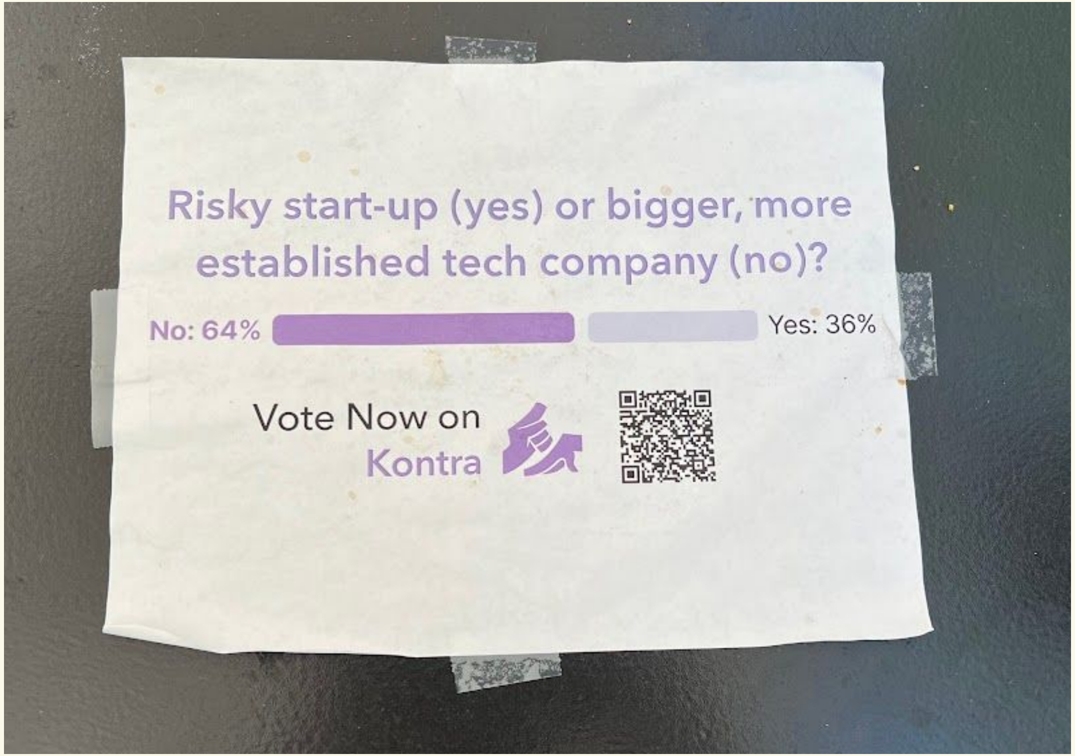
You are aditya. Sorry, you do not have admin access to this endpoint. logout

Name	Value	Domain	P...	Exp...	Size	Htt...	Sec...	Sa...	Par...	Pr...
userId	YWRpdHlh	catsha...	/	202...	14					Me...
_ga_L56FWTBKBM	GS1.1.1678494354.2.0.1678494...	.saligr...	/	202...	51					Me...
_ga_GJHJW3T457	GS1.1.1678484352.2.0.1678484...	.saligr...	/	202...	51					Me...
_ga	GA1.1.1533338694.1678432921	.saligr...	/	202...	30					Me...
_ga_L1P68K8054	GS1.1.1678438249.1.0.1678438...	.saligr...	/	202...	51					Me...

What to look for is in red (logged in as aditya here)

- https://catshare.saligrama.io/login
  - Login with stanford:stanford

Session handling case study: Kontra (2022)

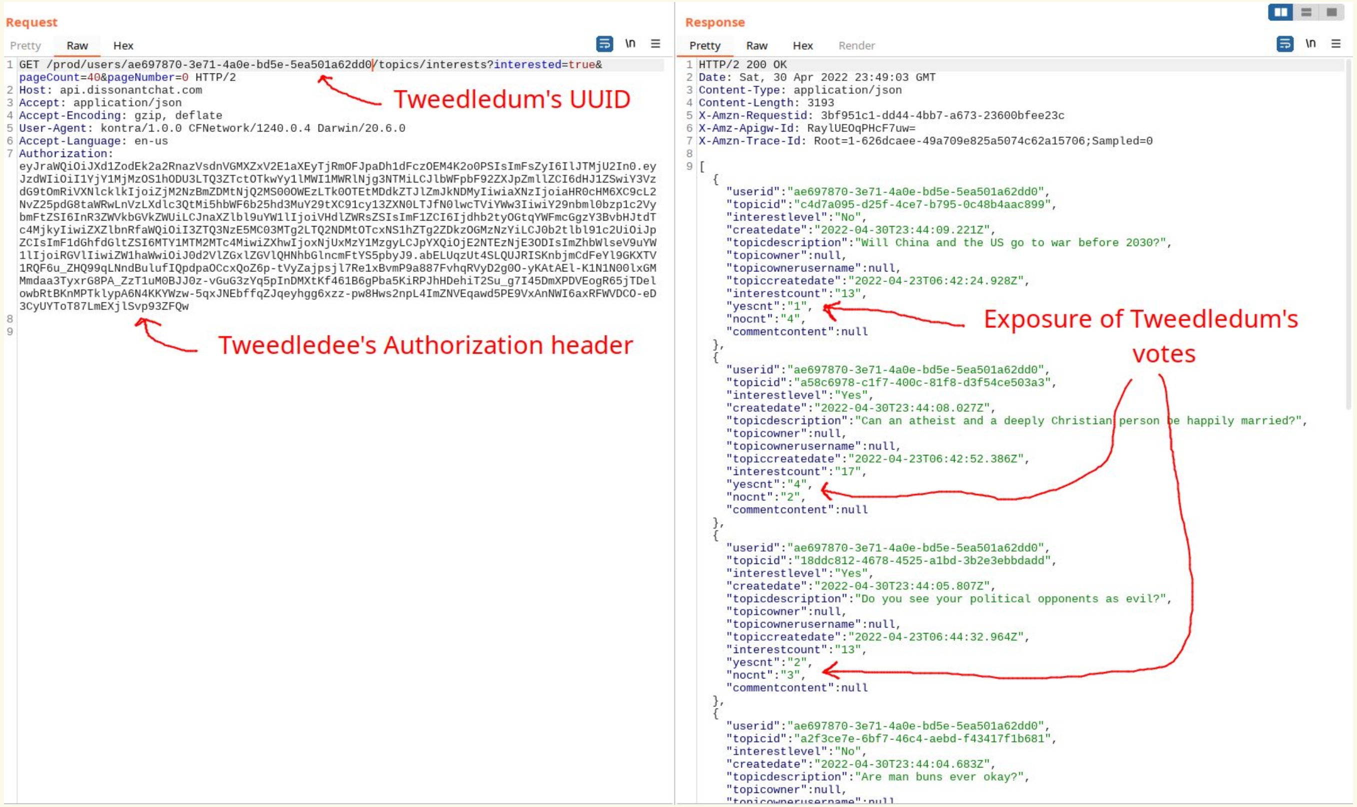


Risky start-up (yes) or bigger, more established tech company (no)?

