

MICHIGAN STATE

U N I V E R S I T Y

Alpha Presentation

Open Source Intel

The Capstone Experience

Team GM

Ben Buscarino

Will Crecelius

Taylor Zachar

Qiming Ren

Igli Ndoj

Department of Computer Science and Engineering
Michigan State University

Spring 2020



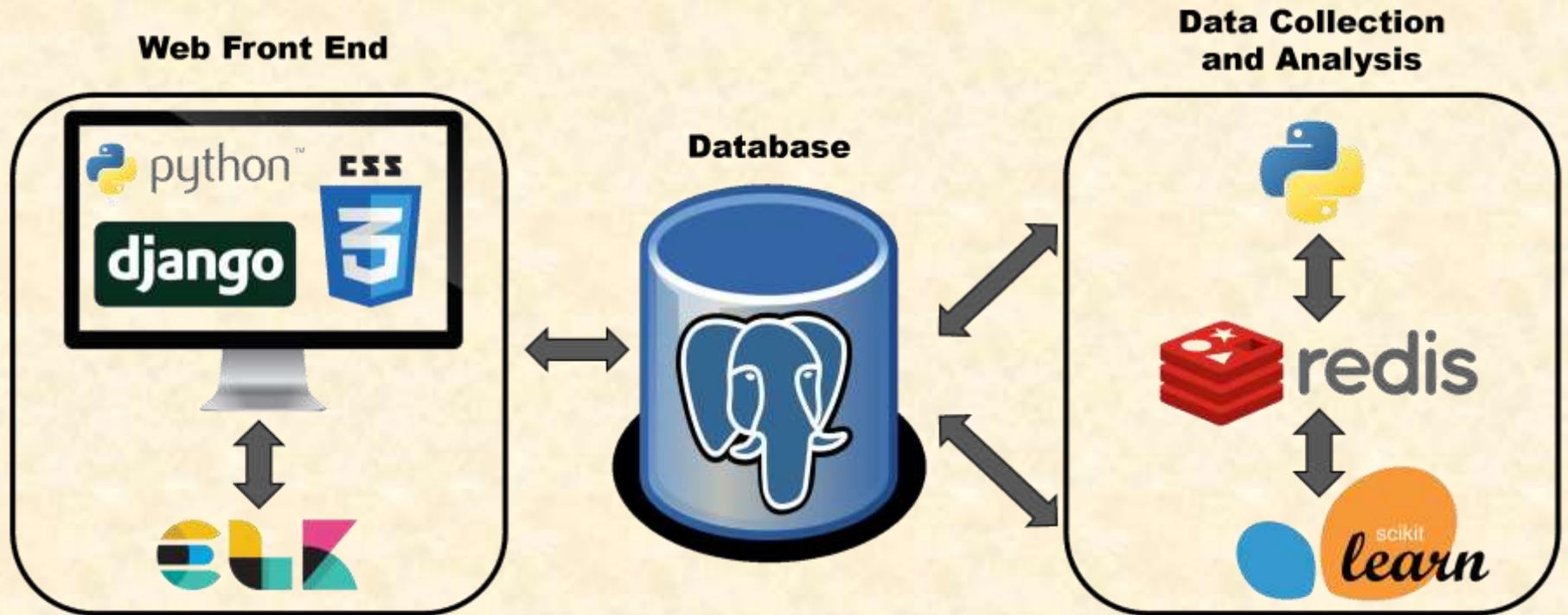
*From Students...
...to Professionals*

Project Overview

- Scan public repositories such as GitHub, PasteBin, BitBucket for leaked GM intellectual property.
- Assign a confidence rating to a leak with machine learning.
- Display the leaks and a URL to the leak in a web application frontend.



System Architecture



Dashboard



Leaks Page

The screenshot displays the 'New Leaks' page in the Open Source Intel application. The page features a dark sidebar with navigation options: Dashboard, Crawler Status, Search, Profile, New Leaks (1), High Confidence Leaks (1), and Resolved Leaks (1). The main content area shows a summary of leak statistics and a table of individual leaks.

