

# Making Vulnerability Management Suck Less

 **DEFECT**dojo





# Hello!

**I'm Greg**

Senior Security Engineer @ Pearson

DefectDojo Creator

Former San Antonio OWASP Chapter Leader

And a Bunch of Other Boring Stuff....



“

*I know, I don't like new  
tools either....*





*So Why Dojo?*





# Vulnerability Management for Me:

The screenshot displays the Dradis Framework v2.9.0 web interface in a Mozilla Firefox browser. The address bar shows the URL `https://127.0.0.1:3004`. The interface includes a sidebar with a tree view of uploaded files, including a folder named 'plugin.nessus'. The main content area displays a 'Summary' of a 'Nessus output' category. It contains three entries, each with a description and a timestamp of '05 Feb 2012 12:42'.

**Description**

The remote LDAP server supports search requests with a null, or empty, base object. This allows information to be retrieved without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user may be able to query your LDAP server using a tool such as 'LdapMiner'.

Note that there are valid reasons to allow queries with a null base. For example, it is required in version 3 of the LDAP protocol to provide access to the root DSA-Specific Entry (DSE), with information about the supported naming context, authentication types, and the like. It also means that legitimate users can find information in the directory without any a priori knowledge of its structure. As such, this finding may be a false-positive.

**Solution**

If the remote LDAP server supports a version of the LDAP protocol before v3, consider whether to disable NULL BASE queries on your LDAP server.

**Plugin output**

The interface also features a 'Find a Node' search bar at the bottom left and a 'what's new in this version?' link at the bottom right.







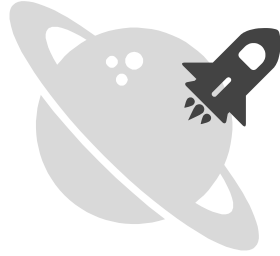






## Why Dojo?

- DefectDojo is a tool created by security professionals for security professionals.
- It attempts to streamline the testing process by offering features such as templating, report generation, metrics, and baseline self-service tools.



# DefectDojo

*Allowing you to focus on what is important to you:*

***Hacking***



# DefectDojo is Well Documented



**Read *the* Docs**



# Launch Easily

## **Standalone**

Traditional deployment is simplified with built in scripts allowing for customization for your specific environment.

## **Dockerized**

Love containers? So do we. DefectDojo is easily deployed in a Docker environment and comes ready with its own Dockerfile





## Easy to Change

- `models.py` - DB
- `views.py` - process data
- `templates` - html



## Features That Make Dojo Stand Out

### Templating



Many findings are common and seen across multiple tests. DefectDojo makes it easy to reuse any or all verbiage associated with these findings.

### Report Generation



From canned reports to custom built ones, AsciiDoc or PDF, DefectDojo gives you the options to present findings to allow for greater impact.

### Metrics that Matter



We have the data, you need the trends, DefectDojo aims to provide you with details about engagements, tests, and findings in a visual way to help tell the overall story.

### Scanner Consolidation



You have the tools: Burp, Nexpose, Appspider, Checkmarx, Nessus, Veracode, Zap; DefectDojo plays nice with them all.

### Self-Service Tools



Launch nmap scans, and view results. Use the built API to manage Findings, Engagements and Tests.

### Plugins



DefectDojo is a Django project which allows for easy extensibility via applications both existing and new.



