Keeping up with the Pwnses

An overview of Talkback

elttam

Hi!

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

What: https://talkback.sh/

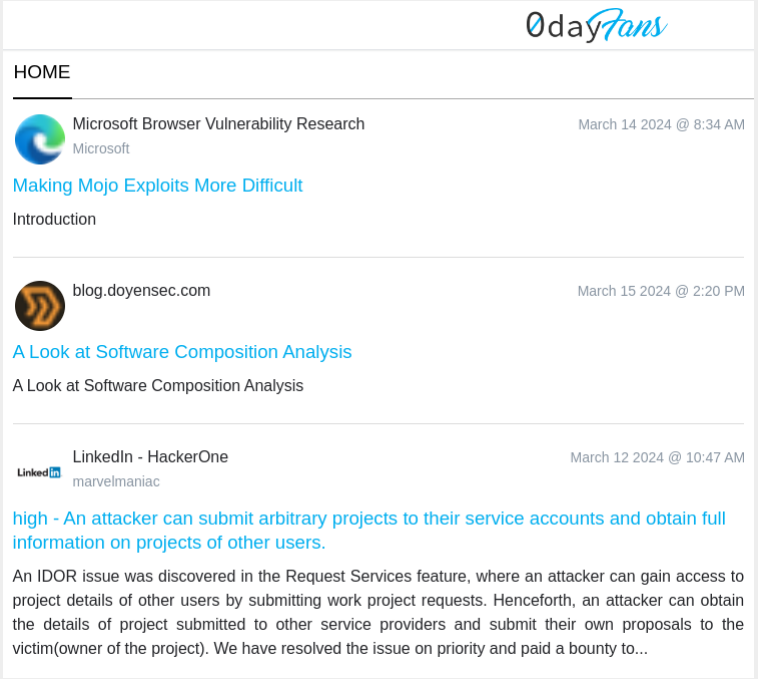
Why: Keeping up with infosec is hard

Main motivators:

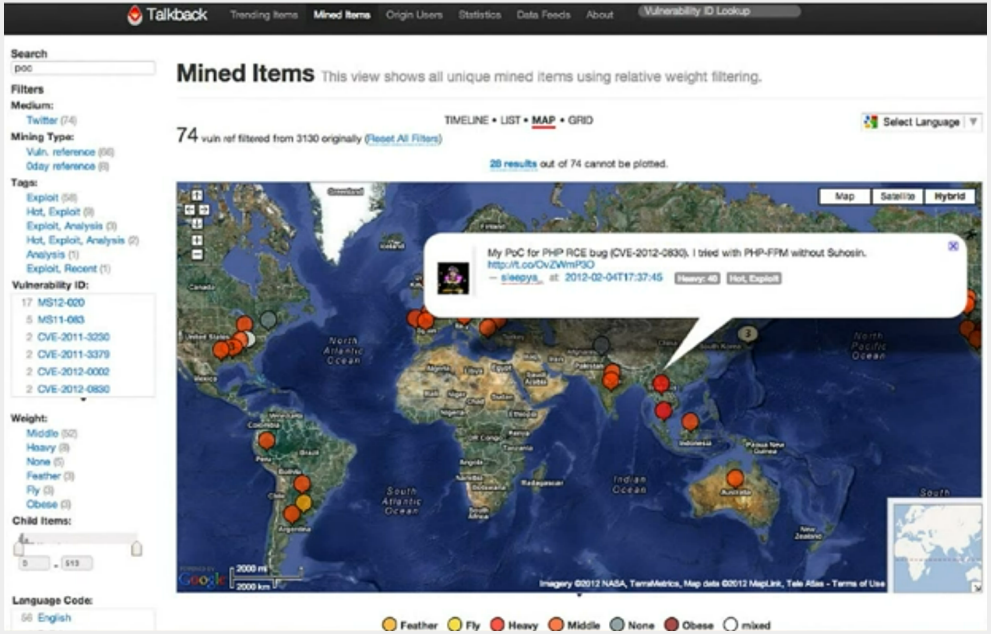
- Keep up with infosec more efficiently.
- Get to relevant technical information faster.
- Support a bunch of our own use-cases.

