PRACTICAL SECURE CODE REVIEW

(SETH & KEN'S EXCELLENT ADVENTURE IN SECURE CODE REVIEW)

FEBRUARY 2022

INTRODUCTIONS - SETH

Seth Law - Founder, Redpoint Security

Based out of Salt Lake, Utah

Consultant, Programmer, Trainer, Speaker and of course... a lot of code review.

@sethlaw

Redpoint

INTRODUCTIONS - KEN

Staff Engineer - GitHub

Based out of Gainesville, VA

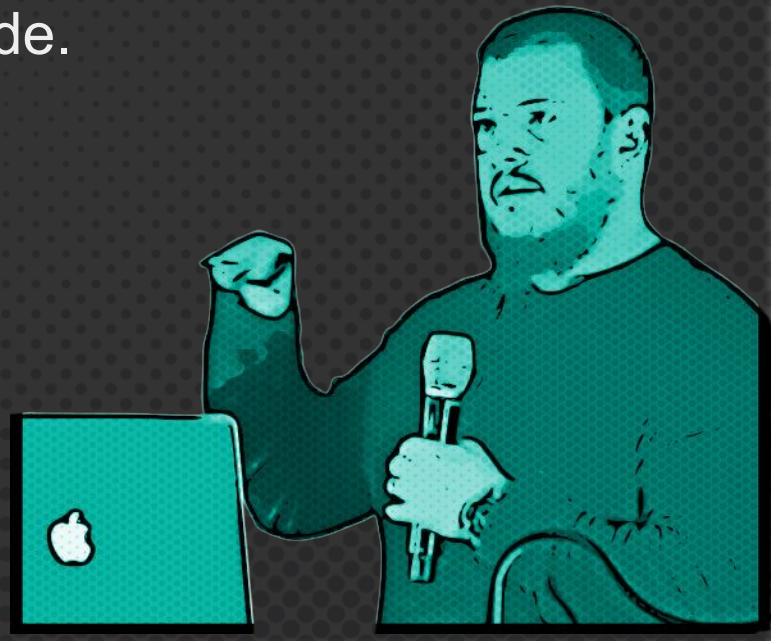
Coder, Consultant, Defender, Trainer, Speaker… and similarly… a lot of code review along the way.

@cktricky

ABSOLUTE AppSec

OVERVIEW

- Repeat after me:
  - The best way to identify vulnerabilities and exploits in an application is to look at source code.



Philosophy - Part 1

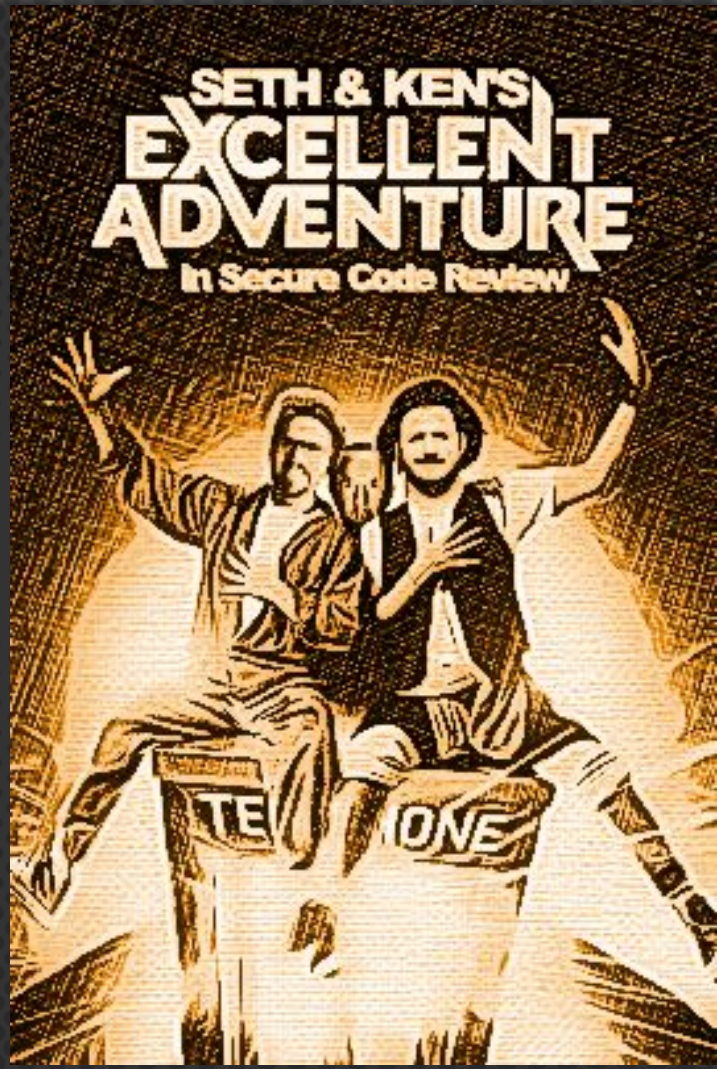
- Increase the likelihood of success. Not “find every bug imaginable”.
- Successful is defined as:
  - Focusing on what matters by taking a risk based approach
  - Comprehensive
  - Timely
  - Easily consumed, well drafted reporting
  - Detailed notes

Philosophy - Part 2

- Language Agnostic Principles
  - Learn how to be an expert in becoming an expert
- We’re here to learn a repeatable systematic approach to finding bugs
  - With the understanding that you *should* tweak this approach to suit your experience

WHAT TO EXPECT

- Our Experience and Stories
- Specific Information about Reviewing Code
- Interactive Hands-On Exercises
- Practice, practice, practice



LET'S TALK ABOUT APPROACH

LET'S TALK ABOUT APPROACH

Several types of reviews:

- You decide how much time you spend (ideal world)
- You have no time at all (real world)
- Consulting middleground where you have a set time and scoped (hopefully) well or at least semi “okay”

NONE OF THESE TYPES MEAN “RUN A SCANNER AND ANALYZE THE RESULTS”

First, let's talk about what we're doing here

This course is intended to do the following, at a high level:

1. Show you where to look - Source to Sink
2. Show you what to look for, examples:
    a. AuthZ/AuthN
    b. Vulns specific to the type of app
    c. General/OWASP AppSec vulns
3. Show where automation fits in the source code review process
4. Show some validation and remediation of the issues

Also, let's talk about what we aren't doing

This course is not intended to:

1. Teach you the OWASP Top 10
2. Review web vulnerabilities
3. Cover techniques for finding vulnerabilities in running applications
4. Be a primer on building secure applications
5. Cover all the ways that vulnerabilities manifest in code.

REPOSITORIES

- https://github.com/zactly/handouts - templates
- https://github.com/zactly/skea_django
- https://github.com/zactly/skea_node
- https://github.com/zactly/skea_rails
- https://github.com/Atutor/atutor - PHP App
- https://github.com/sethlaw/vtm - Vulnerable Task Manager
- https://github.com/IMA-WorldHealth/bhima - Node App
- https://github.com/discourse/discourse - RAILS App

OWASP

- How does the OWASP Top 10 relate?
- What resources does OWASP provide?
- How does this course differ from the OWASP Code Review Methodology?

Secure Code Review Methodology

Overview

SECURE CODE REVIEW METHODOLOGY

1. Application Overview & Risk Assessment
2. Information Gathering
3. Checklist Creation
4. Perform Reviews

Checklists/Reviews

- Authorization
- Authentication
- Auditing
- Injection
- Cryptographic
- Configuration
- Reporting

THE CIRCLE-K FRAMEWORK

1. Open a file, take notes :-)
2. Identify the application purpose
3. Map the application
4. Brainstorm risks to the application
5. **Build list of review items**
6. Perform all reviews
7. Double back (3-6)

GENERAL PRINCIPLES

- Give yourself adequate time
- Work in small chunks
- Stay on task with current objective
- Don’t make it personal
- Ask questions
- Framework/Code documentation is your friend
- Build the code
- Run the tests

FOCUS ON WHAT'S IMPORTANT

- What happens when you run into 2 million lines of code?
- And only have two weeks to look at it?
- We will talk more about this...

NOTE TAKING

NOTE TAKING

- Format typically used
  - Commit # (if available)
  - Two sections
    i. Actual Findings
    ii. Notes from the review
- Actual findings filled out at the end
  - Description / Recommendation
  - Optional (or not) - Impact/Risk
  - Includes links to the code in question and/or screenshots
  - If applicable, reproduction steps but that might not be possible if purely static
  - Avoid emotive words

- Notes from the review include (at a minimum)
  a. Route mapping
  b. “Threat model” details (really, rambling thoughts about what could go wrong”
     i. PAIR WITH OTHERS!!!
  c. Checklist of items you’ve checked for based on your threat model but also your normal “things” you should look at

NOTE TAKING - EXAMPLE

We assessed commit `#74e64e1ccb617c83ba1db4cbbb24a33051e169f8`

Notes for you/your team

Behavior

- What does it do? (business purpose)

  Task Manager

- Who does it do this for? (internal / external customer base)

  Internal Employees & External Customers

- What kind of information will it hold?

  Tasks, Notes, Projects.. could be sensitive Date of Birth of users

Brainstorming / Risks

- XSS - notes, projects and tasks
- Appears to use MD5 for passwords?
- TM employees using the product for managing their own products... ramific
- noticed file uploads for profile pics - file access/handling
- What if sensitive pics are uploaded to the projects - CONFIRMED THAT PR
- Image processing... RCE? Something else like traversal/LFI/RFI?

Checklist of things to review based on Brainstorm

- [ ] Command Injection: system, call, popen, stdout, stderr, import os
- [ ] SQL Injection: raw, execute, select, where
- [ ] XSS: Autoescape, |safe, escapejs
  - [ ] Take a look at filenames and see if we render those unsafely anywhere
- [ ] File handling: `File`, `django.core.files`
- [x] CSRF on the password change?
- [ ] IDOR on Projects/Notes/Tasks/Profile

REVIEW TYPES

REVIEW TYPES

- Full assessment
- Assessment of new code since last review
- Single pull request or small code changes review
- Scanner findings

REVIEW TYPES

1. FULL ASSESSMENT 💯
2. ONLY NEW CODE 👍
3. PULL REQUEST REVIEW 🔎
4. SCANNER FINDINGS 🪲

1. Everything is applicable !!
2. Depends 👀… seen this app before?
3. Context specific bits (authz functions, logic processing, db queries, etc.)
4. Meh 🤷

Application Overview & Risk Assessment

APPLICATION OVERVIEW & RISK ASSESSMENT

Build a portrait of the application

- Behavior Profile
- Technology Stack
- App Archeology

BEHAVIOR PROFILING

- What does it do? (business purpose)
- Who does it do this for? (internal / external customer base)
- What kind of information will it hold?
- What are the different types of roles?
- What aspects concern your client/customer/staff the most?

TECHNOLOGY STACK

- Framework & Language - Rails/Ruby, Django/Python, mux/Golang
- 3rd party components, Examples:
  - Supporting libraries (rubygem, npm, jar, etc.)
  - JavaScript widgets - (marketing tracking, sales chat widget)
  - Reliant upon other applications - such as receiving webhook events
- Datastore - Postgresql, MySQL, Memcache, Redis, Mongodb, etc.

APPLICATION ARCHEOLOGY

- Look at the documentation. Examples:
  - Using SSO? SAML/OAuth?
  - What third-party elements does communicate with? (eg: external reporting, billing)
  - Custom authentication schemas - for instance - different auth for API versus web interface
- Git allows you to do a little spelunking
- Unit Tests
  - Learn about the data endpoints expect to receive
  - Learn about expected behavior
  - Often can find the way to form/craft a request

APPLICATION OVERVIEW & RISK ASSESSMENT

https://github.com/IMA-WorldHealth/bhima

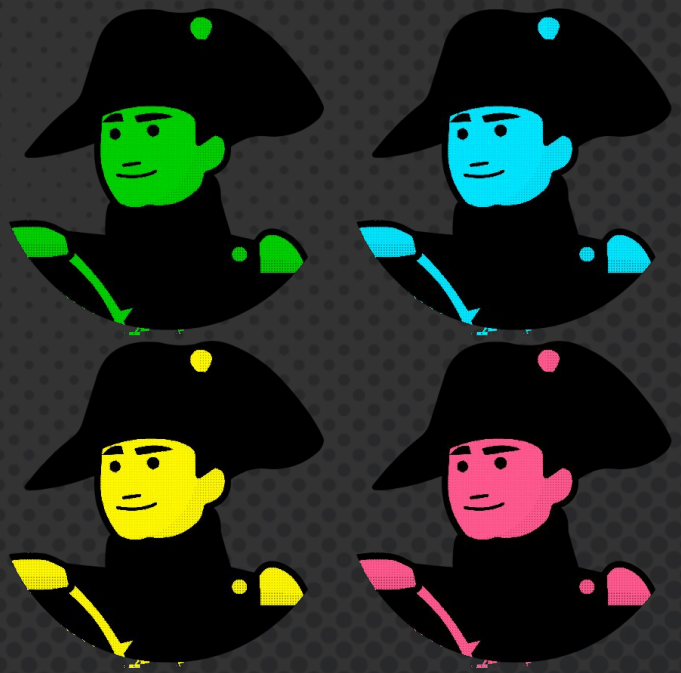
```
/* global inject, expect */

describe('PasswordMeterService', () => {
  let PasswordMeterService;
  let Session;

  beforeEach(module(
    'ngStorage',
    'angularMoment',
    'bhima.services',
    'bhima.mocks',
    'ui.router'
  ));

  const WEAK_PASSWORD = 'hello';
  const MEDIUM_PASSWORD = 'L0b1Ec0simba';
  const STRONG_PASSWORD = 'N@pM@ch3N#L1my3B0ndy3@!';

  beforeEach(inject((_PasswordMeterService_, _SessionService_, _MockDataService_) => {
    PasswordMeterService = _PasswordMeterService_;
    Session = _SessionService_;

    const user = _MockDataService_.user();
    const project = _MockDataService_.project();
    const enterprise = _MockDataService_.enterprise();
    Session.create(user, enterprise, project);

    // make sure password validation is on
    Session.enterprise.settings.enable_password_validation = true;
  }));
```

```
it('#counter() should return -1 for no password', () => {
  const count = PasswordMeterService.counter();
  expect(count).to.equal(-1);
});

it('#validate() should return false for no password', () => {
  const validate = PasswordMeterService.validate();
  expect(validate).to.equal(false);
});

it('#counter() should return 0 for a weak password', () => {
  const count = PasswordMeterService.counter(WEAK_PASSWORD);
  expect(count).to.equal(0);
});

it('#validate() should return false for a weak password', () => {
  const validate = PasswordMeterService.validate(WEAK_PASSWORD);
  expect(validate).to.equal(false);
});

it('#counter() should return 3 for a medium password', () => {
  const count = PasswordMeterService.counter(MEDIUM_PASSWORD);
  expect(count).to.equal(3);
});

it('#validate() should return true for a medium password', () =>
  const validate = PasswordMeterService.validate(MEDIUM_PASSWORD)
  expect(validate).to.equal(true);
});

it('#counter() should return 4 for a strong password', () => {
  const count = PasswordMeterService.counter(STRONG_PASSWORD);
```

APPLICATION OVERVIEW & RISK ASSESSMENT

EXERCISE NAPOLEON

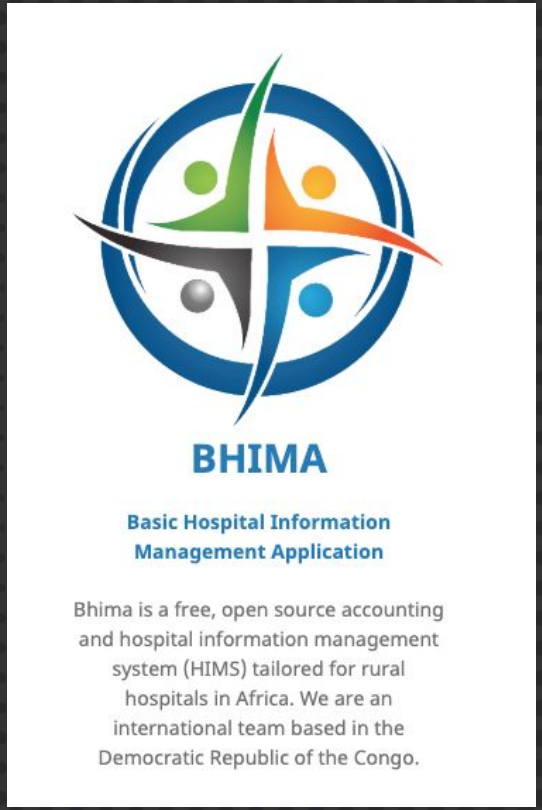
1. **bhima**
    a. Tech Stack
    b. Business Purpose
    c. Application Risk
    d. Anything else?



