

# Web Hacking for Social Good

Aditya Saligrama  
Cooper de Nicola

# **Security and its relevance to Stanford students**

## 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?***

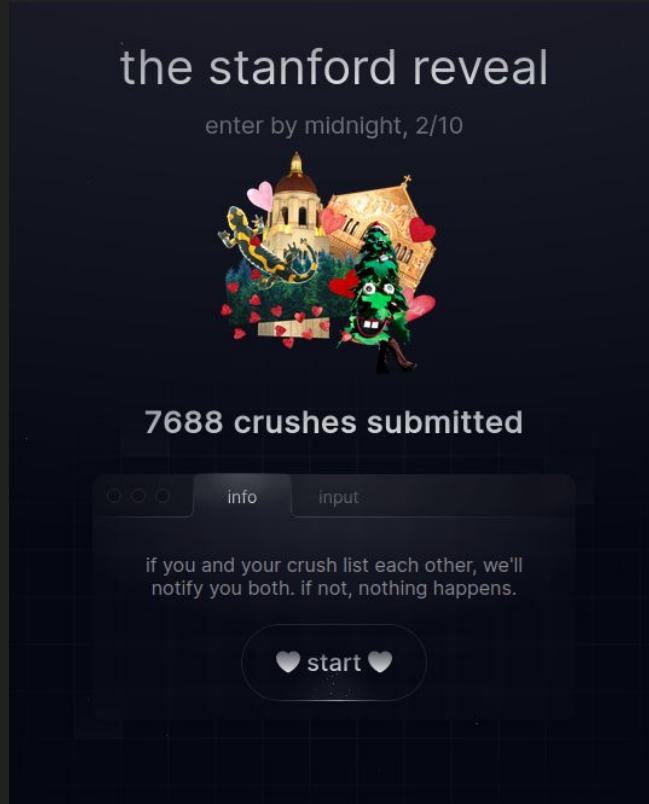
# Case study: Stanford Link (2020)

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)



```
44  {
45      "submittingUserFullName": "Aditya Saligrama",
46      "user": "4yz2FPyYDgND8KhtVOQLCeeGsaq2",
47      "submittingUserEmail": "akps@stanford.edu",
48      "fullNames": []
49  },
50
51
52  {
53      "submittingUserEmail": "mccain@stanford.edu",
54      "submittingUserFullName": "Robert Miles Redd McCain",
55      "user": "N3Q9CkeKeJfKQzOhqt7qFbpanat1",
56      "fullNames": [
57          "isabelle levent"
58      ]
59  },
```

