

Open Source SAST and DAST Tools for WebApp Pen Testing

Drew Kirkpatrick



Funded by:

Department of Homeland Security
Science and Technology Directorate
Cyber Security Division

Web Application Pen Testing

White Hats have plenty of disadvantages over their malicious counterparts

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

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

Open Source Tools for White Hats



OWASP Code Pulse – Provides insight into the real-time code coverage of black box testing activities by monitoring the execution of the web application



Attack Surface Detector – Performs static code analysis of a web application to detect the application endpoints, parameters, and parameter datatypes, and makes that data available in Burp Suite and OWASP ZAP



Code Pulse

 Code Pulse an  OWASP project

https://owasp.org/index.php/OWASP_Code_Pulse_Project

Code Pulse Need

Coverage gaps – by definition, penetration testing is typically a purely black box perspective, which makes it almost impossible to ascertain the attack surface coverage gaps

Test tuning – DAST tools are tricky to configure, due to the complex variations in the target applications. Manual testers have challenges tying web requests to the underlying source code.

Coverage data communication – lack of coverage insight from the black box perspective makes this currently challenging, and comparing testing tools and techniques difficult

How Code Pulse Works

Leverages Java and .NET instrumentation libraries to provide real-time measurement of application method calls

- JVM Code Pulse agent runs in the same JVM as the target application
- .NET Code Pulse tracer based on OpenCover code coverage tool

Instruments server bytecode—no changes in source code are needed

Sends method coverage to Code Pulse client for real-time visualization

Code Pulse Benefit

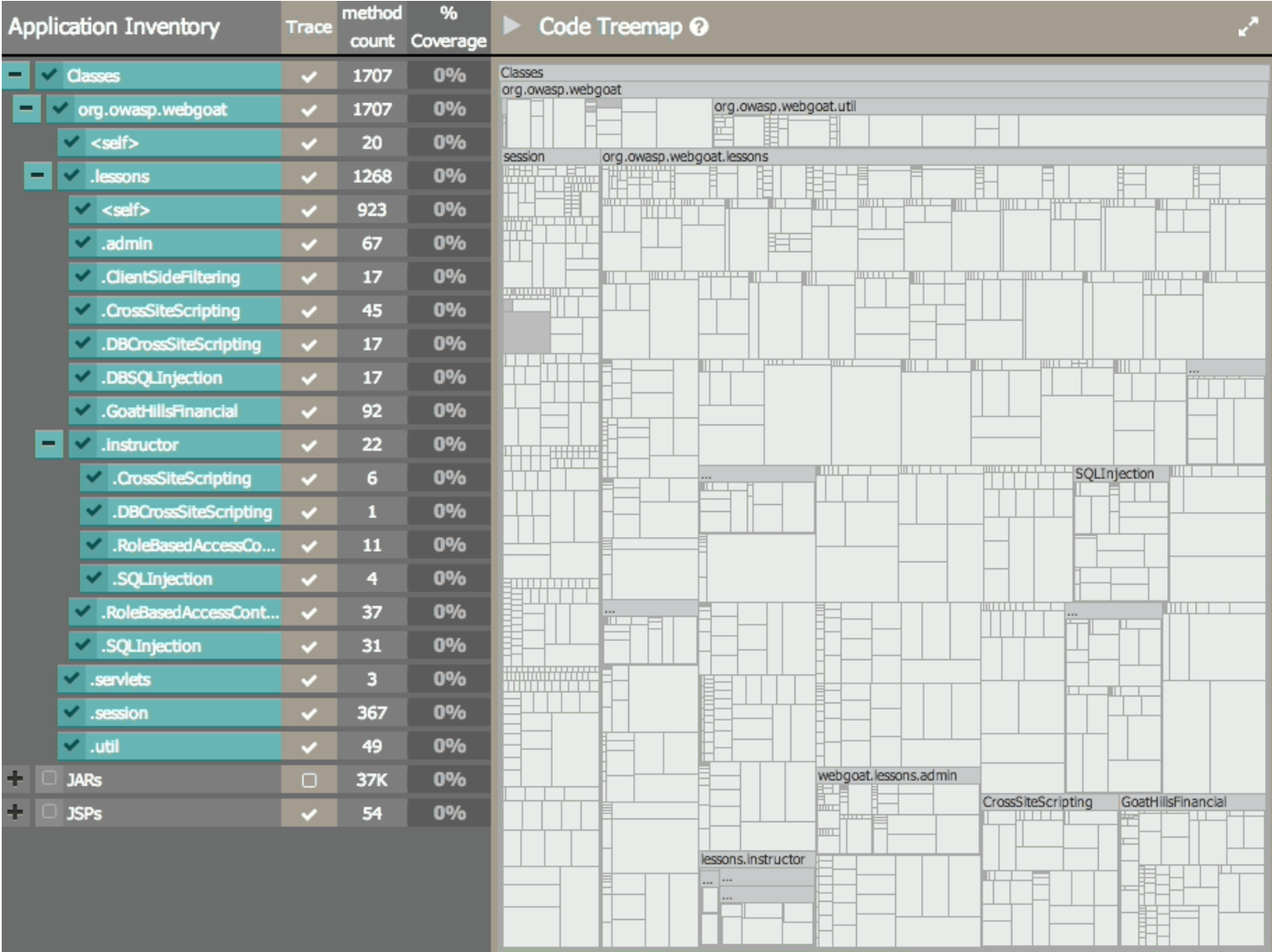
Helps web application testers associate the endpoints they interact with to the underlying classes and methods called in the application server

Find gaps in the test coverage

Allows comparison and tuning of dynamic testing tools and techniques

Percentage of code coverage is a useful metric for communicating testing activity

Code Pulse Screenshot



Future Code Pulse Plans

Provide line-level code display in Code Pulse

- Will allow more accurate measurement of code coverage
- Will simplify code review

Better integration of attack surface detection

- Display specific endpoints to access methods visualized in Code Pulse

Attack Surface Detector



Attack Surface Detector Need

Attack surface gaps – black box testing by penetration testers can miss unlinked endpoints without extensive endpoint brute forcing

Parameter detection – Identifying optional parameters during a black box test can be time-consuming and often miss valid parameters that affect execution of the software

Enumeration effort – Manual penetration testing is costly, and the available time may not allow for thorough enumeration of an application's attack surface

How the Attack Surface Detector Works

Static code analysis identifies web application endpoints by parsing routes and identifying parameters in the supported languages and frameworks

Multiple parsers are needed in order to support different languages and frameworks

Supported Frameworks:

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

Attack Surface Detector Benefit

Provides a faster and more thorough enumeration of a web application's attack surface

Detects the endpoints of a web application, the parameters, and parameter data types, including:

- Unlinked endpoints a spider won't find in client side code
- Optional parameters never used in the client side code

Imports this data into Burp Suite and OWASP ZAP to use during assessment

Pre-seeding in Burp Suite

Source Code Analysis

Use Attack Surface Detector to analyze the server side source code to detect endpoints and parameters. 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
/redirect/uriTemplate	0	
/async/callable/response-body	0	
/async/callable/custom-timeout-handling	0	
/messageconverters/string	0	
/messageconverters/string	0	
/async/deferred-result/exception	0	
/form	8	
/form	0	
/mapping/path	0	
/views/*/pathVariables/{foo}/{fruit}	2	
/data/param	1	
/data/group	0	
/data/body	0	
/data/path/{var}	1	
/data/standard/response/writer	0	

Selected Endpoint

URL:
/views/*/pathVariables/{foo}/{fruit}

Methods:
GET

Parameters and type:
fruit - String
foo - String

Future Attack Surface Detector Plans

Ability to analyze zip files of source code

Attack Surface Difference Generator

- Endpoints and parameters that are new or modified between two different versions of software will be detected
- This “difference” in attack surface will be imported into Burp Suite and OWASP ZAPS

Enough! Just show me already



LIVE DEMO



Contacts and Source Code

Drew Kirkpatrick

drew.kirkpatrick@owasp.org

twitter.com/hoodoer

info@securedecisions.com

GITHUB LINKS

Attack Surface Detector plugin for Burp Suite

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

Attack Surface Detector plugin for OWASP ZAP

<https://github.com/secdec/attack-surface-detector-zap>

OWASP Code Pulse real-time code coverage monitor

<https://github.com/secdec/codepulse>



QUESTIONS?

