OWASP
Open Web Application
Security Project

The White Hat's Advantage: Open-source OWASP tools to aid in penetration testing coverage

Ken Prole

October 25, 2018

About me

Ken Prole

CTO, Code Dx
Principal Investigator, Secure Decisions

- Project lead for Code Pulse and Attack Surface Detector (ASD)
- 20+ years of software development experience
- Passionate about helping organizations build more secure software

Applied Visions, Inc.

- Software development since 1987
- Primarily develops business applications

dba, Secure Decisions

- Cyber R&D, focusing on application security
- Primarily serving DHS and DoD,
  some intelligence and commercial projects

Code Dx, Inc.

- Spin-out to commercialize DHS-funded AppSec R&D

Outline of today’s talk

Overview

- Summary of tools
- The White Hat’s advantage
- Typical penetration testing workflow
- The importance of understanding the attack surface

OWASP Code Pulse

- Challenges addressed, how it works, demo

OWASP Attack Surface Detector (ASD)

- Challenges addressed, how it works, demo

Wrap-up

- Where to learn more
- Q&A

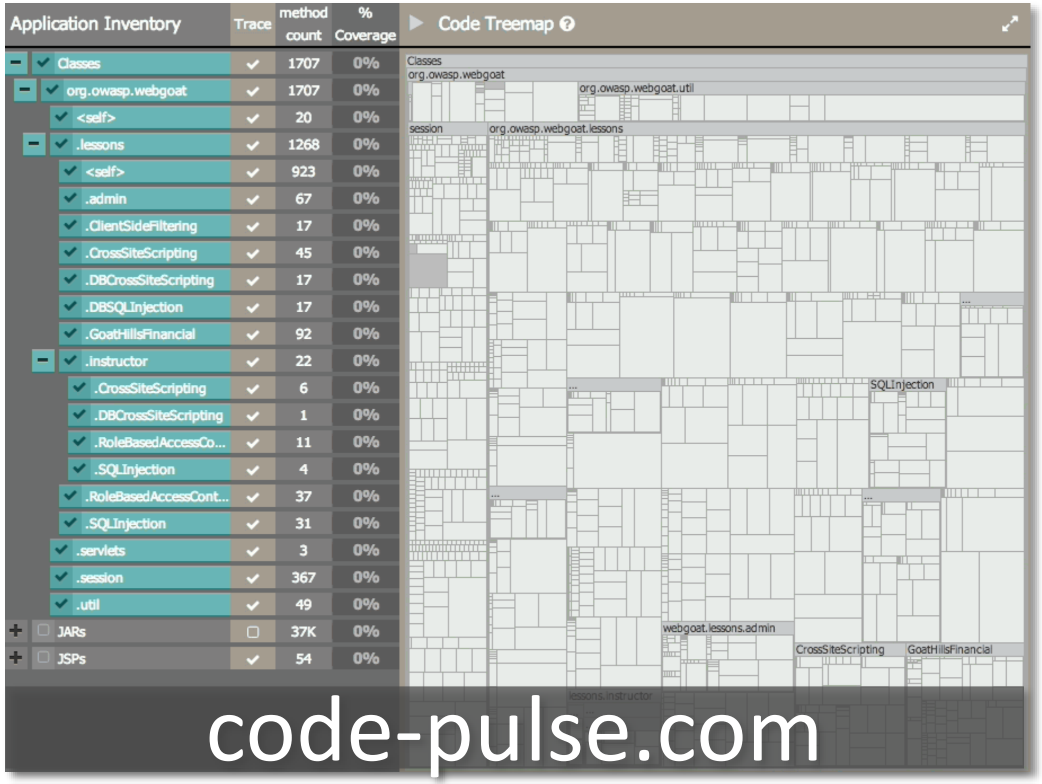
Making black box testing less opaque

Overview

Overview of tools; pen-testing workflow; understanding application attack surface

OWASP Code Pulse

Provides insight into the real-time code coverage of black box testing activities by monitoring the execution of the web application.

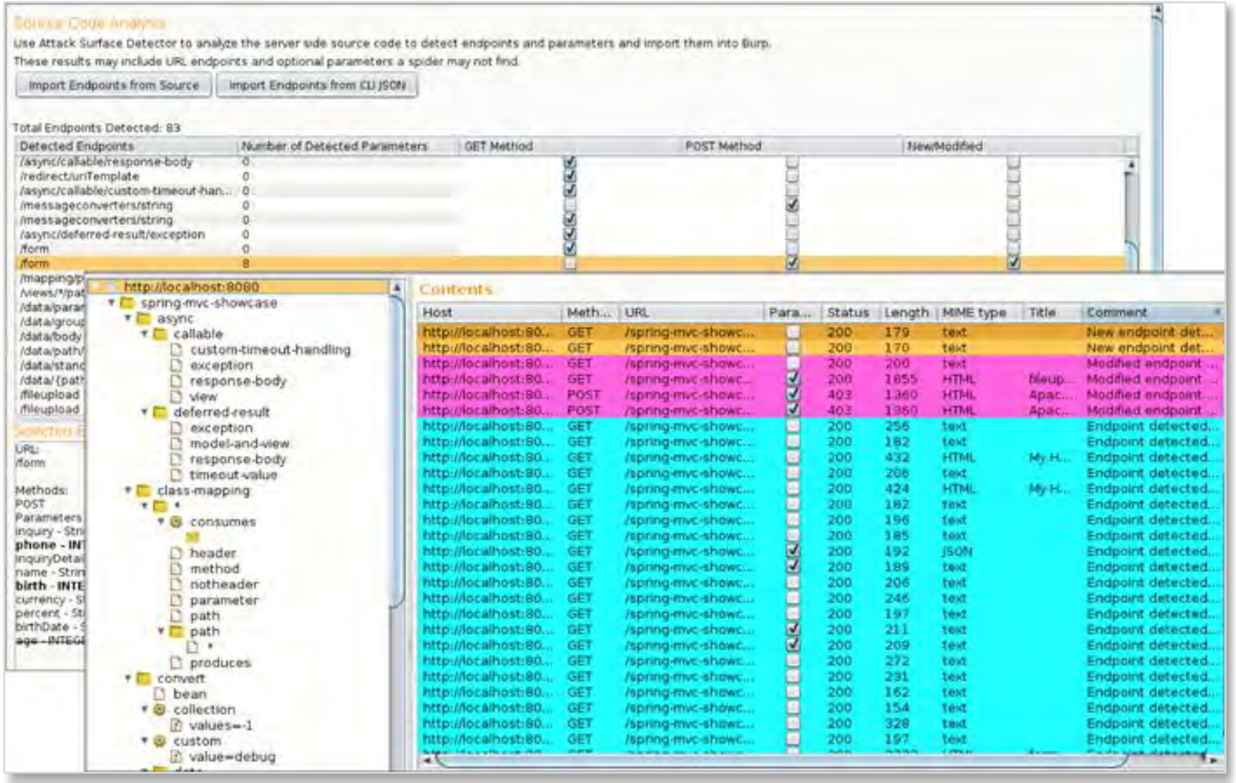


Application Inventory	Trace	method count	% Coverage
− ☑ Classes	✓	1707	0%
− ☑ org.owasp.webgoat	✓	1707	0%
☑ <self>	✓	20	0%
− ☑ .lessons	✓	1268	0%
☑ <self>	✓	923	0%
☑ .admin	✓	67	0%
☑ .ClientSideFiltering	✓	17	0%
☑ .CrossSiteScripting	✓	45	0%
☑ .DBCrossSiteScripting	✓	17	0%
☑ .DBSQLInjection	✓	17	0%
☑ .GoatHillsFinancial	✓	92	0%
− ☑ .instructor	✓	22	0%
☑ .CrossSiteScripting	✓	6	0%
☑ .DBCrossSiteScripting	✓	1	0%
☑ .RoleBasedAccessCo...	✓	11	0%
☑ .SQLInjection	✓	4	0%
☑ .RoleBasedAccessCont...	✓	37	0%
☑ .SQLInjection	✓	31	0%
☑ .servlets	✓	3	0%
☑ .session	✓	367	0%
☑ .util	✓	49	0%
+ □ JARs	□	37K	0%
+ □ JSPs	✓	54	0%

code-pulse.com

Attack Surface Detector

Provides a complete picture of a web application's exposed *attack surface*. Output used to "pre-seed" ZAP and Burp Suite for more thorough pen testing.



Source Code Analysis

Use Attack Surface Detector to analyze the server side source code to detect endpoints and parameters and import them into Burp.
These results may include URL endpoints and optional parameters a spider may not find.

Total Endpoints Detected: 83

Detected Endpoints	Number of Detected Parameters	GET Method	POST Method	New/Modified
/async/callable/response-body	0	☑	□	□
/redirect/uriTemplate	0	☑	□	□
/async/callable/custom-timeout-han...	0	☑	□	□
/messageconverters/string	0	□	☑	□
/messageconverters/string	0	☑	□	□
/async/deferred-result/exception	0	☑	□	□
/form	0	☑	□	□
/form	8	□	☑	☑
/mapping/p				
/views/*/pa				
/data/para				
/data/grou				
/data/body				
/data/path/				
/data/stanc				
/data/{pat				
/fileupload				
/fileupload				

URL:
/form

Methods:
POST
Parameters
inquiry - Str
phone - INT
inquiryDetai
name - Strin
birth - INTE
currency - S
percent - St
birthDate - S
~~age - INTEGE~~

```
http://localhost:8080
  spring-mvc-showcase
    async
      callable
        custom-timeout-handling
        exception
        response-body
        view
      deferred-result
        exception
        model-and-view
        response-body
        timeout-value
    class-mapping
      *
        consumes
        header
        method
        notheader
        parameter
        path
        path
          *
        produces
    convert
      bean
      collection
        values=-1
      custom
        value=debug
```

Contents

Host	Meth...	URL	Para...	Status	Length	MIME type	Title	Comment
http://localhost:80...	GET	/spring-mvc-showc...	□	200	179	text		New endpoint det...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	170	text		New endpoint det...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	200	text		Modified endpoint ...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	1855	HTML	fileup...	Modified endpoint ...
http://localhost:80...	POST	/spring-mvc-showc...	☑	403	1360	HTML	Apac...	Modified endpoint ...
http://localhost:80...	POST	/spring-mvc-showc...	☑	403	1360	HTML	Apac...	Modified endpoint ...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	256	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	182	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	432	HTML	My H...	Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	206	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	424	HTML	My H...	Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	182	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	196	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	185	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	192	JSON		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	189	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	206	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	246	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	197	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	211	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	209	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	272	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	231	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	162	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	154	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	328	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	197	text		Endpoint detected...

The White Hat advantage

White Hats have plenty of disadvantages over their malicious counterparts

- Huge task of securing web app against *all* vulnerabilities
- Very limited time
- Hard to lock-step with dev team

There are a few advantages we can leverage with better penetration testing tools:

- Access to server binaries/bytecode
- Access to server-side source code

Breakers

Ethical Hackers

White Hat Pen Testers

OWASP

Zed Attack Proxy
(ZAP)

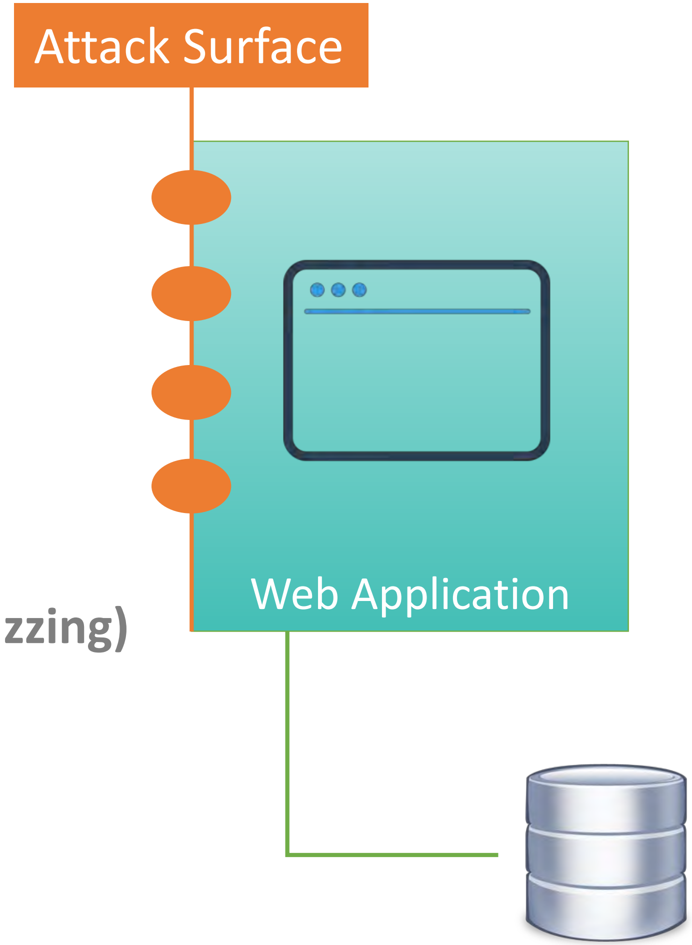
BURPSUITE

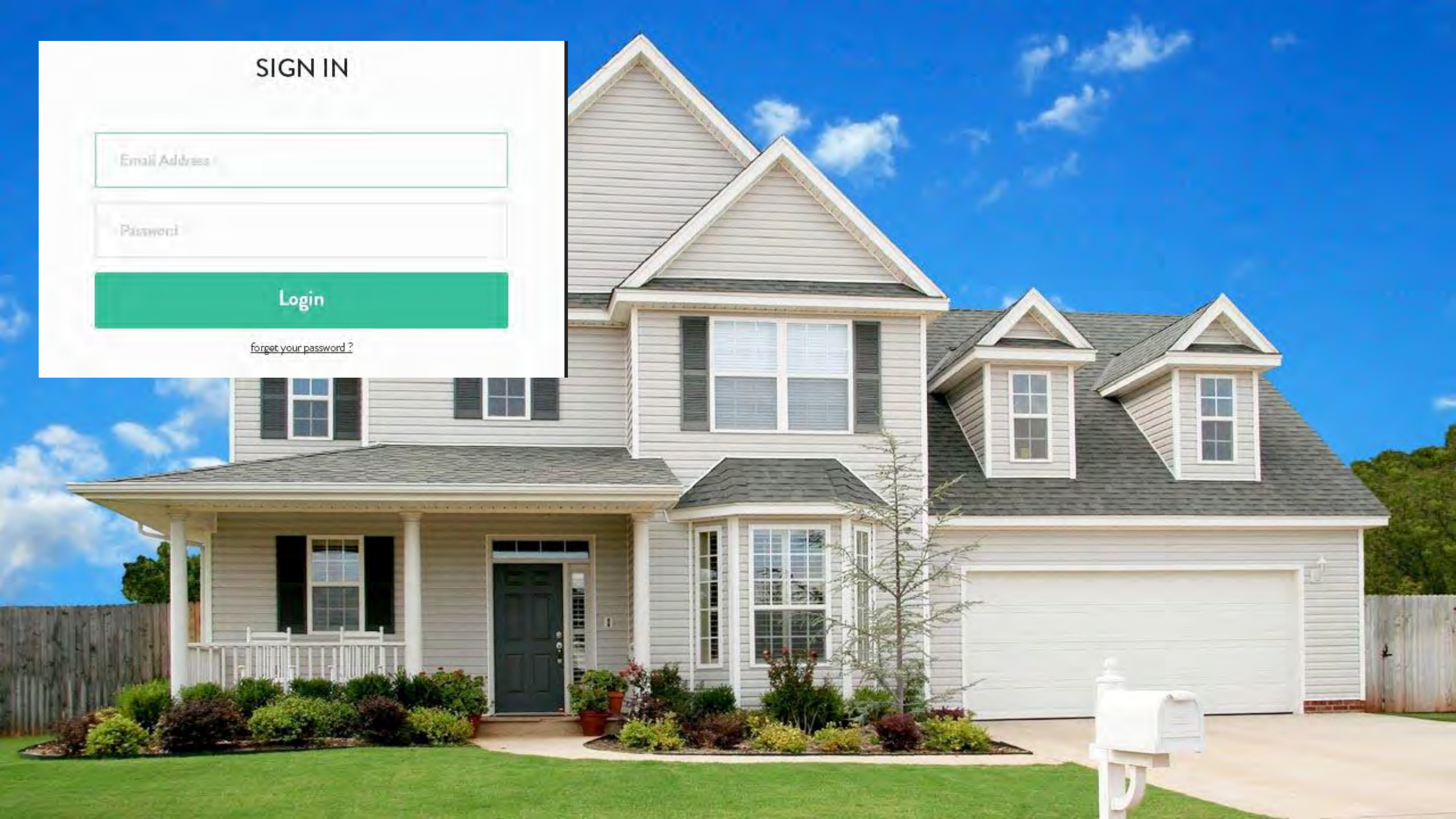
PROFESSIONAL

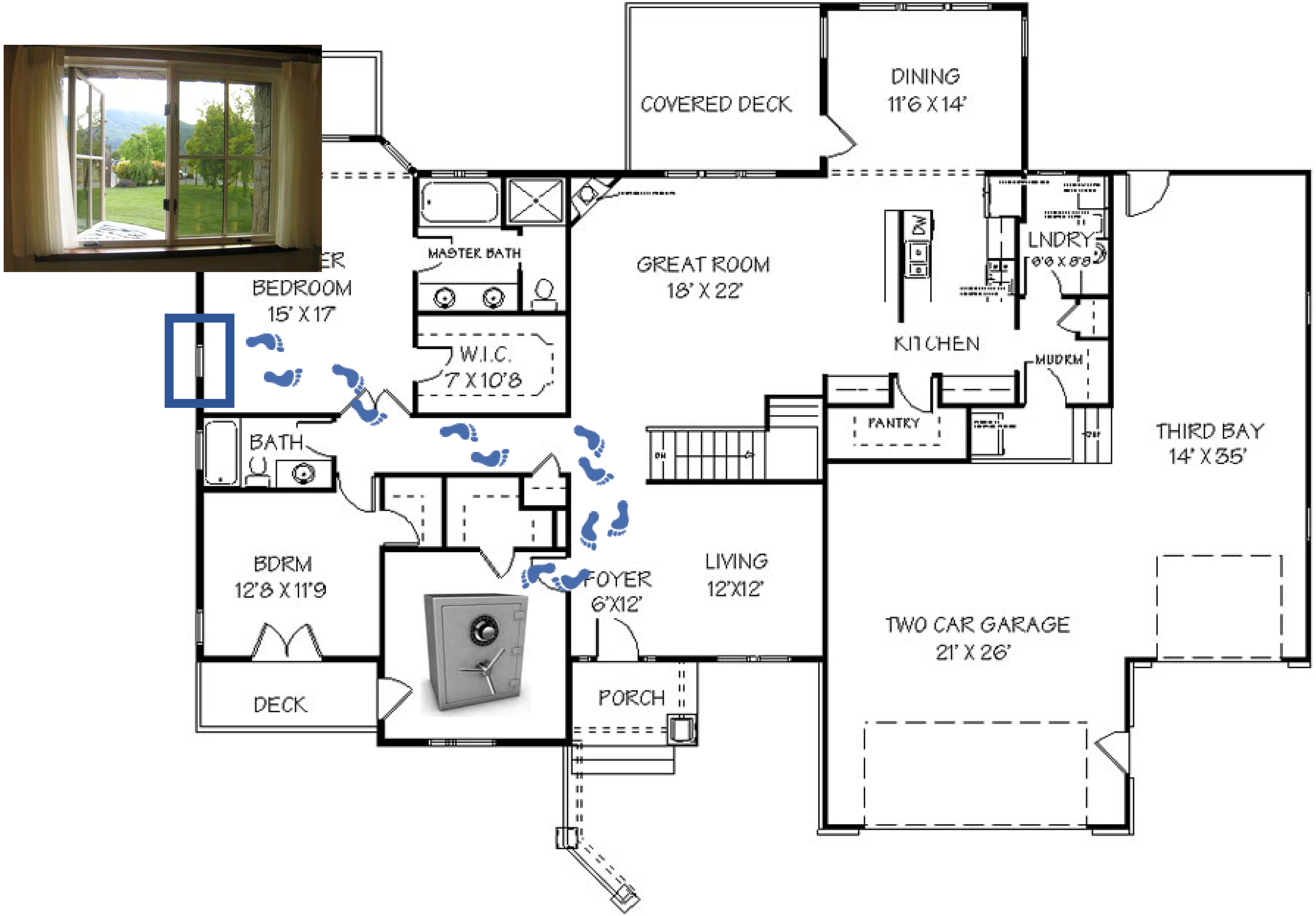
Typical penetration testing workflow

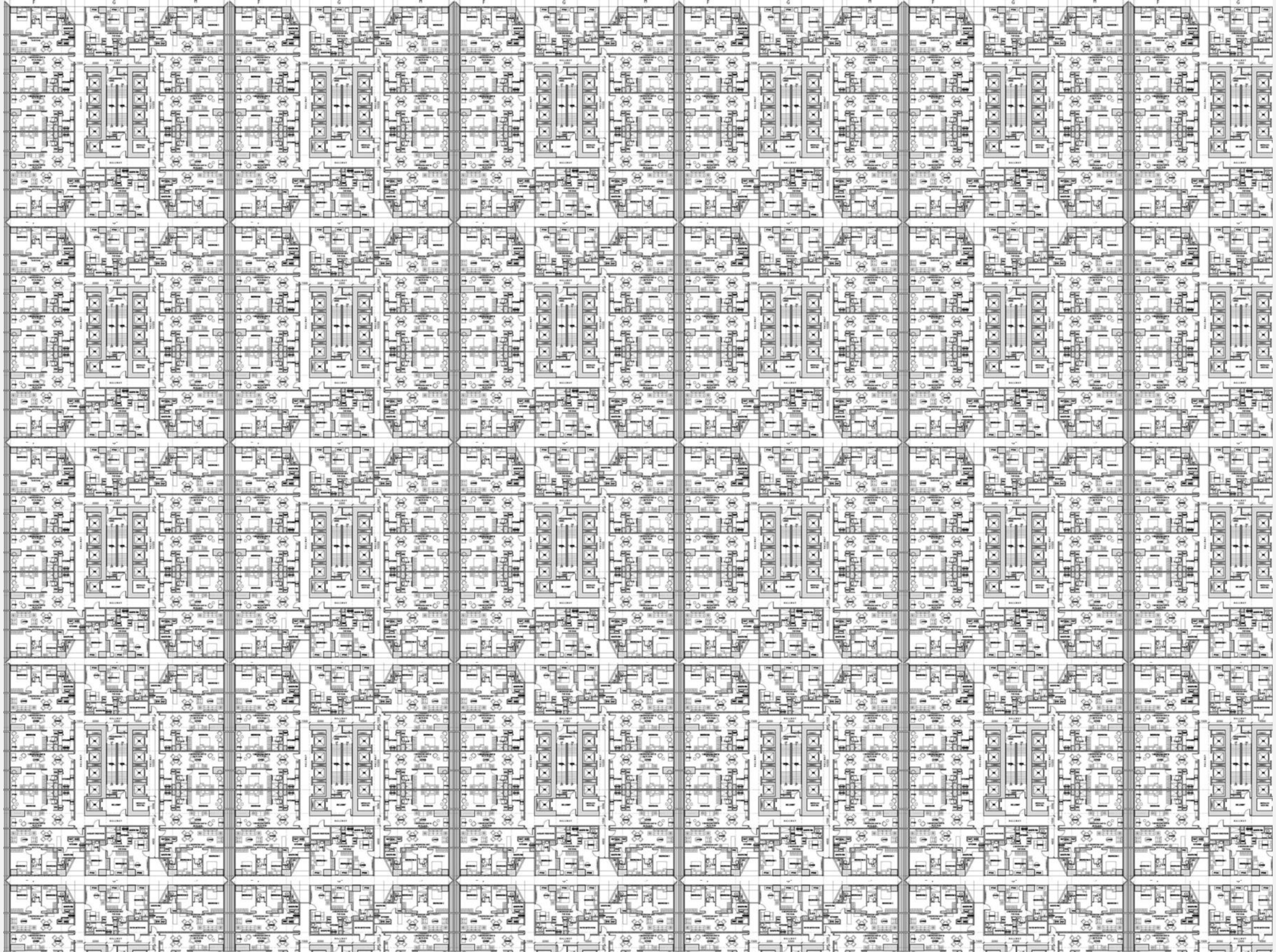
Penetration Tester

1. Authenticate with different user roles
2. Endpoint enumeration
   - → Manually map out the application
   - → Automated spider/crawler
   - → Brute force/forced browsing
3. Vulnerability discovery (passive, active, fuzzing)




SIGN IN
Email Address
Password
Login
forget your password ?


COVERED DECK
DINING
11'6 X 14'
ER
BEDROOM
15' X 17
MASTER BATH
W.I.C.
7 X 10'8
GREAT ROOM
18' X 22'
DW
KITCHEN
LNDRY
8'0 X 8'8
MUDRM
PANTRY
THIRD BAY
14' X 35'
BATH
BDRM
12'8 X 11'9
FOYER
6'X12'
LIVING
12'X12'
TWO CAR GARAGE
21' X 26'
DECK
PORCH


F
G
H
HALLWAY
LIVING

OWASP Code Pulse

A real-time code coverage visualization tool for penetration testing activities

“The penetration tester should look at the ***coverage*** of the web application or of its ***attack surface*** to know if the tool was configured correctly or was able to understand the web application.

Wikipedia, Web application security scanner

Penetration testing challenges addressed by Code Pulse

Did testing reach all parts of the application?

For actions just performed, which parts of the source code were executed?

Which tools are getting better coverage?

Which testers are getting better coverage?

How can I tune testing to get better coverage?

How can I communicate testing coverage?