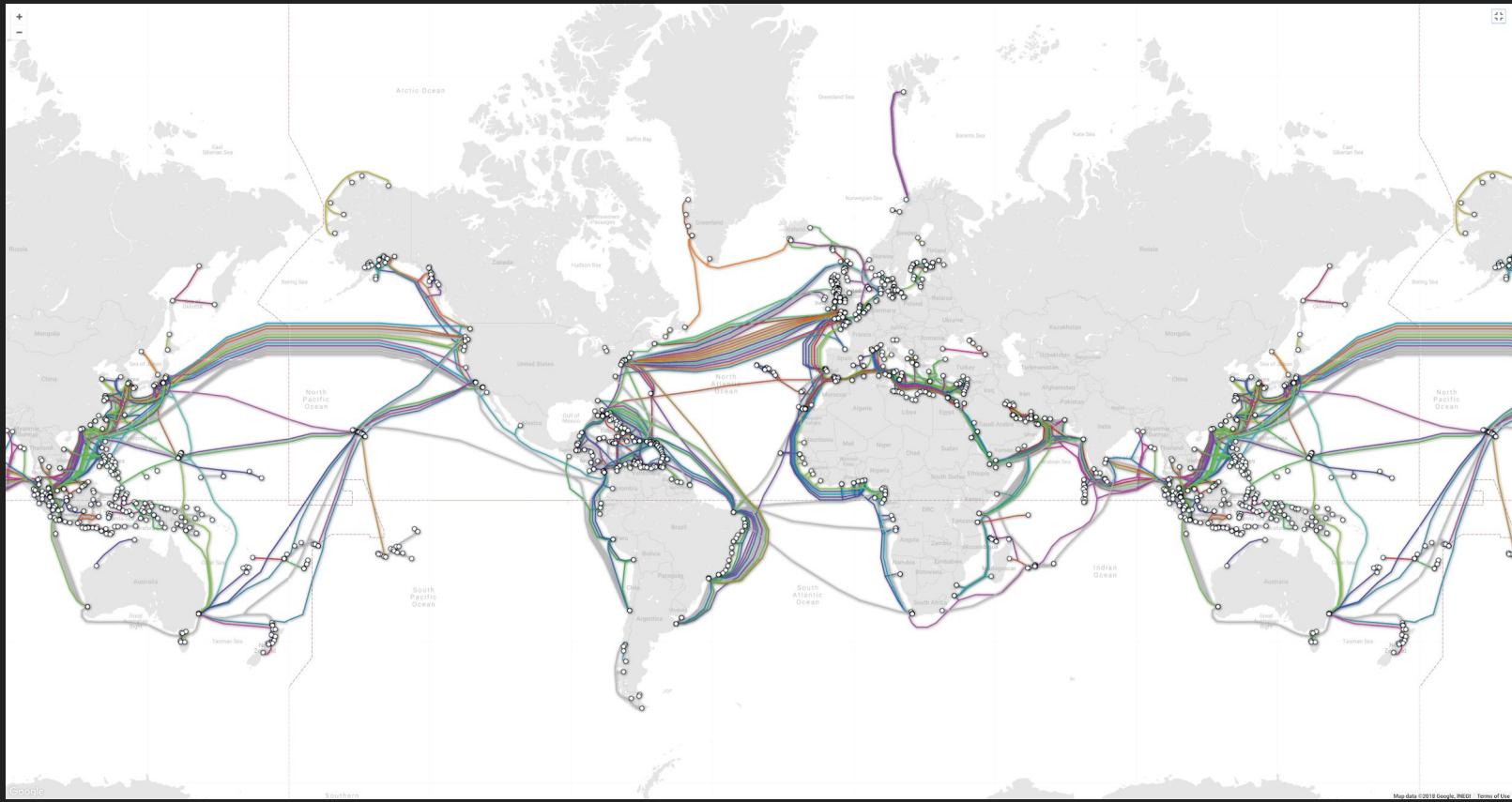
**The fastest web crash course ever**

# What language does the web speak?

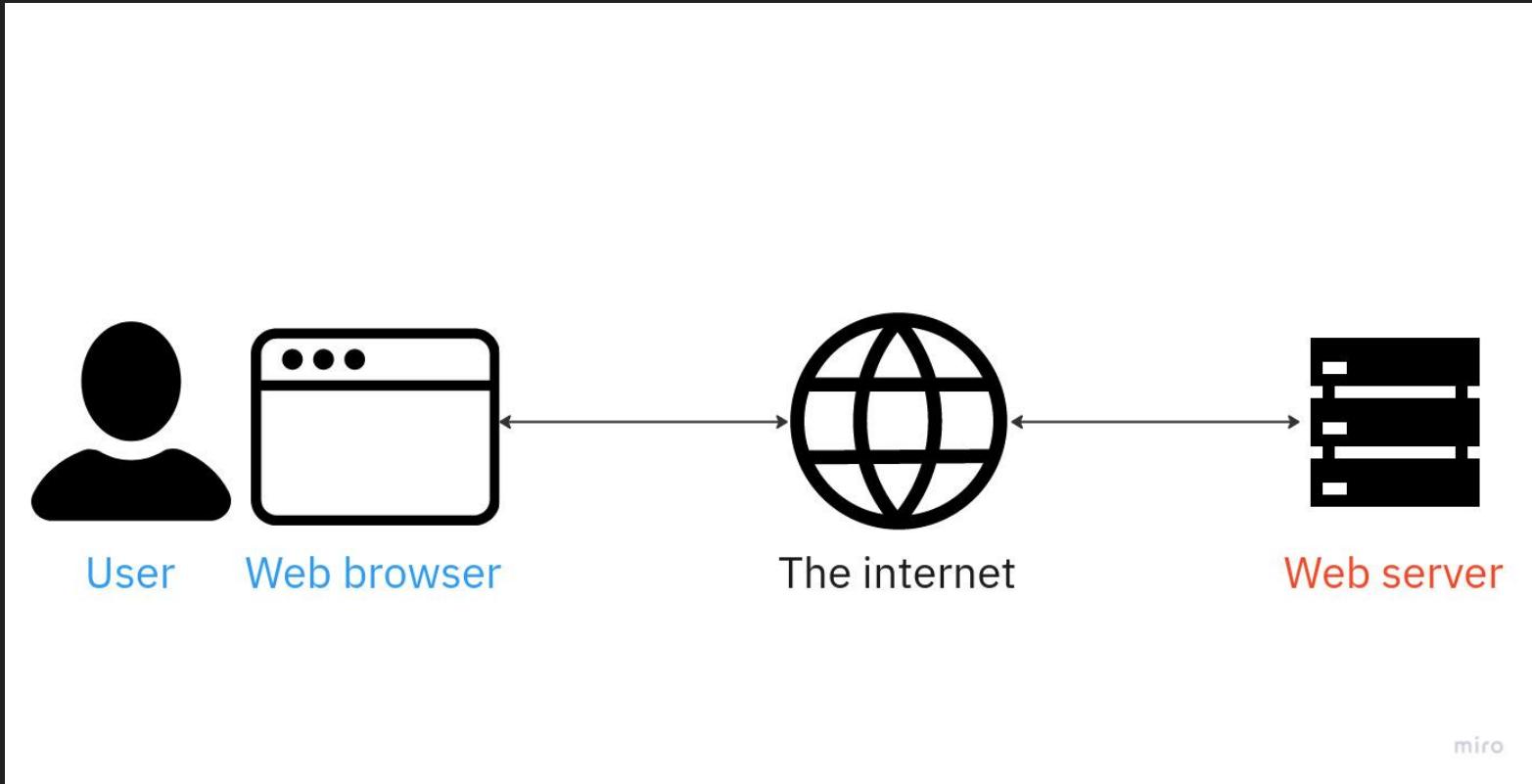
<body>  
<div>  
<h1>

```
26 .screen-reader-text:hover,  
27 .screen-reader-text:active,  
28 .screen-reader-text:focus {  
    background-color: #f1f1f1;  
  
0, 0, 0.6);  
  
<link rel="stylesheet" href="http://localhost/css.css" type="text/css" />  
<script type="text/javascript" src="http://localhost/javascript.js"></script>  
  
10  
11 <script type="text/javascript">  
12     (function(){  
13         onLoaded: function(request) {  
14             if (request.name == 'log_error') return;  
15             log.trace("Ajax.Request: " + (request.name || request.url.substr(0, 30)  
16             ) + "...");  
17         },  
18         onComplete: function(request) {  
19             if (request.name == 'log_error') return;  
20         },  
21         onException: function(request, e) {  
22             if (request.name == 'log_error') {  
23                 log.error(request.url + ': ' + e.name + ' | ' + e.message + ' | ' +  
24                 e.stack);  
25             }  
26         },  
27     })();  
28 </script>  
29  
lbar. */
```