NAPOLEON EXERCISE - POST-MORTEM

At a minimum, these items were of note:

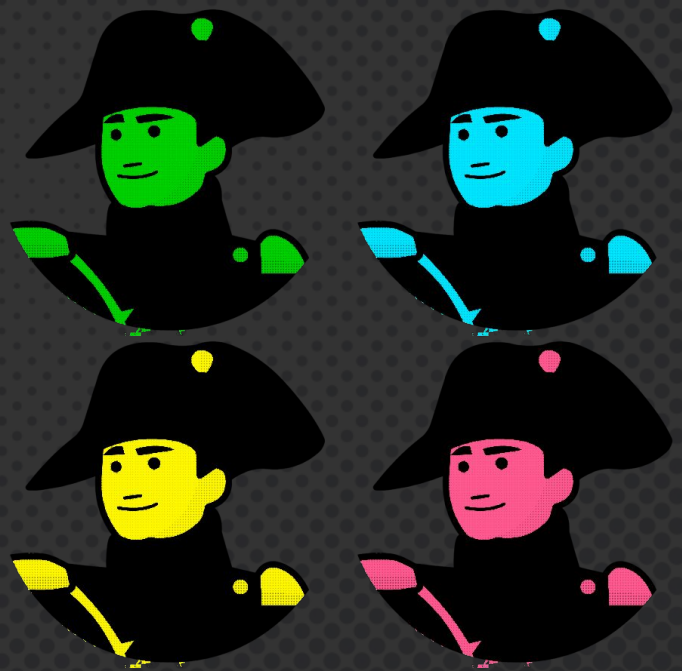
- Business Purpose
  - Basic Hospital Information Management Application
- Tech Stack
  - Node.js / Express
  - Angular
  - MySQL/Redis
- Documentation
  - https://github.com/IMA-WorldHealth/bhima/wiki
  - https://docs.bhi.ma/en/
- Risks
  - Patient Data
  - Employee Payroll Information



NAPOLEON EXERCISE - POST-MORTEM

Other important security portions of the app:

- Express Configuration -
  - server/config/express.js
  - Uses default helmet.js
- User Authentication
  - server/controllers/auth.js
- Admin folder
  - Logic for admin logins - server/controllers/admin/users/index.js



INFORMATION GATHERING

INFORMATION GATHERING

"THE MOST IMPORTANTEST THING IS TO UNDERSTAND THE APP"

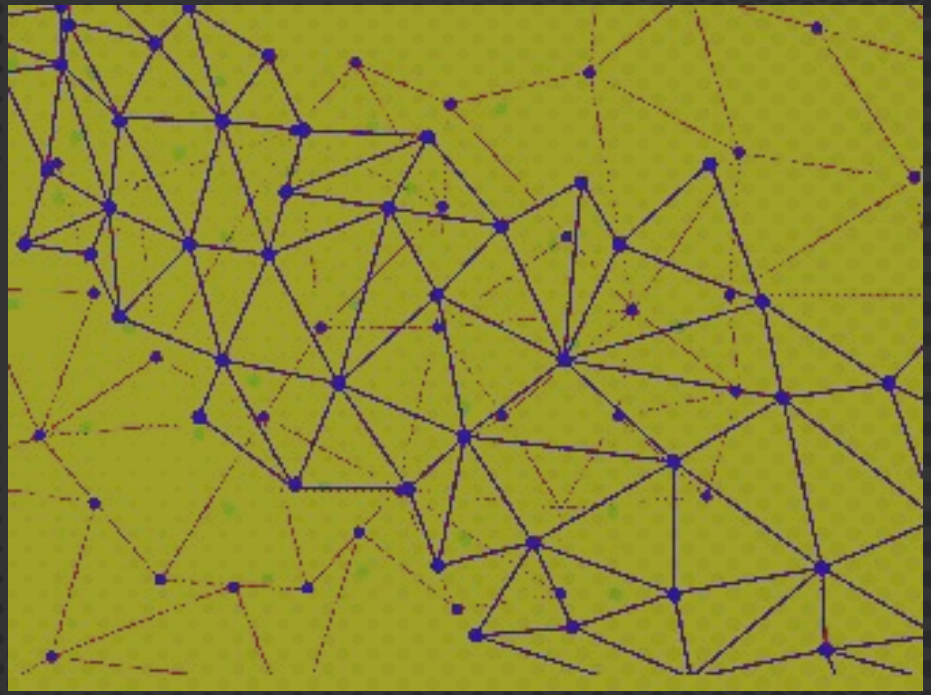
"- @sethlaw"

- @cktricky

INFORMATION GATHERING

1. Create Application Map

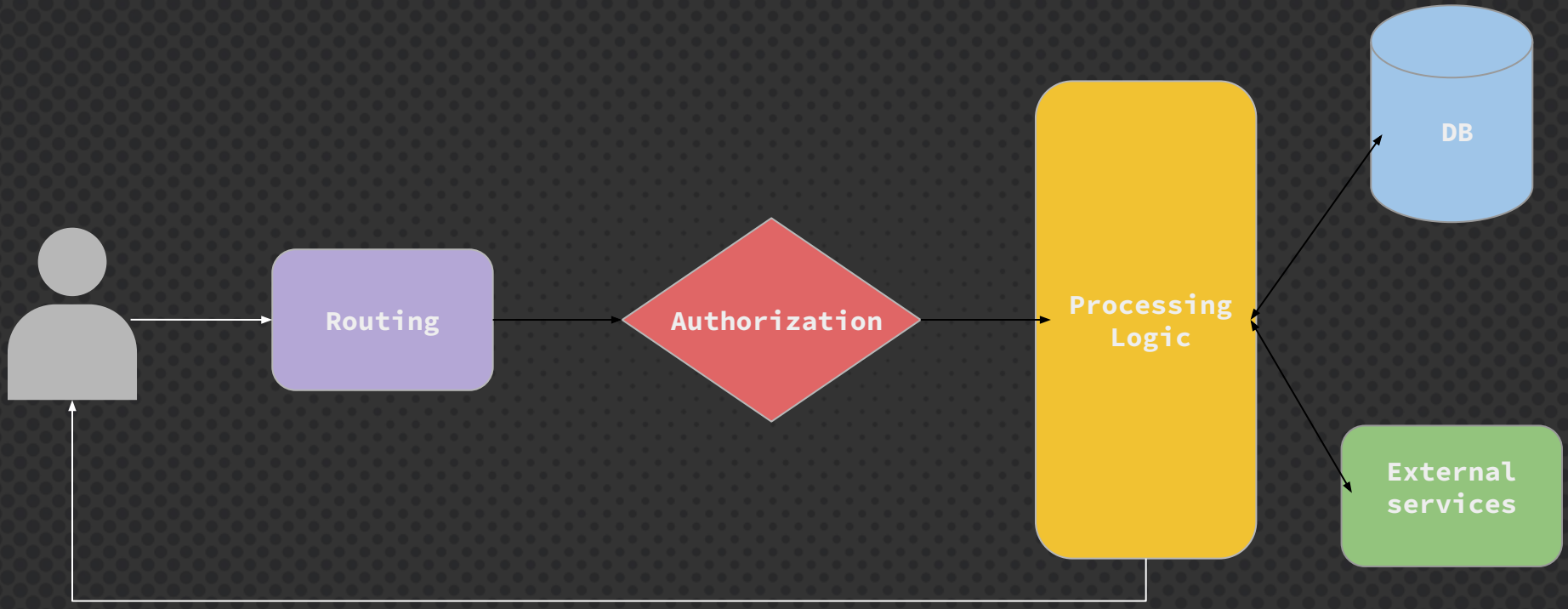
2. Identify Authorization Functions



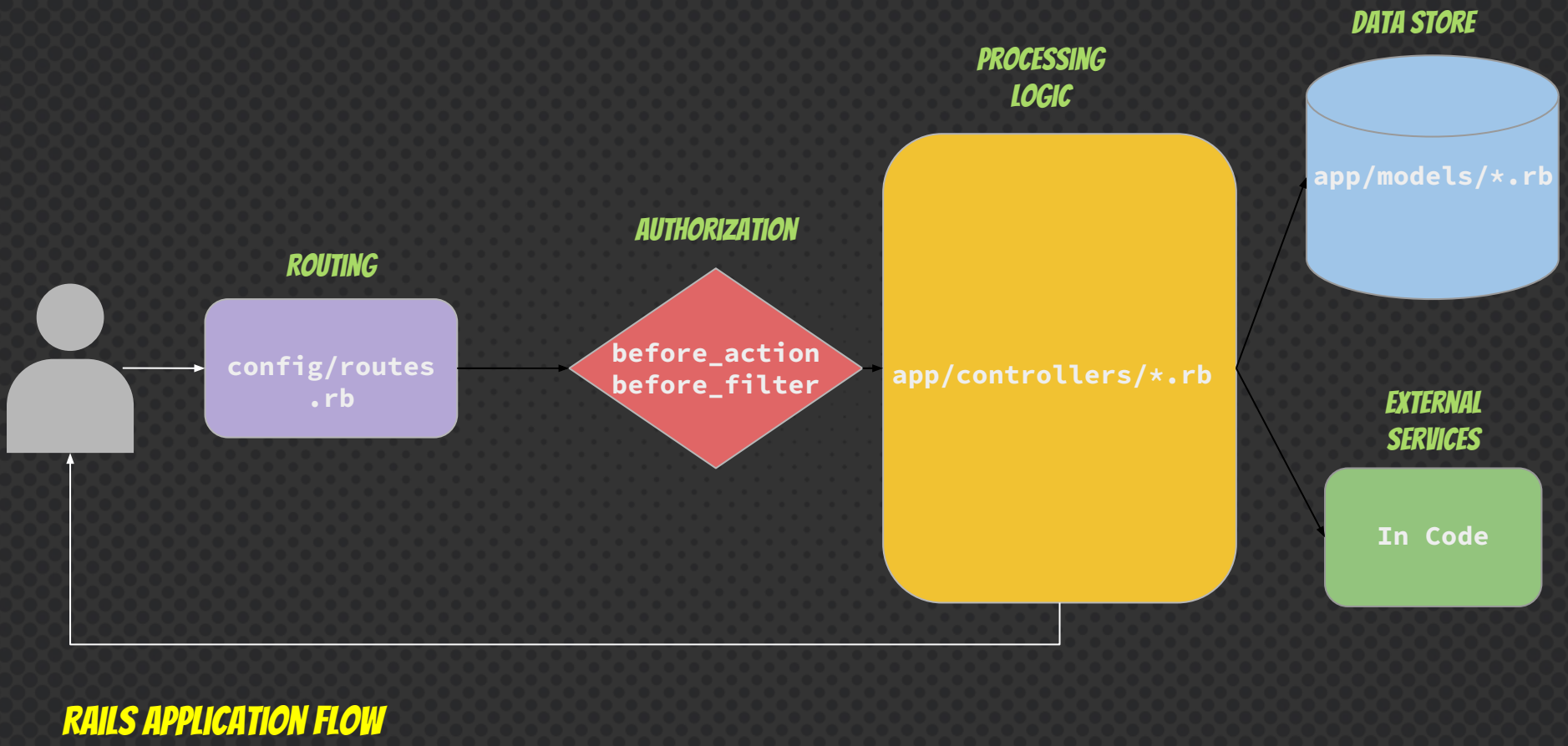
MAPPING

Information Gathering - Create a Map

- Identify endpoints, typical examples:
  - Rails = config/routes.rb - `rake routes`
  - Django= urls.py - `manage show_urls`
  - Node.js = index.js
  - Java Spring = *Controller.java
  - .Net Core = *Controller.cs
- Endpoints typically have at least three qualities
  - Authorization Filter
  - Logic processing
  - Datastore access



TYPICAL APPLICATION FLOW



RAILS APPLICATION FLOW

RAILS - MAP

- Run `rake routes` If you can!

1. cktricky@Kens-MacBook-Pro: ~/code/railsgoat (zsh)

```
cktricky@Kens-MacBook-Pro ~/code/railsgoat master rake routes
                  Prefix Verb   URI Pattern                                                 Controller#Action
                   login GET    /login(.:format)                                            sessions#new
                  signup GET    /signup(.:format)                                           users#new
                  logout GET    /logout(.:format)                                           sessions#destroy
         forgot_password GET    /forgot_password(.:format)                                  password_resets#forgot_password
                         POST   /forgot_password(.:format)                                  password_resets#send_forgot_password
         password_resets GET    /password_resets(.:format)                                  password_resets#confirm_token
                         POST   /password_resets(.:format)                                  password_resets#reset_password
           dashboard_doc GET    /dashboard/doc(.:format)                                    dashboard#doc
                sessions GET    /sessions(.:format)                                         sessions#index
                         POST   /sessions(.:format)                                         sessions#create
             new_session GET    /sessions/new(.:format)                                     sessions#new
            edit_session GET    /sessions/:id/edit(.:format)                                sessions#edit
                 session GET    /sessions/:id(.:format)                                     sessions#show
                         PATCH  /sessions/:id(.:format)                                     sessions#update
                         PUT    /sessions/:id(.:format)                                     sessions#update
                         DELETE /sessions/:id(.:format)                                     sessions#destroy
user_account_settings GET    /users/:user_id/account_settings(.:format)                  users#account_settings
user_retirement_index GET    /users/:user_id/retirement(.:format)                        retirement#index
```

RAILS - MAP

```
forgot_password GET    /forgot_password(.:format)                password_resets#forgot_password
```

- Four parts
  - Path name (eg: forgot_password_path)
  - HTTP Verb (eg: GET)
  - HTTP Path (eg(s): forgot_password, forgot_password.json, forgot_password.xml)
  - Controller and Action (eg: Controller = password_resets, Action = forgot_password)

RAILS - MAP

```
forgot_password GET    /forgot_password(.:format)          password_resets#forgot_password
```

- Four parts
  - Path name (eg: forgot_password_path)
  - HTTP Verb (eg: GET)
  - HTTP Path (eg(s): forgot_password, forgot_password.json, forgot_password.xml)
  - Controller and Action (eg: Controller = password_resets, Action = forgot_password)

RAILS - MAP

- If you cannot run rake routes, you'll have to review the config/routes.rb file:

routes.rb — ~/code/ra

routes.rb

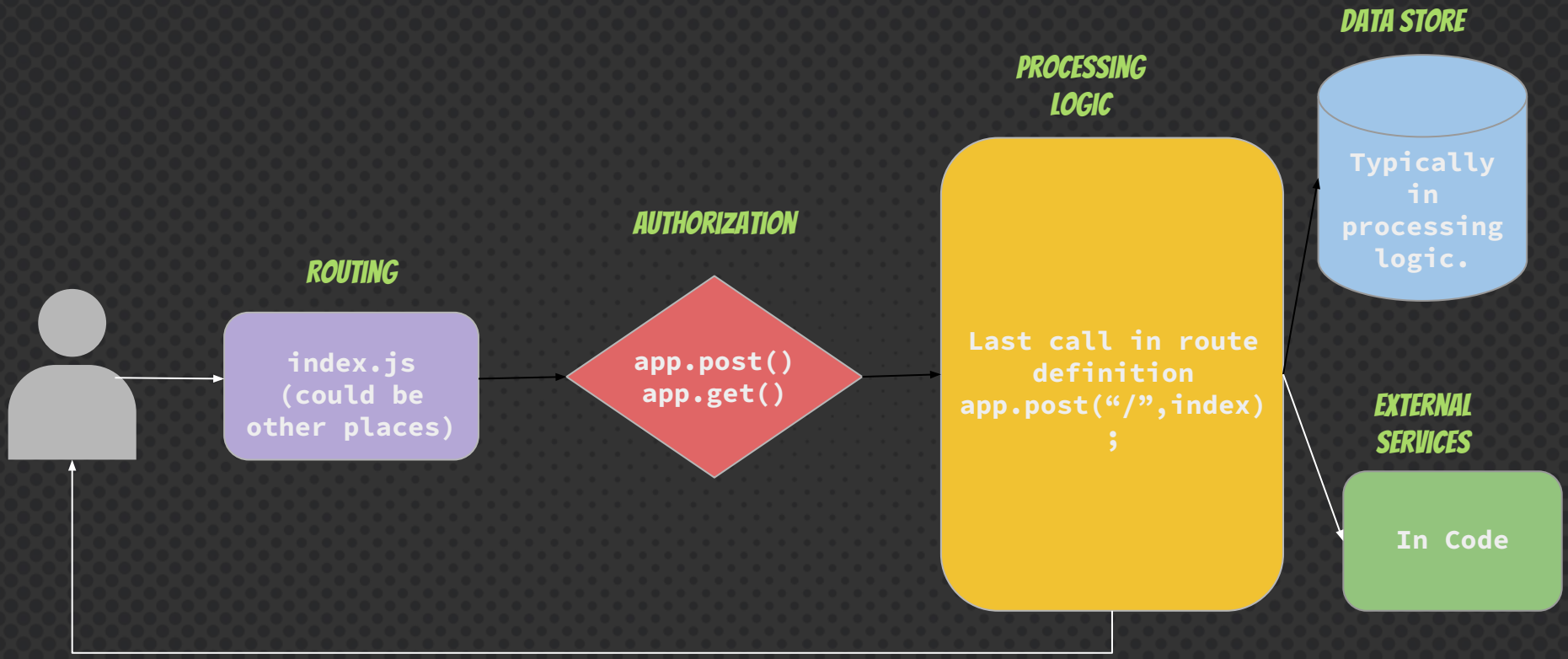
```
1   # frozen_string_literal: true
2   Railsgoat::Application.routes.draw do
3
4     get "login" => "sessions#new"
5     get "signup" => "users#new"
6     get "logout" => "sessions#destroy"
7
8     get "forgot_password" => "password_resets#forgot_password"
9     post "forgot_password" => "password_resets#send_forgot_password"
10    get "password_resets" => "password_resets#confirm_token"
11    post "password_resets" => "password_resets#reset_password"
12
13    get "dashboard/doc" => "dashboard#doc"
14
15    resources :sessions
16
17    resources :users do
18      get "account_settings"
```

