

# Keeping up with the Pwnses

*An overview of Talkback*



# Hi!

**Who:** I'm **Seb** @ **elttam**

**What:** <https://talkback.sh/>

**Why:** Keeping up with infosec is hard

Main motivators:

- Keep up with infosec more efficiently.
- Get to relevant technical information faster.
- Support a bunch of our own use-cases.



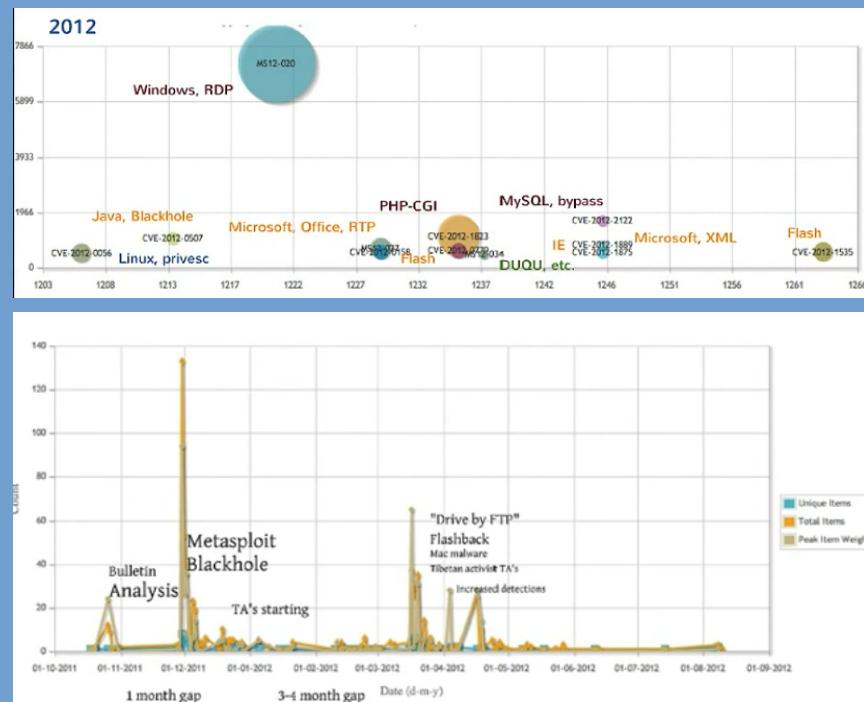
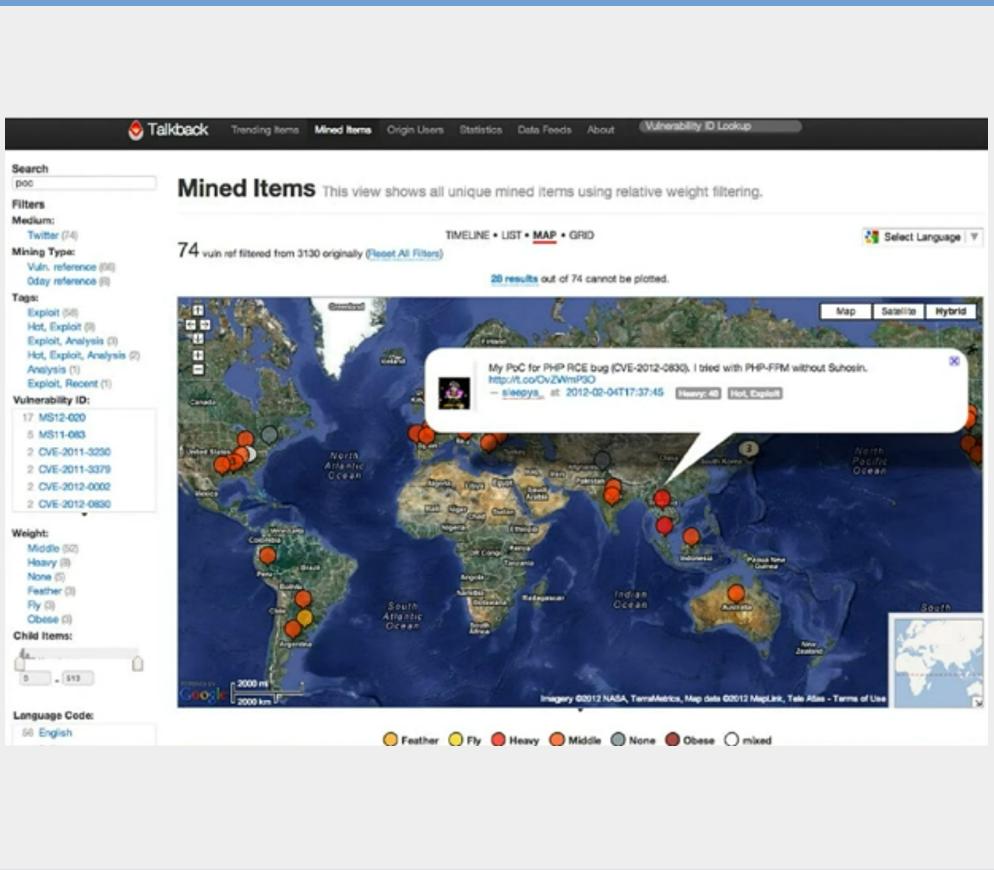
# Smart?

