Bug Hunters dump user data.

Can they keep it?

Well they're keeping it anyway.

Who?

Whitney Merrill

@wbm312

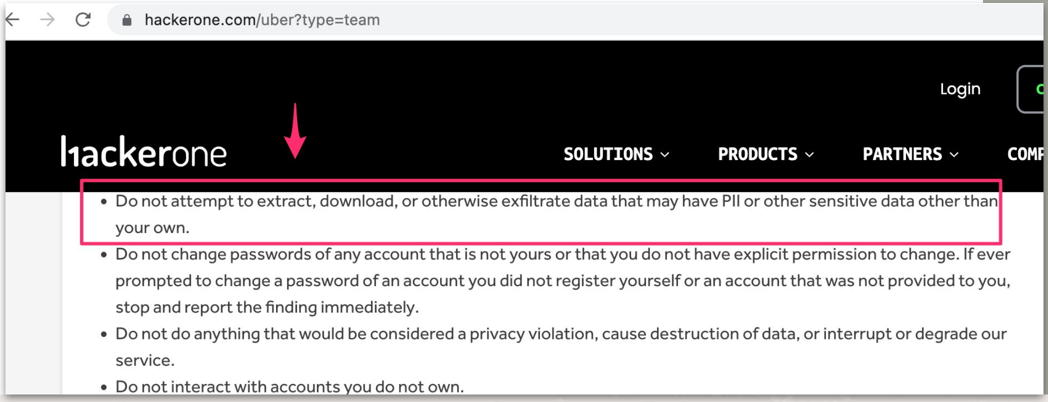
Data Protection Officer & Privacy Attorney - a lawyer, but not your lawyer

Dylan Ayrey

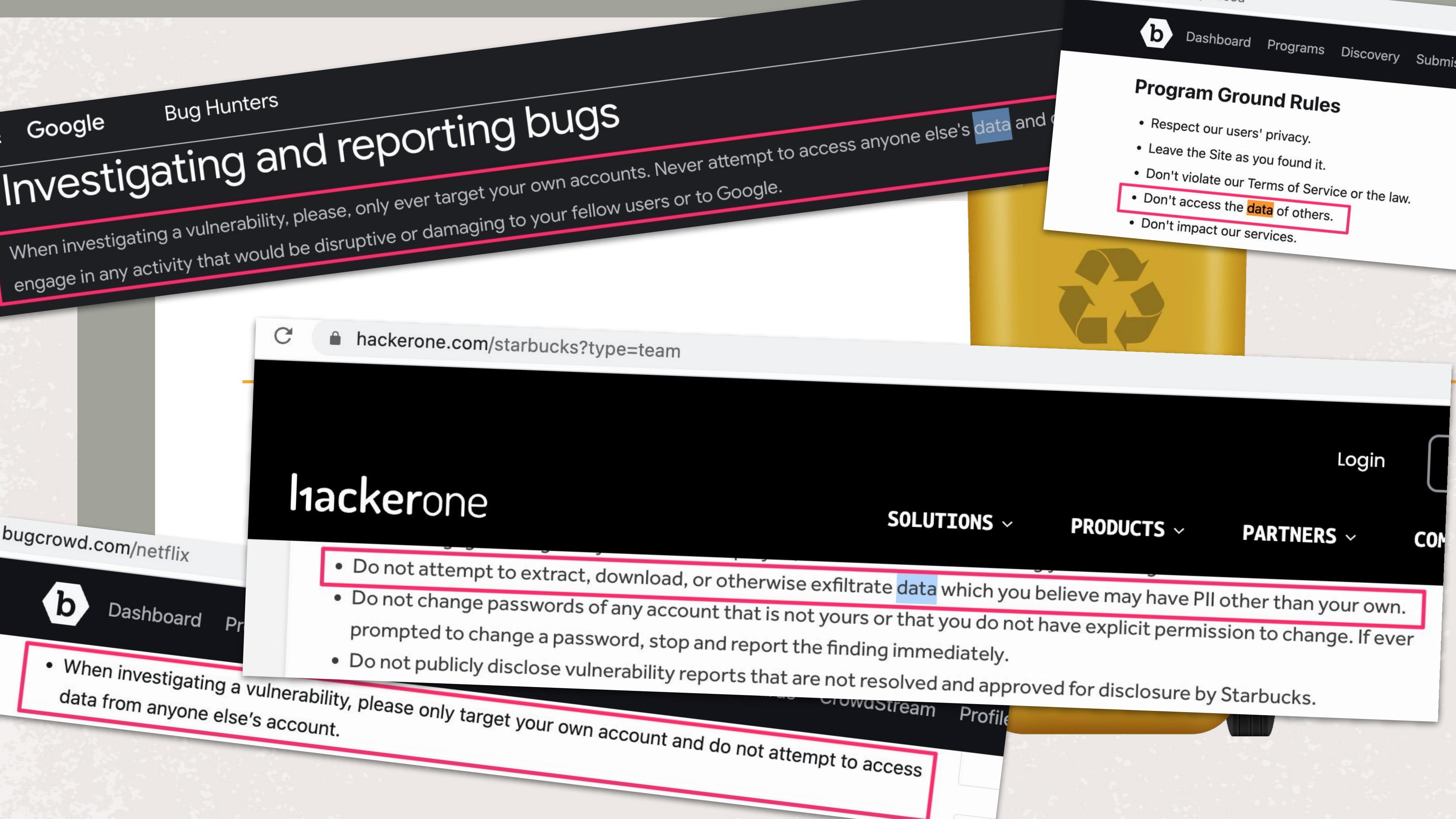
@InsecureNature

Co-Founder of Truffle Security, TruffleHog author, bug hunter, security researcher, etc...

Do bug hunters touch your data?



- Do not attempt to extract, download, or otherwise exfiltrate data that may have PII or other sensitive data other than your own.
- Do not change passwords of any account that is not yours or that you do not have explicit permission to change. If ever prompted to change a password of an account you did not register yourself or an account that was not provided to you, stop and report the finding immediately.
- Do not do anything that would be considered a privacy violation, cause destruction of data, or interrupt or degrade our service.
- Do not interact with accounts you do not own.



Investigating and reporting bugs

When investigating a vulnerability, please, only ever target your own accounts. Never attempt to access anyone else's data and engage in any activity that would be disruptive or damaging to your fellow users or to Google.

Program Ground Rules

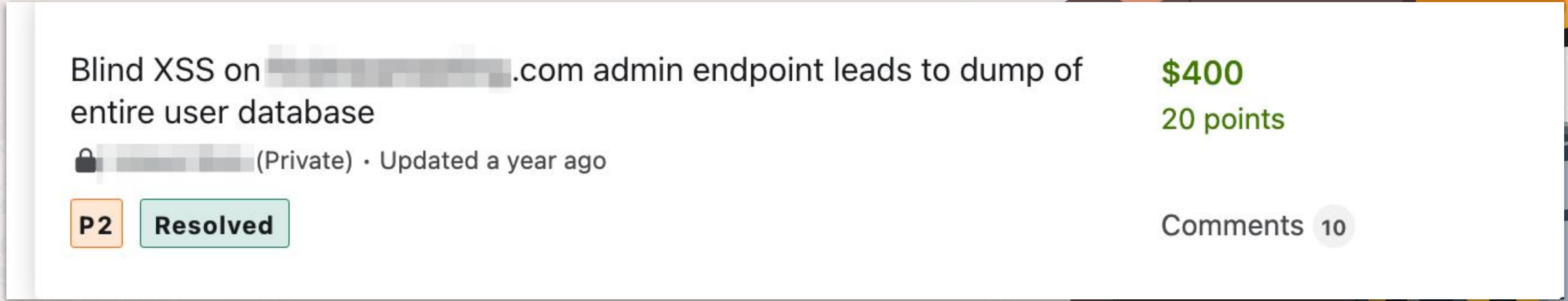
- Respect our users' privacy.
- Leave the Site as you found it.
- Don't violate our Terms of Service or the law.
- Don't access the data of others.
- Don't impact our services.

- Do not attempt to extract, download, or otherwise exfiltrate data which you believe may have PII other than your own.
- Do not change passwords of any account that is not yours or that you do not have explicit permission to change. If ever prompted to change a password, stop and report the finding immediately.
- Do not publicly disclose vulnerability reports that are not resolved and approved for disclosure by Starbucks.

- When investigating a vulnerability, please only target your own account and do not attempt to access data from anyone else's account.

Job done.

Crap.