RAILS - ROUTING WEIRDNESS ALERT

- What do `PUT`, `PATCH`, `DELETE`, and `POST` all have in common?
- That's right, they are all `POST` requests
- Rails uses the `_method` parameter to determine what kind of request it is

RAILS - ROUTING WEIRDNESS ALERT

```
POST /join HTTP/1.1
Host: github.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://github.com/join?source=header-home
Content-Type: application/x-www-form-urlencoded
Content-Length: 233
Connection: close
Cookie: logged_in=no
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&authenticity_token=1YJBp5UZPnafW2qSy6GhEgg4ob05APDlMVUbmvLCCv
VqQS5JYA5cuVOcLWOS%2FDELy7z8J1AeH1TyxGCWojSxcw%3D%3D&user%5Blogin%5D=cktric
ky-example&user%5Bemail%5D=cktricky-example%40skea.com&user%5Bpassword%5D=d
olphin1&_method=patch
```



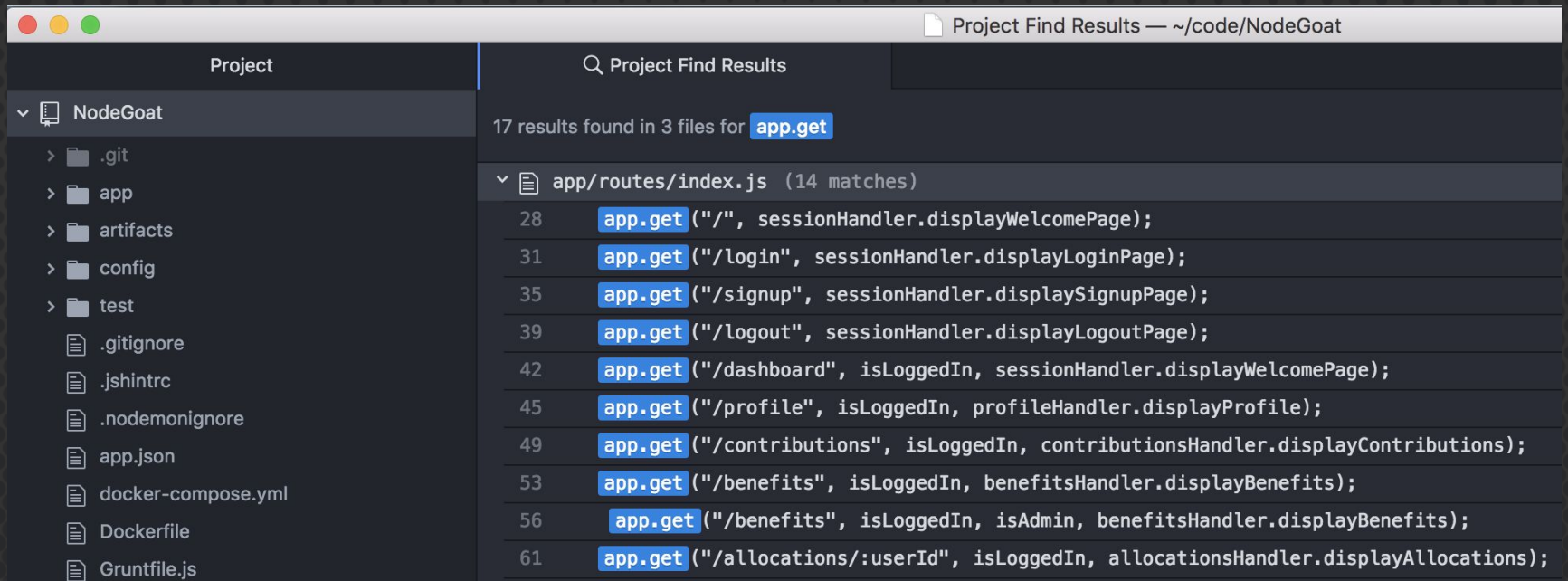
NODE.JS/EXPRESS APPLICATION FLOW

NODE.JS/EXPRESS - MAP

- Our formula has been super basic, searching for:
  - `app.get`
  - `app.post`
  - `app.delete`
- We like to annotate which of these is actually using middleware
- We'll create a checklist from this for tracing

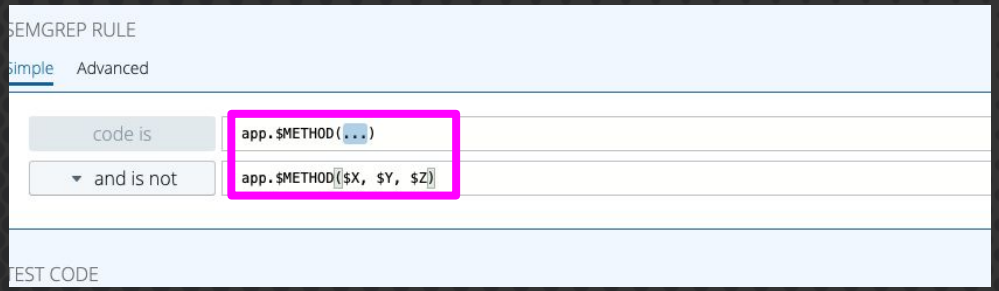
NODE.JS/EXPRESS - MAP

Here is an example from Nodegoat, I downloaded it, and searched for app.get



NODE.JS/EXPRESS - SEMGREP

Semgrep is a fast, easy, lightweight way to get started (no we don't endorse and it is free for community use) - semgrep.dev



TEST CODE

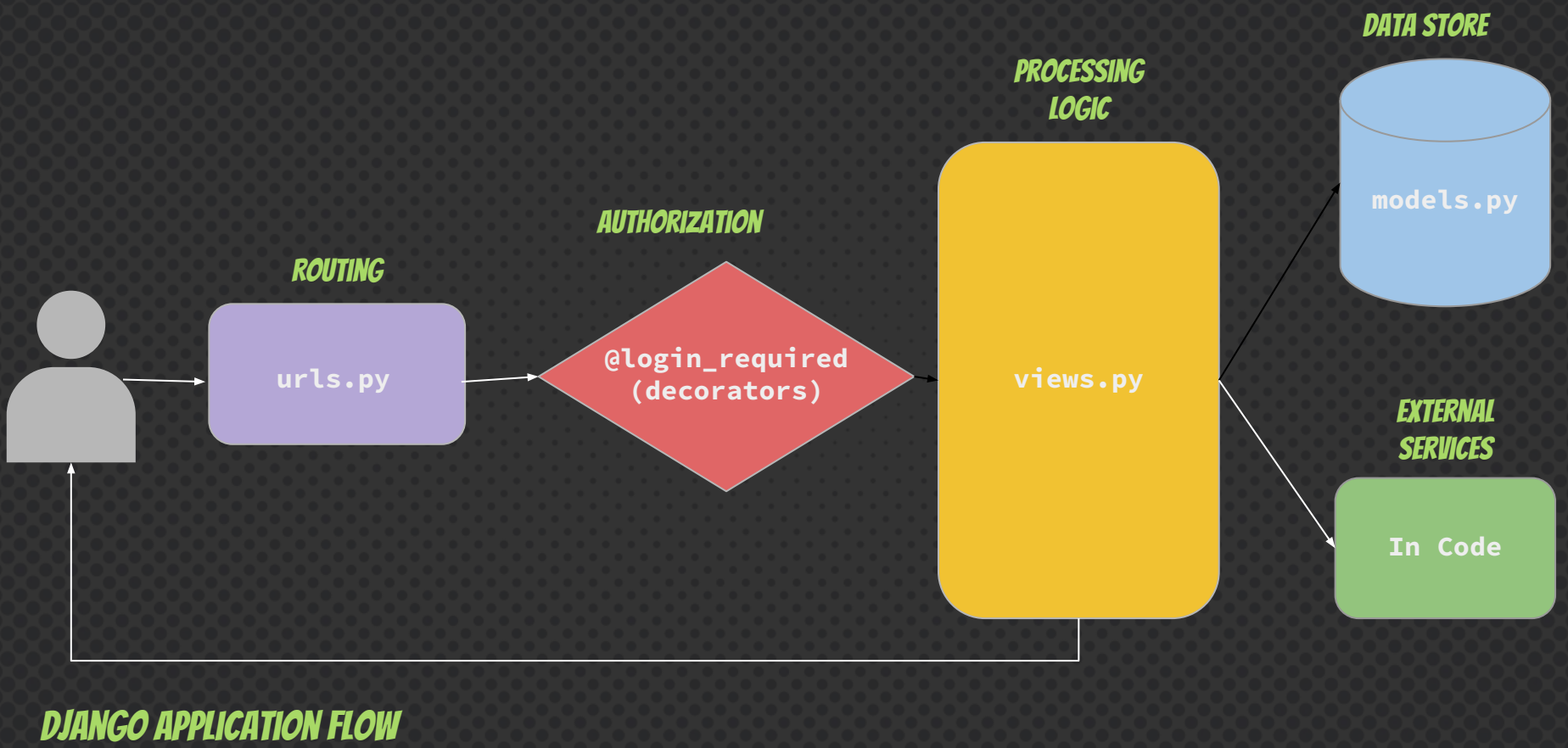
```
"use strict";

var sessionHandler = new SessionHandler(db);
var profileHandler = new ProfileHandler(db);
var benefitsHandler = new BenefitsHandler(db);
var contributionsHandler = new ContributionsHandler(db);
var allocationsHandler = new AllocationsHandler(db);
var memosHandler = new MemosHandler(db);

// Middleware to check if a user is logged in
var isLoggedIn = sessionHandler.isLoggedInMiddleware;

//Middleware to check if user has admin rights
var isAdmin = sessionHandler.isAdminUserMiddleware;

// The main page of the app

// Login form
app.get("/login", sessionHandler.displayLoginPage);
app.post("/login", sessionHandler.handleLoginRequest);

// Signup form
app.get("/signup", sessionHandler.displaySignupPage);
app.post("/signup", sessionHandler.handleSignup);

// Logout page
app.get("/logout", sessionHandler.displayLogoutPage);

// The main page of the app

// Profile page
app.get("/profile", isLoggedIn, profileHandler.displayProfile);
app.post("/profile", isLoggedIn, profileHandler.handleProfileUpdate);

// Contributions Page
app.get("/contributions", isLoggedIn, contributionsHandler.displayContributions);
```

DEMO TIME! (SEMGREP)

NODE.JS/EXPRESS - MAP

Take a close looksie

```
42    app.get("/dashboard", isLoggedIn, sessionHandler.displayWelcomePage);
```



DJANGO APPLICATION FLOW

DJANGO - MAP

urls.py — ~/code/vtm

urls.py

```
# Vulnerable Task Manager

from django.conf.urls import include, url
from django.contrib import admin
from django.http import HttpResponseRedirect
from django.conf import settings
from django.views.defaults import page_not_found

from taskManager.views import index

urlpatterns = [
    url(r'^$', index, name='index'),
    url(r'^taskManager/', include(('taskManager.taskManager_urls','taskManager'), namespace="taskManager")),
    url(r'^admin/', admin.site.urls ),
   ]

```

DJANGO - MAP

taskManager_urls.py

```
# Vulnerable Task Manager

from django.conf.urls import url

from taskManager import views

urlpatterns = [
                        url(r'^$', views.index, name='index'),

                        # User details
                        url(r'^view_all_users/$',
                            views.view_all_users, name='view_all_users'),

                        # File
                        url(r'^download/(?P<file_id>\d+)/$',
                            views.download, name='download'),
                        url(r'^(?P<project_id>\d+)/upload/$',
                            views.upload, name='upload'),
                        url(r'^downloadprofilepic/(?P<user_id>\d+)/$',
                            views.download_profile_pic, name='download_profile_pic'),

                        # Authentication & Authorization
                        url(r'^register/$', views.register, name='register'),
                        url(r'^login/$', views.login, name='login'),
                        url(r'^logout/$', views.logout_view, name='logout'),
                        url(r'^manage_groups/$', views.manage_groups,
```

DJANGO - MAP

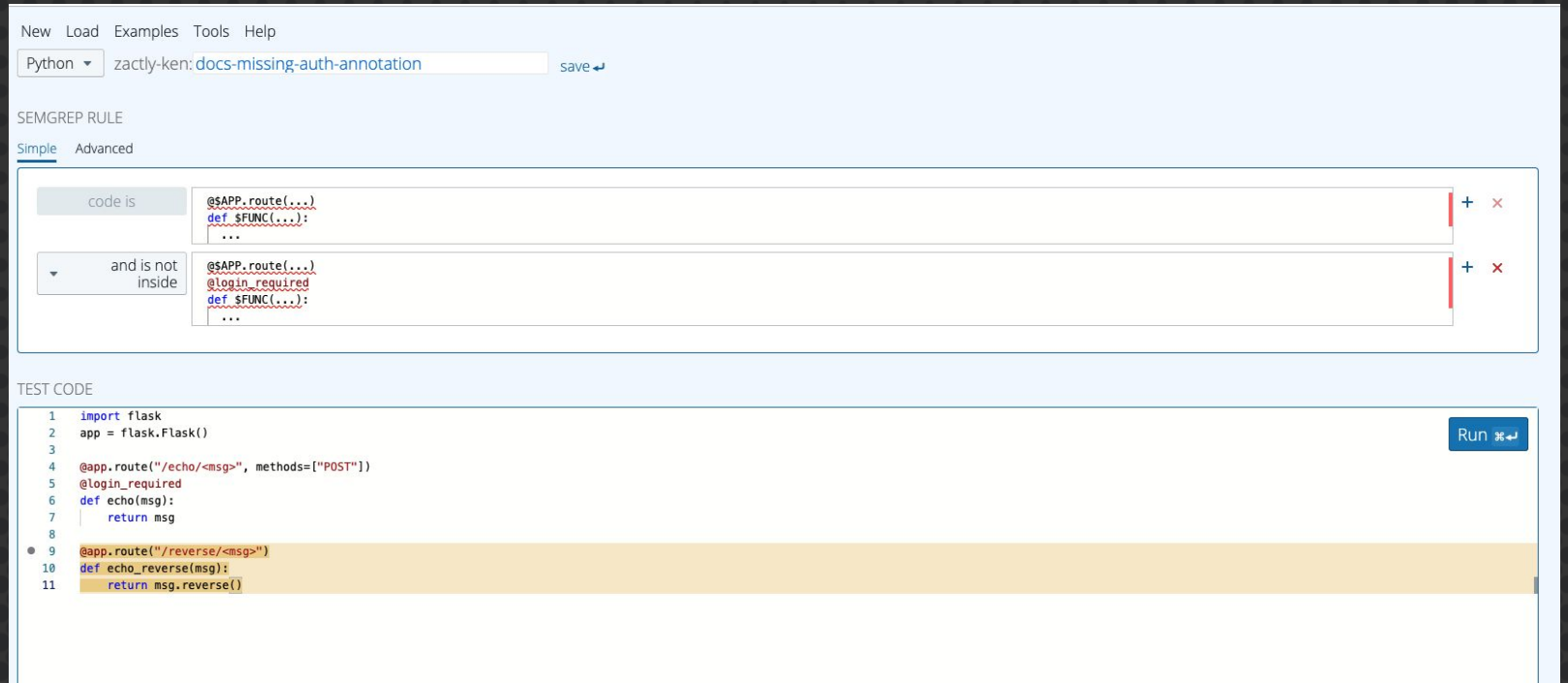
```
# User details
url(r'^view_all_users/$',
    views.view_all_users, name='view_all_users'),
```