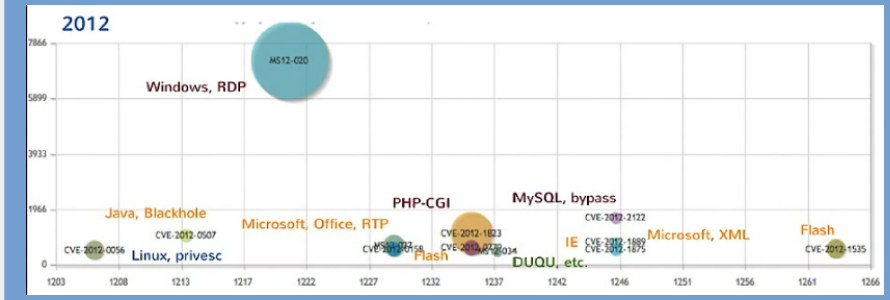
Smart?

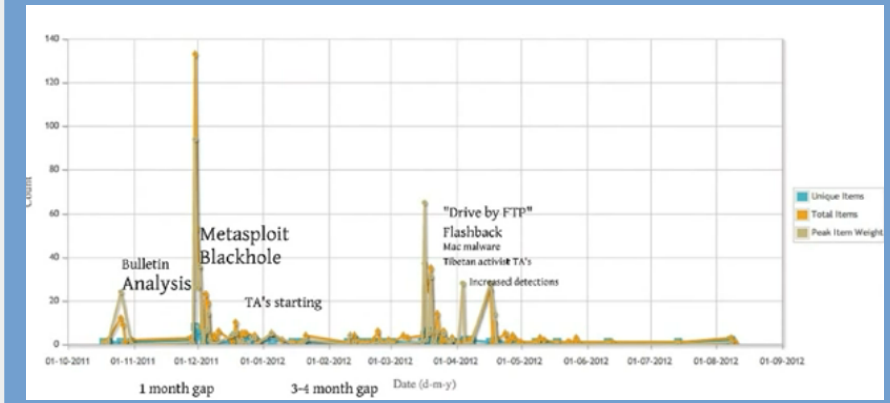
- Smart infosec aggregator
- Similar projects (we know of)
  - https://0dayfans.com/
  - https://allinfosecnews.com/
  - https://hacker-trends.com/
  - https://threatable.io/
  - https://morningstarsecurity.com/news
  - https://hackdojo.io/