Plan B – Backup slides





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.

Projects ▶ Contoso University

created on 4/12/18 11:33 AM

[Export](#)

Application Inventory	Trace	method count	% Coverage	
- <input type="checkbox"/> Classes	<input checked="" type="checkbox"/> 0	1198	<input type="checkbox"/> 0%	
+ <input type="checkbox"/> Antr.Runtime	<input checked="" type="checkbox"/>	898	<input type="checkbox"/> 0%	
- <input type="checkbox"/> ContosoUniversity	<input checked="" type="checkbox"/>	300	<input type="checkbox"/> 0%	
<input type="checkbox"/> <self>	<input checked="" type="checkbox"/>	6	<input type="checkbox"/> 0%	
<input type="checkbox"/> .Controllers	<input checked="" type="checkbox"/>	54	<input type="checkbox"/> 0%	
<input type="checkbox"/> .DAL	<input checked="" type="checkbox"/>	34	<input type="checkbox"/> 0%	
<input type="checkbox"/> .Logging	<input checked="" type="checkbox"/>	13	<input type="checkbox"/> 0%	
<input type="checkbox"/> .Migrations	<input checked="" type="checkbox"/>	112	<input type="checkbox"/> 0%	
<input type="checkbox"/> .Models	<input checked="" type="checkbox"/>	65	<input type="checkbox"/> 0%	
<input type="checkbox"/> .ViewModels	<input checked="" type="checkbox"/>	16	<input type="checkbox"/> 0%	

Treemap Legend

- All Activity
- Overlaps

Recordings

+ Start a Recording

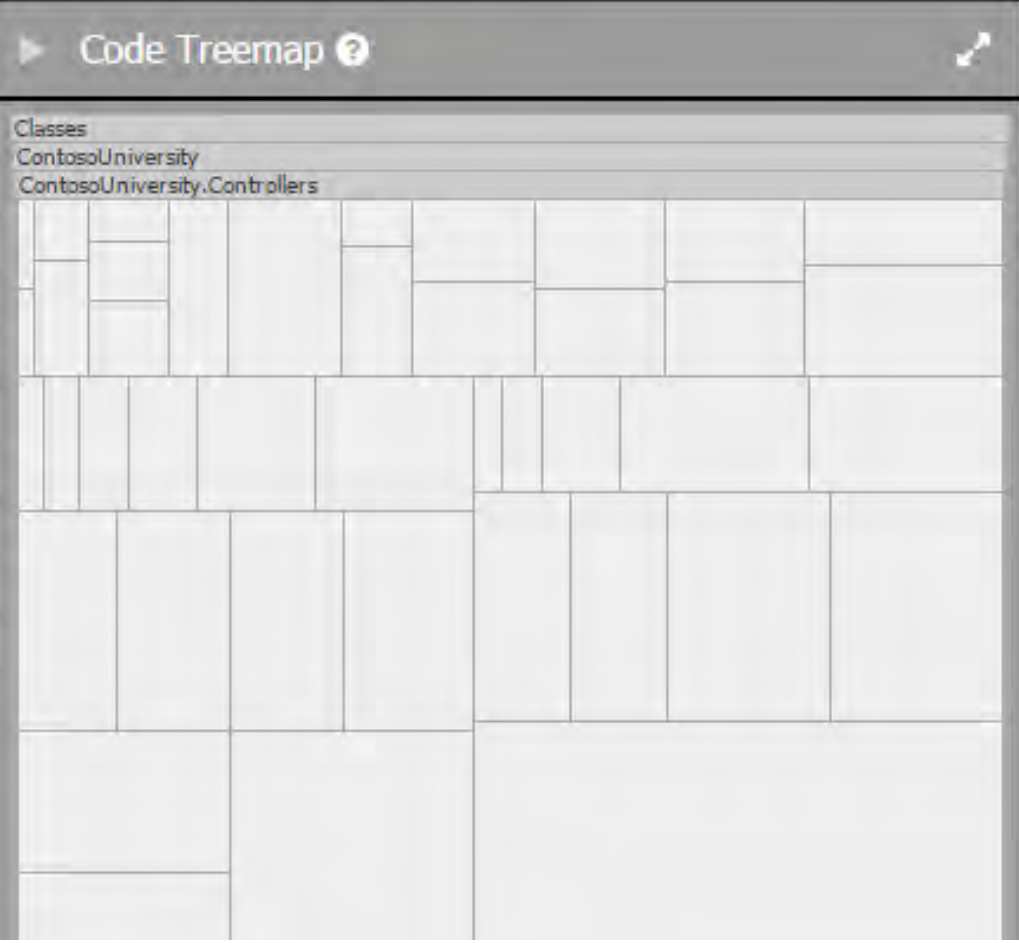
Projects ▶ Contoso University

created on 4/12/18 11:33 AM

[Export](#)

Code

Application Inventory	Trace	method count	% Coverage
<input checked="" type="checkbox"/> Classes ★ 0	<input checked="" type="checkbox"/>	1198	0%
<input type="checkbox"/> Antlr.Runtime	<input checked="" type="checkbox"/>	898	0%
<input checked="" type="checkbox"/> ContosoUniversity	<input checked="" type="checkbox"/>	300	0%
<input type="checkbox"/> <self>	<input checked="" type="checkbox"/>	6	0%
<input checked="" type="checkbox"/> .Controllers	<input checked="" type="checkbox"/>	54	0%
<input type="checkbox"/> .DAL	<input checked="" type="checkbox"/>	34	0%
<input type="checkbox"/> .Logging	<input checked="" type="checkbox"/>	13	0%
<input type="checkbox"/> .Migrations	<input checked="" type="checkbox"/>	112	0%
<input type="checkbox"/> .Models	<input checked="" type="checkbox"/>	65	0%
<input type="checkbox"/> .ViewModels	<input checked="" type="checkbox"/>	16	0%



Treemap controls and navigation elements.