# How does the Internet work?



# Our Internet Abstraction



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

Verb

Object (noun)

Protocol

# 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



The diagram illustrates an HTTP request. It features a yellow arrow pointing left from the word "Request" to the "GET / HTTP/1.1" line. Another orange arrow points left from the word "Headers" to the "Host:" line. A third orange arrow points left from the word "Headers" to the "Upgrade-Insecure-Requests: 1" line.

# HTTP Responses

HTTP/1.1 302 Found

Response Code

Date: Mon, 02 Apr 2018 02:37:56 GMT

Headers

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">

Body

<html><head>

<title>302 Found</title>

</head><body>

<h1>Found</h1>

<p>The document has moved <a

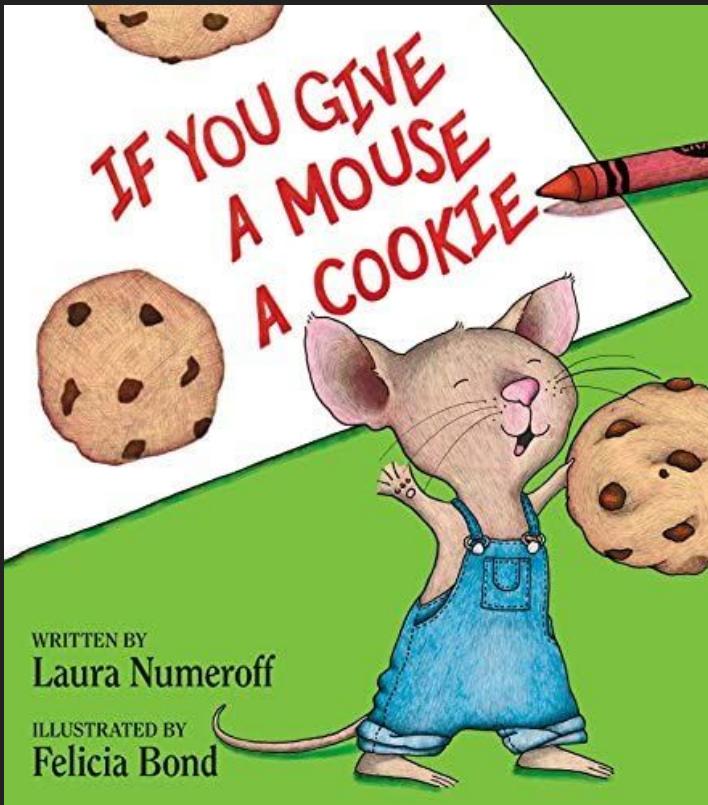
href="https://www.stanford.edu/">here</a>.</p>

</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!**
- 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