No: 64% Yes: 36%

Vote Now on Kontra

Session handling case study: Kontra (2022)



```
GET /prod/users/ae697870-3e71-4a0e-bd5e-5ea501a62dd0/topics/interests?interested=true&
pageCount=40&pageNumber=0 HTTP/2
Host: api.dissonantchat.com
Accept: application/json
Accept-Encoding: gzip, deflate
User-Agent: kontra/1.0.0 CFNetwork/1240.0.4 Darwin/20.6.0
Accept-Language: en-us
Authorization:
eyJraWQiOiJXd1ZodEk2a2RnazVsdnVGMXZxV2E1aXEyTjRmOFJpaDh1dFczOEM4K2o0PSIsImFsZyI6IlJTMjU2In0.ey
JzdWIiOiI1YjY1MjMzOS1hODU3LTQ3ZTctOTkwYy1lMWI1MWRlNjg3NTMiLCJlbWFpbF92ZXJpZmllZCI6dHJ1ZSwiY3Vz
dG9tOmRiVXNlcklkIjoiZjM2NzBmZDMtNjQ2MS00OWEzLTk0OTEtMDdkZTJlZmJkNDMyIiwiaXNzIjoiaHR0cHM6XC9cL2
NvZ25pdG8taWRwLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tXC91cy13ZXN0LTJfN0lwcTViYWw3IiwiY29nbml0bzp1c2Vy
bmFtZSI6InR3ZWVkbGVkZWUiLCJnaXZlbl9uYW1lIjoiVHdlZWRsZSIsImF1ZCI6Ijdhb2tyOGtqYWFmcGgzY3BvbHJtdT
c4MjkyIiwiZXZlbnRfaWQiOiI3ZTQ3NzE5MC03MTg2LTQ2NDMtOTcxNS1hZTg2ZDkzOGMzNzYiLCJ0b2tlbl91c2UiOiJp
ZCIsImF1dGhfdGltZSI6MTY1MTM2MTc4MiwiZXhwIjoxNjUxMzY1MzgyLCJpYXQiOjE2NTEzNjE3ODIsImZhbWlseV9uYW
1lIjoiRGVlIiwiZW1haWwiOiJ0d2VlZGxlZGVlQHNhbGlncmFtYS5pbyJ9.abELUqzUt4SLQUJRISKnbjmCdFeYl9GKXTV
1RQF6u_ZHQ99qLNndBulufIQpdpaOCcxQoZ6p-tVyZajpsjl7Re1xBvmP9a887FvhqRVyD2gOO-yKAtAEl-K1N1N00lxGM
Mmdaa3TyxrG8PA_ZzT1uM0BJJ0z-vGuG3zYq5pInDMXtKf461B6gPba5KiRPJhHDehiT2Su_g7I45DmXPDVEogR65jTDel
owbRtBKnMPTklypA6N4KKYWzw-5qxJNEbffqZJqeyhgg6xzz-pw8Hws2npL4ImZNVEqawd5PE9VxAnNWI6axRFWVDCO-eD
3CyUYToT87LmEXjlSvp93ZFQw
```

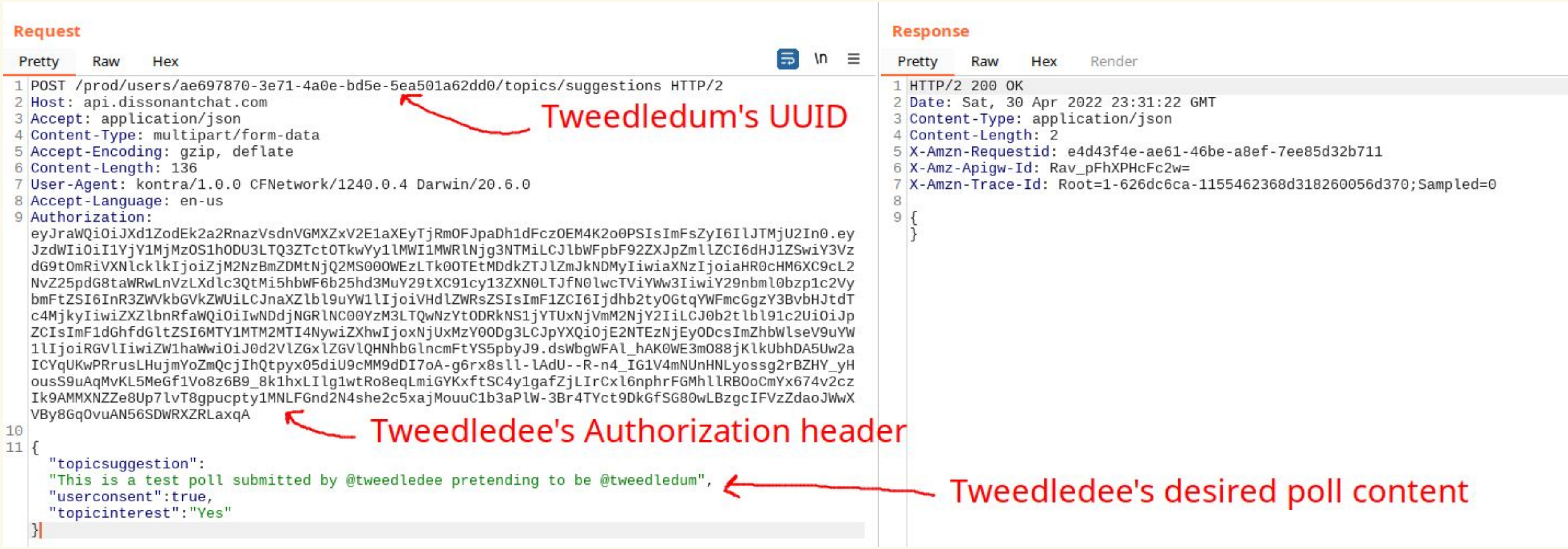
Tweedledum's UUID

Tweedledee's Authorization header

```
HTTP/2 200 OK
Date: Sat, 30 Apr 2022 23:49:03 GMT
Content-Type: application/json
Content-Length: 3193
X-Amzn-Requestid: 3bf951c1-dd44-4bb7-a673-23600bfee23c
X-Amz-Apigw-Id: RaylUEOqPHcF7uw=
X-Amzn-Trace-Id: Root=1-626dcaee-49a709e825a5074c62a15706;Sampled=0

[
  {
    "userid":"ae697870-3e71-4a0e-bd5e-5ea501a62dd0",
    "topicid":"c4d7a095-d25f-4ce7-b795-0c48b4aac899",
    "interestlevel":"No",
    "createdate":"2022-04-30T23:44:09.221Z",
    "topicdescription":"Will China and the US go to war before 2030?",
    "topicowner":null,
    "topicownerusername":null,
    "topiccreatedate":"2022-04-23T06:42:24.928Z",
    "interestcount":"13",
    "yescnt":"1",
    "nocnt":"4",
    "commentcontent":null
  },
  {
    "userid":"ae697870-3e71-4a0e-bd5e-5ea501a62dd0",
    "topicid":"a58c6978-c1f7-400c-81f8-d3f54ce503a3",
    "interestlevel":"Yes",
    "createdate":"2022-04-30T23:44:08.027Z",
    "topicdescription":"Can an atheist and a deeply Christian person be happily married?",
    "topicowner":null,
    "topicownerusername":null,
    "topiccreatedate":"2022-04-23T06:42:52.386Z",
    "interestcount":"17",
    "yescnt":"4",
    "nocnt":"2",
    "commentcontent":null
  },
  {
    "userid":"ae697870-3e71-4a0e-bd5e-5ea501a62dd0",
    "topicid":"18ddc812-4678-4525-a1bd-3b2e3ebbdadd",
    "interestlevel":"Yes",
    "createdate":"2022-04-30T23:44:05.807Z",
    "topicdescription":"Do you see your political opponents as evil?",
    "topicowner":null,
    "topicownerusername":null,
    "topiccreatedate":"2022-04-23T06:44:32.964Z",
    "interestcount":"13",
    "yescnt":"2",
    "nocnt":"3",
    "commentcontent":null
  },
  {
    "userid":"ae697870-3e71-4a0e-bd5e-5ea501a62dd0",
    "topicid":"a2f3ce7e-6bf7-46c4-aebd-f43417f1b681",
    "interestlevel":"No",
    "createdate":"2022-04-30T23:44:04.683Z",
    "topicdescription":"Are man buns ever okay?",
    "topicowner":null,
    "topicownerusername":null
```

Exposure of Tweedledum's votes
]