Blind XSS on [redacted].com admin endpoint leads to dump of entire user database

🔒 [redacted] (Private) · Updated a year ago

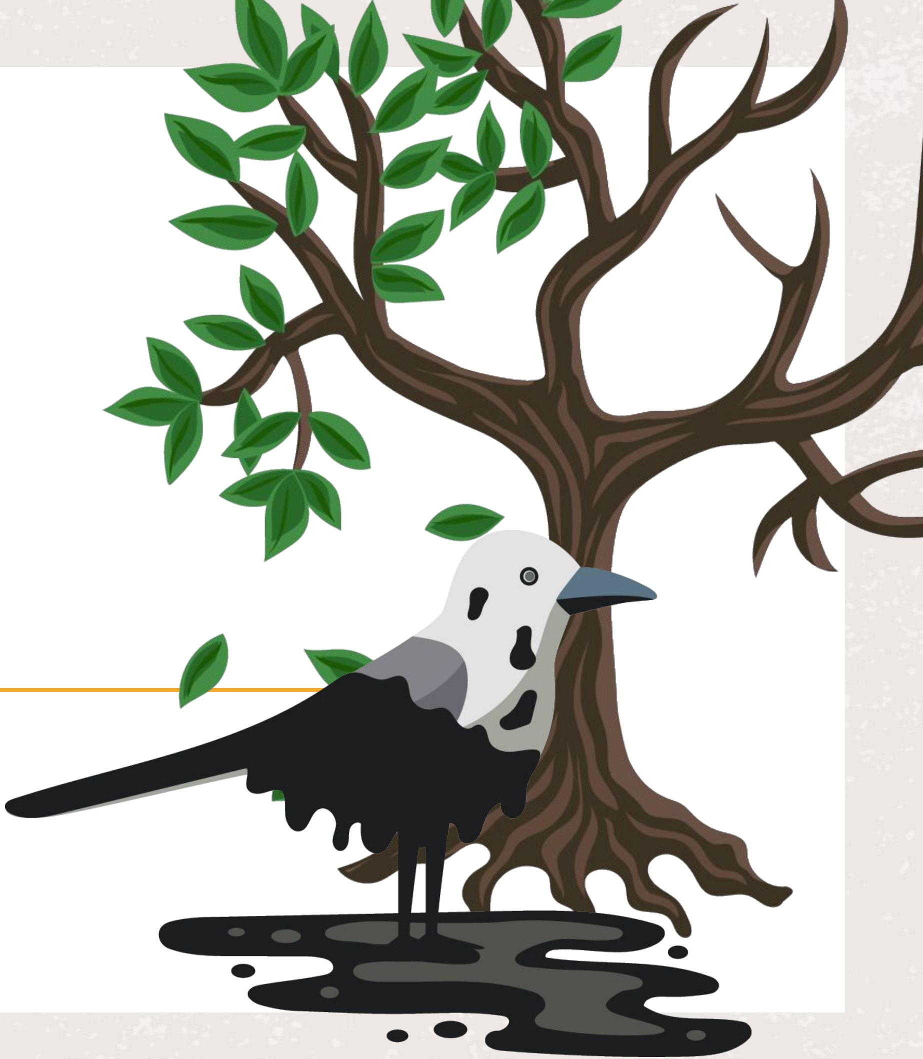
P2 Resolved

$400

20 points

Comments 10

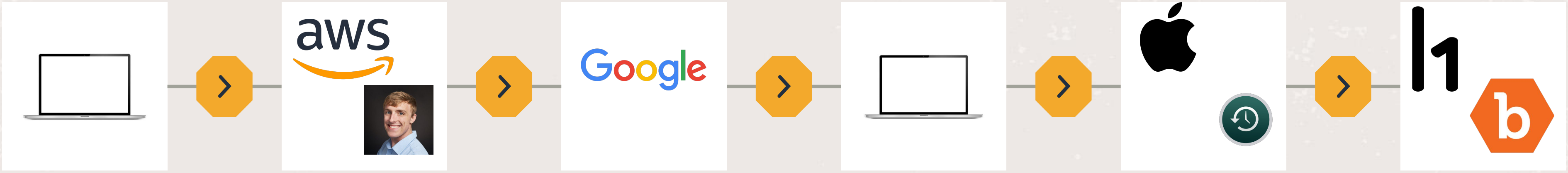
Yes.



Not yet

There’s data everywhere

Data flow diagram



Employee laptop

XSSHunter*

Gmail

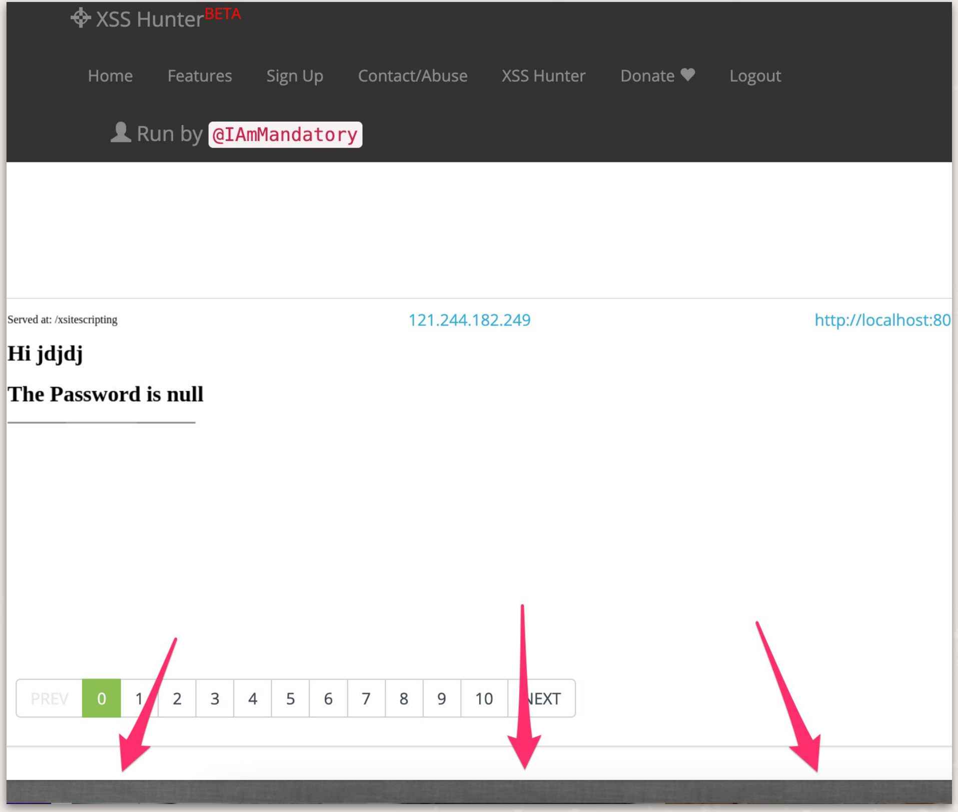
My Hard drive

Time machine

Bug tracker

*and/or other similarly situated third-party tool

XSSHunter isn't clear



Served at: /xsitescripting

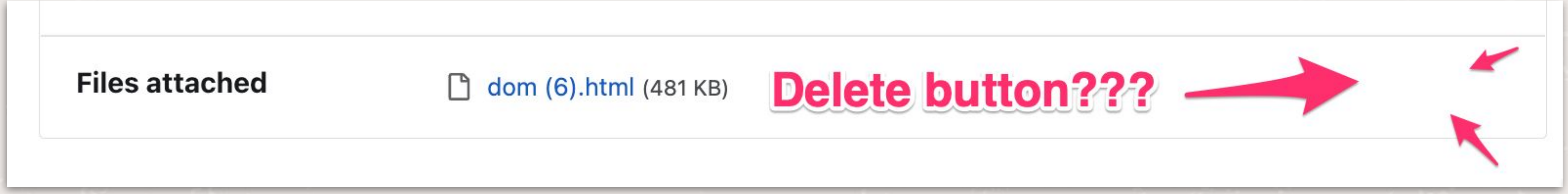
121.244.182.249

http://localhost:80

Hi jdjdj

The Password is null

The bug platform itself



Files attached

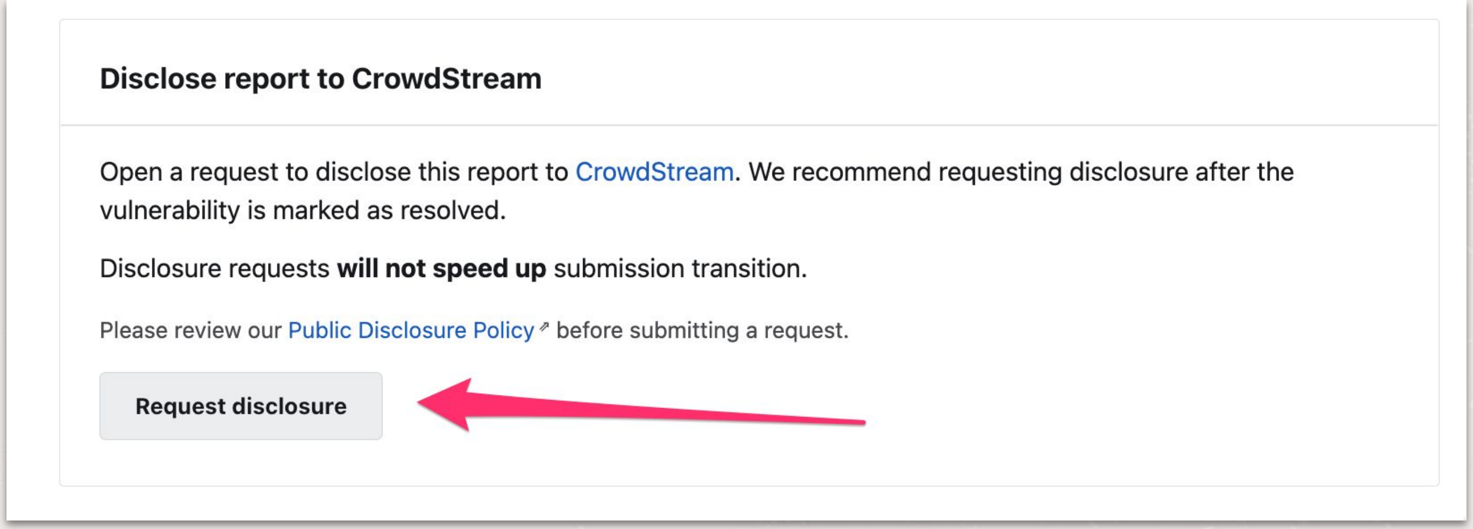
dom (6).html (481 KB)

This incident isn’t isolated

“Uh… yeah”

—All the bug hunters I asked

Never hurts to ask

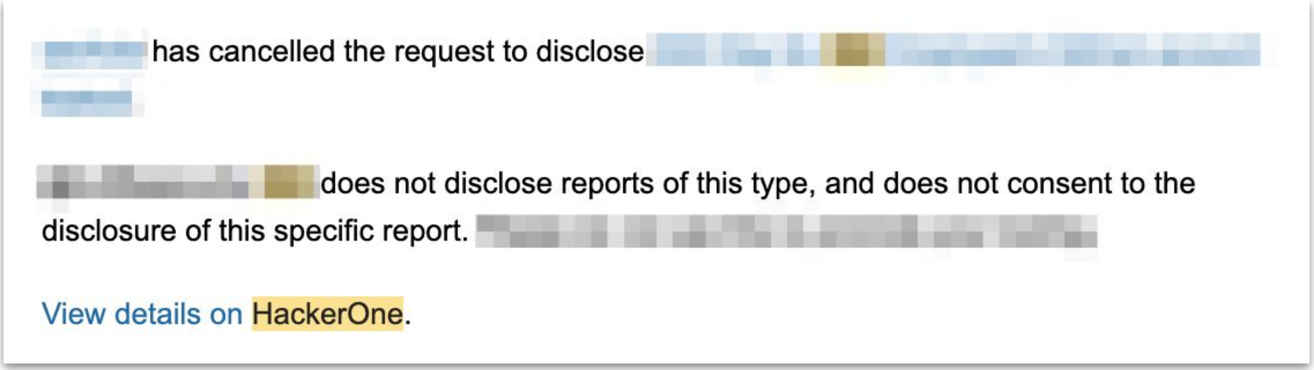


Disclose report to CrowdStream

Open a request to disclose this report to CrowdStream. We recommend requesting disclosure after the vulnerability is marked as resolved.

Disclosure requests **will not speed up** submission transition.

Please review our Public Disclosure Policy before submitting a request.

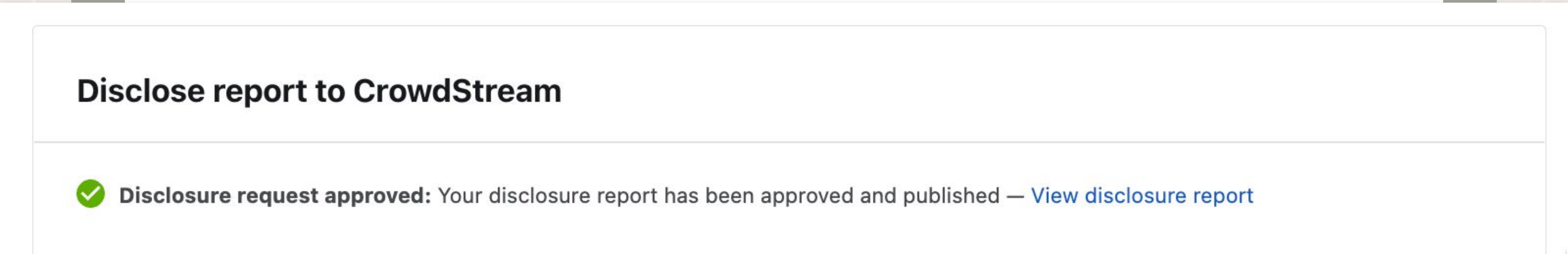


[redacted] has cancelled the request to disclose [redacted]

[redacted] does not disclose reports of this type, and does not consent to the disclosure of this specific report. [redacted]

View details on HackerOne.

