

Navigating The Coordinated Vulnerability Disclosure Landscape

@EdOverflow



By **Tim Blazytko**



14:35 - 15:05

Edzo Botjes

By **Edzo Botjes**



15:10 - 15:40

**Navigating The
Coordinated
Vulnerability
Disclosure
Landscape**

By **Edwin Foudil**



15:40 - 16:20

Coffee Break



Hi, I'm Ed 🙌





NEWS

Home | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politics | Culture | Tech

England | Local News | Regions | London

Euston station: Major train disruption after signal failure

🕒 21 hours ago



Passengers were told to expect delays and cancellations





Coordinated **V**ulnerability **D**isclosure





Researcher says he was threatened after finding major DJI security flaw

154

Published Nov 27, 2017 | [Brittany Hillen](#)



🕒 This article is more than 1 year old

Former Uber security chief found guilty of concealing data breach

Joe Sullivan failed to report a cybersecurity incident to authorities in 2016



**was threatened after
urity flaw**

154

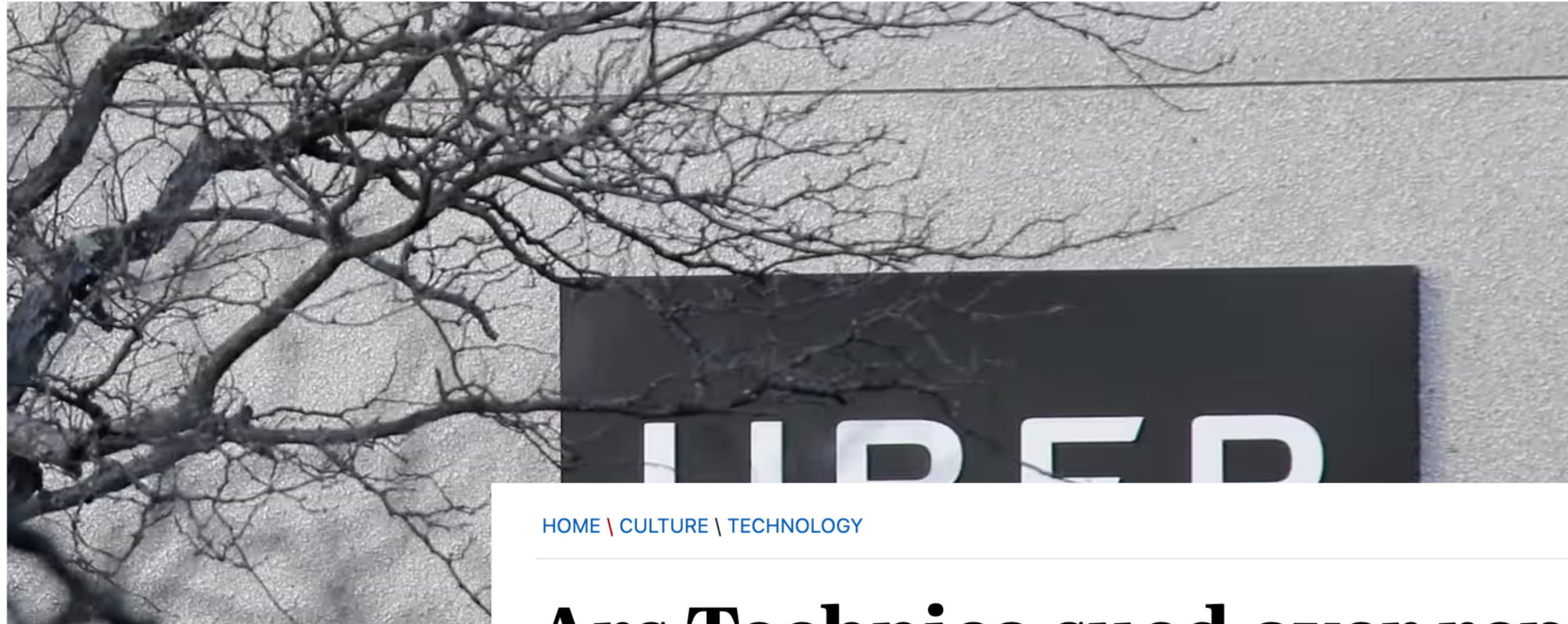
Search dpreview.com 🔍

Sample Images Videos Cameras Lenses Phones

🕒 This article is more than 1 year old

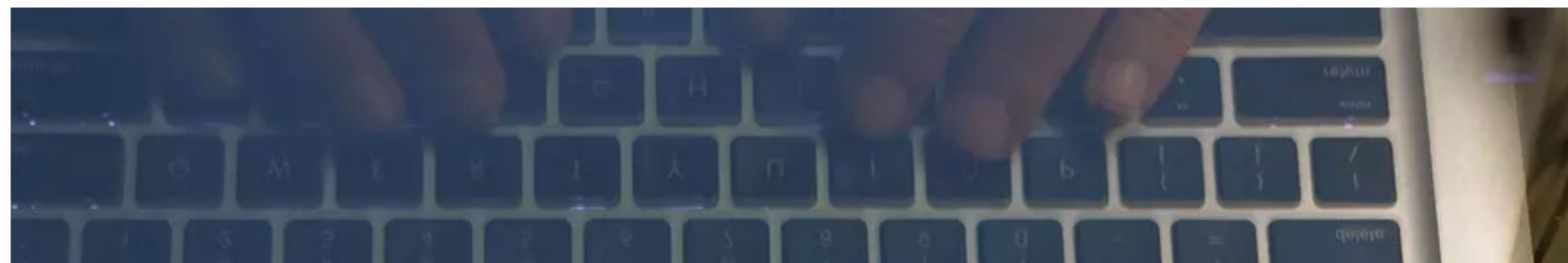
Former Uber security chief found guilty of concealing data breach

Joe Sullivan failed to report a cybersecurity incident to authorities in 2016



[HOME](#) | [CULTURE](#) | [TECHNOLOGY](#)

Ars Technica sued over reporting on 'critically flawed' password manager



Search dpreview.com



Sample Images

Videos

Cameras

Lenses

Phones

was threatened after security flaw

154

Follow Us

Search



FRONT PAGE PODCAST

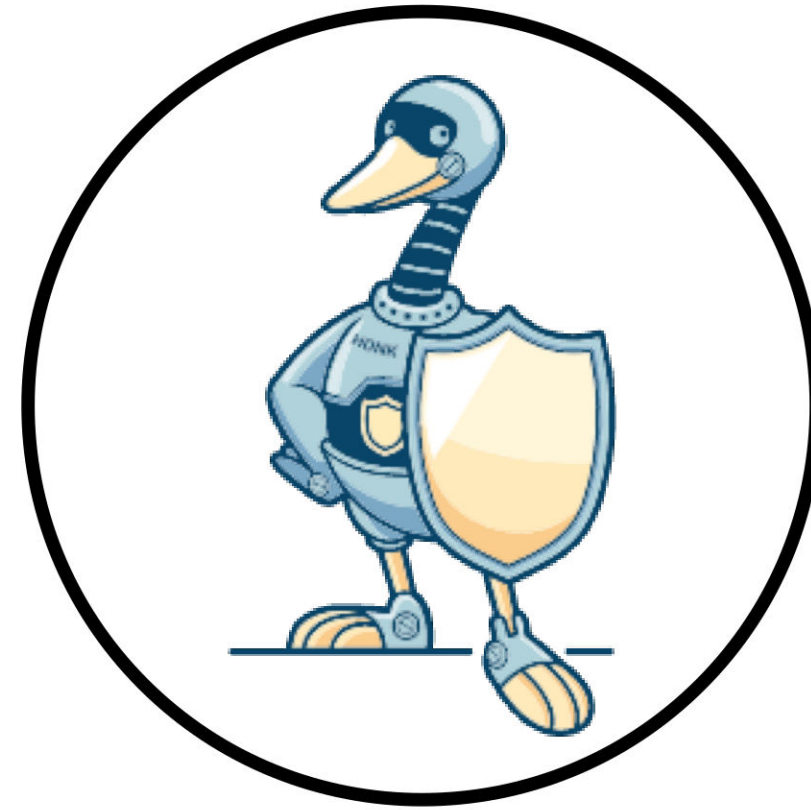


Dr Amit Elazari
Legal Safe Harbours



Content Creators

@LiveOverflow, @NahamSec, @InsiderPhD, etc.



OpenSSH

Open source security initiatives



A Glass of cold, home crafted bee...