Coverage gaps **Tuning** **Communication**

Code Pulse

Visual

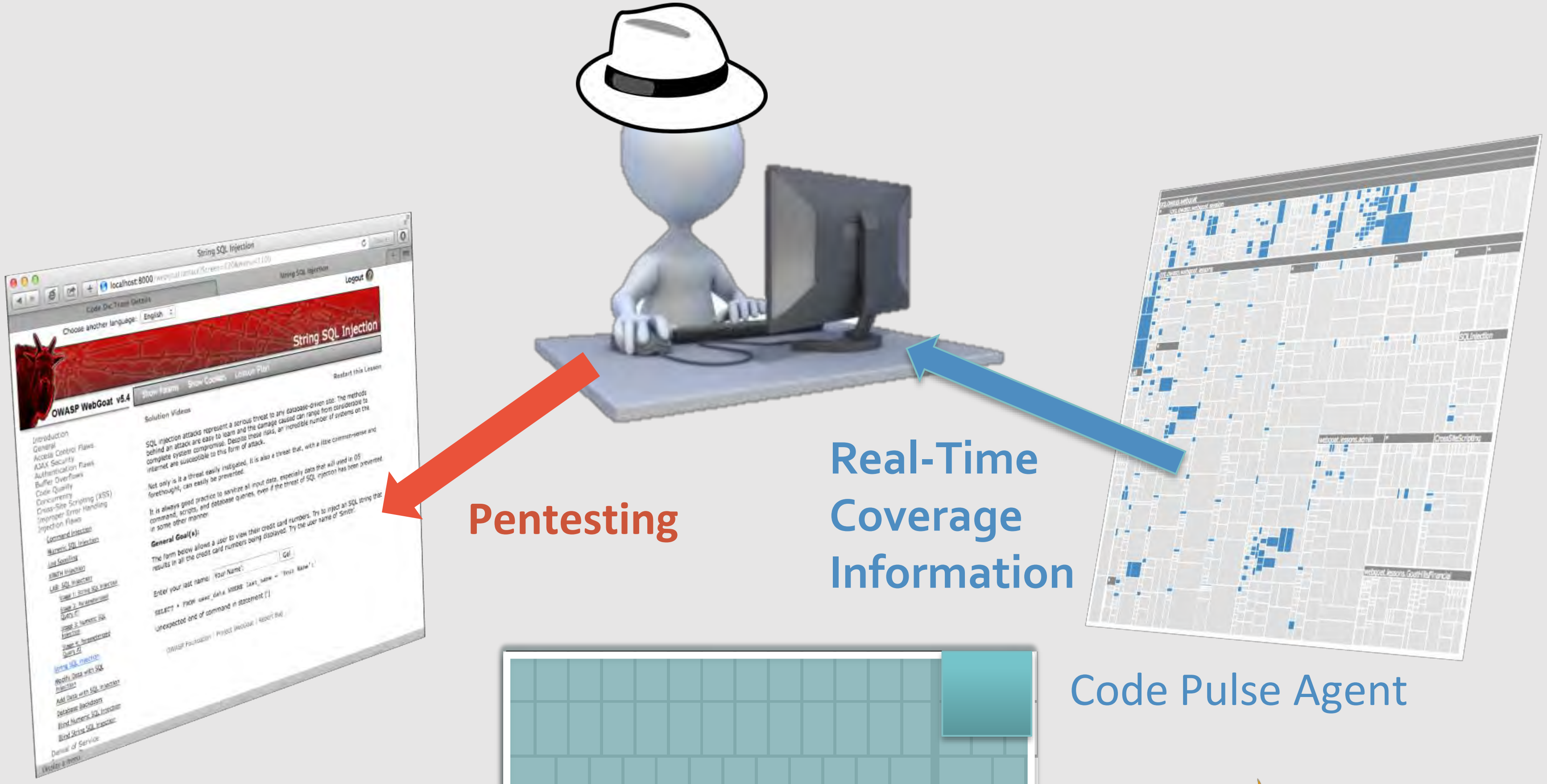
Real-Time

Code Coverage

for Penetration Testing
Activities

Code Pulse

Real-time code coverage visualization tool for penetration testing activities



String SQL Injection

localhost:8000

Choose another language: English

OWASP WebGoat v5.4

String SQL Injection

Logout

Restart this Lesson

Solution Videos

SQL injection attacks represent a serious threat to any database-driven site. The methods behind an attack are easy to learn and the damage caused can range from considerable to complete system compromise. Despite these risks, an incredible number of systems on the internet are susceptible to this form of attack.

Not only is it a threat easily instigated, it is also a threat that, with a little common-sense and forethought, can easily be prevented.

It is always good practice to sanitize all input data, especially data that will used in OS command, scripts, and database queries, even if the threat of SQL injection has been prevented in some other manner.

General Goal(s):

The form below allows a user to view their credit card numbers. Try to inject an SQL string that results in all the credit card numbers being displayed. Try the user name of 'Smith'.

Enter your last name: Your Name' Go!

```
SELECT * FROM user_data WHERE last_name = 'Your Name''
```

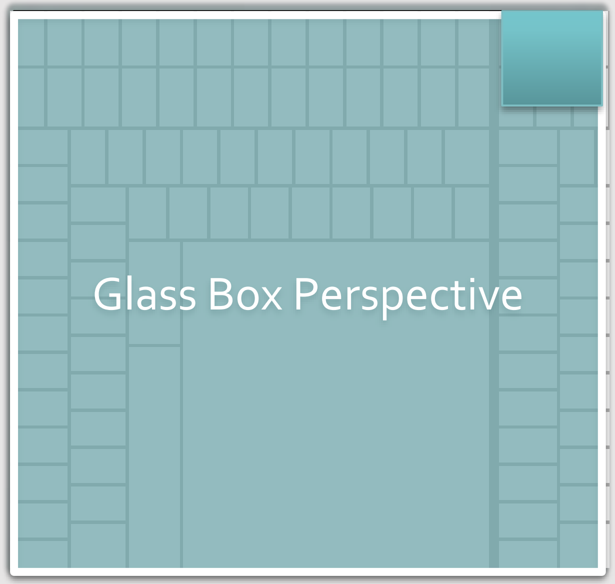
Unexpected end of command in statement [']

OWASP Foundation | Project WebGoat | Report Bug

Pentesting

Real-Time
Coverage
Information

Code Pulse Agent



Java

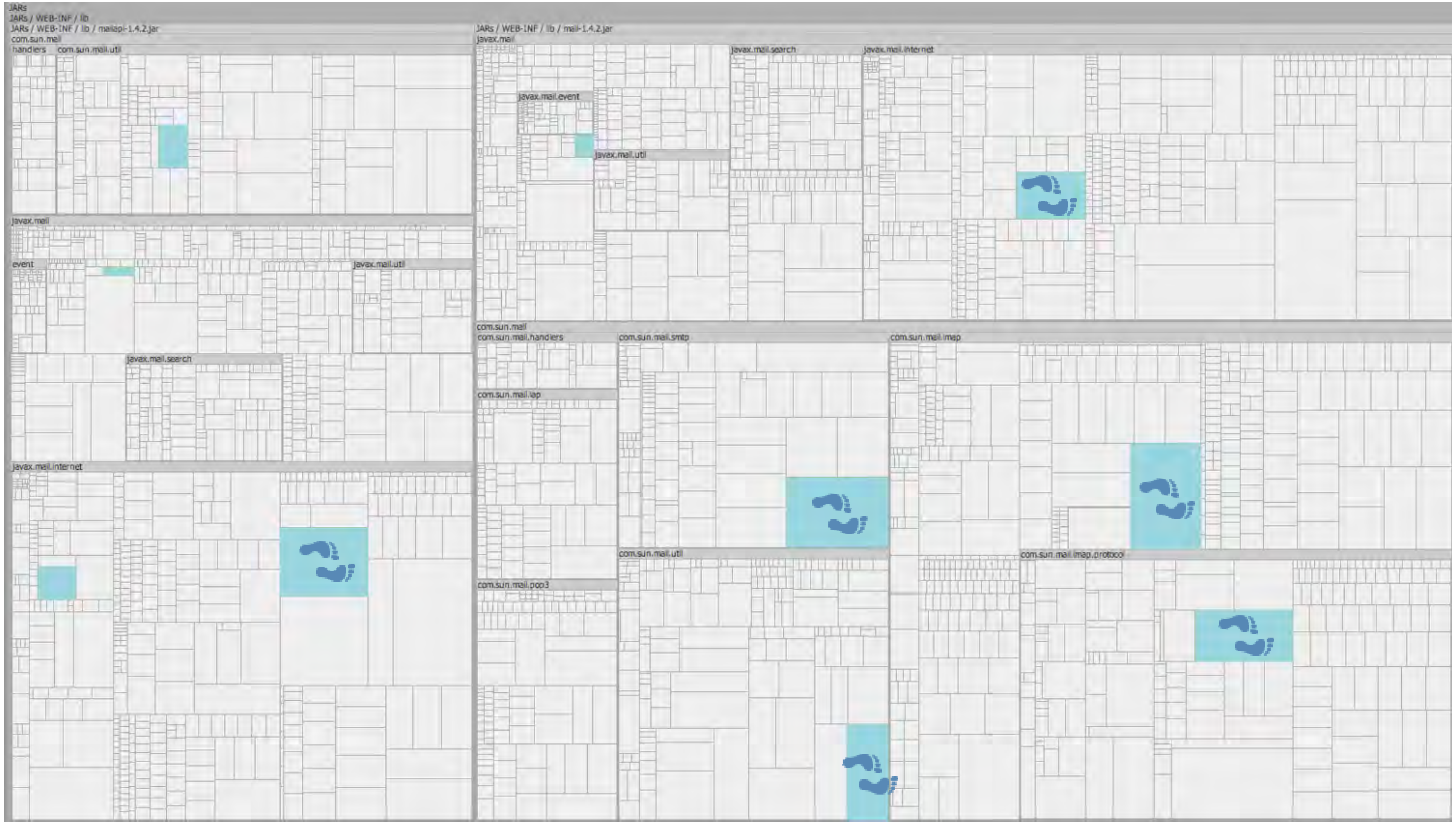
Microsoft
.NET

Transparency

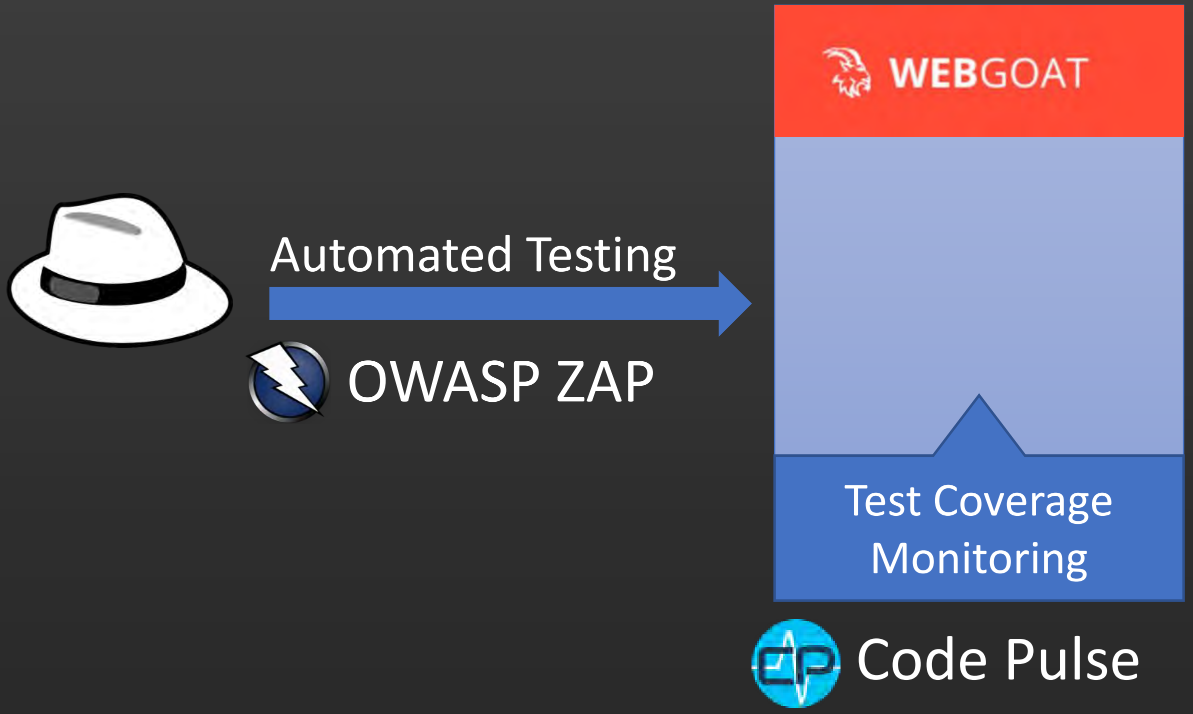
Feedback

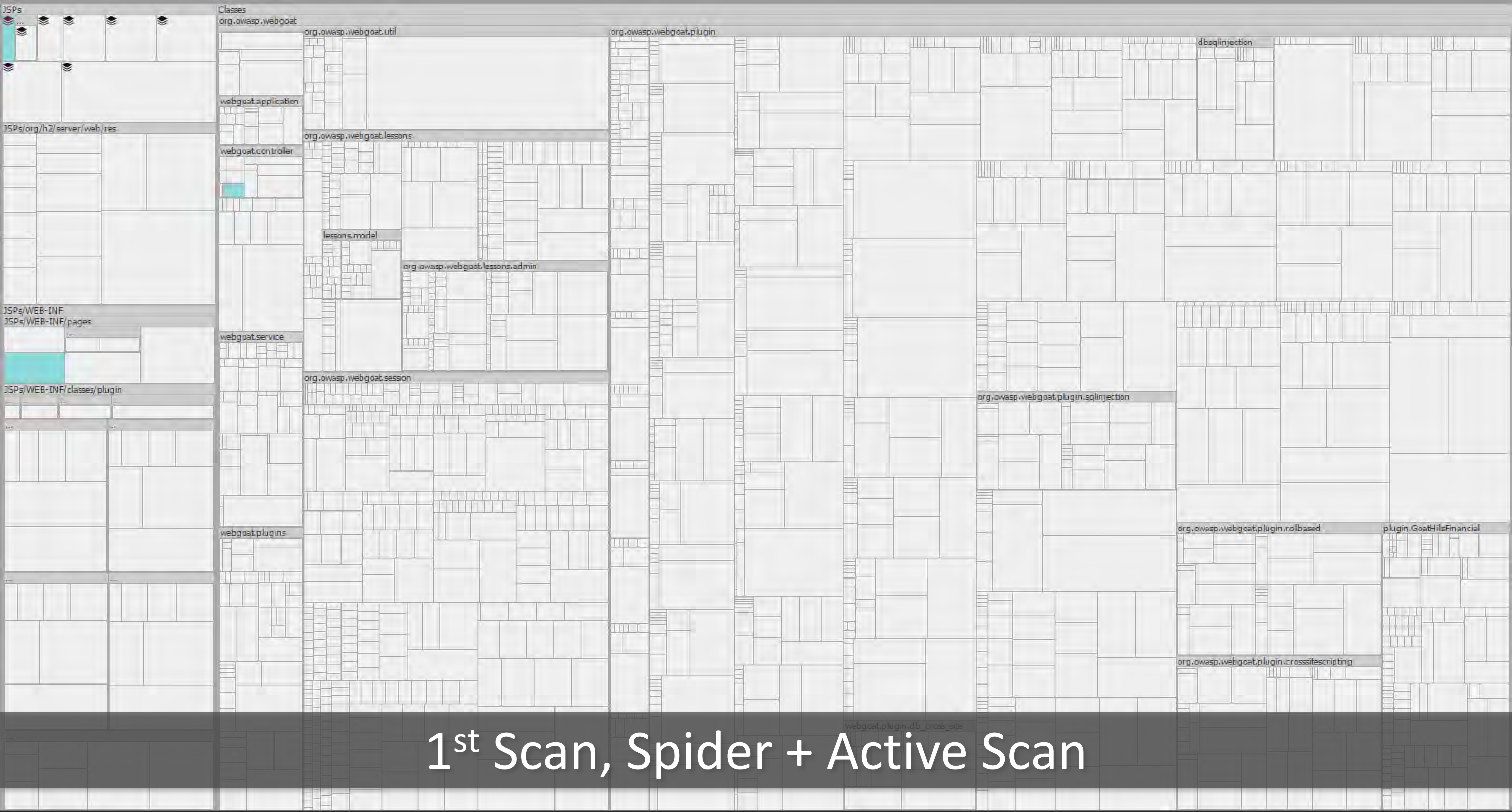
Tuning

Penetration Testing Coverage

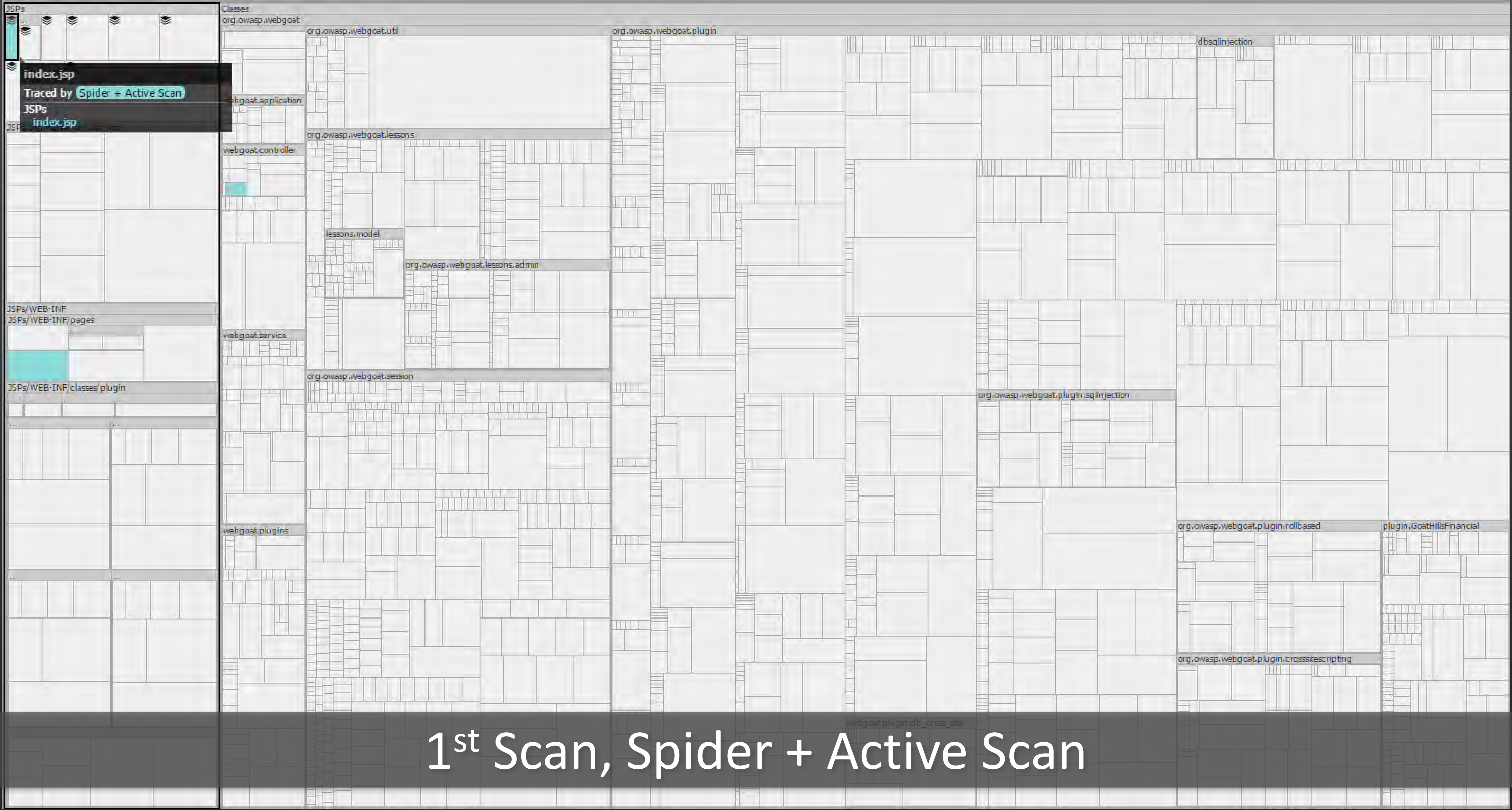


Coverage scenario



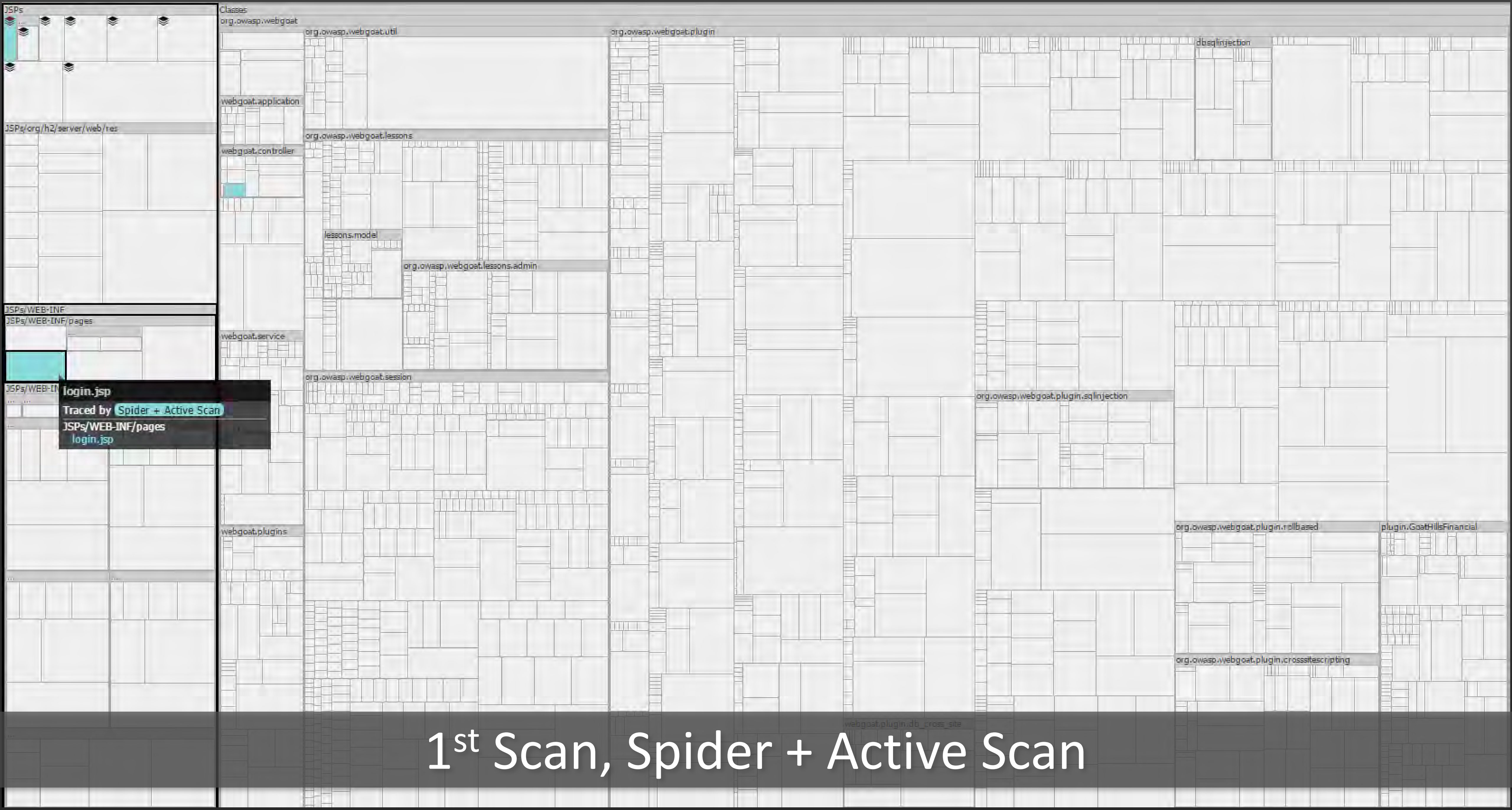

JSPs
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
org.owasp.webgoat.lessons
webgoat.controller
JSPs/org/h2/server/web/res
lessons.model
org.owasp.webgoat.lessons.admin
JSPs/WEB-INF
JSPs/WEB-INF/pages
webgoat.service
org.owasp.webgoat.session
JSPs/WEB-INF/classes/plugin
org.owasp.webgoat.plugin.sqlinjection
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
webgoat.plugins
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

1st Scan, Spider + Active Scan


JSPs
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
org.owasp.webgoat.lessons
webgoat.controller
lessons.model
org.owasp.webgoat.lessons.admin
JSPs/WEB-INF
JSPs/WEB-INF/pages
webgoat.service
org.owasp.webgoat.session
JSPs/WEB-INF/classes/plugin
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

index.jsp
Traced by Spider + Active Scan
JSPs
index.jsp

1st Scan, Spider + Active Scan

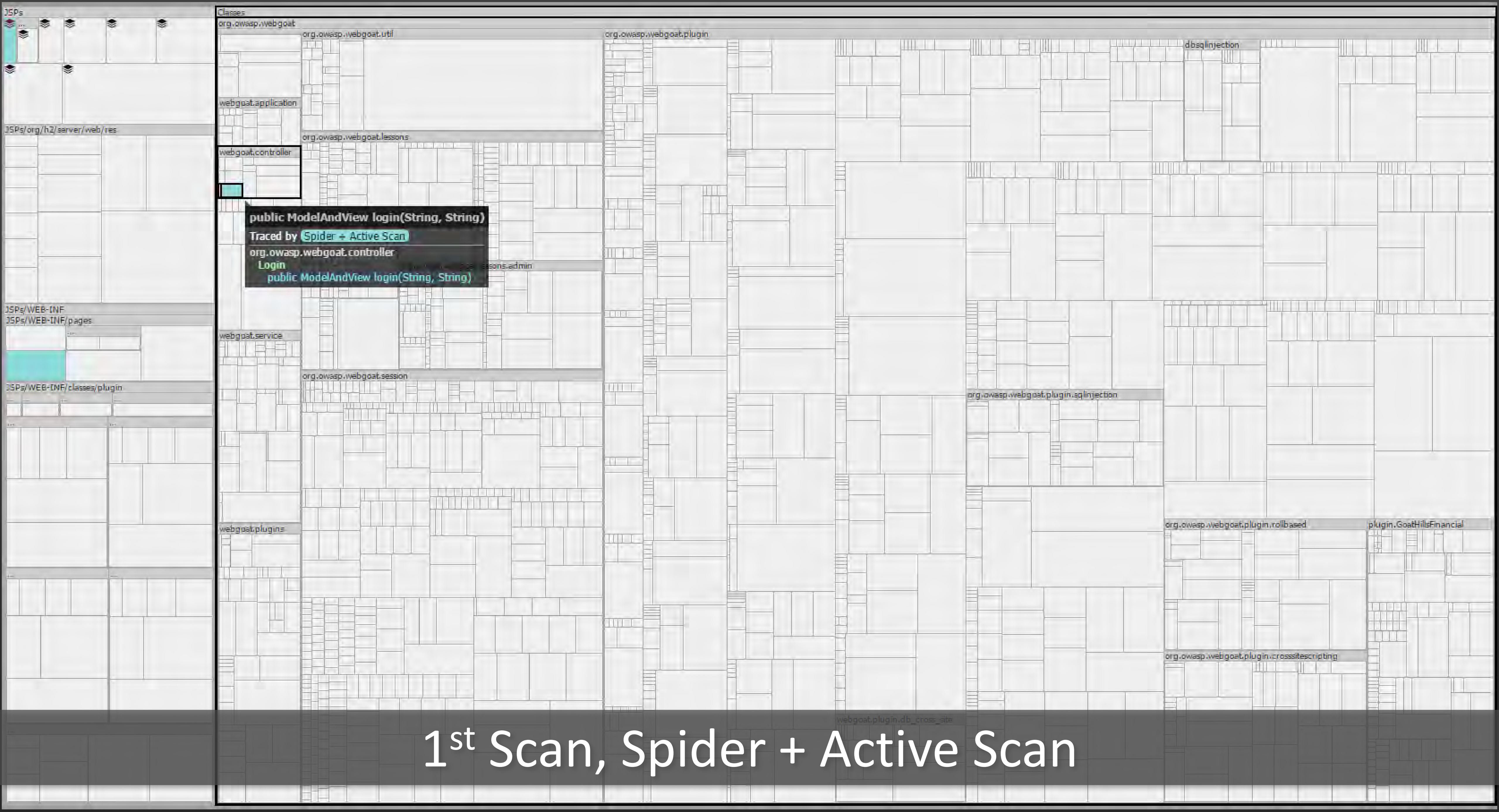

JSPs
JSPs/org/h2/server/web/res
JSPs/WEB-INF
JSPs/WEB-INF/pages
JSPs/WEB-IN
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
webgoat.controller
org.owasp.webgoat.lessons
lessons.model
org.owasp.webgoat.lessons.admin
webgoat.service
org.owasp.webgoat.session
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