- Treemap icon
- Refresh icon
- Zoom controls
- Reset icon

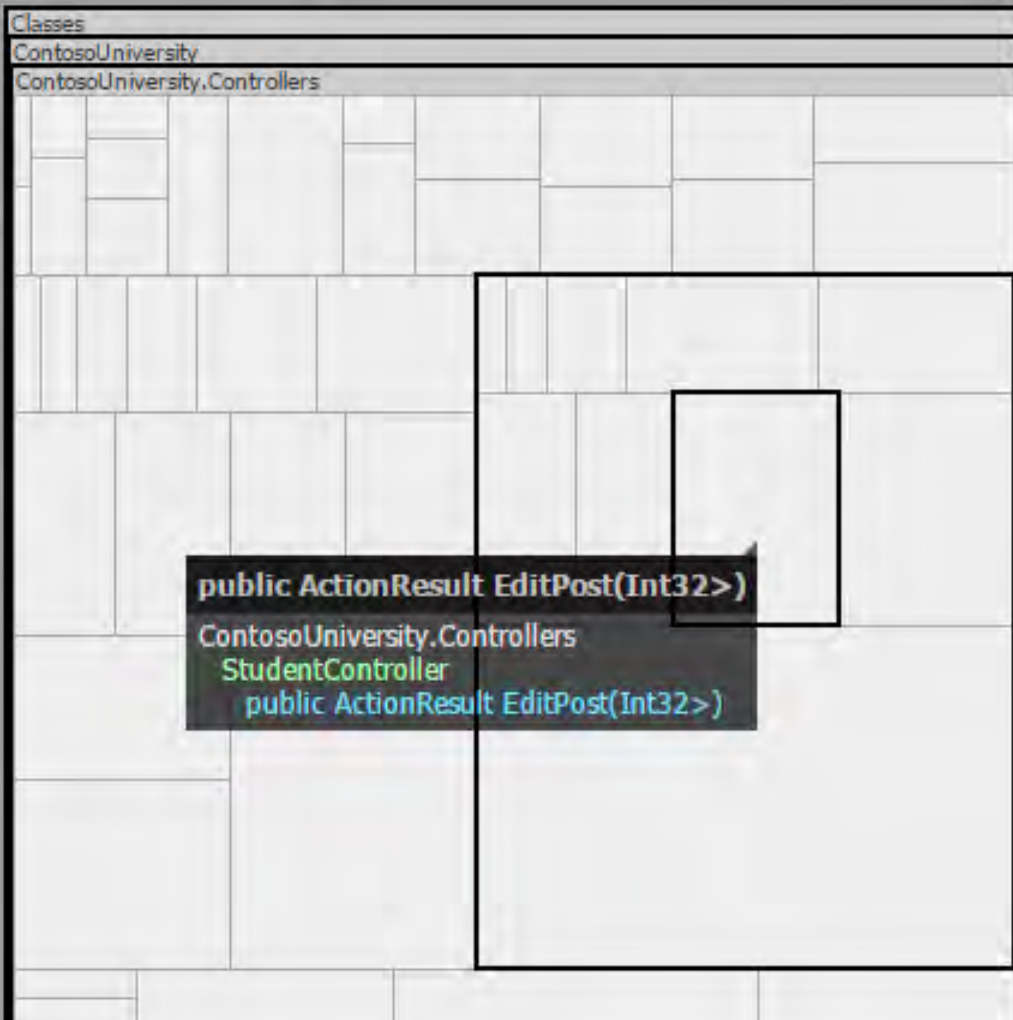
Projects **Contoso University**

created on 4/12/18 11:33 AM

[Export](#)

Application Inventory	Trace	method count	% Coverage
<input checked="" type="checkbox"/> Classes 0	<input checked="" type="checkbox"/>	1198	0%
<input type="checkbox"/> Antr.Runtime	<input checked="" type="checkbox"/>	898	0%
<input checked="" type="checkbox"/> ContosoUniversity	<input checked="" type="checkbox"/>	300	0%
<input type="checkbox"/> <self>	<input checked="" type="checkbox"/>	6	0%
<input checked="" type="checkbox"/> .Controllers	<input checked="" type="checkbox"/>	54	0%
<input type="checkbox"/> .DAL	<input checked="" type="checkbox"/>	34	0%
<input type="checkbox"/> .Logging	<input checked="" type="checkbox"/>	13	0%
<input type="checkbox"/> .Migrations	<input checked="" type="checkbox"/>	112	0%
<input type="checkbox"/> .Models	<input checked="" type="checkbox"/>	65	0%
<input type="checkbox"/> .ViewModels	<input checked="" type="checkbox"/>	16	0%

Code Treemap



Contoso University

created on 4/12/18 11:33 AM

A new agent connected. Click to trace [this project](#), [another project](#), or [drop](#) the connection

Trace	method count	% Coverage
0	1198	0%
	898	0%
	300	0%
	6	0%
	54	0%
	34	0%
	13	0%
	112	0%
	65	0%
	16	0%

Code Treemap

Classes

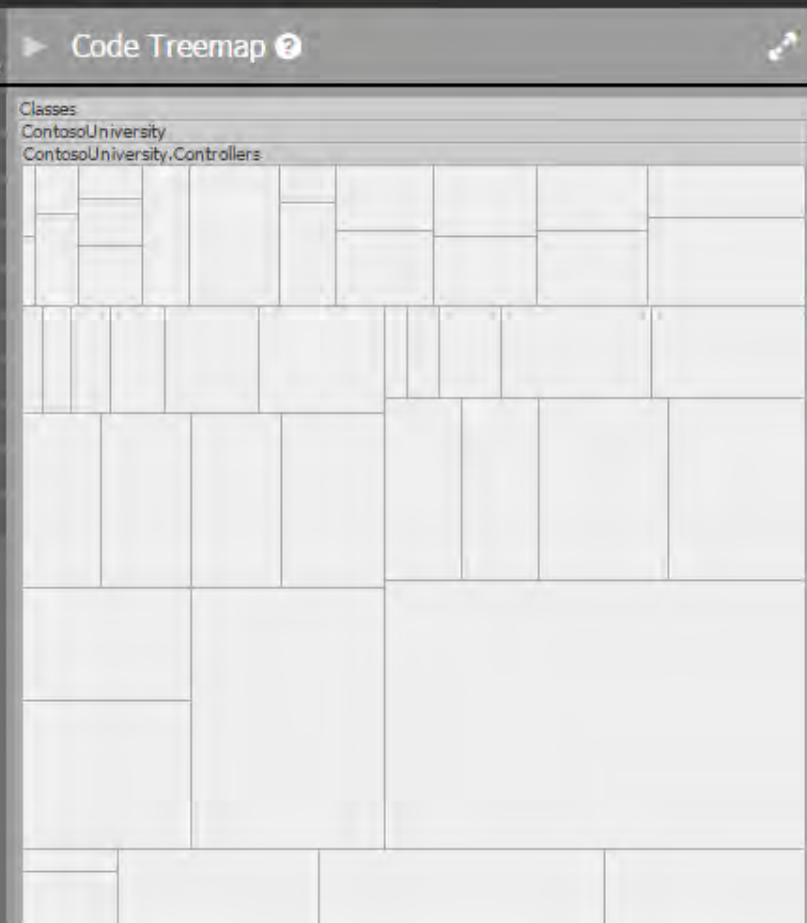
- ContosoUniversity
- ContosoUniversity.Controllers

Treemap Legend

- All Activity
- Overlaps

```
Administrator: Command Prompt - "C:\Program Files (x86)\Code Pulse .NET Tracer\CodePulse.DotNet.Tracer.exe" -iis "-iisappoolidentity:iis appool\...  
Microsoft Windows [Version 10.0.16299.309]  
(c) 2017 Microsoft Corporation. All rights reserved.  
  
C:\WINDOWS\system32>"C:\Program Files (x86)\Code Pulse .NET Tracer\CodePulse.DotNet.Tracer.exe" -iis "-iisappoolid  
y:iis appool\defaultappool" -targetdir:c:\inetpub\wwwroot\contosou\bin  
  
Attempting to add access rule because expected owner of application under test (iis appool\defaultappool) may not  
read and execute permissions to profiler library (C:\Program Files (x86)\Code Pulse .NET Tracer\x86\OpenCover.Prof  
dll)...  
  
Attempting to add access rule because expected owner of application under test (iis appool\defaultappool) may not  
read and execute permissions to profiler library (C:\Program Files\Code Pulse .NET Tracer\x64\OpenCover.Profiler.d  
.  
  
Starting...  
  
Connecting to Code Pulse...  
  
Open Code Pulse, select a project, wait for the connection, and start a trace.
```

Application Inventory	Trace	method count	% Coverage
Classes 🌟 0	✓	1198	0%
+ <input type="checkbox"/> Antr.Runtime	✓	898	0%
- ContosoUniversity	✓	300	0%
<input type="checkbox"/> <self>	✓	6	0%
<input checked="" type="checkbox"/> .Controllers	✓	54	0%
<input type="checkbox"/> .DAL	✓	34	0%
<input type="checkbox"/> .Logging	✓	13	0%
<input type="checkbox"/> .Migrations	✓	112	0%
<input type="checkbox"/> .Models	✓	65	0%
<input type="checkbox"/> .ViewModels	✓	16	0%



Treemap Legend

- All Activity
- Overlaps

Recordings

+ Start a Recording

- Spider Only



ome to Contoso University

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

Proxy Switcher

Define proxy server for each protocol (HTTP, HTTP...