Session handling case study: Kontra (2022)



```
POST /prod/users/ae697870-3e71-4a0e-bd5e-5ea501a62dd0/topics/suggestions HTTP/2
Host: api.dissonantchat.com
Accept: application/json
Content-Type: multipart/form-data
Accept-Encoding: gzip, deflate
Content-Length: 136
User-Agent: kontra/1.0.0 CFNetwork/1240.0.4 Darwin/20.6.0
Accept-Language: en-us
Authorization:
eyJraWQiOiJXd1ZodEk2a2RnazVsdnVGMXZxV2E1aXEyTjRmOFJpaDh1dFczOEM4K2o0PSIsImFsZyI6IlJTMjU2In0.ey
JzdWIiOiI1YjY1MjMzOS1hODU3LTQ3ZTctOTkwYy1lMWI1MWRlNjg3NTMiLCJlbWFpbF92ZXJpZmllZCI6dHJ1ZSwiY3Vz
dG9tOmRiVXNlcklkIjoiZjM2NzBmZDMtNjQ2MS00OWEzLTk0OTEtMDdkZTJlZmJkNDMyIiwiaXNzIjoiaHR0cHM6XC9cL2
NvZ25pdG8taWRwLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tXC91cy13ZXN0LTJfN0lwcTViYWw3IiwiY29nbml0bzp1c2Vy
bmFtZSI6InR3ZWVkbGVkZWUiLCJnaXZlbl9uYW1lIjoiVHdlZWRsZSIsImF1ZCI6Ijdhb2tyOGtqYWFmcGgzY3BvbHJtdT
c4MjkyIiwiZXZlbnRfaWQiOiIwNDdjNGRlNC00YzM3LTQwNzYtODRkNS1jYTUxNjVmM2NjY2IiLCJ0b2tlbl91c2UiOiJp
ZCIsImF1dGhfdGltZSI6MTY1MTM2MTI4NywiZXhwIjoxNjUxMzY0ODg3LCJpYXQiOjE2NTEzNjEyODcsImZhbWlseV9uYW
1lIjoiRGVlIiwiZW1haWwiOiJ0d2VlZGxlZGVlQHNhbGlncmFtYS5pbyJ9.dsWbgWFAl_hAK0WE3mO88jKlkUbhDA5Uw2a
ICYqUKwPRrusLHujmYoZmQcjIhQtpyx05diU9cMM9dDI7oA-g6rx8sll-lAdU--R-n4_IG1V4mNUnHNLyossg2rBZHY_yH
ousS9uAqMvKL5MeGf1Vo8z6B9_8k1hxLIlg1wtRo8eqLmiGYKxftSC4y1gafZjLIrCxl6nphrFGMhllRBOoCmYx674v2cz
Ik9AMMXNZZe8Up7lvT8gpucpty1MNLFGnd2N4she2c5xajMouuC1b3aPlW-3Br4TYct9DkGfSG80wLBzgcIFVzZdaoJWwX
VBy8GqOvuAN56SDWRXZRLaxqA

{
  "topicsuggestion":
  "This is a test poll submitted by @tweedledee pretending to be @tweedledum",
  "userconsent":true,
  "topicinterest":"Yes"
}
```

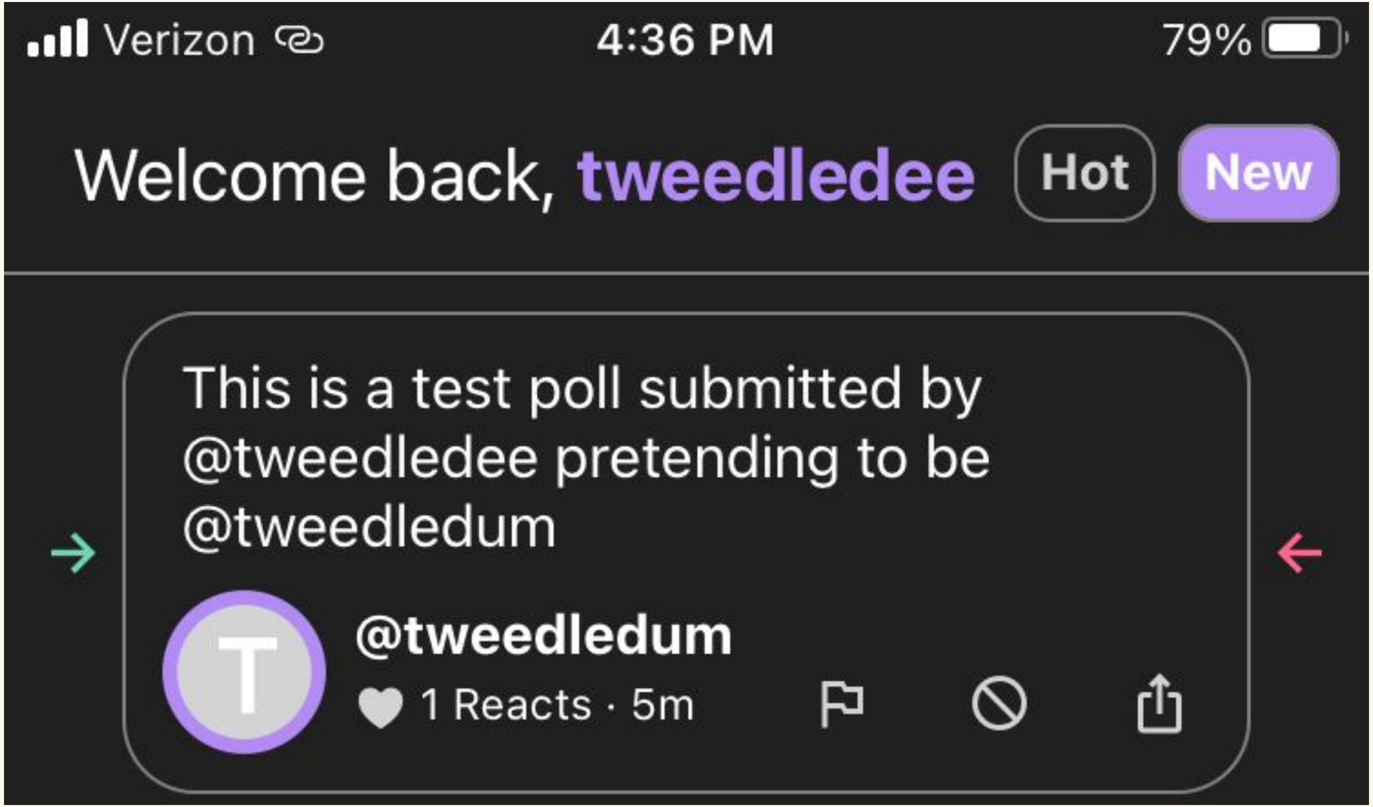
Tweedledum's UUID

Tweedledee's Authorization header

Tweedledee's desired poll content

```
HTTP/2 200 OK
Date: Sat, 30 Apr 2022 23:31:22 GMT
Content-Type: application/json
Content-Length: 2
X-Amzn-Requestid: e4d43f4e-ae61-46be-a8ef-7ee85d32b711
X-Amz-Apigw-Id: Rav_pFhXPHcFc2w=
X-Amzn-Trace-Id: Root=1-626dc6ca-1155462368d318260056d370;Sampled=0

{
}
```

Session handling case study: Kontra (2022)