107

Reputation Rank

274

#393615

Physical Laptop Takeover

Share:     

State ● Resolved (Closed)

Severity ■ Critical (9 ~ 10)

Disclosed **August 12, 2018 10:19am +0200**

Participants 

Reported To **Ed**

Visibility **Disclosed (Full)**

Asset **Personal machine
(Hardware/IoT)**



Bug bounty hunters



News

Opinion

Sport

Culture

Lifestyle

More ▾

[Education](#) ▶ [Schools](#) [Teachers](#) [Universities](#) [Students](#)

**Animal
behaviour**

Why dolphins are deep thinkers

**The more we study dolphins, the brighter they turn out to be,
writes Anuschka de Rohan**

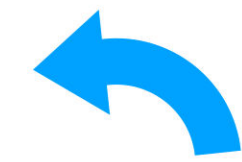
*Anuschka de
Rohan*

Thu 3 Jul 2003 02.25 BST





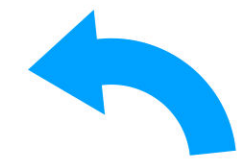
=



Kelly



=



Kelly



HACKERMAN

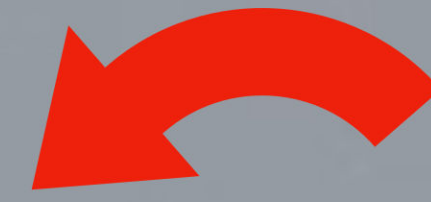
hello sir



bounty pls



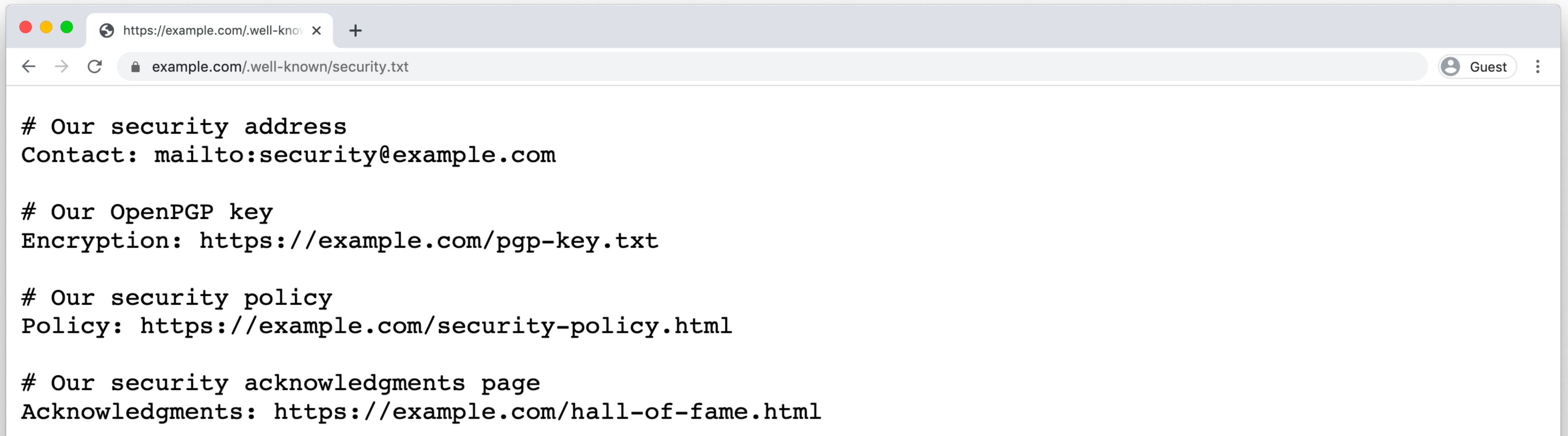
bounty pls



**Beg bounty
hunter**

Have a way to be contacted

security.txt

A screenshot of a web browser window. The address bar shows the URL 'https://example.com/well-known/security.txt'. The page content is a plain text file with four sections, each starting with a comment line and followed by a specific URL or email address.

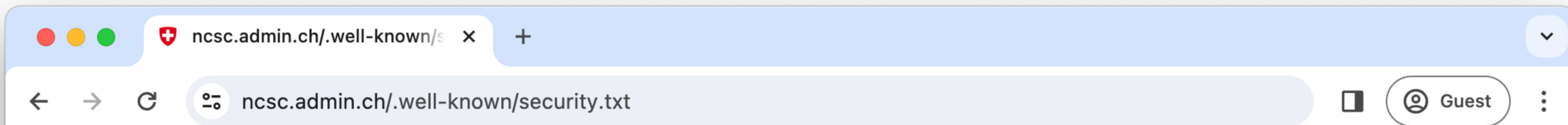
```
# Our security address
Contact: mailto:security@example.com

# Our OpenPGP key
Encryption: https://example.com/pgp-key.txt

# Our security policy
Policy: https://example.com/security-policy.html

# Our security acknowledgments page
Acknowledgments: https://example.com/hall-of-fame.html
```