Direct Auto-detect System Proxy **Manual Proxy** PAC-Script Error Log

Profile: **Burp Pro**

HTTP Proxy: 127.0.0.1 Port: 8080

SSL Proxy: 127.0.0.1 Port: 8080

FTP Proxy: 127.0.0.1 Port: 8080

Fallback Proxy: 0.0.0.0 Port:

Server Type: HTTP HTTPS SOCKS v4 SOCKS v5 Remote DNS

Direct: comma separated list of IPs

Tools: [Check external IP](#) | [Check DNS Leakage](#) | [Open FAQs page](#) | [Options](#)

Projects **Contoso University**

created on 4/12/18 11:33 AM

[Export](#)

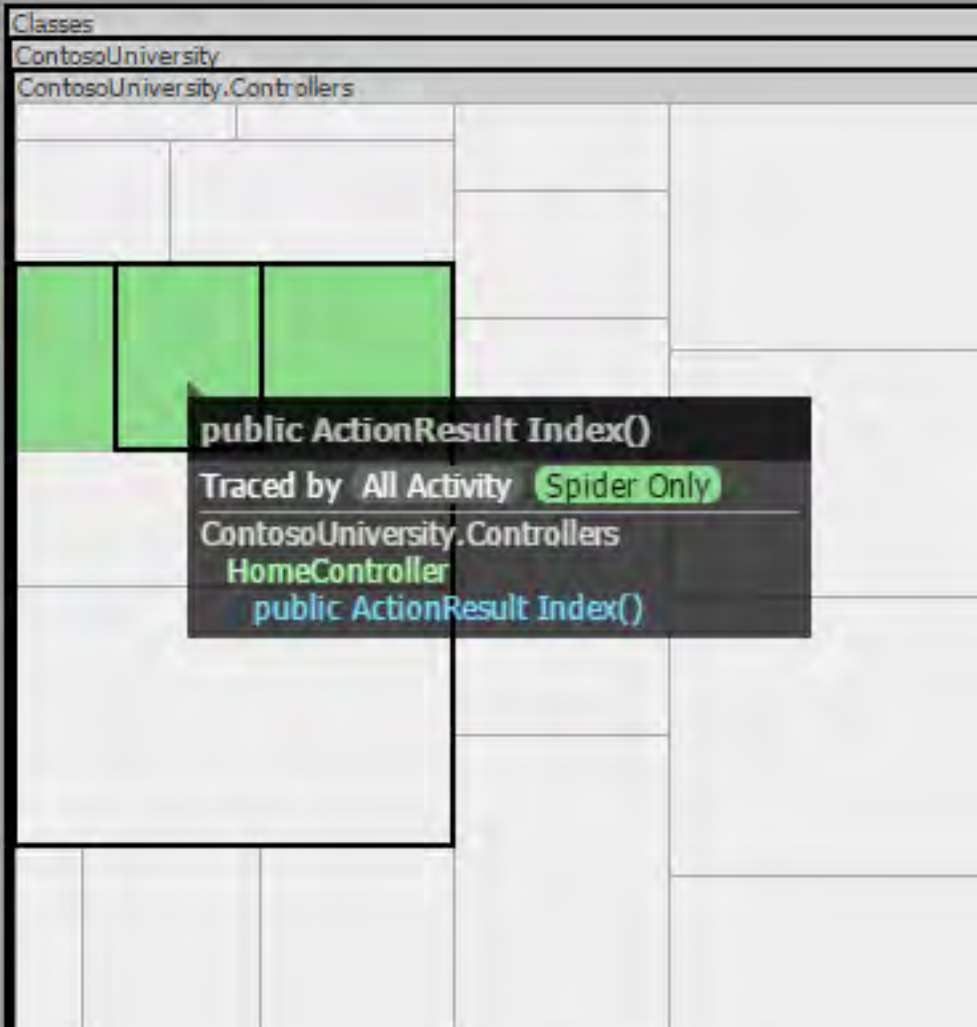
Application Inventory

Trace

method
count%
Coverage

▶ Code Treemap ?

Application Inventory	Trace	method count	% Coverage
Classes ★ 0	✓	1198	<1%
+ <input type="checkbox"/> Antr.Runtime	✓	898	0%
- <input checked="" type="checkbox"/> ContosoUniversity	✓	300	3%
<input type="checkbox"/> <self>	✓	6	33%
<input checked="" type="checkbox"/> .Controllers	✓	54	5%
<input type="checkbox"/> .DAL	✓	34	11%
<input type="checkbox"/> .Logging	✓	13	0%
<input type="checkbox"/> .Migrations	✓	112	0%
<input type="checkbox"/> .Models	✓	65	0%
<input type="checkbox"/> .ViewModels	✓	16	0%



- Target
- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Sequencer
- Decoder
- Comparer
- Extender
- F

- Site map
- Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding emp

- ▶ http://az416426.vo.msecnd.net
- ▶ http://localhost
- ▶ http://www.w3.org

Contents

- ▶ http://localhost/
 - Add to scope
 - Spider this host
 - Actively scan this host
 - Passively scan this host
 - Engagement tools ▶
 - Compare site maps
 - Expand branch
 - Expand requested items
 - Delete host

URL
/ContosoU/
/ContosoU/bundles/...
/ContosoU/bundles/j...
/ContosoU/bundles/...
/
/ContosoU/Content/...
/ContosoU/Course
/ContosoU/Departm...

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender

Control Options

? Spider Status

Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application.