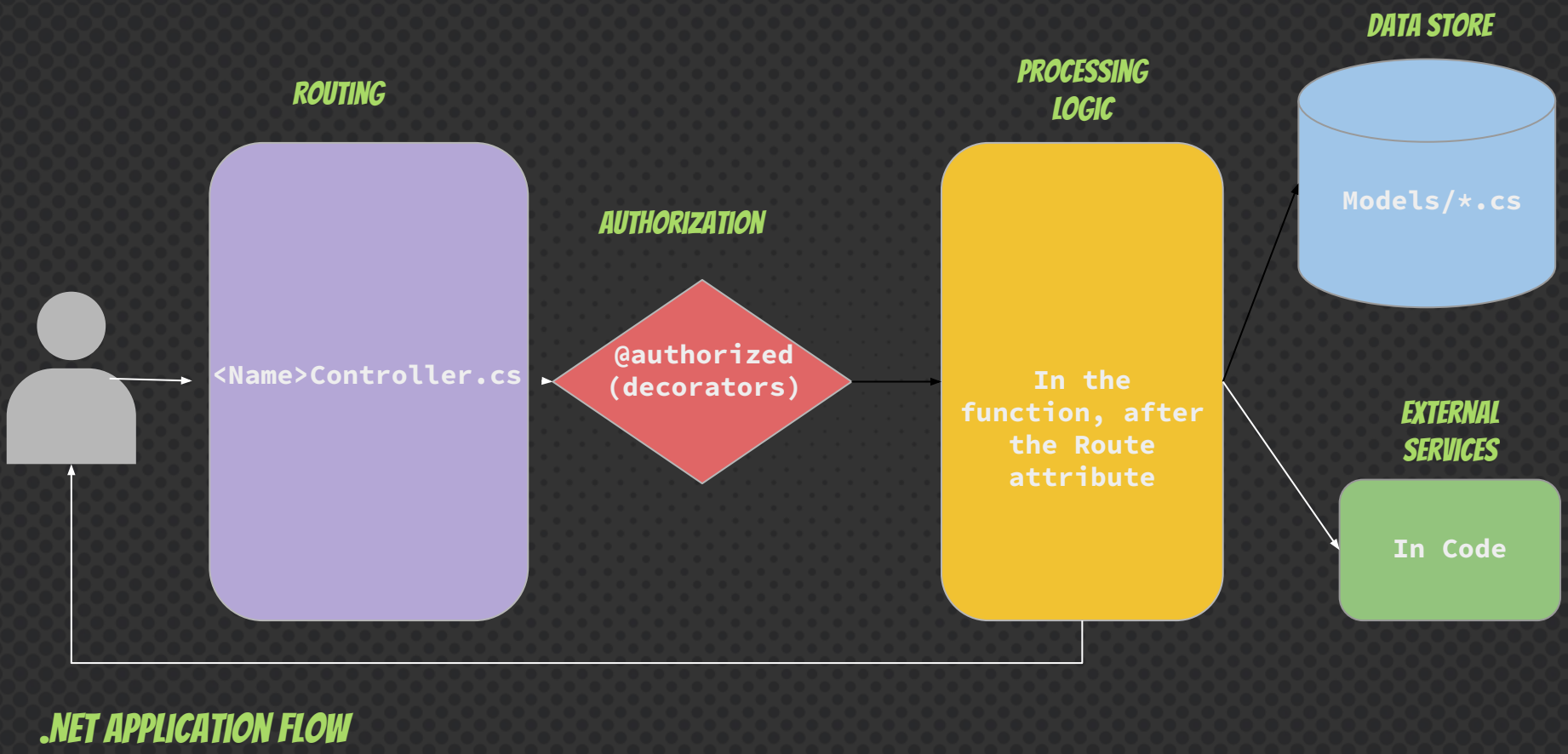
DJANGO - MAP

```
cktricky@Kens-MBP ~/code/vtm master ./manage.py show_urls                    ✓ 5281 01:08:18
/       taskManager.views.index index   login_required
/admin/ django.contrib.admin.sites.index        admin:index
/admin/<app_label>/     django.contrib.admin.sites.app_index    admin:app_list
/admin/auth/group/      django.contrib.admin.options.changelist_view    admin:auth_group_changelist
/admin/auth/group/<path:object_id>/     django.views.generic.base.RedirectView
/admin/auth/group/<path:object_id>/change/      django.contrib.admin.options.change_view        admin:auth_group_change
/admin/auth/group/<path:object_id>/delete/      django.contrib.admin.options.delete_view        admin:auth_group_delete
/admin/auth/group/<path:object_id>/history/     django.contrib.admin.options.history_view       admin:auth_group_history
/admin/auth/group/add/  django.contrib.admin.options.add_view   admin:auth_group_add
/admin/auth/group/autocomplete/ django.contrib.admin.options.autocomplete_view  admin:auth_group_autocomplete
/admin/auth/user/       django.contrib.admin.options.changelist_view    admin:auth_user_changelist
/admin/auth/user/<id>/password/ django.contrib.auth.admin.user_change_password  admin:auth_user_password_change
/admin/auth/user/<path:object_id>/      django.views.generic.base.RedirectView
/admin/auth/user/<path:object_id>/change/       django.contrib.admin.options.change_view        admin:auth_user_change
/admin/auth/user/<path:object_id>/delete/       django.contrib.admin.options.delete_view        admin:auth_user_delete
/admin/auth/user/<path:object_id>/history/      django.contrib.admin.options.history_view       admin:auth_user_history
/admin/auth/user/add/   django.contrib.auth.admin.add_view      admin:auth_user_add
/admin/auth/user/autocomplete/  django.contrib.admin.options.autocomplete_view  admin:auth_user_autocomplete
/admin/jsi18n/  django.contrib.admin.sites.i18n_javascript      admin:jsi18n
/admin/login/   django.contrib.admin.sites.login        admin:login
/admin/logout/  django.contrib.admin.sites.logout       admin:logout
/admin/password_change/ django.contrib.admin.sites.password_change      admin:password_change
/admin/password_change/done/    django.contrib.admin.sites.password_change_done admin:password_change_done
```

DJANGO - MAP (*SEMGREP)

https://semgrep.dev/s/minusworld:docs-missing-auth-annotation





.NET APPLICATION FLOW

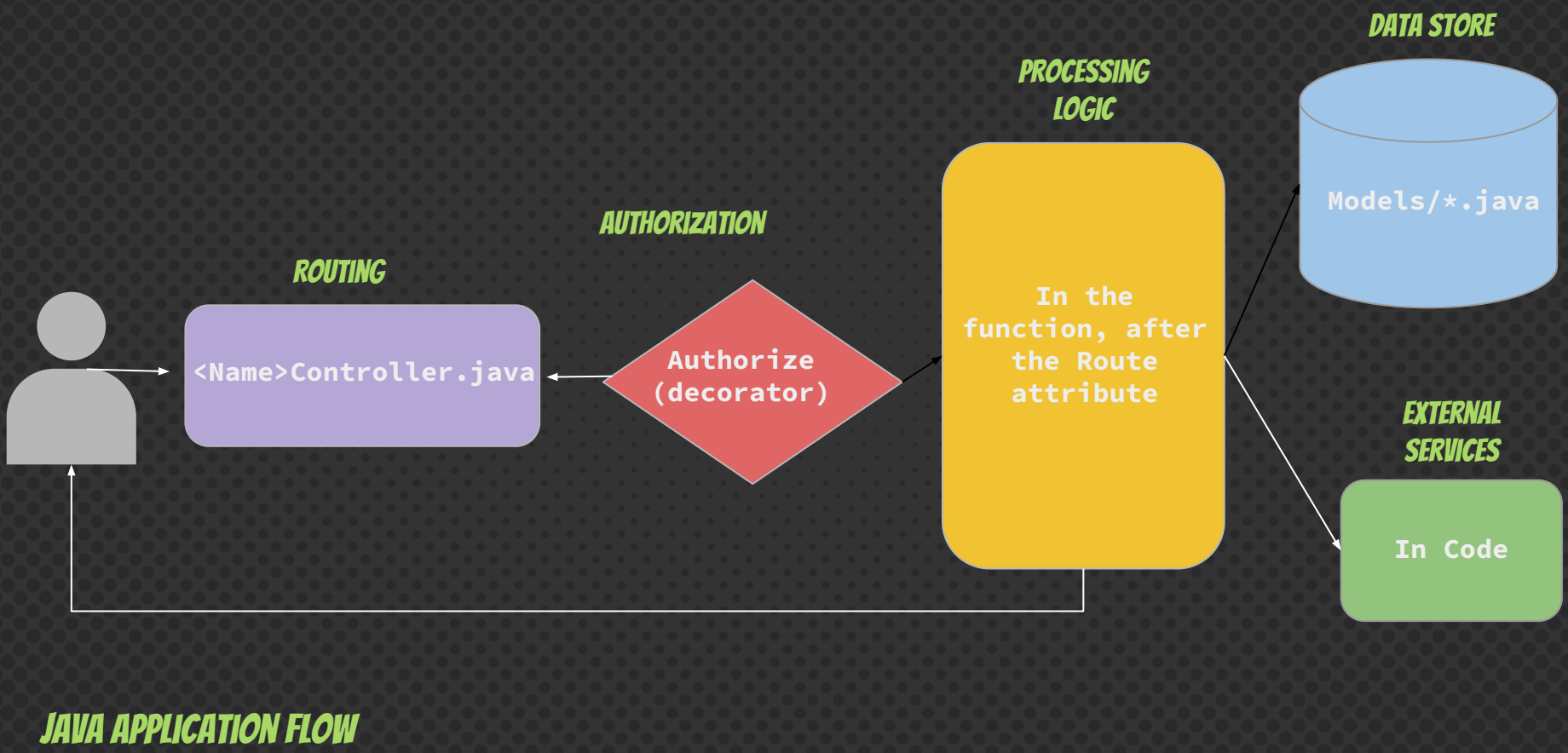
.NET CORE - MAP

AccountController.cs

```
1   using Microsoft.AspNetCore.Authentication;
2   using Microsoft.AspNetCore.Authentication.Cookies;
3   using Microsoft.AspNetCore.Authorization;
4   using Microsoft.AspNetCore.Mvc;
5   using Miniblog.Core.Models;
6   using System.Security.Claims;
7   using System.Threading.Tasks;
8   using Miniblog.Core.Services;
9
10  namespace Miniblog.Core.Controllers
11  {
12      [Authorize]
13      public class AccountController : Controller
14      {
15          private readonly IUserServices _userServices;
16
```

.NET CORE - MAP

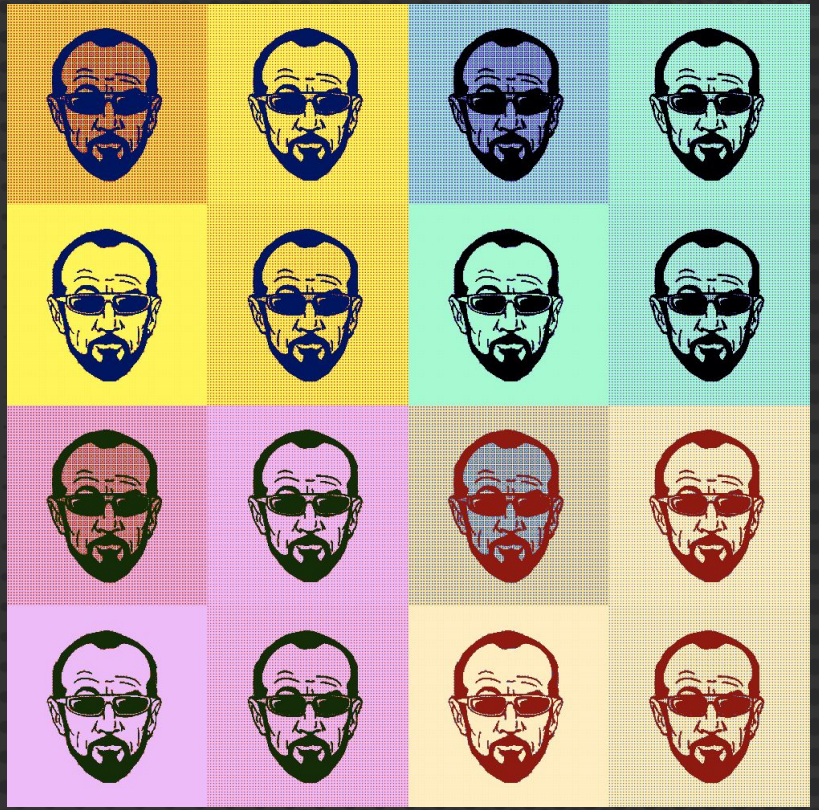
```
[Route("/login")]
[AllowAnonymous]
[HttpGet]
public IActionResult Login(string returnUrl = null)
{
    ViewData["ReturnUrl"] = returnUrl;
    return View();
}

[Route("/login")]
[HttpPost, AllowAnonymous, ValidateAntiForgeryToken]
public async Task<IActionResult> LoginAsync(string returnUrl, LoginViewModel
```


DATA STORE
PROCESSING LOGIC
Models/*.java
AUTHORIZATION
ROUTING
In the function, after the Route attribute
<Name>Controller.java
Authorize (decorator)
EXTERNAL SERVICES
In Code
JAVA APPLICATION FLOW

MAPPING

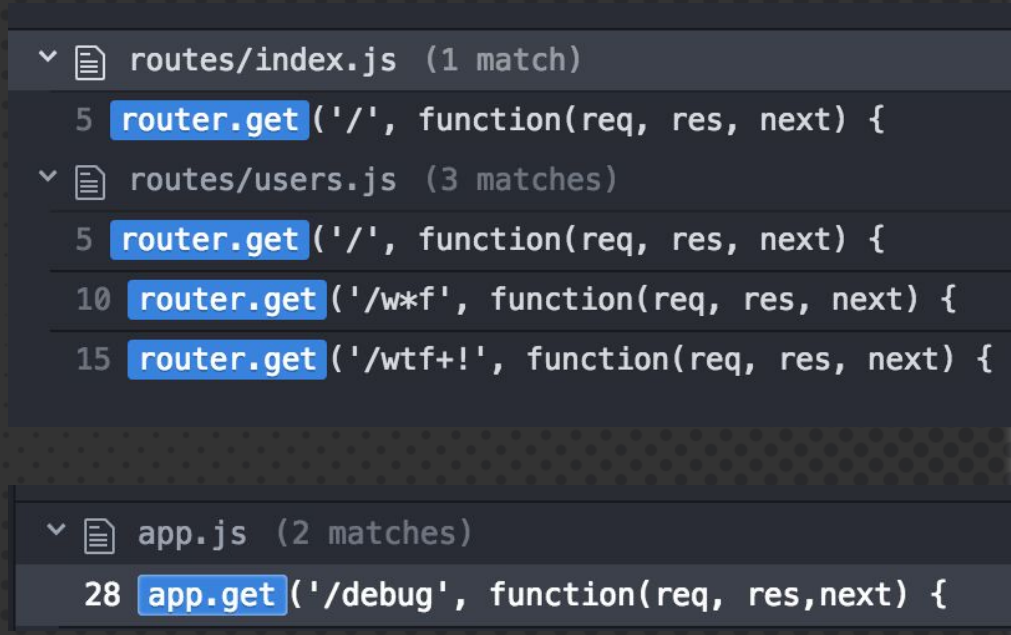
EXERCISE RUFUS

1. **skea_node**
    a. Perform Info Gathering
        i. (Tech Stack/Biz Purpose/Risk Assessment)
    b. Map Routes
2. **bhima**
    a. Map Routes



RUFUS EXERCISE - POST-MORTEM

- Notes should include:
  - Commit #
  - End points shown here
  - Any else you found interesting, such as:
    - auth function doesn't do anything
    - debug statement in our app and its printing env variables



Authorization Functions

Information Gathering - Authorization Functions

- A later step is dedicated to creating authorization checks
- This is about getting to know the application better
- Get to know how users are identified/authorized to perform actions