Summary:

- LEAKS DETECTED: 6
- NEW LEAKS: 2
- HIGH CONFIDENCE LEAKS: 1
- RESOLVED LEAKS: 1

Table:

Leak ID	Leak Link	Status	Date Created	Date Discovered
1		No Tags	02-18-2020	02-18-2020
2		No Tags	02-18-2020	02-18-2020
3		No Tags	02-18-2020	02-18-2020
4		No Tags	02-18-2020	02-18-2020
5		No Tags	02-18-2020	02-18-2020
6		No Tags	02-18-2020	02-18-2020

Page 1 of 1.



Single Leak Page

The screenshot shows the Open Source Intel web application interface. The left sidebar contains navigation options: Dashboard, Crawler Status, Search, Profile, New Leaks (1), High Confidence Leaks (11), and Resolved Leaks (1). The main content area is titled 'Leak #2' and features two tables.

Summary Table:

Leak id	Status	Created At	Updated At
2	new	2020-02-18 03:28:20.371072+00:00	2020-02-18 03:28:20.440128+00:00

Hit List Table:

Leak id	Hit id	Content	Line	Created At
2	2	iginfo@gm.com	2	2020-02-18 03:28:20.380189+00:00
2	3	gm.com	2	2020-02-18 03:28:20.383915+00:00
2	4	naproxygm.com	14	2020-02-18 03:28:20.388458+00:00
2	5	aperaha01.ext.gm.com	15	2020-02-18 03:28:20.392257+00:00
2	6	naeraha02.ext.gm.com	16	2020-02-18 03:28:20.395514+00:00
2	7	saeraha01.ext.gm.com	17	2020-02-18 03:28:20.398709+00:00
2	8	eueraha05.ext.gm.com	18	2020-02-18 03:28:20.401527+00:00
2	9	aperaha02.ext.gm.com	19	2020-02-18 03:28:20.404090+00:00
2	10	aperaha01.ext.gm.com	20	2020-02-18 03:28:20.407120+00:00
2	11	aperaha03.ext.gm.com	21	2020-02-18 03:28:20.410234+00:00
2	12	aperaha04.ext.gm.com	22	2020-02-18 03:28:20.414460+00:00
2	13	nam.corp.gm.com	27	2020-02-18 03:28:20.419137+00:00
2	14	ext.gm.com	28	2020-02-18 03:28:20.422418+00:00
2	15	autoproxy.gm.com	29	2020-02-18 03:28:20.425991+00:00
2	16	eur.corp.gm.com	30	2020-02-18 03:28:20.431593+00:00
2	17	onstar.gm.com	31	2020-02-18 03:28:20.434702+00:00



Repository Page

The screenshot displays the Open Source Intel web application interface. On the left is a dark sidebar with navigation options: Dashboard, Crawler Status, Search, Profile, New Leaks (1), High Confidence Leaks (11), and Resolved Leaks (1). The main content area is titled "Repository: OSITest" and features a table with the following data:

Repo Name	Default Branch	Owner Id	Hash	Date Created	Last Updated	Last Scanned
OSITest	master	1	6cce0afbc0d2fd0e2b9817d4d05aaf6c3714c6aa	2020-02-18 03:28:16.426419+00:00	2020-02-18 03:28:31.613598+00:00	2020-02-18 03:28:31.613166+00:00

Below the table is an email composition form with the following fields:

- Sender (email):** opemsourceintel@gmail.com
- Recipient (email):** JohnDoe@gmail.com
- Subject Line:** Newly found repository with leak
- Message:** Hello John Doe, Open Source Intel has discovered a new leak. Please investigate the attached repository, it's owner, and any other closely related files. Report to me with any findings.

A blue "send" button is located at the bottom of the email form.



What's left to do?

- Scan and collect data from other public web open source hosts (BitBucket, PasteBin, etc.)
- Continue training and finetuning the machine learning module.
- Implement notification system and inter-user communication.



Questions?

?

?

?

?

?

?

?

?

?