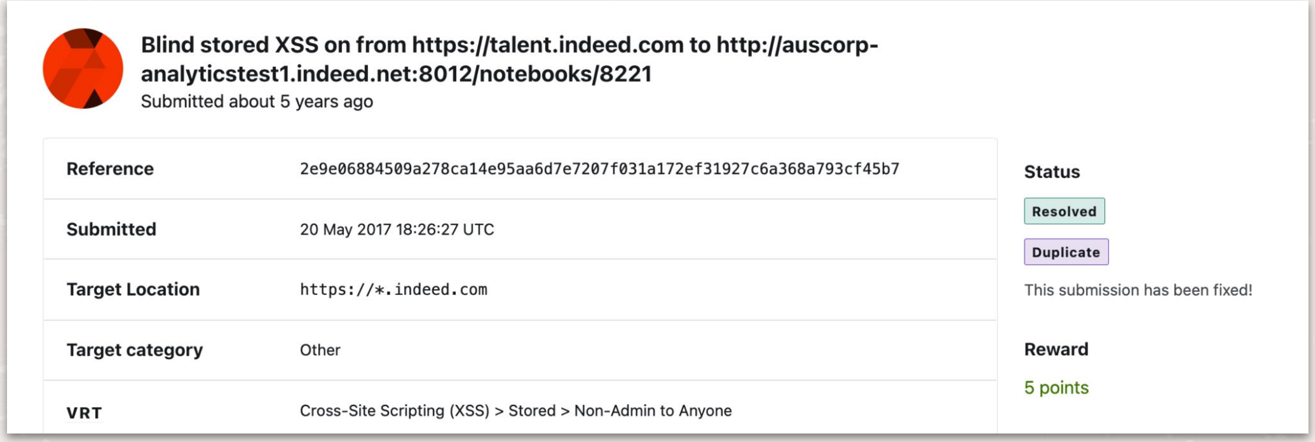
Dang.



Disclose report to CrowdStream

✓ **Disclosure request approved:** Your disclosure report has been approved and published — View disclosure report

Holy crap that worked.



Blind stored XSS on from https://talent.indeed.com to http://auscorp-analyticstest1.indeed.net:8012/notebooks/8221

Submitted about 5 years ago

Reference	2e9e06884509a278ca14e95aa6d7e7207f031a172ef31927c6a368a793cf45b7
Submitted	20 May 2017 18:26:27 UTC
Target Location	https://*.indeed.com
Target category	Other
VRT	Cross-Site Scripting (XSS) > Stored > Non-Admin to Anyone

Status

Resolved

Duplicate

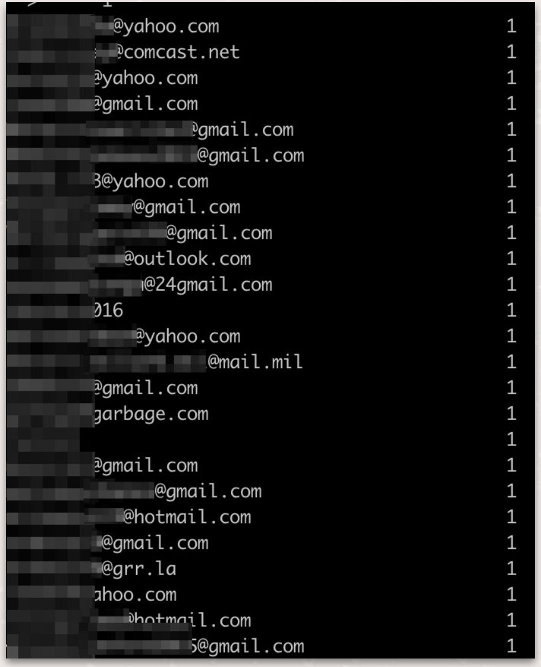
This submission has been fixed!

Reward

5 points

“Your PoC exfiltrated **email addresses** but it seems other PII could have been hypothetically at risk. The user base was relatively small **(a few thousand)** as this was an experimental project."

“Be sure that any **PII** that was in your PoC should **be obfuscated**. We are excited that we can be included in your talk and help give back to the security community."



```
[redacted]@yahoo.com                      1
[redacted]@comcast.net                    1
[redacted]@yahoo.com                      1
[redacted]@gmail.com                      1
[redacted]@gmail.com                      1
[redacted]@gmail.com                      1
[redacted]3@yahoo.com                     1
[redacted]@gmail.com                      1
[redacted]@gmail.com                      1
[redacted]@outlook.com                    1
[redacted]@24gmail.com                    1
[redacted]016                             1
[redacted]@yahoo.com                      1
[redacted]@mail.mil                       1
[redacted]@gmail.com                      1
[redacted]garbage.com                     1
[redacted]                                1
[redacted]@gmail.com                      1
[redacted]@gmail.com                      1
[redacted]@hotmail.com                    1
[redacted]@gmail.com                      1
[redacted]@grr.la                         1
[redacted]ahoo.com                        1
[redacted]@hotmail.com                    1
[redacted]5@gmail.com                     1
```

Asked to delete data?

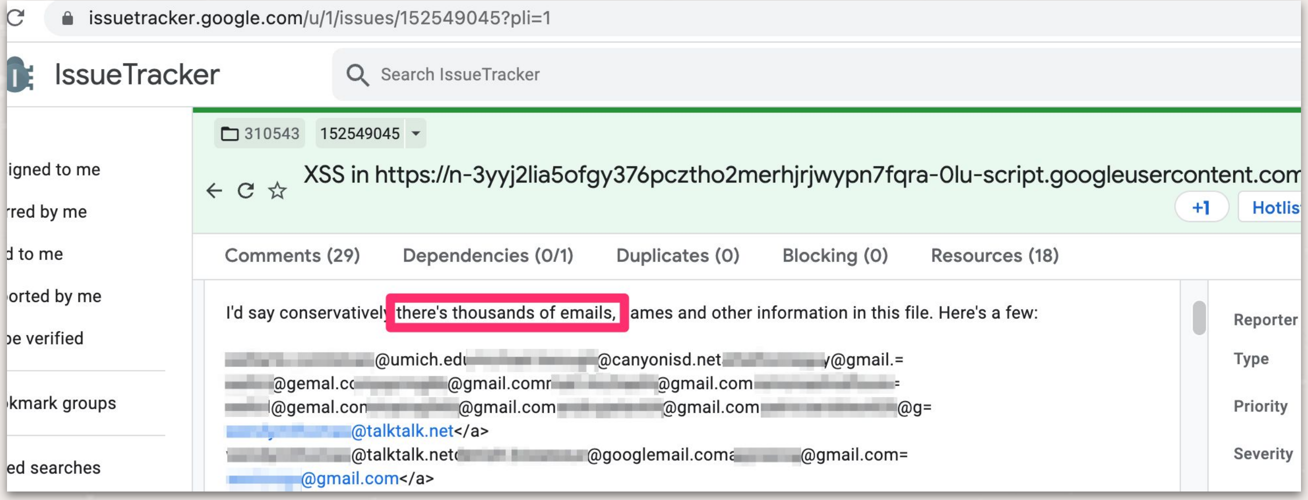
No.

Maintain data access through ticket?

Yes.

Disclosure notifications?

Not to my knowledge.



XSS in https://n-3yyj2lia5ofgy376pcztho2merhjrjwypn7fqra-0lu-script.googleusercontent.com

I'd say conservatively there's thousands of emails, names and other information in this file. Here's a few:

[redacted]@umich.edu[redacted]@canyonisd.net[redacted]y@gmail.=
[redacted]@gemal.co[redacted]@gmail.comr[redacted]@gmail.com[redacted]=
[redacted]l@gemal.com[redacted]@gmail.com[redacted]@gmail.com[redacted]@g=
[redacted]@talktalk.net</a>
[redacted]@talktalk.net[redacted]@googlemail.coma[redacted]@gmail.com=
[redacted]@gmail.com</a>

> “Re: notification. We are following our usual privacy incident process, that includes notification of customers in case it's necessary. **Not sure if it was necessary in this case, our team doesn't see that part of the process."**

Asked to delete data?

No.

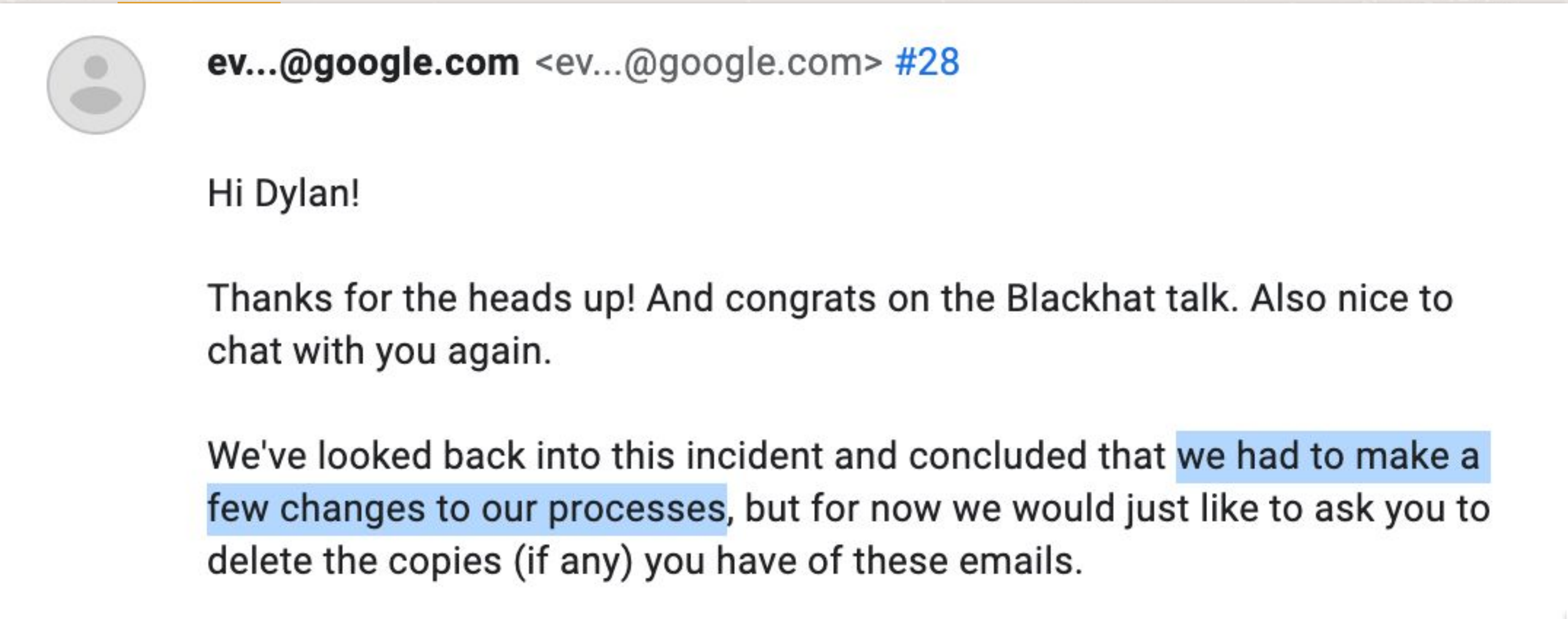
Maintain data access through ticket?