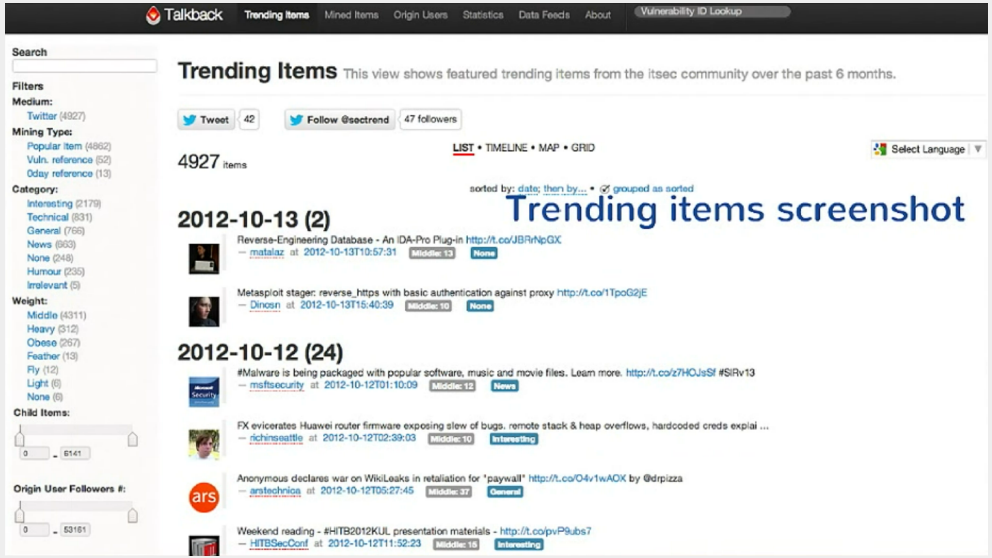
Original version from 2010-2012

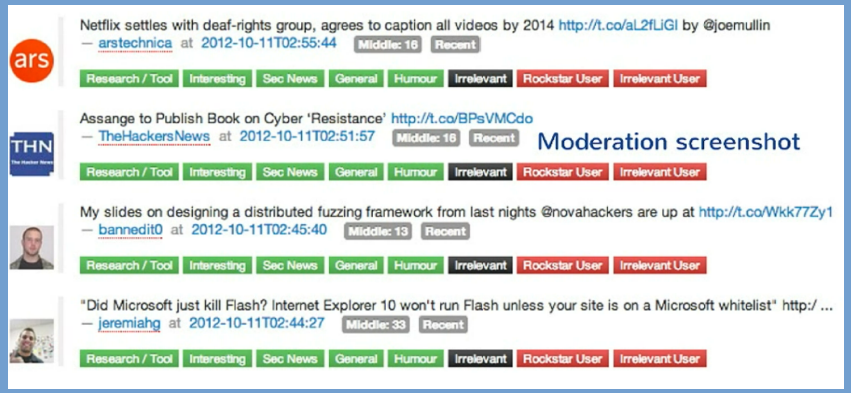






Original version from 2010-2012





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

Showing resources 1 to 10 of 78

Past 3 days 10 / page

Attacking Android app crypto net
1 day ago - blog.devsecopsguides.com
post

CVE-2024-22857: Critical Flaw in Popular Zlog Library Opens Door to Arbitrary Code Execution app exp
1 day ago - securityonline.info
news

Formation of the Open Source Digital Forensics Developer's Council for
2 days ago - sleuthkitlabs.com
post

Game of Active Directory (GOAD) | Ludus
3 days ago - docs.ludus.cloud
type n/a

Robots Dream of Root Shells app exp sys
1 day ago - blog.isosceles.com
post

CVE-2024–23897 – Arbitrary file read in Jenkins app exp net
1 day ago - blog.securelayer7.net
post

GitHub - 0xor0ne/awesome-list: Cybersecurity oriented awesome list
1 day ago - github.com/0xor0ne
oss

BianLian GOs for PowerShell After TeamCity Exploitation exp net mal
2 days ago - guidepointsecurity.com
post

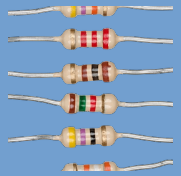
CVE-2024-21378 — Remote Code Execution in Microsoft Outlook app exp net
1 day ago - netspi.com
post

NextChat: An AI Chatbot That Lets You Talk to Anyone You Want To app cloud
1 day ago - horizon3.ai
news

Curators

ThinkstScapes Quarterly
- https://thinkst.com/ts

tl;dr sec
- https://tldrsec.com/



INT3
- https://int3.substack.com/

Risky Biz
- https://risky.biz/
- https://riskybiznews.substack.com/
- https://srslyriskybiz.substack.com/

PentesterLab Weekly
- https://x.com/pentesterlab

CTO at NCSC
- https://ctoatncsc.substack.com/

Talkback | Home | Technical | News | Featured | Saved | About | Search

Showing resources 1 to 10 of 6551

« 1 2 3 4 5 6 ... »

My first impressions of web3 crypto
2 years ago - - moxie.org

Can you trust ChatGPT's package recommendations? mal
9 months ago - - vulcan.io

New attack campaign utilized a new 0-day RCE vulnerability on Microsoft Exchange Server | Blog | GTSC exp
1 year ago - - gteltsc.vn

How I made $31500 by submitting a bug to Facebook exp
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

My first impressions of web3
— *moxie.org* 14 min
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

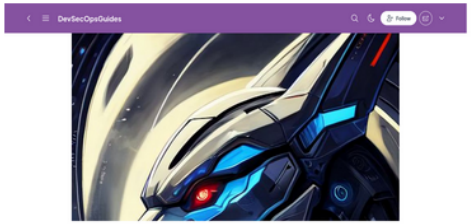
Open Destination | View Full Details | Close

Showing resources 1 to 10 of 78

- Attacking Android app crypto net
  1 day ago - 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
- Formation of the Open Source Digital Forensics Developer's Council for
  2 days ago - sleuthkitlabs.com
- Game of Active Directory (GOAD) | Ludus
  3 days ago - docs.ludus.cloud
- Robots Dream of Root Shells app exp sys
  1 day ago - blog.isosceles.com
- CVE-2024–23897 – Arbitrary file read in Jenkins app exp net
  1 day ago - blog.securelayer7.net
- GitHub - 0xor0ne/awesome-list: Cybersecurity oriented awesome list
  1 day ago - github.com/0xor0ne
- BianLian GOs for PowerShell After TeamCity Exploitation exp net mal
  2 days ago - guidepointsecurity.com
- CVE-2024-21378 — Remote Code Execution in Microsoft Outlook app exp net
  1 day ago - netspi.com
- NextChat: An AI Chatbot That Lets You Talk to Anyone You Want To app cloud
  1 day ago - horizon3.ai

Showing resources 1 to 10 of 78

« 1 2 3 4 5 6 ... »



Attacking Android

Attacking Android

— *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.