Contact: `mailto:security@example.com`



In the event that you have discovered a technical vulnerability in an IT system of the federal government,
we encourage you to report it to the National Cyber Security Centre NCSC using the Coordinated Vulnerability Disclosure program.
We forward your request to the appropriate unit.
If you are interested in participating in the NCSC bug bounty programs you can apply here: <https://www.bugbounty.ch/ncsc>

Contact: <https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html>

Contact: <mailto:incidents@ncsc.ch>

Expires: 2023-12-31T23:59:59.000Z

Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/pgp_ncsc_incidents.asc.download.asc/NCSC_Incidents.asc

Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/smime_incidents_ncsc_ch_22.cer.download.cer/smime_incidents_ncsc_ch_22.cer

Preferred-Languages: en, de, fr, it

Canonical: <https://www.ncsc.admin.ch/.well-known/security.txt>

Policy: <https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html>

**Define a process for
addressing incoming reports**

Hi team,

I have discovered a reflected XSS vulnerability on example.com via the the *?search=* parameter.

[...]

All the best!

- Kelly



SUE THEM

Dear sir,

I have hacked your website. I demand a \$100'000 ransom otherwise I will leak your data!

Klaus





Uber disguised \$100,000 hacker payoff as bug bounty, claims Reuters

Can a hacker's extortion demand ever be paid off as though it were a bug bounty? Or is that a step too far?

Written by Paul Ducklin

DECEMBER 08, 2017

NAKED SECURITY

BREACH

ICO

REUTERS

UBER

Remember [the 2017 Uber breach?](#)

The one that was actually discovered in 2016, except that Uber conveniently [forgot about it for a year](#) before

Hi Kelly,

Thank you for the report! This email is to acknowledge we have received your report.

- Ed



TIMELINE



edoverflow submitted a report to [Keybase](#).

January 21, 2018

Description

The following snippet in `js/identities.js` allows all hostnames ending in `twitter.com`, `facebook.com`, etc. to display the Keybase message window. The issue stems from the fact that you use `\.` instead of `\\.` in your regular expression.

Code 252 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 {
2   service: "twitter",
3   getUsername: function(loc) { return loc.pathname.split('/')[1]; },
4   locationMatches: new RegExp('\.twitter\.com/([\w]+)[/]?$'),
5   originAndPathMatches: '\.twitter\.com/[\\w]+[/]?$',
6   css: ['body.ProfilePage']
7 },
```

PoC

Code 46 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 $ cat /etc/hosts
2 IP_HERE totallynottwitter.com
```

Start up a little server and navigate to `IP_HERE/edoverflow`. Click on the Keybase extension's icon and the message window will pop up, typing [@EdOverflow](#) Twitter's identity to `totallynottwitter.com`.



[maxtaco](#)

Keybase staff

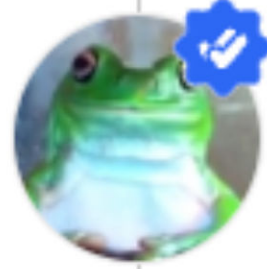
changed the status to ● **Triaged**.

thank you for this report, PR up here: <https://github.com/keybase/client/pull/10277/files>



[maxtaco](#) Keybase staff posted a comment.

Should be fixed in the new extension. Can you confirm?



[edoverflow](#) posted a comment.

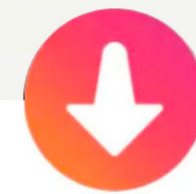
Wow, once again, very impressive resolution time! I can confirm that this issue has been resolved.



[maxtaco](#) Keybase staff closed the report and changed the status to ● **Resolved**.

Fixed.