login.jsp

Traced by Spider + Active Scan

JSPs/WEB-INF/pages
login.jsp

1st Scan, Spider + Active Scan

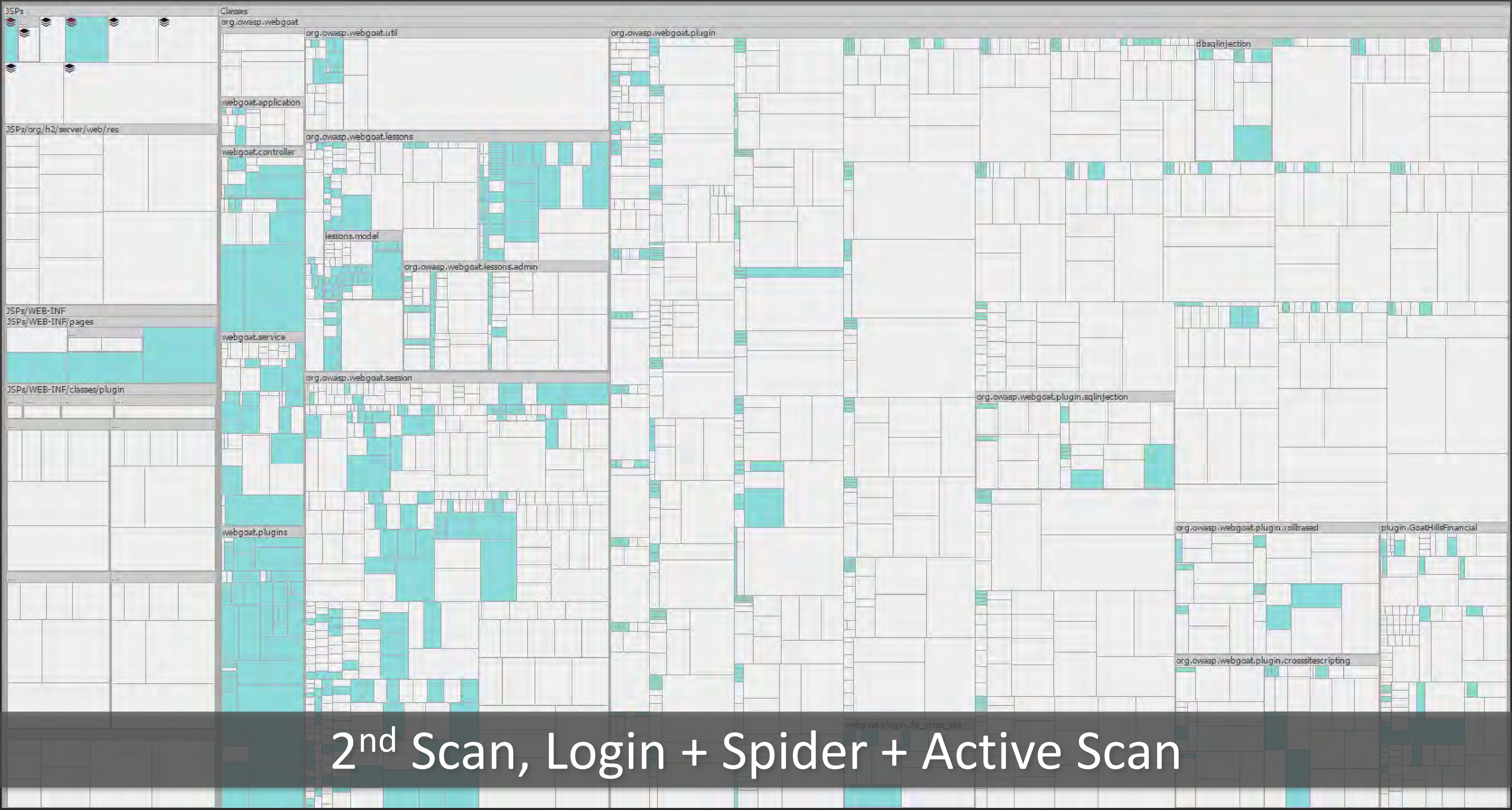

JSPs
JSPs/org/h2/server/web/res
JSPs/WEB-INF
JSPs/WEB-INF/pages
JSPs/WEB-INF/classes/plugin
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
org.owasp.webgoat.lessons
webgoat.controller
ssons.admin
webgoat.service
org.owasp.webgoat.session
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHilsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

public ModelAndView login(String, String)

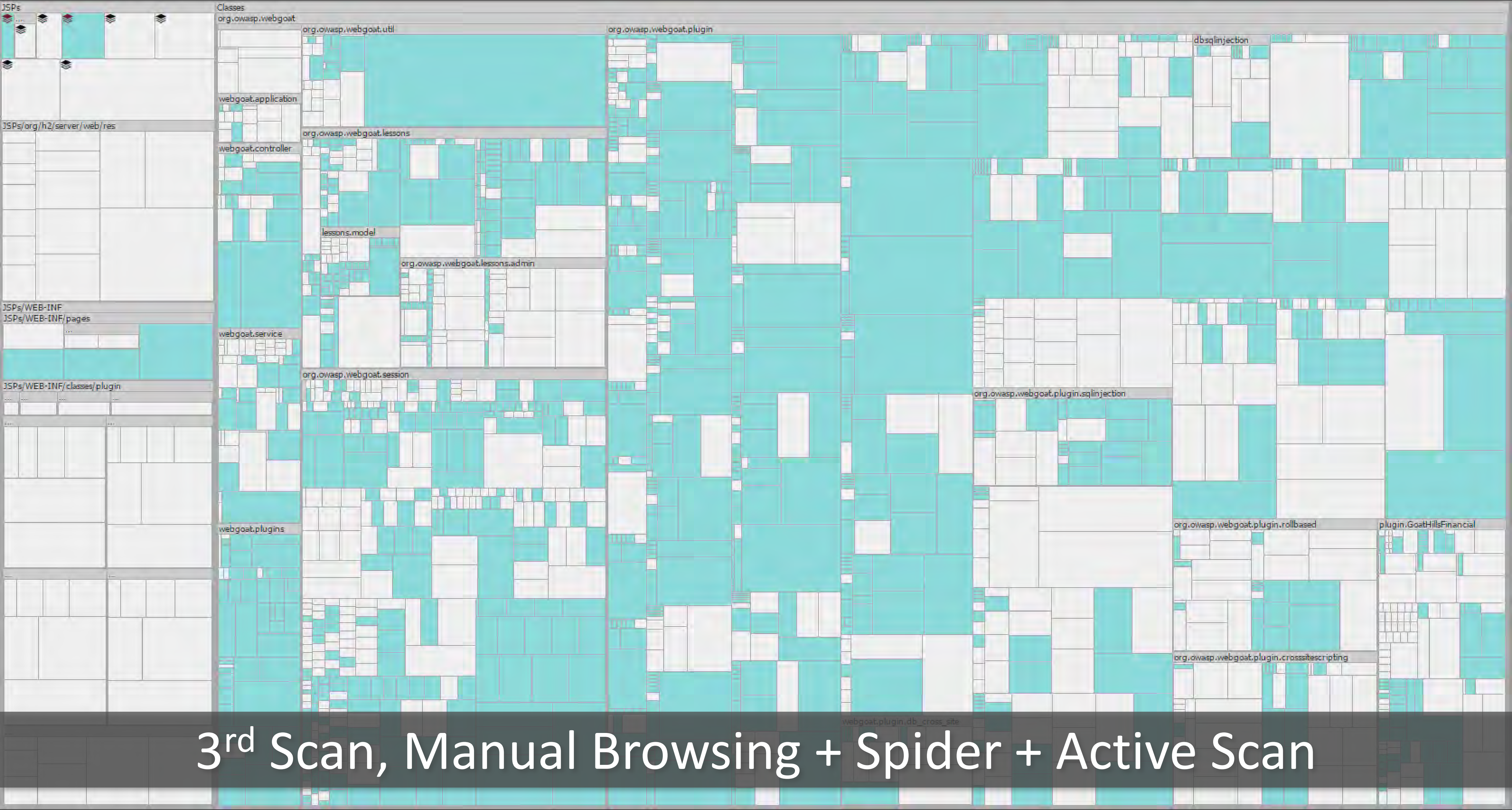
Traced by Spider + Active Scan

org.owasp.webgoat.controller
  Login
    public ModelAndView login(String, String)

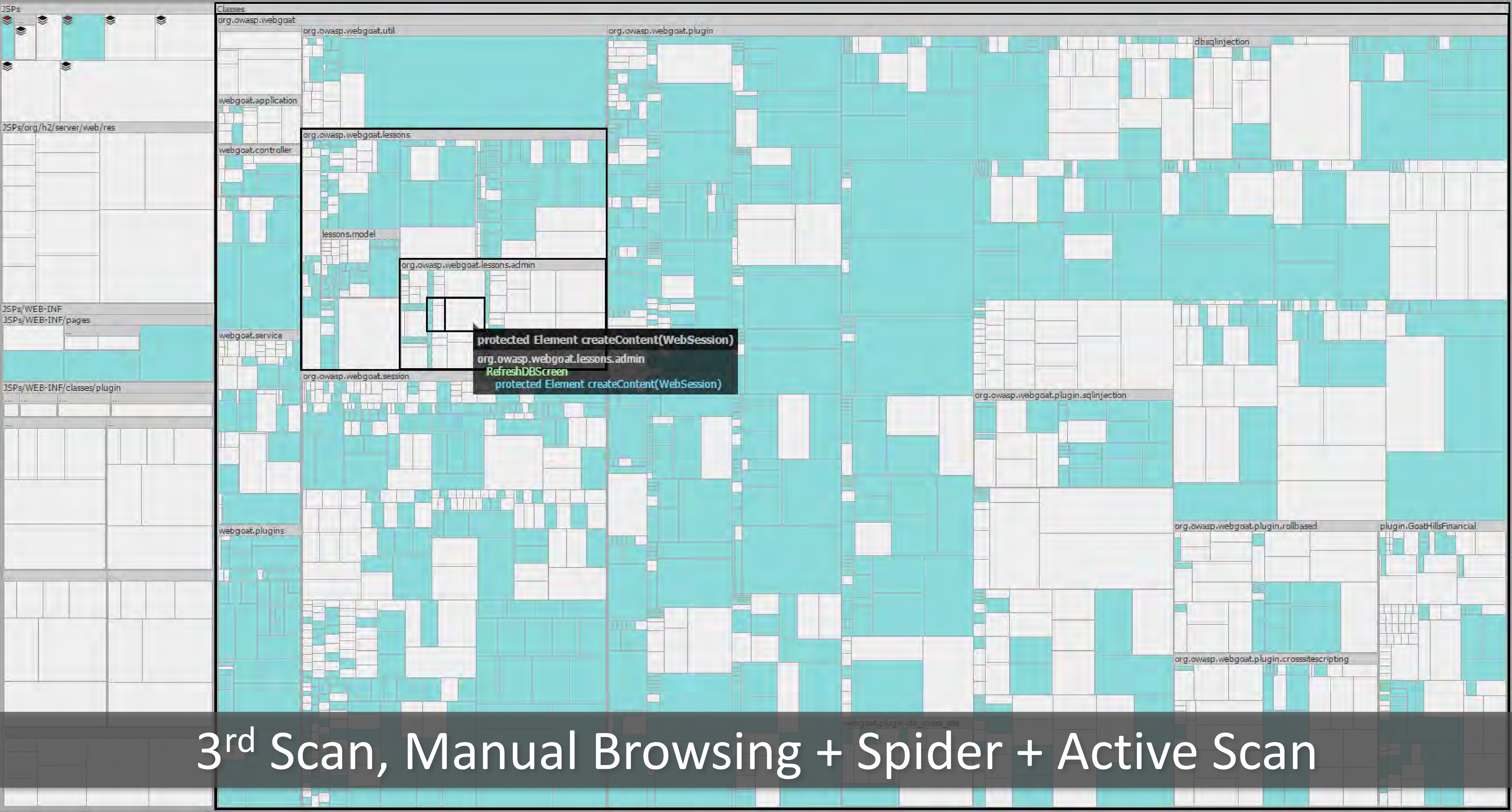
1st Scan, Spider + Active Scan


JSPs
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
JSPs/org/h2/server/web/res
webgoat.controller
org.owasp.webgoat.lessons
lessons.model
org.owasp.webgoat.lessons.admin
JSPs/WEB-INF
JSPs/WEB-INF/pages
webgoat.service
org.owasp.webgoat.session
JSPs/WEB-INF/classes/plugin
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

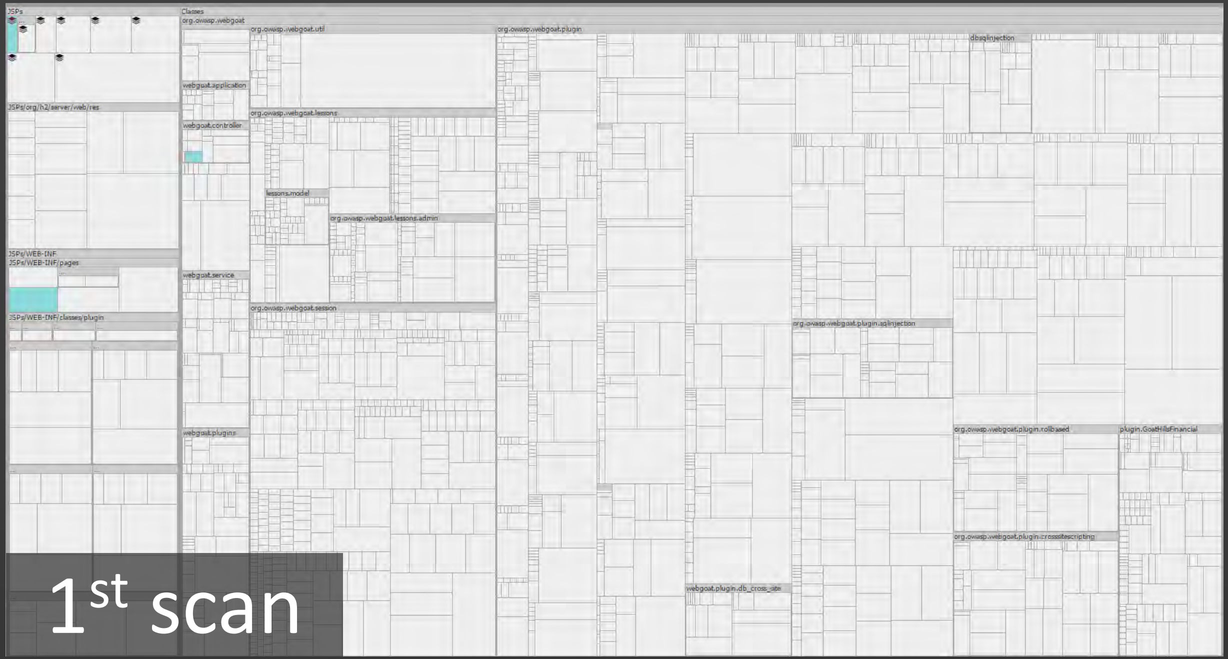
2nd Scan, Login + Spider + Active Scan


JSPs
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
JSPs/org/h2/server/web/res
org.owasp.webgoat.lessons
webgoat.controller
lessons.model
org.owasp.webgoat.lessons.admin
JSPs/WEB-INF
JSPs/WEB-INF/pages
webgoat.service
org.owasp.webgoat.session
JSPs/WEB-INF/classes/plugin
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

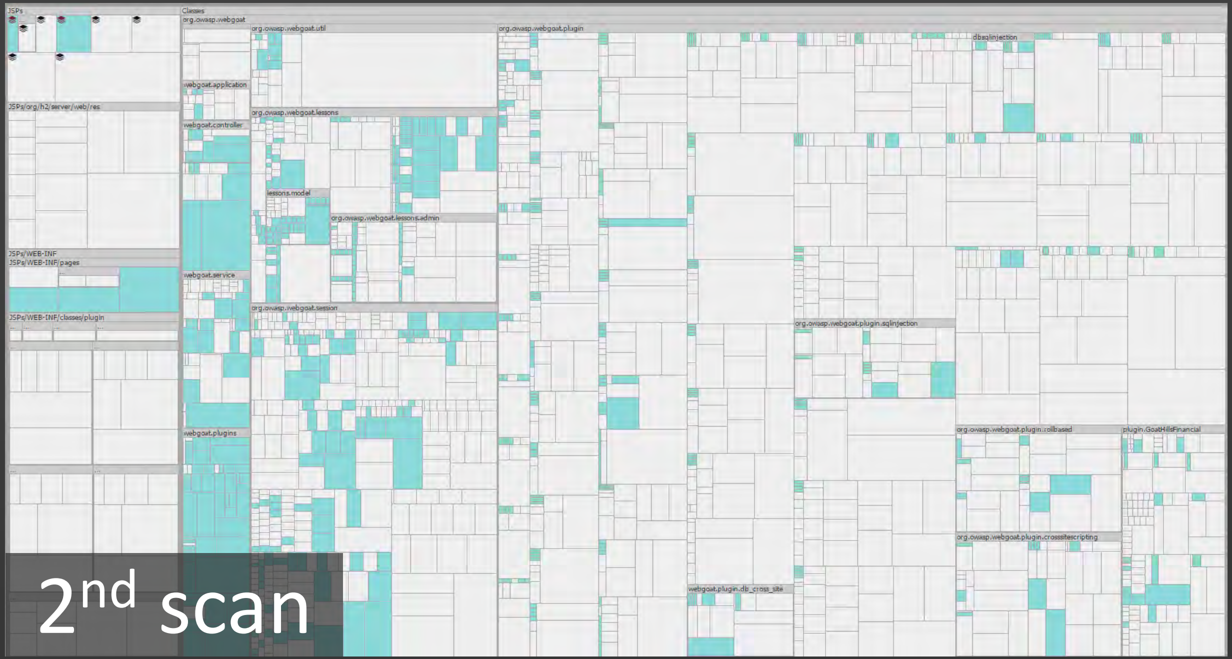
3rd Scan, Manual Browsing + Spider + Active Scan


JSPs
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
JSPs/org/h2/server/web/res
org.owasp.webgoat.lessons
webgoat.controller
lessons.model
org.owasp.webgoat.lessons.admin
JSPs/WEB-INF
JSPs/WEB-INF/pages
webgoat.service
protected Element createContent(WebSession)
org.owasp.webgoat.lessons.admin
RefreshDBScreen
protected Element createContent(WebSession)
org.owasp.webgoat.session
JSPs/WEB-INF/classes/plugin
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

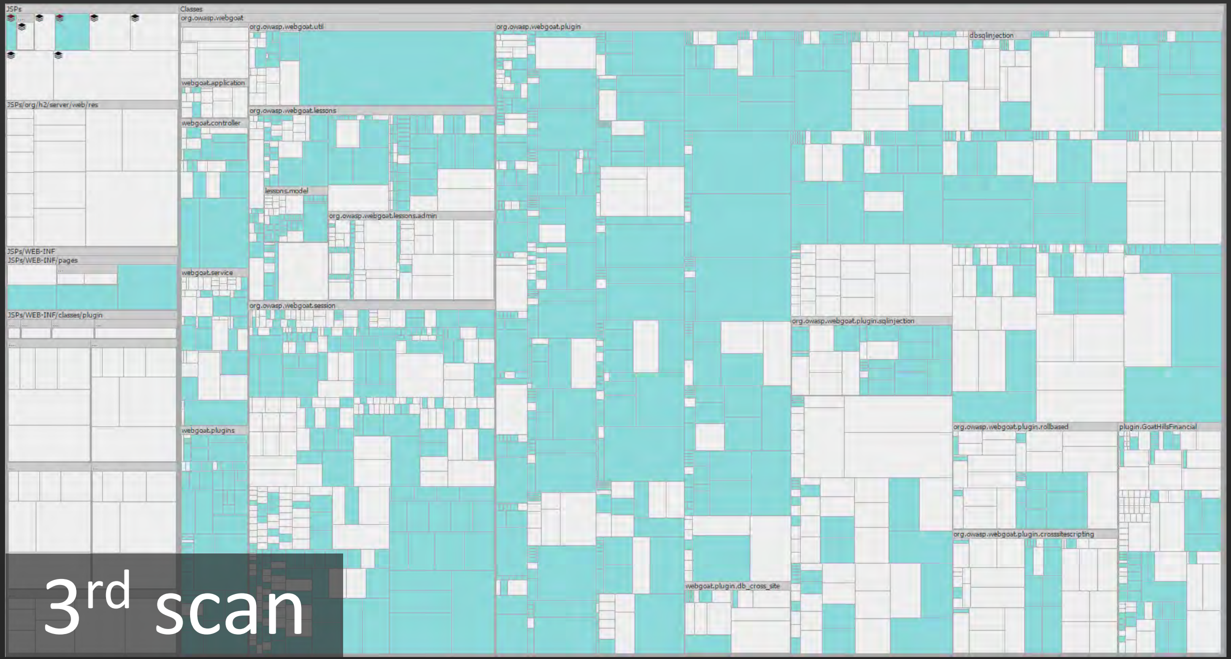
3rd Scan, Manual Browsing + Spider + Active Scan


JSPs
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
webgoat.controller
org.owasp.webgoat.lessons
lessons.model
org.owasp.webgoat.lessons.admin
JSPs/org/h2/server/web/res
JSPs/WEB-INF
JSPs/WEB-INF/pages
JSPs/WEB-INF/classes/plugin
webgoat.service
org.owasp.webgoat.session
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

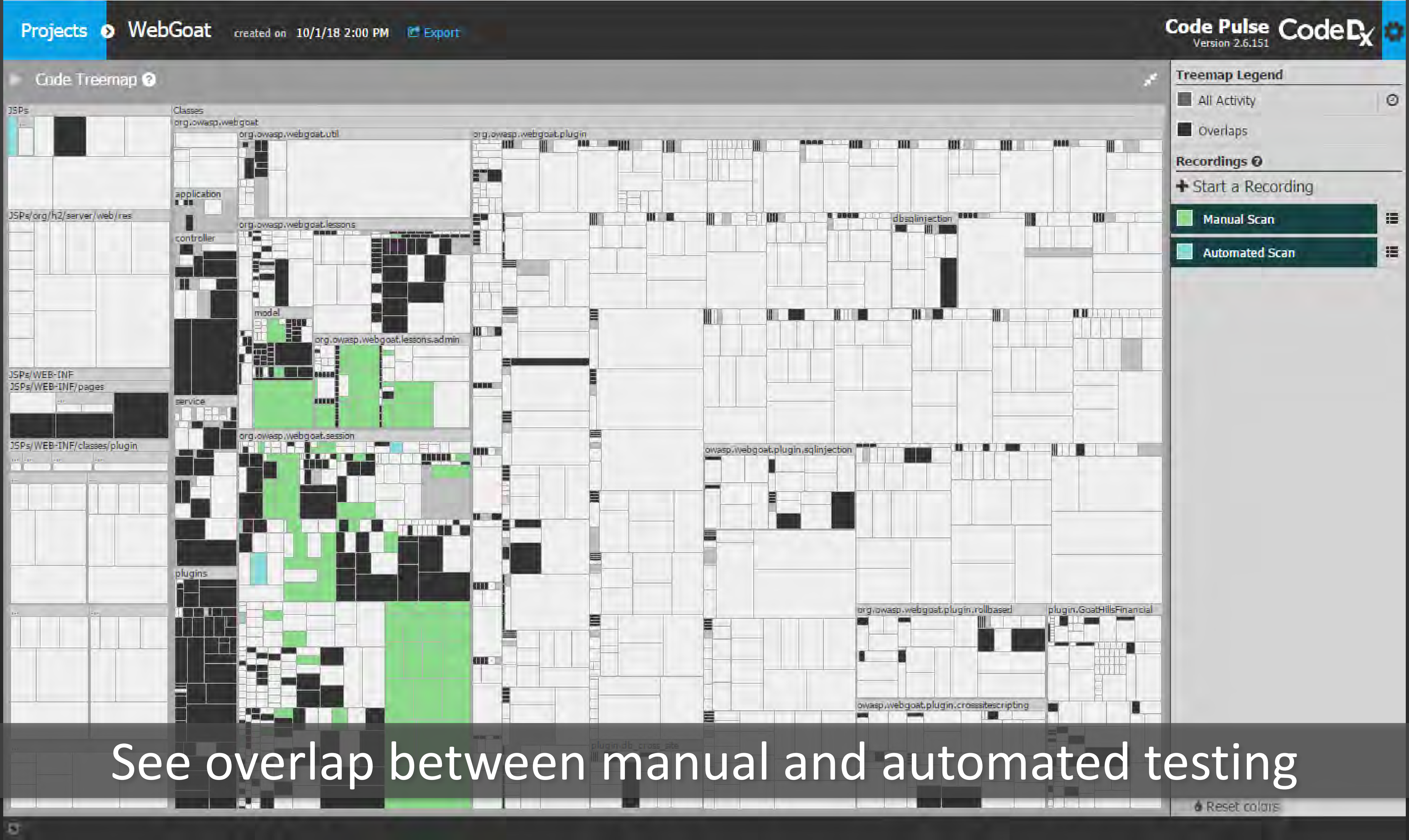
1st scan


JSPs
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
webgoat.controller
org.owasp.webgoat.lessons
lessons.model
org.owasp.webgoat.lessons.admin
JSPs/org/h2/server/web/res
JSPs/WEB-INF
JSPs/WEB-INF/pages
JSPs/WEB-INF/classes/plugin
webgoat.service
org.owasp.webgoat.session
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