# Common insecure design patterns

# CatShare

<http://catshare.saligrama.io>

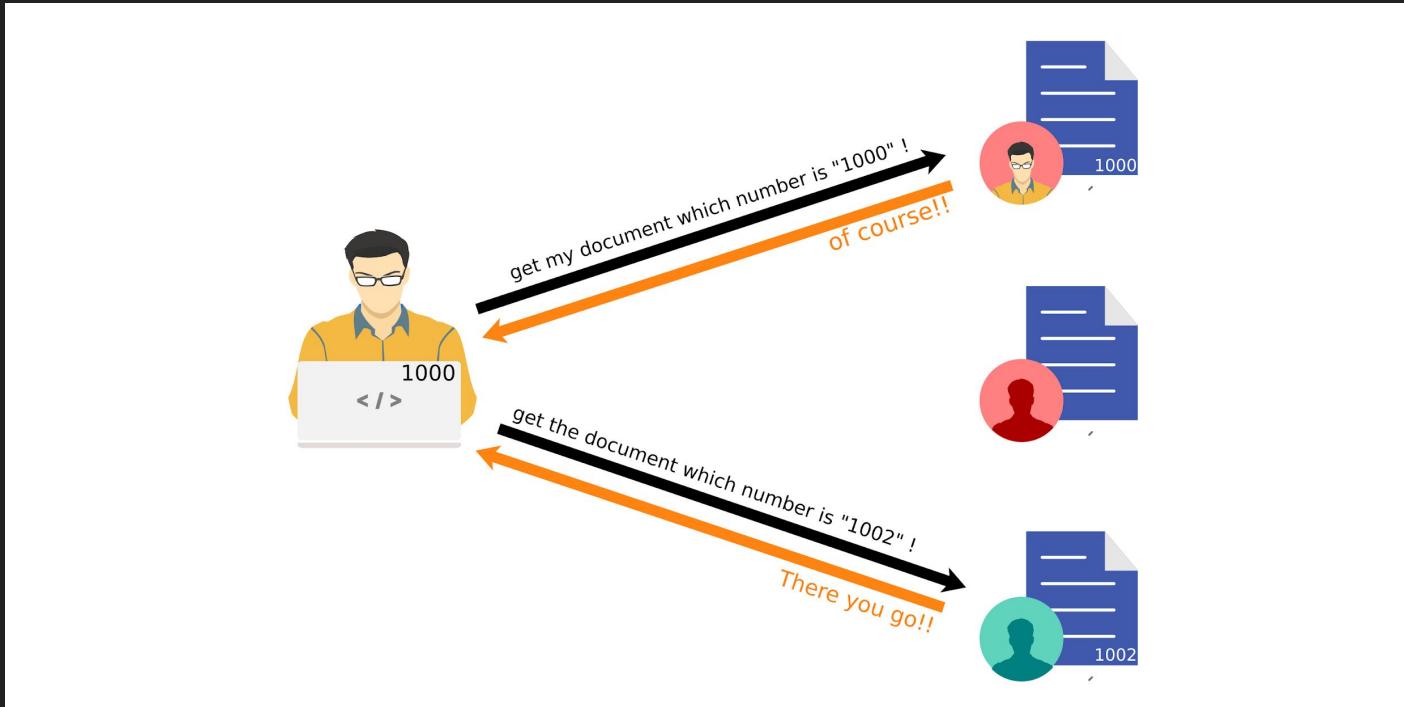


# Vulnerabilities

- 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



# IDOR case study I: Parler

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



# TRY IT!

- The CatShare team has a website <http://catshare.saligramma.io/> that **stores personal information**
- There's an endpoint <http://catshare.saligramma.io/user> to access this info
  - e.g. <http://catshare.saligramma.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 us 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**

# IDOR case study II: Stanford Marriage Pact (2020)

<https://mp.com/29d2223b196d87e8e9292308c074e593>

**29d2223b196d87e8e9292308c074e593**

mccain@stanford.edu

saligramam@stanford.edu

MD5

**65af214d836bb936fd32c5c11f93c70d**

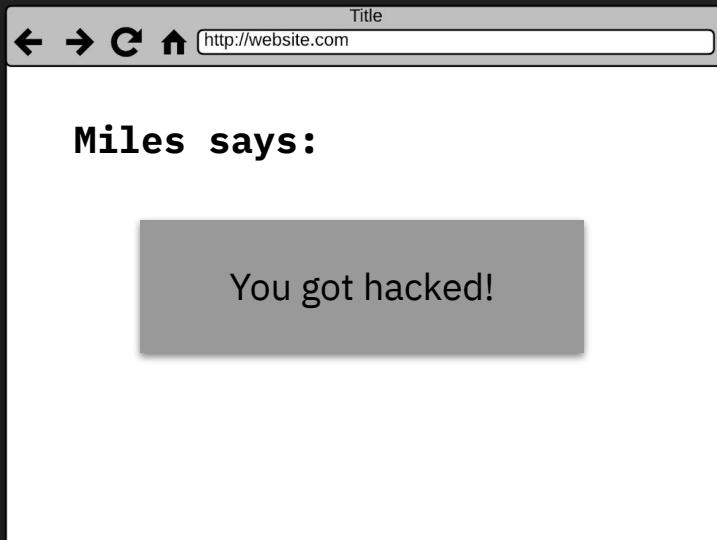
<https://mp.com/65af214d836bb936fd32c5c11f93c70d>

MD5

# 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)



GET /myfeed

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

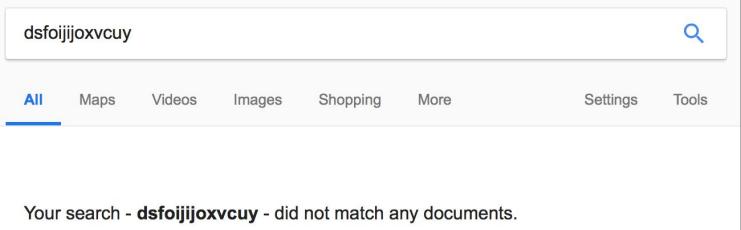
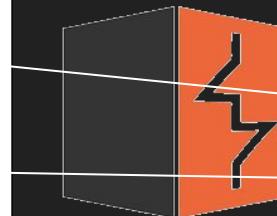
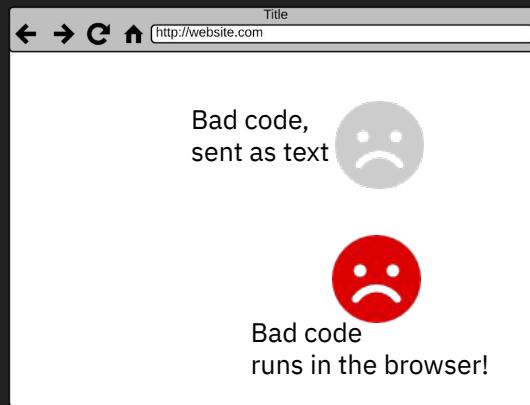
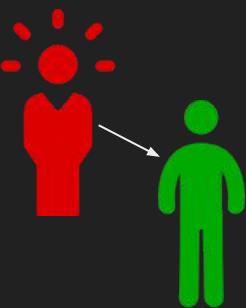
<b>Miles says:</b>
<script>
    alert("You got hacked!");
</script>

