OWASP

Open Web Application Security Project

甲方安全&OWASP 项目分享

目录

CONTENTS

01 我对安全的理解

02 甲方安全与开源

03 OWASP项目分享

OWASP
Open Web Application Security Project

共计**14**个大项

以及**65**个细分小项之多

OWASP
Open Web Application Security Project

信息安全演变

网络安全

时间04年-10年

设备防火墙

原因能做的坏事比较有限

数据安全

10年后至今

数据库防火墙，网闸，各种web防护

重要数据触网

网络空间安全

17年至未来

ABC安全、物联网安全

智慧城市、智慧生活

01 我对信息安全的理解

02 甲方安全与开源技术

03 OWASP项目分享

甲方安全

阶段一：能够进行安全技术检查以及行业安全预警跟踪，发现部分安全脆弱性并加固。

手段：完善网络架构安全、部分安全设备软件

阶段二：重视内网安全、有计划强化人员信息安全意识，初步建立安全预警和安全管理体系。

手段：网络安全域、安全预警及应急保障培训

阶段三：能够及时发现WEB安全问题、拥有系统上线变更、数据防泄漏等安全能力。

手段：全面安全设备、源代码安全审计、ITLE

阶段四：健全的安全体系包括管理、审计和考核，重视软件安全，能够实现主动防御以及强大的追踪能力。

手段：SDL应用、SOC平台、蜜罐系统

开源技术

开源的日志审计系统：ELK
开源的监控平台：ZABBIX
开源的云平台：OpenStack, CloudStack, Docker, Hadoop
开源的移动平台：Android
开源的运维系统：Nagios
开源的运维管理平台：itop
开源的开发平台：Eclipse, Git, Jenkins
开源的后台服务：LAMP, Nginx, Spring/Tomcat/JBoss, Redis, LevelDB, Spark, NodeJs, MySQL, Postgresql, Django
开源的针对某个领域的平台： Caffe, Theano, Torch, BT

作为工程，其实很多没有必要去造一个质量更差的轮子。在系统/软件开发/信息安全项目的生命周期的所有环节中，研究，设计，开发，部署，运营运维中，都有很成熟的，解决了绝大部分需求的开源软件，只需要把精力放在提升效果和完成业务的部分。

OWASP项目库

OWASP项目是具有已定义的路线图和团队成员的相关任务的集合。OWASP项目负责人负责定义项目的愿景，路线图和任务。项目负责人还推动项目并建立团队。OWASP目前有超过93个“ 活跃项目”，每周都会提交新的项目申请。

OWASP项目

甲方痛点

OWASP OWTF	缺乏安全检测工具
OWASP DefectDojo	缺乏漏洞管理工具
OWASP Juice Shop	缺乏安全培训工具
OWASP Top Ten	缺乏安全标准文档

OWASP
Open Web Application Security Project

Pages in category "OWASP Project"

The following 200 pages are in this category, out of 388 total.

(previous page) (next page)

- OWASP in Action: Tools for the DISA ASD STIG

A

- OWASP Alchemist Project
- OWASP Anti-Malware Project
- AntiSamy Java 中文项目
- OWASP Application Security Program for Managers
- OWASP Application Security Skills Assessment
- AppSensor Summit
- OWASP Autumn of Code 2006 – Projects: Testing Guide

B

- Benchmark
- Best Practice: Projektierung der Sicherheitsprüfung von Webanwendungen
- Best Practices: Einsatz von Web Application Firewalls
- OWASP Bricks
- GPC Project Details/OWASP BWA Project
- OWASP Browser Security ACID Tests Project
- OWASP Web Browser Testing System Project

C

- Classic ASP Security Project
- GPC Project Details/OWASP Cloud - 10 Project
- GPC Project Details/OWASP Code Crawler
- Code review
- OWASP Codes of Conduct
- Collaborate

- OWASP iGoat Project
- Intelligent Security
- OWASP Internationalization

J

- OWASP Java HTML Sanitizer Project
- OWASP Java XML Templates Project
- JBroFuzz
- GPC Project Details/OWASP JBroFuzz
- GPC Project Details/OWASP JSReg Project

K

- Key Project Information:OWASP PCI Project

M

- OWASP Mantra – Security Framework
- Virtual Patching Best Practices
- Modsecurity crs 10 config.conf
- OWASP Myth Breakers Project

O

- O-Saft
- O-Saft/Documentation
- OWASP O2 Platform Project – Project Identification
- Octoms
- Opa
- Projects/Opa
- OWASP OVAL Content Project
- OWASP 1-Liner
- OWASP A&D Project
- OWASP Academy Portal Project

- OWASP Cyber Defense Matrix
- Owasp Cyber Security at the Board Level Project
- OWASP Damn Vulnerable Web Sockets (DVWS)
- OWASP DeepViolet TLS/SSL Scanner
- OWASP DefectDojo Project
- OWASP Dependency Check
- OWASP Dependency Track Project
- OWASP Desktop Goat and Top 5 Project
- OWASP DevSecOps Studio Project
- OWASP DevSlop Project
- OWASP Documentation Project Template
- OWASP Droid Fusion
- OWASP Droid10 Project
- OWASP DVSA
- OWASP Ecuador
- OWASP EJSF Project
- OWASP Embedded Application Security
- OWASP Encoder Comparison Reference Project
- OWASP Example Incubator
- OWASP Excess XSS Project
- OWASP Faux Bank Project
- OWASP File Hash Repository
- OWASP Financial Information Exchange Security Project
- OWASP Focus
- OWASP Framework Security Project
- OWASP Game Security Framework Project
- OWASP Global Chapter Meetings Project
- OWASP Glue Tool Project
- OWASP Good Component Practices Project
- OWASP Guide Project