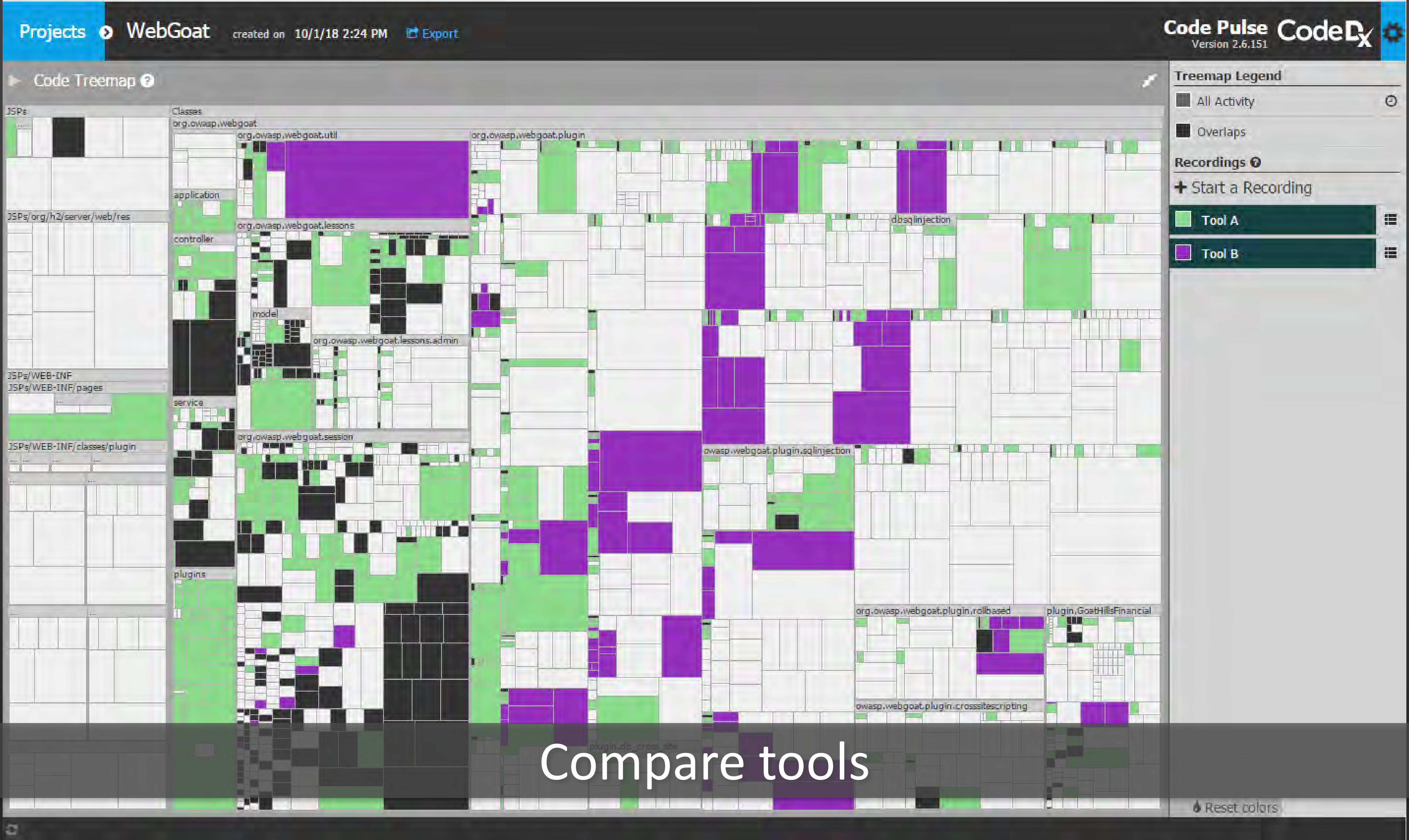
2nd scan


JSPs
Classes
org.owasp.webgoat
org.owasp.webgoat.util
org.owasp.webgoat.plugin
dbsqlinjection
webgoat.application
webgoat.controller
org.owasp.webgoat.lessons
lessons.model
org.owasp.webgoat.lessons.admin
JSPs/org/h2/server/web/res
JSPs/WEB-INF
JSPs/WEB-INF/pages
JSPs/WEB-INF/classes/plugin
webgoat.service
org.owasp.webgoat.session
org.owasp.webgoat.plugin.sqlinjection
webgoat.plugins
org.owasp.webgoat.plugin.rollbased
plugin.GoatHillsFinancial
org.owasp.webgoat.plugin.crosssitescripting
webgoat.plugin.db_cross_site

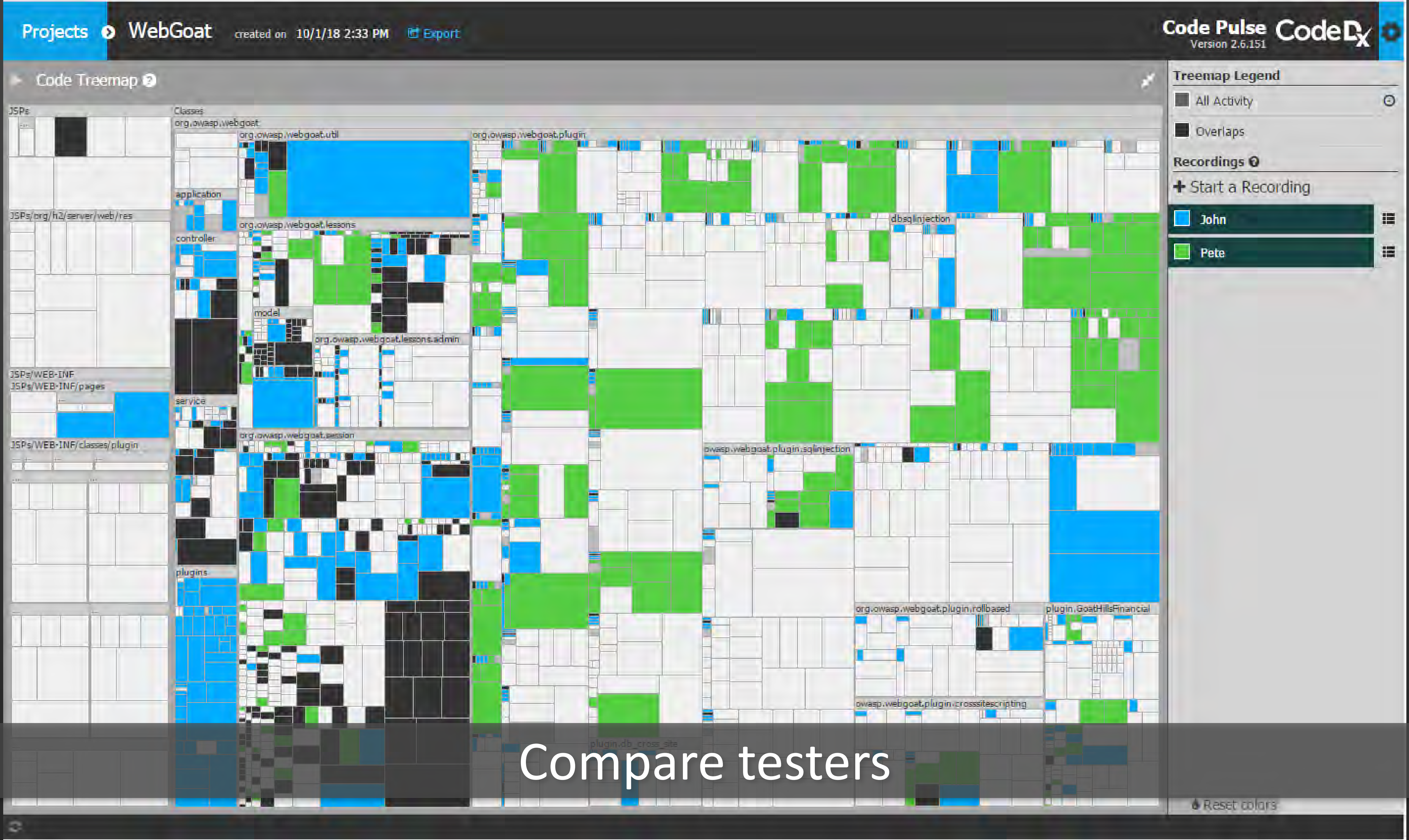
3rd scan



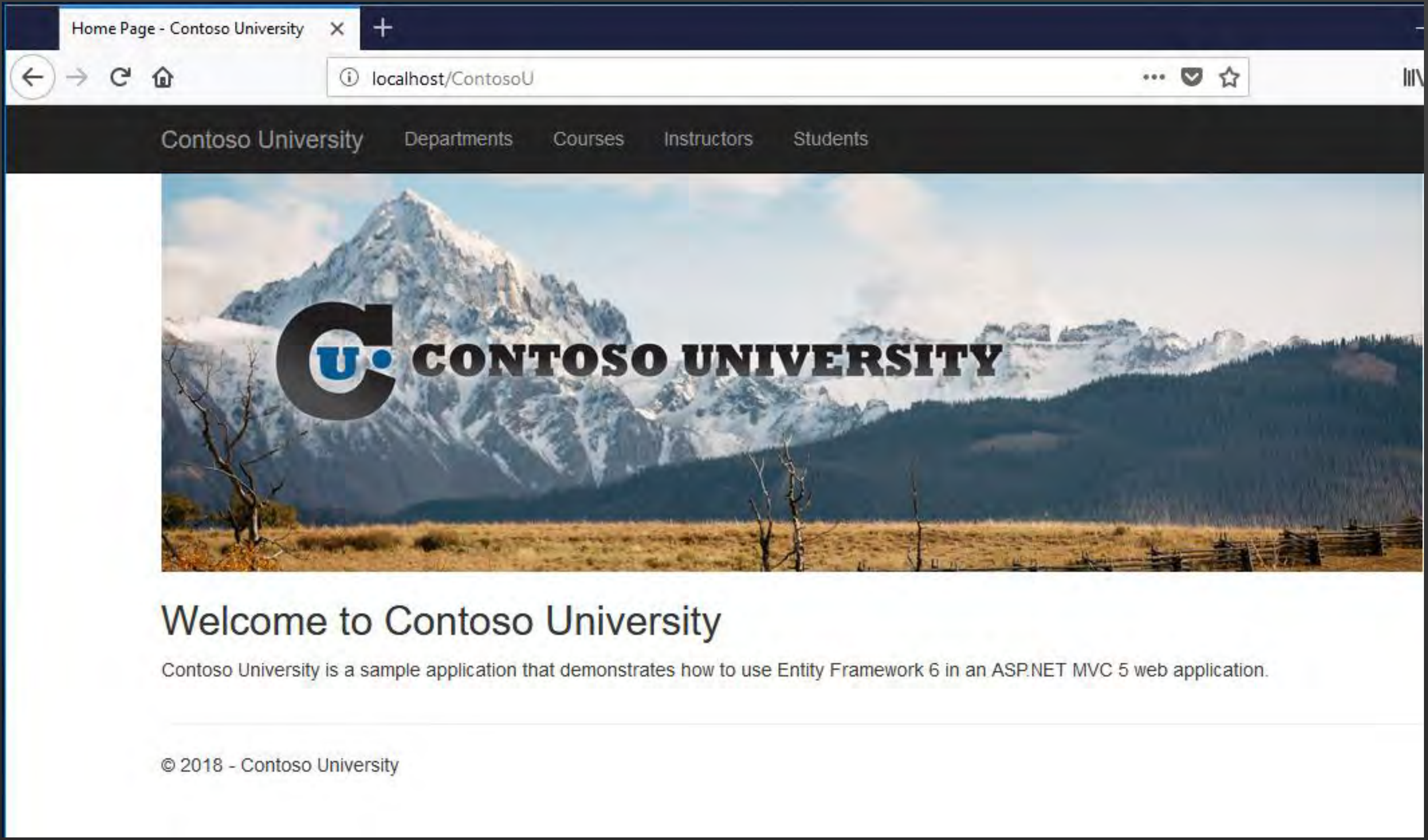
See overlap between manual and automated testing



Compare tools



Compare testers



Welcome to Contoso University

Contoso University is a sample application that demonstrates how to use Entity Framework 6 in an ASP.NET MVC 5 web application.

© 2018 - Contoso University

Live demonstration

Attack Surface Detector

Uncover your hidden attack surface!

PROBLEM Current penetration techniques miss parts of attack surface or revert to endpoint brute forcing

GOAL Develop an open source solution that provides a complete picture of the web applications exposed attack surface, pre-seed existing testing tools for more thorough and targeted testing

What Attack Surface Detector provides

Abbreviates pen testing efforts by automating the attack surface discovery process

Discovers hidden/unlinked endpoints and optional parameters and data types

Pre-seeds ZAP and Burp Suite with attack surface

Compares different versions of an application to focus testing on new/modified endpoints

How Attack Surface Detector works

Performs static source code analysis to identify web application endpoints by parsing routes and identifying parameters in the supported languages and frameworks

Supported *languages* and *frameworks*:

C#

Java

python™

Ruby

Microsoft® .NET
ASP.NET | MVC | Web API

ASP.NET
Webforms

.NET
Core

spring
source

Struts

Servlet
&
JSP

django

RAILS

Attack Surface Detector benefits

Minimize attack surface gaps

- Black box testing by penetration testers can miss unlinked endpoints without extensive endpoint brute forcing
- Mapping the full attack surface allows for testing of any unlinked endpoints

Parameter detection

- Identifying optional parameters during a black box test can be time-consuming and often miss valid parameters that affect the execution of the software
- Provides a more thorough list of parameters allowing more comprehensive and focused testing

Attack Surface Detector benefits

DAST Pre-Seeding

- Manual penetration testing is costly and time-consuming
- Provides common web application DAST tools (e.g. ZAP, Burp Suite) with endpoints and parameters objectively focusing on the manual and automated testing tasks

Time reduction

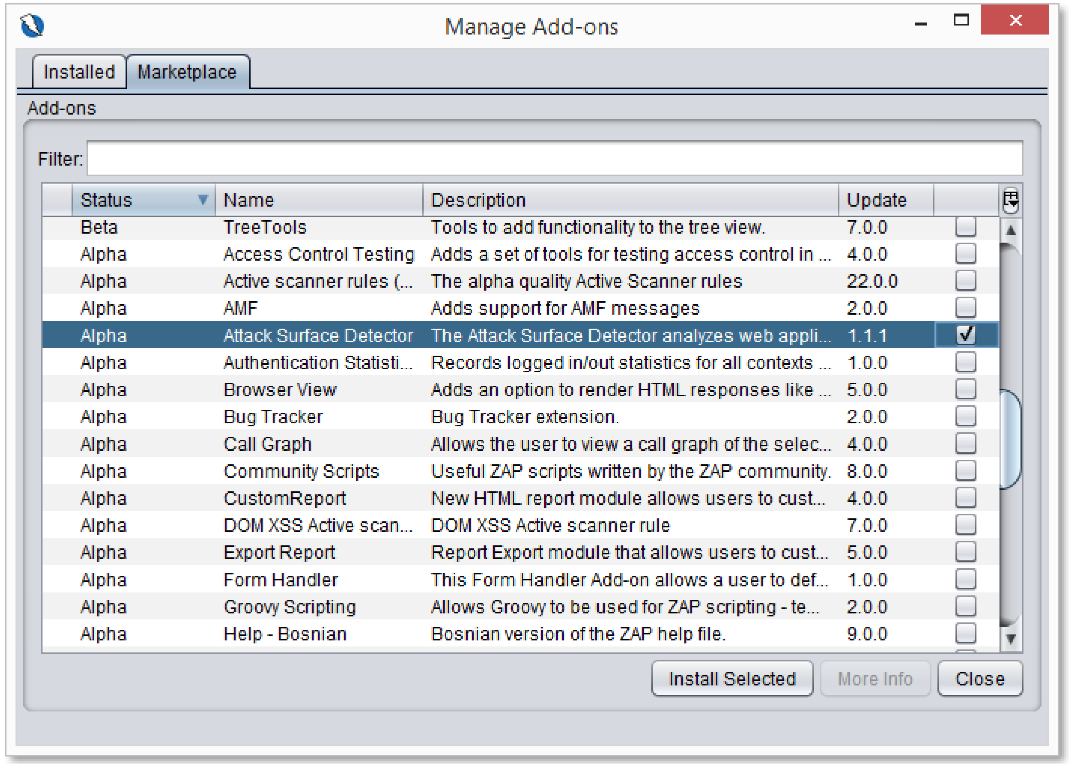
- Reduces the time required to enumerate an application attack surface
- Compare different versions of an application allowing for focus on new/modified endpoints

Available today directly in ZAP and Burp via extensions

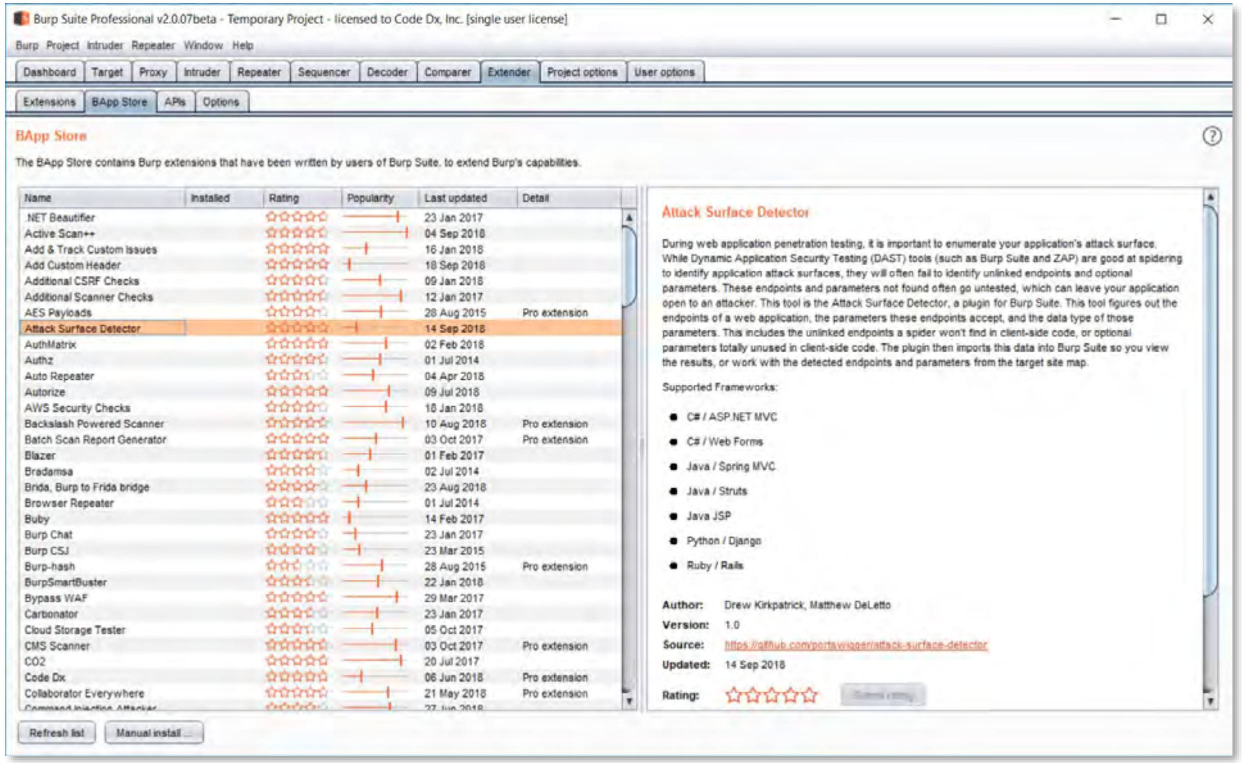
OWASP

Zed Attack Proxy
(ZAP)

BURPSUITE
PROFESSIONAL



Status	Name	Description	Update	
Beta	TreeTools	Tools to add functionality to the tree view.	7.0.0	☐
Alpha	Access Control Testing	Adds a set of tools for testing access control in ...	4.0.0	☐
Alpha	Active scanner rules (...	The alpha quality Active Scanner rules	22.0.0	☐
Alpha	AMF	Adds support for AMF messages	2.0.0	☐
Alpha	Attack Surface Detector	The Attack Surface Detector analyzes web appli...	1.1.1	☑
Alpha	Authentication Statisti...	Records logged in/out statistics for all contexts ...	1.0.0	☐
Alpha	Browser View	Adds an option to render HTML responses like ...	5.0.0	☐
Alpha	Bug Tracker	Bug Tracker extension.	2.0.0	☐
Alpha	Call Graph	Allows the user to view a call graph of the selec...	4.0.0	☐
Alpha	Community Scripts	Useful ZAP scripts written by the ZAP community.	8.0.0	☐
Alpha	CustomReport	New HTML report module allows users to cust...	4.0.0	☐
Alpha	DOM XSS Active scan...	DOM XSS Active scanner rule	7.0.0	☐
Alpha	Export Report	Report Export module that allows users to cust...	5.0.0	☐
Alpha	Form Handler	This Form Handler Add-on allows a user to def...	1.0.0	☐
Alpha	Groovy Scripting	Allows Groovy to be used for ZAP scripting - te...	2.0.0	☐
Alpha	Help - Bosnian	Bosnian version of the ZAP help file.	9.0.0	☐



BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popularity	Last updated	Detail
.NET Beautifier				23 Jan 2017	
Active Scan++				04 Sep 2018	
Add & Track Custom Issues				16 Jan 2018	
Add Custom Header				18 Sep 2018	
Additional CSRF Checks				09 Jan 2018	
Additional Scanner Checks				12 Jan 2017	
AES Payloads				28 Aug 2015	Pro extension
Attack Surface Detector				14 Sep 2018	
AuthMatrix				02 Feb 2018	
Authz				01 Jul 2014	
Auto Repeater				04 Apr 2018	
Autorize				09 Jul 2018	
AWS Security Checks				18 Jan 2018	
Backslash Powered Scanner				10 Aug 2018	Pro extension
Batch Scan Report Generator				03 Oct 2017	Pro extension
Blazer				01 Feb 2017	
Bradamsa				02 Jul 2014	
Brida, Burp to Frida bridge				23 Aug 2018	
Browser Repeater				01 Jul 2014	
Buby				14 Feb 2017	
Burp Chat				23 Jan 2017	
Burp CSJ				23 Mar 2015	
Burp-hash				28 Aug 2015	Pro extension
BurpSmartBuster				22 Jan 2018	
Bypass WAF				29 Mar 2017	
Carbonator				23 Jan 2017	
Cloud Storage Tester				05 Oct 2017	
CMS Scanner				03 Oct 2017	Pro extension
CO2				20 Jul 2017	
Code Dx				06 Jun 2018	Pro extension
Collaborator Everywhere				21 May 2018	Pro extension
Command Injection Attacker				27 Jun 2018	

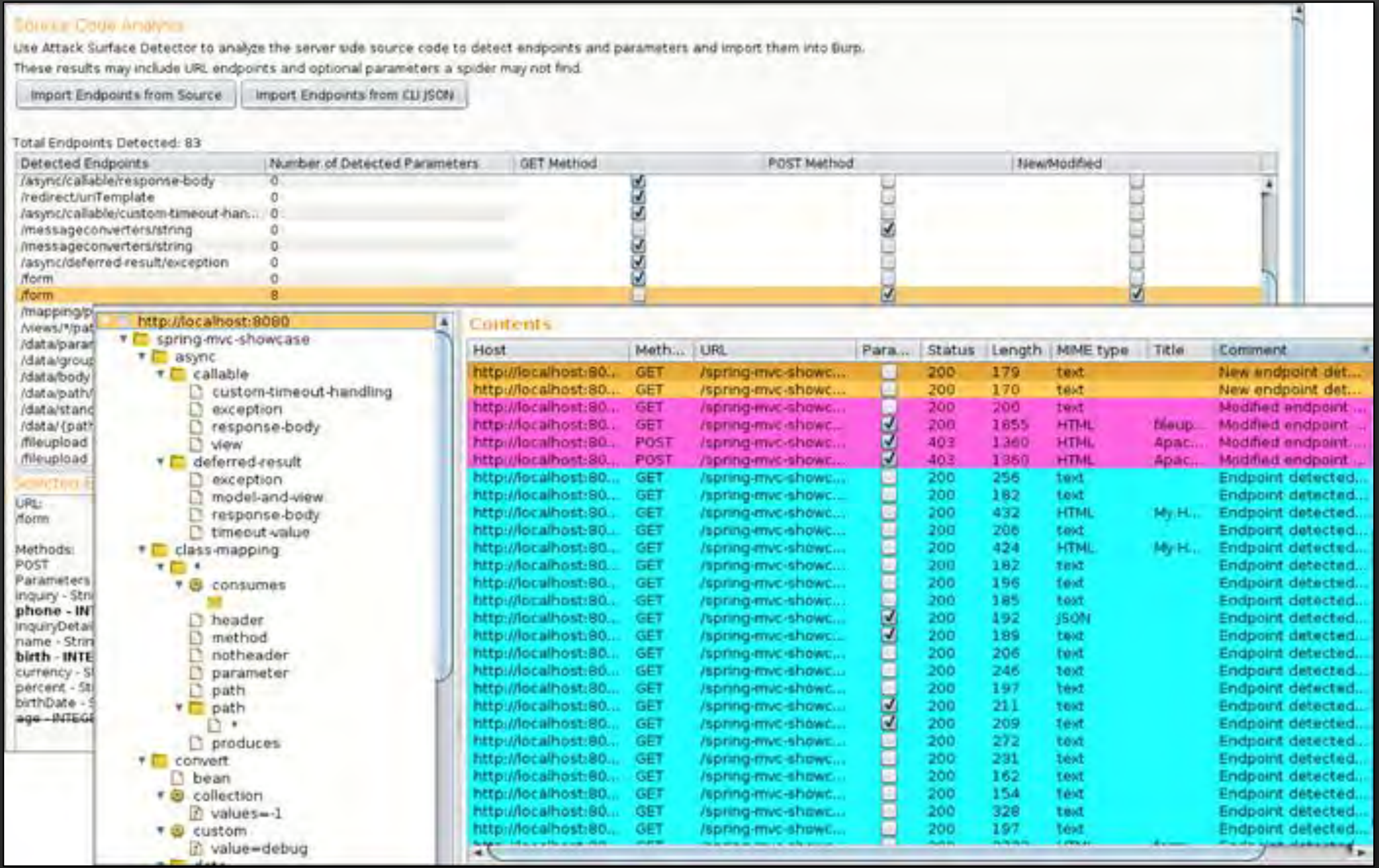
Attack Surface Detector

During web application penetration testing, it is important to enumerate your application's attack surface. While Dynamic Application Security Testing (DAST) tools (such as Burp Suite and ZAP) are good at spidering to identify application attack surfaces, they will often fail to identify unlinked endpoints and optional parameters. These endpoints and parameters not found often go untested, which can leave your application open to an attacker. This tool is the Attack Surface Detector, a plugin for Burp Suite. This tool figures out the endpoints of a web application, the parameters these endpoints accept, and the data type of those parameters. This includes the unlinked endpoints a spider won't find in client-side code, or optional parameters totally unused in client-side code. The plugin then imports this data into Burp Suite so you view the results, or work with the detected endpoints and parameters from the target site map.

Supported Frameworks:

- C# / ASP.NET MVC
- C# / Web Forms
- Java / Spring MVC
- Java / Struts
- Java JSP
- Python / Django
- Ruby / Rails

Author: Drew Kirkpatrick, Matthew DeLetto
Version: 1.0
Source: https://github.com/portswigger/attack-surface-detector
Updated: 14 Sep 2018
Rating: ☆☆☆☆☆



Source Code Analysis

Use Attack Surface Detector to analyze the server side source code to detect endpoints and parameters and import them into Burp.

These results may include URL endpoints and optional parameters a spider may not find.

