

Analysis of Authentication Code

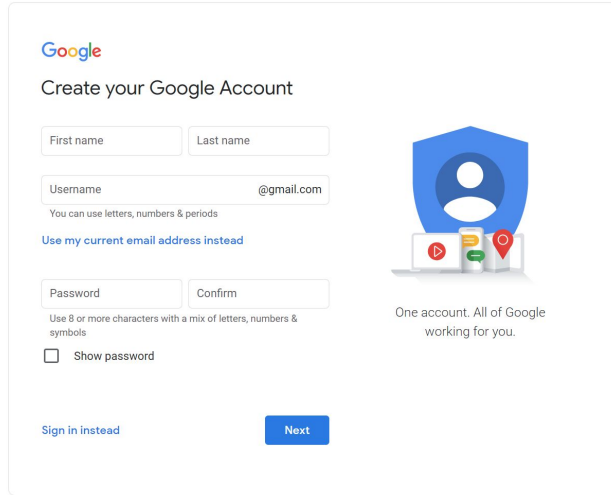
BSc Thesis

2nd Presentation

09 November 2021

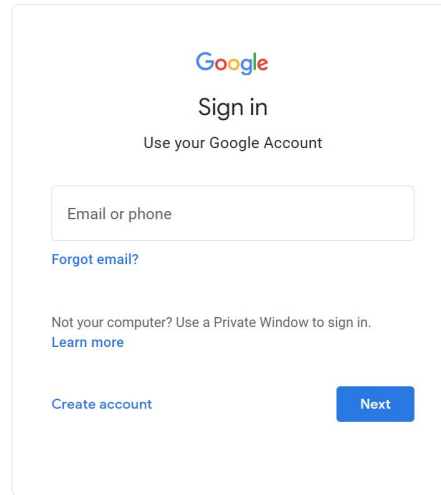
Adrian Jörg

Where is Authentication Code?



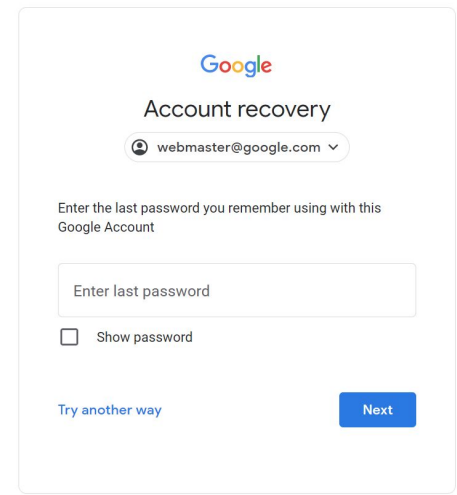
The screenshot shows the Google Account creation interface. It features the Google logo at the top left, followed by the heading "Create your Google Account". Below this are input fields for "First name", "Last name", "Username", and "Password" (with a "Confirm" field). A note states "Use 8 or more characters with a mix of letters, numbers & symbols". There is a checkbox for "Show password" and a "Sign in instead" link. To the right, there is a blue shield icon with a person silhouette and the text "One account. All of Google working for you." Below the shield are icons for YouTube, Gmail, and Google Maps. A blue "Next" button is at the bottom right.

account creation



The screenshot shows the Google Sign in interface. It features the Google logo at the top center, followed by the heading "Sign in" and the sub-heading "Use your Google Account". Below this is a large input field for "Email or phone". A link for "Forgot email?" is below the field. Further down, there is text: "Not your computer? Use a Private Window to sign in. [Learn more](#)". At the bottom, there is a "Create account" link and a blue "Next" button.

account log-in



The screenshot shows the Google Account recovery interface. It features the Google logo at the top center, followed by the heading "Account recovery". Below this is a dropdown menu showing "webmaster@google.com". The text "Enter the last password you remember using with this Google Account" is displayed. Below this is an input field for "Enter last password" and a checkbox for "Show password". At the bottom, there is a "Try another way" link and a blue "Next" button.