- Smart infosec aggregator
- Similar projects (we know of)
  - <https://0dayfans.com/>
  - <https://allinfosecnews.com/>
  - <https://hacker-trends.com/>
  - <https://threatable.io/>
  - <https://morningstarsecurity.com/news>
  - <https://hackdojo.io/>

The screenshot shows a list of news items on the 0dayFans website:

- Microsoft Browser Vulnerability Research** (March 14 2024 @ 8:34 AM) - A Microsoft logo icon. Article title: Making Mojo Exploits More Difficult. Subtitle: Introduction.
- blog.doyensec.com** (March 15 2024 @ 2:20 PM) - A stylized orange 'D' icon. Article title: A Look at Software Composition Analysis. Subtitle: A Look at Software Composition Analysis.
- LinkedIn - HackerOne** (March 12 2024 @ 10:47 AM) - A LinkedIn logo icon. Article title: high - An attacker can submit arbitrary projects to their service accounts and obtain full information on projects of other users. Subtitle: An IDOR issue was discovered in the Request Services feature, where an attacker can gain access to project details of other users by submitting work project requests. Henceforth, an attacker can obtain the details of project submitted to other service providers and submit their own proposals to the victim(owner of the project). We have resolved the issue on priority and paid a bounty to...

# Original version from 2010-2012



# Original version from 2010-2012

**Talkback** Trending Items Mined Items Origin Users Statistics Data Feeds About Vulnerability ID Lookup

Search

Filters

Medium: Twitter (4927)

Mining Type: Popular item (4862), Vuln. reference (62), Today reference (113)

Category: Interesting (2179), Technical (831), General (766), News (665), None (248), Humour (235), Irrelevant (5)

Weight: Middle (4311), Heavy (512), Obeso (257), Feather (13), Fly (12), Light (0), None (0)

Child Items:

Origin User Followers #: 0 - 53161

**Trending Items** This view shows featured trending items from the itsec community over the past 6 months.

4927 items

sorted by: date, then by... grouped as sorted

**2012-10-13 (2)**

Reverse-Engineering Database - An IDA-Pro Plug-in <http://t.co/JBRvNpGX>  
— matzalas at 2012-10-13T10:57:31 **News**

Metasploit stager: reverse\_https with basic authentication against proxy <http://t.co/1TpqGjE>  
— Dinoxyd at 2012-10-13T15:40:39 **None**

**2012-10-12 (24)**

#Malware is being packaged with popular software, music and movie files. Learn more. [#SRv13">http://t.co/z7HQjsSf">#SRv13](http://t.co/z7HQjsSf)  
— msftsecurity at 2012-10-12T01:10:09 **Middle** **News**

FX evictates Huawei router firmware exposing slew of bugs, remote stack & heap overflows, hardcoded creds exploit ...  
— richesattle at 2012-10-12T02:39:03 **Middle** **10** **Interesting**

Anonymous declares war on WikiLeaks in retaliation for "paywall" [@drpizza">http://t.co/O4v1wAOX](http://t.co/O4v1wAOX) @drpizza  
— arstechnica at 2012-10-12T05:27:45 **Middle** **37** **General**

Weekend reading - #HTB2012KUL presentation materials - <http://t.co/pvPubs7>  
— HITBSecConf at 2012-10-12T11:52:23 **Middle** **10** **Interesting**

Netflix settles with deaf-rights group, agrees to caption all videos by 2014 <http://t.co/aL2fLGI> by @joemullin  
— arstechnica at 2012-10-11T02:55:44 **Middle** **16** **Recent**