Information Gathering - Authorization Functions

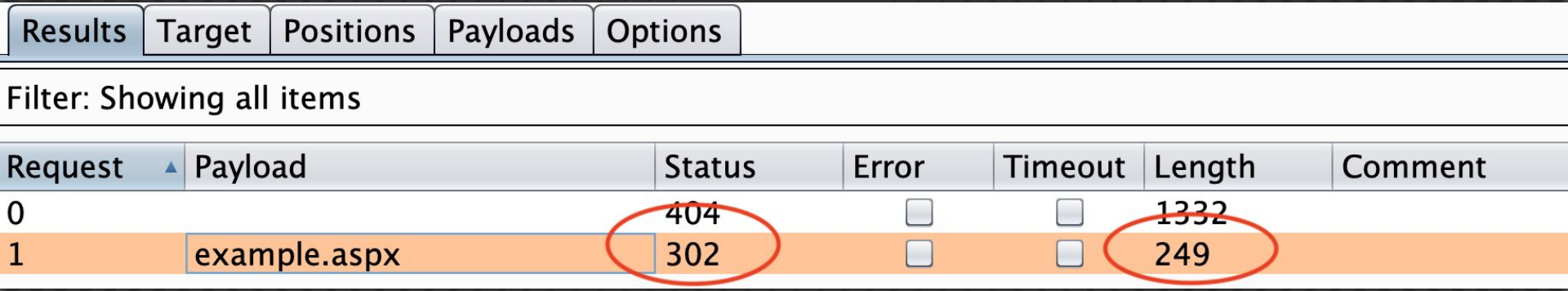
- Patterns & Anti-patterns
  - How do we identify the user? eg: Session, Token, Basic Auth
  - What is the purpose? Authenticated users, Role check, or something else?
- Identify what could go wrong
  - User-supplied parameters (IDOR)
  - CSRF
  - Client-side cookies, JWTs etc. (just general wonkiness in persistence)

Story Time:

Redirection & Authorization in .NET

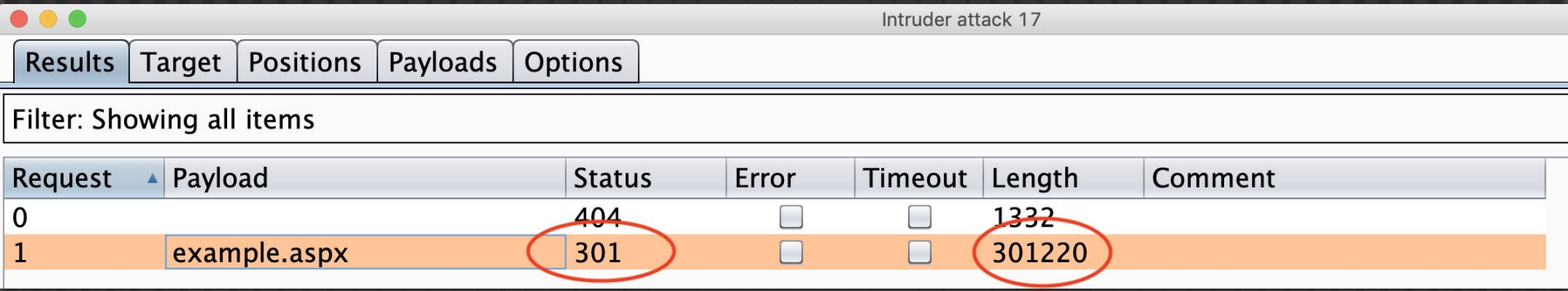
REDIRECTION & AUTHORIZATION ISSUE IN .NET

NORMAL



REDIRECTION & AUTHORIZATION ISSUE IN .NET

DEFINITELY NOT NORMAL



REDIRECTION & AUTHORIZATION ISSUE IN .NET

Redirect(String, Boolean)

Redirects a client to a new URL. Specifies the new URL and whether execution of the current page should terminate.

C# Copy

```
public void Redirect (string url, bool endResponse);
```

Parameters

`url` String

The location of the target.

`endResponse` Boolean

Indicates whether execution of the current page should terminate.

AUTHZ FUNCTIONS - INCORRECTLY CONFIGURED EXAMPLE

application_controller.rb

```
1  # frozen_string_literal: true
2  class ApplicationController < ActionController::Base
3    before_action :authenticated, :has_info, :create_analytic, :mailer_optic
4    helper_method :current_user, :is_admin?, :sanitize_font
5
6    # Our security guy keep talking about sea-surfing, cool story bro.
7    # Prevent CSRF attacks by raising an exception.
8    # For APIs, you may want to use :null_session instead.
9    protect_from_forgery #with: :exception
10
```

Authorization Functions Checklist

How is user access controlled?

- Session
- Token
- Basic Authentication
- Something… else?

AUTHZ FUNCTIONS CHECKLIST

Identify its purpose

- Is it just checking that we're authenticated?
  - ❑ AuthN
- Is it looking for a specific role?
  - ❑ RBAC
- Is it doing some sort of HMAC verification for events?

AUTHZ FUNCTIONS CHECKLIST

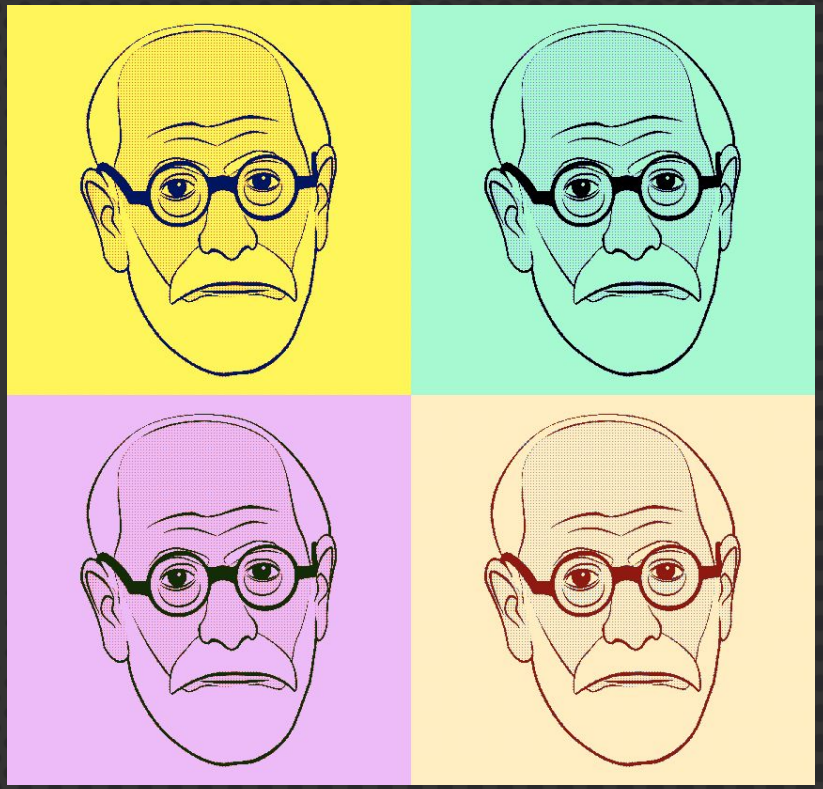
- ❑ What could go wrong?
  - Insecure timing comparisons
  - Framework nuances
  - IDOR (Insecure Direct Object reference)
  - Lack of rate limiting (see this often with basic auth or tokens)
  - Think about if it was *not* applied, what would happen
  - **Get creative, you're trying to decide what the risk, if any, is here**

AUTHZ FUNCTIONS

EXERCISE SIGMUND FREUD

1. **skea_rails**
   a. Perform Info Gathering
      i. (Tech Stack/Biz Purpose/Risk Assessment)
   b. Map Routes
   c. Map AuthZ Functions

2. How are users authorized in skea_rails?
   a. Could take some time



SIGMUND FREUD EXERCISE - POST-MORTEM

Yeah, you probably have questions re: **`authenticate_user!`**

a. Which is why its part of the exercise :=D. THIS HAPPENS A LOT!

home_controller.rb

```
1  class HomeController < ApplicationController
2    before_action :authenticate_user!
3
```

How to decipher where this action is defined will be defined by:

b. Access to an interactive runtime env?
c. Experience with the framework/libs?
d. No previous experience with it, only access to source?

SIGMUND FREUD EXERCISE - POST-MORTEM

Did you catch the CSRF? - “Framework Nuance”

```
post    "/articles", to: "articles#create"
get     "/articles/new", to: "articles#new", as: :new_article
get     "/articles/:id/:action", to: "articles#edit", as: :edit_article
get     "/articles/:id", to: "articles#show", as: :article
post    "/articles/:id/vote/:type", to: "articles#vote", as: :vote
```

SIGMUND FREUD EXERCISE - POST-MORTEM

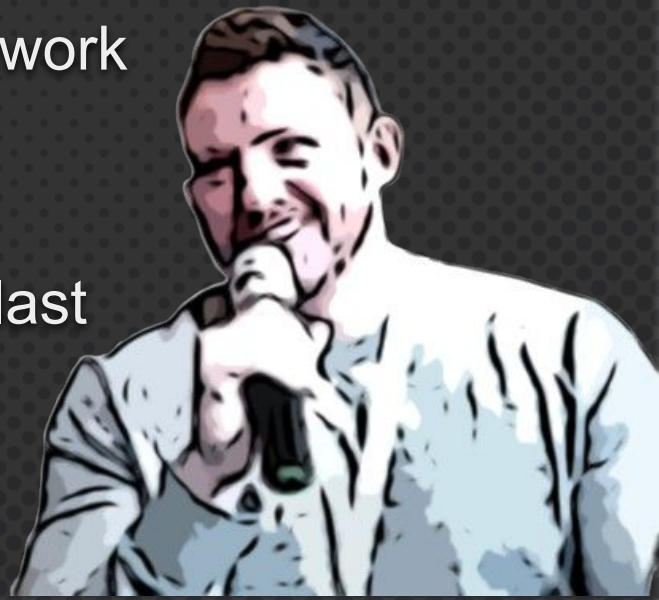
Anyone know what the request attack string would look like?


```
get     "/articles/:id/:action", to: "articles#edit", as: :edit_article
```

Sigmund Freud Exercise - Post-Mortem

So what's the point of this whole thing?

- Do your homework on framework nuances
- Good example of why we double-back and check one last time… (story time)



PULL REQUEST REVIEWS

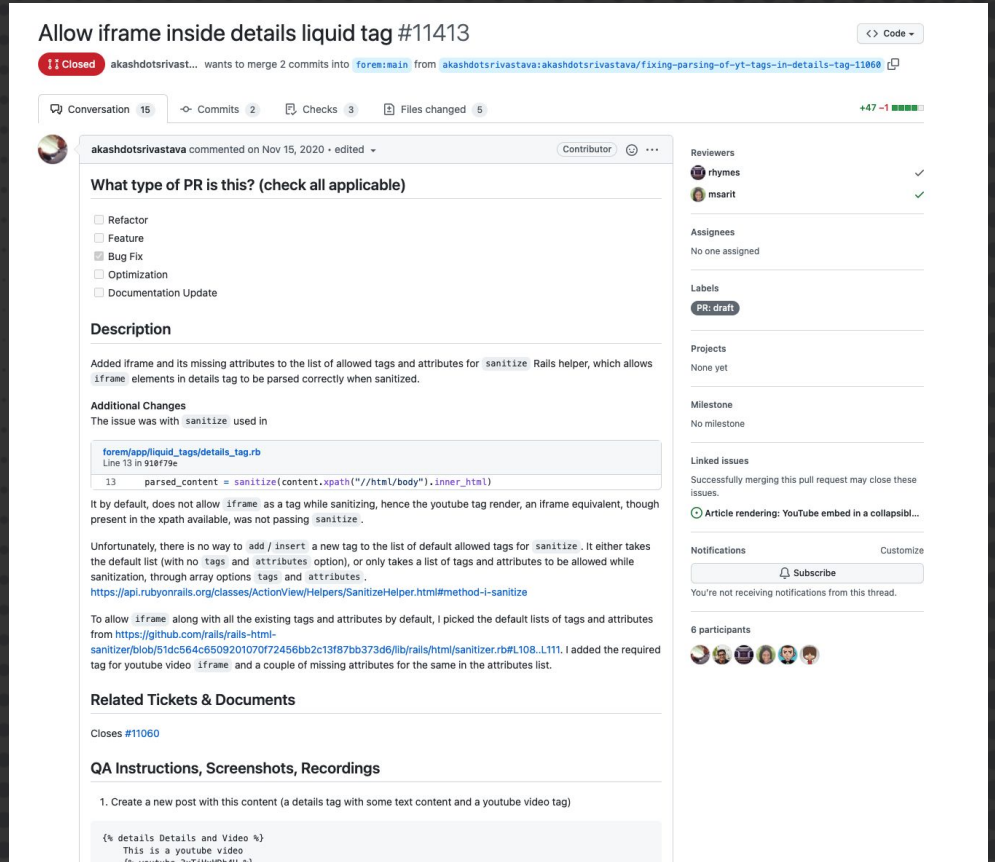
PULL REQUEST REVIEWS - OVERVIEW

Not an end-to-end code review

Snippets are often accompanied by fuzzy context and Understanding context is critical

Common components:

- Tests (and there NEeds to be tests)
- Conversation (context)
- code



Allow iframe inside details liquid tag #11413

Code

Closed akashdotsrivast... wants to merge 2 commits into forem:main from akashdotsrivastava:akashdotsrivastava/fixing-parsing-of-yt-tags-in-details-tag-11060

Conversation 15 Commits 2 Checks 3 Files changed 5 +47 −1

akashdotsrivastava commented on Nov 15, 2020 • edited Contributor

What type of PR is this? (check all applicable)

- [ ] Refactor
- [ ] Feature
- [x] Bug Fix
- [ ] Optimization
- [ ] Documentation Update

Description

Added iframe and its missing attributes to the list of allowed tags and attributes for `sanitize` Rails helper, which allows `iframe` elements in details tag to be parsed correctly when sanitized.

Additional Changes

The issue was with `sanitize` used in

forem/app/liquid_tags/details_tag.rb
Line 13 in 910f79e

```
13      parsed_content = sanitize(content.xpath("//html/body").inner_html)
```

It by default, does not allow `iframe` as a tag while sanitizing, hence the youtube tag render, an iframe equivalent, though present in the xpath available, was not passing `sanitize`.

Unfortunately, there is no way to `add / insert` a new tag to the list of default allowed tags for `sanitize`. It either takes the default list (with no `tags` and `attributes` option), or only takes a list of tags and attributes to be allowed while sanitization, through array options `tags` and `attributes`.
https://api.rubyonrails.org/classes/ActionView/Helpers/SanitizeHelper.html#method-i-sanitize

To allow `iframe` along with all the existing tags and attributes by default, I picked the default lists of tags and attributes from https://github.com/rails/rails-html-sanitizer/blob/51dc564c6509201070f72456bb2c13f87bb373d6/lib/rails/html/sanitizer.rb#L108..L111. I added the required tag for youtube video `iframe` and a couple of missing attributes for the same in the attributes list.

Related Tickets & Documents

Closes #11060

QA Instructions, Screenshots, Recordings

1. Create a new post with this content (a details tag with some text content and a youtube video tag)

```
{% details Details and Video %}
    This is a youtube video
```

Reviewers
rhymes
msarit

Assignees
No one assigned

Labels
PR: draft

Projects
None yet

Milestone
No milestone

Linked issues
Successfully merging this pull request may close these issues.
Article rendering: YouTube embed in a collapsibl...

Notifications Customize
Subscribe
You're not receiving notifications from this thread.

6 participants

PULL REQUEST REVIEWS - OVERVIEW

General steps:

- Get to know the app
- Get to know the purpose of the pull request
- Read through other's comments
- Use git blame if necessary
- Ask questions!!!
- Seek data flow diagrams or something similar
- Common flaws associated with the portion of code you are reviewing (eg: controller == authz issues)

CHECKLISTS & REVIEWS

AUTHORIZATION

AUTHORIZATION REVIEW

- Analyze source for role enforcement, appropriate user boundaries, privileges required for access, and business-logic flaws
- aRoles and associated enforcement routines must be identified during information gathering
- Pay attention to any endpoints that include sensitive data or functionality
  - Vertical authorization weaknesses - escalated privileges
    - Authenticated and unauthenticated access
  - Horizontal authorization weaknesses - access another user’s data

Authorization Review Vulnerabilities

- Broken Access Control - OWASP Top 10 A01:2021
  - Privilege Escalation
  - Missing Function Level Access Control
  - Insecure Direct Object Reference
- Sensitive Data Exposure - OWASP Top 10 A3:2017
- Mass Assignment
- Business Logic Flaws

```java
/** Check if userUid has access to a specific application at Organization group Level */
 @ReadOnlyTransaction
 public boolean isApplicationAllowedByUser(
     final Organization org,
     final Application app,
     final String userUid,
     final boolean includeArchived) {
   if (app.isArchived() && !includeArchived) {
     return false;
   }

   // check if application exists
   final EacUser eacUser =
       eacUserAccessControlService.getAccessControlForUser(org.getId(), userUid);
   if (eacUser.isViewAllApplications()) {
     return true;
   }

   return eacUser.getAllowedApplications().contains(app.getId());
 }
```

SPOT THE BUG

AUTHORIZATION REVIEW CHECKLIST

- What are the different authorization functions?
  - Token/User/Role validation?
  - Is this handled by custom framework functionality?
  - Decorators vs. static source code
- Can non-privileged users view, add, or alter accounts?
- Is there functionality to add accounts with higher access levels than their own access?
- How is separation of duties handled?
- Are disabled accounts prevented from accessing content?
- Can password-protected pages be directly accessed without authentication?