Welcome back, tweedledee

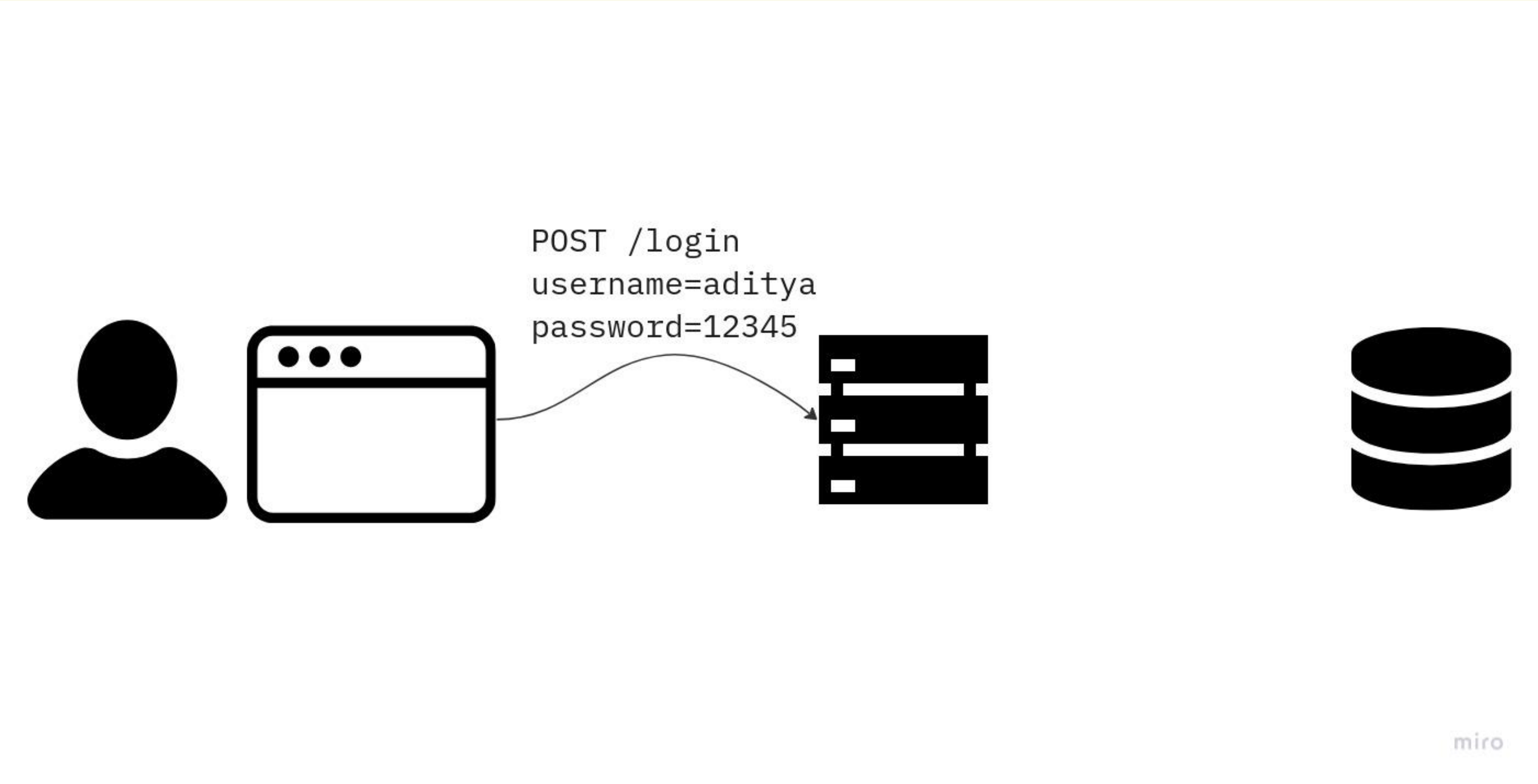
This is a test poll submitted by @tweedledee pretending to be @tweedledum