Total Endpoints Detected: 83

Detected Endpoints	Number of Detected Parameters	GET Method	POST Method	New/Modified
/async/callable/response-body	0	☑	□	□
/redirect/uriTemplate	0	☑	□	□
/async/callable/custom-timeout-han...	0	☑	□	□
/messageconverters/string	0	□	☑	□
/messageconverters/string	0	☑	□	□
/async/deferred-result/exception	0	☑	□	□
/form	0	☑	□	□
/form	8	□	☑	☑

/mapping/p
/views/*/pat
/data/parar
/data/group
/data/body
/data/path/
/data/stand
/data/{path
/fileupload
/fileupload

Selected E

URL:
/form

Methods:
POST
Parameters
inquiry - Stri
phone - INT
inquiryDetai
name - Strin
birth - INTE
currency - S
percent - St
birthDate - S
~~age - INTEGE~~

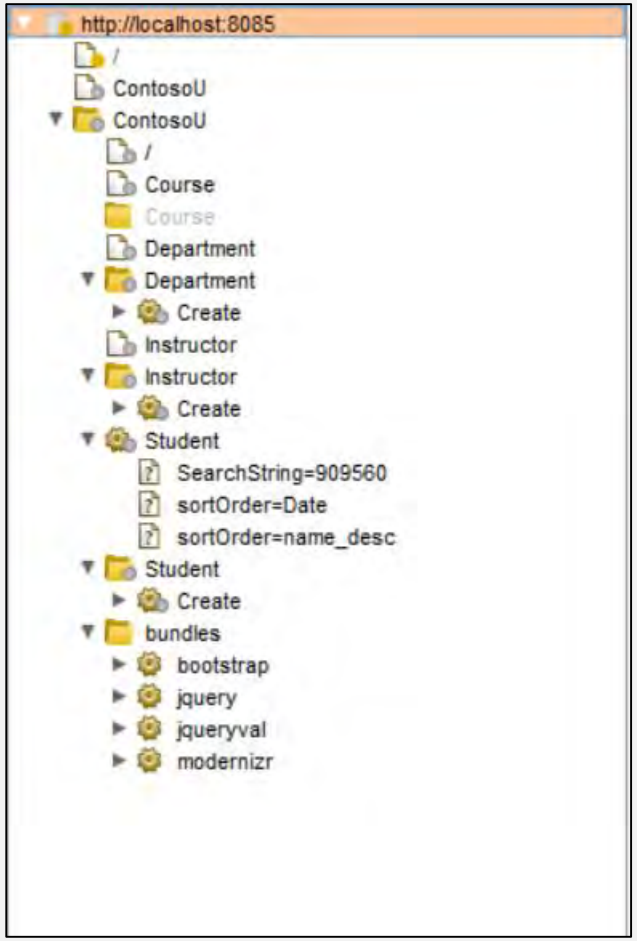
```
http://localhost:8080
  ▾ spring-mvc-showcase
    ▾ async
      ▾ callable
          custom-timeout-handling
          exception
          response-body
          view
      ▾ deferred-result
          exception
          model-and-view
          response-body
          timeout-value
    ▾ class-mapping
      ▾ *
        ▾ consumes

          header
          method
          notheader
          parameter
          path
        ▾ path
            *
          produces
    ▾ convert
        bean
      ▾ collection
          values=-1
      ▾ custom
          value=debug
```

Contents

Host	Meth...	URL	Para...	Status	Length	MIME type	Title	Comment
http://localhost:80...	GET	/spring-mvc-showc...	□	200	179	text		New endpoint det...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	170	text		New endpoint det...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	200	text		Modified endpoint ...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	1855	HTML	fileup...	Modified endpoint ...
http://localhost:80...	POST	/spring-mvc-showc...	☑	403	1360	HTML	Apac...	Modified endpoint ...
http://localhost:80...	POST	/spring-mvc-showc...	☑	403	1360	HTML	Apac...	Modified endpoint ...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	256	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	182	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	432	HTML	My H...	Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	206	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	424	HTML	My H...	Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	182	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	196	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	185	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	192	JSON		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	189	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	206	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	246	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	197	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	211	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	☑	200	209	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	272	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	231	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	162	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	154	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	328	text		Endpoint detected...
http://localhost:80...	GET	/spring-mvc-showc...	□	200	197	text		Endpoint detected...

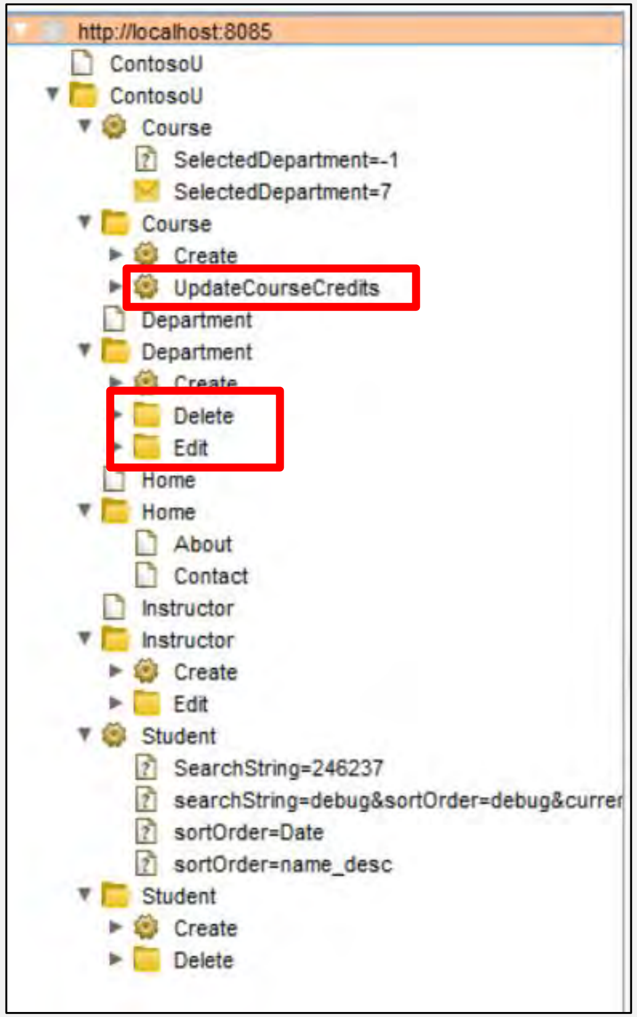
Live demonstration

Before Pre-Seeding



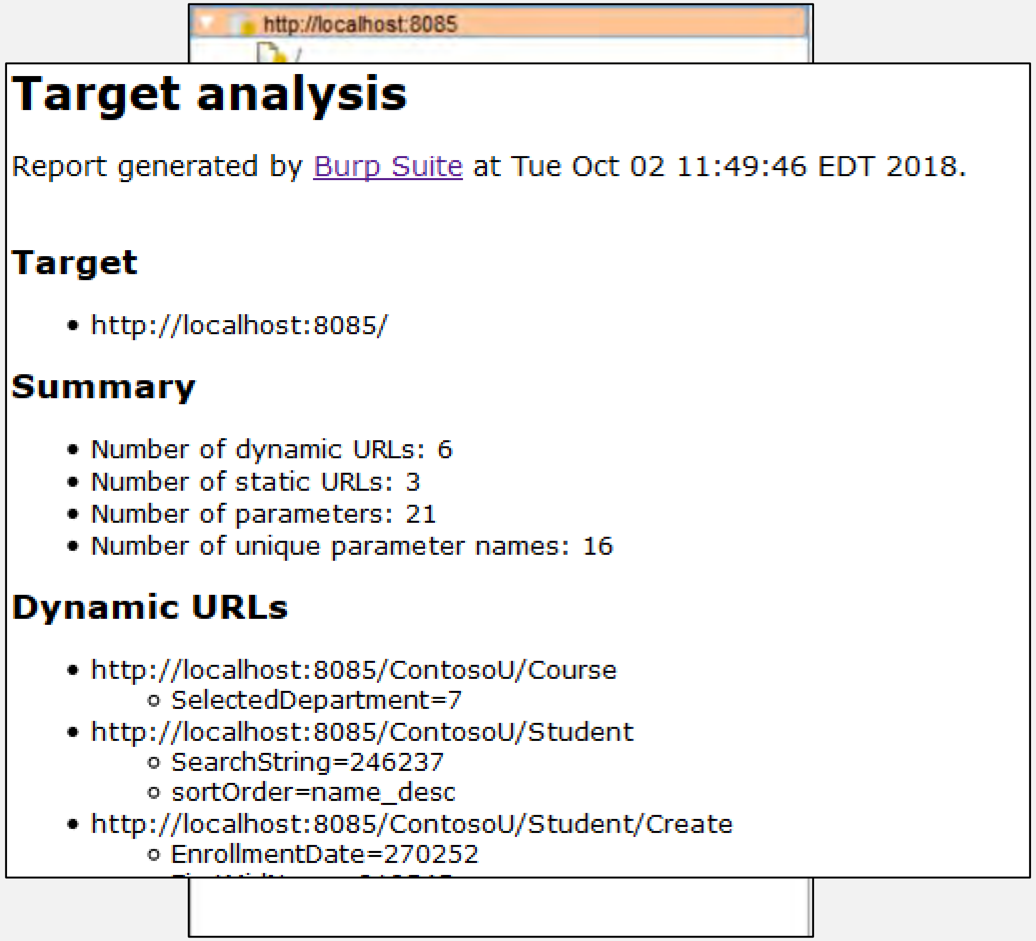
- http://localhost:8085
  - /
  - ContosoU
  - ContosoU
    - /
    - Course
    - Course
    - Department
    - Department
      - Create
    - Instructor
    - Instructor
      - Create
    - Student
      - SearchString=909560
      - sortOrder=Date
      - sortOrder=name_desc
    - Student
      - Create
    - bundles
      - bootstrap
      - jquery
      - jqueryval
      - modernizr

After Pre-Seeding



- http://localhost:8085
  - ContosoU
  - ContosoU
    - Course
      - SelectedDepartment=-1
      - SelectedDepartment=7
    - Course
      - Create
      - UpdateCourseCredits
    - Department
    - Department
      - Create
      - Delete
      - Edit
    - Home
    - Home
      - About
      - Contact
    - Instructor
    - Instructor
      - Create
      - Edit
    - Student
      - SearchString=246237
      - searchString=debug&sortOrder=debug&currer
      - sortOrder=Date
      - sortOrder=name_desc
    - Student
      - Create
      - Delete

Before Pre-Seeding



Target analysis

Report generated by Burp Suite at Tue Oct 02 11:49:46 EDT 2018.

Target

- http://localhost:8085/

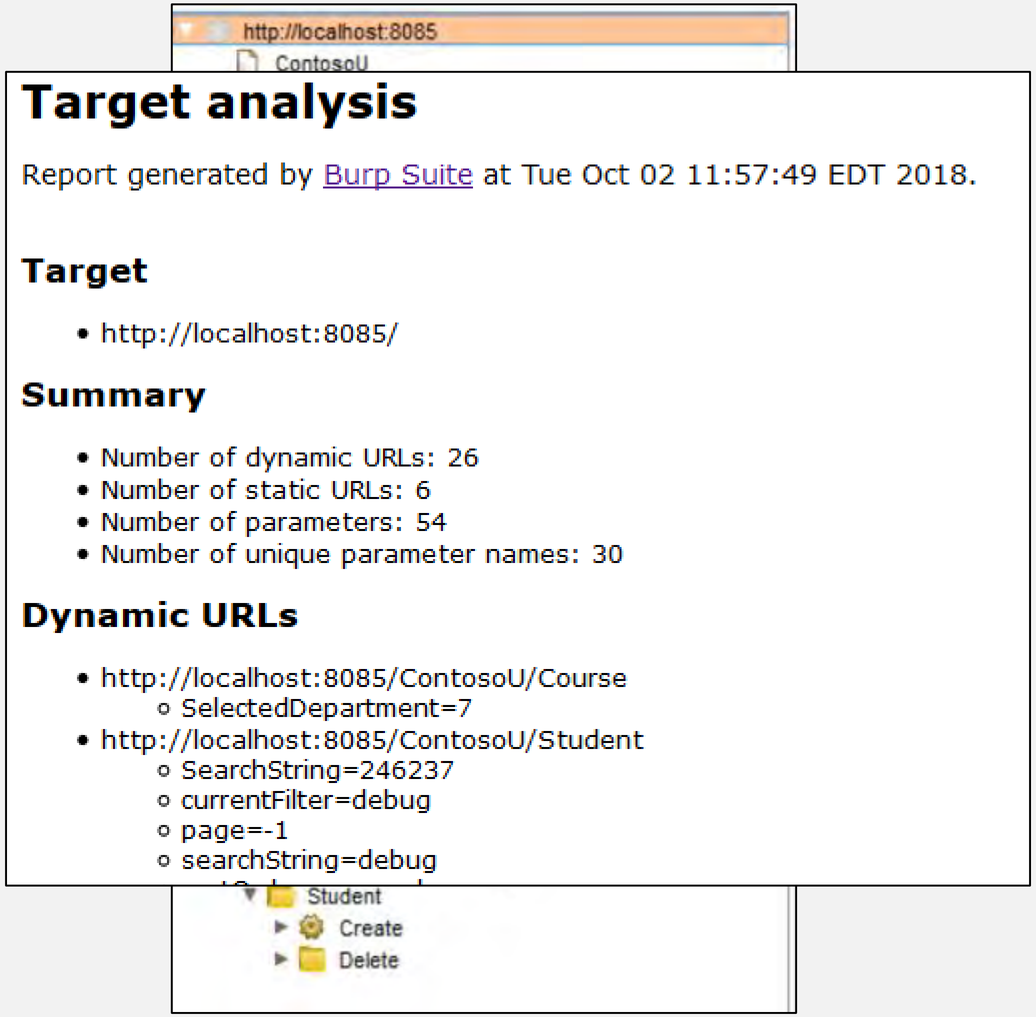
Summary

- Number of dynamic URLs: 6
- Number of static URLs: 3
- Number of parameters: 21
- Number of unique parameter names: 16

Dynamic URLs

- http://localhost:8085/ContosoU/Course
  - SelectedDepartment=7
- http://localhost:8085/ContosoU/Student
  - SearchString=246237
  - sortOrder=name_desc
- http://localhost:8085/ContosoU/Student/Create
  - EnrollmentDate=270252

After Pre-Seeding



Target analysis

Report generated by Burp Suite at Tue Oct 02 11:57:49 EDT 2018.

Target

- http://localhost:8085/

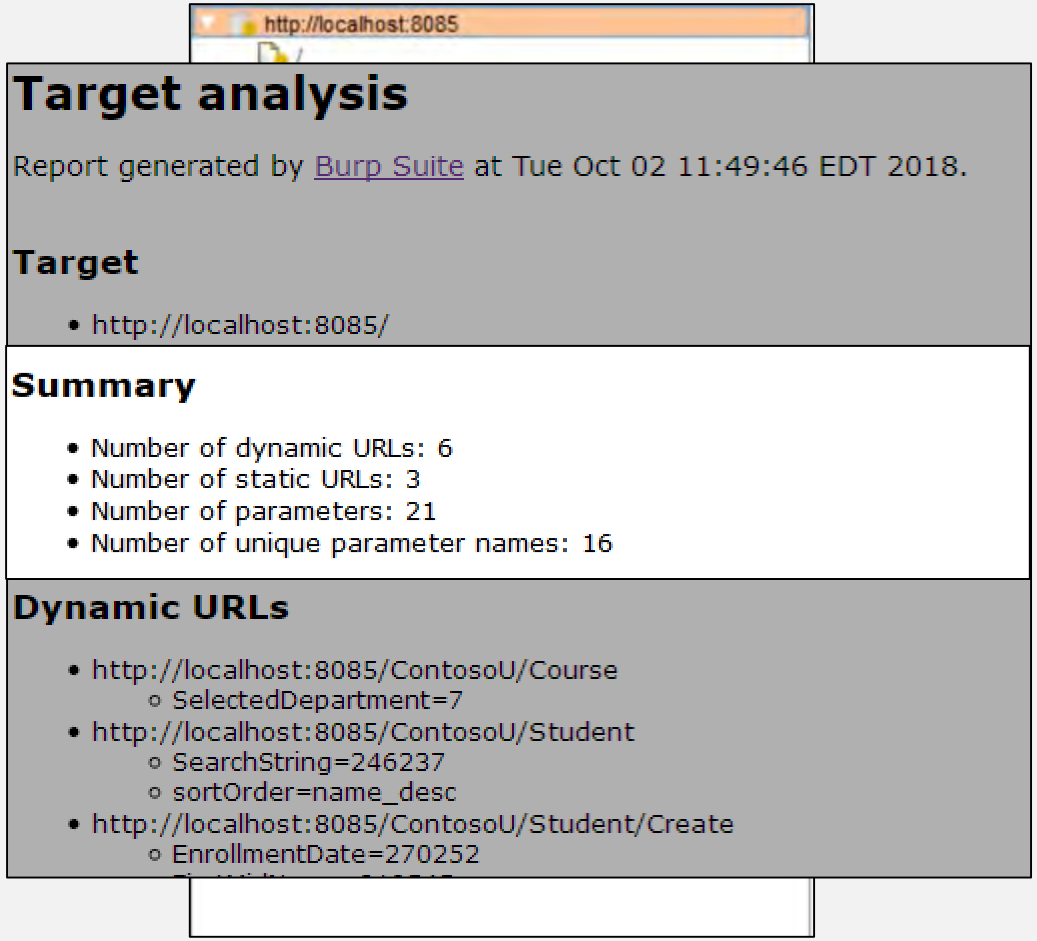
Summary

- Number of dynamic URLs: 26
- Number of static URLs: 6
- Number of parameters: 54
- Number of unique parameter names: 30

Dynamic URLs

- http://localhost:8085/ContosoU/Course
  - SelectedDepartment=7
- http://localhost:8085/ContosoU/Student
  - SearchString=246237
  - currentFilter=debug
  - page=-1
  - searchString=debug

Before Pre-Seeding



Target analysis

Report generated by Burp Suite at Tue Oct 02 11:49:46 EDT 2018.

Target

- http://localhost:8085/

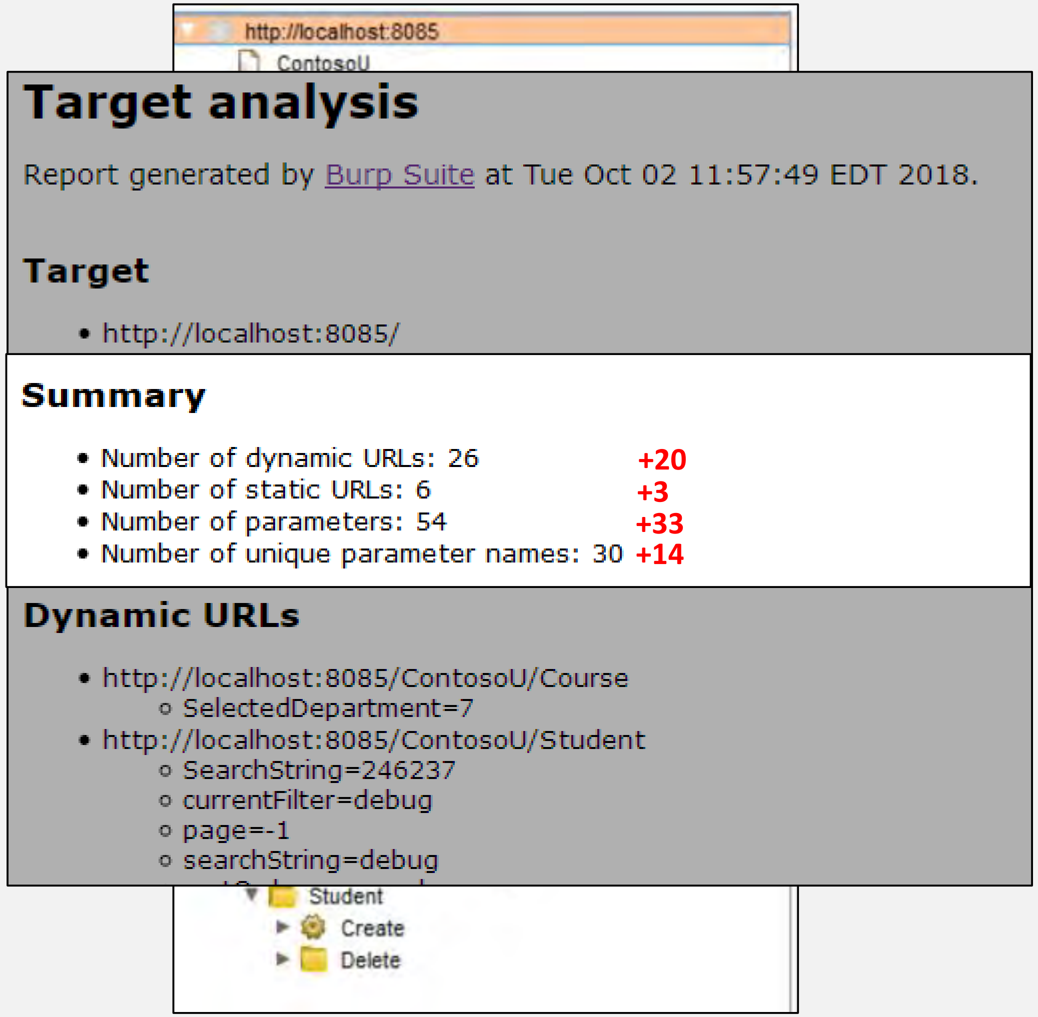
Summary

- Number of dynamic URLs: 6
- Number of static URLs: 3
- Number of parameters: 21
- Number of unique parameter names: 16

Dynamic URLs

- http://localhost:8085/ContosoU/Course
  - SelectedDepartment=7
- http://localhost:8085/ContosoU/Student
  - SearchString=246237
  - sortOrder=name_desc
- http://localhost:8085/ContosoU/Student/Create
  - EnrollmentDate=270252

After Pre-Seeding



Target analysis

Report generated by Burp Suite at Tue Oct 02 11:57:49 EDT 2018.

Target

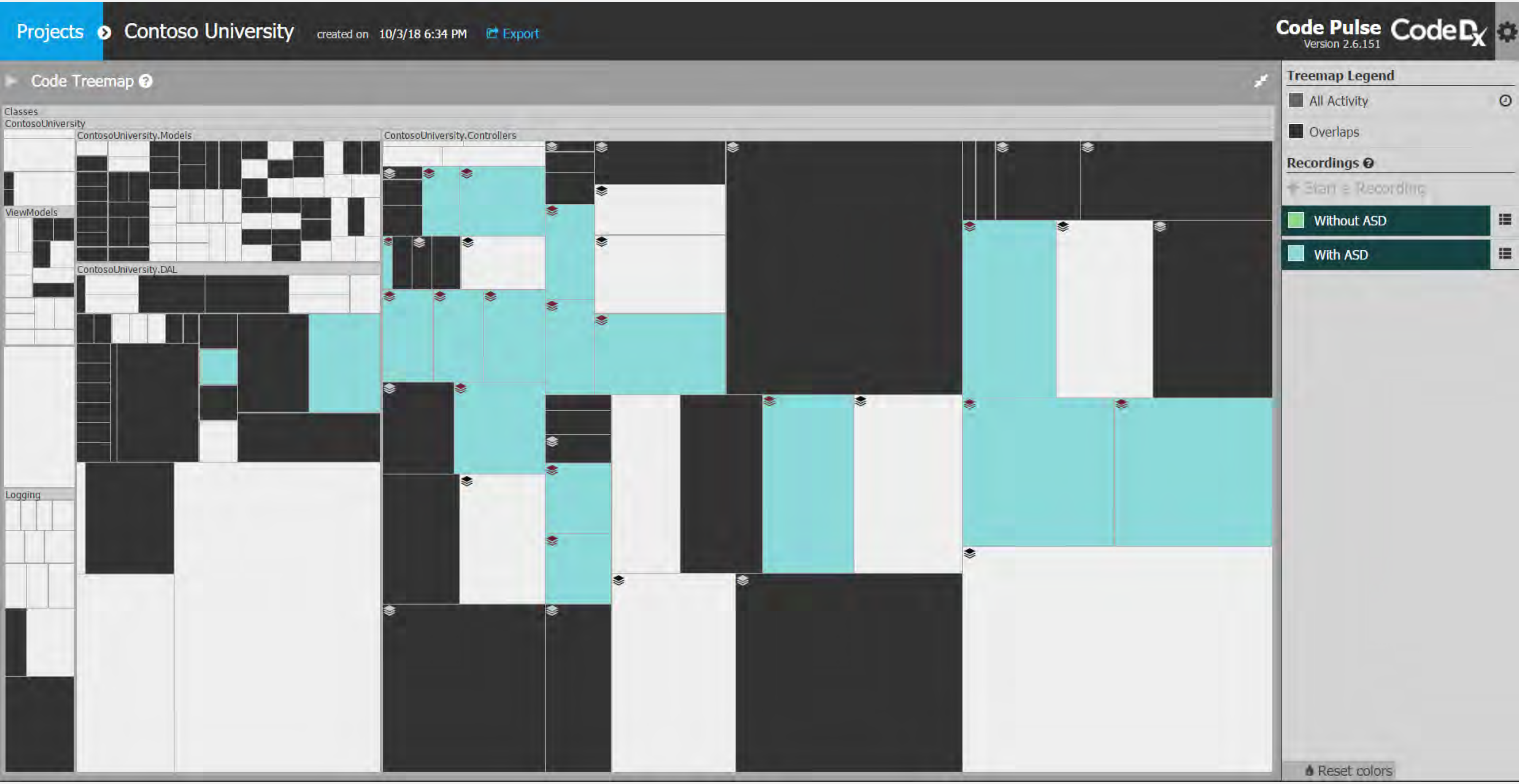
- http://localhost:8085/

Summary

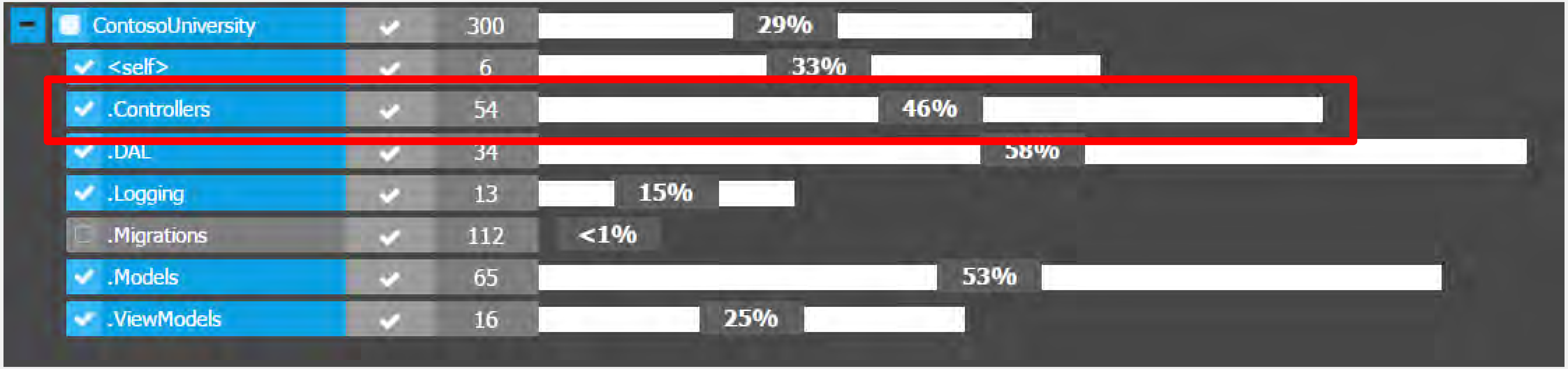
- Number of dynamic URLs: 26 **+20**
- Number of static URLs: 6 **+3**
- Number of parameters: 54 **+33**
- Number of unique parameter names: 30 **+14**

Dynamic URLs

- http://localhost:8085/ContosoU/Course
  - SelectedDepartment=7
- http://localhost:8085/ContosoU/Student
  - SearchString=246237
  - currentFilter=debug
  - page=-1
  - searchString=debug

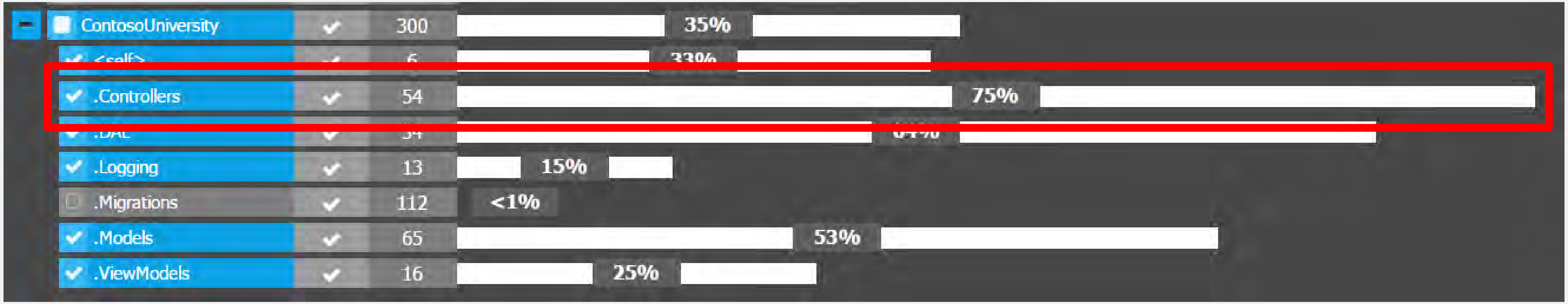

Projects
Contoso University
created on 10/3/18 6:34 PM
Export
Code Pulse
Version 2.6.151
CodeDx
Code Treemap
Classes
ContosoUniversity
ContosoUniversity.Models
ContosoUniversity.Controllers
ViewModels
ContosoUniversity.DAL
Logging
Treemap Legend
All Activity
Overlaps
Recordings
Start a Recording
Without ASD
With ASD
Reset colors