MASS-ASSIGNMENT

- https://cheatsheetseries.owasp.org/cheatsheets/Mass_Assignment_Cheat_Sheet.html
- Goes by a few names
  - Insecure Binder Vulnerability
  - Insecure Object Mapping
  - Mass-Assignment
- Typically happens when a database entry is created or modified and we do so by throwing in *all* user-supplied parameters
- For example...

MASS-ASSIGNMENT - NODE

```
var user = new User(req.body);
user.save();
```

MASS-ASSIGNMENT- RAILS 2/3

```ruby
def create
  user = User.new(params[:user])
  if user.save
    session[:user_id] = user.id
    redirect_to home_dashboard_index_path
  else
    @user = user
    flash[:error] = user.errors.full_messages.to_sentence
    redirect_to :signup
  end
end
```

RAILS 4+

```ruby
def create
  user = User.new(user_params)
  if user.save
    session[:user_id] = user.id
    redirect_to home_dashboard_index
```

```ruby
def user_params
  params.require(:user).permit!
end
```

AUTHORIZATION REVIEW CHECKLIST

- Is it possible to bypass authorization restrictions by accessing content directly (e.g. can a non-privileged user access the administration pages of an application)?
- Can a user escalate privileges through cookie modification, altering form input values and HTTP headers, or by fuzzing URL-based parameters?
- Are there horizontal escalation/Insecure Direct Object References in the source code?
- Are authentication and authorization flows the first logic executed for each request?
- Are authorization checks granular (page and directory level) or per-application?

AUTHORIZATION REVIEW CHECKLIST

- Are access to sensitive pages and data denied by default?
- Are users forced to re-assert their credentials for requests that have critical side-effect (account changes, password reset, etc)?
- Do authorization checks have clearly defined roles?
- Can authorization be circumvented by parameter or cookie/token manipulation?
- Are CSRF protections in place and appropriate?

AUTHORIZATION

EXERCISE GENGHIS KHAN

1. **skea_django**
    a. Info Gathering
        i. (Tech Stack/Biz Purpose/Risk Assessment)
    b. Map Routes
    c. AuthZ Functions
2. Build an authorization checklist
3. Test checklist items

GENGHIS KHAN EXERCISE - POST-MORTEM

First of all look into views.py

settings.py × views.py ×

... RPS > Training > SKEA > skea_django > intro > views.py > create_todo

```
12
13 # Create your views here.
14 def index(request):
15     return HttpResponse("Welcome to Seth & Ken's Excellent Adventures
16
17 @login_required
18 def todo(request, todo_id):
19     if request.method == 'GET':
20         try:
```

GENGHIS KHAN EXERCISE - POST-MORTEM

What about objects? Does it protect against IDOR? How?

```
17 @login_required
18 def todo(request, todo_id):
19     if request.method == 'GET':
20         try:
21             todo = Todo.objects.get(pk=todo_id,owner=request.user)
22             form = TodoForm(initial={'todo_text':todo.todo_text,
23                                      'todo_date':todo.todo_date,
24                                      'completed':todo.completed})
```

AUTHENTICATION

AUTHENTICATION REVIEW

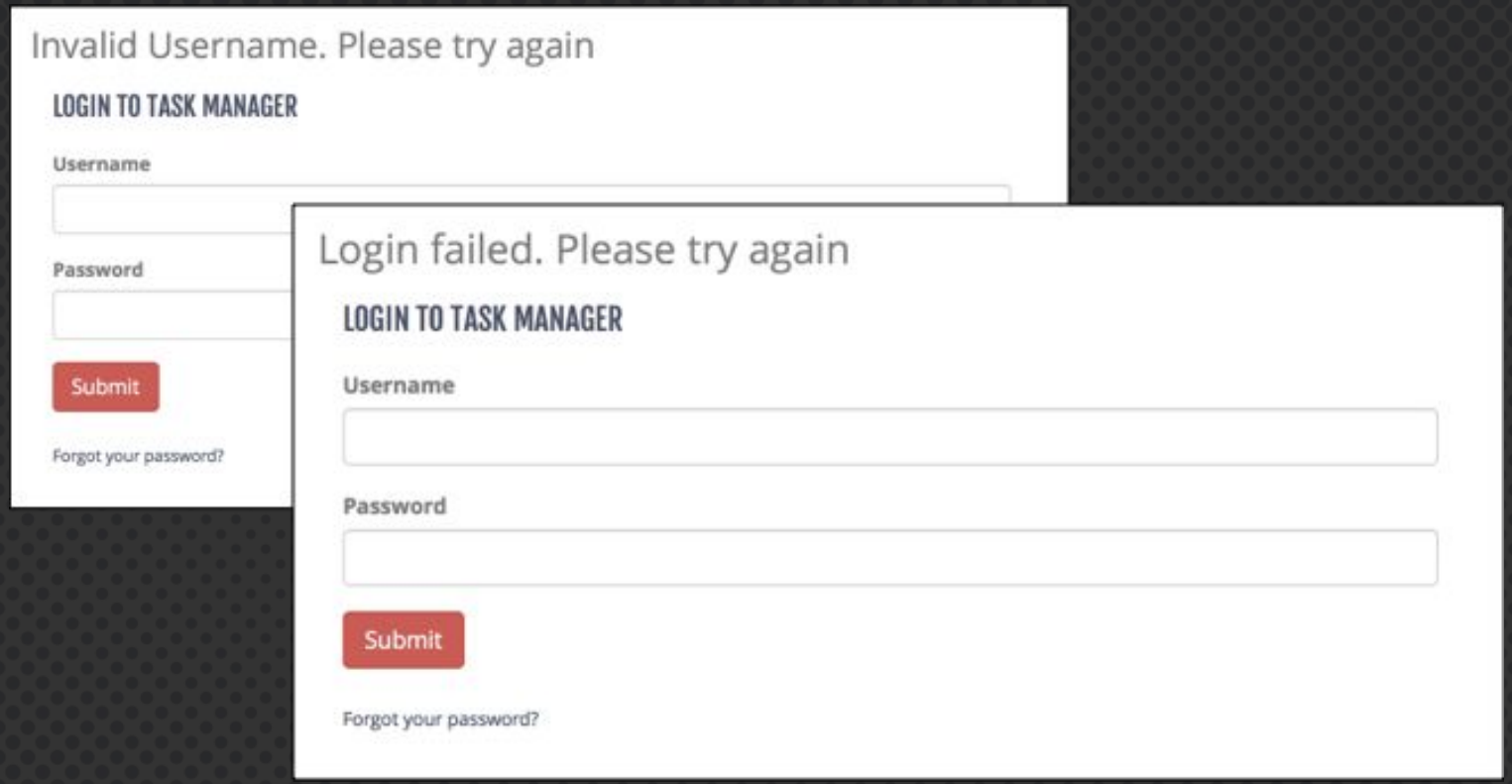
- Authentication establishes user identity
- Examine the user identification process of the application.
- Available application resources include both unidentified and identified users
- Use enumeration of the application endpoints to trace the authentication flow and functions.
- Sensitive application and business functionality should redirect as appropriate to the authentication flow to properly identify a user
- Include an application functionality that identifies a user in this review

Authentication Review

How does an application confirm identity?

Authentication Review Vulnerabilities

- Identification and Authentication Failures - OWASP Top 10 A07:2021
- User Enumeration
- Session Management Issues
- Authentication Bypass
- Brute-Force Attacks


Invalid Username. Please try again
LOGIN TO TASK MANAGER
Username
Password
Submit
Forgot your password?
Login failed. Please try again
LOGIN TO TASK MANAGER
Username
Password
Submit
Forgot your password?

SPOT THE BUG

```
exports.update = function(req, res) {

    if (req.body.new_password = req.body.new_password_confirmation){
        username = req.body.username
        current_password = req.body.current_password
        isMatch = true

        db.User.find({where: {username: username}}).success(function (user){
            hash = user ? user.password : ''
            isMatch = db.User.validPassword(current_password, hash, function () { console.lo
        });
        if (isMatch) {
            req.user.username = username
            req.user.password = req.body.new_password
            req.user.save()
        } else {
            console.log('Bad Password')
        }
    }

    res.redirect('/account')
};
```

SPOT THE BUG

Authentication Review Checklist

- Identify all the authentication flows
  - User Login
  - User Registration
  - Forgot Password
- How are users identified? What information do they have to provide?
  - Username, email, password, 2fa token, etc.
- How is authentication handled on each application endpoint?
  - Sensitive endpoints should require authentication
- Are there any hard-coded accounts?
- Does application allow for easily-guessed, default, or common passwords?

AUTHENTICATION REVIEW CHECKLIST

- How are usernames determined, what naming conventions?
  - Does registration allow for easy enumeration?
- Does the application allow for account enumeration through server responses or information disclosure?
  - login/registration/forgot password flows
- Are user credentials protected in the data store using modern password hashing algorithms?
- Are security policies are configurable via environment variables and not hard-coded?
- What standard security frameworks are used?
  - Is there code specific to the application, especially when dealing with password storage?

Authentication Review Checklist

- How are user management events such as authentication failures, password resets, password changes, account lockout and disabled accounts handled?
- Are suspicious event handling such as multiple failed login attempts, session replay and attempted access to restricted resources handled properly?
- Does the application implement strong password policies?
- Are authentication credentials being passed using technologies that could be cached (HTTP GET, lack of proper cache-control settings)?
- If applicable, are encryption mechanisms in place during authentication for secure communications (TLS, etc)?

Authentication Review Checklist (Registration)

- Are limits on application access, such as geographical boundaries, enforced properly?
- Is there a manual approval process or is access granted automatically?
  - Can the automated process be abused or bypassed using scripting or brute-forcing?
- In cases where a validation email and link are required, how are the tokens generated?
- Can users elevate their initial access via mass assignment or business-logic bypasses?
- Are files and objects owned by a user removed or archived?

Authentication Review Checklist (Sessions)

- Are encryption and hashing used properly?
- Do encryption protocols use strong algorithms and industry-standard key lengths?
- Are authentication tokens set with time limits?
- Are cookies security parameters set properly (e.g. Secure, HTTPOnly, path)?
- Are session IDs sent over a secure channel?
- Are session IDs invalidated before a new login is made?
- Are CSRF tokens set for all authentication requests?

```
31      User.findOne({
32              username: req.body.username
33      }, function(err, user) {
34              if (err){
35                      res.send(err);
36              }
37              else{
38                      if (!user) {
39                              res.send("User not found");
40                      }
41                      else {
42                              if (user.password == req.body.password) {
43                                      var token = jwt.sign(user, config.secret, {expi
44
45                                      res.redirect('/homepage?token='+token);
46
47                              } else {
48                                      res.send("Incorrect Password");
49                              }
```

SPOT THE BUG

```
387         if User.objects.filter(username=username).exists():
388             user = authenticate(username=username, password=password)
389             if user is not None:
390                 if user.is_active:
391                     auth_login(request, user)
392                     # Redirect to a success page.
393                     return redirect(request.GET.get('next', '/taskManager/'))
394                 else:
395                     # Return a 'disabled account' error message
396                     return redirect('/taskManager/', {'disabled_user': True})
397             else:
398                 # Return an 'invalid login' error message.
399                 return render(request,
400                               'taskManager/login.html',
401                               {'failed_login': False})
402         else:
403             return render(request,
404                           'taskManager/login.html',
405                           {'invalid_username': False})
```

SPOT THE BUG

AUTHENTICATION

EXERCISE SOCRATES

1. **skea_django**
   a. Build Authentication Checklist
   b. Review AuthN Checklist

2. **bhima**
   a. Build/Review AuthN Checklist

SO-CRATES EXERCISE - POST-MORTEM

So what exactly are we looking for?

a. ./manage.py show_urls (django extensions have to be enabled).

```
/admin/jsi18n/  django.contrib.admin.sites.i18n_javascript      admin:jsi18n
/admin/login/   django.contrib.admin.sites.login        admin:login
/admin/logout/  django.contrib.admin.sites.logout       admin:logout
/admin/password_change/ django.contrib.admin.sites.password_change      admin:pa
ssword_change
/admin/password_change/done/    django.contrib.admin.sites.password_change_donea
dmin:password_change_done
/admin/r/<int:content_type_id>/<path:object_id>/        django.contrib.contentty
pes.views.shortcut      admin:view_on_site
/intro/ intro.views.index       index
/intro/<int:todo_id>/   intro.views.todo        todo
/intro/login/   django.contrib.auth.views.LoginView     login
/intro/logout/  django.contrib.auth.views.LogoutView    logout
/intro/password/        django.contrib.auth.views.PasswordChangeView    password
/intro/password_change/ django.contrib.auth.views.PasswordChangeView    password
```

SO-CRATES EXERCISE - POST-MORTEM

Where do they go?

intro/urls.py has no references to login????

urls.py

```
from django.urls import path
from django.contrib.auth import views as auth_views
from . import views

urlpatterns = [
    path('', views.index, name='index'),
    path('signup/', views.SignUp.as_view(), name='signup'),
    path('password/', auth_views.PasswordChangeView.as_view(template_name='change_password.html'), name='password'),
    path('<int:todo_id>/',views.todo, name='todo'),
    path('todo/',views.create_todo, name='create todo'),
    path('todos/',views.todos, name='todos'),
    path('todos/completed/',views.todos_completed, name='completed todos')
]
```

SO-CRATES EXERCISE - POST-MORTEM

Neither does skea_django/urls.py but.. there is a reference to **`django.contrib.auth.urls`**

urls.py — intro | urls.py — skea_django

```
1  from django.contrib import admin
2  from django.urls import include, path
3  from django.views.generic.base import TemplateView
4
5  urlpatterns = [
6      path('', TemplateView.as_view(template_name='home.html'), name='home'),
7      path('admin/', admin.site.urls),
8      path('intro/', include('intro.urls')),
9      path('intro/',include('django.contrib.auth.urls')),
10 ]
11
```

SO-CRATES EXERCISE - POST-MORTEM

Configuration documentation for **django.contrib.auth** leads us to *skea_django/settings.py*

```
103
104   AUTH_USER_MODEL = 'intro.TodoUser'
105
106   LOGIN_REDIRECT_URL = 'home'
107   LOGOUT_REDIRECT_URL = 'home'
108   LOGIN_URL = '/intro/login/'
109
```

SO-CRATES EXERCISE - POST-MORTEM

Searching for django.contrib.auth leads us to *intro/models.py*

login.html | *models.py* | views.py

```
1  from django.db import models
2  from django.contrib.auth.models import AbstractUser
3
4  # Create your models here.
5
6  class TodoUser(AbstractUser):
7
8      def __str__(self):
9          return self.email
10
11 class Todo(models.Model):
12     todo_text = models.TextField()
```

SO-CRATES EXERCISE - POST-MORTEM

If we go back to the **`django.contrib.auth`** documentation, it uses the templates in the registration directory.

login.html | forms.py | views.py

```
1  <!-- templates/registration/login.html -->
2  {% extends 'base.html' %}
3
4  {% block title %}Login{% endblock %}
5
6  {% block content %}
7  <div class="row">
8    <div class="col-3"></div>
9      <div class="col-6">
10     <h2>Login</h2>
11     <form method="post">
12       {% csrf_token %}
13       {{ form.as_p }}
14         <button type="submit" class="btn btn-secondary">Login</button>
```

AUDITING

AUDITING REVIEW

- Validate that appropriate logging and exception handling are handled within application source
- One path in the trace of sensitive data from source to sink
- Logging functions and error messages are considered a data sink
- Logging should happen in any endpoint that performs a state-changing operation or has security implications
- This data is used for immediate analysis and future forensics needs.
- Check that sensitive data is appropriately handled (no credit card numbers, etc) and the correct details are logged
- Administrators must trust that logs may not be manipulated by unauthorized parties

AUDITING REVIEW VULNERABILITIES

- Cryptographic Failures - OWASP Top 10 A02:2021
- Security Logging & Monitoring Failures - OWASP Top 10 A09:2021
- Debug Messages
- Error Handling
- Information Leakage

```
superadminService.manageOrganizationByUserUid(userUid, org);
ImpersonateHelper.configureImpersonateWebSettings(
    request, response, ImpersonateReturnMode.USERS_MODE);
apiResponse.setOrgUuid(org.getUuid());
apiResponse.registerSuccess(String.format("Switching to user '%s' successfully", userUid));

return new ResponseEntity<>(apiResponse, HttpStatus.OK);
```

SPOT THE BUG

AUDITING REVIEW CHECKLIST

- If an exception occurs, does the application fails securely?
- Do error messages reveal sensitive application or unnecessary execution details?
- Are Component, framework, and system errors displayed to end user?
- Does exception handling that occurs during security sensitive processes release resources safely and roll back any transactions?
- Are relevant user details and system actions logged?
- Is sensitive user input flagged, identified, protected, and not written to the logs?
    - Credit Card #s, Social Security Numbers, Passwords, PII, keys

AUDITING REVIEW CHECKLIST

- Are unexpected errors and inputs logged?
  - Multiple login attempts, invalid logins, unauthorized access attempts
- Are log details should be specific enough to reconstruct events for audit purposes?
- Are logging configuration settings configurable through settings or environment variables and not hard-coded into the source?
- Is User-controlled data validated and/or sanitized before logging to prevent log injection?