🏠 Dashboard

📁 Products

📁 Engagements

🔍 Findings

👥 Endpoints

📄 Reports

📊 Metrics

👤 Users

📅 Calendar

🔍 Collapse Menu

## Dashboard for Dojo Admin


8


Active Engagements

View Details →


1

Findings In Last Seven Days

View Details →


0

Findings Closed In Last Seven Days

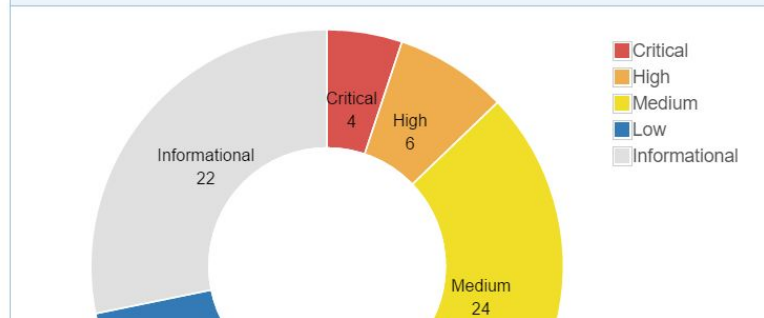
View Details →


0

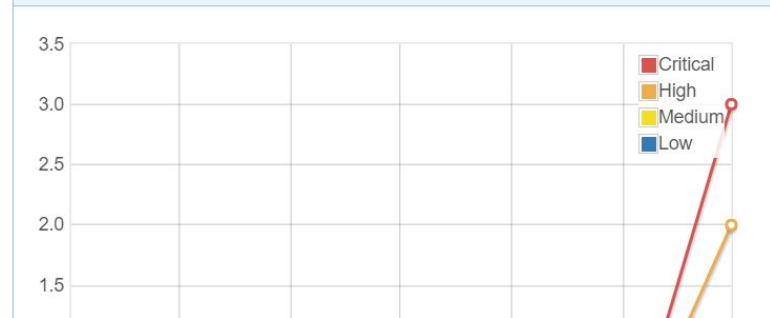
Findings Accepted In Last Seven Days

View Details →

### Historical Finding Severity



### Reported Finding Severity by Month





# *Thinking in Dojo*





Models / Workflows

# Thinking in Dojo By Example



## Models / Workflows

Google





## Models / Workflows



Google docs



## Models / Workflows

**Product Type - Organization or Product Line**







## Models / Workflows

Product Type - Tech Org

- **Product - Application or Product**



Google docs



## Models / Workflows

### Product Type - Tech Org

- Product - Some Application
  - **Engagement - Assessment or Mission**







## Models / Workflows

### Product Type - Tech Org

- Product - Some Application
  - Engagement - Quality PCI Scan
    - **Test - Tool Being Used**

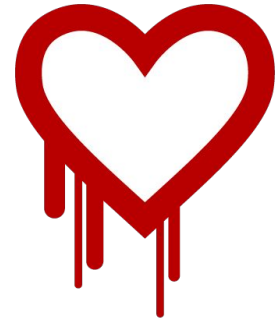




## Models / Workflows

### Product Type - Tech Org

- Product - Some Application
  - Engagement - Quality PCI Scan
    - Test - Tool Being Used
      - Finding - What you found







# Models / Workflows

## Product Type - Tech Org

- Product - Some Application
  - Engagement - Quality PCI Scan
    - Test - Tool Being Used
      - Finding - What you found
        - Endpoint - Where you found it





## Scanner Consolidation / Integration

**VERACODE**



**CHECKMARX**



**ZAPROXY**

**arachni**

web application security scanner framework



**nexpose**<sup>®</sup>

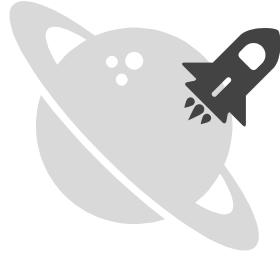


**appspider**



**BURPSUITE**  
PROFESSIONAL





Demo Time!



**BAD IDEA**

Some Things Are Just A Bad Idea!!!





# Scanner Integration

DEFECTdojo



19



Home / Active Engagements / IOT / Engagement: New Project (Oct 29, 2016)

Threat Model / Test Strategy / Tests / In Progress

## New Project In Progress



Testing Lead: Dojo Admin

Engagement Name: New Project

Target Start Date: Oct. 29, 2016

Target End Date: Oct. 31, 2016

Test Strategy

View Test Strategy

Threat Model

Upload Model

## Tests



Type	Start Date	End Date	Findings	Notes	Actions
------	------------	----------	----------	-------	---------



## Scanner Integration Gen 2 (In Progress)



**CHECKMARX**





# Templating

DEFECTdojo



[Home](#) / [Active Engagements](#) / [IOT](#) / [Engagement: New Project \(Oct 29, 2016\)](#) / [WebApp Scan \(Oct 31, 2016\)](#)

Finding deleted successfully.

## WebApp Scan

Environment	Engagement	Target Start Date	Target End Date	Progress
Development	<a href="#">Engagement: New Project (Oct 29, 2016)</a>	Oct. 31, 2016	Nov. 1, 2016	<div><div>80%</div></div>

## Findings

No findings found.

## Potential Findings

+ Add Potential Finding



# Report Generation



[Home](#) / [Report List](#) / [Test Product](#) / Engagement: Test Engagement (Nov 01, 2016)

[Tests](#) / In Progress

## Test Engagement In Progress



Testing Lead: matt

Engagement Name: Test Engagement

Target Start Date: Nov. 1, 2016

Target End Date: Nov. 9, 2016

Test Strategy

[Edit this engagement to add a test strategy.](#)

Threat Model

[Upload Model](#)

## Tests



Type	Start Date	End Date	Findings	Notes	Actions
------	------------	----------	----------	-------	---------





# Metrics

DEFECTdojo

Search...