</body>
</html>
```

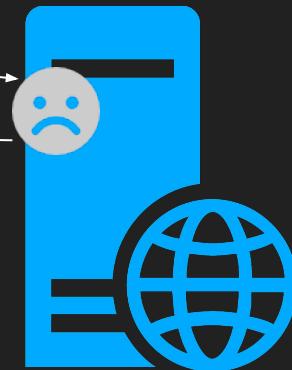


# Reflected XSS

Hey, click  
this link

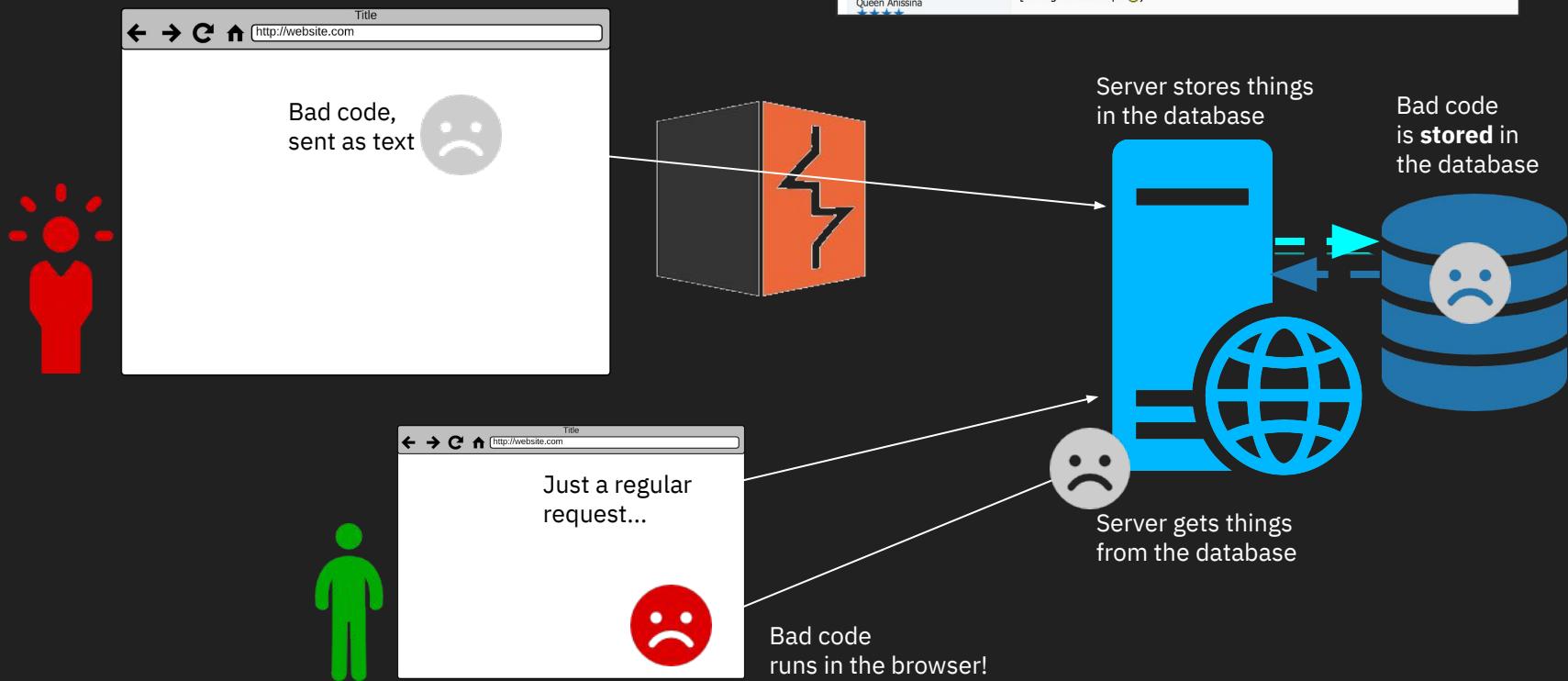


Bad code  
is **reflected**



[https://vulnerable.website/search?query=<script>alert\('pwned'\)</script>](https://vulnerable.website/search?query=<script>alert('pwned')</script>)

# Stored XSS



[www.yourwebsite.com/law/<?StealAllTheData.js>/supersecretdata](http://www.yourwebsite.com/law/<?StealAllTheData.js>/supersecretdata)

# 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 <http://catshare.saligrama.io/hello> that takes a user's name and greets them kindly. Ya' know, to show we care
  - e.g. <http://catshare.saligrama.io/hello?name=User1>
- We think this is harmless and will only build customer trust. **Show us our mistake.**

# XSS on Tweetdeck

 \*andy  
@derGeruhn

[Follow](#)