Spider is running

Clear queues

Requests made: 9

Bytes transferred: 246,976

Requests queued: 5

Forms queued: 0

? Spider Scope



Use suite scope [defined in Target tab]

Use custom scope

Application Inventory

Trace

method
count%
Coverage

Code Treemap

	Trace	method count	% Coverage
<input checked="" type="checkbox"/> Classes	<input checked="" type="checkbox"/>	1198	12%
<input checked="" type="checkbox"/> Antr.Runtime	<input checked="" type="checkbox"/>	898	0%
<input checked="" type="checkbox"/> ContosoUniversity	<input checked="" type="checkbox"/>	300	49%
<input checked="" type="checkbox"/> <self>	<input checked="" type="checkbox"/>	6	33%
<input checked="" type="checkbox"/> .Controllers	<input checked="" type="checkbox"/>	54	83%
<input checked="" type="checkbox"/> .DAL	<input checked="" type="checkbox"/>	34	64%
<input checked="" type="checkbox"/> .Logging	<input checked="" type="checkbox"/>	13	30%
<input checked="" type="checkbox"/> .Migrations	<input checked="" type="checkbox"/>	112	<1%
<input checked="" type="checkbox"/> .Models	<input checked="" type="checkbox"/>	65	98%
<input checked="" type="checkbox"/> .ViewModels	<input checked="" type="checkbox"/>	16	68%

Classes

ContosoUniversity

ContosoUniversity.Controllers

ContosoUniversity.ViewModels



Logging of o

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- ▶ http://az416426.vo.msecnd.net
- ▶ http://go.microsoft.com
- ▶ https://go.microsoft.com
- ▼ http://localhost
 - /
 - ▼ ContosoU
 - /
 - ▶ Content
 - ▶ Course
 - ▶ Course
 - ▶ Custom
 - ▶ Department
 - ▶ Department
 - ▶ Instructor
 - ▶ Instructor
 - ▶ Student
 - ▶ Student
 - ▶ bundles
- ▶ http://www.apache.org
- ▶ http://www.w3.org

Contents

Host	Method	URL	Params	Sta...	Length	MI
http://localhost	GET	/		200	963	HT
http://localhost/		/ContosoU/		200	3365	HT
		/ContosoU/Content/		200	867	HT
		/ContosoU/Course		200	26170	HT
		/ContosoU/Course	✓	200	4664	HT
		/ContosoU/Course/		200	26171	HT
		/ContosoU/Course/	✓	200	4665	HT
		/ContosoU/Course/		200	6185	HT

- http://localhost/
 - Remove from scope
 - Spider this host
 - Actively scan this host
 - Passively scan this host
 - Engagement tools**
 - Compare site maps
 - Expand branch
 - Expand requested items
 - Collapse branch
 - Delete host
 - Copy URLs in this host
 - Copy links in this host
 - Save selected items
 - Issues
 - View
 - Show new site map window
 - Site map help

- Search
- Find comments
- Find scripts
- Find references
- Analyze target**
- Discover content
- Schedule task
- Simulate manual testing

upgrade-insecure-requests: 1
Cache-Control: max-age=0

Summary

Dynamic URLs


Static URLs


Parameters

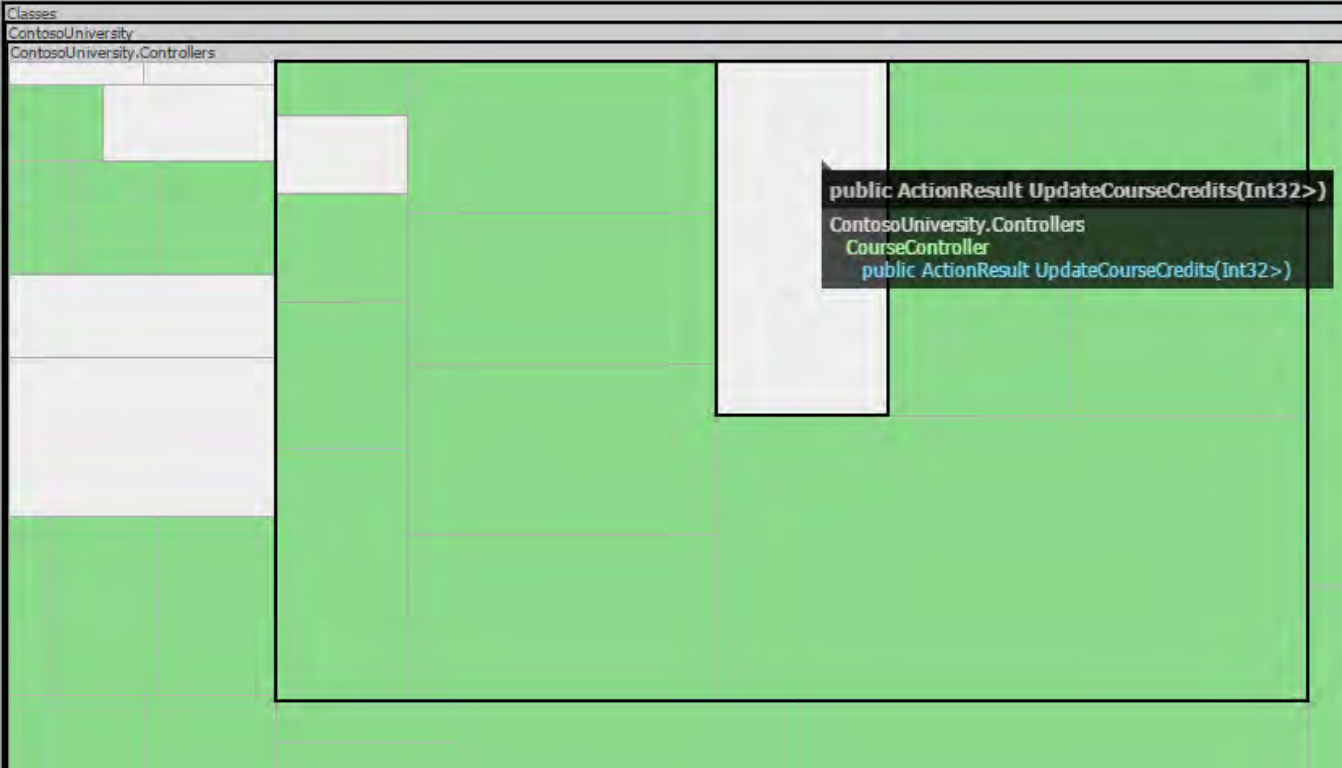
?	Number of dynamic URLs:	88
	Number of static URLs:	66
	Total number of parameters:	273
	Number of unique parameter names:	21

Note: This analysis is based on the current contents of the site map, and no new requests. The query string and request body are included in the analysis. URLs identified as "static" parameters, though their responses may still be dynamically generated.

Save report

Application Inventory	Trace	method count	% Coverage
- Classes 	✓	1198	12%
+ <input type="checkbox"/> Antlr.Runtime	✓	898	0%
- ContosoUniversity	✓	300	49%
<input type="checkbox"/> <self>	✓	6	33%
<input checked="" type="checkbox"/> .Controllers	✓	54	83%
<input type="checkbox"/> .DAL	✓	34	64%
<input type="checkbox"/> .Logging	✓	13	30%
<input type="checkbox"/> .Migrations	✓	112	<1%
<input type="checkbox"/> .Models	✓	65	98%
<input type="checkbox"/> .ViewModels	✓	16	68%

Code Treemap 



Projects **Contoso University**

created on 4/12/18 11:33 AM

[Export](#)

Application Inventory	Trace	method count	% Coverage	Code Treemap ?
<input checked="" type="checkbox"/> Classes 0	<input checked="" type="checkbox"/>	1198	12%	
<input type="checkbox"/> Antlr.Runtime	<input checked="" type="checkbox"/>	898	0%	
<input checked="" type="checkbox"/> ContosoUniversity	<input checked="" type="checkbox"/>	300	49%	
<input type="checkbox"/> <self>	<input checked="" type="checkbox"/>	6	33%	
<input checked="" type="checkbox"/> .Controllers	<input checked="" type="checkbox"/>	54	83%	
<input type="checkbox"/> .DAL	<input checked="" type="checkbox"/>	34	64%	
<input type="checkbox"/> .Logging	<input checked="" type="checkbox"/>	13	30%	
<input type="checkbox"/> .Migrations	<input checked="" type="checkbox"/>	112	<1%	
<input type="checkbox"/> .Models	<input checked="" type="checkbox"/>	65	98%	
<input type="checkbox"/> .ViewModels	<input checked="" type="checkbox"/>	16	68%	



