MICHIGAN STATE UNIVERSITY

Beta Presentation
Open Source Intel

The Capstone Experience

Team GM

Ben Buscarino
Will Crecelius
Igli Ndoj
Qiming Ren
Taylor Zachar

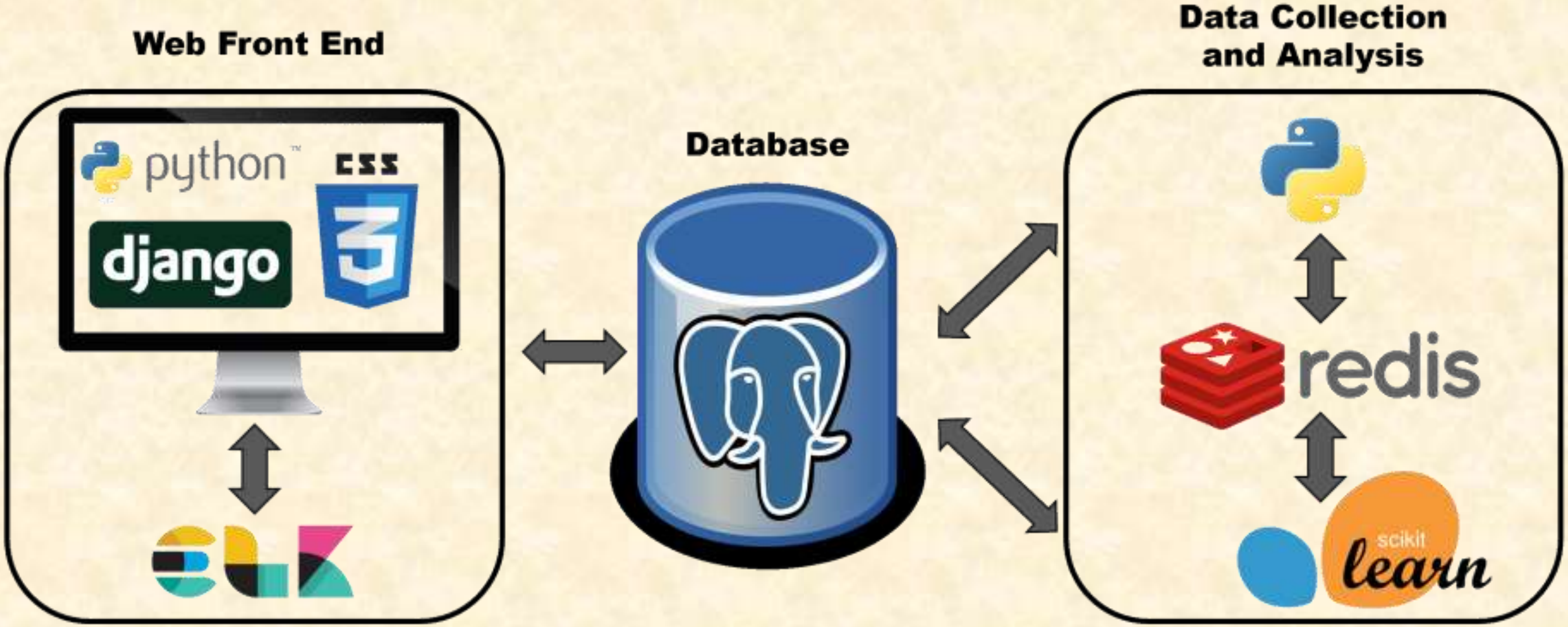
Department of Computer Science and Engineering
Michigan State University
Spring 2019