19



## Dashboard for Dojo Admin



8

Active Engagements

[View Details](#)



1

Findings In Last Seven Days

[View Details](#)



0

Findings Closed In Last Seven Days

[View Details](#)



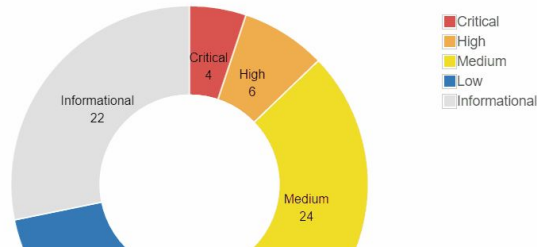
0

Findings Accepted In Last Seven Days

[View Details](#)



### Historical Finding Severity



### Reported Finding Severity by Month





# Product Metrics



[Home](#) / [Product List](#) / [Test Product](#)

## Test Product

2 affected endpoints



### Details

Product Type	Team Manager	Product Manager	Technical Contact	Authorized Users
Research and Development	0	0	0	

### Description

I'm testing.

### Active Engagements



Name	Lead	Start Date	End Date	Actions
------	------	------------	----------	---------





# Endpoint Analytics

DEFECTdojo



20



Dashboard

Products

Engagements

Findings

Endpoints

Reports

Metrics

Users

Calendar

Collapse Menu

Home / All Endpoints

## All Endpoints



Endpoint ↕	Product ^	Number of Open Findings
www.google.com	Banana Stand	0
127.0.0.1	Demo Product	75
localhost	IOT	0
oracle.com	IOT	0
www.iot.com	IOT	0
www.owasp.org	IOT	2
104.130.192.89	IOT	2
www.example.com	IOT	1



# Tagging

[Dashboard](#)[Products](#)[Engagements](#)[Findings](#)[Endpoints](#)[Reports](#)[Metrics](#)[Users](#)[Calendar](#)[Collapse Menu](#)[Home](#) / [Product List](#) / [Test Product](#)

## Test Product

2 affected endpoints



### Details

Product Type	Team Manager	Product Manager	Technical Contact	Authorized Users
Research and Development	0	0	0	

### Description

I'm testing.

### Active Engagements



Name	Lead	Start Date	End Date	Actions
------	------	------------	----------	---------





# Self Service Tools

**DEFECT**dojo



19



Dashboard

Products

Engagements

Findings

Endpoints

Reports

Metrics

Users

Calendar

Collapse Menu

## Active Engagements

Name	Lead	Start Date	End Date	Actions
Nu c00l dashboard	admin	June 8, 2016	June 30, 2016	<a href="#">View Details</a>
Demo Engagement	admin	May 29, 2015	May 29, 2015	<a href="#">View Details</a>
Demo Engagement	admin	May 29, 2015	May 29, 2015	<a href="#">View Details</a>

## Scans

Creator	Date	Frequency	Protocol	Actions
admin	Sept. 16, 2016, 1:29 a.m.	Weekly	TCP	<a href="#">View Details</a>



v. 1.0.5

DefectDojo is licensed under the [Simplified BSD license](#).





# Team Calendar

DEFECTdojo

Search...



1



Home / Calendar

< > today

November 2016

month week day

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
		Test Product: Test Engagement		Test Product: Big Assessment		
6	7	8	9	10	11	12
Test Product: Test Engagement		Test Product: Big Assessment				
13	14	15	16	17	18	19
Test Product: Big Assessment						

54.245.18.251:9000/engagement/2





# Threat Modeling

DEFECTdojo

Search...



[Home](#) / [Calendar](#) / [Test Product](#) / [New Engagement](#) / Engagement: Test Engagement 2 (Nov 03, 2016)

In Progress

## Test Engagement 2 In Progress

Testing Lead: matt

Engagement Name: Test Engagement 2

Target Start Date: Nov. 3, 2016

Target End Date: Nov. 4, 2016

Test Strategy

[Edit this engagement to add a test strategy.](#)

Threat Model

[Upload Model](#)

## Tests

No tests found



# Test Strategies

[Dashboard](#)[Products](#)[Engagements](#)[Findings](#)[Endpoints](#)[Reports](#)[Metrics](#)[Users](#)[Calendar](#)[Collapse Menu](#)[Home](#) / [Product List](#) / [Test Product](#) / Engagement: Test Engagement 2 (Nov 03, 2016)[Threat Model](#) / In Progress

## Test Engagement 2 In Progress



Testing Lead: matt

Engagement Name: Test Engagement 2

Target Start Date: Nov. 3, 2016

Target End Date: Nov. 4, 2016

Test Strategy

*Edit this engagement to add a test strategy.*

Threat Model

[Download Model](#)[Edit](#)