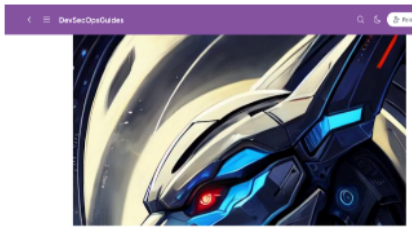
Access control for ContentProvider in Android is crucial to prevent unauthorized access to sensitive data.

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



Attacking Android

Attacking Android
— *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

Talkback Home Technical News Featured Saved About Search Search Sign in

Showing resources 1 to 2 of 2 « 1 » Past 50 years 10 / page

Attacking Android app crypto net
1 week ago - blog.devsecopsguides.com post

Formation of the Open Source Digital Forensics Developer's Council for
1 week ago - sleuthkitlabs.com post

Attacking Android

— *blog.devsecopsguides.com*

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	https://blog.devsecopsguides.com/attacking-android
Age	1 day ago
Categories	appsec cryptography netsec

OpenAI Summary

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

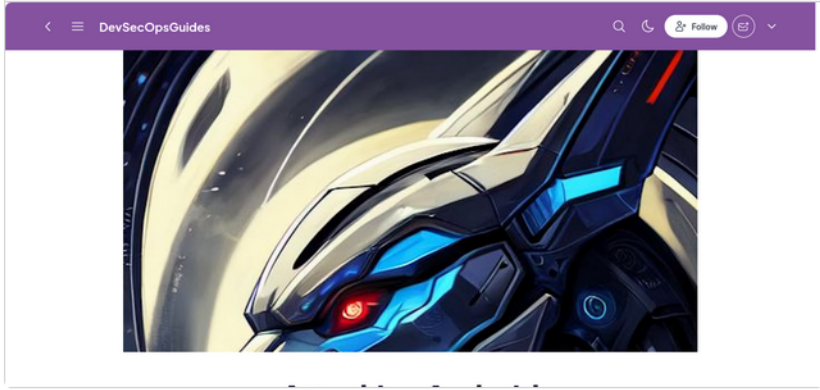
- Access control for ContentProvider in Android is crucial to prevent unauthorized access to sensitive data.