From Students…
…to Professionals

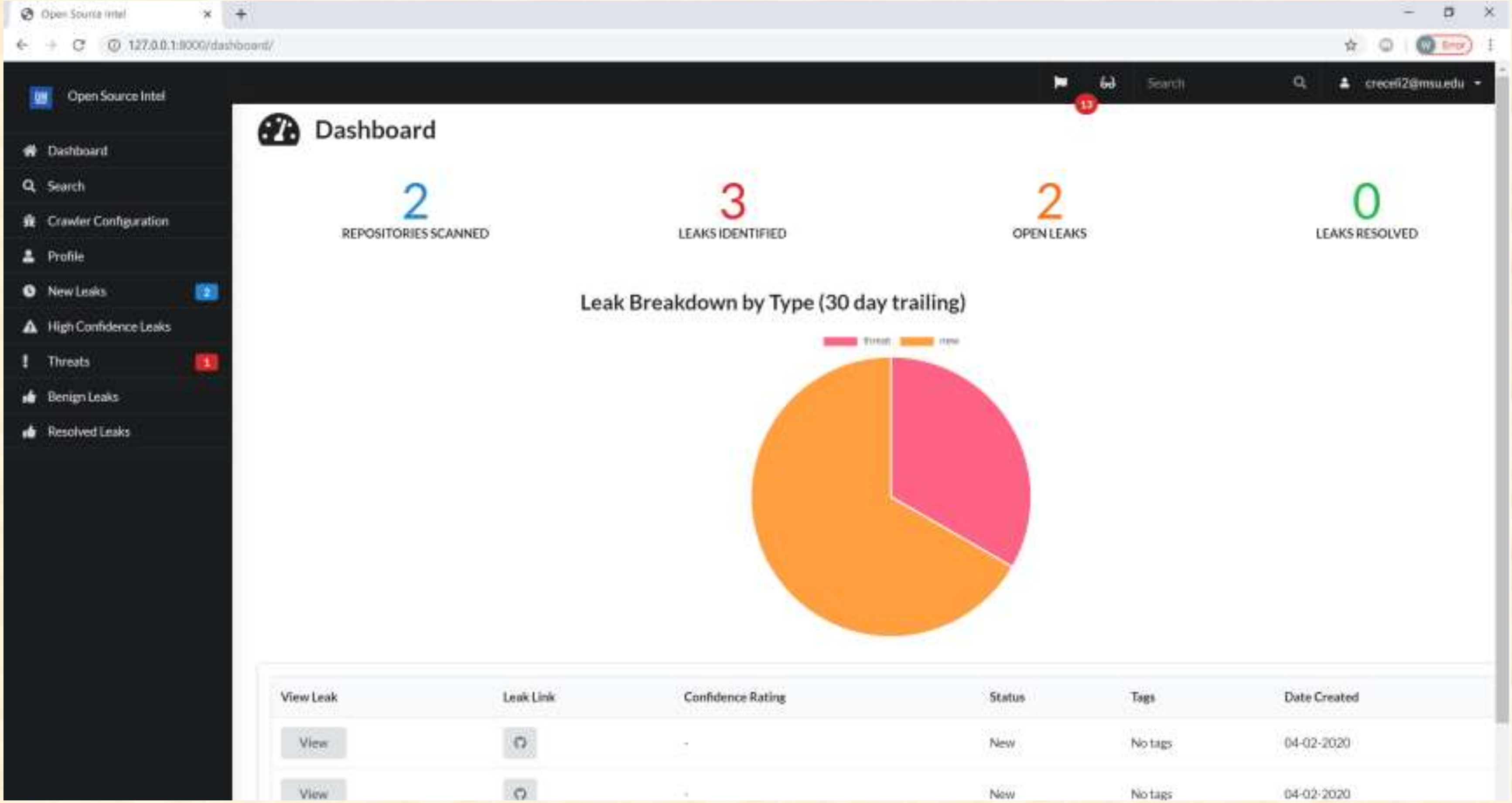
Project Overview

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

System Architecture



Dashboard



Open Source Intel

127.0.0.1:8000/dashboard/

Open Source Intel

- Dashboard
- Search
- Crawler Configuration
- Profile
- New Leaks 2
- High Confidence Leaks
- Threats 1
- Benign Leaks
- Resolved Leaks