Without Attack Surface Detector

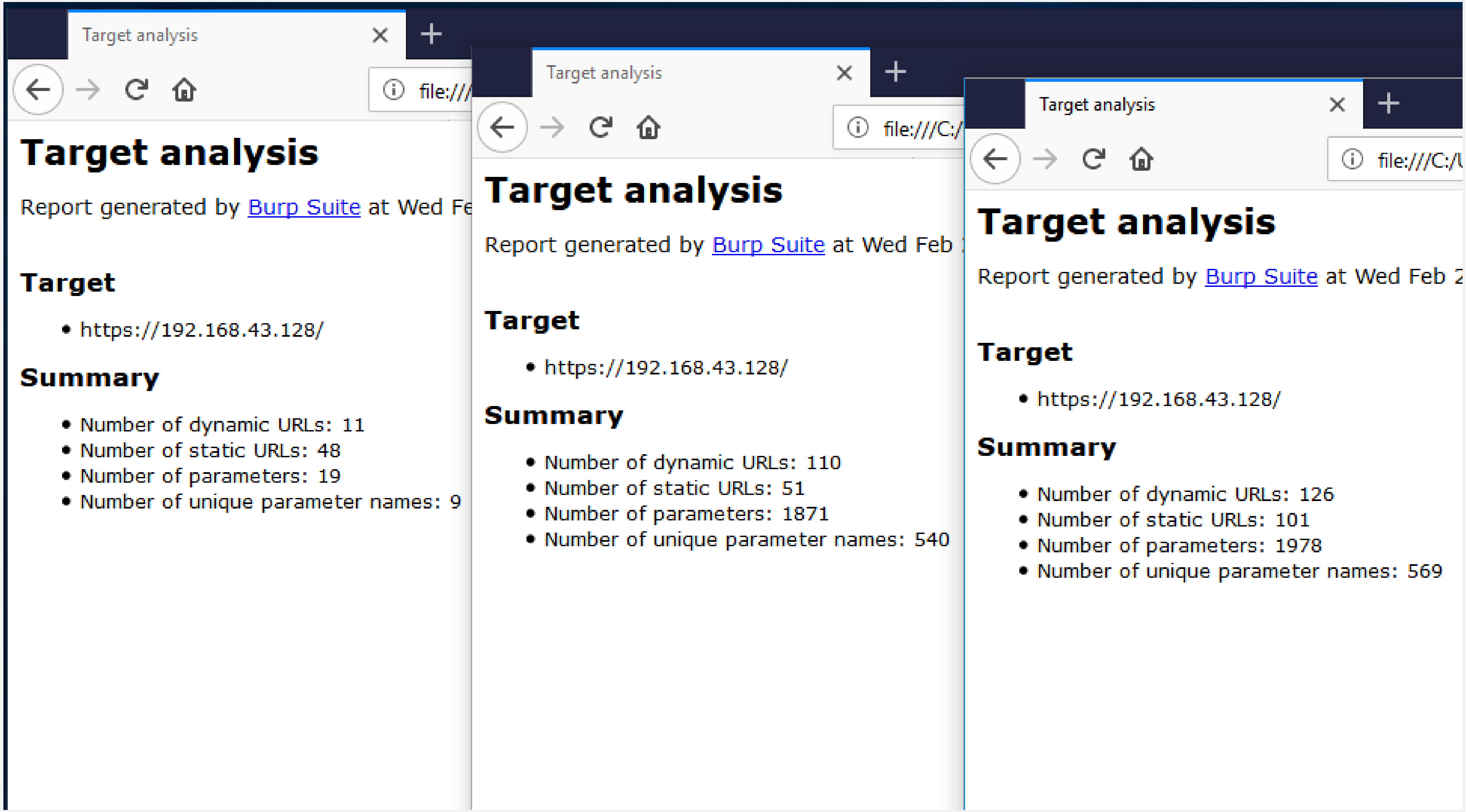


ContosoUniversity	✓	300	29%
✓ <self>	✓	6	33%
✓ .Controllers	✓	54	46%
✓ .DAL	✓	34	58%
✓ .Logging	✓	13	15%
□ .Migrations	✓	112	<1%
✓ .Models	✓	65	53%
✓ .ViewModels	✓	16	25%

With Attack Surface Detector: 29% improvement



ContosoUniversity	✓	300	35%
✓ <self>	✓	6	33%
✓ .Controllers	✓	54	75%
✓ .DAL	✓	34	64%
✓ .Logging	✓	13	15%
□ .Migrations	✓	112	<1%
✓ .Models	✓	65	53%
✓ .ViewModels	✓	16	25%



Target analysis

Report generated by Burp Suite at Wed Fe

Target

- https://192.168.43.128/

Summary

- Number of dynamic URLs: 11
- Number of static URLs: 48
- Number of parameters: 19
- Number of unique parameter names: 9

Target analysis

Report generated by Burp Suite at Wed Feb

Target

- https://192.168.43.128/

Summary

- Number of dynamic URLs: 110
- Number of static URLs: 51
- Number of parameters: 1871
- Number of unique parameter names: 540

Target analysis

Report generated by Burp Suite at Wed Feb 2

Target

- https://192.168.43.128/

Summary

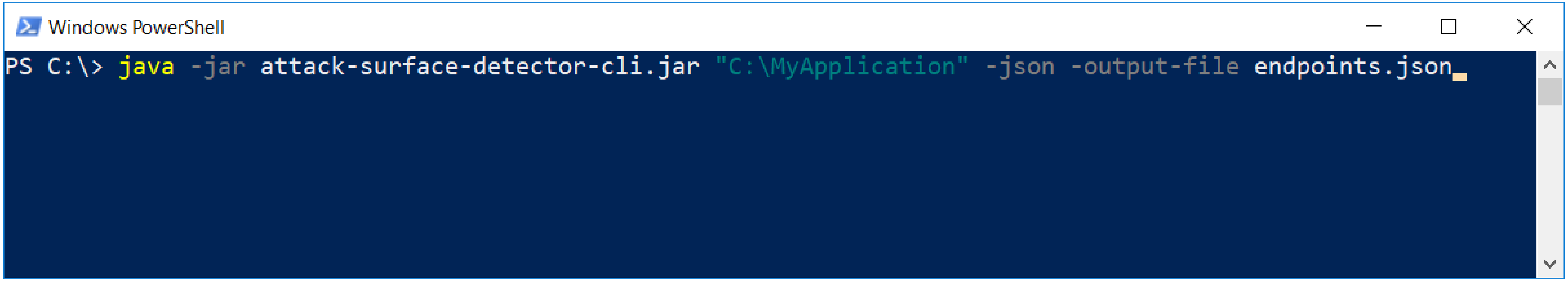
- Number of dynamic URLs: 126
- Number of static URLs: 101
- Number of parameters: 1978
- Number of unique parameter names: 569

Attack Surface Detector Command Line Interface (CLI)

The `attack-surface-detector-cli` takes in a folder containing code and outputs the set of endpoints detected within that codebase

Optionally they can be saved to a JSON file

This JSON can then be imported by the Burp and ZAP plugins



```
PS C:\> java -jar attack-surface-detector-cli.jar "C:\MyApplication" -json -output-file endpoints.json
```

Wrap-up

Where to learn more; Q&A

Where to learn more

OWASP Code Pulse:
http://www.code-pulse.com
https://www.owasp.org/index.php/OWASP_Code_Pulse_Project

OWASP Attack Surface Detector:
https://www.owasp.org/index.php/OWASP_Attack_Surface_Detector_Project

OWASP ZAP:
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP WebGoat: https://www.owasp.org/index.php/OWASP_WebGoat_Project

OWASP Dependency Check:
https://www.owasp.org/index.php/OWASP_Dependency_Check

Contoso University: https://bit.ly/2mPlDDo

Burp Suite: https://portswigger.net/burp

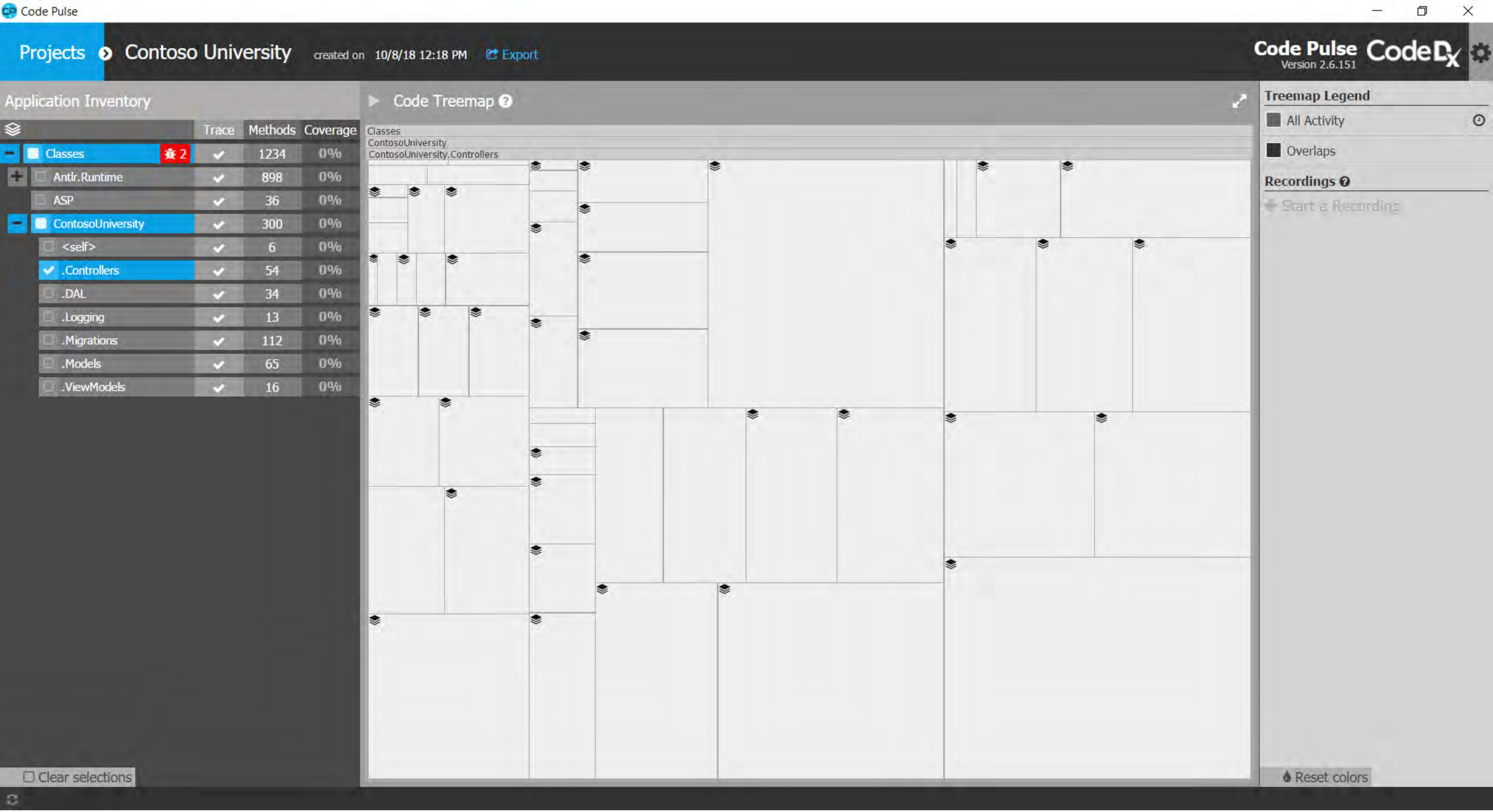
Contact information

Ken Prole

CTO, Code Dx
Principal Investigator, Secure Decisions

@KenProle
ken.prole@codedx.com ✉

IN EMERGENCY BREAK GLASS



Projects › Contoso University created on 10/8/18 12:18 PM

Application Inventory

	Trace	Methods	Coverage
− □ Classes 🐞 2	✓	1234	0%
+ □ Antlr.Runtime	✓	898	0%
□ ASP	✓	36	0%
− □ ContosoUniversity	✓	300	0%
□ <self>	✓	6	0%
☑ .Controllers	✓	54	0%
□ .DAL	✓	34	0%
□ .Logging	✓	13	0%
□ .Migrations	✓	112	0%
□ .Models	✓	65	0%
□ .ViewModels	✓	16	0%

Code Treemap

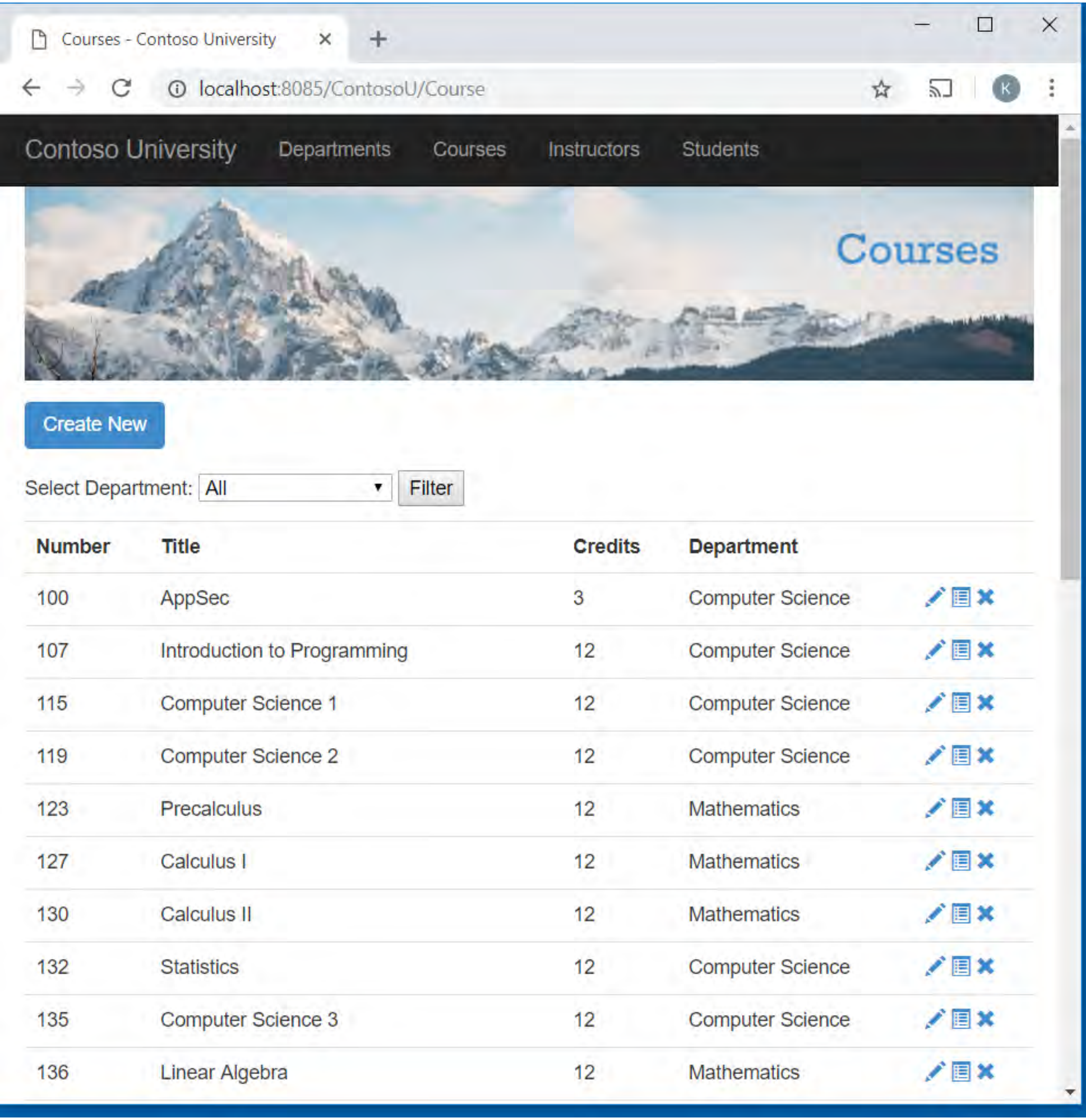
Classes
ContosoUniversity
ContosoUniversity.Controllers

Treemap Legend

▨ All Activity

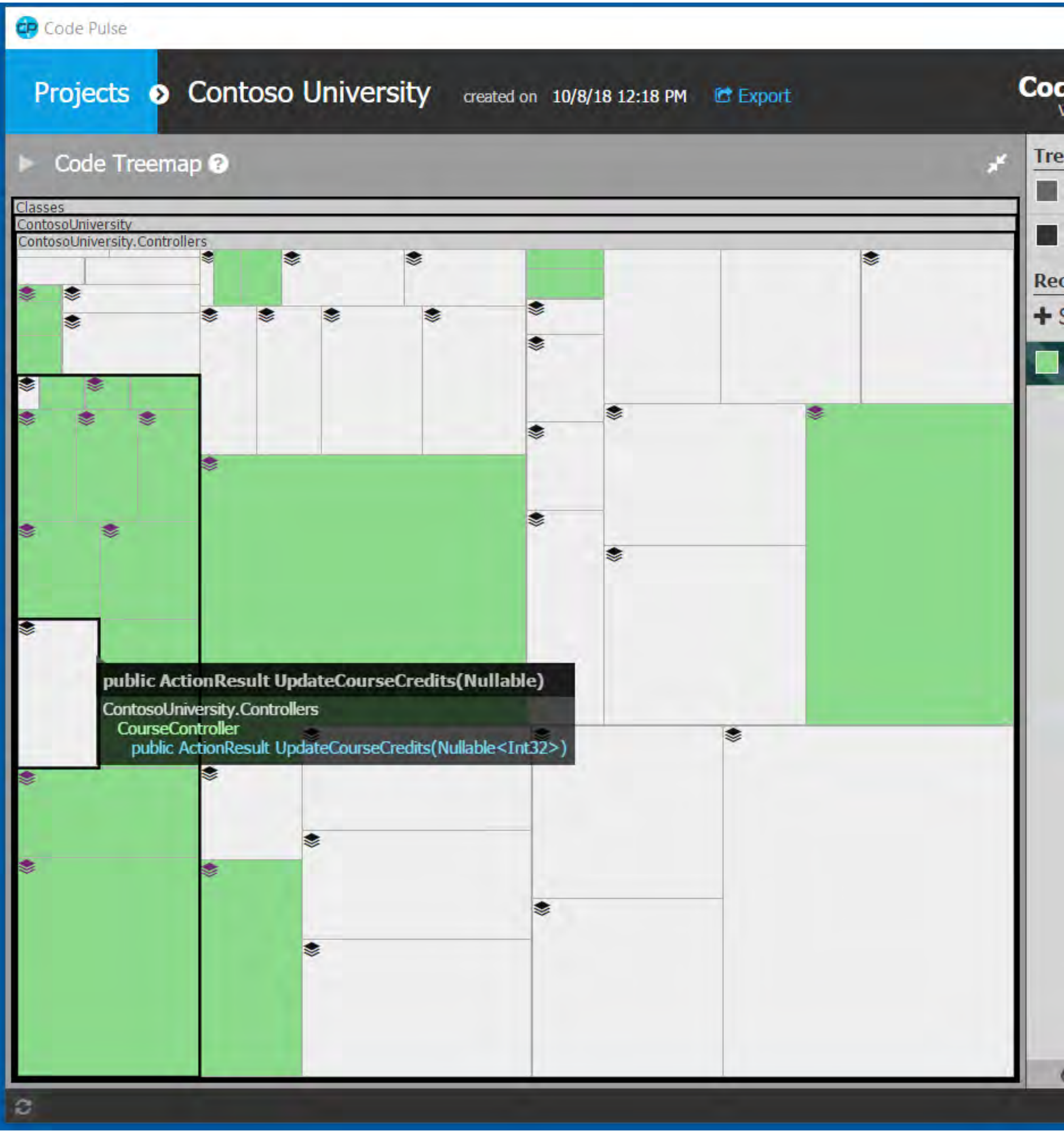
■ Overlaps

Recordings



Select Department: All

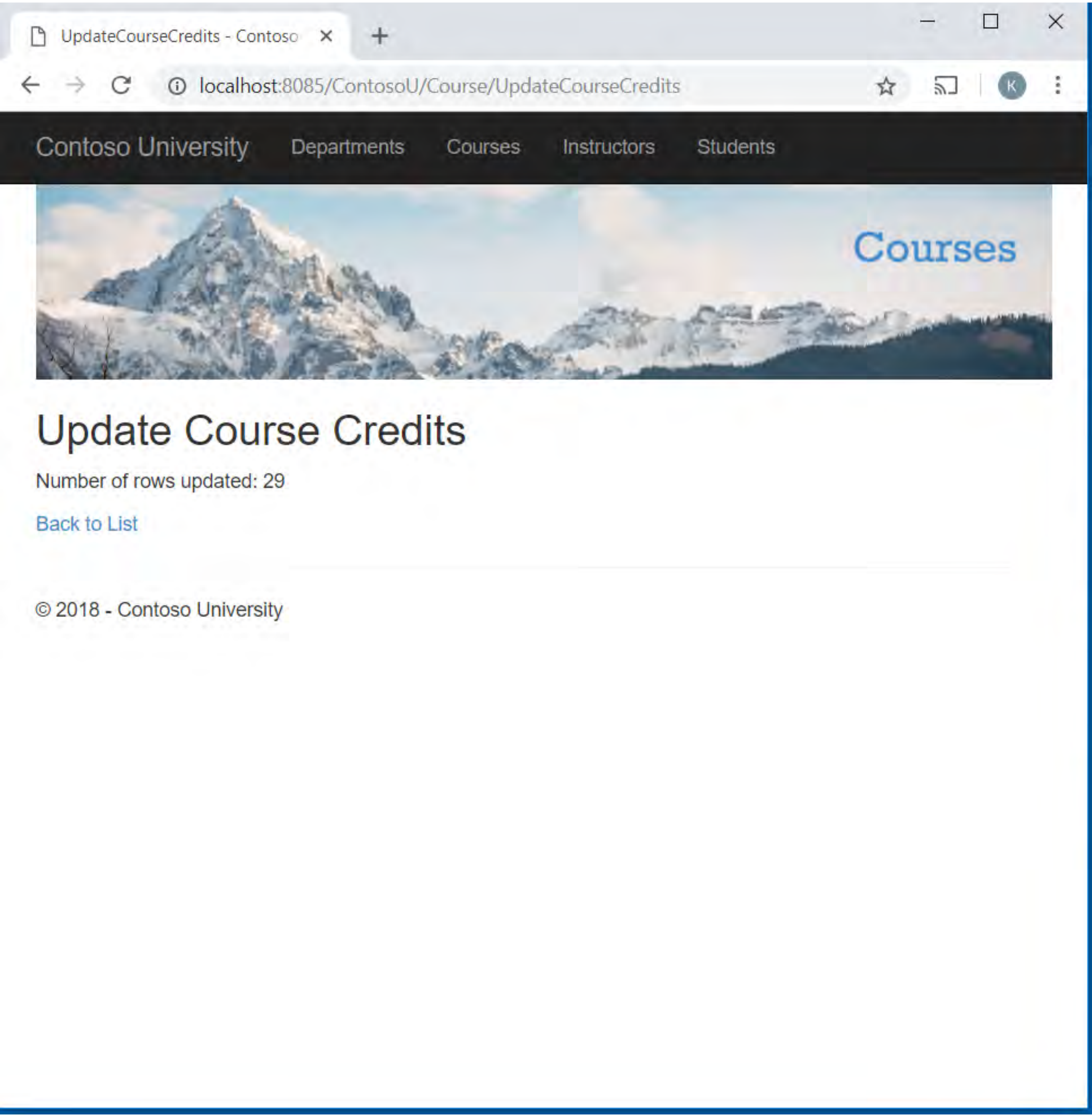
Number	Title	Credits	Department
100	AppSec	3	Computer Science
107	Introduction to Programming	12	Computer Science
115	Computer Science 1	12	Computer Science
119	Computer Science 2	12	Computer Science
123	Precalculus	12	Mathematics
127	Calculus I	12	Mathematics
130	Calculus II	12	Mathematics
132	Statistics	12	Computer Science
135	Computer Science 3	12	Computer Science
136	Linear Algebra	12	Mathematics



created on 10/8/18 12:18 PM

public ActionResult UpdateCourseCredits(Nullable)

ContosoUniversity.Controllers
CourseController
public ActionResult UpdateCourseCredits(Nullable<Int32>)



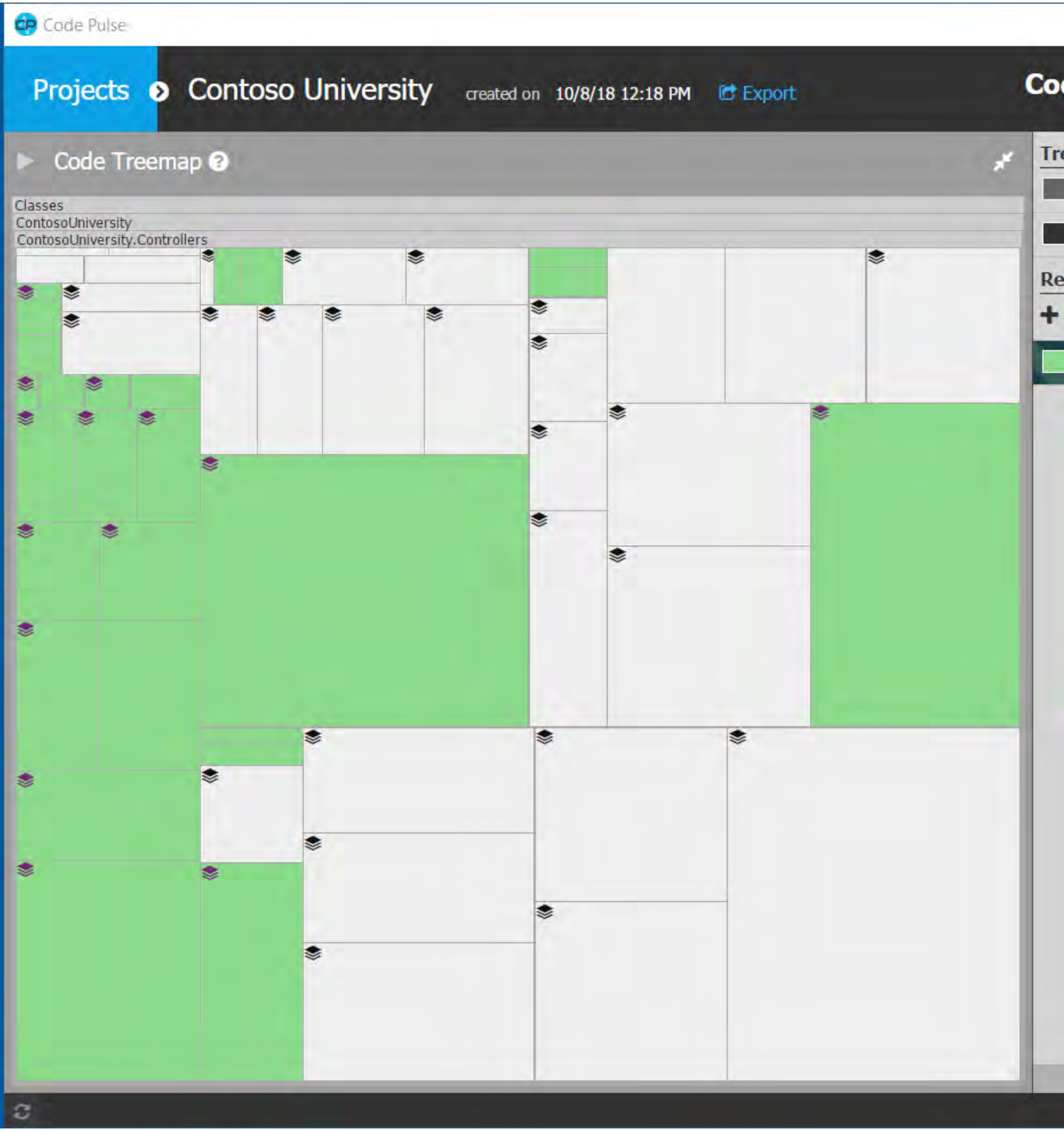
UpdateCourseCredits - Contoso
localhost:8085/ContosoU/Course/UpdateCourseCredits
Contoso University
Departments
Courses
Instructors
Students
Courses