Yes.

Disclosure notifications?

Not to my knowledge.

Wait hold up....

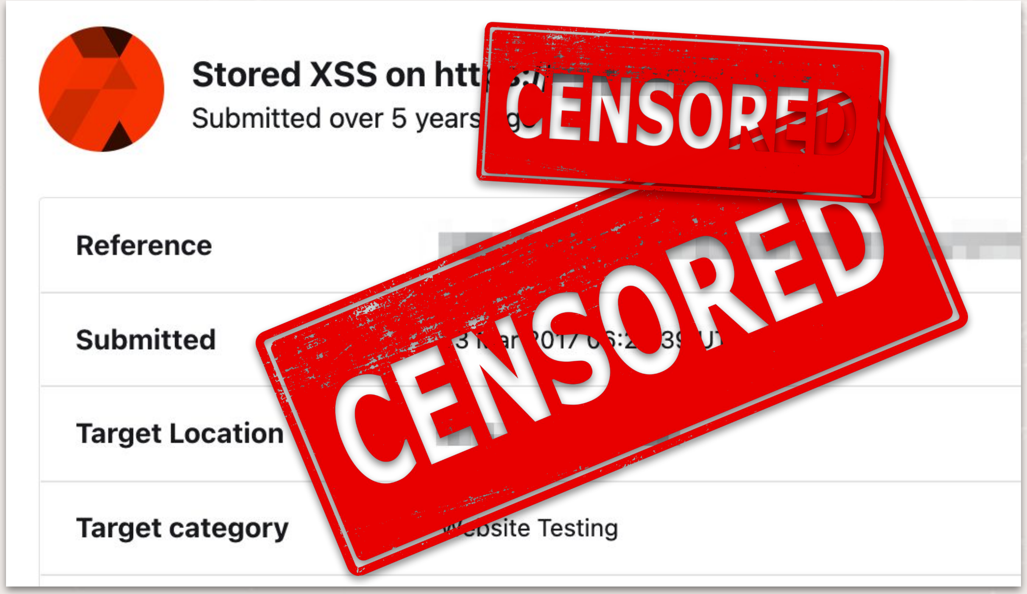


ev...@google.com <ev...@google.com> #28

Hi Dylan!

Thanks for the heads up! And congrats on the Blackhat talk. Also nice to chat with you again.

We've looked back into this incident and concluded that we had to make a few changes to our processes, but for now we would just like to ask you to delete the copies (if any) you have of these emails.



Stored XSS on htt[redacted]

Submitted over 5 years [redacted]

CENSORED

CENSORED

Reference	[redacted]
Submitted	[redacted]
Target Location	[redacted]
Target category	[redacted]ebsite Testing

bigBugGuy sent a message

[redacted]

The affected data [redacted]

[redacted]

Als[redacted] expo[redacted]ed: [redacted] and [redacted] of [redacted]

CENSORED

CENSORED

Asked to delete data?

No.

Maintain data access through ticket?

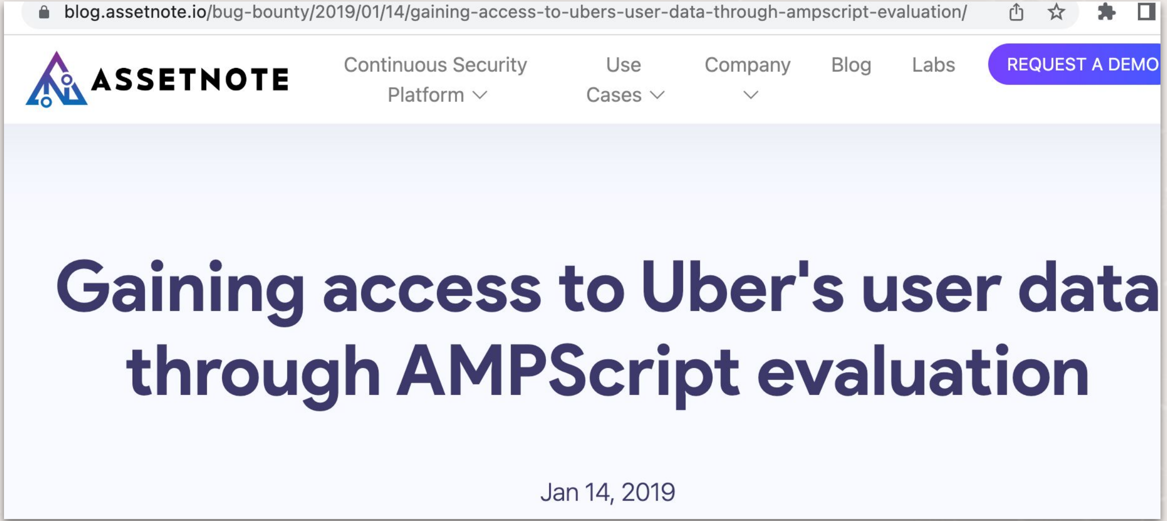
Yes.

Disclosure notifications?

Not to my knowledge.

What about other researchers?

What about other researchers?



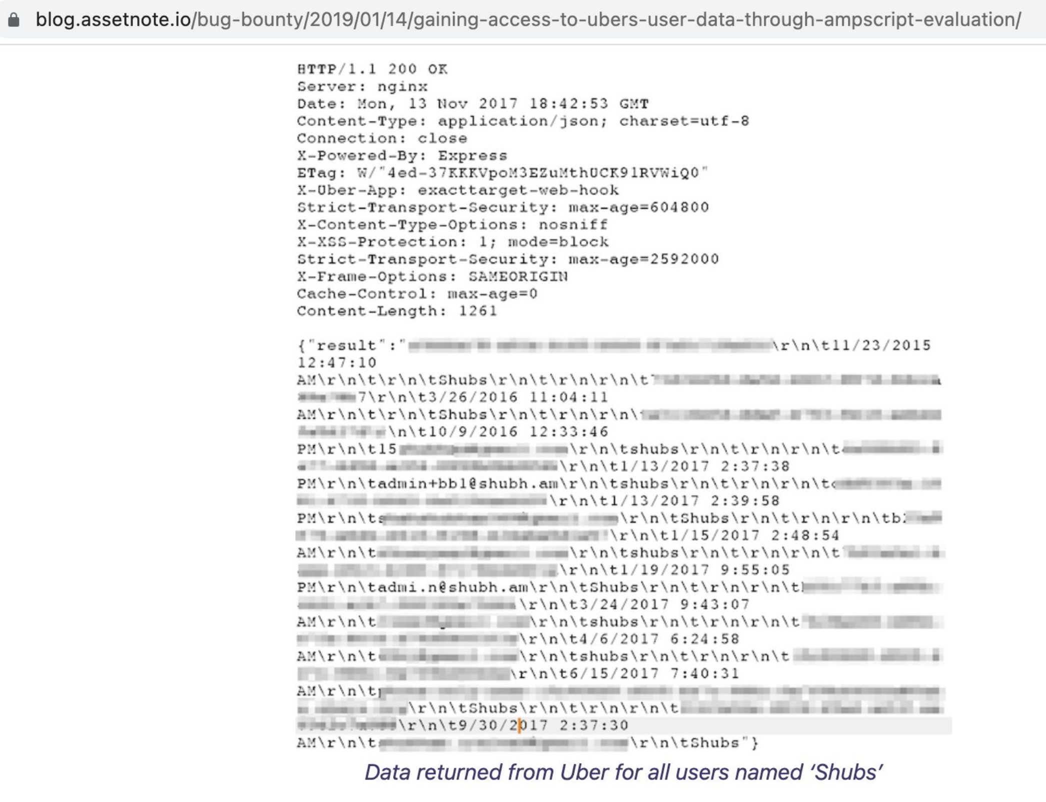
blog.assetnote.io/bug-bounty/2019/01/14/gaining-access-to-ubers-user-data-through-ampscript-evaluation/

Gaining access to Uber's user data through AMPScript evaluation

Jan 14, 2019

https://blog.assetnote.io/bug-bounty/2019/01/14/gaining-access-to-ubers-user-data-through-ampscript-evaluation/

Making it rain Shubs



blog.assetnote.io/bug-bounty/2019/01/14/gaining-access-to-ubers-user-data-through-ampscript-evaluation/

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 13 Nov 2017 18:42:53 GMT
Content-Type: application/json; charset=utf-8
Connection: close
X-Powered-By: Express
ETag: W/"4ed-37KKKVpoM3EZuMthUCK91RVWiQ0"
X-Uber-App: exacttarget-web-hook
Strict-Transport-Security: max-age=604800
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=2592000
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=0
Content-Length: 1261