Search

creceli2@msu.edu

Dashboard

2 REPOSITORIES SCANNED

3 LEAKS IDENTIFIED

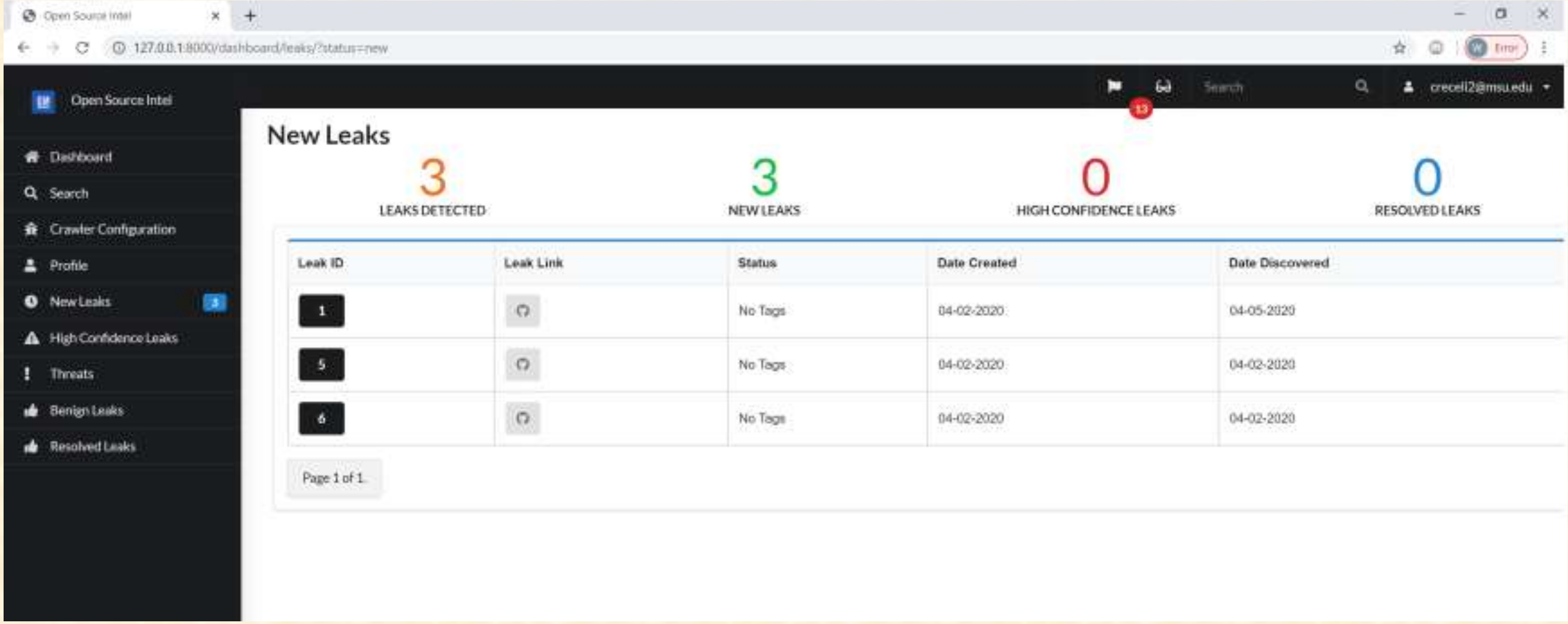
2 OPEN LEAKS

0 LEAKS RESOLVED

Leak Breakdown by Type (30 day trailing)

View Leak	Leak Link	Confidence Rating	Status	Tags	Date Created
View		-	New	No tags	04-02-2020
View		-	New	No tags	04-02-2020