- 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



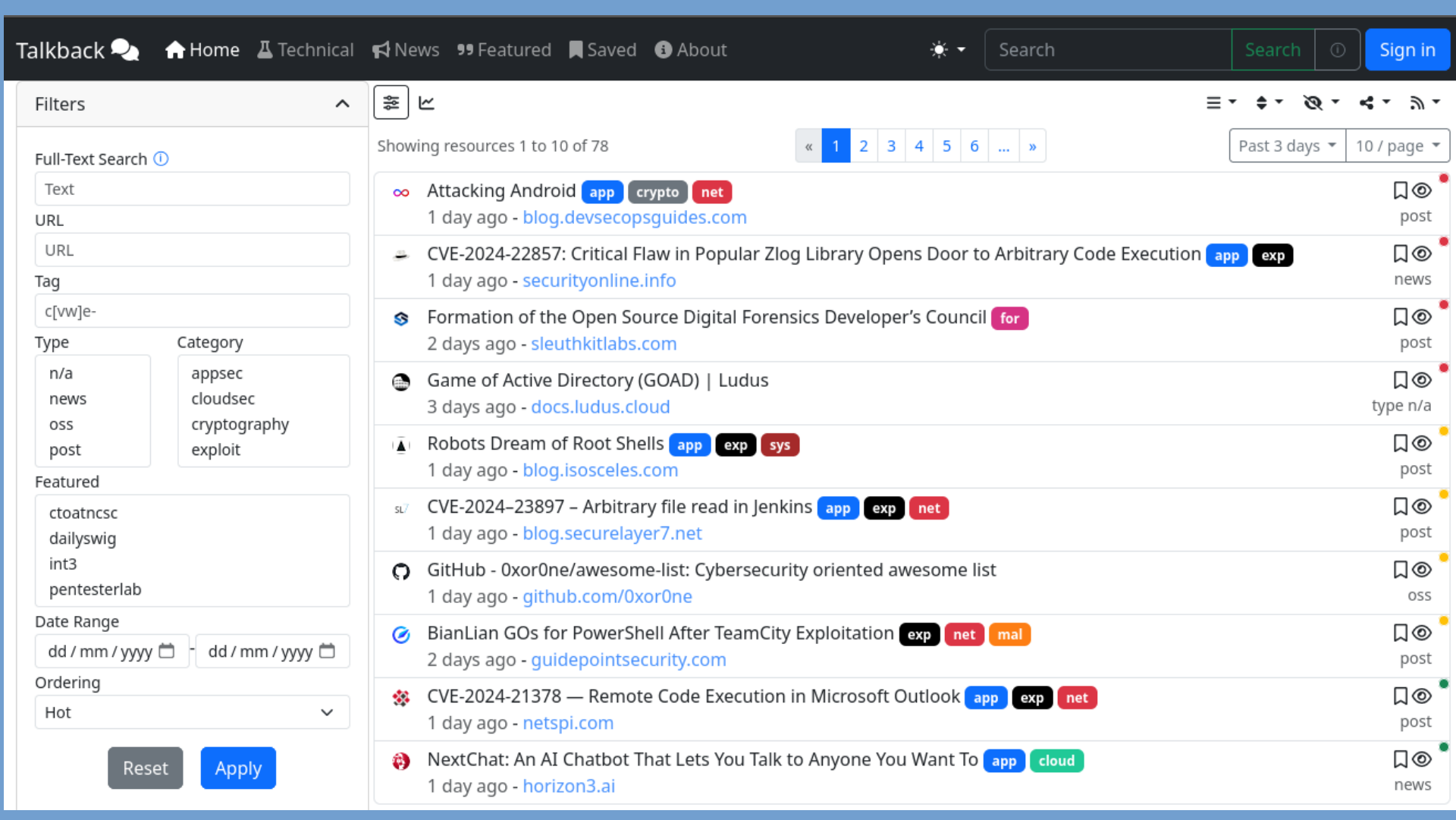
Wordcloud

Hosting Information

blog.devsecopsguides.com

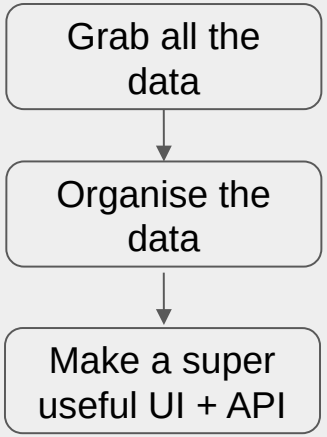
First resource	2023-11-20
Last resource	2024-03-11
Resources	4