Assange to Publish Book on Cyber 'Resistance' <http://t.co/BPsVMCd0>  
— TheHackersNews at 2012-10-11T02:51:57 **Middle** **10** **Recent** **Moderation screenshot**

My slides on designing a distributed fuzzing framework from last nights @novahackers are up at <http://t.co/Wkk77Zy1>  
— bannedito at 2012-10-11T02:45:40 **Middle** **13** **Recent**

"Did Microsoft just kill Flash? Internet Explorer 10 won't run Flash unless your site is on a Microsoft whitelist" <http://t.co/...>  
— jeremiahg at 2012-10-11T02:44:27 **Middle** **33** **Recent**

**Daily & weekly paper**  
This is now my news source

Talkback 7day Report

Topics Photos Videos

Relentless Coding: Analyzing the Blackhole Exploit Kit 2.0 with JSbeautify

The Guide to Nmap 02/2012 | Issue 17 Security Magazine - HackIt! www.hackit.org

Malware Hooks in the Windows GUI Subsystem

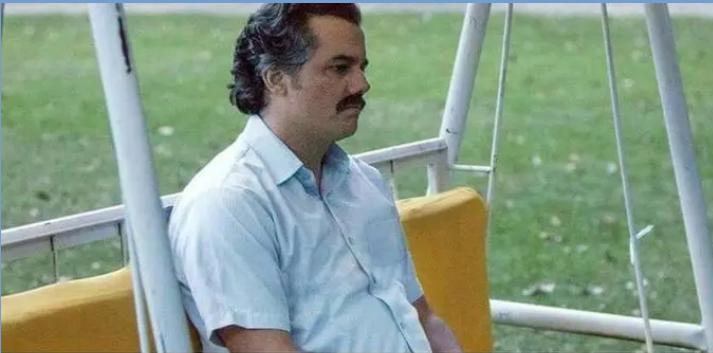
Valid Adobe Certificate Used to Sign Malicious Utilities Common in Targeted Attacks

malwarelab.blogspot.com - Malware L1: Detecting Malware Hooks in the Windows GUI Subsystem

thehackernews.org - Assange to Publish Book on Cyber 'Resistance'

thehackernews.org - Assange to Publish Book on Cyber 'Resistance'

**Me (2013-2022): \*waiting for someone to write something free that met all my requirements\***





Showing resources 1 to 10 of 78

[«](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [...](#) [»](#)

Past 3 days 10 / page

- Attacking Android 1 day ago - [blog.devsecopsguides.com](http://blog.devsecopsguides.com) post
- CVE-2024-22857: Critical Flaw in Popular Zlog Library Opens Door to Arbitrary Code Execution 1 day ago - [securityonline.info](http://securityonline.info) news
- Formation of the Open Source Digital Forensics Developer's Council 2 days ago - [sleuthkitlabs.com](http://sleuthkitlabs.com) post
- Game of Active Directory (GOAD) | Ludus 3 days ago - [docs.ludus.cloud](http://docs.ludus.cloud) type n/a
- Robots Dream of Root Shells 1 day ago - [blog.isosceles.com](http://blog.isosceles.com) post
- CVE-2024-23897 – Arbitrary file read in Jenkins 1 day ago - [blog.securelayer7.net](http://blog.securelayer7.net) post
- GitHub - Oxor0ne/awesome-list: Cybersecurity oriented awesome list 1 day ago - [github.com/Oxor0ne](http://github.com/Oxor0ne) oss
- BianLian GOs for PowerShell After TeamCity Exploitation 2 days ago - [guidepointsecurity.com](http://guidepointsecurity.com) post
- CVE-2024-21378 — Remote Code Execution in Microsoft Outlook 1 day ago - [netspi.com](http://netspi.com) post
- NextChat: An AI Chatbot That Lets You Talk to Anyone You Want To 1 day ago - [horizon3.ai](http://horizon3.ai) news

# Curators



## ThinkstScapes Quarterly

- <https://thinkst.com/ts>



## Risky Biz

- <https://risky.biz/>
- <https://riskybiznews.substack.com/>
- <https://srslyriskybiz.substack.com/>



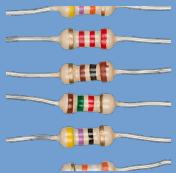
## tl;dr sec

- <https://tldrsec.com/>



## PentesterLab Weekly

- <https://x.com/pentesterlab>



## INT3

- <https://int3.substack.com/>



## CTO at NCSC

- <https://ctoatncsc.substack.com/>

Showing resources 1 to 10 of 6551

« 1 2 3 4 5 6 ... »