{"result":"[redacted]\r\n\t11/23/2015
12:47:10
AM\r\n\t\r\n\tShubs\r\n\t\r\n\r\n\t[redacted]
[redacted]7\r\n\t3/26/2016 11:04:11
AM\r\n\t\r\n\tShubs\r\n\t\r\n\r\n\[redacted]
[redacted]\n\t10/9/2016 12:33:46
PM\r\n\t15[redacted]\r\n\tshubs\r\n\t\r\n\r\n\t[redacted]
[redacted]\r\n\t1/13/2017 2:37:38
PM\r\n\tadmin+bb1@shubh.am\r\n\tshubs\r\n\t\r\n\r\n\t[redacted]
[redacted]\r\n\t1/13/2017 2:39:58
PM\r\n\t[redacted]\r\n\tShubs\r\n\t\r\n\r\n\t[redacted]
[redacted]\r\n\t1/15/2017 2:48:54
AM\r\n\t[redacted]\r\n\tshubs\r\n\t\r\n\r\n\t[redacted]
[redacted]\r\n\t1/19/2017 9:55:05
PM\r\n\tadmi.n@shubh.am\r\n\tShubs\r\n\t\r\n\r\n\t[redacted]
[redacted]\r\n\t3/24/2017 9:43:07
AM\r\n\t[redacted]\r\n\tshubs\r\n\t\r\n\r\n\t[redacted]
[redacted]\r\n\t4/6/2017 6:24:58
AM\r\n\t[redacted]\r\n\tshubs\r\n\t\r\n\r\n\t[redacted]
[redacted]\r\n\t6/15/2017 7:40:31
AM\r\n\t[redacted]
[redacted]\r\n\tShubs\r\n\t\r\n\r\n\t[redacted]
[redacted]\r\n\t9/30/2017 2:37:30
AM\r\n\t[redacted]\r\n\tShubs"}
```

Data returned from Uber for all users named 'Shubs'

Asked to delete data?

No.

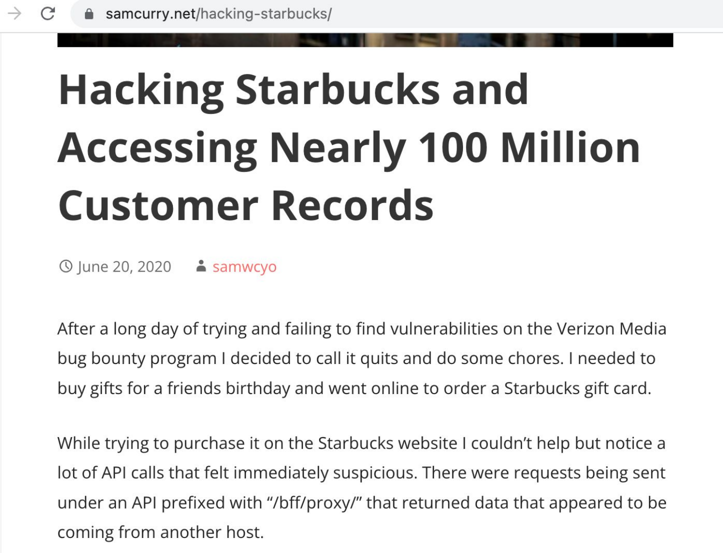
Maintain data access through ticket?

Yes.

Disclosure notifications?

Not to his knowledge.

What about other researchers?



Hacking Starbucks and Accessing Nearly 100 Million Customer Records

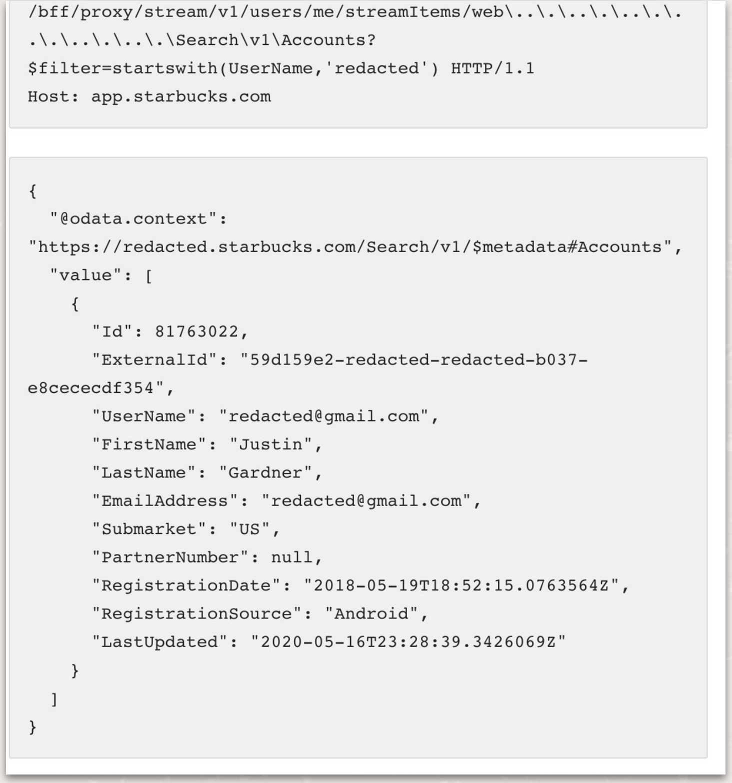
June 20, 2020 samwcyo

After a long day of trying and failing to find vulnerabilities on the Verizon Media bug bounty program I decided to call it quits and do some chores. I needed to buy gifts for a friends birthday and went online to order a Starbucks gift card.

While trying to purchase it on the Starbucks website I couldn't help but notice a lot of API calls that felt immediately suspicious. There were requests being sent under an API prefixed with "/bff/proxy/" that returned data that appeared to be coming from another host.

https://samcurry.net/hacking-starbucks/

““I tried my best to limit is as I didn't want to cause any problems from their side, so I only included like **5-6 other peoples** records”“



```
/bff/proxy/stream/v1/users/me/streamItems/web\..\.\..\.\..\.\.
.\.\..\.\..\.\Search\v1\Accounts?
$filter=startswith(UserName,'redacted') HTTP/1.1
Host: app.starbucks.com
```