@tweedledum

1 Reacts · 5m

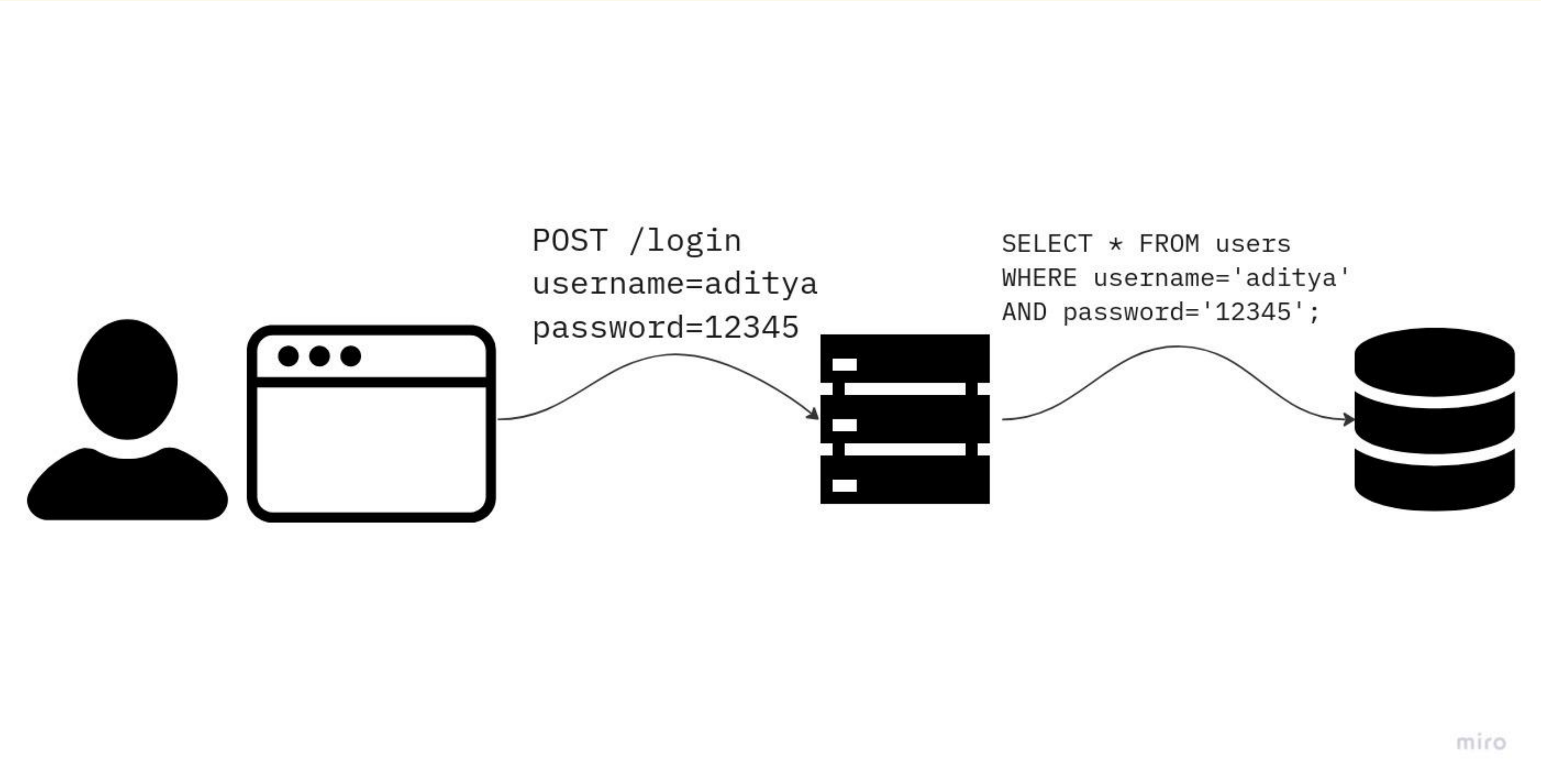
Database vulnerabilities

Logging in with a database



```
POST /login
username=aditya
password=12345
```

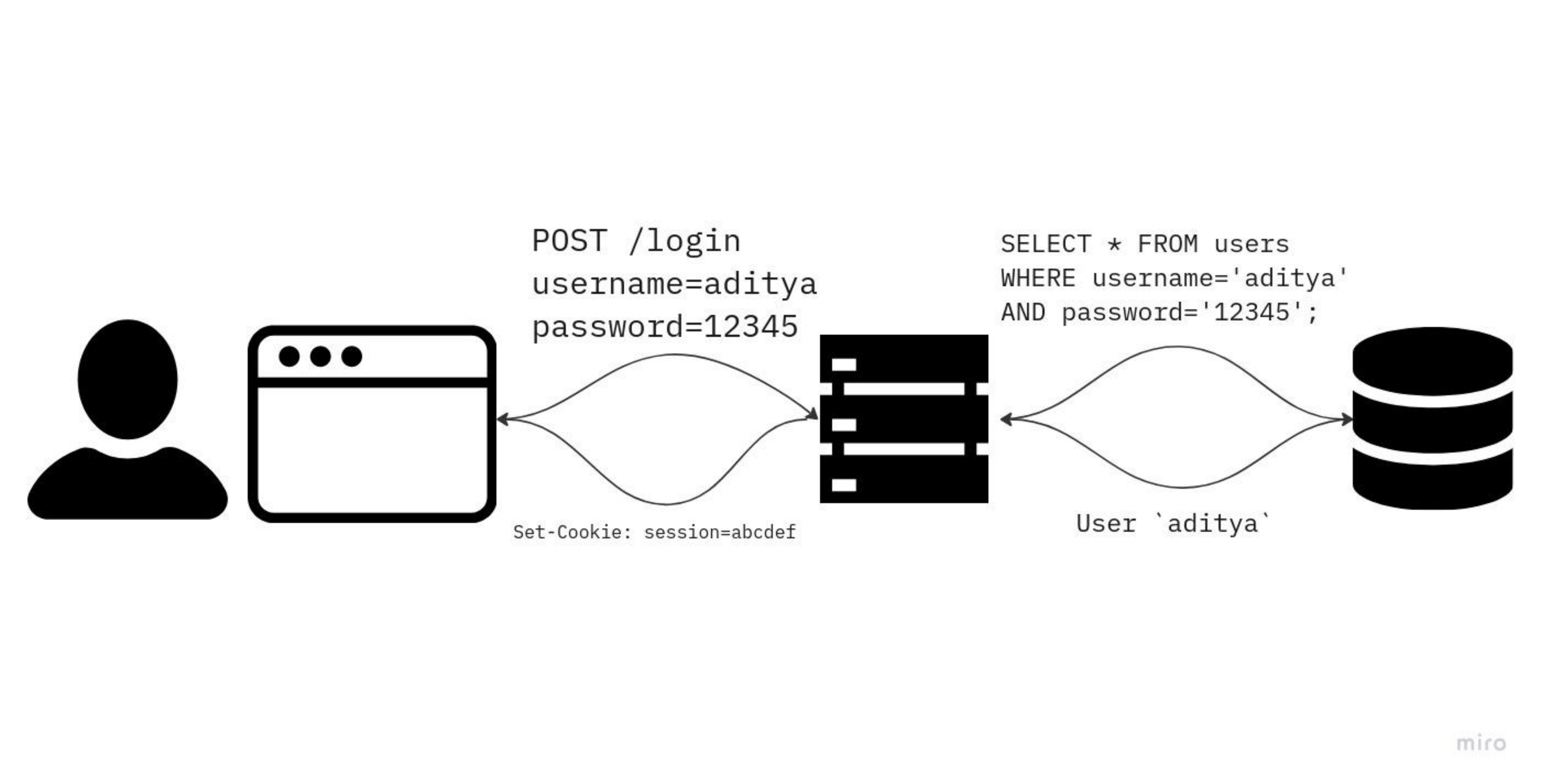
Logging in with a database



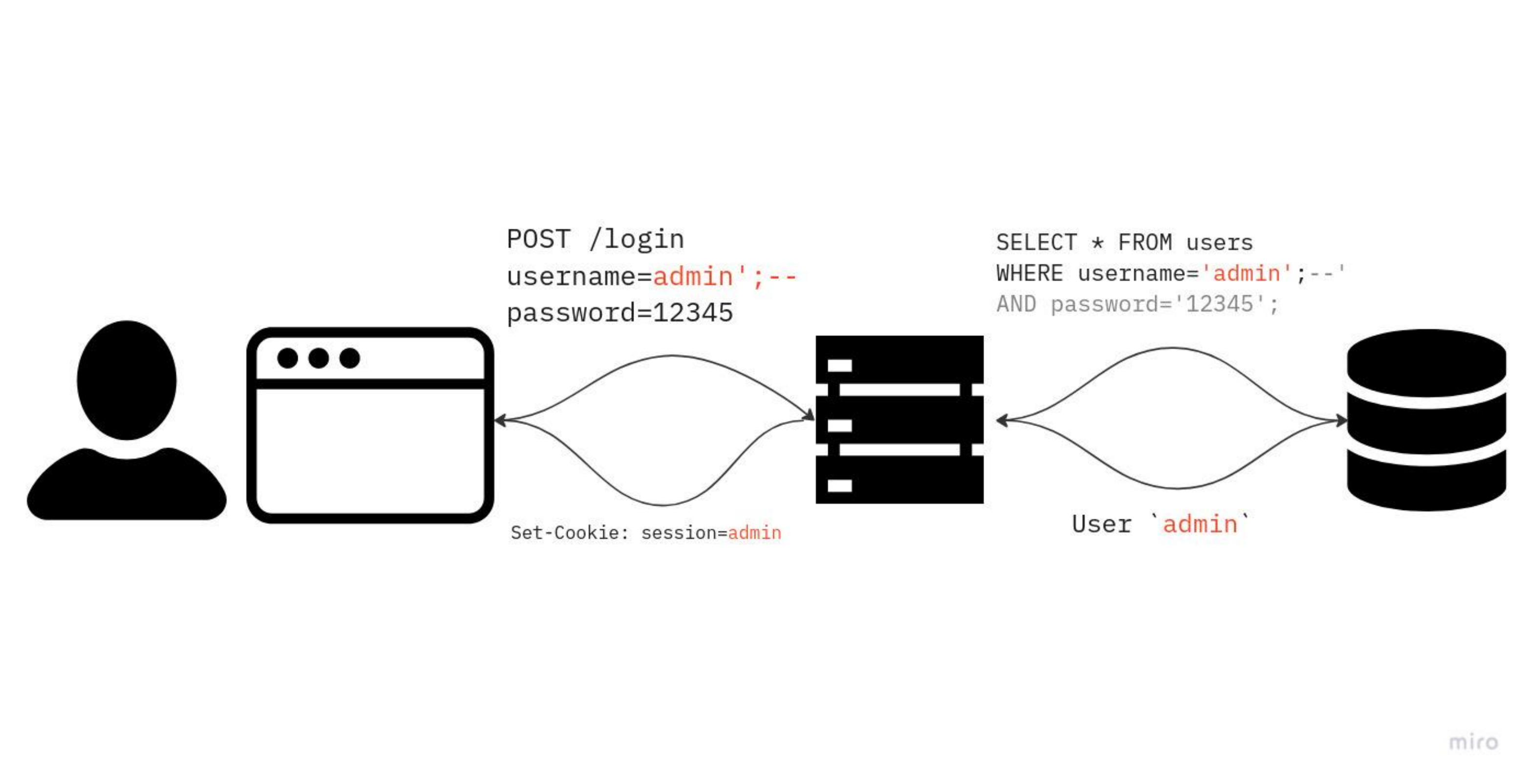
```
POST /login
username=aditya
password=12345
```

```
SELECT * FROM users
WHERE username='aditya'
AND password='12345';
```

Logging in with a database



SQL injection: logging in with malicious input



```
POST /login
username=admin';--
password=12345
```

```
SELECT * FROM users
WHERE username='admin';--'
AND password='12345';
```

`Set-Cookie: session=admin`

User `admin`

Common SQL injection payloads

- **‘;--** ends the string, and terminates the rest of the command
  - e.g. `SELECT * FROM users WHERE username=’admin’;-- AND password=’12345’;`

- **‘OR 1=1 ;--** disables any filters applied to the query
  - e.g. `SELECT * FROM users WHERE username=’admin’ OR 1=1;-- AND password=’12345’;`

- **‘AND 0=1 ;--** guarantees an empty result
  - e.g. `SELECT * FROM banned WHERE username=’me’ AND 0=1;--;`

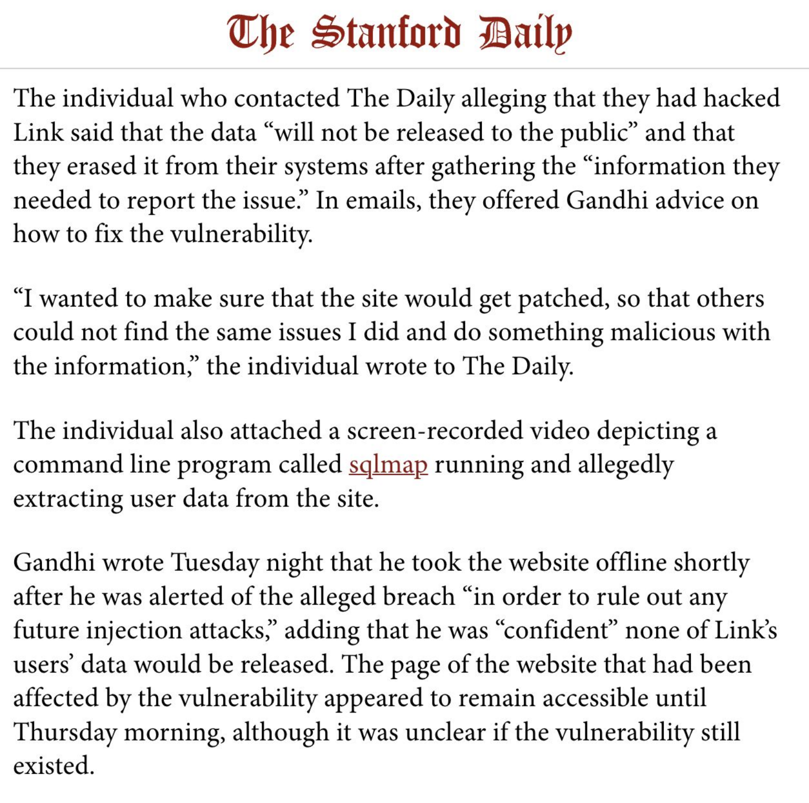
TRY IT!

