

Analysis of Authentication Code available on GitHub

BSc Thesis

1st Presentation

13 April 2021

Adrian Jörg

Existing Password Policies...



Create your Google Account

Continue to Gmail

You can use letters, numbers & periods

Use 8 or more characters with a mix of letters, numbers & symbols

Show password

[Sign in instead](#)

Next

...may decrease security



Mohammad Ghafari
@ghafarii



Hey [@LinkedIn](#), it seems you have two password policies (a bug?) in place. A password can include "many sequential numbers" when signing up, but not when resetting a password.

[Tweet übersetzen](#)

10:08 vorm. · 10. Apr. 2020 · Twitter Web App

Existing problems

Fewer updates for duplicated code

Less readable and understandable code

Fewer test cases

Impaired functionality


Where can we find code about policies?


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 Features:

Password Policy

Length
Pattern

Inconsistencies in Policies

Duplication
Impaired Functionality

File- & Functionnames

Sign Up
Login
Password Reset

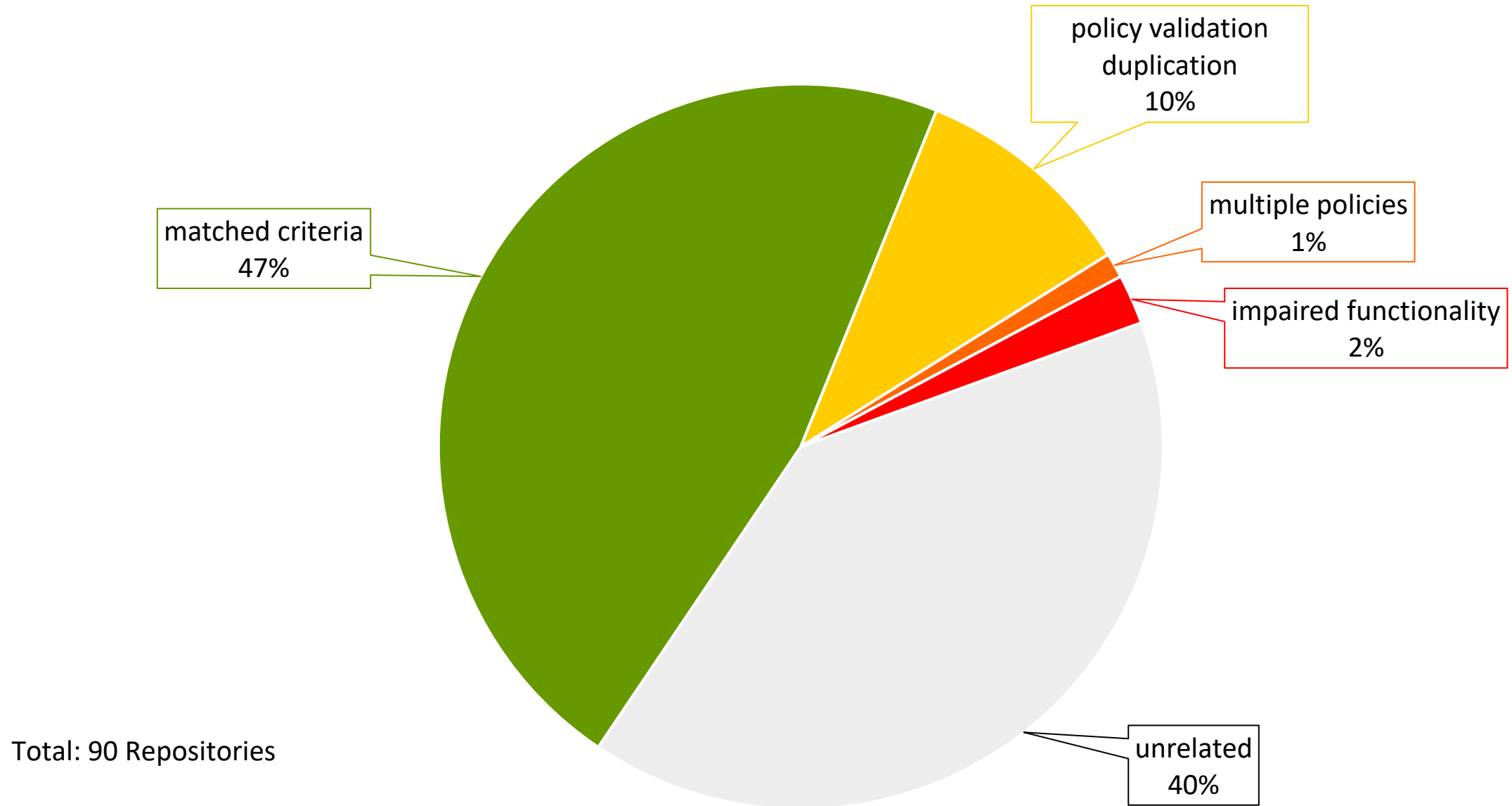
Libraries

Authentication
Validation
Encryption

Metadata

Forks & Stars
First & Last commit

Initial Results



Total: 90 Repositories

Example

```
public function add_user() {  
  
    $data['email_address'] = $this->request->getPost('email_address');  
    $data['first_name'] = $this->request->getPost('first_name');  
    $data['last_name'] = $this->request->getPost('last_name');  
    $data['user_sex'] = $this->request->getPost('user_sex');  