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

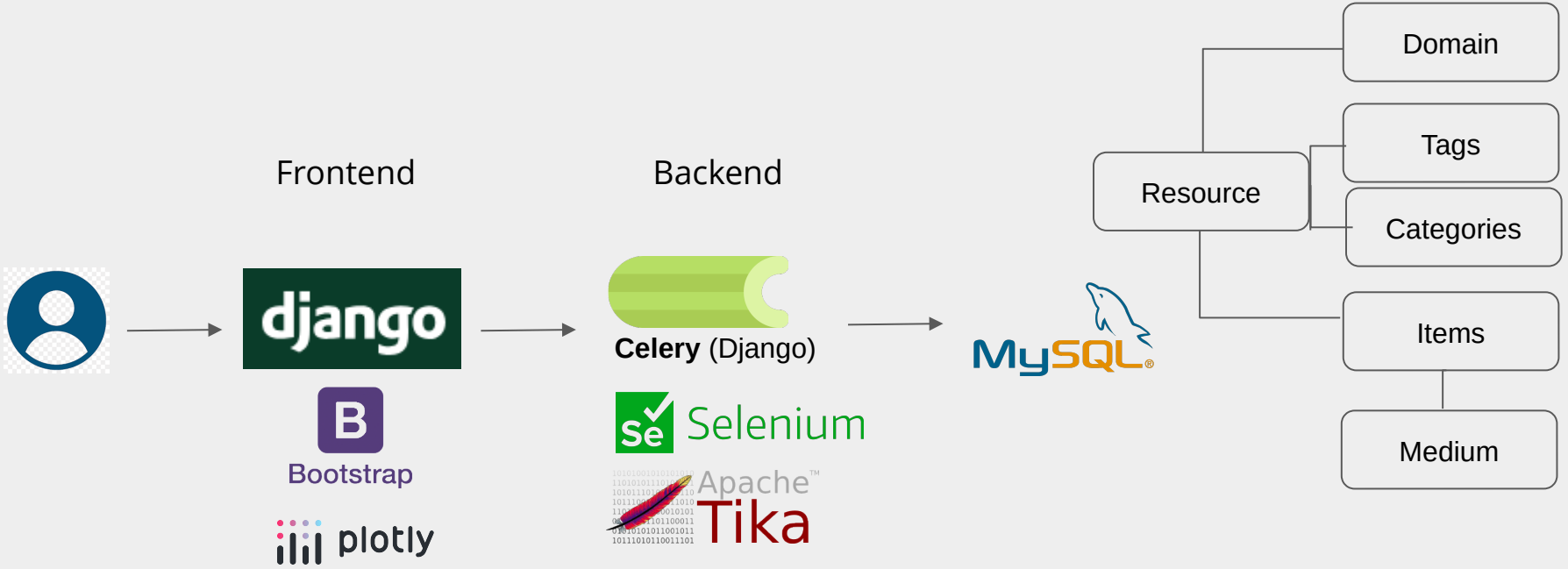

Talkback
Home
Technical
News
Featured
Saved
About
Search
Search
Sign in
Filters
Full-Text Search
Text
URL
URL
Tag
c[vw]e-
Type
n/a
news
oss
post
Category
appsec
cloudsec
cryptography
exploit
Featured
ctoatncsc
dailyswig
int3
pentesterlab
Date Range
dd / mm / yyyy
dd / mm / yyyy
Ordering
Hot
Reset
Apply
Showing resources 1 to 10 of 78
« 1 2 3 4 5 6 ... »
Past 3 days
10 / page
Attacking Android app crypto net
1 day ago - blog.devsecopsguides.com
post
CVE-2024-22857: Critical Flaw in Popular Zlog Library Opens Door to Arbitrary Code Execution app exp
1 day ago - securityonline.info
news
Formation of the Open Source Digital Forensics Developer's Council for
2 days ago - sleuthkitlabs.com
post
Game of Active Directory (GOAD) | Ludus
3 days ago - docs.ludus.cloud
type n/a
Robots Dream of Root Shells app exp sys
1 day ago - blog.isosceles.com
post
CVE-2024–23897 – Arbitrary file read in Jenkins app exp net
1 day ago - blog.securelayer7.net
post
GitHub - 0xor0ne/awesome-list: Cybersecurity oriented awesome list
1 day ago - github.com/0xor0ne
oss
BianLian GOs for PowerShell After TeamCity Exploitation exp net mal
2 days ago - guidepointsecurity.com
post
CVE-2024-21378 — Remote Code Execution in Microsoft Outlook app exp net
1 day ago - netspi.com
post
NextChat: An AI Chatbot That Lets You Talk to Anyone You Want To app cloud
1 day ago - horizon3.ai
news

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)