```
<script
class="xss">$('.xss').parents().eq(1).find('a')
.eq(1).click(); $('[data-
action=retweet]').click(); alert('XSS in
Tweetdeck')</script> ❤
```

[Reply](#) [Retweet](#) [Favorite](#) [More](#)

---

RETWEETS **39,868** FAVORITES **3,686**



9:36 AM - 11 Jun 2014

# Improper session handling

## *Cookie itself is insecure*

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

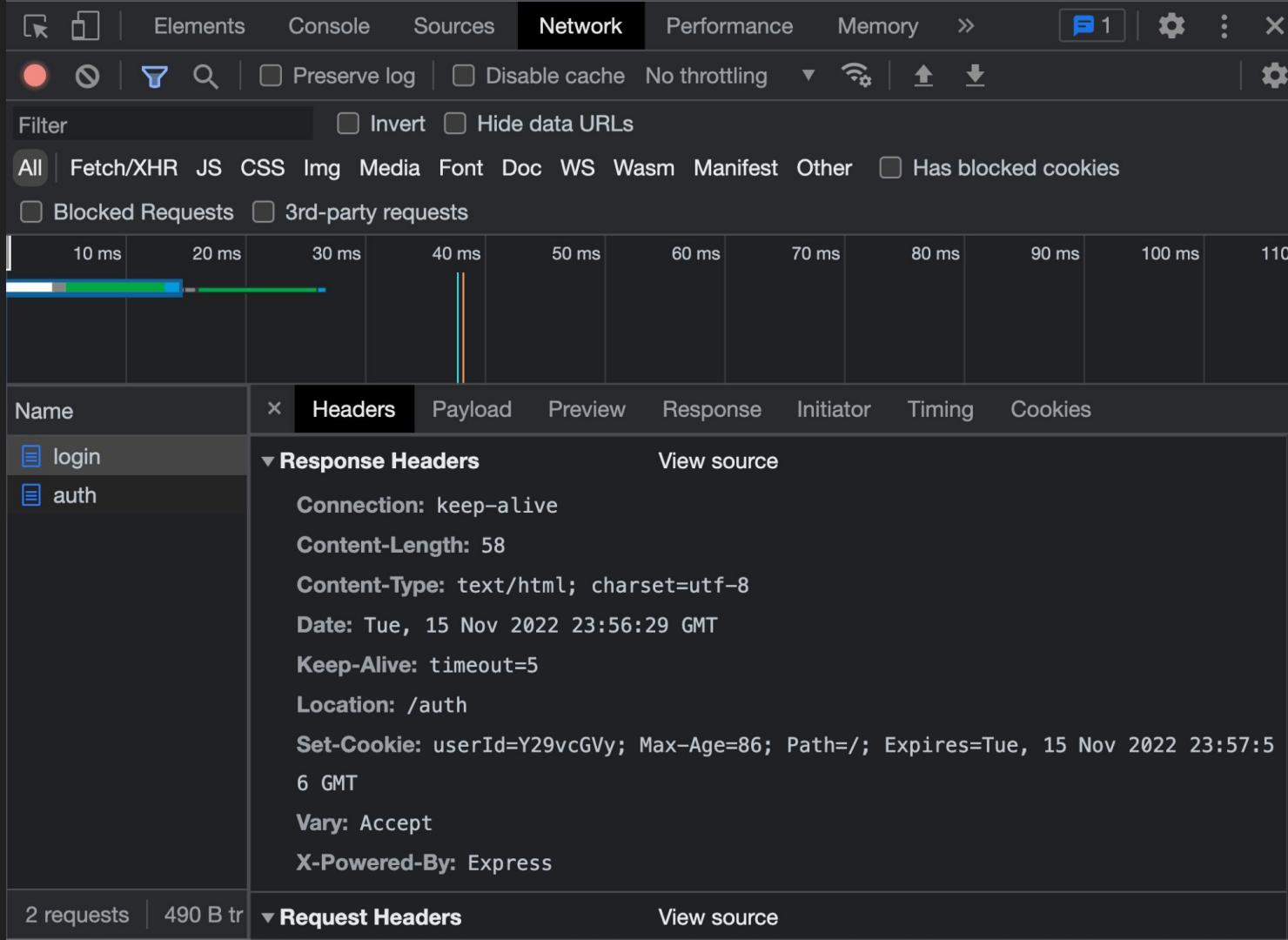
## *Cookie not checked for authorization*

- Use your own account to
  - Impersonate someone else
  - Escalate privileges to admin

Consequences are IDOR-like, even when resource IDs are randomized

# Improper Session Handling

- CatShare added an **admin view** to <http://catshare.saligrama.io/login> for admins to **view user data**
- One set of credentials is **cooper:cooper**
- Can you become **admin** and view the user data?
- **Some handy tools:**
  - Your browser's Developer Tools (accessible from Inspect Element)
  - <https://kk.lol> (Base64 Encode/Decode)



You are cooper. Sorry, you do not have admin access to this endpoint. [logout](#)

The screenshot shows the Chrome DevTools interface with the Application tab selected. On the left, the Storage panel is open, showing sections for Manifest, Service Workers, Storage, and Cookies. The Cookies section is expanded, and a cookie from the domain `http://catshare` is selected. The main pane displays a table of cookies with columns for Name, Value, Domain, and various flags like HttpOnly and SameSite.

Name	Value	Domain	P..	E..	S..	HttpOnly	S	S	S	P	P
userId	Y29vcGVy	catshare.salig... .saligrama.io	/	2...	14						M..
_ga_GJHJW3...	GS1.1.16...	.saligrama.io	/	2...	51						M..
_ga	GA1.1.94...	.saligrama.io	/	2...	29						M..

**Select a cookie to preview its value**

# Session handling case study: Kontra (2022)



# Session handling case study: Kontra (2022)

Request

Pretty	Raw	Hex