```
{
  "@odata.context":
"https://redacted.starbucks.com/Search/v1/$metadata#Accounts",
  "value": [
    {
      "Id": 81763022,
      "ExternalId": "59d159e2-redacted-redacted-b037-
e8cececdf354",
      "UserName": "redacted@gmail.com",
      "FirstName": "Justin",
      "LastName": "Gardner",
      "EmailAddress": "redacted@gmail.com",
      "Submarket": "US",
      "PartnerNumber": null,
      "RegistrationDate": "2018-05-19T18:52:15.0763564Z",
      "RegistrationSource": "Android",
      "LastUpdated": "2020-05-16T23:28:39.3426069Z"
    }
  ]
}
```

Asked to delete data?

No.

Maintain data access through ticket?

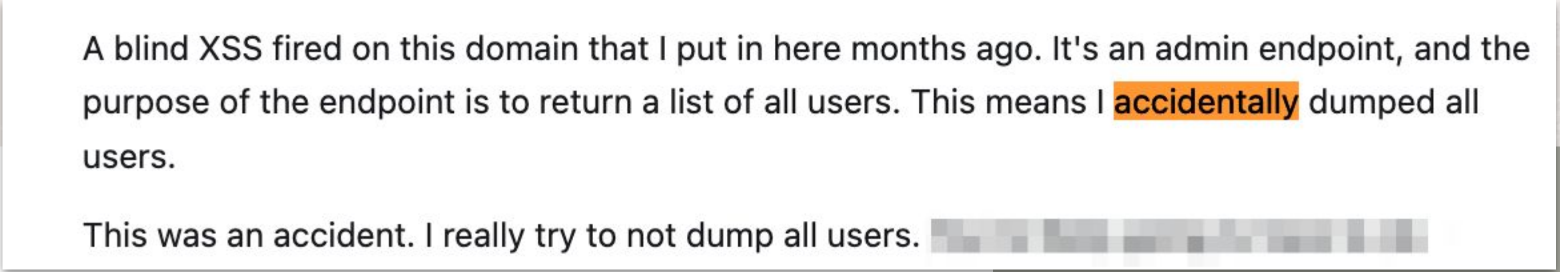
Yes.

Disclosure notifications?

Not to his knowledge.

These aren’t one-off’s.

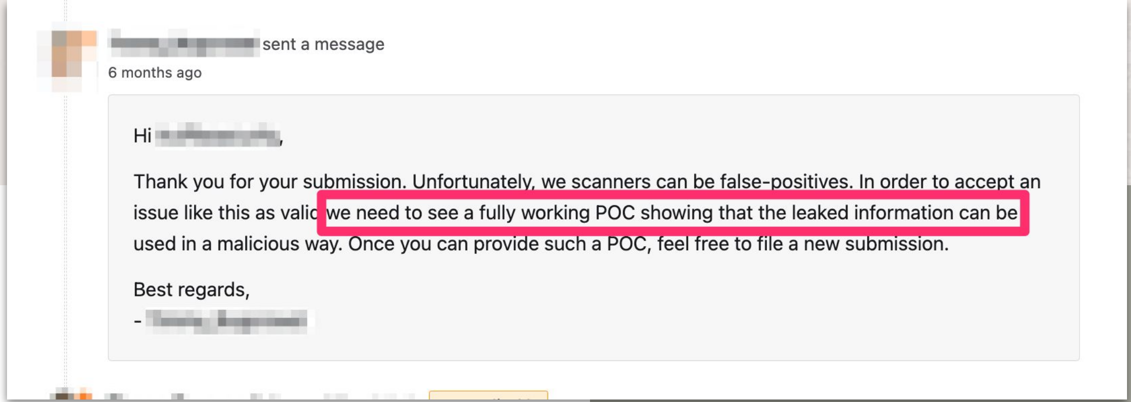
Why does it happen?



A blind XSS fired on this domain that I put in here months ago. It's an admin endpoint, and the purpose of the endpoint is to return a list of all users. This means I accidentally dumped all users.

This was an accident. I really try to not dump all users. [redacted]

Sometimes it’s an accident.



[redacted] sent a message

6 months ago

Hi [redacted],

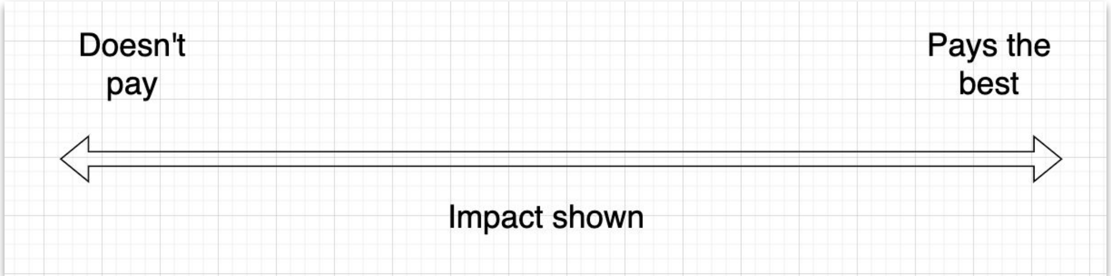
Thank you for your submission. Unfortunately, we scanners can be false-positives. In order to accept an issue like this as valid we need to see a fully working POC showing that the leaked information can be used in a malicious way. Once you can provide such a POC, feel free to file a new submission.

Best regards,

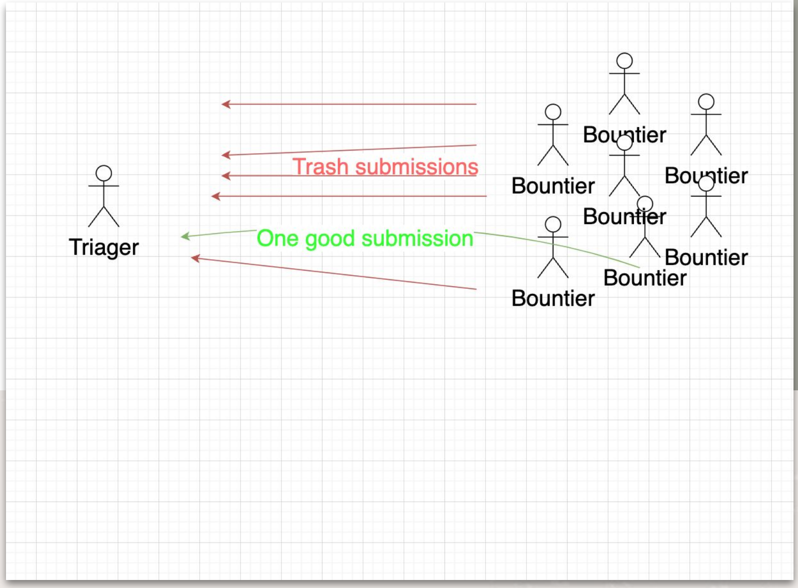
- [redacted]

Sometimes it's not an accident.

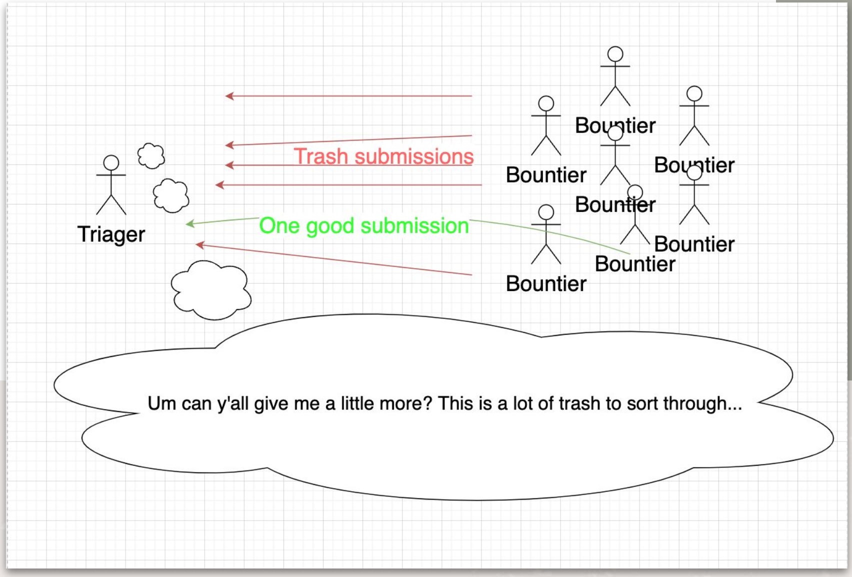
Bountier incentives



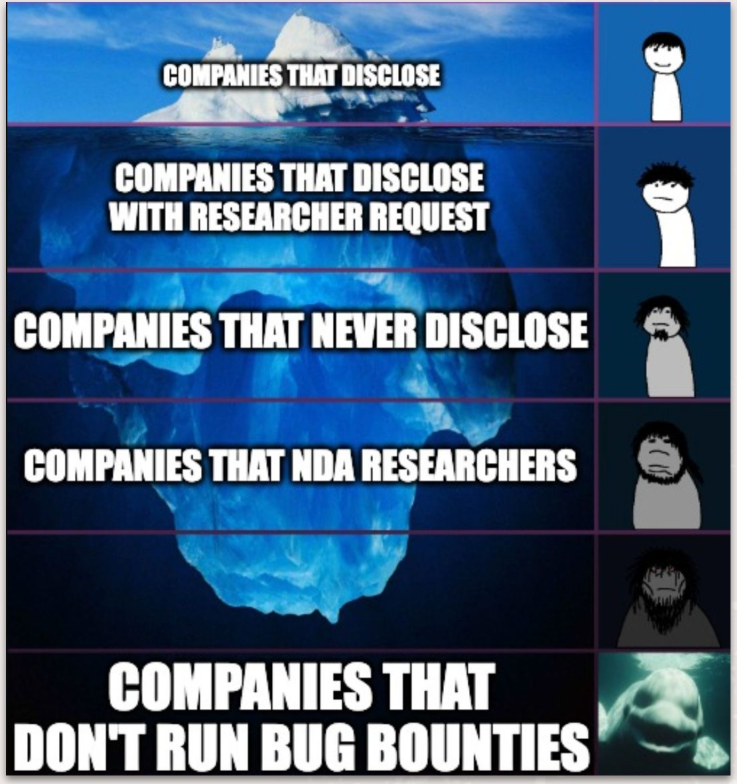
Triager incentives



Triager incentives

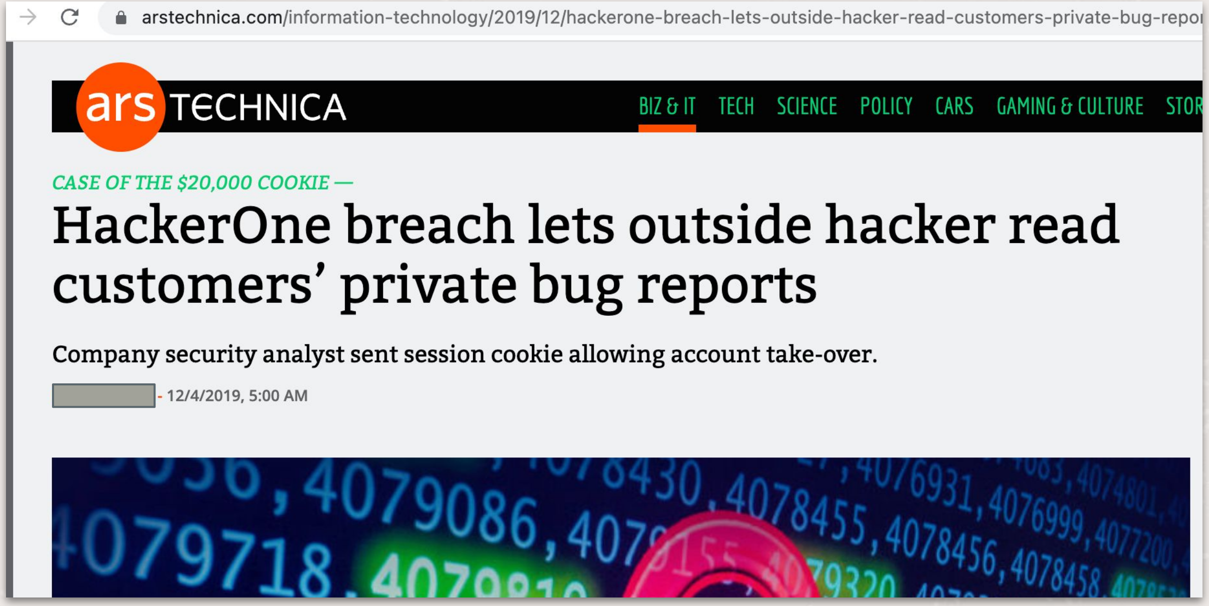


Thank you to the companies that let us talk about it


COMPANIES THAT DISCLOSE
COMPANIES THAT DISCLOSE WITH RESEARCHER REQUEST
COMPANIES THAT NEVER DISCLOSE
COMPANIES THAT NDA RESEARCHERS
COMPANIES THAT DON'T RUN BUG BOUNTIES

Shame on journalists punishing transparent companies

Not helpful



arstechnica.com/information-technology/2019/12/hackerone-breach-lets-outside-hacker-read-customers-private-bug-repor
ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
STOR

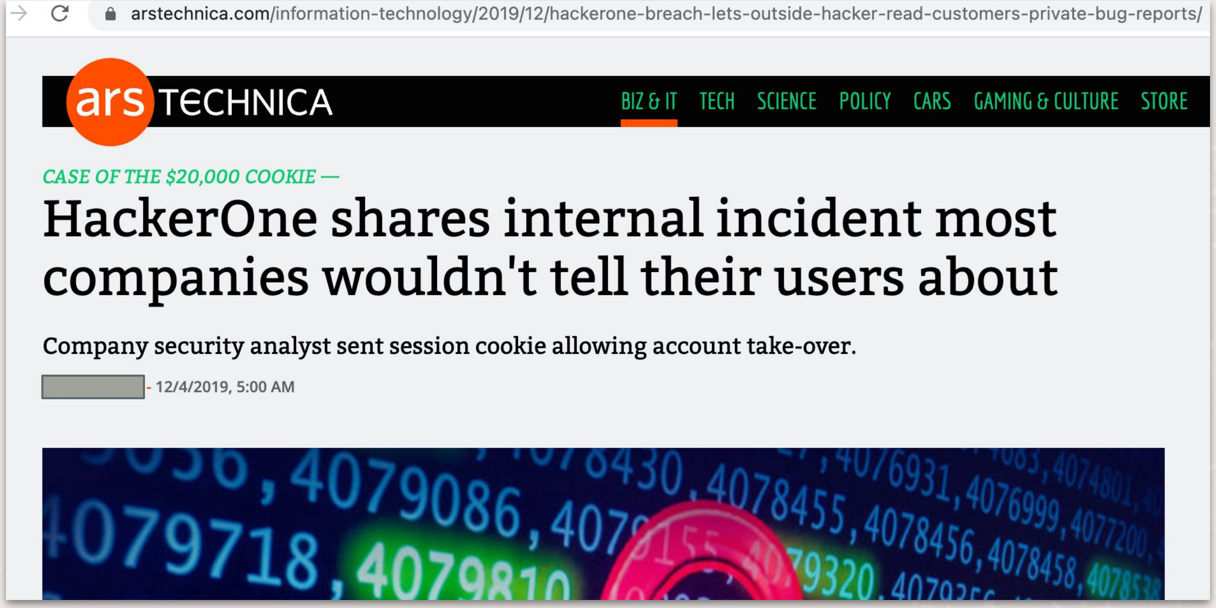
CASE OF THE $20,000 COOKIE —

HackerOne breach lets outside hacker read customers’ private bug reports

Company security analyst sent session cookie allowing account take-over.

[redacted] - 12/4/2019, 5:00 AM

Howbout this?