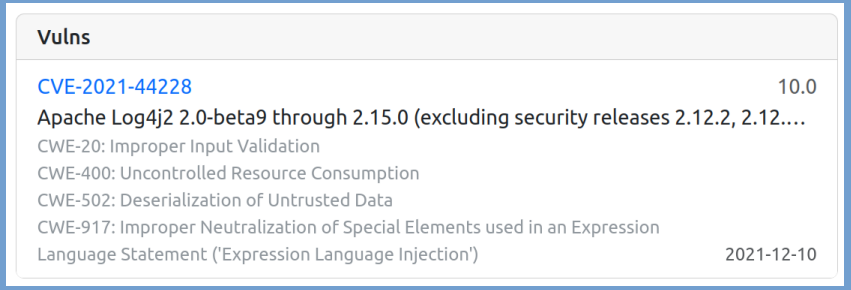
Integrations: OpenAI SHODAN NVD

Data Feeds

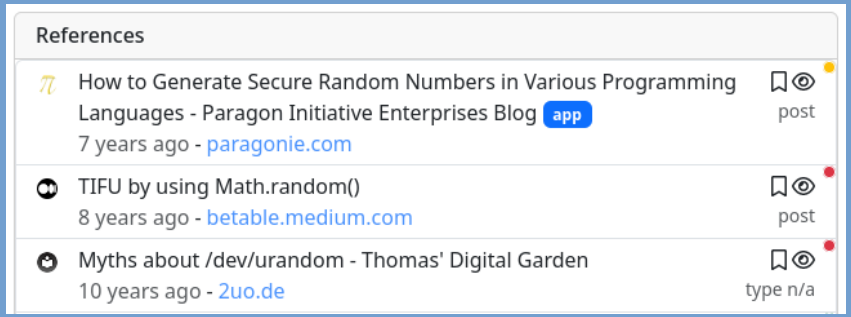
1) Initial seeds:
   - Reddit, Twitter
   - Conference archives (Blackhat, USENIX Security, CCC, Recon etc.)
2) Find RSS feed
3) Subscribe to RSS feed
   - Automatic when reputation high (otherwise need manual vetting)
   - Reputation based on Home site score
     - Featured by curators
     - Avg score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



- CVE info via the NVD API



- 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

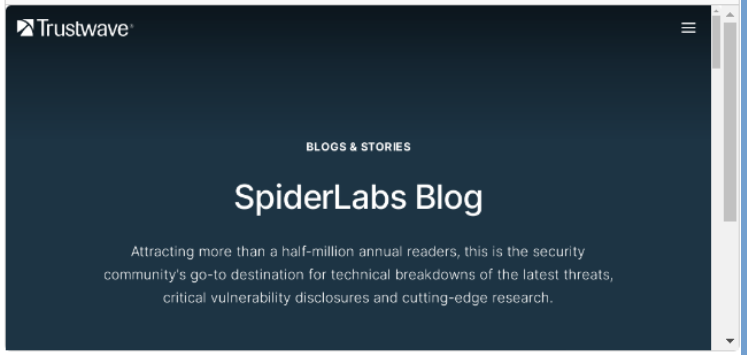
CVE-2006-5229 2.6
OpenSSH portable 4.1 on SUSE Linux, and possibly other platforms and versio...
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor 2006-10-10

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 r/netsec post
9 years ago - behindthefirewalls.com