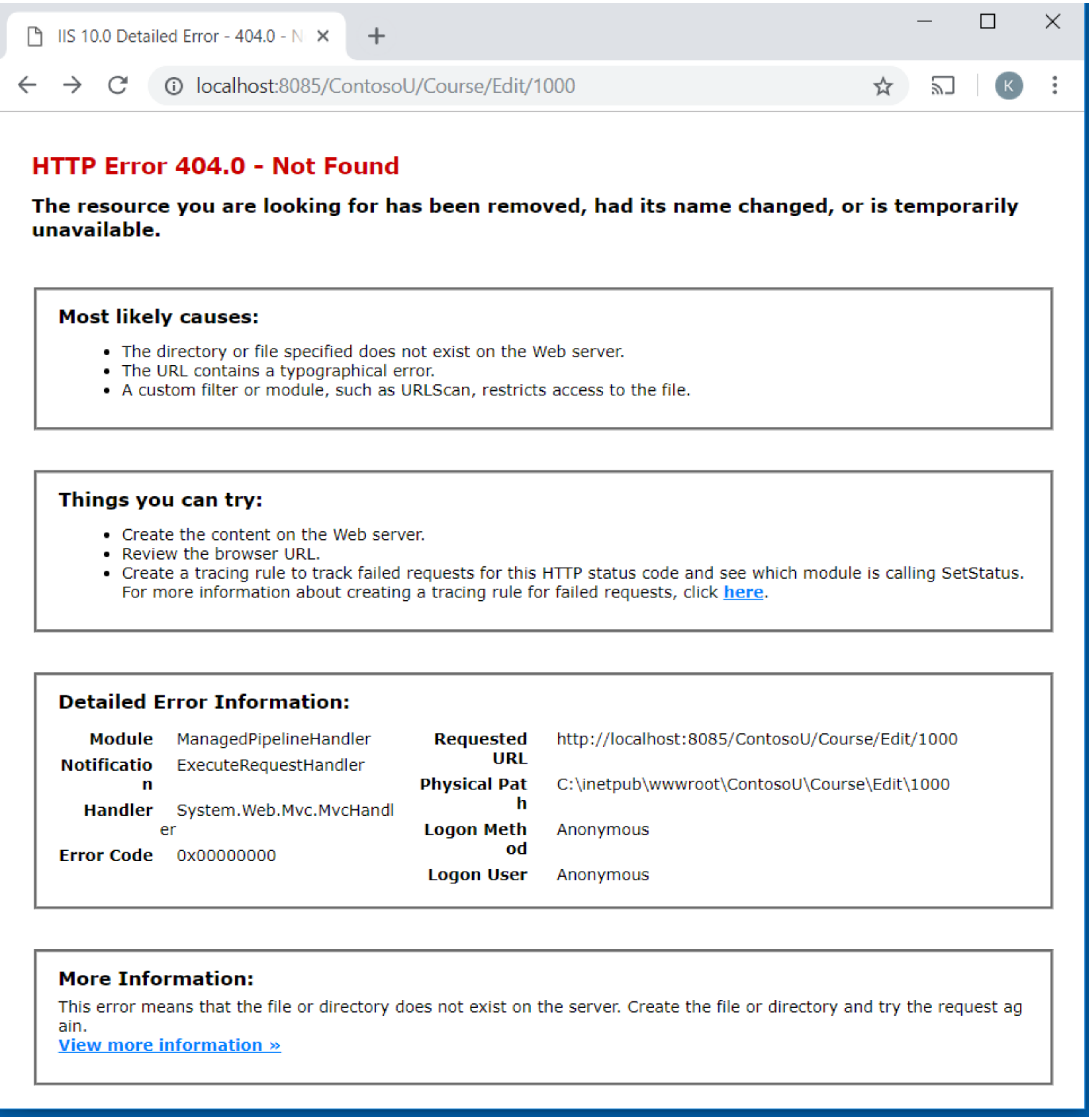
Update Course Credits

Number of rows updated: 29

Back to List

© 2018 - Contoso University




IIS 10.0 Detailed Error - 404.0 - N
localhost:8085/ContosoU/Course/Edit/1000

HTTP Error 404.0 - Not Found

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.

Most likely causes:

- The directory or file specified does not exist on the Web server.
- The URL contains a typographical error.
- A custom filter or module, such as URLScan, restricts access to the file.

Things you can try:

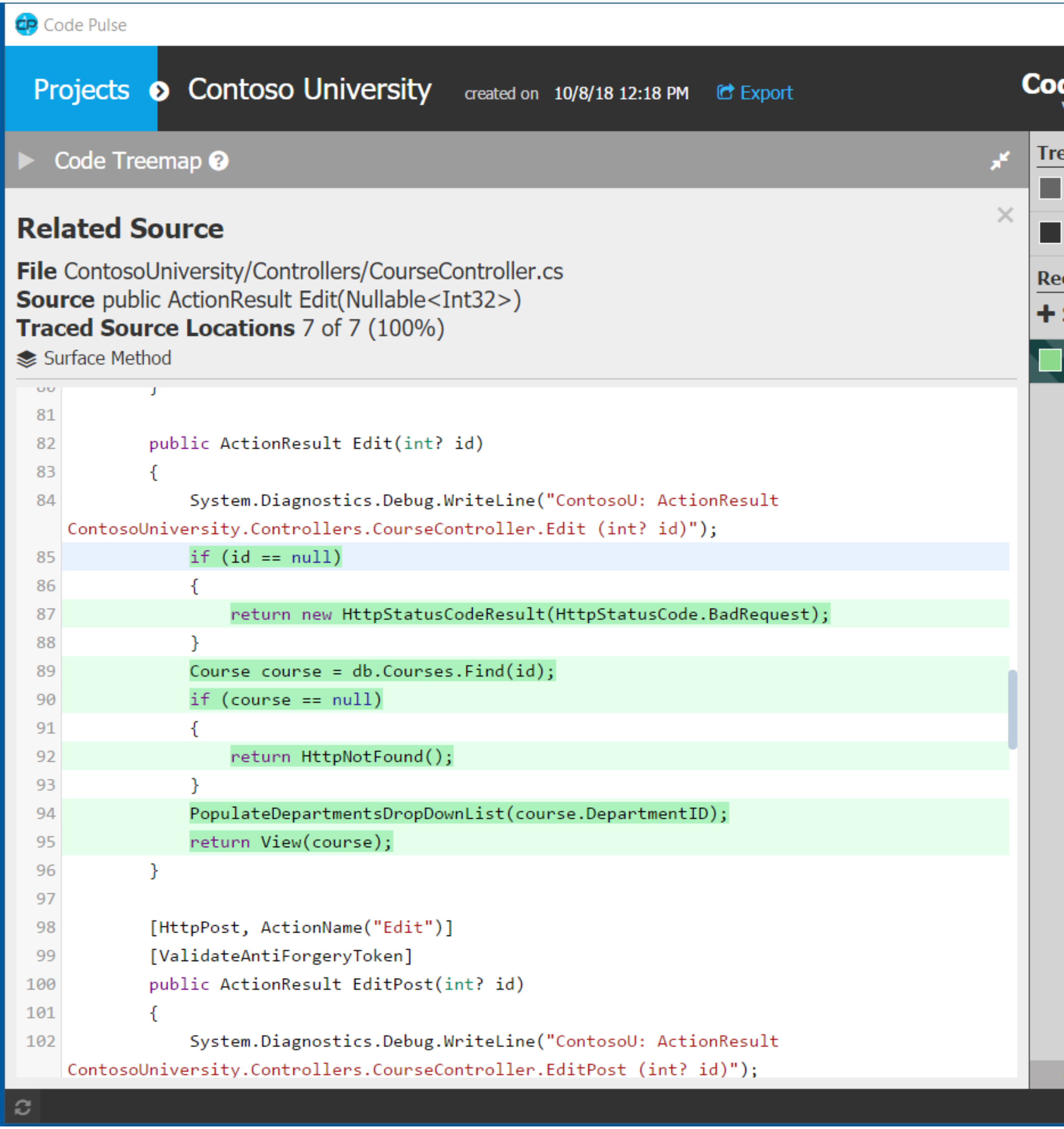
- Create the content on the Web server.
- Review the browser URL.
- Create a tracing rule to track failed requests for this HTTP status code and see which module is calling SetStatus. For more information about creating a tracing rule for failed requests, click here.

Detailed Error Information:

Module	ManagedPipelineHandler	**Requested URL**	http://localhost:8085/ContosoU/Course/Edit/1000
Notification	ExecuteRequestHandler	**Physical Path**	C:\inetpub\wwwroot\ContosoU\Course\Edit\1000
Handler	System.Web.Mvc.MvcHandler	**Logon Method**	Anonymous
Error Code	0x00000000	**Logon User**	Anonymous

More Information:

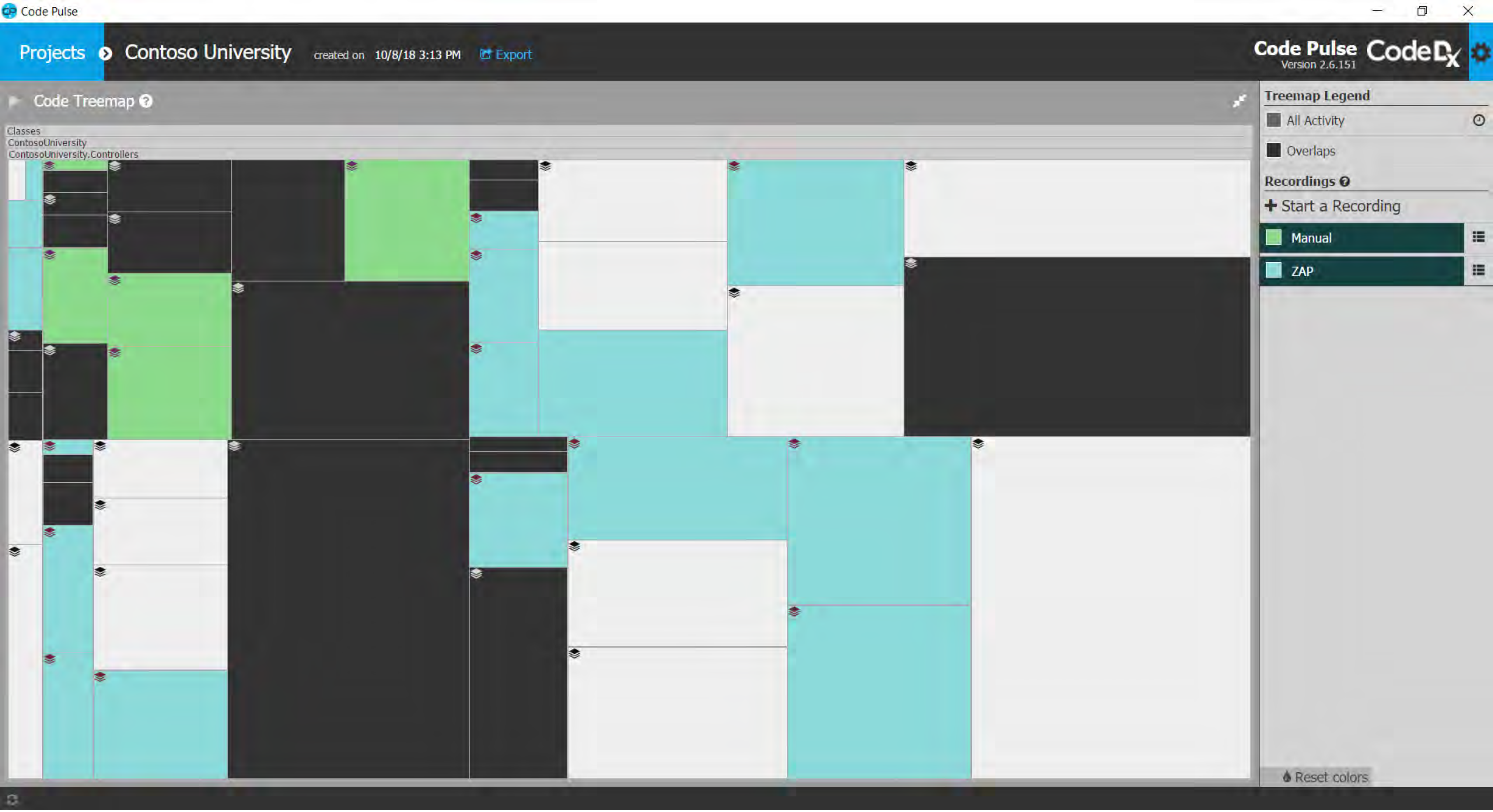
This error means that the file or directory does not exist on the server. Create the file or directory and try the request again.
View more information »

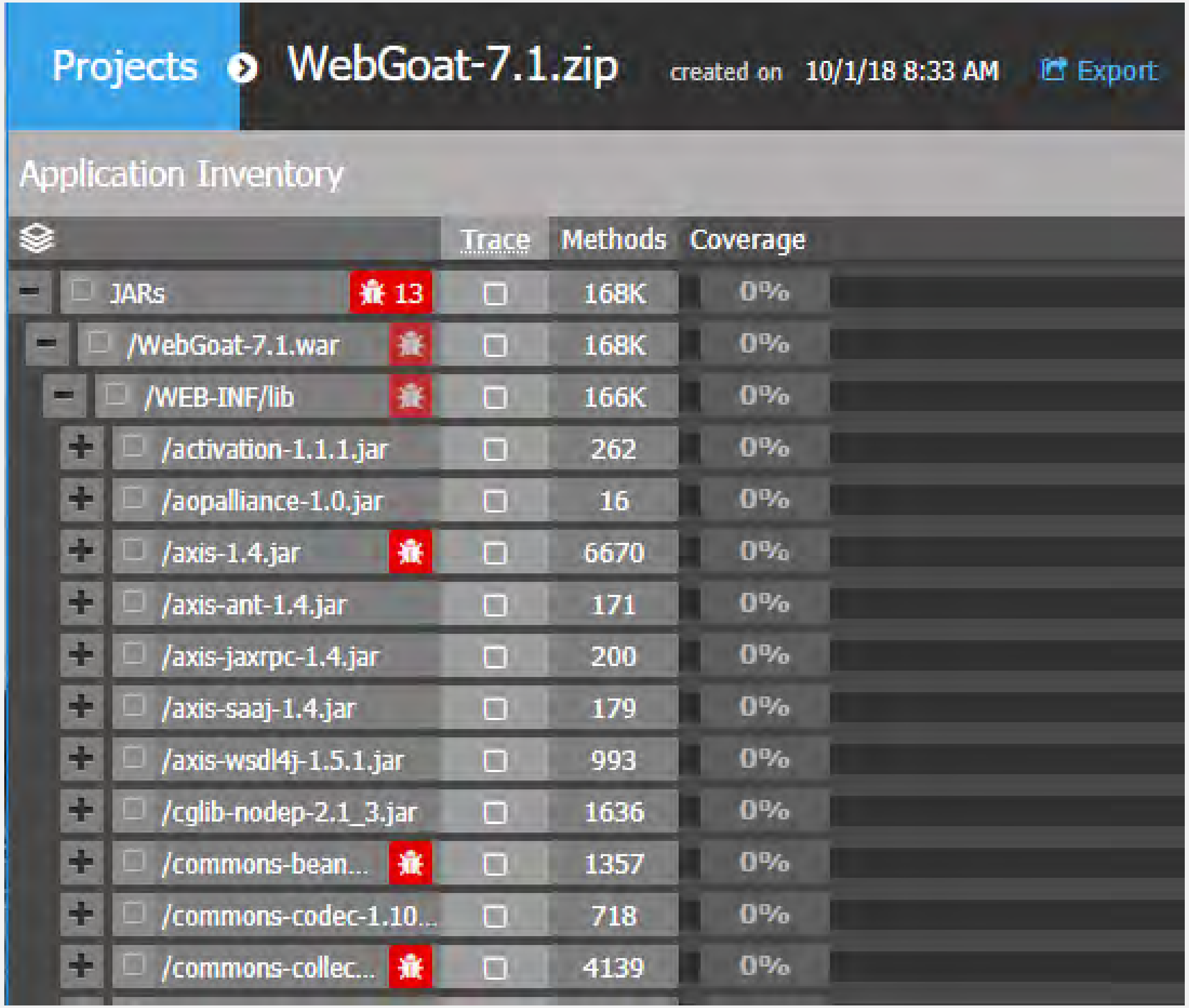


Related Source

File ContosoUniversity/Controllers/CourseController.cs
Source public ActionResult Edit(Nullable<Int32>)
Traced Source Locations 7 of 7 (100%)
Surface Method

```
        }

        public ActionResult Edit(int? id)
        {
            System.Diagnostics.Debug.WriteLine("ContosoU: ActionResult ContosoUniversity.Controllers.CourseController.Edit (int? id)");
            if (id == null)
            {
                return new HttpStatusCodeResult(HttpStatusCode.BadRequest);
            }
            Course course = db.Courses.Find(id);
            if (course == null)
            {
                return HttpNotFound();
            }
            PopulateDepartmentsDropDownList(course.DepartmentID);
            return View(course);
        }

        [HttpPost, ActionName("Edit")]
        [ValidateAntiForgeryToken]
        public ActionResult EditPost(int? id)
        {
            System.Diagnostics.Debug.WriteLine("ContosoU: ActionResult ContosoUniversity.Controllers.CourseController.EditPost (int? id)");
```

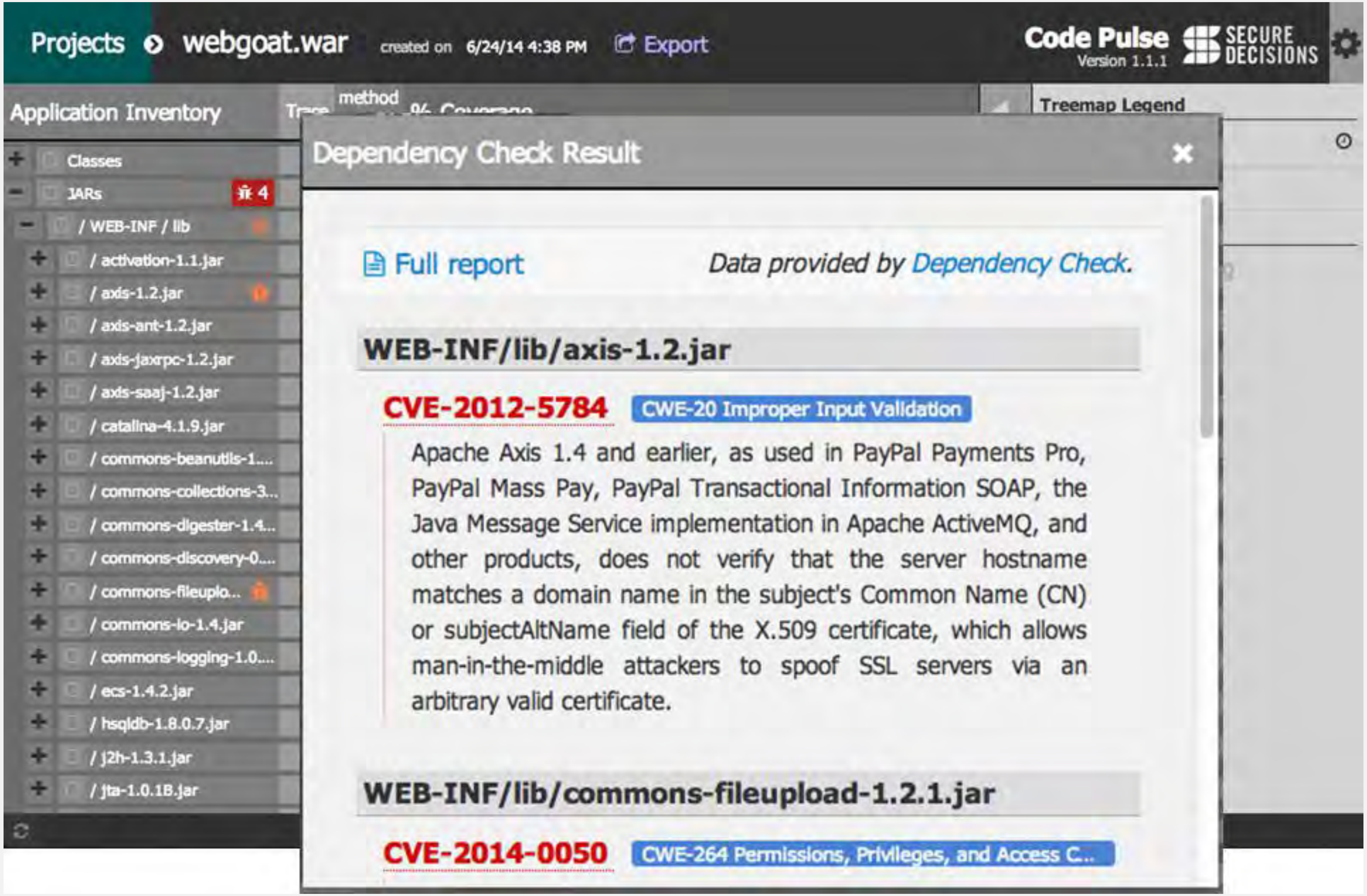

Code Pulse
Projects
Contoso University
created on 10/8/18 3:13 PM
Export
Code Pulse
Version 2.6.151
CodeDx
Code Treemap
Classes
ContosoUniversity
ContosoUniversity.Controllers
Treemap Legend
All Activity
Overlaps
Recordings
Start a Recording
Manual
ZAP
Reset colors



WebGoat-7.1.zip created on 10/1/18 8:33 AM

Application Inventory

	Trace	Methods	Coverage
− □ JARs 🐞 13	□	168K	0%
− □ /WebGoat-7.1.war 🐞	□	168K	0%
− □ /WEB-INF/lib 🐞	□	166K	0%
+ □ /activation-1.1.1.jar	□	262	0%
+ □ /aopalliance-1.0.jar	□	16	0%
+ □ /axis-1.4.jar 🐞	□	6670	0%
+ □ /axis-ant-1.4.jar	□	171	0%
+ □ /axis-jaxrpc-1.4.jar	□	200	0%
+ □ /axis-saaj-1.4.jar	□	179	0%
+ □ /axis-wsdl4j-1.5.1.jar	□	993	0%
+ □ /cglib-nodep-2.1_3.jar	□	1636	0%
+ □ /commons-bean... 🐞	□	1357	0%
+ □ /commons-codec-1.10...	□	718	0%
+ □ /commons-collec... 🐞	□	4139	0%



Dependency Check Result

Full report

Data provided by Dependency Check.

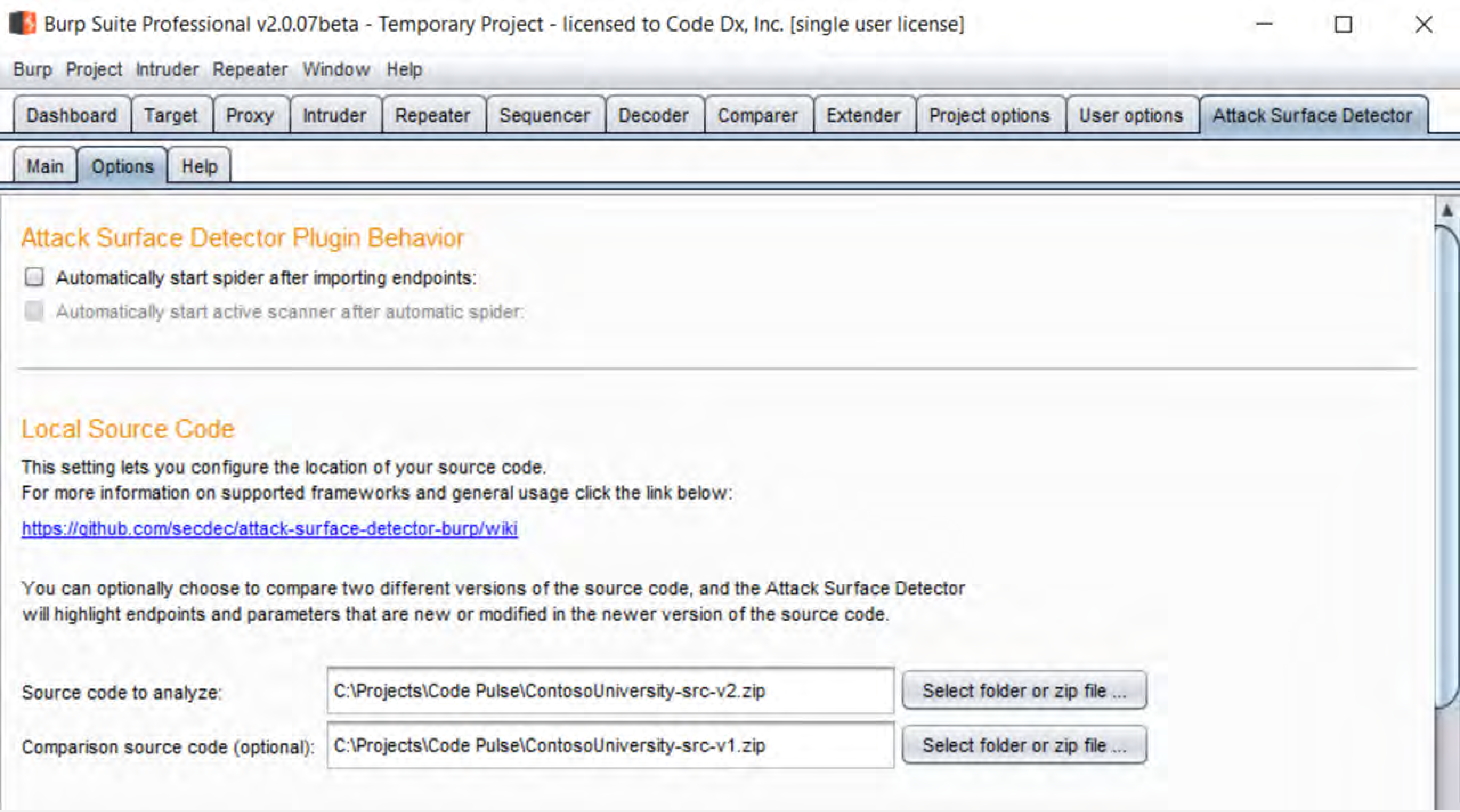
WEB-INF/lib/axis-1.2.jar

CVE-2012-5784 CWE-20 Improper Input Validation

Apache Axis 1.4 and earlier, as used in PayPal Payments Pro, PayPal Mass Pay, PayPal Transactional Information SOAP, the Java Message Service implementation in Apache ActiveMQ, and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

WEB-INF/lib/commons-fileupload-1.2.1.jar

CVE-2014-0050 CWE-264 Permissions, Privileges, and Access C...