- The CatShare team isn’t immune to having two vulnerabilities in the same endpoint!

- Remember endpoint **https://catshare.saligrama.io/user** to access user info
    - e.g. **https://catshare.saligrama.io/user?id=10** – the admin you can’t access

- Use SQL injection to get the admin’s (and everyone else’s) user info!
    - The user ID is an integer, so don’t worry about escaping the string

SQL injection in Stanford Link (2020)



The Stanford Daily

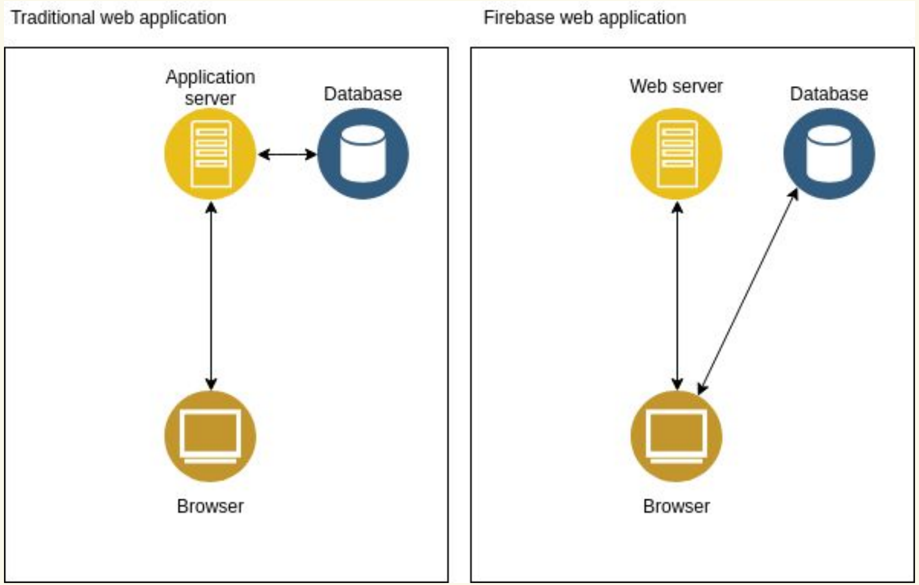
The individual who contacted The Daily alleging that they had hacked Link said that the data "will not be released to the public" and that they erased it from their systems after gathering the "information they needed to report the issue." In emails, they offered Gandhi advice on how to fix the vulnerability.

"I wanted to make sure that the site would get patched, so that others could not find the same issues I did and do something malicious with the information," the individual wrote to The Daily.

The individual also attached a screen-recorded video depicting a command line program called sqlmap running and allegedly extracting user data from the site.

Gandhi wrote Tuesday night that he took the website offline shortly after he was alerted of the alleged breach "in order to rule out any future injection attacks," adding that he was "confident" none of Link's users' data would be released. The page of the website that had been affected by the vulnerability appeared to remain accessible until Thursday morning, although it was unclear if the vulnerability still existed.

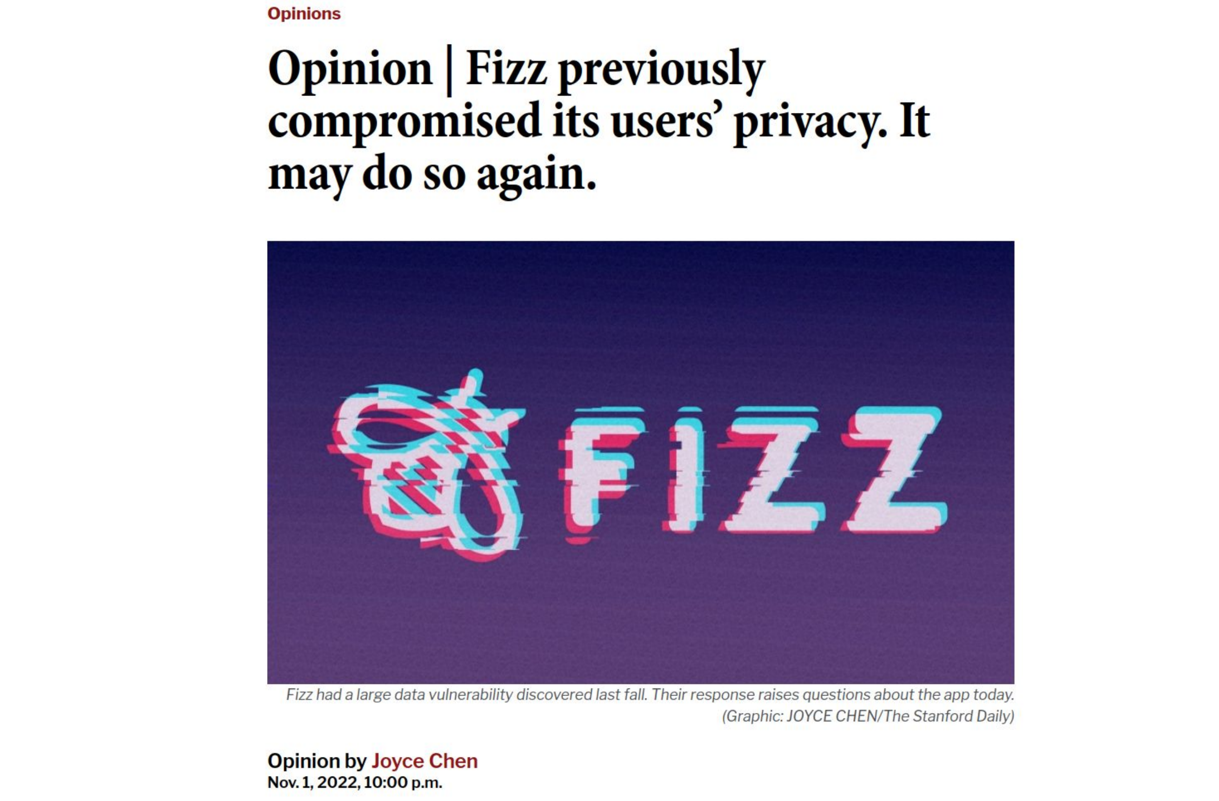
Misconfigured Firebase security rules



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

Case study: Fizz (2021)



Opinions

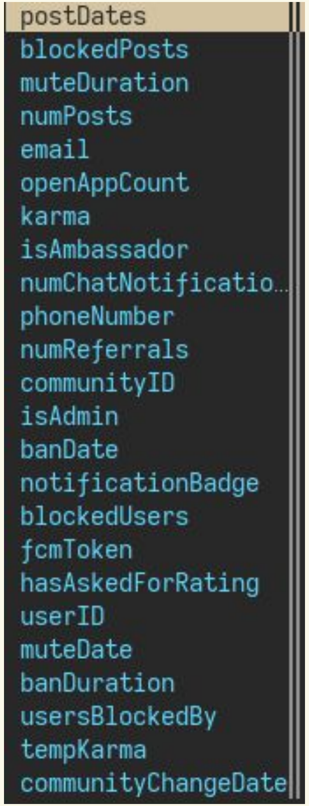
Opinion | Fizz previously compromised its users' privacy. It may do so again.