 My first impressions of web3   
2 years ago -    - [moxie.org](#)

 Can you trust ChatGPT's package recommendations?   
9 months ago -    - [vulcan.io](#)

 New attack campaign utilized a new 0-day RCE vulnerability on Microsoft Exchange Server | Blog | GTSC   
1 year ago -   [gtelsc.vn](#)

 How I made \$31500 by submitting a bug to Facebook   
3 years ago -  [win3zz.medium.com](#)

 I've Just Launched "Pwned Passwords" V2 With Half a Billion Passwords for Download  
6 years ago -  [troyhunt.com](#)

 Domain Details Page  
7 years ago -  [boris.in](#)

 GitHub - mandiant/red\_team\_tool\_countermeasures  
3 years ago -   [github.com/fireeye](#)

ABOUT LIFE PROJECTS BLOG @ 

### My first impressions of web3

June 05, 2022

Despite considering myself a cryptographer, I have not found myself particularly drawn to "crypto." I don't think I've ever actually said the words "get off my lawn," but I'm much more likely to click on Pepperidge Farm Remembers flavored memes about how "crypto" used to mean "cryptography" than I am the latest NFT drop.

Also - cards on the table here - I don't share the same generational excitement for moving all aspects of life into an instrumented economy.

Even strictly on the technological level, though, I haven't yet managed to become a believer. So given all of the recent attention into what is now being called web3, I decided to explore some of what has been happening in that space more thoroughly to see what I may be missing.

How I think about 1 and 2

My first impressions of web3  
— [moxie.org](#)

Despite considering myself a cryptographer, I have not found myself particularly drawn to "crypto." I don't think I've ever actually said the words "get off my lawn," but I'm much more likely to click on Pepperidge Farm Remembers flavored memes about how "crypto" used to mean "cryptography" than ...

**» Featured on**

 [tldrsec](#)  
 [riskybiz](#)  
 [pentesterlab](#)



Showing resources 1 to 10 of 78

[«](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [...»](#)

- Attacking Android [app](#) [crypto](#) [net](#)  
1 day ago - [blog.devsecopsguides.com](https://blog.devsecopsguides.com)

- CVE-2024-22857: Critical Flaw in Popular Zlog Library Opens Door to Arbitrary Code Execution [app](#) [exp](#)  
1 day ago - [securityonline.info](https://securityonline.info)

- Formation of the Open Source Digital Forensics Developer's Council [for](#)  
2 days ago - [sleuthkitlabs.com](https://sleuthkitlabs.com)

- Game of Active Directory (GOAD) | Ludus  
3 days ago - [docs.ludus.cloud](https://docs.ludus.cloud)

- Robots Dream of Root Shells [app](#) [exp](#) [sys](#)  
1 day ago - [blog.isosceles.com](https://blog.isosceles.com)

- CVE-2024-23897 – Arbitrary file read in Jenkins [app](#) [exp](#) [net](#)  
1 day ago - [blog.securelayer7.net](https://blog.securelayer7.net)

- GitHub - 0xor0ne/awesome-list: Cybersecurity oriented awesome list  
1 day ago - [github.com/0xor0ne](https://github.com/0xor0ne)

- BianLian GOs for PowerShell After TeamCity Exploitation [exp](#) [net](#) [mal](#)  
2 days ago - [guidepointsecurity.com](https://guidepointsecurity.com)

- CVE-2024-21378 — Remote Code Execution in Microsoft Outlook [app](#) [exp](#) [net](#)  
1 day ago - [netspi.com](https://netspi.com)

- NextChat: An AI Chatbot That Lets You Talk to Anyone You Want To [app](#) [cloud](#)  
1 day ago - [horizon3.ai](https://horizon3.ai)

Showing resources 1 to 10 of 78

[«](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [...»](#)

# DevSecOpsGuides

## Attacking Android

Attacking Android — [blog.devsecopsguides.com](https://blog.devsecopsguides.com) 22 min In this comprehensive guide, we delve into the world of Android security from an offensive perspective, shedding light on the various techniques and methodologies used by attackers to compromise Android devices and infiltrate their sensitive data. Fr.. ▾ OpenAI Summary

Android security from an offensive perspective is explored, covering various attack techniques and methodologies.