LOGGING - JAVA

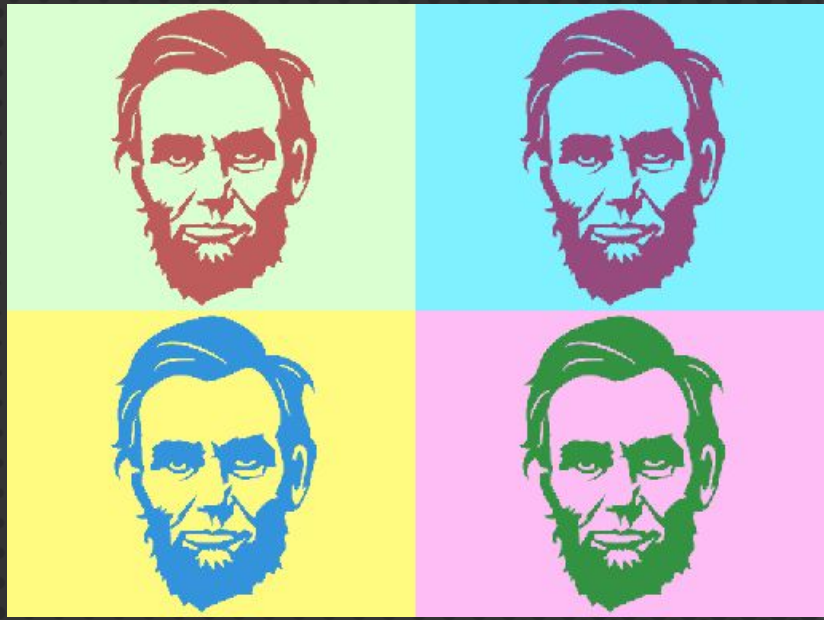
```
    return new ResponseEntity<>(apiResponse, HttpStatus.OK);
} catch (final ServiceException e) {
    log.error("ERROR: " + e.getMessage());
    ErrorHelper.addErrorMessage(
        String.format("Failed to impersonate user '%s'", userUid), apiResponse, e);
}
```

AUDITING

EXERCISE ABRAHAM LINCOLN

1. **skea_django**
   a. Build/Review Auditing Checklist

2. **bhima**
   a. Build/Review Auditing Checklist



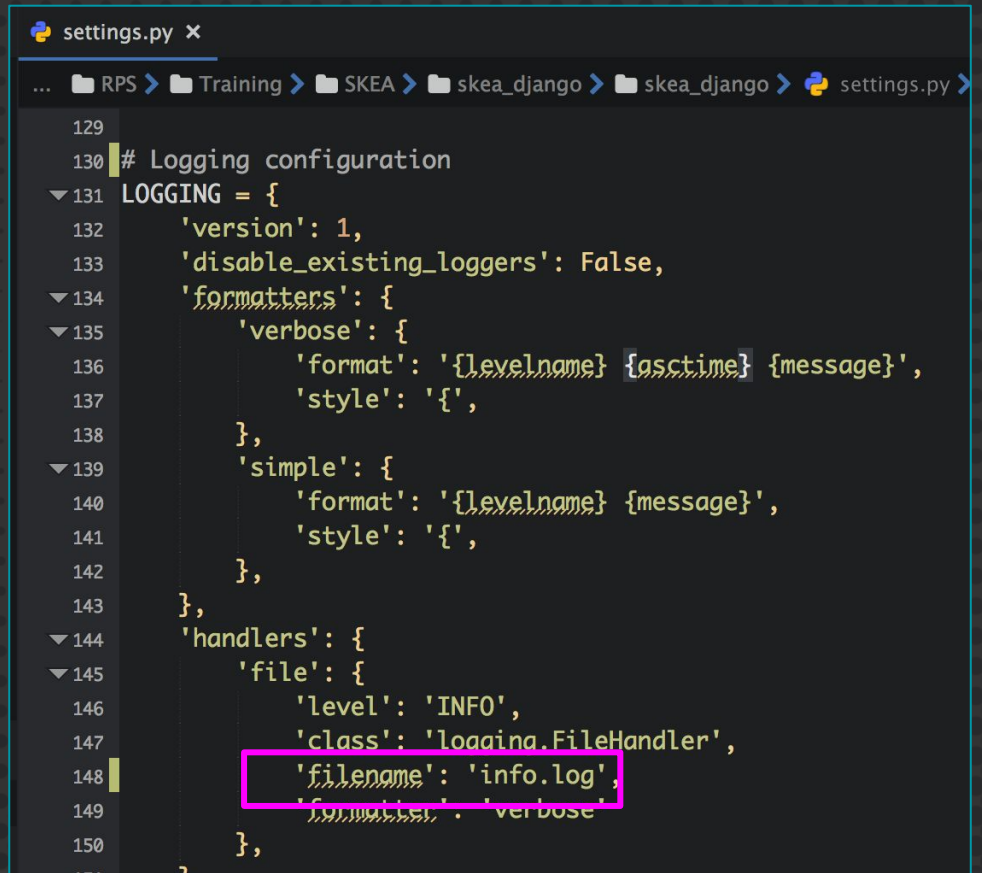
ABRAHAM LINCOLN EXERCISE - POST-MORTEM

So where should we look? Sensitive functions.

```
47 @login_required
48 def create_todo(request):
49     if request.method == 'POST':
50         form = TodoForm(request.POST)
51         if form.is_valid():
52             t = Todo( todo_text=form.cleaned_data['todo_text'],
53                       todo_date = form.cleaned_data['todo_date'],
54                       completed = form.cleaned_data['completed'])
55             t.owner = request.user
56             t.save()
57             logger.info("Created todo %s by %s" % (todo_id,request.user.username))
58             return HttpResponseRedirect('/intro/todos/')
59
60     else:
61         form = TodoForm()
```

ABRAHAM LINCOLN EXERCISE - POST-MORTEM

- It's django, so everything is setup in settings.py.
- The intro application goes right along with this.



INJECTION

INJECTION

- Causes:
  - Input Validation
  - Output Encoding
- Types
  - SQL Injection
  - HTML Injection (XSS)
  - LDAP, XML, Command ...

Injection Vulnerabilities

- Injection - OWASP Top 10 A03:2021
- XML External Entities (XXE)
- Cross-Site Scripting (XSS)
- Redirects
- Server Side Request Forgery (SSRF) - OWASP Top 10 A10:2021

```
if (FormsAuthenticationHelper.IsRelativeUrl(redirectUrl))
{
        this.Response.Redirect(redirectUrl, true);
}
else
```

```
/// <summary>
/// Tests the incomming url to see if it relative.
/// </summary>
/// <param name="url"></param>
/// <returns></returns>
public static bool IsRelativeUrl(string url)
{
        Uri result;
        return Uri.TryCreate(url, UriKind.Relative, out result);
}
```

SPOT THE BUG

INPUT VALIDATION

- Analyze code that handles user input for type, format, and content validation before being used or stored by the application.
- Compile list of data sources to work through.
- Start with the routes identified in the information gathering phase, but also include:
  - Configuration files
  - Environment variables
  - External services
  - Database calls to external and internal databases.
  - ...

INPUT VALIDATION - CHECKLIST

- Is all input is validated without exception?
- Do the validation routines check for known good characters and cast to the proper data type (integer, date, etc.)?
- Is the user data validated on the client or server or both (security should not rely solely on client-side validations that may be bypassed)?

INPUT VALIDATION - CHECKLIST

- If both client-side and server-side data validation is taking place, are these validations consistent and synchronized?
- Do string input validation use regular expressions?
- Do these regular expressions use DenyLists or AcceptLists?
- What bypasses exist within the regular expressions?

INPUT VALIDATION - CHECKLIST

- Does the application validate numeric input by type and reject unexpected input?
- How does the application evaluate and process input length?
- Is a strong separation enforced between data and commands (filtering out injection attacks)?

INPUT VALIDATION - CHECKLIST

- Is there separation between data and client-side scripts?
- Is provided data checked for special characters before being passed to SQL, LDAP, XML, OS and third party services?
- For web applications, are often forgotten HTTP request components, including HTTP headers (e.g. referrer) validated?

SQL INJECTION - DJANGO

```
@csrf_exempt
def forgot_password(request):

    if request.method == 'POST':
        t_email = request.POST.get('email')

        try:
            result = User.objects.raw("SELECT * FROM auth_user where email = '%s'" % t_email)

            if len(list(result)) > 0:
                result_user = result[0]
                # Generate secure random 6 digit number
                res = ""
                nums = [x for x in os.urandom(6)]
```

SQL INJECTION - NODE.JS

```
10
11 exports.search = function(req,res) {
12     q = "";
13     users = [];
14     if (req.query.q) {
15         q = req.query.q;
16         db.User.findAll({attributes: ['id', 'username'], where: {username: { like: '%'
           +req.query.q+'%' } }}).success(function(users){
17             //console.log('Users:', users)
18             res.render("search.ejs", { q: q, username: req.user.username, users: users
                });
19         });
20     } else {
21         db.User.findAll().then(function(users){
22             //console.log('Users:', users)
23             res.render("search.ejs", { q: q, username: req.user.username, users: users
                });
24         });
```

OUTPUT ENCODING

- Analyze code that sends user data to client for context, type, and format before sending to uncontrolled data sinks.
- Start with a list of data sinks where data is being stored, sent, processed.
  - Source code libraries
  - 3rd-party services
  - Storage components (database in any of its possible forms)
  - File system interactions
  - Log files
- XSS, SSRF

OUTPUT ENCODING - CHECKLIST

- Do databases interactions use parameterized queries?
- Do input validation functions properly encode or sanitize data for the output context?
- How do framework-provided database ORM functions used?
- Does the source code use potentially-dangerous ORM functions? (.raw, etc)

OUTPUT ENCODING - CHECKLIST

- What output encoding libraries are used?
- Are output encoding libraries up-to-date and patched?
- Is proper output encoding used for the context of each output location?
- Are output encoding routines dependent on regular expressions? Are there any weaknesses or blind-spots in these expressions?

XSS - NODE.JS (EJS TEMPLATES)

```
106     <tbody>
107
108       <% for(var i=0; i < listings.length; i++) { %>
109       <tr>
110         <td><%- listings[i].created %></td>
111         <td><%- listings[i].name %></td>
112         <td><%- listings[i].description %></td>
113         <td><%- listings[i].deadline %>
114
115         </td>
116         <td><a class="icon-ok" href="javascript:alert('Apply for Position')"></a><a c
117       </tr>
118       <% } %>
119     </tbody>
120   </table>
121   </div>
```

XSS - DJANGO

```
<!-- user login dropdown start-->
<li class="dropdown">
    <a data-toggle="dropdown" class="dropdown-toggle" href="#">
        <!--User Identity -->
        <span class="username"><i class="fa fa-user fa-fw"></i> {{ user.username|safe }}</span>
        <b class="caret"></b>
    </a>
    <ul class="dropdown-menu extended logout">
        {% if user.id %}
```

INJECTION

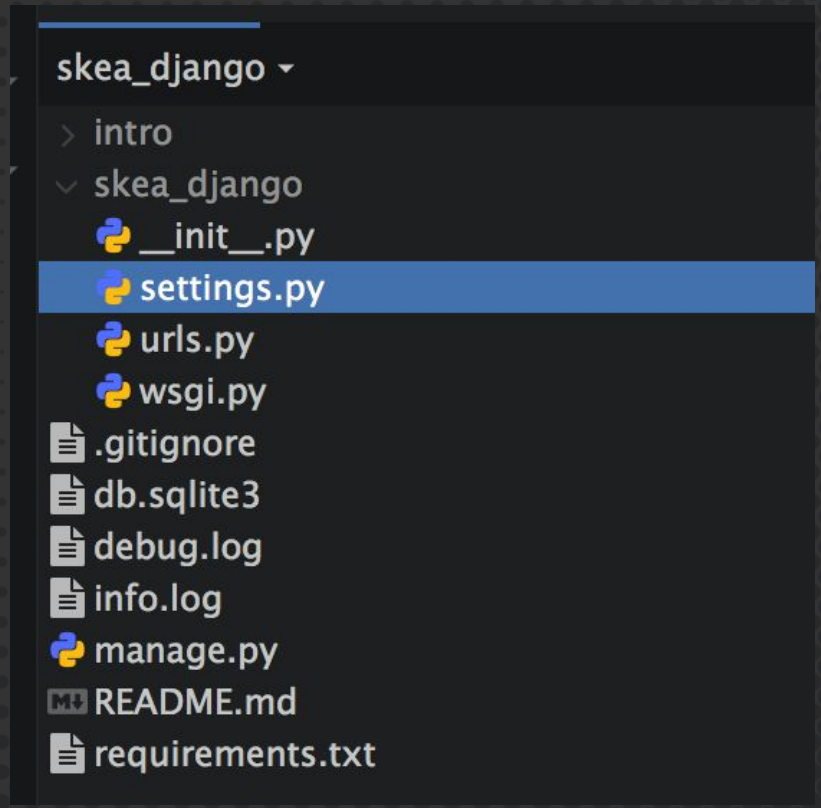
EXERCISE BILLY THE KID

1. **skea_django**
   a. Build Injection Checklist
   b. Trace all sources To sinks

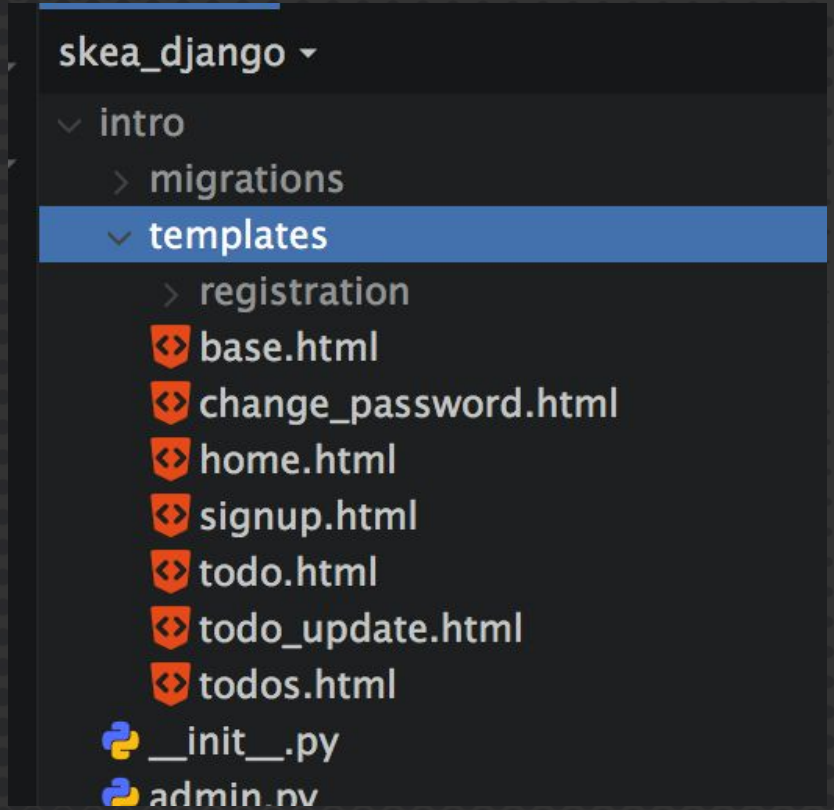
2. **bhima**
   a. Build Injection Checklist
   b. Trace at least 3 different sources to sinks

EXERCISE BILLY THE KID - POST-MORTEM

- Some sources have already been identified. Are there others?
- Configuration files, additional services, even databases.
- Settings.py is somewhat trusted, but other people could manipulate data in the database before it gets to us.



EXERCISE BILLY THE KID - POST-MORTEM



- Now for sinks, we know that the database file is one, but what else?
- Anywhere data is /sent/ somewhere, file system, user, etc.