Leaks Page



New Leaks

3 LEAKS DETECTED

3 NEW LEAKS

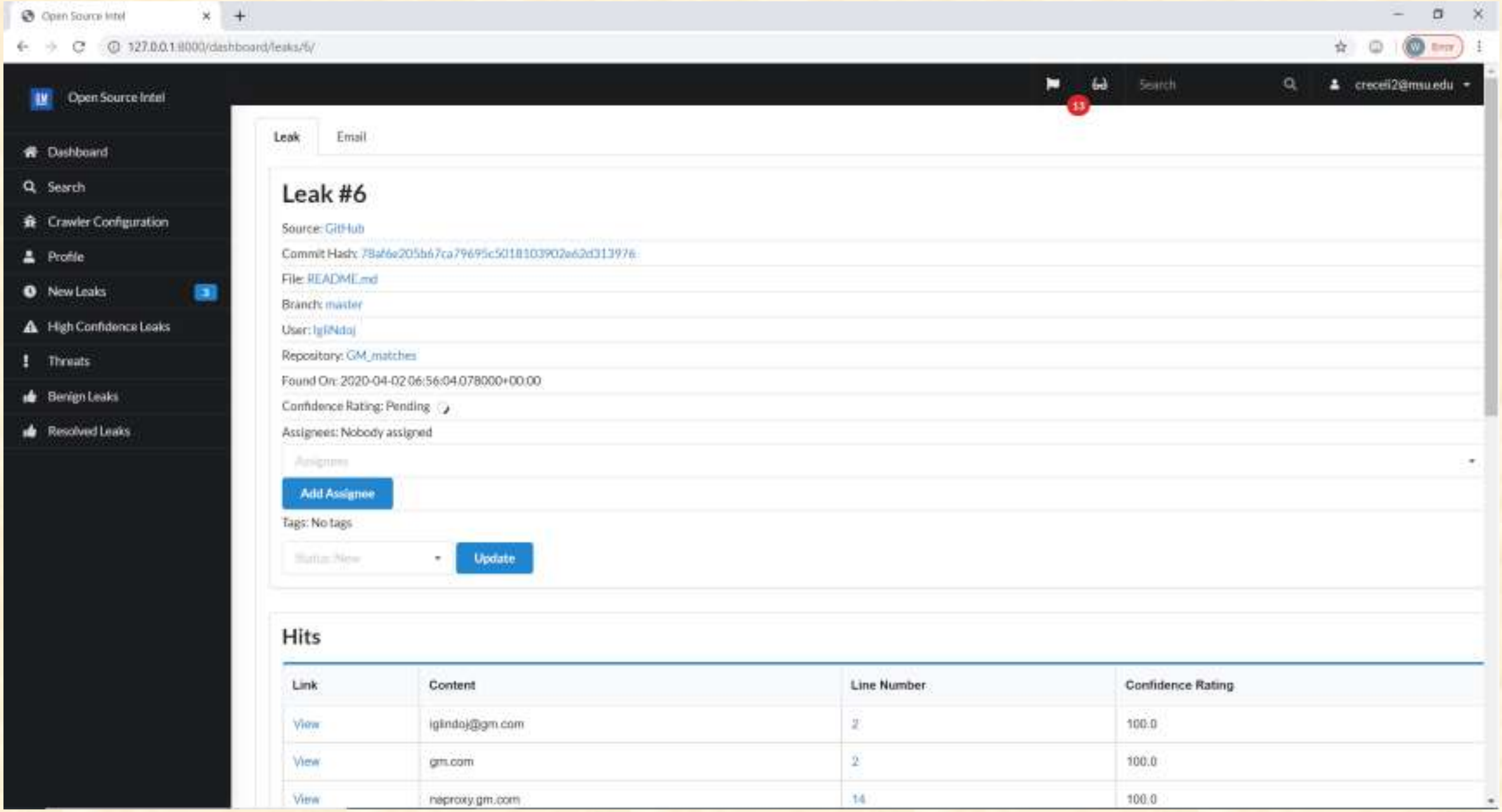
0 HIGH CONFIDENCE LEAKS

0 RESOLVED LEAKS

Leak ID	Leak Link	Status	Date Created	Date Discovered
1		No Tags	04-02-2020	04-05-2020
5		No Tags	04-02-2020	04-02-2020
6		No Tags	04-02-2020	04-02-2020

Page 1 of 1.