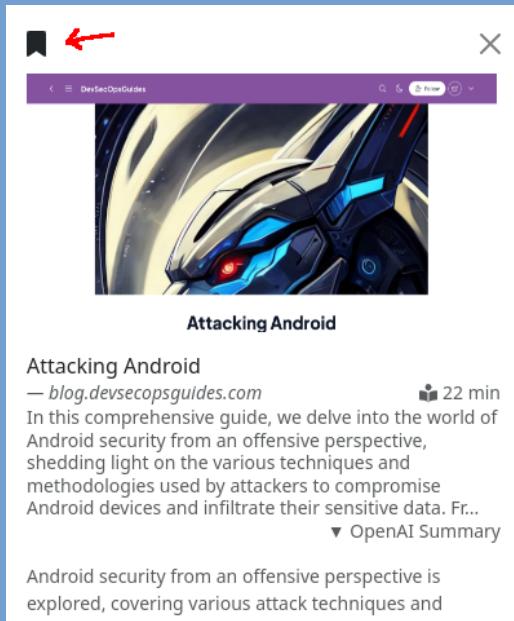
Access control for ContentProvider in Android is crucial to prevent unauthorized access to sensitive data.

Guidelines for implementing restricted access, securing broadcast intents, and handling sensitive data are provided.

Risks and compliant solutions for directory traversal vulnerabilities, logging sensitive information, and caching data are discussed.

Best practices for using WebView, native methods, exception handling, and SSL communication are outlined to enhance security.

[Open Destination](#) [View Full Details](#) [Close](#)



Talkback Home Technical News Featured Saved About Search Sign in Past 50 years

Showing resources 1 to 2 of 2

Attacking Android   
1 week ago - [blog.devsecopsguides.com](http://blog.devsecopsguides.com) post

Formation of the Open Source Digital Forensics Developer's Council   
1 week ago - [sleuthkitlabs.com](http://sleuthkitlabs.com) post

# Attacking Android

— [blog.devsecopsguides.com](https://blog.devsecopsguides.com/attacking-android)

In this comprehensive guide, we delve into the world of Android security from an offensive perspective, shedding light on the various techniques and methodologies used by attackers to compromise Android devices and infiltrate their sensitive data. Fr...

👤 22 min read

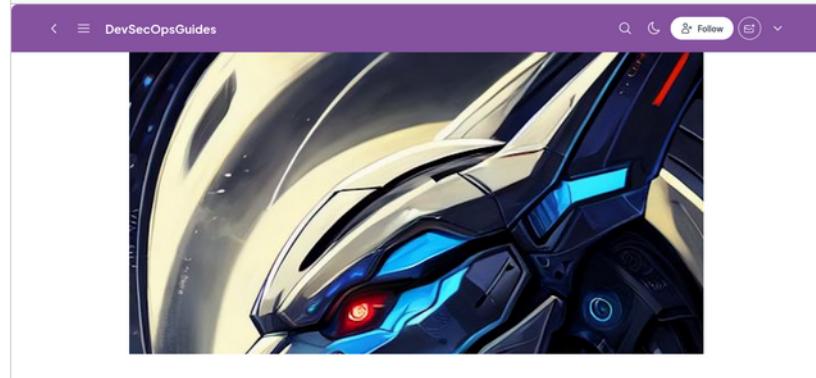
## Key Details

URL	<a href="https://blog.devsecopsguides.com/attacking-android">https://blog.devsecopsguides.com/attacking-android</a>
Age	1 day ago
Categories	<a href="#">appsec</a> <a href="#">cryptography</a> <a href="#">netsec</a>

## OpenAI Summary

- Android security from an offensive perspective is explored, covering various attack techniques and methodologies.
- Access control for ContentProvider in Android is crucial to prevent unauthorized access to sensitive data.
- Guidelines for implementing restricted access, securing broadcast intents, and handling sensitive data are provided.
- Risks and compliant solutions for directory traversal vulnerabilities, logging sensitive information, and caching data are discussed.
- Best practices for using WebView, native methods, exception handling, and SSL communication are outlined to enhance security.