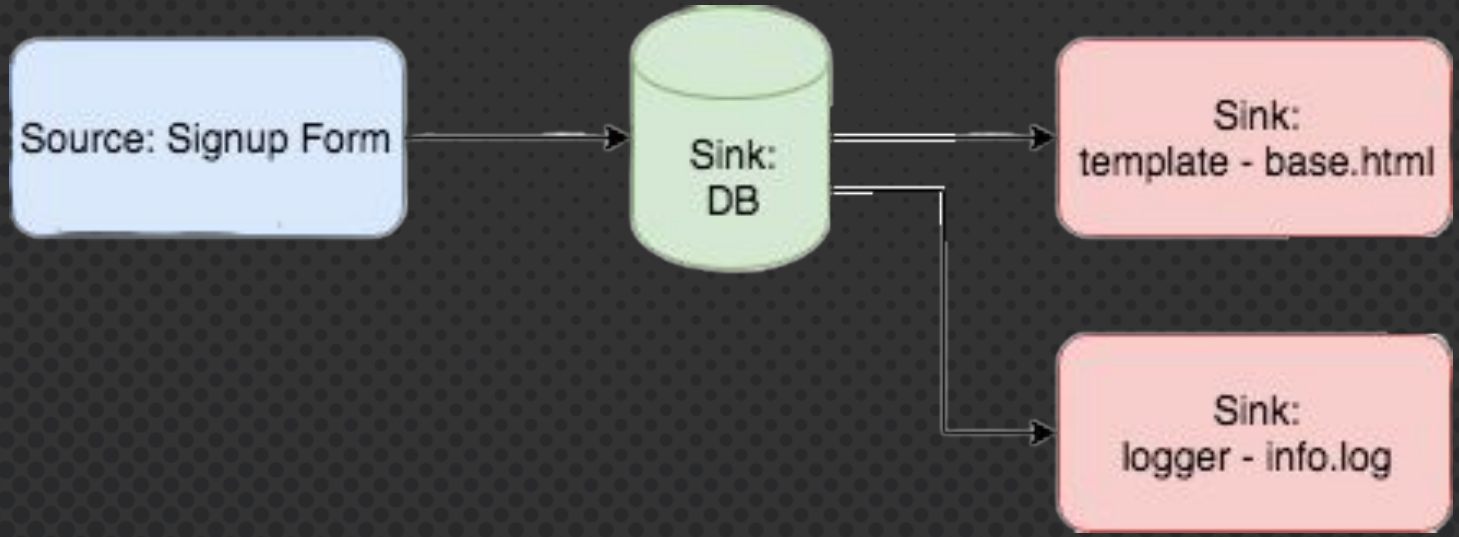
EXERCISE BILLY THE KID - POST-MORTEM

Search for `user.username` shows multiple references.

File	Line	Content
<skea_django>/intro/admin.py	12	list_display = ['email', 'username',]
<skea_django>/intro/forms.py	12	fields = ('username', 'first_name', 'last_name', 'email')
<skea_django>/intro/forms.py	18	fields = ('username', 'first_name', 'last_name', 'email')
<skea_django>/intro/views.py	28	logger.info("GET todo %s by %s" % (todo_id,request.user.username))
<skea_django>/intro/views.py	43	logger.info("Updated todo %s by %s" % (todo_id,request.user.username))
<skea_django>/intro/views.py	57	logger.info("Created todo %s by %s" % (todo_id,request.user.username))
<skea_django>/intro/views.py	68	logger.info("GET todos by %s" % (request.user.username))
<skea_django>/intro/views.py	74	logger.info("GET completed todos by %s" % (request.user.username))
<skea_django>/intro/migrations/0001_initial.py	27	('username', models.CharField(error_messages={'unique': 'A us
<skea_django>/intro/migrations/0001_initial.py	27	('username', models.CharField(error_messages={'unique': 'A us
<skea_django>/intro/migrations/0001_initial.py	27	('username', models.CharField(error_messages={'unique': 'A us
<skea_django>/intro/migrations/0001_initial.py	27	('username', models.CharField(error_messages={'unique': 'A us
<skea_django>/intro/templates/base.html	30	{{user.username}} |

EXERCISE BILLY THE KID - POST-MORTEM

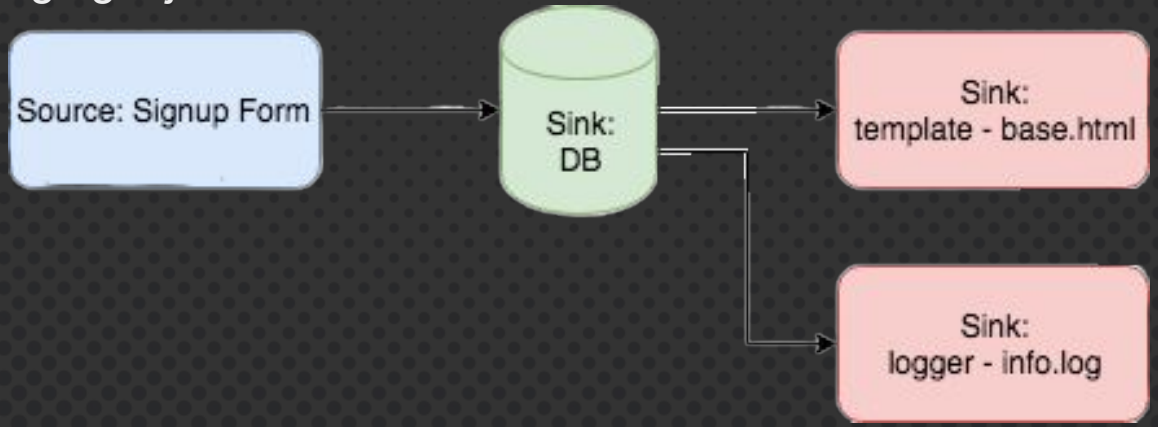
Diagram for user.username ends up looking like this.



EXERCISE BILLY THE KID - POST-MORTEM

This means we will be looking for the following injection flaws:

a. SQL Injection (database storage)
b. XSS (Stored/Reflected)
c. Log Forging/Injection



CRYPTOGRAPHIC ANALYSIS

Cryptographic Analysis

- Analyze code for encryption flaws, outdated protocols, custom-developed algorithms, weak encryption, and misuse
- Automated tools will uncover some of this, including
  - Use of older hashing algorithms (MD5, SHA-1, etc)

Cryptographic Analysis

- Code and routes that handles sensitive information specifically should be reviewed
  - API Tokens
  - Credit Card Numbers
  - Social Security Numbers
  - Customer Data
- IDE Search for the following terms:
  - md5, sha1, base64, encrypt, decrypt, secure

Cryptographic Analysis Vulnerabilities

- Cryptographic Failures - OWASP Top 10 A02:2021
- Lack of Encryption
- Improper Encryption
- Insecure Token Generation/Randomness

CRYPTOGRAPHIC ANALYSIS - CHECKLIST

- What are the standard encryption libraries are used for?
  - Hashing functions - password hashing, cryptographic signing, etc
  - Encryption functions - data storage, communications
- Do the strength of implemented ciphers meet industry standards?
  - Less than 256-bit encryption
  - MD5/SHA1 for password hashing
  - Any RC4 stream ciphers
  - Certificates with less than 1024-bit length keys
  - All SSL protocol versions
- Are cryptographic private keys, passwords, and secrets properly protected?

CRYPTOGRAPHIC ANALYSIS

EXERCISE BEETH-OVEN

1. **skea_django**
   a. Build Crypto Checklist
   b. How are passwords stored/tokens generated
2. **bhima**
   a. Build Crypto Checklist
   b. What hashing/crypto is being used?

EXERCISE BEETHOVEN - POST-MORTEM

Sessions - Only indication we have of activity is settings.py

```
33 INSTALLED_APPS = [
34     'intro.apps.IntroConfig',
35     'django.contrib.admin',
36     'django.contrib.auth',
37     'django.contrib.contenttypes',
38     'django.contrib.sessions',
39     'django.contrib.messages',
40     'django.contrib.staticfiles',
41     'django_extensions',
42 ]
43
44 MIDDLEWARE = [
45     'django.middleware.security.SecurityMiddleware',
46     'django.contrib.sessions.middleware.SessionMiddleware',
47     'django.middleware.common.CommonMiddleware',
48     'django.middleware.csrf.CsrfViewMiddleware',
```

EXERCISE BEETHOVEN - POST-MORTEM

Sessions - Django documentation helps us out a little.

Configuring the session engine

By default, Django stores sessions in your database (using the model **`django.contrib.sessions.models.Session`**). Though this is convenient, in some setups it's faster to store session data elsewhere, so Django can be configured to store session data on your filesystem or in your cache.

EXERCISE BEETHOVEN - POST-MORTEM

Sessions - but also gives us a warning...

Warning

If the SECRET_KEY is not kept secret and you are using the `PickleSerializer`, this can lead to arbitrary remote code execution.

An attacker in possession of the **SECRET_KEY** can not only generate falsified session data, which your site will trust, but also remotely execute arbitrary code, as the data is serialized using pickle.

If you use cookie-based sessions, pay extra care that your secret key is always kept completely secret, for any system which might be remotely accessible.

EXERCISE BEETHOVEN - POST-MORTEM

Alright, so we should check the randomness of the **SECRET_KEY**

```
21
22 # SECURITY WARNING: keep the secret key used in production secret!
23 SECRET_KEY = '*@ty00=62-recu@lsczr-o0(%y97c(ll1gnv9pu7o^)h%#e17d'
24
```

Looks random and secure, right? What are the concerns you have with this? Bueller?

EXERCISE BEETHOVEN - POST-MORTEM

- Possible issues (outside of encryption routines):
  a. Hardcoded values stored in source
  b. Same key used for dev/staging/production

EXERCISE BEETHOVEN - POST-MORTEM

Password Storage? Nothing in settings.py?

How Django stores passwords

Django provides a flexible password storage system and uses PBKDF2 by default.

The **password** attribute of a **User** object is a string in this format:

```
<algorithm>$<iterations>$<salt>$<hash>
```

EXERCISE BEETHOVEN - POST-MORTEM

PASSWORD_HASHERS in settings.py

```
[
    'django.contrib.auth.hashers.PBKDF2PasswordHasher',
    'django.contrib.auth.hashers.PBKDF2SHA1PasswordHasher',
    'django.contrib.auth.hashers.Argon2PasswordHasher',
    'django.contrib.auth.hashers.BCryptSHA256PasswordHasher',
    'django.contrib.auth.hashers.BCryptPasswordHasher',
    'django.contrib.auth.hashers.SHA1PasswordHasher',
    'django.contrib.auth.hashers.MD5PasswordHasher',
    'django.contrib.auth.hashers.UnsaltedSHA1PasswordHasher',
    'django.contrib.auth.hashers.UnsaltedMD5PasswordHasher',
    'django.contrib.auth.hashers.CryptPasswordHasher',
]
```

EXERCISE BEETHOVEN - POST-MORTEM

Did you run the app?

```
sqlite> select * from intro_todouser;
1|pbkdf2_sha256$120000$GJ1WIimqmSAl$6+WnzERREqiR44/FFLy8JjaEx160ysYFJW60MpdGizo=
|2018-10-05 21:14:37.054197|1|admin|||admin@test.com|1|1|2018-10-05 20:20:38.818
426
2|pbkdf2_sha256$120000$a2sGvDgOaIXT$Qa1LbL4hWolywacEqdEatLsH2Vcv0NlKopjq14oTC/E=
|2018-10-08 02:05:50.669012|0|test|Firsc|Last|test@test.com|0|1|2018-10-05 20:21
:00.520448
```

CONFIGURATION REVIEW

Configuration Review

- Analyze any configurations included for security flaws
  - Includes language, framework, and server configurations
- Highly specific to the targeted language/framework
- Consult the server/framework documentation for guides on security flags and settings.
- Examples:
  - Administrative Functionality enabled through configuration files
  - CSRF settings
  - Cookie parameters

CONFIGURATION REVIEW VULNERABILITIES

- Security Misconfiguration - OWASP Top 10 A05:2021
  - Insecure defaults
  - Incomplete configurations
  - Open cloud storage
- Vulnerable and Outdated Components - OWASP Top 10 A06:2021
  - Any dependencies, libraries, services

Stopping [redacted]

By default, the [redacted] requires an administrator password to initiate a server shutdown. The default (and permanent) administrator account is ADMIN with an initial default password of ADMIN.

SPOT THE BUG

CONFIGURATION REVIEW - CHECKLIST

- Are any endpoints enabled through configurations properly protected with authentication and authorization?
- Are security protections implemented in framework properly configured?

Configuration Review - Checklist

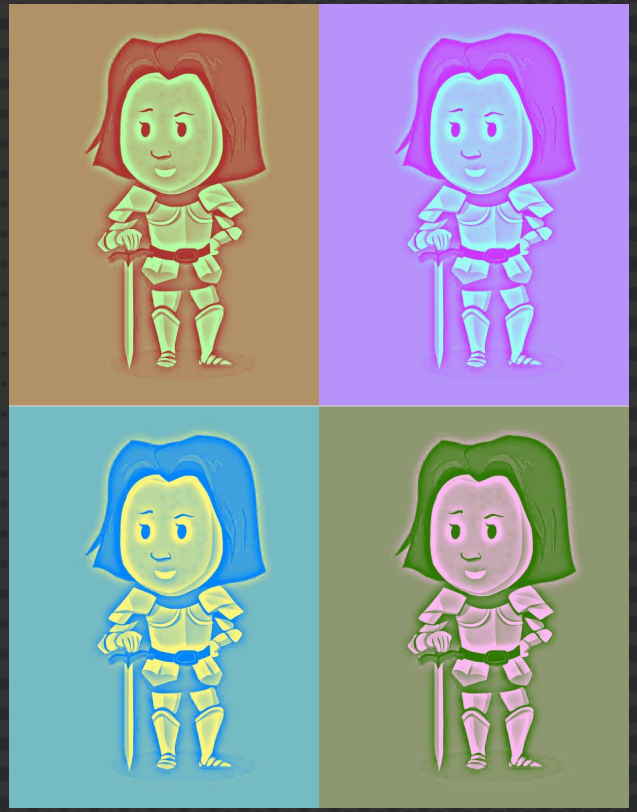
- Does the target language and framework version have any known security issues?
- Are configuration-controlled security headers implemented according to recommended best practices?

CONFIGURATION ANALYSIS

EXERCISE JOAN OF ARC

1. **skea_node and bhima**
   a. Build Config Checklist
   b. Run/review npm audit and nodejsscan

2. **skea_rails and railsgoat**
   a. Build Config Checklist
   b. Run/review brakeman



SECURITY MISCONFIGURATION - JAVA SPRING

```
# Database Configuration
spring.datasource.url=jdbc:h2:mem:AZ;DB_CLOSE_DELAY=-1;DB_CLOSE_ON_EXIT=FALSE
spring.datasource.driverClassName=org.h2.Driver
spring.datasource.username=sa
spring.datasource.password=
spring.jpa.database-platform=org.hibernate.dialect.H2Dialect
hibernate.hbm2ddl.import_files_sql_extractor=org.hibernate.tool.hbm2ddl.MultipleLinesSqlCommandExtractor
hibernate.hbm2ddl.auto=create

# H2 Options
security.basic.enabled=true
security.basic.authorize-mode=none
spring.h2.console.enabled=true
spring.h2.console.settings.web-allow-others=true
spring.h2.console.path=/console
```

SECURITY MISCONFIGURATION - .NET

```
<sessionState mode="Off"
stateConnectionString="tcpip=localhost:42424"
sqlConnectionString="data source=localhost;user
id=sa;password=" cookieless="false" timeout="20"/>
```

ADDITIONAL RESOURCES

ADDITIONAL RESOURCES

- OWASP Code Review Guide - Includes some language-specific best practices for Java, .Net, C, C++.
- Simplicable Secure Code Review Checklist
- Infosec Institute - Secure Code Review: A Practical Approach
- OWASP Input Validation Cheatsheet
- OWASP XSS Prevention Cheatsheet
- Recommended headers for internal and external Web User Interfaces
- Wikipedia - Principle of Layered Security
- Wikipedia - Principle of Least Privilege
- OWASP ASVS (Application Security Verification Standard)

REPORTING & RETESTING

REPORTING & RETESTING

- This phase of the methodology is critical.
- Document findings in a manner that can be understood by a developer.
- Review the source after remediation using the same techniques (rinse & repeat).
- **THIS IS THE WHOLE POINT.**

Report Writing (or Ticket Creation)

- Detailed findings include:
  - Description
  - Applicable File, Function, Variables, Line Numbers
  - Risk Severity
  - Likelihood of Exploitation
  - Ease of Exploitation
  - Remediation Approach
  - References

Walkthrough:
Vulnerable Task Manager

GROUP PROJECTS


THANK YOU!!!

CONTACT

ABSOLUTE APPSEC - ABSOLUTEAPPSEC.COM
@ABSOLUTEAPPSEC
KEN - @CKTRICKY - KEN@ABSOLUTEAPPSEC.COM
SETH - @SETHLAW - SETH@ABSOLUTEAPPSEC.COM