account recovery

Authentication Code

... is a wall of defense against various attacks

... should be secure

... is transparent to the user and often forgotten in tutorials

... should always satisfy the ever-evolving safety requirements

Authentication Code In Practice

Find a Location

BONOBOS

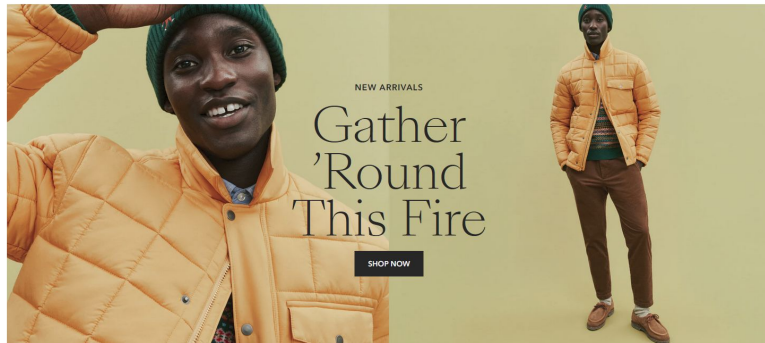
Search

Get 25% Off

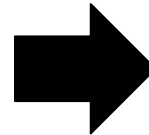
Sign In



New Pants & Jeans Shirts Shorts & Swim Golf Sweaters Suits & Blazers Outerwear Gifts & Accessories Sale



Get free shipping in the US + extended free holiday returns through 1/16/22



Welcome Back!

Please log in to your account

Email Address

Enter Password

By clicking "Continue" you agree to our [Terms of Service + updated Privacy Policy](#).

Continue

[Forgot Password?](#)

[Create an Account](#)

Bonobos clothing store suffers a data breach, hacker leaks 70GB database

By [Lawrence Abrams](#)

January 22, 2021 02:11 PM 0



1491774	91a49e6	50a0fx	et	\N	\N	\N
1796865	7b57d2a	7959fN	ail.com	\N	\N	\N
1796857	7a495f2	2dee98	ail.com	\N	\N	\N
1008919	25ab98e	b10dfR	yahoo.com	\N	\N	\N
1802591	d534ba3	92b41E	ail.com	\N	\N	\N
386351	19c39a9	0de73B	ord@hotmail.com	\N	\N	\N
1802587	eb1c6d0	29791u	ail.com	\N	\N	\N
232405	495958b	5b24c7	@gmail.com	\N	\N	\N
753569	dde83af	613630	mail.com	\N	\N	\N
904720	ea0c418	68012C	oo.com	\N	\N	\N
1344437	5513134	56150Z	@gmail.com	\N	\N	\N
90927	04e846e	c40fch	global.net	\N	\N	\N
438810	473ddb9	0d574Y	son08@gmail.com	\N	\N	\N
659442	daa1267	72c96h	n@condenast.com	\N	\N	\N
338179	64ba6dd	520fat	tonline.net	\N	\N	\N
269072	aa4e73f	3619ad	il.com	\N	\N	\N
1796859	f6a7676	97e39y	ail.com	\N	\N	\N
1796858	0a03255	2d44fv	ail.com	\N	\N	\N
1802590	c3460e8	57925m	a@hotmail.com	\N	\N	\N
1796874	f015cd8	d2cc4p	il.com	\N	\N	\N
1796862	a819bb6	06949U	ail.com	\N	\N	\N
1443804	bb1df3f	9bb53s	gmail.com	\N	\N	\N
347631	5bb92a1	37bd9y	6@yahoo.com	\N	\N	\N
607974	289e8d3	e5b1an	@optonline.net	\N	\N	\N
1319777	36a1f04	da569N	e@comcast.net	\N	\N	\N

Leaked user records table

The passwords stored in the database are **hashed using SHA-256** or SHA-512 according to threat actors who have started to analyze the database. One threat actor claims to have already cracked the passwords for 158,000 SHA-256 passwords but has been **unable to crack the SHA-512 passwords**.

How Secure Is Authentication Code In Open-source Projects?

Where Can We Find Relevant Code?

GitHub!

Languages

HTML	5,237
JavaScript	5,228
Python	3,155
CSS	2,593
Java	2,253
PHP	1,584
TypeScript	770
Ruby	708
Dart	520
Swift	344

26,810 repository results

Sort: Best match ▾

[EpicGames/Signup](#)

Information about signing up for a free Epic Games account, and getting access to UnrealEngine source code.

☆ 1.9k Updated on Jan 18

[sibtc/simple-signup](#)

Code samples used in the blog post "How to Create User Sign Up View"

[python](#) [django](#) [tutorial](#) [tutorial-code](#)

☆ 128  Python MIT license Updated on Oct 24, 2020


[abuanwar072/Welcome-Login-Signup-Page-Flutter](#)

Mobile app onboarding, Login, **Signup** page with #flutter.

☆ 473  Dart Updated on Nov 18, 2020

[aws-samples/py-flask-signup-docker](#)

Sample Python application to show the capabilities of EC2 Container Service.