arstechnica.com/information-technology/2019/12/hackerone-breach-lets-outside-hacker-read-customers-private-bug-reports/
ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
STORE

CASE OF THE $20,000 COOKIE —

HackerOne shares internal incident most companies wouldn't tell their users about

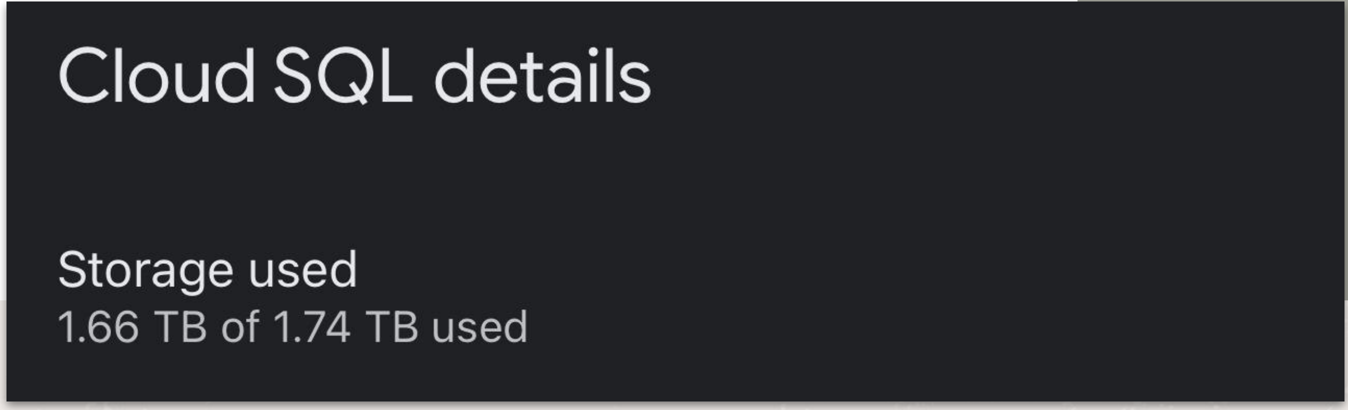
Company security analyst sent session cookie allowing account take-over.

[redacted] - 12/4/2019, 5:00 AM

Why should you care?

So what if this data is everywhere?

XSSHunter has 1.66TB of data in it

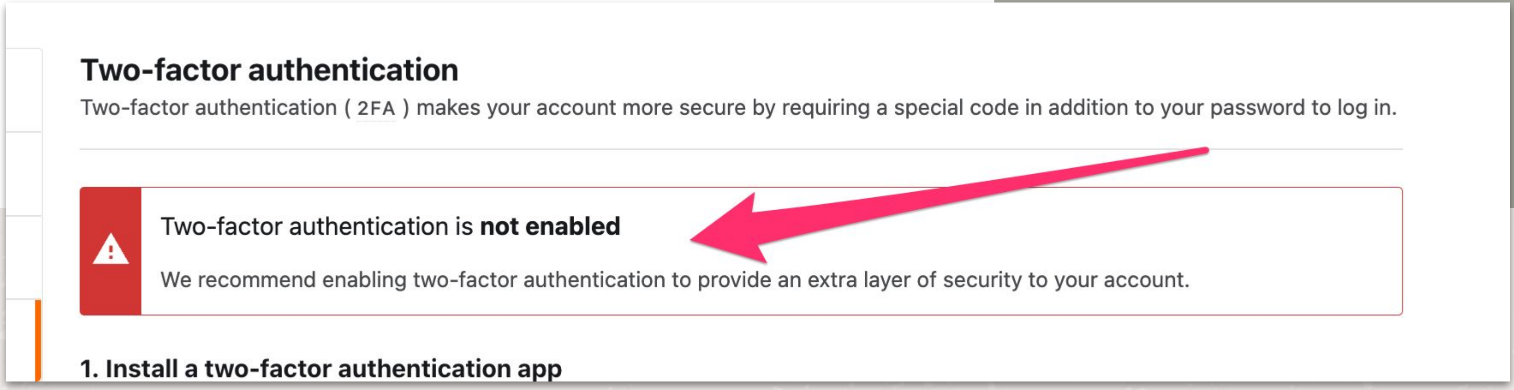


Cloud SQL details

Storage used
1.66 TB of 1.74 TB used

2 weeks ago

My bounty account didn’t have 2fac



Two-factor authentication

Two-factor authentication (2FA) makes your account more secure by requiring a special code in addition to your password to log in.

Two-factor authentication is **not enabled**

We recommend enabling two-factor authentication to provide an extra layer of security to your account.

1. Install a two-factor authentication app

It’s a trend

Time to clean up and try to contain sensitive data while still advancing security programs

If you build it…

Prepare for the worst…

Major requirements

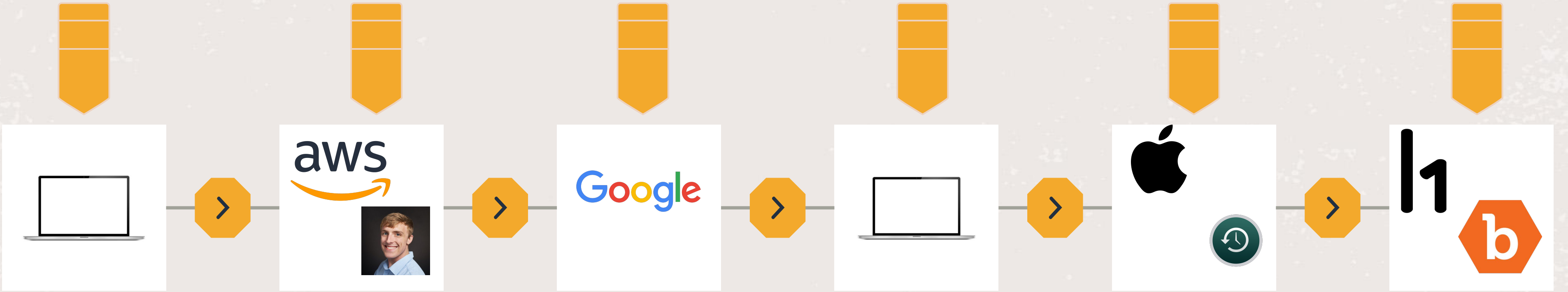
Prevent

Be ready.
Set policies to prevent data leaks and continually enhance them.
Work with your privacy team or compliance teams.

Cleanup

If you know confidential or personal data is on a system, clean it up - and keep a record of the clean up.

Prevention & cleanup opportunities



Employee laptop

XSSHunter & other platforms

Gmail

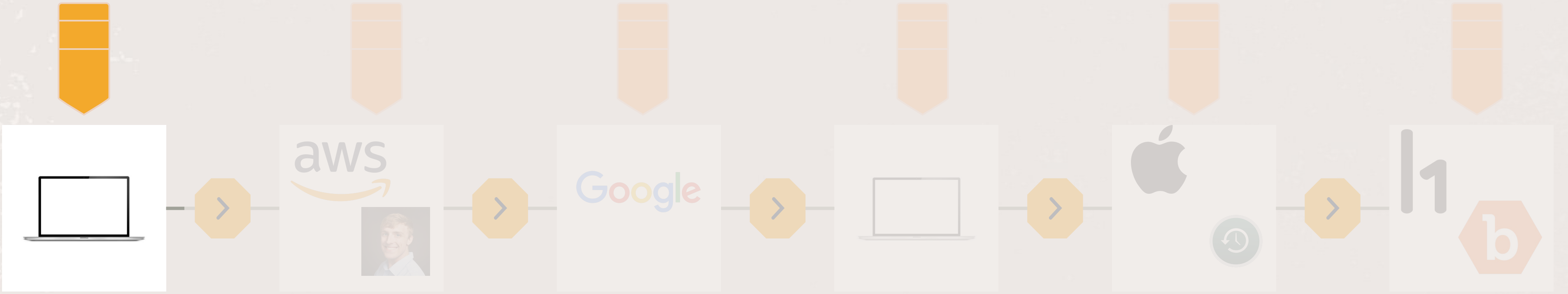
My Hard drive

Backups

Bug tracker

*or company assets

Prevention & cleanup opportunities



Employee laptop*

XSSHunter & other platforms

Gmail

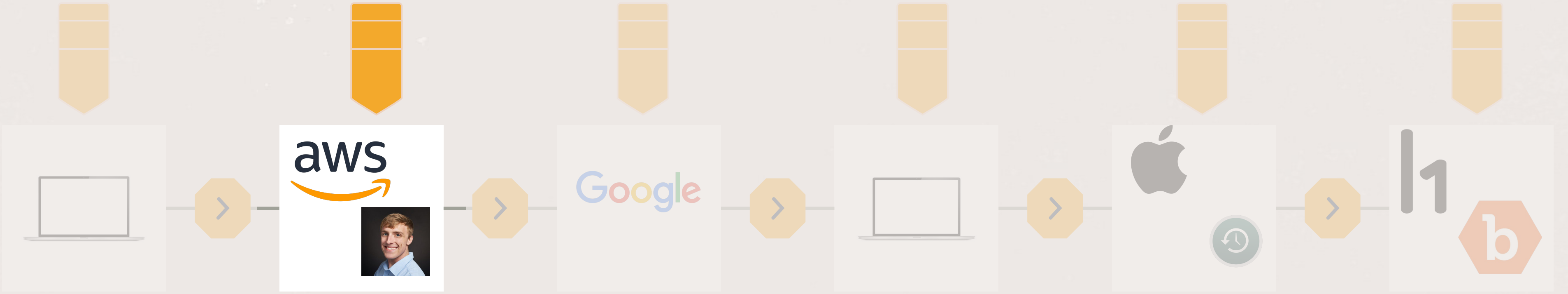
My Hard drive

Backups

Bug tracker

*or company assets

Prevention & cleanup opportunities



Employee laptop*

XSSHunter & other platforms

Gmail

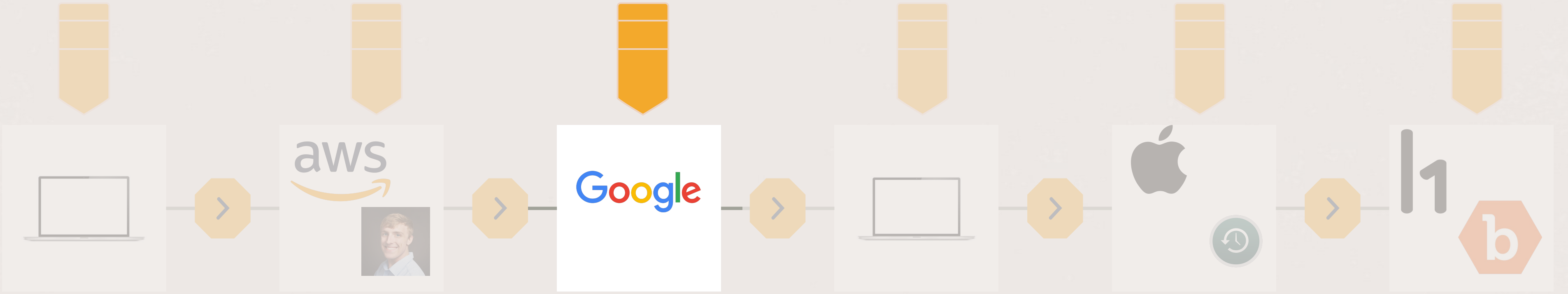
My Hard drive

Backups

Bug tracker

*or company assets

Prevention & cleanup opportunities



Employee laptop*

XSSHunter & other platforms

Gmail

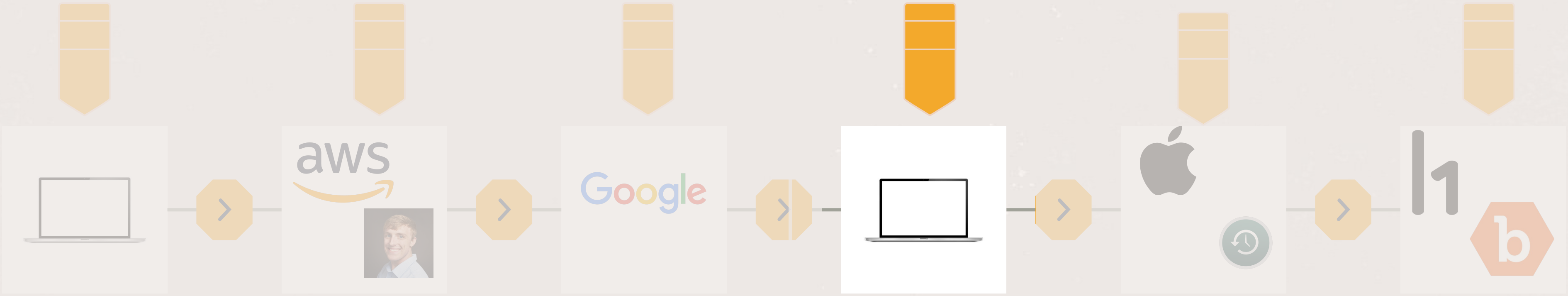
My Hard drive

Backups

Bug tracker

*or company assets

Prevention & cleanup opportunities



Employee laptop*

XSSHunter & other platforms

Gmail

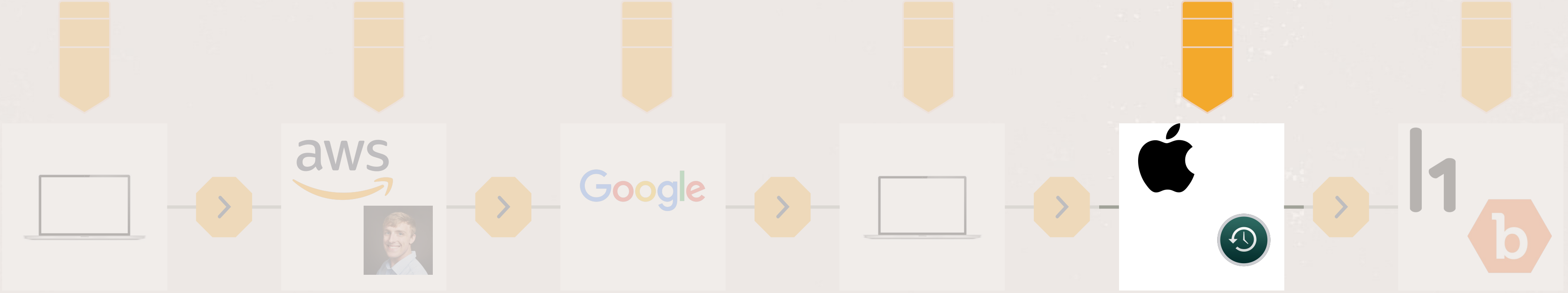
My Hard drive

Backups

Bug tracker

*or company assets

Prevention & cleanup opportunities



Employee laptop*

XSSHunter & other platforms

Gmail

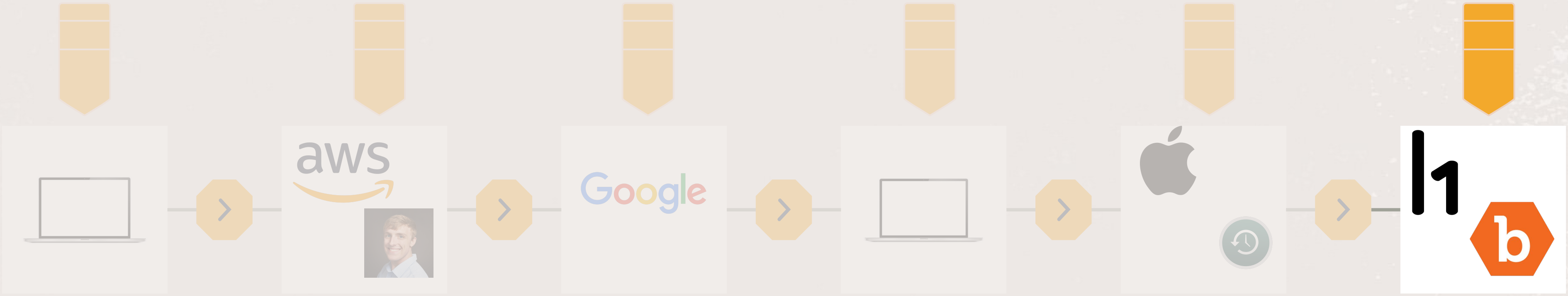