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

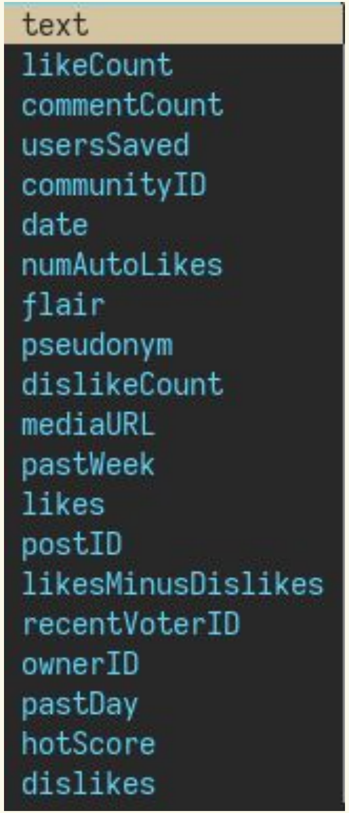
Nov. 1, 2022, 10:00 p.m.

Case study: Fizz (2021)



```
postDates
blockedPosts
muteDuration
numPosts
email
openAppCount
karma
isAmbassador
numChatNotificatio...
phoneNumber
numReferrals
communityID
isAdmin
banDate
notificationBadge
blockedUsers
fcmToken
hasAskedForRating
userID
muteDate
banDuration
usersBlockedBy
tempKarma
communityChangeDate
```

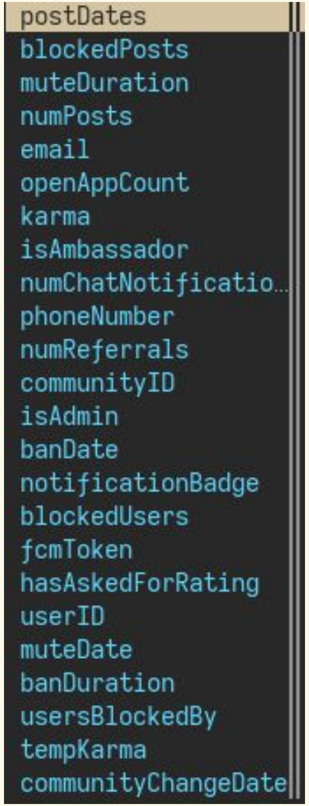
Users



```
text
likeCount
commentCount
usersSaved
communityID
date
numAutoLikes
flair
pseudonym
dislikeCount
mediaURL
pastWeek
likes
postID
likesMinusDislikes
recentVoterID
ownerID
pastDay
hotScore
dislikes
```

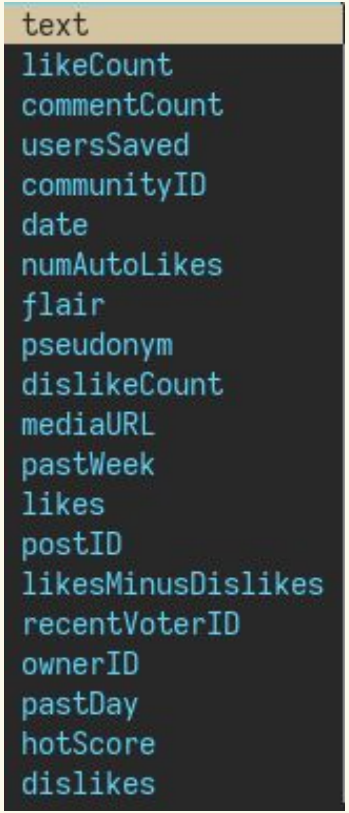
Posts

Case study: Fizz (2021)



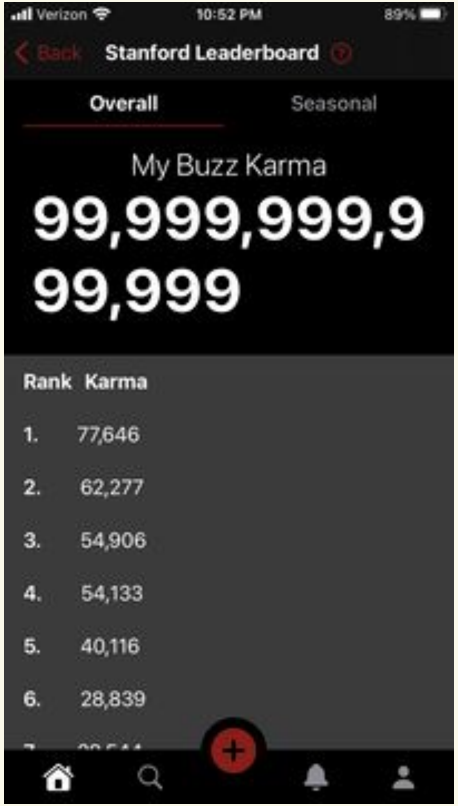
```
postDates
blockedPosts
muteDuration
numPosts
email
openAppCount
karma
isAmbassador
numChatNotificatio…
phoneNumber
numReferrals
communityID
isAdmin
banDate
notificationBadge
blockedUsers
fcmToken
hasAskedForRating
userID
muteDate
banDuration
usersBlockedBy
tempKarma
communityChangeDate
```

Users



```
text
likeCount
commentCount
usersSaved
communityID
date
numAutoLikes
flair
pseudonym
dislikeCount
mediaURL
pastWeek
likes
postID
likesMinusDislikes
recentVoterID
ownerID
pastDay
hotScore
dislikes
```