Tests



No tests found





*Where we are now*





Travis CI



ZAPROXY



Read *the* Docs



docker

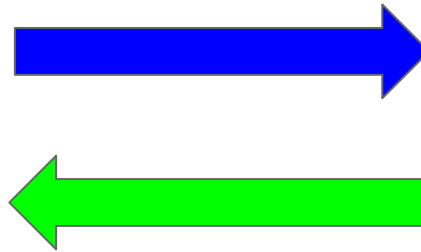




## JIRA Integration

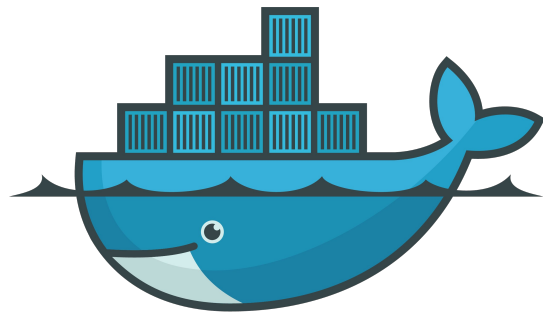


**DefectDojo**





## One-Click Installations



docker



Deploy to Cloud





# *The Future*

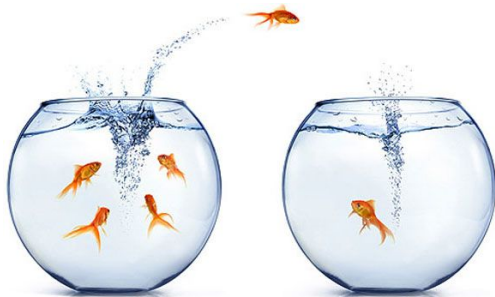




# The Future



Deploy to Heroku



PostgreSQL





# The Future



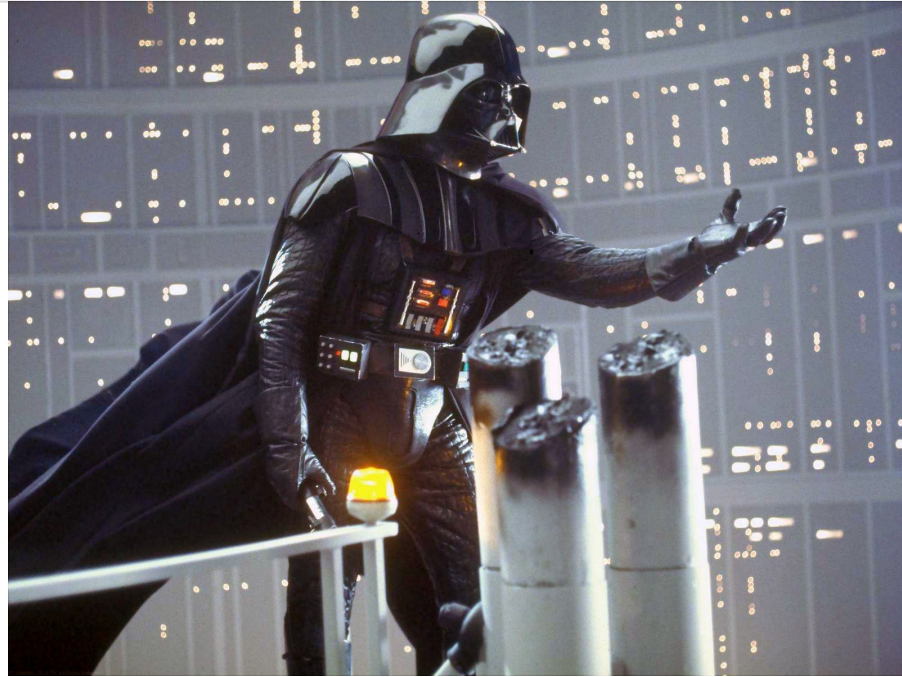
## Travis CI







# Contributing







## Trying it Out

```
git clone
```

```
https://github.com/OWASP/django-DefectDojo
```

```
cd django/defectDojo
```

```
./setup.bash
```

```
python manage.py runserver
```



## References

DefectDojo is open source and fully documented:

- Github: <https://github.com/OWASP/django-DefectDojo>
- Docs: <http://defectdojo.readthedocs.io/>
- Demo: <https://defectdojo.pythonanywhere.com>





# Thanks!

**Any questions?**

Contacting Me:

- [greg.anderson@owasp.org](mailto:greg.anderson@owasp.org)