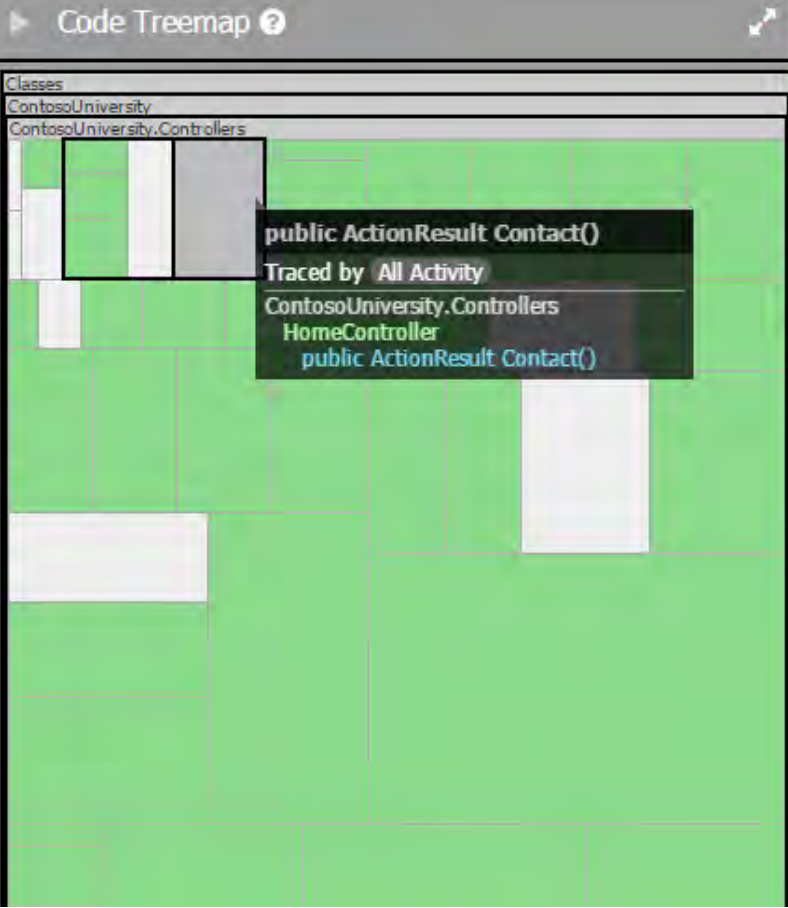
Contact.

Your contact page.

One Microsoft Way
Redmond, WA 98052-6399
P: 425.555.0100

Support: Support@example.com
Marketing: Marketing@example.com

Application Inventory	Trace	method count	% Coverage
Classes 🚩 0	✓	1198	12%
Antlr.Runtime	✓	898	0%
ContosoUniversity	✓	300	49%
<self>	✓	6	33%
.Controllers	✓	54	83%
.DAL	✓	34	64%
.Logging	✓	13	30%
.Migrations	✓	112	<1%
.Models	✓	65	98%
.ViewModels	✓	16	68%



Treemap Legend

- All Activity
- Overlaps

Recordings

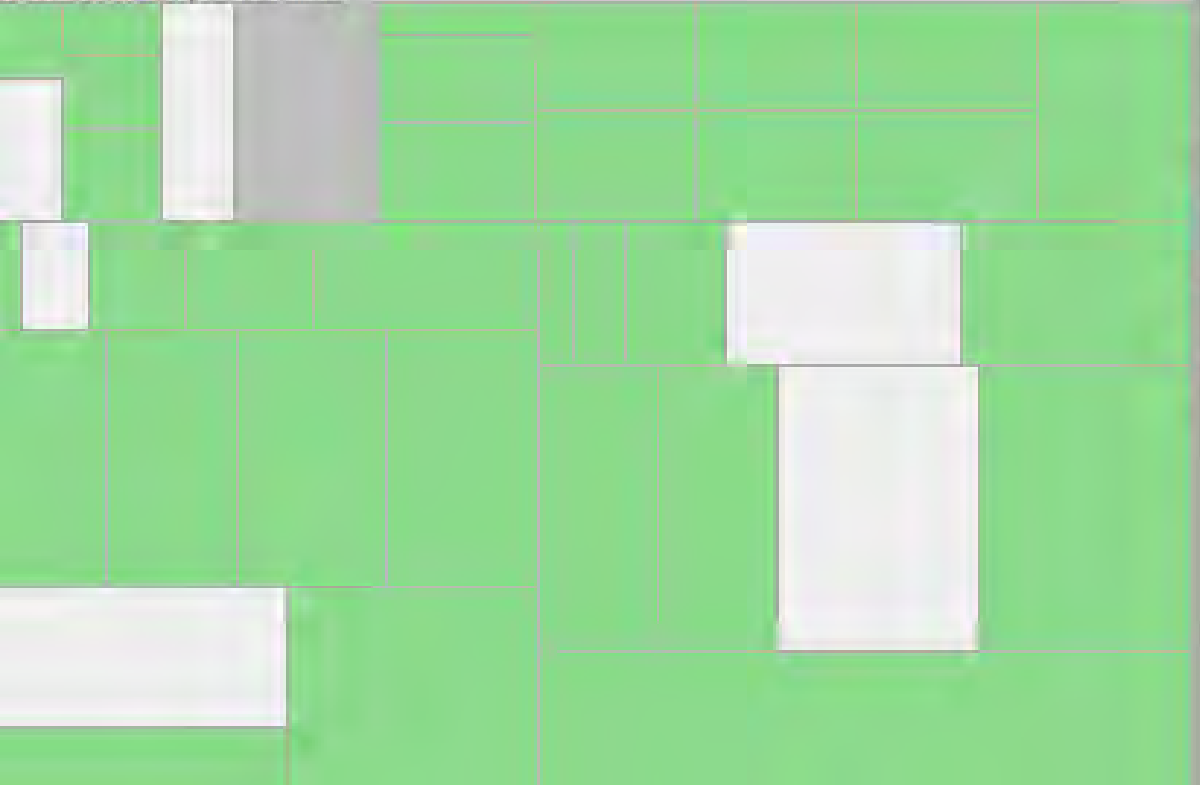
- + Start a Recording**
- Spider Only



Code Treemap ?



Classes
Microsoft.AspNetCore.Mvc
Microsoft.AspNetCore.Mvc.Controllers



Treemap Legend

- All Activity ?
- Overlaps

Recordings ?

[+ Start a Recording](#)

- Spider Only ☰
- Attack Surface Detector ☰

Burp Intruder Repeater Window Help

Target

Proxy

Spider

Scanner

Intruder

Repeater

Sequencer

Decoder

Comparer

Extender

Project options

User options

Alerts

Attack Surface Detector

Main

Options

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.

Location of source code folder:

Select folder ...

Burp Configuration File

This setting lets you configure the location of your Burp configuration file.

Location of configuration file :

Select file ...

Target Configuration

Host: Port: Path (optional): Use Https

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder
Comparer	Extender	Project options		User options	Alerts	Attack Surface Detector	

Main Options

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.

Import Endpoints from Source

Total Endpoints Detected: 37

Detected Endpoints	Number of Detected Parameters	GET Method	POST Method
/Course	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/Details/{id}	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/Create	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/Create	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
/Course/Edit/{id}	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/EditPost/{id}	1	<input type="checkbox"/>	<input type="checkbox"/>
/Course/Delete/{id}	1	<input type="checkbox"/>	<input type="checkbox"/>
/Course/DeleteConfirmed/{id}	1	<input type="checkbox"/>	<input type="checkbox"/>
/Course/UpdateCourseCredits	0	<input type="checkbox"/>	<input type="checkbox"/>
/Course/UpdateCourseCredits	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Message



The endpoints were successfully generated from source.