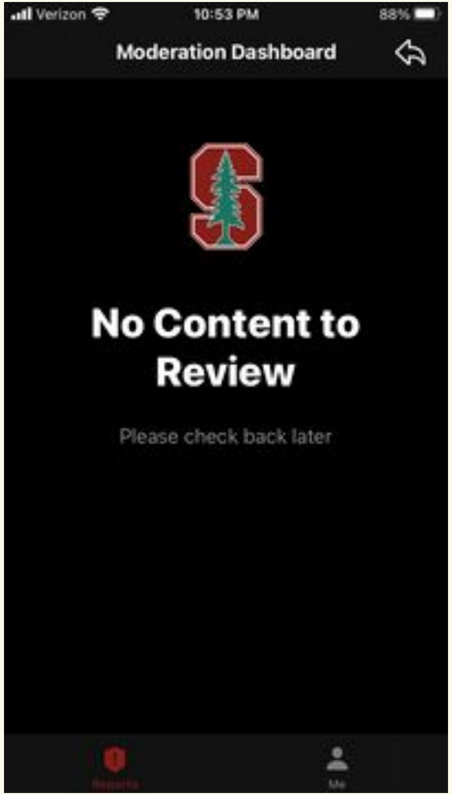
Posts



My Buzz Karma

99,999,999,999,999

Rank	Karma
1.	77,646
2.	62,277
3.	54,906
4.	54,133
5.	40,116
6.	28,839



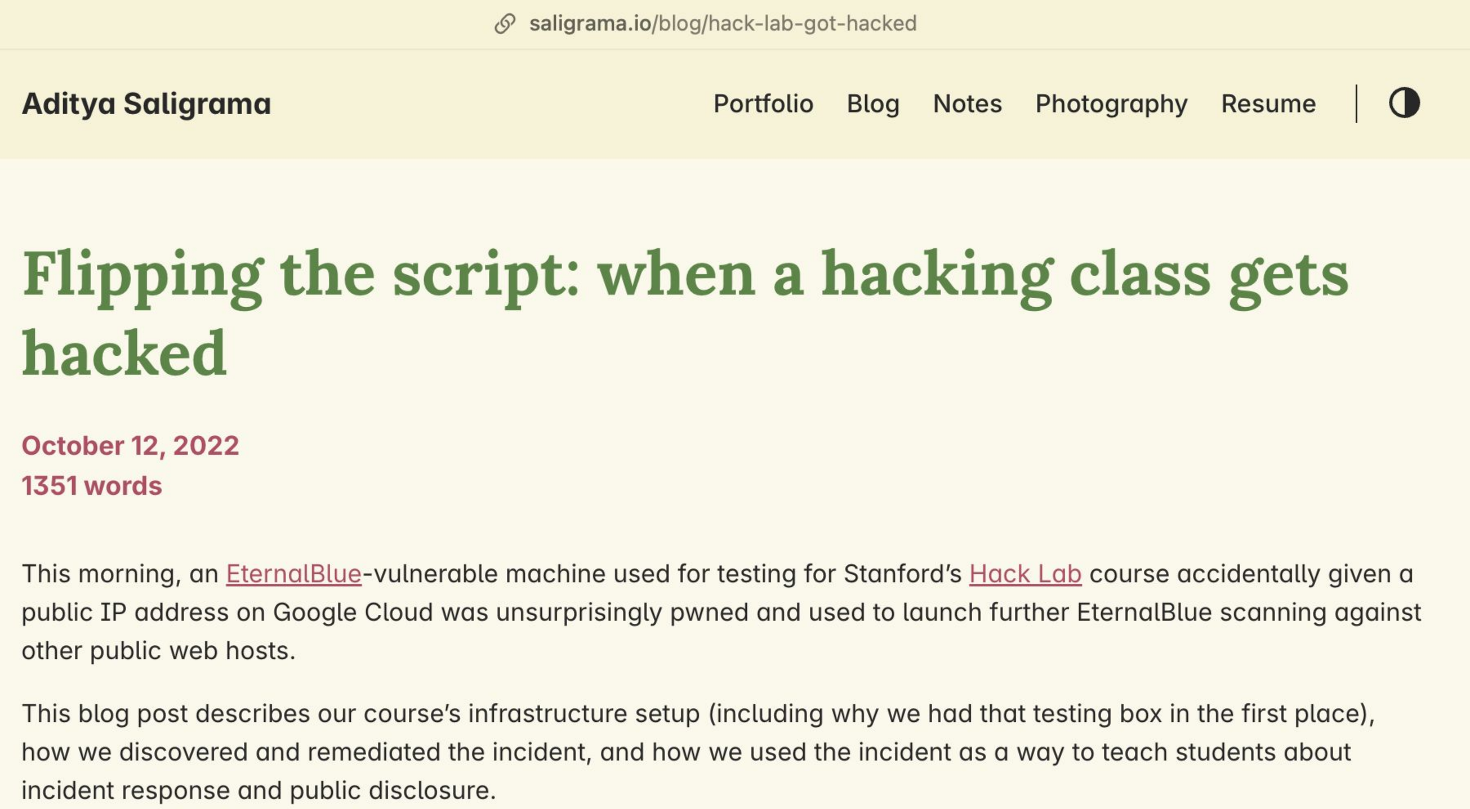
No Content to Review

Please check back later

Wrapping up

Nothing is 100% secure

It happens to the best of us



saligrama.io/blog/hack-lab-got-hacked

Aditya Saligrama

Portfolio Blog Notes Photography Resume

Flipping the script: when a hacking class gets hacked

October 12, 2022
1351 words

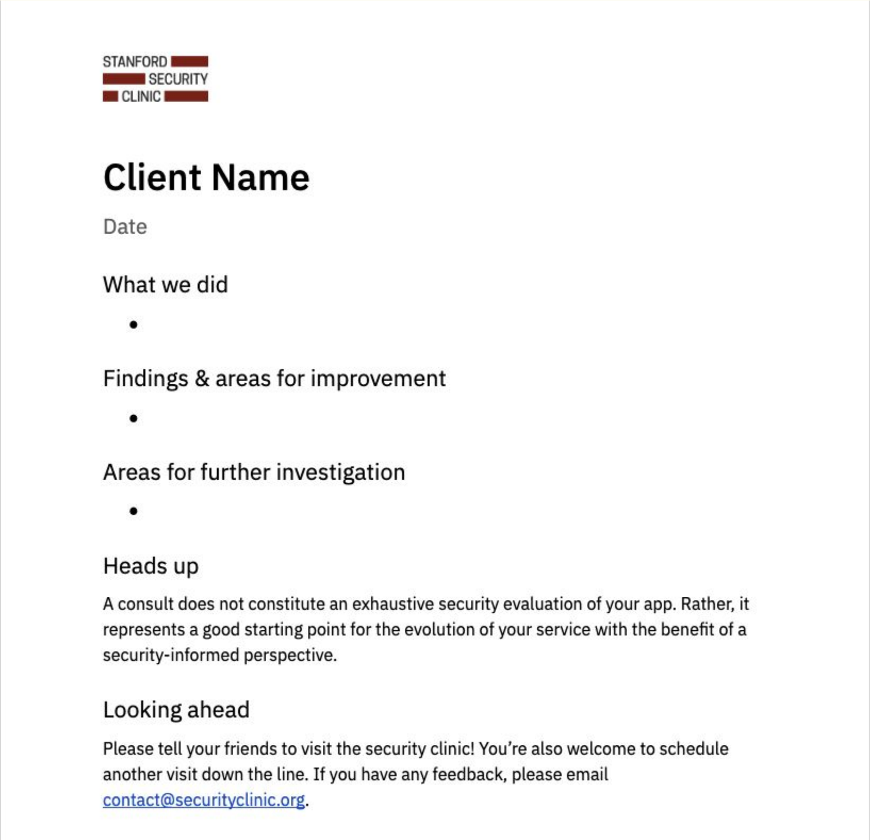
This morning, an EternalBlue-vulnerable machine used for testing for Stanford's Hack Lab course accidentally given a public IP address on Google Cloud was unsurprisingly pwned and used to launch further EternalBlue scanning against other public web hosts.

This blog post describes our course's infrastructure setup (including why we had that testing box in the first place), how we discovered and remediated the incident, and how we used the incident as a way to teach students about incident response and public disclosure.

The community can help!

*A **vulnerability disclosure policy** is intended to give ethical hackers clear guidelines for submitting potentially unknown and harmful security vulnerabilities to organizations.*

Disclosing vulnerabilities ethically



STANFORD
SECURITY
CLINIC

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.

https://securityclinic.org

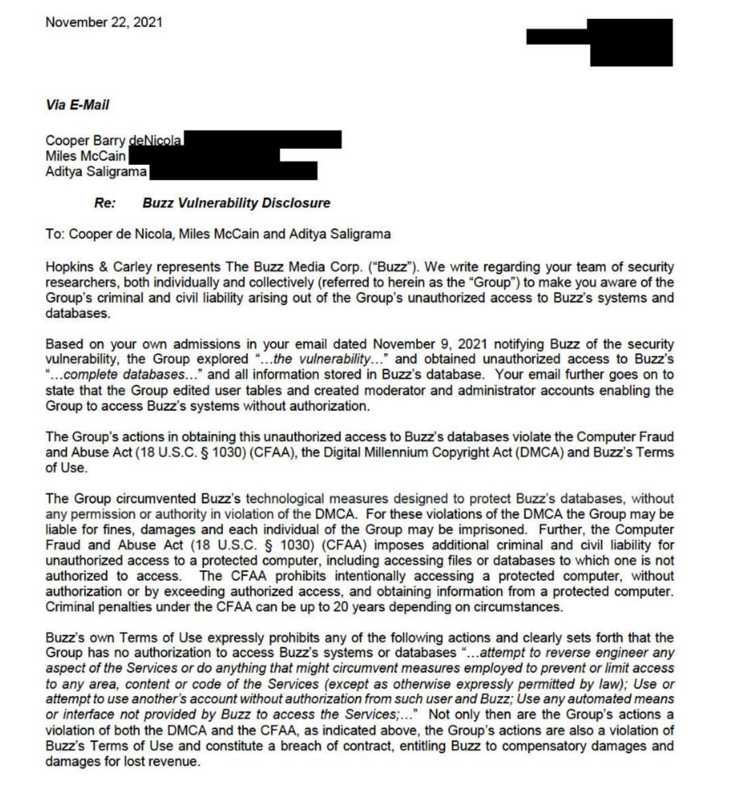
Bug bounty programs

Stanford Bug Bounty Program

Securing Stanford Together

Bug bounty programs incentivize the community to responsibly disclose security vulnerabilities to the vendor, in exchange for an (often monetary) reward.

Potential legal consequences to ethical hacking



November 22, 2021

[redacted]

Via E-Mail

Cooper Barry deNicola [redacted]
Miles McCain
Aditya Saligrama

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.

Credits

CatShare source code

https://github.com/saligrama/catshare-serverless

Other materials

- *Web Crash Course* – Alex Stamos, INTLPOL 268 *Hack Lab*
- *Web Crash Course, IDOR/XSS/Session Handling Slides, Marriage Pact IDOR Case Study* – Cooper de Nicola
- *Stanford Link, Fizz, Stanford Reveal articles* – The Stanford Daily
- *CatShare* – Cooper de Nicola, Aditya Saligrama, George Hosono