## Screenshot



## Wordcloud



## Hosting Information

🌐 [blog.devsecopsguides.com](https://blog.devsecopsguides.com)

First resource	2023-11-20
Last resource	2024-03-11
Resources	4

ISP	Cloudflare, Inc.
Location	United States
DNS	cloudflare.com
Ports	8080, 2082, 2083, 2086,

## Filters

Full-Text Search

Text

URL

URL

Tag

c[vw]e-

Type

n/a

news

oss

post

## Featured

ctoatncsc

dailyswig

int3

pentesterlab

## Date Range

dd / mm / yyyy - dd / mm / yyyy

## Ordering

Hot



Showing resources 1 to 10 of 78

« 1 2 3 4 5 6 ... »

Past 3 days 10 / page

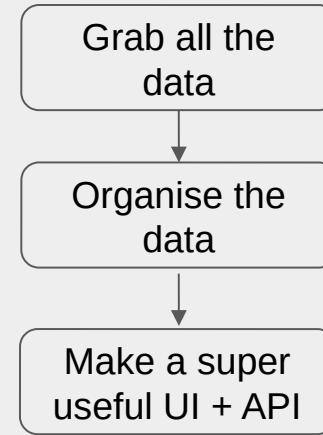
- Attacking Android 1 day ago - [blog.devsecopsguides.com](#) post
- CVE-2024-22857: Critical Flaw in Popular Zlog Library Opens Door to Arbitrary Code Execution 1 day ago - [securityonline.info](#) news
- Formation of the Open Source Digital Forensics Developer's Council 2 days ago - [sleuthkitlabs.com](#) post
- Game of Active Directory (GOAD) | Ludus 3 days ago - [docs.ludus.cloud](#) post
- Robots Dream of Root Shells 1 day ago - [blog.isosceles.com](#) post
- CVE-2024-23897 - Arbitrary file read in Jenkins 1 day ago - [blog.securelayer7.net](#) post
- GitHub - Oxor0ne/awesome-list: Cybersecurity oriented awesome list 1 day ago - [github.com/Oxor0ne](#) oss
- BianLian GOs for PowerShell After TeamCity Exploitation 2 days ago - [guidepointsecurity.com](#) post
- CVE-2024-21378 — Remote Code Execution in Microsoft Outlook 1 day ago - [netspi.com](#) post
- NextChat: An AI Chatbot That Lets You Talk to Anyone You Want To 1 day ago - [horizon3.ai](#) news