☆ 78  HTML Apache-2.0 license Updated 15 days ago

Initial Exploration



Collected Properties

Password policies

Length

Pattern

Policy inconsistencies

Code duplication

Impaired functionality

Names of files & functions

Sign up

Login

Password reset

Used libraries

Authentication

Validation

Encryption

Metadata

Forks & stars

Date of first & last commit

Further observations

Insecure hashing algorithms

Outdated encryption libraries

Performance issues

Risk of (No-)SQL injections

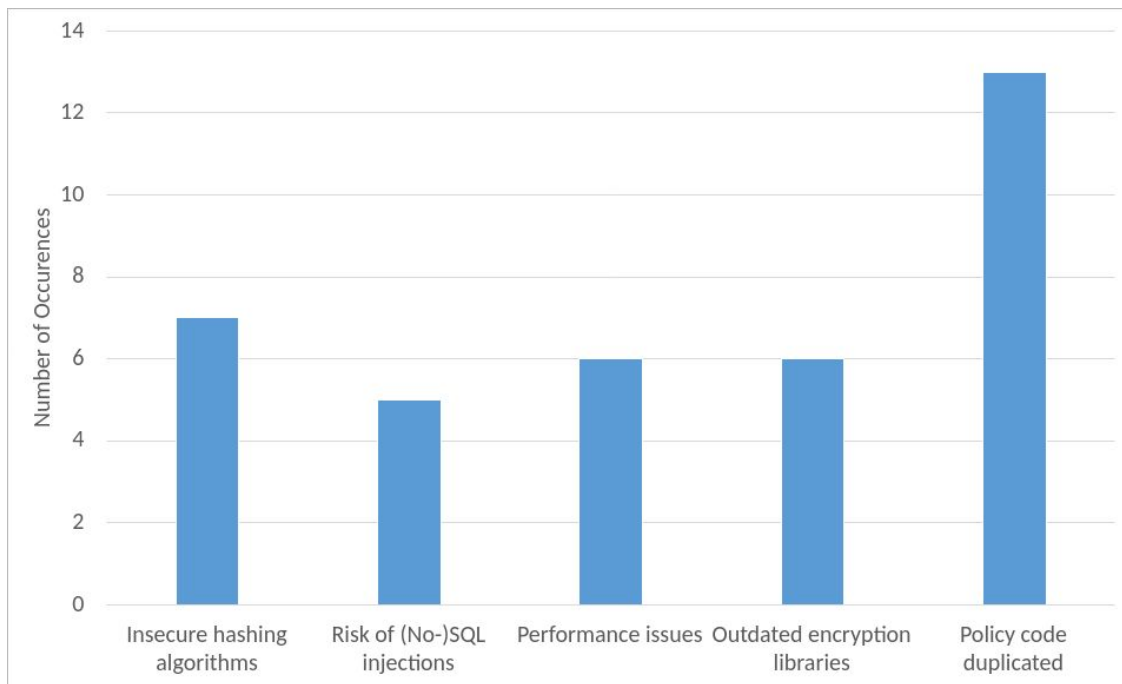
Initial Findings

Dataset:

54 GitHub repositories

3 different languages

5 problem categories
with occurrences > 1



How can we detect
such problems
on GitHub?

CodeQL Queries!

CodeQL

Free semantic code analysis engine offered by GitHub:

codeql.github.com

Supports many programming languages

C/C++, C#, Go, Java, JavaScript,
Typescript, Python

Supports many frameworks

ASP.NET, Express, ...

Displaying 11 alerts, ordered by significance. ⓘ

1 Error 6 Warnings 4 Recommendations

Missing rate limiting ▾

security external/cwe/cwe-770 external/cwe/cwe-307 external/cwe/cwe-400

Source root/routes/routes.js

```
↑ 1-25
26   });
27
28   app.get('/profile', isLoggedIn, function(req, res){
29     res.render('profile.ejs', {user:req.user});
30   });
↓ 31-57
```

This route handler performs authorization, but is not rate-limited. ⓘ ⓘ

13

CodeQL Query Example

```
import javascript

from Function f
where f.getName().matches("%$f$")
select f.getName(), f.getParameter(0)
```