    $data['user_password'] = md5($this->request->getPost('user_password'));  
    $id = $this->Signup_Model->add_user($data);  
    $data['id'] = $id;  
    return view('dashboard/signin.php',$data);  
  
}
```

```
public function auth_user()  
{  
  
    // get form input  
    $data['email_address'] = $this->request->getPost("email_address");  
    $data['user_password'] = md5($this->request->getPost("user_password"));  
  
    $this->validation->setRules([  
        'email_address' => 'required',  
        'user_password' => 'required|min_length[4]'  
    ]);  
    // form validation  
  
    if ($this->validation->run($data) == FALSE)  
    {  
  
        // validation fail  
        $id['invalid_credential'] = 'Email/Password Required ';  
        return view('dashboard/signin.php', $id);  
    }  
    else  
    {
```


How can we **detect** broken policies on GitHub?

CodeQL Queries!

CodeQL Queries

Free semantic code analysis engine by GitHub

codeql.github.com or lgtm.com

Supports

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

and many frameworks (e.g. 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   });
```

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

↓ 31-57

Hard-coded credentials ▾

security external/cwe/cwe-259 external/cwe/cwe-321 external/cwe/cwe-798

Source root/server.js

↑ 1-30

```
31
32 //required for passport
33 app.use(expressSession({ secret: 'mySecretKey', cookie: { maxAge: 60000 }, resave: true, saveUninitialized: true }));
```

The hard-coded value "mySecretKey" is used as key.

CodeQL Queries Example