Reset

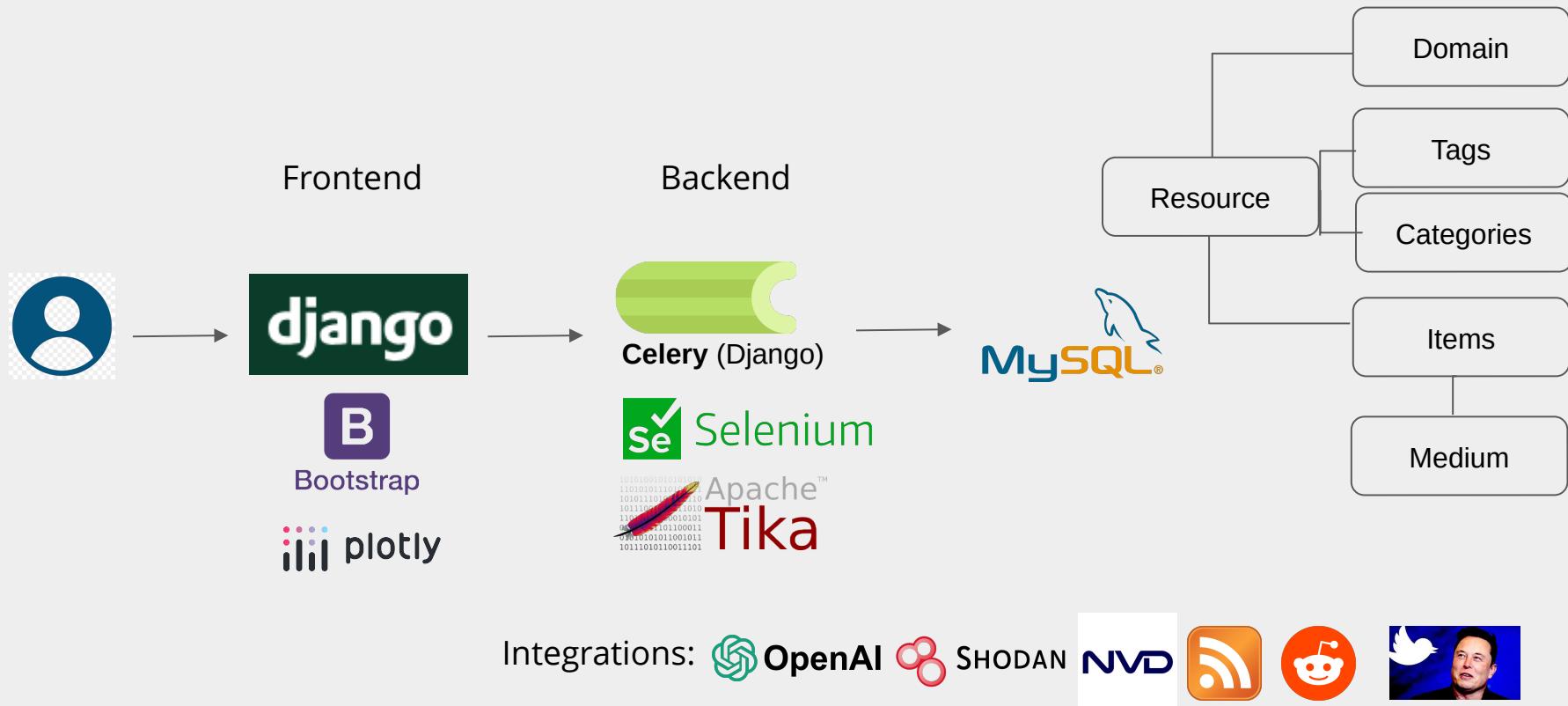
Apply

# General goals

- Make a smart infosec library that's fully automated and allows various use-cases.
- Perform a mix of content analysis to extract useful features and enrich the data-set.
- Iterate some considered algorithms to classify/rank infosec resources in the system.
- Simple UI + mobile friendly app.
- API for integrations.



# Architecture (simplified)



# Data Feeds

- 1) Initial seeds:
  - Reddit, Twitter
  - Conference archives (Blackhat, USENIX Security, CCC, Recon etc.)
- 2) Find RSS feed
- 3) Subscribe to RSS feed
  - Automatic when reputation high (otherwise need manual vetting)
  - Reputation based on Home site score
    - Featured by curators
    - Avg score of resources
- 4) Go back to 1

# Content Analysis

- Download resource

- Use headless browser
- Save raw data to S3 bucket

- Extract content

- main article only (exclude footer/sidebar)

- Parse content

- Find CVEs/CWEs
- Find cross-references to other resources

## Vulns

[CVE-2021-44228](#)

10.0

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12....)

CWE-20: Improper Input Validation

CWE-400: Uncontrolled Resource Consumption

CWE-502: Deserialization of Untrusted Data

CWE-917: Improper Neutralization of Special Elements used in an Expression

Language Statement ('Expression Language Injection')

2021-12-10

- CVE info via the NVD API

## References

- π How to Generate Secure Random Numbers in Various Programming Languages - Paragon Initiative Enterprises Blog [app](#) post  
7 years ago - [paragonie.com](#)
- ⌚ TIFU by using Math.random() [post](#)  
8 years ago - [betalbe.medium.com](#)
- ⌚ Myths about /dev/urandom - Thomas' Digital Garden [type n/a](#)  
10 years ago - [Zuo.de](#)

- Cross references to other resources

# Username Enumeration against OpenSSH/SELinux with CVE-2015-3238 | Trustwave | SpiderLabs

— trustwave.com

Trustwave is a leading cybersecurity and managed security services provider focused on threat detection and response. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries.

4 min read

## Key Details

**URL** <https://www.trustwave.com/Resources/SpiderLabs-Blog/Username-Enumeration-against-OpenSSH-SELinux-with-CVE-2015-3238/>  

**Age** 8 years ago

**Tags** cve-2014-9034 cve-2014-9016 cve-2006-5229 cve-2003-0190

## Vulns

**CVE-2014-9034** 5.0  
wp-includes/class-phpass.php in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9...  
CWE-19: Data Processing Errors 2014-11-25

**CVE-2014-9016** 5.0  
The password hashing API in Drupal 7.x before 7.34 and the Secure Password ... 2014-11-24

**CVE-2006-5229** 2.6  
OpenSSH portable 4.1 on SUSE Linux, and possibly other platforms and versio...  
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor 2006-10-10

**CVE-2003-0190** 5.0  
OpenSSH-portable (OpenSSH) 3.6.1p1 and earlier with PAM support enabled i... 2003-05-12

## References

Drupal Denial of Service Responsible Disclosure - Attacking with long passwords 9 years ago - [behindthefirewalls.com](http://behindthefirewalls.com)

r/netsec    post

## Screenshot



## Wordcloud



## Hosting Information

 [trustwave.com](https://www.trustwave.com)

<b>First resource</b>	2010-03-15	<b>ISP</b>	Microsoft Corporation
<b>Last resource</b>	2024-03-12	<b>Location</b>	Japan
<b>Resources</b>	95	<b>DNS</b>	akam.net
		<b>Ports</b>	80

# Content Analysis

- Screenshots
- Wayback Machine
- RSS feeds
- Curators
- Scoring
- etc.