angular/angular 7a40d8c 2'373 results Show 338 non-source results

col0	col1
defineProperty	obj define-property.ts:27
defineProperty	obj jasmine.ts:166
defineProperties	obj define-property.ts:38
stringify	value jasmine-custom-async-matchers.ts:47
stringify	token util.ts:176
stringify	token stringify.ts:9
stringify	params create_util_9tree.ts:331
stringify	obj util.js:9
shift	event index.ts:53

```
export function propertyPatch() {
  zoneSymbol = Zone.__symbol__;
  _defineProperty = (Object as any)[zoneSymbol('defineProperty')] = Object.defineProperty;
  _getOwnPropertyDescriptor = (Object as any)[zoneSymbol('getOwnPropertyDescriptor')] =
    Object.getOwnPropertyDescriptor;
  _create = Object.create;
  unconfigurablesKey = zoneSymbol('unconfigurables');
  Object.defineProperty = function(obj: any, prop: string, desc: any) {
    if (isUnconfigurable(obj, prop)) {
      throw new TypeError('Cannot assign to read only property \'' + prop + '\' of ' + obj);
    }
    const originalConfigurableFlag = desc.configurable;
    if (prop !== 'prototype') {
      desc = rewriteDescriptor(obj, prop, desc);
    }
    return _tryDefineProperty(obj, prop, desc, originalConfigurableFlag);
  };

  Object.defineProperties = function(obj, props) {
    Object.keys(props).forEach(function(prop) {
      Object.defineProperty(obj, prop, props[prop]);
    });
    return obj;
  };
};
```

Custom CodeQL Queries

Our CodeQL queries can detect ...

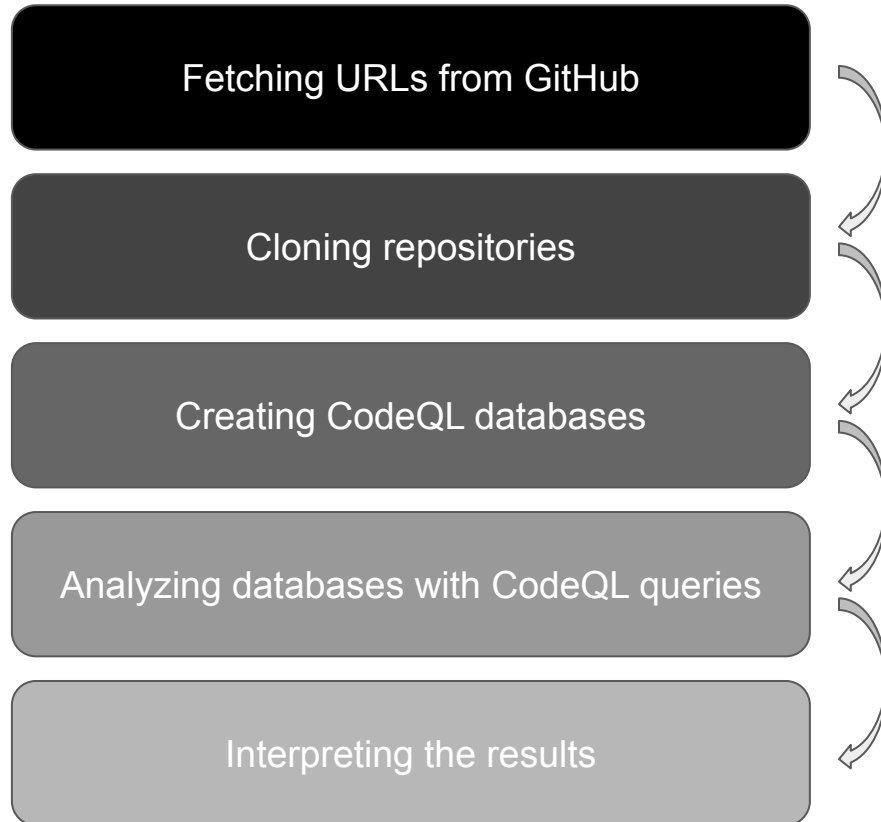
- ... insecure hashing algorithms
- ... outdated encryption libraries
- ... performance issues
- ... ~~exposure to (No-)SQL injections~~
- ... ~~duplicated authentication code~~



Custom CodeQL Query Example

```
/**  
 * @id synchronous-hashing  
 * @kind problem  
 * @precision very-high  
 * @problem.severity warning  
 */  
import javascript  
  
from MethodCallExpr e  
where e.getMethodName().matches("hashSync")  
select e,  
    "This method uses synchronous hashing, which will block the event loop and  
    prevent your application from servicing any other inbound requests or  
    events"
```