Burp Suite Professional v2.0.07beta - Temporary Project - licensed to Code Dx, Inc. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Attack Surface Detector
Main Options Help

Attack Surface Detector Plugin Behavior

□ Automatically start spider after importing endpoints:

□ Automatically start active scanner after automatic spider:

Local Source Code

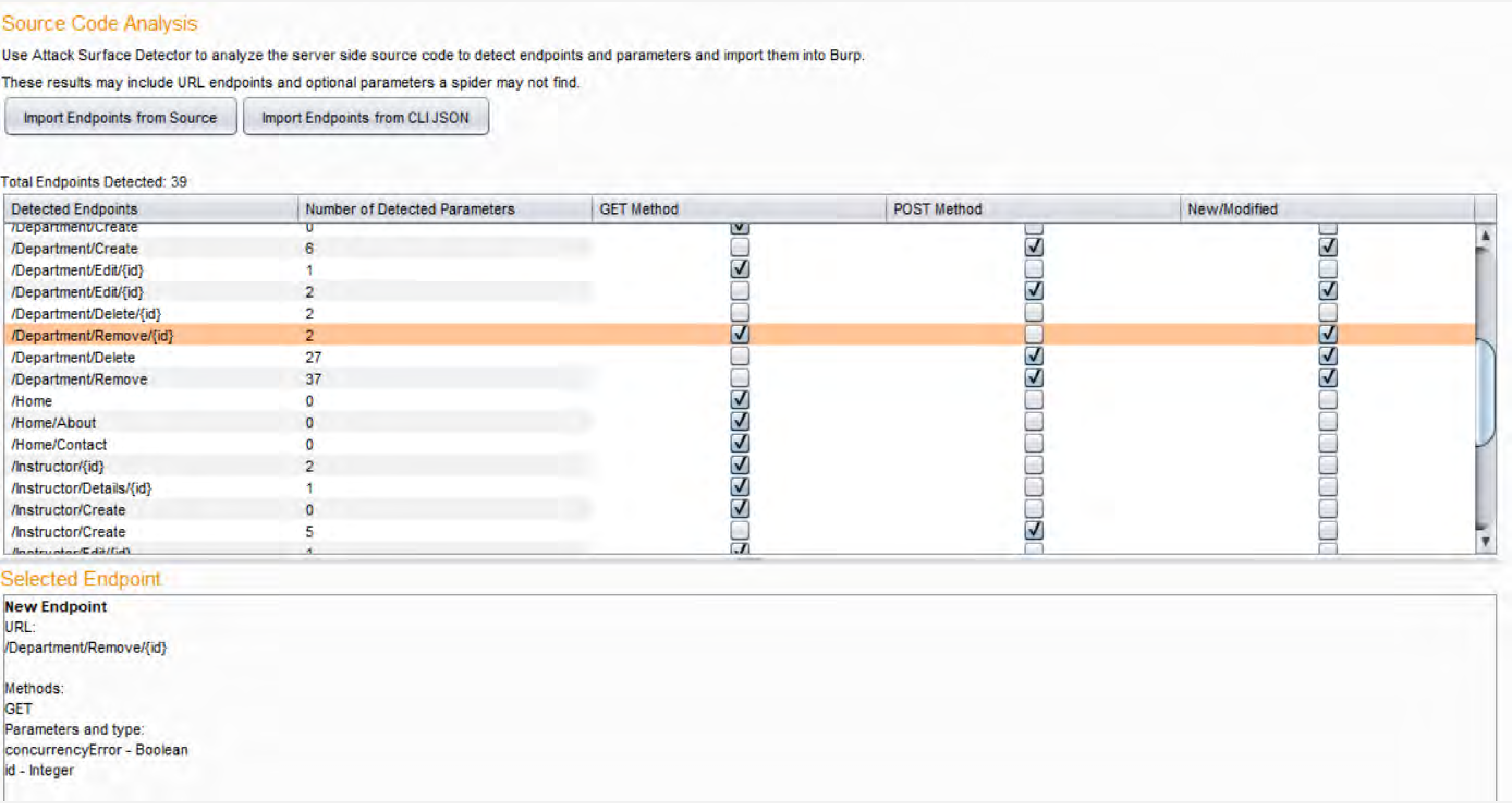
This setting lets you configure the location of your source code.
For more information on supported frameworks and general usage click the link below:

https://github.com/secdec/attack-surface-detector-burp/wiki

You can optionally choose to compare two different versions of the source code, and the Attack Surface Detector will highlight endpoints and parameters that are new or modified in the newer version of the source code.

Source code to analyze: C:\Projects\Code Pulse\ContosoUniversity-src-v2.zip [Select folder or zip file ...]

Comparison source code (optional): C:\Projects\Code Pulse\ContosoUniversity-src-v1.zip [Select folder or zip file ...]



Source Code Analysis

Use Attack Surface Detector to analyze the server side source code to detect endpoints and parameters and import them into Burp.

These results may include URL endpoints and optional parameters a spider may not find.

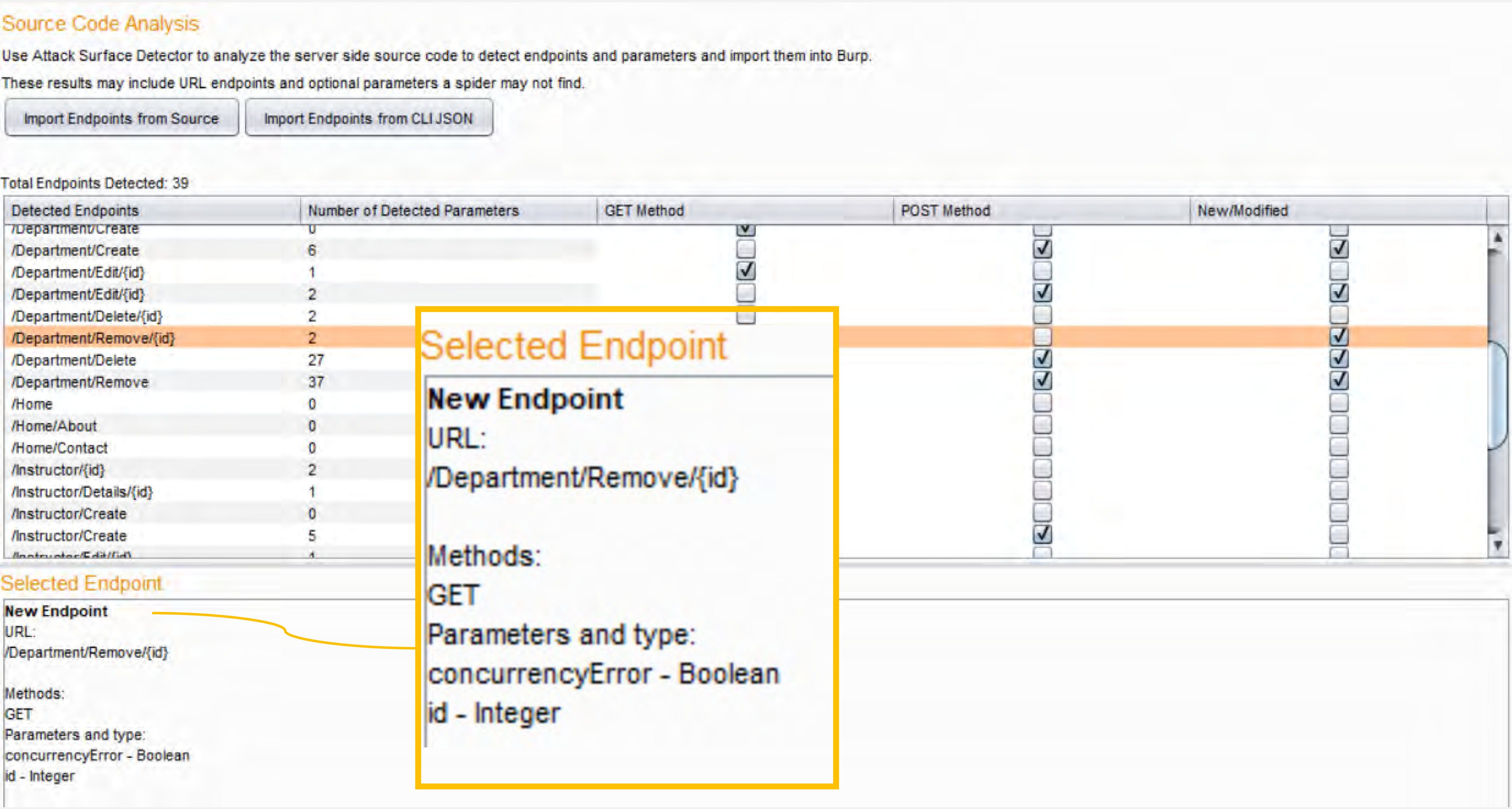
Total Endpoints Detected: 39

Detected Endpoints	Number of Detected Parameters	GET Method	POST Method	New/Modified
/Department/Create	0	☑	□	□
/Department/Create	6	□	☑	☑
/Department/Edit/{id}	1	☑	□	□
/Department/Edit/{id}	2	□	☑	☑
/Department/Delete/{id}	2	□	□	□
/Department/Remove/{id}	2	☑	□	☑
/Department/Delete	27	□	☑	☑
/Department/Remove	37	□	☑	☑
/Home	0	☑	□	□
/Home/About	0	☑	□	□
/Home/Contact	0	☑	□	□
/Instructor/{id}	2	☑	□	□
/Instructor/Details/{id}	1	☑	□	□
/Instructor/Create	0	☑	□	□
/Instructor/Create	5	□	☑	□
/Instructor/Edit/{id}	1	☑	□	□

Selected Endpoint

New Endpoint
URL:
/Department/Remove/{id}

Methods:
GET
Parameters and type:
concurrencyError - Boolean
id - Integer



Source Code Analysis

Use Attack Surface Detector to analyze the server side source code to detect endpoints and parameters and import them into Burp.

These results may include URL endpoints and optional parameters a spider may not find.

Total Endpoints Detected: 39

Detected Endpoints	Number of Detected Parameters	GET Method	POST Method	New/Modified
/Department/Create	0	☑	□	□
/Department/Create	6	□	☑	☑
/Department/Edit/{id}	1	☑	□	□
/Department/Edit/{id}	2	□	☑	☑
/Department/Delete/{id}	2	□	□	□
/Department/Remove/{id}	2		□	☑
/Department/Delete	27		☑	☑
/Department/Remove	37		☑	☑
/Home	0		□	□
/Home/About	0		□	□
/Home/Contact	0		□	□
/Instructor/{id}	2		□	□
/Instructor/Details/{id}	1		□	□
/Instructor/Create	0		□	□
/Instructor/Create	5		☑	□
/Instructor/Edit/{id}	1		□	□

Selected Endpoint

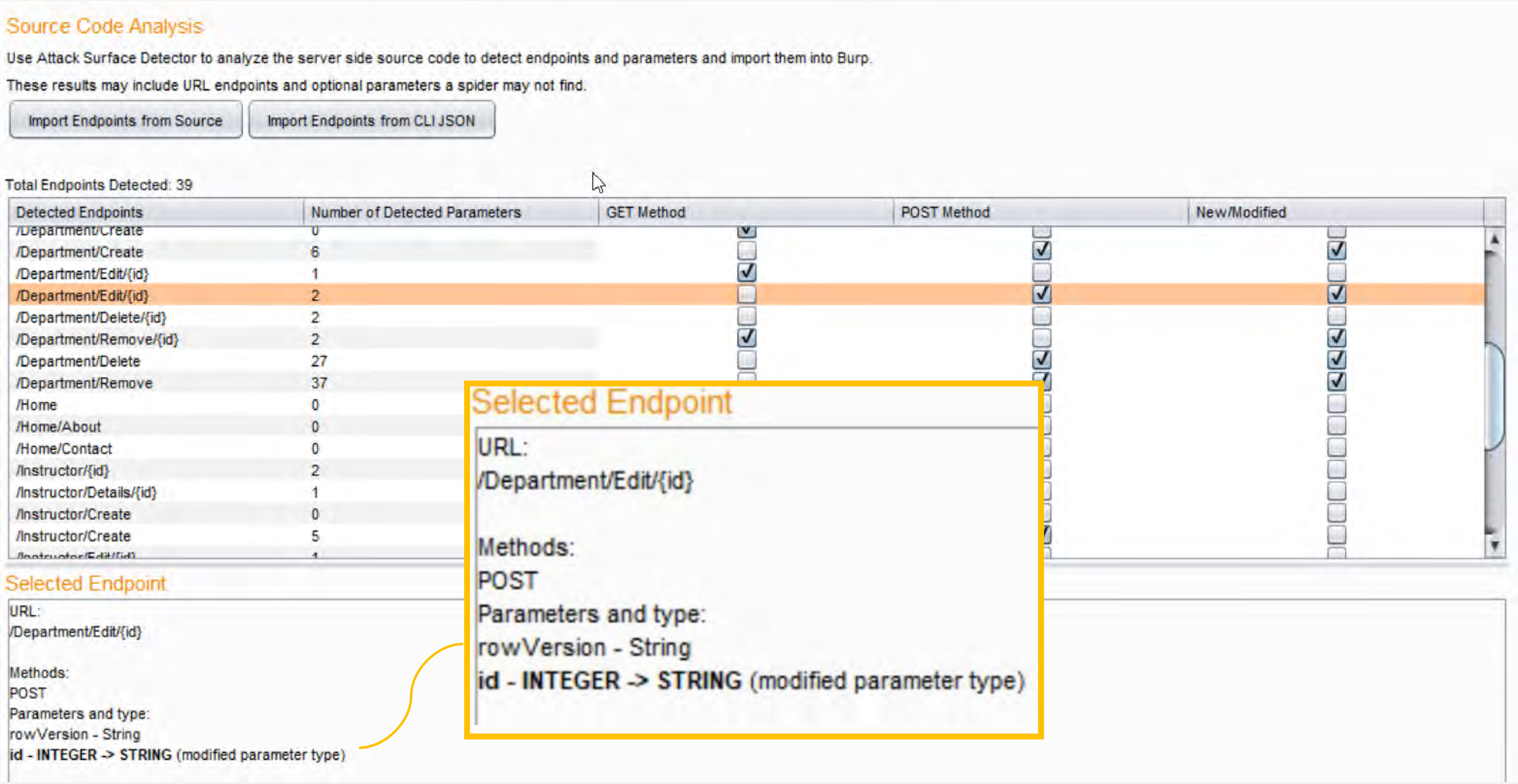
New Endpoint
URL:
/Department/Remove/{id}

Methods:
GET
Parameters and type:
concurrencyError - Boolean
id - Integer

Selected Endpoint

New Endpoint
URL:
/Department/Remove/{id}

Methods:
GET
Parameters and type:
concurrencyError - Boolean
id - Integer



Source Code Analysis

Use Attack Surface Detector to analyze the server side source code to detect endpoints and parameters and import them into Burp.

These results may include URL endpoints and optional parameters a spider may not find.

Total Endpoints Detected: 39

Detected Endpoints	Number of Detected Parameters	GET Method	POST Method	New/Modified
/Department/Create	0	☑	□	□
/Department/Create	6	□	☑	☑
/Department/Edit/{id}	1	☑	□	□
/Department/Edit/{id}	2	□	☑	☑
/Department/Delete/{id}	2	□	□	□
/Department/Remove/{id}	2	☑	□	☑
/Department/Delete	27	□	☑	☑
/Department/Remove	37	□	☑	☑
/Home	0			□
/Home/About	0			□
/Home/Contact	0			□
/Instructor/{id}	2			□
/Instructor/Details/{id}	1			□
/Instructor/Create	0			□
/Instructor/Create	5		☑	□
/Instructor/Edit/{id}	1			□

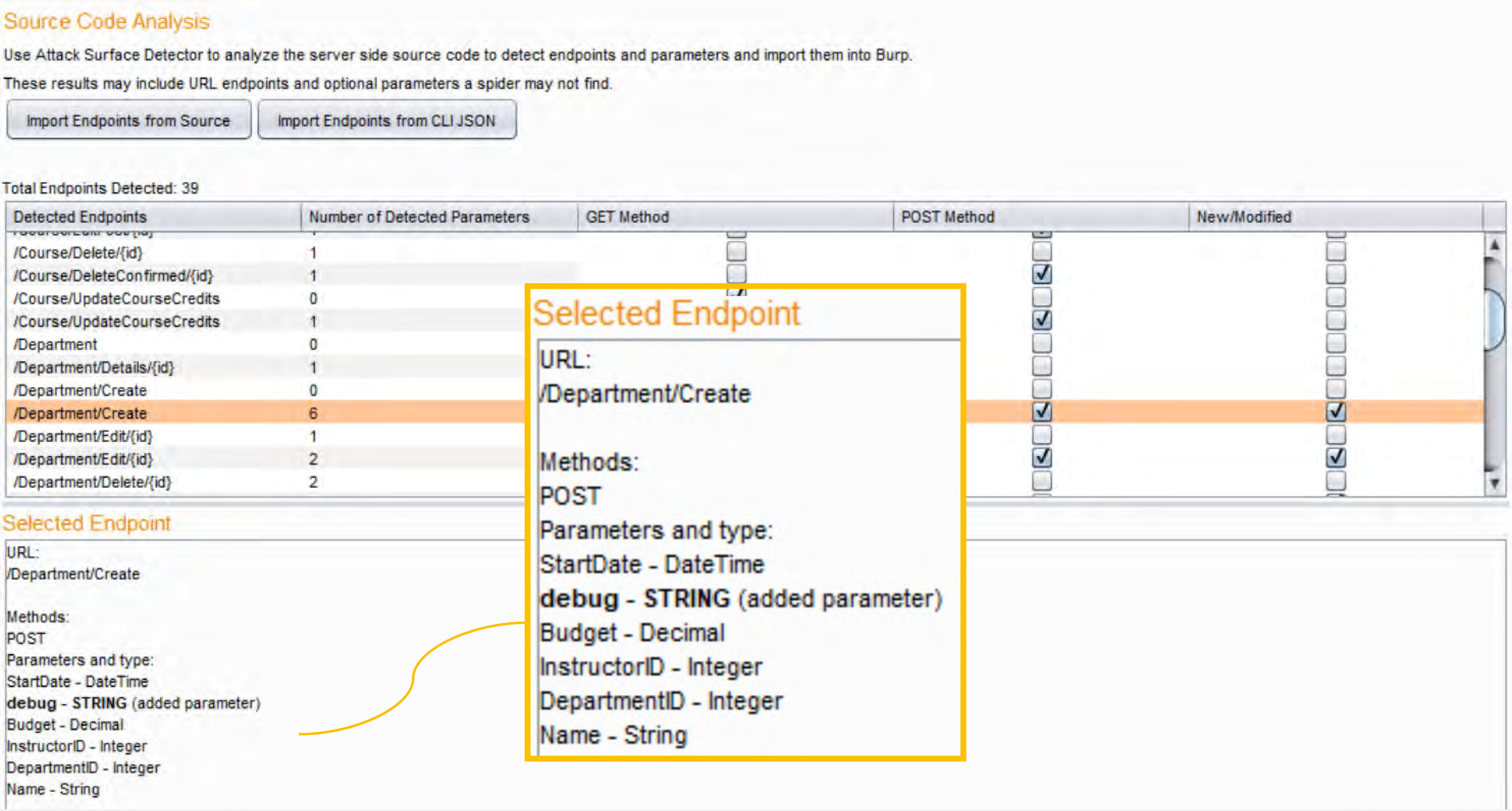
Selected Endpoint

URL:
/Department/Edit/{id}

Methods:
POST
Parameters and type:
rowVersion - String
id - INTEGER -> STRING (modified parameter type)

Selected Endpoint
URL:
/Department/Edit/{id}

Methods:
POST
Parameters and type:
rowVersion - String
id - INTEGER -> STRING (modified parameter type)



Source Code Analysis

Use Attack Surface Detector to analyze the server side source code to detect endpoints and parameters and import them into Burp.

These results may include URL endpoints and optional parameters a spider may not find.

Total Endpoints Detected: 39

Detected Endpoints	Number of Detected Parameters	GET Method	POST Method	New/Modified
/Course/Delete/{id}	1	□	□	□
/Course/DeleteConfirmed/{id}	1	□	☑	□
/Course/UpdateCourseCredits	0	☑	□	□
/Course/UpdateCourseCredits	1		☑	□
/Department	0		□	□
/Department/Details/{id}	1		□	□
/Department/Create	0		□	□
/Department/Create	6		☑	☑
/Department/Edit/{id}	1		□	□
/Department/Edit/{id}	2		☑	☑
/Department/Delete/{id}	2		□	□

Selected Endpoint

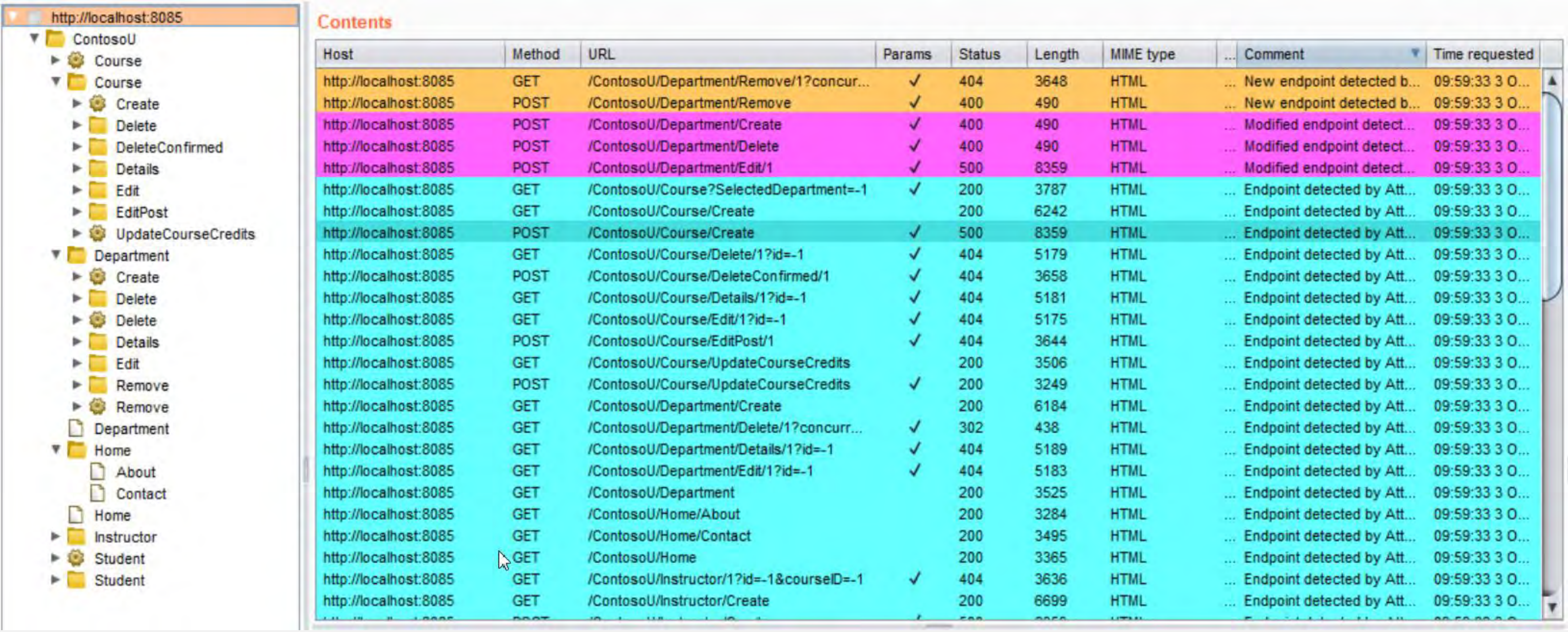
URL:
/Department/Create

Methods:
POST
Parameters and type:
StartDate - DateTime
debug - STRING (added parameter)
Budget - Decimal
InstructorID - Integer
DepartmentID - Integer
Name - String

Selected Endpoint

URL:
/Department/Create

Methods:
POST
Parameters and type:
StartDate - DateTime
debug - STRING (added parameter)
Budget - Decimal
InstructorID - Integer
DepartmentID - Integer
Name - String



- http://localhost:8085
  - ContosoU
    - Course
    - Course
      - Create
      - Delete
      - DeleteConfirmed
      - Details
      - Edit
      - EditPost
      - UpdateCourseCredits
    - Department
      - Create
      - Delete
      - Delete
      - Details
      - Edit
      - Remove
      - Remove
    - Department
    - Home
      - About
      - Contact
    - Home
    - Instructor
    - Student
    - Student

Contents

Host	Method	URL	Params	Status	Length	MIME type	...	Comment	Time requested
http://localhost:8085	GET	/ContosoU/Department/Remove/1?concur...	✓	404	3648	HTML	...	New endpoint detected b...	09:59:33 3 O...
http://localhost:8085	POST	/ContosoU/Department/Remove	✓	400	490	HTML	...	New endpoint detected b...	09:59:33 3 O...
http://localhost:8085	POST	/ContosoU/Department/Create	✓	400	490	HTML	...	Modified endpoint detect...	09:59:33 3 O...
http://localhost:8085	POST	/ContosoU/Department/Delete	✓	400	490	HTML	...	Modified endpoint detect...	09:59:33 3 O...
http://localhost:8085	POST	/ContosoU/Department/Edit/1	✓	500	8359	HTML	...	Modified endpoint detect...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Course?SelectedDepartment=-1	✓	200	3787	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Course/Create		200	6242	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	POST	/ContosoU/Course/Create	✓	500	8359	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Course/Delete/1?id=-1	✓	404	5179	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	POST	/ContosoU/Course/DeleteConfirmed/1	✓	404	3658	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Course/Details/1?id=-1	✓	404	5181	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Course/Edit/1?id=-1	✓	404	5175	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	POST	/ContosoU/Course/EditPost/1	✓	404	3644	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Course/UpdateCourseCredits		200	3506	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	POST	/ContosoU/Course/UpdateCourseCredits	✓	200	3249	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Department/Create		200	6184	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Department/Delete/1?concurr...	✓	302	438	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Department/Details/1?id=-1	✓	404	5189	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Department/Edit/1?id=-1	✓	404	5183	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Department		200	3525	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Home/About		200	3284	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Home/Contact		200	3495	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Home		200	3365	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Instructor/1?id=-1&courseID=-1	✓	404	3636	HTML	...	Endpoint detected by Att...	09:59:33 3 O...
http://localhost:8085	GET	/ContosoU/Instructor/Create		200	6699	HTML	...	Endpoint detected by Att...	09:59:33 3 O...