# GraphQL API

< Docs



## ResourceNode

Implements

Node

Fields

uuid: UUID!

type: TalkbackResourceTypeChoices!

url: String!

createdAt: DateTime!

```
1
2  query {
3    resources(q:"log4j") {
4      edges {
5        node {
6          id
7          url
8          title
9        }
10     }
11   }
12 }
```

```
{
  "data": {
    "resources": [
      {
        "edges": [
          {
            "node": {
              "id": "405eeb61-9882-4973-a934-73848f937011",
              "url": "https://www.greynoise.io/blog/battling-ransomware-one-tag-at-a-time",
              "title": "Battling Ransomware One Tag At A Time | GreyNoise Blog"
            }
          }
        ]
      }
    ]
  }
}
```

Home / Profile

## Profile

Email

seb@elttam.com

Password

\*\*\*\*\*

API Token

eyJhbGci...

Delete account

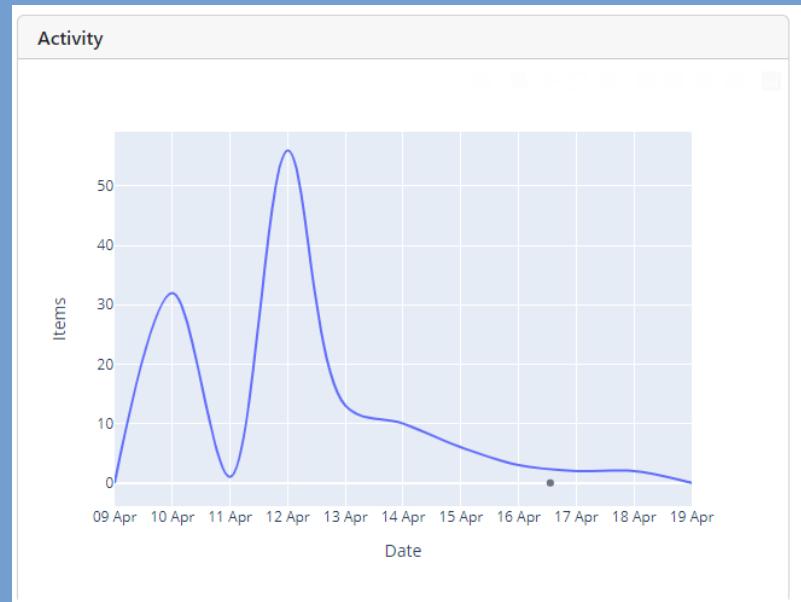
Permanently delete your account.

# GraphQL API

- Demo - Searching for functions

# Challenges

- Duplicates
  - Unwind URL
  - URL c14n (query params order)
  - Remove tracking tokens (?utm\_ etc.)
  - Look at <link ref="canonical" href="...">
- Twitter
- Bot protections (e.g. Cloudflare)
- Resource Home
  - [github.com/foo/repo](https://github.com/foo/repo) → [github.com/foo](https://github.com/foo)
  - [medium.com/@foo](https://medium.com/@foo) → [foo.medium.com](https://foo.medium.com)
  - [blog.google/tech/blah.html](https://blog.google/tech/blah.html) → [blog.google/tech](https://blog.google/tech)



- Number of tweets per day for a resource URL

# Challenges

- Finding the right RSS feed
- OpenAI inconsistencies (hallucinations?)
  - Even with temperature=0
  - Rare
- Resource scoring

$$\text{Resource Score} = Ss * Sw + Fs * Fw + Xs * Xw$$

$S\{s, w\}$ : Social media score & weight

$F\{s, w\}$ : Featured score & weight

$X\{s, w\}$ : Xref score (avg score of all referenced resources) & weight

$$Sw + Fw + Xs = 1.0$$

# Future

- Parse CPEs
  - Ability to search for vendor/product (device, OS, app ...)
- Improve resource type classifier (no more `n/a` type)
- Non-English resources
- Improve UI/UX
- More tailored UI views
  - Break down by Vulnerabilities, Technologies
  - Dashboard
- Smart newsletter (weekly curated list)

---

# Thanks!

---

<https://talkback.sh/>

<https://elttam.com/blog/talkback-intro/>



Follow us for updates