Pipeline



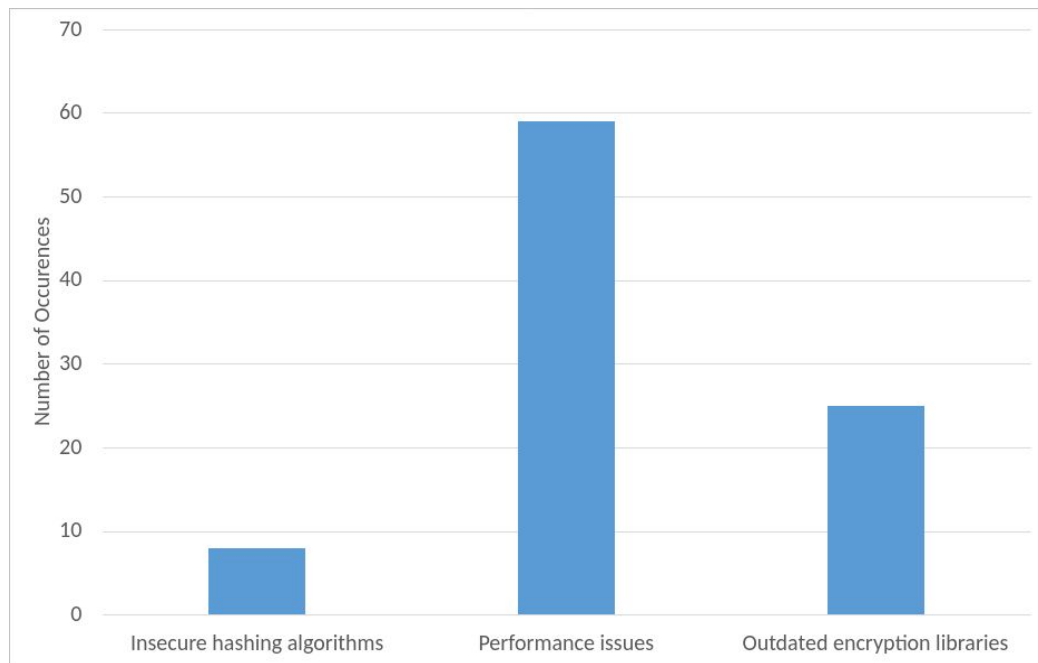
Results

Dataset:

422 GitHub repositories
(only JavaScript)

Fetches from GitHub API
“language:js NodeJS signup
in:filepushed:>2015-01-01”

3 problem categories



Takeaways

Authentication code uses ...

... outdated libraries

... different policies for different use cases

... code from popular repositories and inherits their problems

Future Work

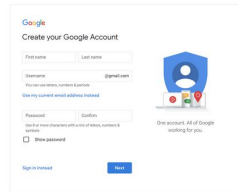
Building **additional queries** to detect more problems

Leveraging **more data**

Translating queries to other programming languages

Summary

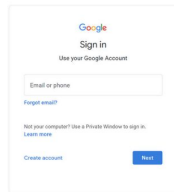
Authentication Code



Google
Create your Google Account

First name Last name
Email
Password
Use my current email address instead
Sign in instead

account creation

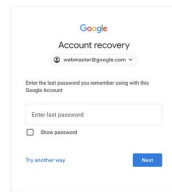


Google
Sign in

Use your Google Account

Email or phone
Forgot email?
Not your computer? Use a Private Window to sign in.
Learn more
Create account Next

account log-in



Google
Account recovery

Enter the last password you remember using with this Google Account
Forgot email?
Enter last password
Show password
Try another way Next

account recovery

2

Custom CodeQL Query Example

```
/**  
 * @id synchronous-hashing  
 * @kind problem  
 * @precision very-high  
 * @problem.severity warning  
 */  
import javascript  
  
from MethodCallExpr e  
where e.getMethodName().matches("hashSync")  
select e,  
    "This method uses synchronous hashing, which will block the event loop and prevent your application from servicing any other inbound requests or events"
```

16

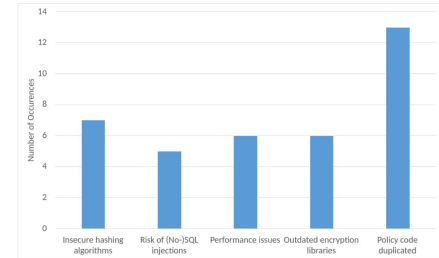
Initial Findings

Dataset:

31 GitHub repositories

3 different languages

5 problem categories
with occurrences > 1



11

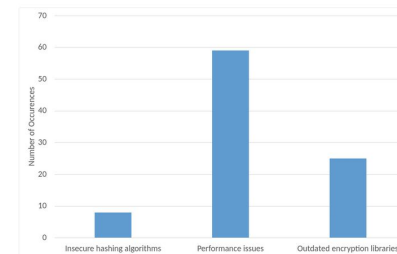
Results

Dataset:

422 GitHub repositories
(only JavaScript)

Fetches from GitHub API
"language:js NodeJS signup
in:filepushed:>2015-01-01"

3 problem categories



18