1 GET /prod/users/ae697870-3e71-4a0e-bd5e-5ea501a62dd0/topics/interests?interested=true&pageCount=40&pageNumber=0	HTTP/2 200 OK	
2 Host: api.disonantchart.com	Date: Sat, 30 Apr 2022 23:49:03 GMT	
3 Accept: application/json	Content-Type: application/json	
4 Accept-Encoding: gzip, deflate	Content-Length: 3193	
5 X-Amzn-Requestid: 3df951c1-dd44-4b7a-a673-233600fee23c	X-Amz-ApiSig-Id: RayUe0qPHf7uw=	
6 X-Amzn-Trace-Id: Root=1-626dcace-49a709e825a5074c62a15706; Sampled=0		
7 Authorization: eyJraW01013Xjd1zodkE2a2rNaZwPsdrn/GMXZxV2ElxEyTjRmOfJpdah1fDcz0EM4K2o0PSIsImFsZyI61lJTmU2In0.eeyJzdWIiOiIyIjY1MjMzO1I0uH03L0Q3ZCt0TkwyY11Mw1IiMwRNjg3NTMhLc1j0wPf9Z2XjPzm1ZlCf6dH3zSw1i3V3Zdg9t0nRiVxN1lc1k1kjoiZjM2n2BeZDMNj02MS000We2LTk0TEtMddkZTlZm1kNDMyliwiaxNh1j0iaHR0cHM6xC9cl2NvZ25pdG8taWlwLnVzLxd1c3Q0tM5hbWf62hd3MuV29tXc1y13ZXN0LTfjN0LwCTV1Yw3i1wiV29nRml0bz1c2VbymfTzS16nR32WVkbGVxZu1lCjnaZLb19uYw11jijoiVHDl2wzsZS1sImF1ZC161jdh2ty0GcqWVmfcGgy3BvbH3jDTc4Mjkj1wiXZx1bnRfaWQ1013ZTQ3NzE5M0C0MTg2L7Q2NDM6OTcXN1h1Ztg2ZDkz0GMhNz1lCj0b2t1b191c2U0i0j3pZC1sImF1dGhfdfG1Lz16MYTM7MTM2tCM4lw1Zxhw1joxNjxUmx21MyzgjLCpJYXQ1j0E2NTEZn1z30Di1mzbhWlsve9uyW11jijoiRGV1liw1Zwhaw101j0d2v1Z6x1QhNhb6lcmFTy5p5byj9.aE1UQzut4SLQR1SKrnbjmcfDeVse19GKXTV1RQf6u_ZH09q9LnhDbu1F1Qpdpa0CQz06p-tvYzajpsj17Re1xbVmP9a87FvhqRVyD2g90-ykAcA1-K1N1N01xGMmdaa3TyxrgpBA_ZzT1lM0B8Jb2-vGu63zYq5In0XtkF461B6gPha5K1RPjhDheh1T2su_g7145mXPDVdEog65j)DelowbRtBhNMptkLyPA6N4KKVfwz-5qxJNebffqZj3qeyhgg6xzz-pw8Hws2npl4ImZNVeqawd5PE9VxanW16axRFwDC0-ed3cyUYToT87LmEkiLsvp93ZFQw		
8		
9		

Tweedledum's UUID

Response

Pretty	Raw	Hex	Render
1 HTTP/2 200 OK			
2 Host: api.disonantchart.com			
3 Content-Type: application/json			
4 Content-Length: 3193			
5 X-Amzn-Requestid: 3df951c1-dd44-4b7a-a673-233600fee23c			
6 X-Amz-ApiSig-Id: RayUe0qPHf7uw=			
7 X-Amzn-Trace-Id: Root=1-626dcace-49a709e825a5074c62a15706; Sampled=0			
8			
9			