**Build strong relationships with
the hackers**



Kelly 25

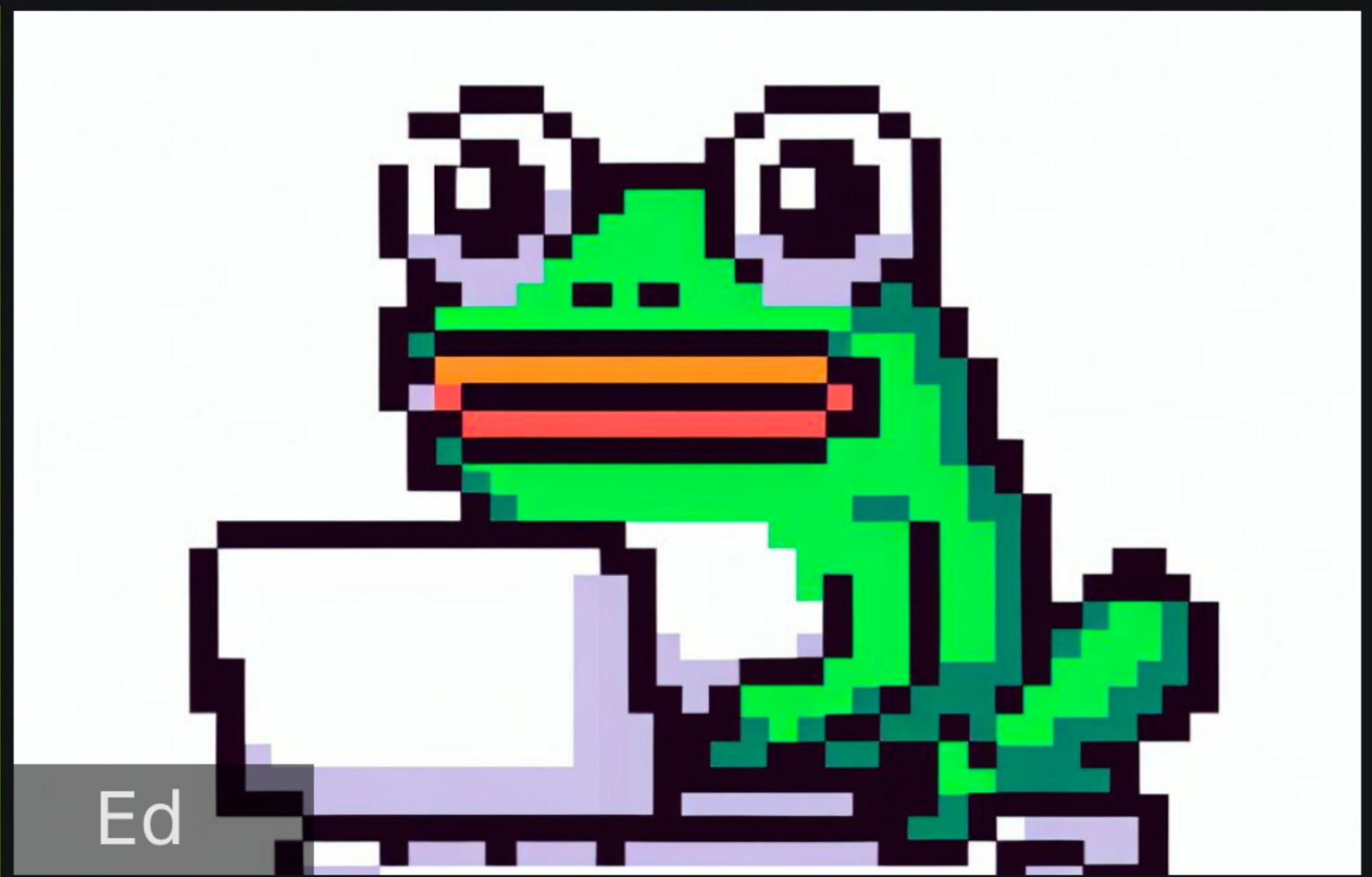
📁 Bug bounty hunter

📍 1 mile away

I love finding 0days









Klaus

Zürich, Switzerland

 28  7

     Oct 14, 2023

If I had a dollar for every time this bug bounty program gave me the cold shoulder, I'd be rich enough not to need bug bounties in the first place!

 Useful

 Funny

 Cool



[maxtaco](#) Keybase staff posted a comment.

January 26, 2018

We think the researcher here did great work, and thought creatively about Keybase's application and how to break it. The bug was a minor escaping issue in the end, but one that could have been exploited with small amounts of social engineering. Awesome job!

Provide legal protection

IANAL

I will investigate legitimate reports and make every effort to quickly resolve any vulnerability. Please make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of my services.

I will not pursue civil action or initiate a complaint to law enforcement for accidental, good faith violations of this policy. I consider a violation consistent with this policy to constitute “authorised” conduct under the Computer Fraud and Abuse Act. I will not bring a D’ for circumventing the technological measures I have implemented in applications in scope of this program.

If legal action is initiated by a third party against me or my company for actions taken in compliance with this security policy, I will take steps to resolve the matter. If legal action were conducted in compliance with this policy, I will take steps to resolve the matter.

It is also important to note, I will not take legal action against you for providing me with a proof of concept of the vulnerability.



Dr Amit Elazari

Let's wrap this up!



```
https://example.com/.well-known/ x +
example.com/.well-known/security.txt
Guest

# Our security address
Contact: mailto:security@example.com

# Our OpenPGP key
Encryption: https://example.com/pgp-key.txt

# Our security policy
Policy: https://example.com/security-policy.html

# Our security acknowledgments page
Acknowledgments: https://example.com/hall-of-fame.html
```





@EdOverflow

contact@edoverflow.com