OK

Selected Endpoint

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer
Decoder	Comparer	Extender	Project options	User options	Alerts	Attack Surface Detector

Main Options

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.

Import Endpoints from Source

Total Endpoints Detected: 37

Detected Endpoints	Number of Detected Parameters	GET Method	POST Method
/Course/Edit/{id}	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/EditPost/{id}	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/Delete/{id}	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/DeleteConfirmed/{id}	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/UpdateCourseCredits	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Course/UpdateCourseCredits	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
/Department	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Department/Details/{id}	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Department/Create	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/Department/Update	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Selected Endpoint

URL:
/Course/UpdateCourseCredits

Methods:
POST

Parameters and type:
multiplier - Integer

Contents

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time
http://localhost	POST	/ContosoU/...	✓	500	13358	HTML	Value cannot be null.		17:...
http://localhost	POST	/ContosoU/...	✓	302	430	HTML	Object moved		17:...
http://localhost	POST	/ContosoU/...	✓	302	430	HTML	Object moved		17:...
http://localhost	POST	/ContosoU/...	✓	302	430	HTML	Object moved		17:...
http://localhost	GET	/ContosoU/...		200	3580	HTML	Student Body Statis...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...		200	3365	HTML	Home Page - Conto...		17:...
http://localhost	GET	/ContosoU/...		200	6366	HTML	Create - Contoso Un...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...		200	5800	HTML	Departments - Cont...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...		200	3365	HTML	Home Page - Conto...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...	✓	500	16540	HTML	The specified cast fr...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...	✓	200	4305	HTML	Delete - Contoso Un...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...		200	3506	HTML	UpdateCourseCredit...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...		200	6269	HTML	Create - Contoso Un...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...	✓	200	6879	HTML	Edit - Contoso Unive...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...		200	6699	HTML	Create - Contoso Un...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...	✓	500	16602	HTML	The specified cast fr...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...	✓	302	438	HTML	Object moved	Generated from source code analy...	17:...
http://localhost	POST	/ContosoU/...	✓	500	12248	HTML	The required anti-for...	Generated from source code analy...	17:...
http://localhost	GET	/ContosoU/...	✓	200	3911	HTML	Courses - Contoso ...	Generated from source code analy...	17:...

Target analysis

Report generated by [Burp Suite](#) at Thu Apr 12 17:18:55 EDT 2018.

Target

- <http://localhost/>

Summary

- Number of dynamic URLs: 88
- Number of static URLs: 66
- Number of parameters: 273
- Number of unique parameter names: 21

Dynamic URLs

- <http://localhost/ContosoU/Content/css>
 - [v=MDbdfKJHba_ctS5x4He1bMV0_RjRq8jpcIA](http://localhost/ContosoU/Content/css?v=MDbdfKJHba_ctS5x4He1bMV0_RjRq8jpcIA)
- <http://localhost/ContosoU/bundles/modernizr>
 - [v=wBEWDufH_8Md-Pbioxomt90vm6tJN2Pyyt](http://localhost/ContosoU/bundles/modernizr?v=wBEWDufH_8Md-Pbioxomt90vm6tJN2Pyyt)
- <http://localhost/ContosoU/bundles/jquery>
 - [v=FVs3ACwOLIVInrAl5sdzR2jrCDmVOWFbZM](http://localhost/ContosoU/bundles/jquery?v=FVs3ACwOLIVInrAl5sdzR2jrCDmVOWFbZM)
- <http://localhost/ContosoU/bundles/bootstrap>
 - [v=2Fz3B0iizV2NnnamQFrX-NbYJNTFeBJ2GM0](http://localhost/ContosoU/bundles/bootstrap?v=2Fz3B0iizV2NnnamQFrX-NbYJNTFeBJ2GM0)
- <http://localhost/ContosoU/bundles/jqueryval>

Target analyzer | <http://localhost/>

Summary

Dynamic URLs

Static URLs

Parameters



Number of dynamic URLs: 105

Number of static URLs: 73

Total number of parameters: 300

Number of unique parameter names: 31

Note: This analysis is based on the current contents of the site map, and the query string and request body are included in the analysis. URLs in the list are static, though their responses may still be dynamically generated.

[Save report](#)

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- ▶ http://az416426.vo.msecnd.net
 - ▶ http://go.microsoft.com
 - ▶ https://go.microsoft.com
 - ▼ http://localhost
 - /
 - ▼ ContosoU
 - /
 - ▶ Content
 - ▶ Course
 - ▼ Course
 - /
 - ▶ Create
 - ▶ Delete
 - ▶ Details
 - ▶ Edit
 - ▼ UpdateCourseCredits
 - multiplier=-1
- ▶ http://www.apache.org
- ▶ http://www.w3.org

Contents

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment
http://localhost	POST	/ContosoU/...	✓	200	3249	HTML	UpdateCourseCredit...	Generated from

Request Response

Raw Params Headers Hex

```
POST /ContosoU/Course/UpdateCourseCredits HTTP/1.1
Host: localhost
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

multiplier=-1
```

Target

Proxy

Spider

Scanner

Intruder

Re

Site map

Scope

Logging of out-of-scope Proxy traffic is disabled

Re-enable

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty fol

- ▶ http://az416426.vo.msecnd.net
- ▶ http://go.microsoft.com
- ▶ https://go.microsoft.com
- ▼ http://localhost

Contents

Host	Method	URL	Params	Status	L
http://localhost	GET	/ContosoU/		200	3
http://localhost/		/ContosoU/...	✓	200	1
	Remove from scope	/ContosoU/...	✓	200	9
	Spider this host	/ContosoU/...	✓	200	3
	Actively scan this host	/ContosoU/...		200	9
	Passively scan this host	/ContosoU/...		200	3
	Engagement tools	/ContosoU/...		200	1
	Compare site maps	/ContosoU/...		200	8
	Expand branch	/ContosoU/...		200	1

- ▶ http://localhost/
- Remove from scope
- Spider this host
- Actively scan this host
- Passively scan this host
- Engagement tools
- Compare site maps**
- Expand branch
- Expand requested items
- Collapse branch
- Delete host
- Copy URLs in this host
- Copy links in this host
- Save selected items

ContosoU

/

Content

Course

Course

/

Create

Delete

Details

Edit

UpdateCourseCredits

multiplier=-1

Custom

Department

Hex

1.1

5.0 (Windows NT 10.0; Win6

Application Inventory

	Trace	method count	% Coverage
- Classes 🕷 0	▼	1198	12%
+ <input type="checkbox"/> Antlr.Runtime	▼	898	0%
- ContosoUniversity	▼	300	49%
<input type="checkbox"/> <self>	▼	6	33%
<input checked="" type="checkbox"/> .Controllers	▼	54	83%
<input type="checkbox"/> .DAL	▼	34	64%
<input type="checkbox"/> .Logging	▼	13	30%
<input type="checkbox"/> .Migrations	▼	112	<1%
<input type="checkbox"/> .Models	▼	65	98%
<input type="checkbox"/> .ViewModels	▼	16	68%

Code Treemap



Treemap Legend

- All Activity
 - Overlaps
- Recordings ⓘ
- + Start a Recording
 - Spider Only
 - Attack Surface Detector