Single Leak Page



Leak #6

Source: GitHub

Commit Hash: 78af6e205b67ca79695c50181039O2e62d313976

File: README.md

Branch: master

User: IgliNdoj

Repository: GM_matches

Found On: 2020-04-02 06:56:04.078000+00:00

Confidence Rating: Pending

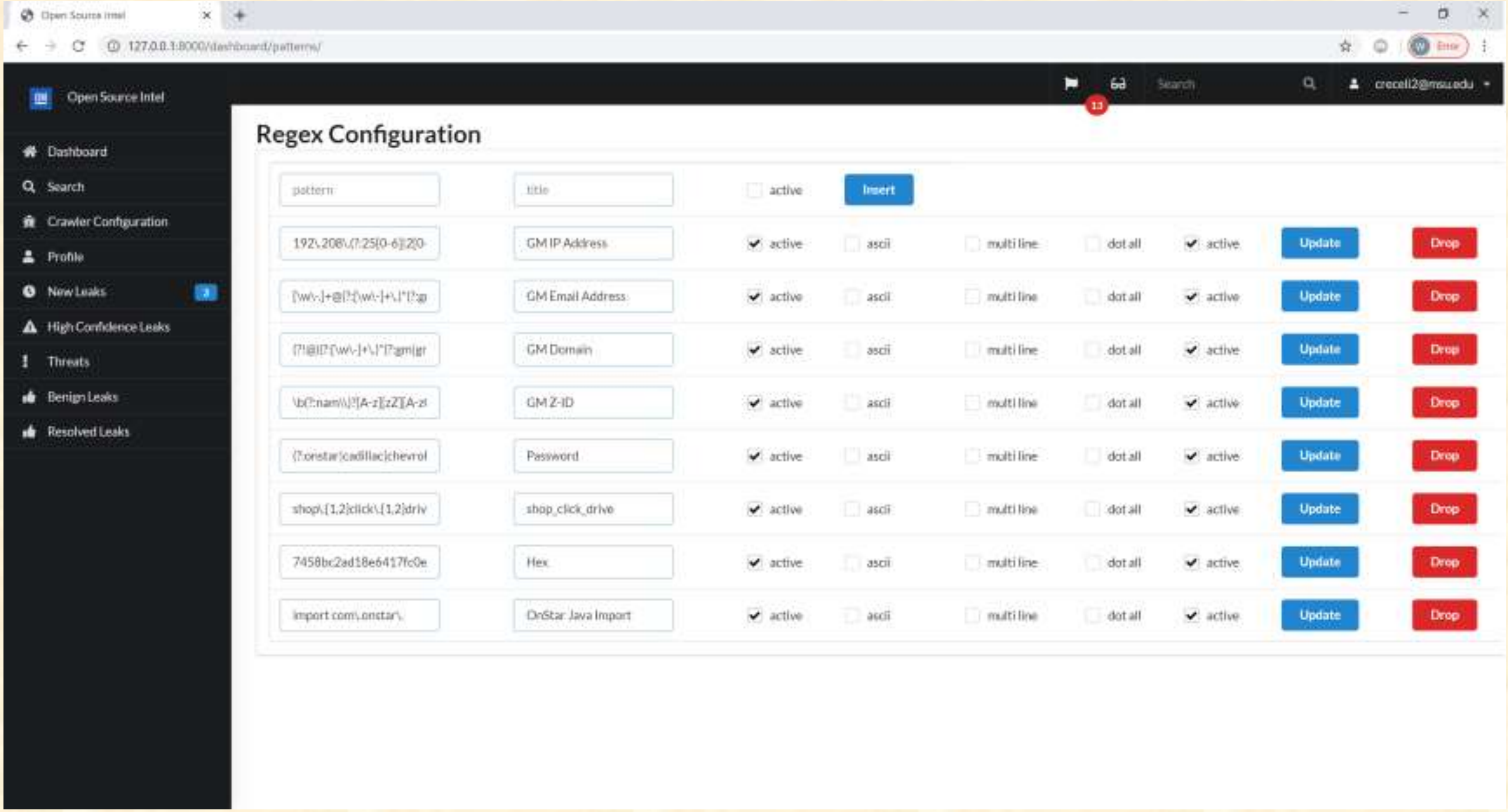
Assignees: Nobody assigned

Tags: No tags

Hits

Link	Content	Line Number	Confidence Rating
View	iglindoj@gm.com	2	100.0
View	gm.com	2	100.0
View	naproxy.gm.com	14	100.0

Crawler Configuration Page



Regex Configuration

pattern	title	□ active	Insert					
192\.208\.(?:25[0-6]|2[0-	GM IP Address	☑ active	□ ascii	□ multi line	□ dot all	☑ active	Update	Drop
[\w\-.]+@(?:[\w\-]+\.)*(?:g	GM Email Address	☑ active	□ ascii	□ multi line	□ dot all	☑ active	Update	Drop
(?!@|(?:[\w\-]+\.)*(?:gm|gr	GM Domain	☑ active	□ ascii	□ multi line	□ dot all	☑ active	Update	Drop
\b(?:nam\\)?[A-z][zZ][A-z	GM Z-ID	☑ active	□ ascii	□ multi line	□ dot all	☑ active	Update	Drop
(?:onstar|cadillac|chevrol	Password	☑ active	□ ascii	□ multi line	□ dot all	☑ active	Update	Drop
shop\.{1,2}click\.{1,2}driv	shop_click_drive	☑ active	□ ascii	□ multi line	□ dot all	☑ active	Update	Drop
7458bc2ad18e6417fc0e	Hex	☑ active	□ ascii	□ multi line	□ dot all	☑ active	Update	Drop
import com\.onstar\.	OnStar Java Import	☑ active	□ ascii	□ multi line	□ dot all	☑ active	Update	Drop

What’s left to do?

- Test software with our client
- U.I. debugging
- Improving U.I. flow
- Train ML, as we confirm more leaks

Questions?

? ? ? ?

? ?

? ? ?