```
import javascript

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

angular/angular 7a49d8c 2'373 results Show 338 non-source results

col0	col1
defineProperty	obj define-property.ts:27
defineProperty	obj jamine.ts:166
defineProperties	obj define-property.ts:38
stringify	value jamine-custom-async-matchers.ts:47
stringify	token util.ts:176
stringify	token stringify.ts:9
stringify	params create_wi_line.ts:331
stringify	obj util.ts: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;
  };
};
```

Current state



Password Policy

Length

Pattern

Inconsistencies in Policies

Duplication

Impaired Functionality

Filenames

Sign Up

Login

Password Reset

Libraries

Authentication

Validation

Encryption

Metadata

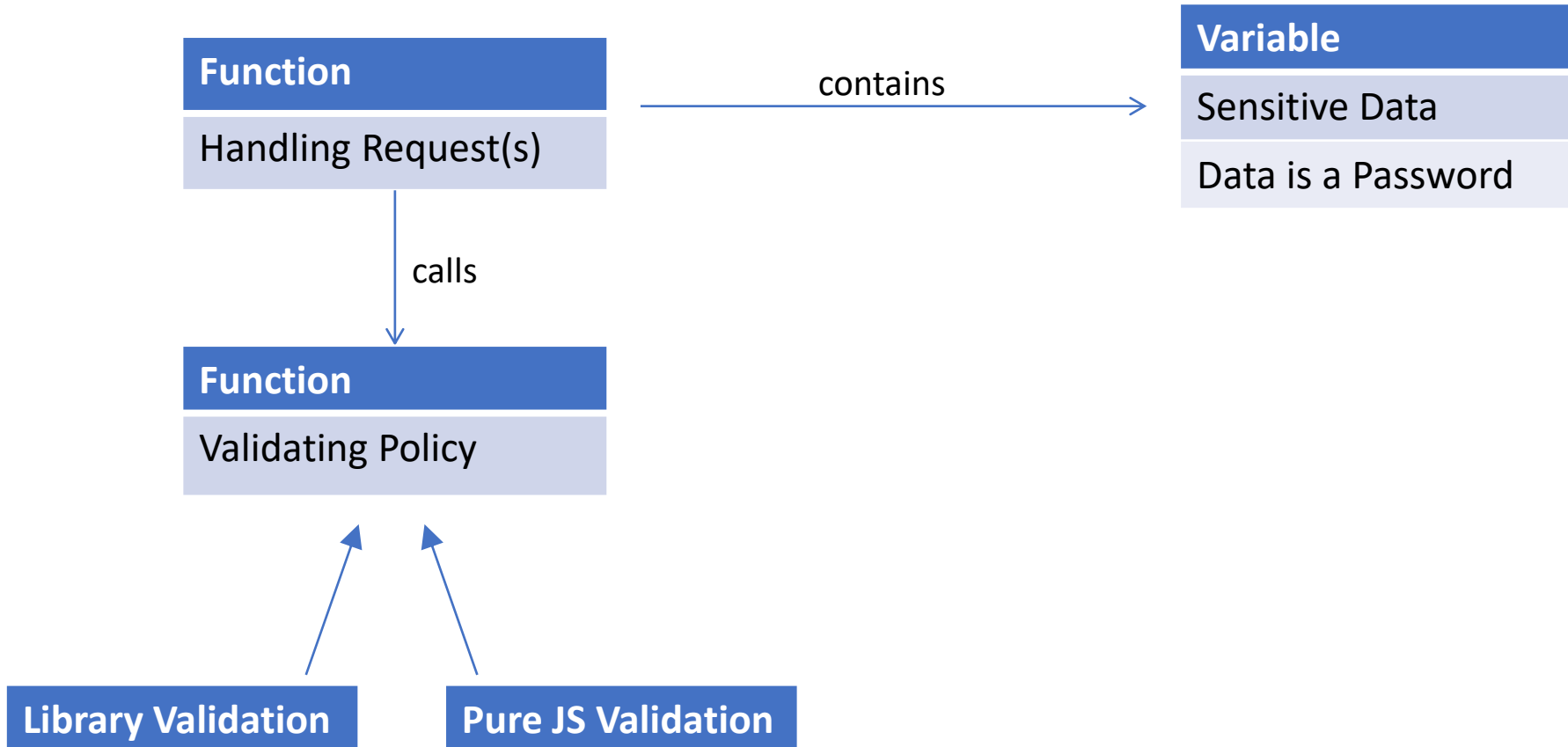
Forks & Stars

First & Last commit

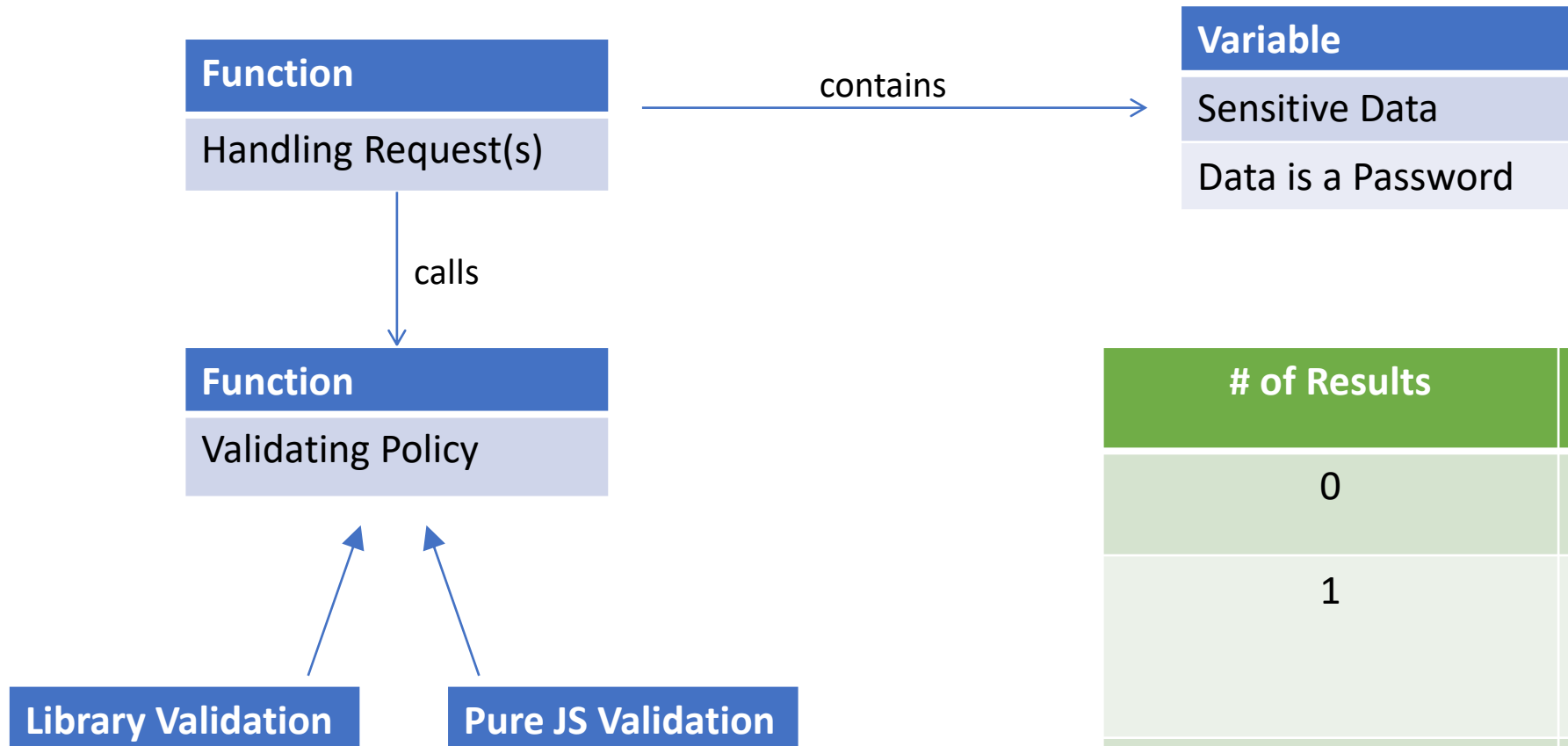
Detector Example (1/3)



Detector Example (2/3)



Detector Example (3/3)



# of Results	Interpretation
0	No password policy
1	Only one password policy
2+	Interesting Case

Interesting Case

Multiple Policies

OR