My Hard drive

Backups

Bug tracker

*or company assets

Prevention & cleanup opportunities



Employee laptop*

XSSHunter & other platforms

Gmail

My Hard drive

Backups

Bug tracker

*or company assets

Prevention & cleanup opportunities

Other
unknown third
parties

Ideal data flow

Who knows???

This stuff is complicated

Legal obligations?

The company

Running the bug bounty program

The platforms

That facilitate the bug bounty program and researcher tools

The researcher

Bug hunter hoping to get $ for bugs

“It depends”

Bug bounty & the law

CFAA (US)

“knowingly accessed a computer without authorization or exceeding authorized access”

Bug bounty / Coordinated Vulnerability Disclosure

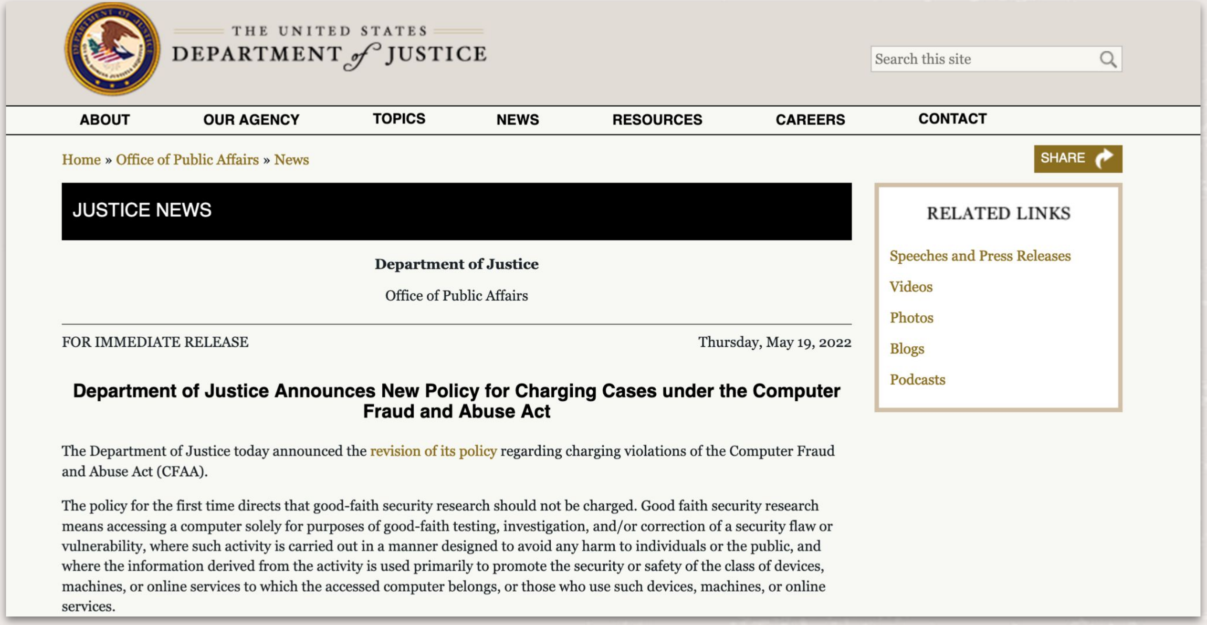
Authorized?
Potentially limited by terms

Privacy laws

Personal data handling requirements could apply

Lawyer help & other resources

- EFF Coder's Rights Project: https://www.eff.org/issues/coders
- Luta Security
- Your in-house legal team



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, May 19, 2022

Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act

The Department of Justice today announced the revision of its policy regarding charging violations of the Computer Fraud and Abuse Act (CFAA).

The policy for the first time directs that good-faith security research should not be charged. Good faith security research means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services.

No but really, legal obligations?

The company

Running the bug bounty program

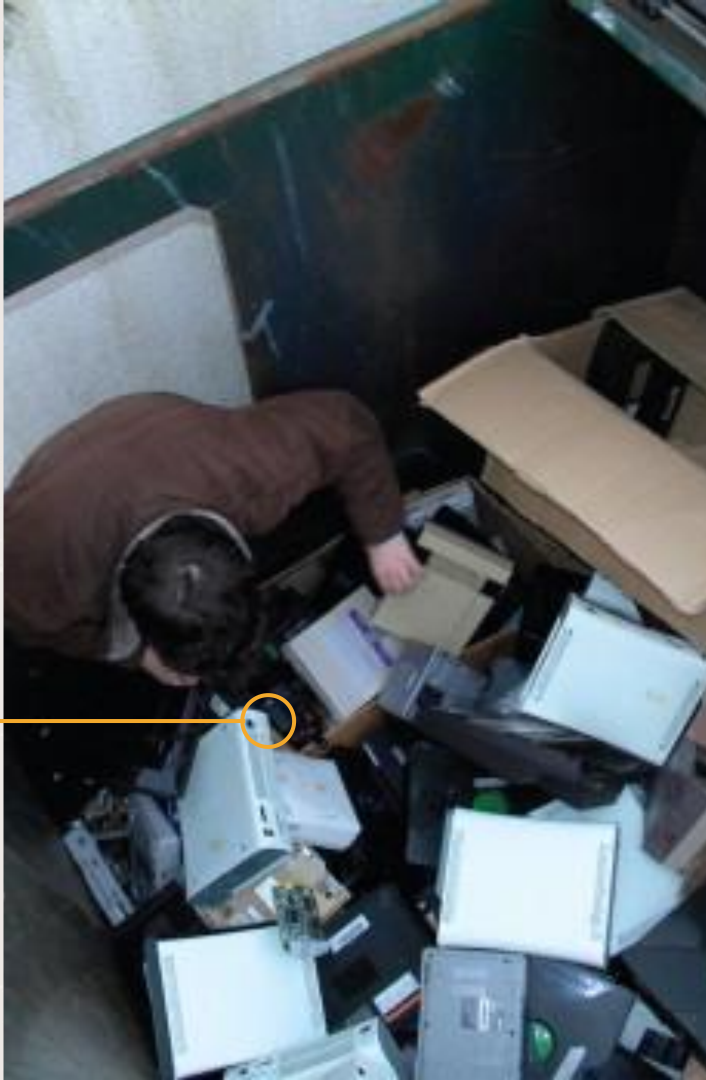
The platforms

That facilitate the bug bounty program and researcher tools

The researcher

Bug hunter hoping to get $ for bugs

Company takeaways



As original stewards of the data, you have legal and contractual obligations to end users or customers - be aware of those. Work with your legal team. Don’t hold on to data forever.

Researcher takeaways

Tell the truth.
Say it, don’t spray it.
Don’t hold on to data.
Stay within bounty terms.
Use 2FA on our H1 and Bugcrowd accounts.

Platform takeaways

Give customers control.
Consider privacy by design.
Clearly communicate privacy practices.
Allow for retention policies for attachments & tickets.

General takeaways

We <3 Bug Bounties

This is not unique to bug bounties, it will exist in general pentesting ecosystem

Good data handling prevents security incidents

Good data governance and a strong foundation will set everyone up for success

Thank you!
Questions?

Dylan Ayrey
@InsecureNature

Whitney Merrill
@wbm312