Screenshot



Wordcloud

Hosting Information

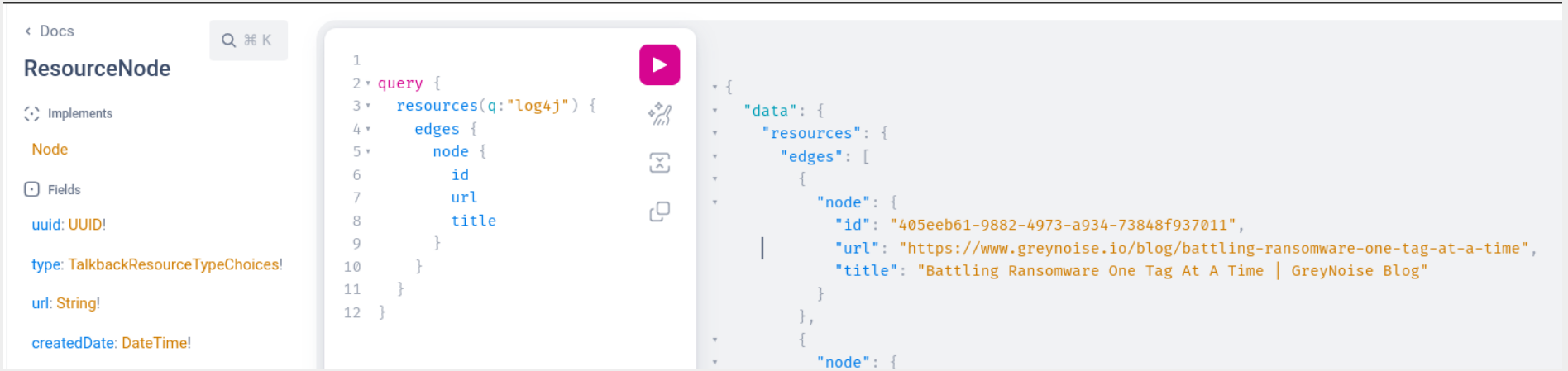
trustwave.com

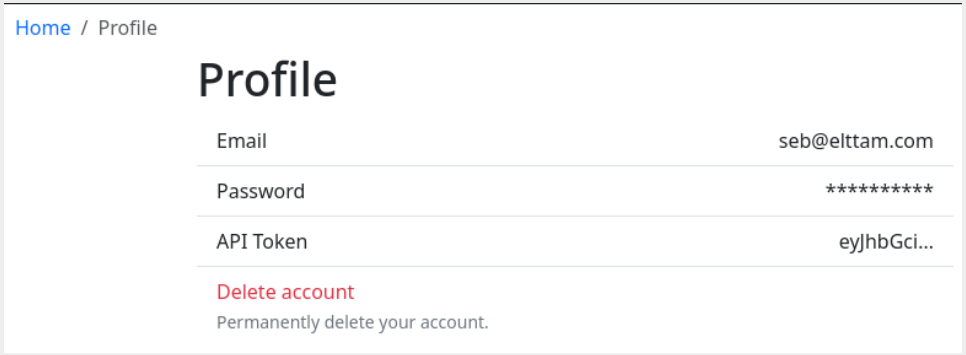
First resource	2010-03-15	**ISP**	Microsoft Corporation
Last resource	2024-03-12	**Location**	Japan
Resources	95	**DNS**	akam.net
		Ports	80

Content Analysis

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

GraphQL API


Docs
⌘ K
ResourceNode
Implements
Node
Fields
uuid: UUID!
type: TalkbackResourceTypeChoices!
url: String!
createdDate: DateTime!
query {
resources(q:"log4j") {
edges {
node {
id
url
title
}
}
}
}
{
"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"
}
},
{
"node": {

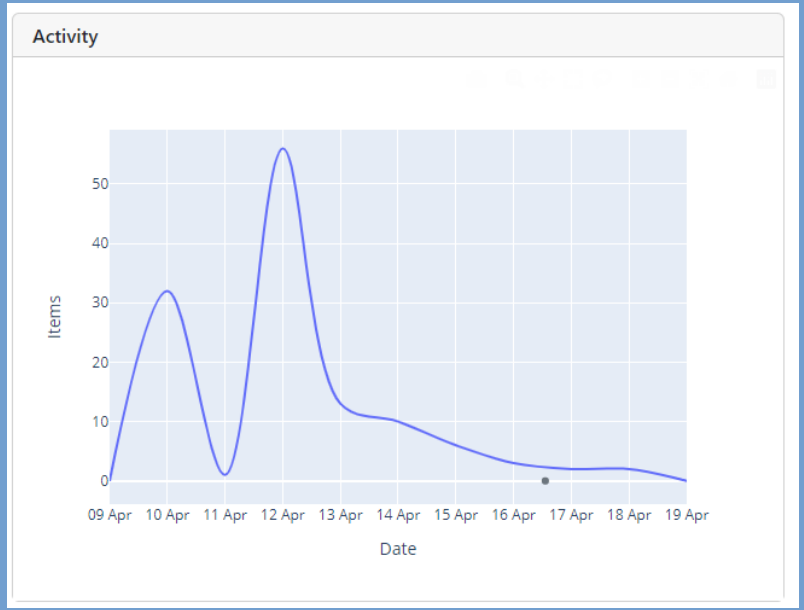

Home / Profile
Profile
Email
seb@elttam.com
Password
****
API Token
eyJhbGci...
Delete account
Permanently delete your account.

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 → github.com/foo
  - medium.com/@foo → foo.medium.com
  - blog.google/tech/blah.html → 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

$$
\begin{gathered}
Resource\ Score\ =\ Ss * Sw\ +\ Fs * Fw\ +\ Xs * Xw \\
S\{s, w\}:\ Social\ media\ score\ \&\ weight \\
F\{s, w\}:\ Featured\ score\ \&\ weight \\
X\{s, w\}:\ Xref\ score\ (avg\ score\ of\ all\ referenced\ resources)\ \&\ weight \\
Sw\ +\ Fw\ +\ Xs\ =\ 1.0
\end{gathered}
$$

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