```
{ "userId": "ae697870-3e71-4a0e-bd5e-5ea501a62dd0", "topicId": "c4d7a095-d25f-4ce7-b795-0c48b4aac899", "interestLevel": "No", "createdDate": "2022-04-30T23:44:09.221Z", "topicDescription": "Will China and the US go to war before 2030?", "topicOwner": null, "topicOwnerUsername": null, "topicCreatedDate": "2022-04-23T06:42:24.928Z", "interestCount": "3", "yesCount": "1", "noCount": "2", "commentContent": null }, { "userId": "ae697870-3e71-4a0e-bd5e-5ea501a62dd0", "topicId": "a58c6978-c1f7-400c-81f8-d3f54ce503a3", "interestLevel": "Yes", "createdDate": "2022-04-30T23:44:08.027Z", "topicDescription": "Can an atheist and a deeply Christian person be happily married?", "topicOwner": null, "topicOwnerUsername": null, "topicCreatedDate": "2022-04-23T06:42:52.386Z", "interestCount": "17", "yesCount": "4", "noCount": "2", "commentContent": null }, { "userId": "ae697870-3e71-4a0e-bd5e-5ea501a62dd0", "topicId": "18d0c112-4678-4525-abd-3b2e3ebbdadd", "interestLevel": "Yes", "createdDate": "2022-04-30T23:44:05.807Z", "topicDescription": "Do you see your political opponents as evil?", "topicOwner": null, "topicOwnerUsername": null, "topicCreatedDate": "2022-04-23T06:44:32.964Z", "interestCount": "13", "yesCount": "2", "noCount": "3", "commentContent": null }, { "userId": "ae697870-3e71-4a0e-bd5e-5ea501a62dd0", "topicId": "a2f3ce7e-6bf7-46c4-aebd-f43417f1b681", "interestLevel": "No", "createdDate": "2022-04-30T23:44:04.683Z", "topicDescription": "Are man buns ever okay?", "topicOwner": null, "topicOwnerUsername": null }
```

Tweedledee's Authorization header

Exposure of Tweedledum's votes

# Session handling case study: Kontra (2022)

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 POST /prod/users/ae697870-3e71-4a0e-bd5e-5ea501a62dd0/topics/suggestions HTTP/2				1 HTTP/2 200 OK			
2 Host: api.dissonantchat.com				2 Date: Sat, 30 Apr 2022 23:31:22 GMT			
3 Accept: application/json				3 Content-Type: application/json			
4 Content-Type: multipart/form-data				4 Content-Length: 2			
5 Accept-Encoding: gzip, deflate				5 X-Amzn-Requestid: e4d43f4e-ae61-46be-a8ef-7ee85d32b711			
6 Content-Length: 136				6 X-Amz-Apigw-Id: Rav_pFhXPHcFc2w=			
7 User-Agent: kontra/1.0.0 CFNetwork/1240.0.4 Darwin/20.6.0				7 X-Amzn-Trace-Id: Root=1-626dc6ca-1155462368d318260056d370;Sampled=0			
8 Accept-Language: en-us				8 {			
9 Authorization:				9 }			
eyJraWQiOjXjd1ZodEk2aRnazVsdxVGmxZv2E1aXEyTjRmOFJpaDh1dFcz0EM4K2o0PSIsImFsZyI6IlJTMjU2In0.eyJzdWIiOiIYjY1MjMzOS1hODU3LTQ3ZTct0Tkwy1lMWl1MWRlNjg3NTMiLCJlbWFpbF92ZXJpZmlzC16dHJ1ZSwiY3Vzdg9t0mRivXNlcLkIjoiZjM2NzBmZDMtNjQ2MS000WEzLtk00TEtMDdkZTjlZmjkNDMyIiwiakXnZljoiaHR0CHM6XC9cL2NvZ25pdG8taWRlwLnVzLxdlc3QtMi5hbWF6b25hd3MuY29tXC91cy13ZkN0LTJfn0lwciYmW3IiwiY29nbml0bzp1c2VybmfZSI6InR3ZWVkbGVkZWUiLCJnaXZlb1l9Y1lIjoiVHdLZWRsZSIsImF1ZC16Ijdhb2ty0GtqYWfmGgzY3BvbHJtdTc4mjkyIiwiZXZLbnkfaWjoiIwNDdjNGRLNC00YzM3LTQwNzYtODRknS1jYTUXNjVmM2NjY2iLCJob2tlbl91c2Ui0iJpZCIsImF1dGhfGltZSI6MTY1MTM2MTI4NywiZXhwIjoxNjUxMzY00Dg3LCJpYXQiOjE2NTezNjEy0DcsImZhbWLseV9uyW1lIjoiRGV1IiwiZWlhaWwiOj0d2VLZgxLZGVlQHNhb6lncmFtYS5pbjJ9.dsWbgWFAl_hAK0WE3m088jklkuUhDA5Uw2aICYqUKwPRrusLHujmYoZmCjIh0tpyx05diu9cMM9dDI7oA-g6rx8sll-lAdU--R-n4__IG1V4mNuHNLyossg2rBZY_yHousS9uAqmVKL5MeGf1Vo8z6B9_8k1hxLlgl1wtRo8eqLmiGYKxfSC4y1gafZjIIRcxL6nphrFGMhlLRBo0CmYx674v2czIk9AMMXNZZe8Up7lvT8gpucpty1MNLFGnd2N4she2c5xajMouuC1b3aPlw-3Br4TYct9DkGfSG80wLbzgcIFVzzdaoJWwXVBy8GqQvuAN56SDWRXZRlaxqA							
10 {				11 Tweedledee's desired poll content			
11 "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

# Session handling case study: Kontra (2022)

Verizon

4:36 PM

79%

Welcome back, **tweedledee**

Hot

New

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



**@tweedledum**

1 Reacts · 5m



# Mitigating risk as a startup

Nothing is 100% secure

# It happens to the best of us

## Aditya's Blog

Thoughts, guides and fun from a security/systems enthusiast @ Stanford

### Flipping the script: when a hacking class gets hacked

October 12, 2022    1316 words    No tag

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.

# Let the community help you

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

# Vulnerability Disclosure Policy Resources

DHS Template: <https://cyber.dhs.gov/bod/20-01/vdp-template/>

DoJ Framework:

<https://www.justice.gov/criminal-ccips/page/file/983996/download>

HackerOne:

<https://www.hackerone.com/blog/What-Vulnerability-Disclosure-Policy-and-Why-You-Need-One>

Example Safe Harbor: <https://github.com/cybertransparency/vdp-terms>

# Please don't do this

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.

# **More Security at Stanford**

# Courses

- *INTLPOL 268*: Hack Lab
- *CS 152*: Trust and Safety Engineering
- *CS 155*: Computer and Network Security
- *CS 255*: Cryptography
- *CS 153*: Applied Security at Scale
- *CS 253*: Web Security
- *INTLPOL 268D*: Online Open Source Investigation

# More security fun and hijinks: Stanford Applied Cyber

**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)

## Aditya's Blog

Thoughts, guides and fun from a security/systems enthusiast @ Stanford

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

February 28, 2023 2591 words No tag

[applied-cyber.stanford.edu](http://applied-cyber.stanford.edu)



# Check-Off Form

<https://tinyurl.com/106SecurityCheckoff>

# Credits

# Source Code for Vulnerable Web App

<https://github.com/cdenicola/CS106S-VulnerabilityExample>

(sharecat branch)

# 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 articles* – The Stanford Daily
- *CatShare* – Cooper de Nicola, Aditya Saligrama, George Hosono