```
set passwordSchema = { required | min:4 };
set emailSchema = { required | email };
set nameSchema = { required }

function validateSignup(user) {
  return
    passwordSchema.validate(user.password) &&
    emailSchema.validate(user.email) &&
    nameSchema.validate(user.name)
}

function validateLogin() {
  return
    passwordSchema.validate(user.password) &&
    emailSchema.validate(user.email) &&
}
```


Next Steps

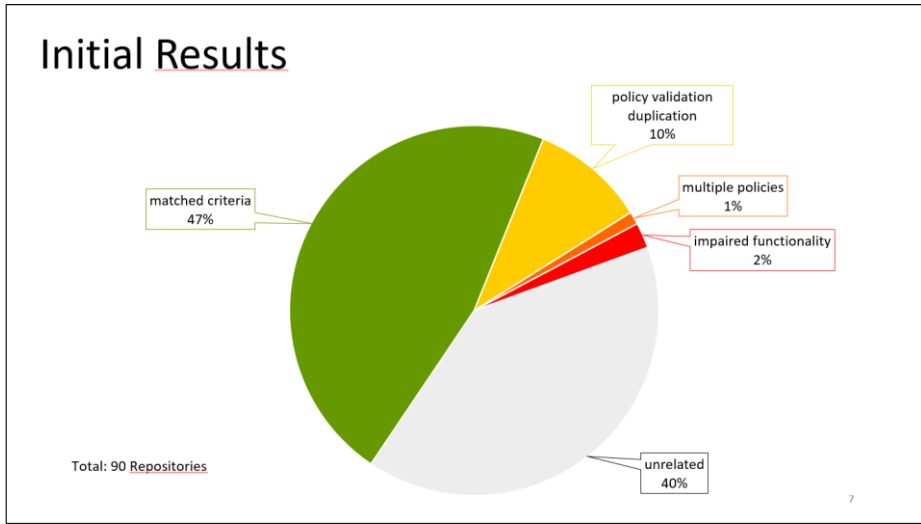
Implement the recognition of more validation libraries

Filter the results which use the same validation codebase in different functions

Apply to larger base of repositories

Make the query available to GitHub for automatic reviews

Summary

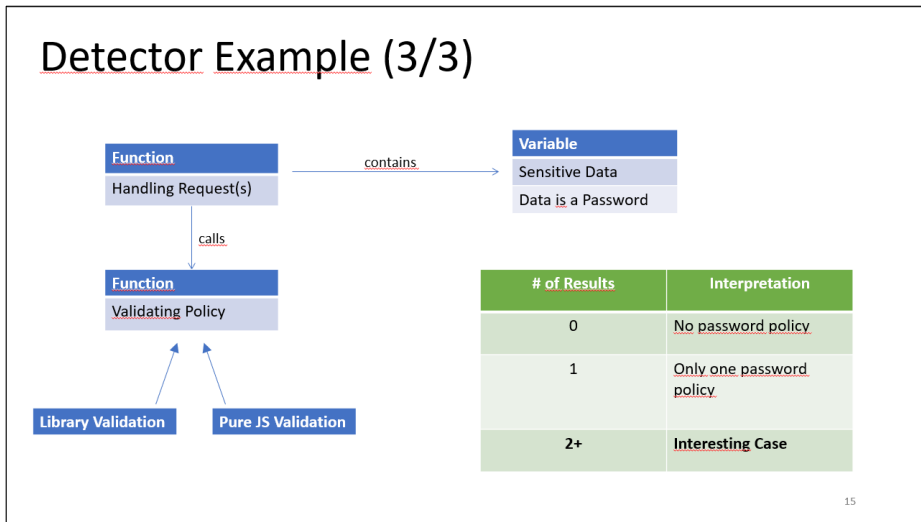
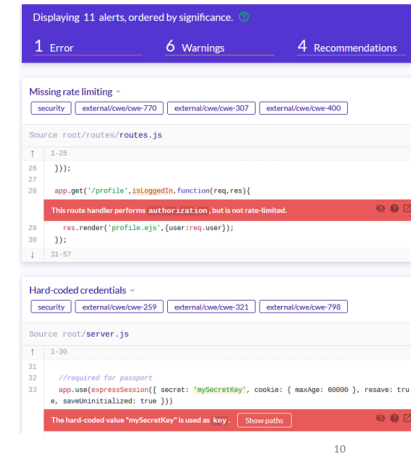


CodeQL Queries

Semantic code analysis engine by Github
codeql.github.com or lgtm.com

Supports

C/C++, C#, Go, Java, Javascript, Typescript, Python
 and many frameworks (e.g. ASP.NET, express...)



Next Steps

Implement the recognition of more validation libraries

Filter the results which use the same validation codebase in different functions

Apply to larger base of repositories

Make the query available to GitHub for automatic reviews