Clear selections


Application Inventory

Trace

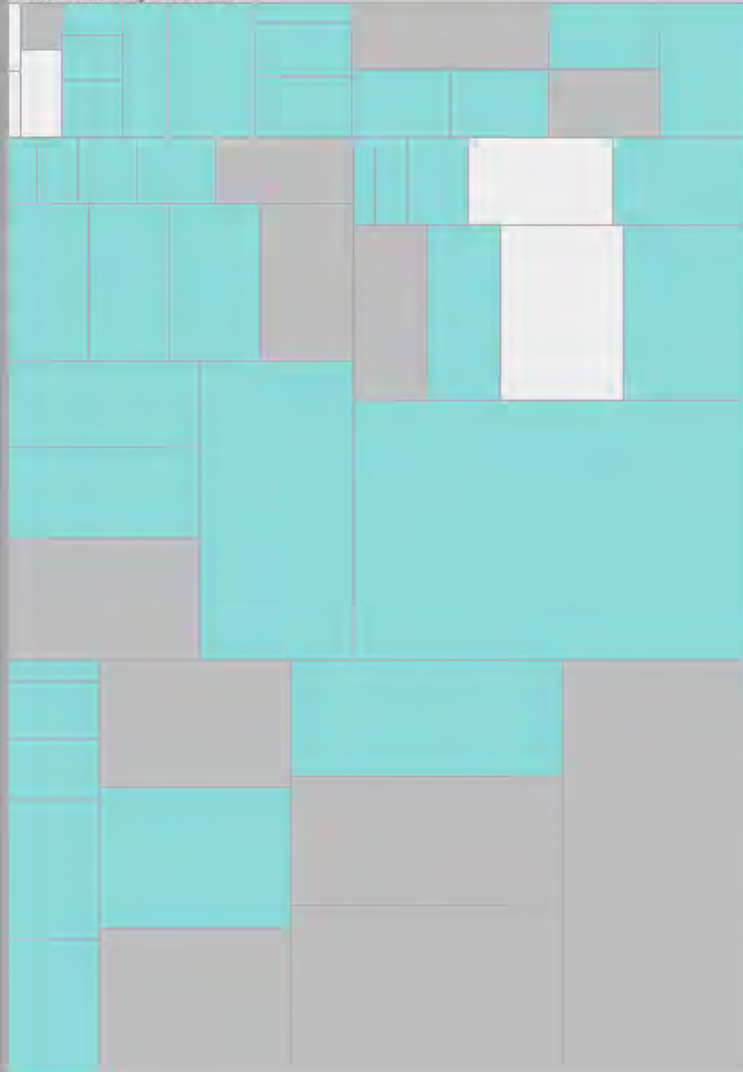
method
count

%



Coverage

Code Treemap 

	Trace	method count	% Coverage
Classes 🔍 0	✓	1198	7%
Antlr.Runtime	✓	898	0%
ContosoUniversity	✓	300	31%
<self>	✓	6	33%
.Controllers	✓	54	66%
.DAL	✓	34	50%
.Logging	✓	13	15%
.Migrations	✓	112	0%
.Models	✓	65	50%
.ViewModels	✓	16	18%

Classes
ContosoUniversity
ContosoUniversity.Controllers

Treemap Legend

 All Activity  OverlapsRecordings **+** Start a Recording Spider Only  Attack Surface Detector  Clear selections Reset colors

Application Inventory

Trace

method
count

%

Coverage

Code Treemap ?

	Trace	method count	% Coverage
Classes 🔍 0	✓	1198	13%
+ <input type="checkbox"/> Antlr.Runtime	✓	898	0%
- ContosoUniversity	✓	300	52%
<input type="checkbox"/> <self>	✓	6	33%
<input checked="" type="checkbox"/> .Controllers	✓	54	90%
<input type="checkbox"/> .DAL	✓	34	64%
<input type="checkbox"/> .Logging	✓	13	30%
<input type="checkbox"/> .Migrations	✓	112	<1%
<input type="checkbox"/> .Models	✓	65	98%
<input type="checkbox"/> .ViewModels	✓	16	87%

Classes
ContosoUniversity
ContosoUniversity.Controllers

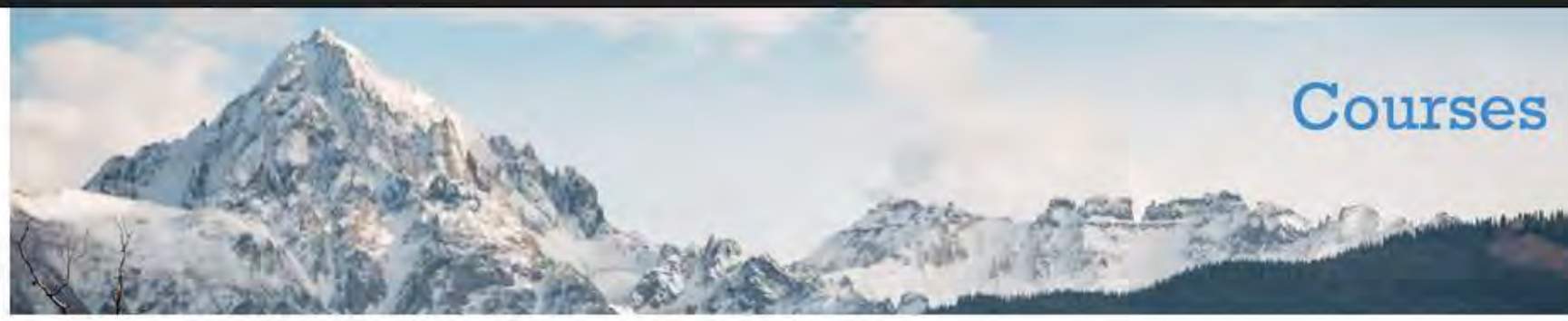
Treemap Legend

 All Activity 🗨 Overlaps

Recordings ?

+ Start a Recording

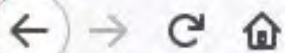
 Spider Only ☰ Attack Surface Detector ☰ Clear selections[Reset colors](#)



Create New

Select Department: All Filter

Number	Title	Credits	Department	
106	Computer Basics	3	Computer Science	  
107	Introduction to Programming	3	Computer Science	  
115	Computer Science 1	3	Computer Science	  
119	Computer Science 2	3	Computer Science	  
123	Precalculus	3	Computer Science	  
127	Calculus I	3	Computer Science	  
130	Calculus II	3	Computer Science	  
131	Calculus III	3	Computer Science	  
132	Statistics	3	Computer Science	  
135	Computer Science 3	3	Computer Science	  



localhost/ContosoU/Course/updatecoursecredits

Contoso University

Departments

Courses

Instructors

Students

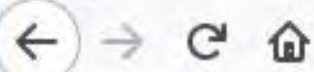


Update Course Credits

Enter a number to multiply every course's credits by:

[Back to List](#)

© 2018 - Contoso University



localhost/ContosoU/Course/updatecoursecredits

Contoso University

Departments

Courses

Instructors

Students



Update Course Credits

Number of rows updated: 29























[Back to List](#)

© 2018 - Contoso University



Create New

Select Department: All Filter

Number	Title	Credits	Department	
106	Computer Basics	126	Computer Science	  
107	Introduction to Programming	126	Computer Science	  
115	Computer Science 1	126	Computer Science	  
119	Computer Science 2	126	Computer Science	  
123	Precalculus	126	Computer Science	  
127	Calculus I	126	Computer Science	  
130	Calculus II	126	Computer Science	  
131	Calculus III	126	Computer Science	  
132	Statistics	126	Computer Science	  

Target analysis

Report generated by [Burp Suite](#) at Wed Feb 20 12:00:00 2020

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 20 12:00:00 2020

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 20 12:00:00 2020

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