- OWASP Common Numbering Project
- GPC Project Details/OWASP CBT Project
- Cornucopia – Ecommerce Website Edition – Wiki Deck
- OWASP Corporate Application Security Rating Guide
- OWASP Cross-Site Request Forgery Research Pool
- OWASP CSRFGuard Project/es
- CSRFProtector Project

D

- OWASP Data Exchange Format Project
- Diez Mayores 2004
- OWASP DVIA

E

- EDU
- Encrypted Token Pattern CSRF Defence Project
- OWASP Enterprise Application Security Project
- OWASP ESAPI C Project
- OWASP ESAPI C++ Project
- OWASP ESAPI Perl Project
- ESAPI Swingset
- OWASP ESOP Framework
- OWASP Exams Project

F

- OWASP Forward Exploit Tool Project

G

- OWASP German Language Project
- Germany/Projekte
- Germany/Projekte/Top 10
- Germany/Projekte/Top 10 fuer Entwickler
- GPC Project Details/OWASP Google Hacking Project
- OWASP Project Details Table 2

- OWASP AJAX Crawling Tool
- OWASP Amass Project
- OWASP Androick Project
- OWASP Anti-Ransomware Guide Project
- OWASP API Security Project
- OWASP APK DISSECTOR
- OWASP Application Fuzzing Framework Project
- OWASP Application Security Curriculum
- OWASP Application Security Guide For CISOs Project
- OWASP Application Security Guide For CISOs Project v2
- OWASP Application Security Program Quick Start Guide Project
- OWASP AppSec Designer Security Functional Requirements & Countermeasures Libraries
- OWASP AppSec Pipeline
- OWASP Appsec Tutorial Series
- OWASP AppSensor Handbook
- OWASP AppSensor Project
- OWASP ASP.NET MVC Boilerplate Project
- OWASP Assimilation Project
- OWASP ASVS Assessment tool
- OWASP Attack Surface Detector Project
- OWASP Auth
- OWASP Automated Threats to Web Applications
- OWASP Autosploit Project
- OWASP Barbarus
- OWASP Basic Expression & Lexicon Variation Algorithms (BELVA) Project
- OWASP Best Practices in Vulnerability Disclosure and Bug Bounty Programs
- OWASP Broken Web Applications Project
- OWASP Browser Security Project
- OWASP Bug Logging Tool

- OWASP H2H Tool Project
- OWASP HA Vulnerability Scanner Project
- OWASP Hackademic Challenges Project
- OWASP Hacking Lab
- OWASP Hacking-the Pentest Tutor Game
- OWASP Hive Project
- OWASP Honeypot Project
- OWASP ICS / SCADA Security Project
- OWASP iGoat Tool Project
- OWASP iMAS iOS Mobile Application Security Project
- OWASP Incident Response Project
- OWASP Information Security Metrics Bank
- OWASP Insecure Web Components Project
- OWASP Internet of Things Project
- OWASP iSABEL Proxy Server
- OWASP ISO IEC 27034 Application Security Controls Project
- OWASP ISO Project
- OWASP Java Encoder Project
- OWASP Java File I O Security Project
- OWASP Java J2EE Secure Development Curriculum
- OWASP Java Uncertain Form Submit Prevention
- OWASP JavaScript Sandboxes
- OWASP JAWS Project
- OWASP JOTP Project
- OWASP JSEC CVE Details
- OWASP JSON Sanitizer
- OWASP Juice Shop Project
- OWASP KALP Mobile Project
- OWASP Kates Project
- OWASP Knowledge Based Authentication Performance Metrics Project
- OWASP Knowledge Graph
- OWASP LAPSE Project

Webanwendungen
- OWASP Risk Rating Management
- OWASP Robot Security Project
- OWASP Ruby on Rails and friends Security Guide
- OWASP S.T.I.N.G Project
- OWASP SaaS Rest API Secure Guide
- OWASP SafeNuGet
- OWASP SafeNuGet Project
- OWASP SamuraiWTF Project
- OWASP Scada Security Project
- OWASP SE – Social Engineering
- OWASP SecLists Project
- OWASP Secu-RT Project
- OWASP Secure Application Design Project
- *OWASP Secure Application Lifecycle Management*
- OWASP Secure Configuration Guide
- OWASP Secure Development Training
- OWASP Secure Headers Project
- OWASP Secure Medical Device Deployment Standard
- OWASP Secure Software Contract Annex German
- OWASP Secure Software Contract Annex Italian
- OWASP Secure Software Development Lifecycle Project
- OWASP Secure TDD Project
- OWASP SecureTea Project
- OWASP Security Catalyst
- OWASP Security Controls in Web Application Development Lifecycle
- OWASP Security Frameworks Project
- OWASP Security JDIs Project
- OWASP Security Knowledge Framework
- OWASP Security Labeling System Project
- OWASP Security Logging Project
- OWASP Security Ninja Program Project
- OWASP Security Ninja Project
- OWASP Virtual Village Project
- OWASP Visual Crime Scene and Security Incident Education Project
- OWASP Vulnerability Management Guide
- OWASP Vulnerable Web Applications Directory Project
- OWASP WAF Project
- OWASP WAP–Web Application Protection
- OWASP WASC Distributed Web Honeypots Project
- OWASP WASC Web Hacking Incidents Database Project
- OWASP Watiqay
- OWASP Web Application Security Quick Reference Guide Project
- OWASP Web Malware Scanner Project
- OWASP Web Mapper Project
- OWASP WebSandBox Project
- OWASP WebSpa Project
- OWASP Windows Binary Executable Files Security Checks Project
- OWASP Wordpress Security Implementation Guideline
- OWASP Wordpress Vulnerability Scanner Project
- OWASP WS Amplification DoS Project
- OWASP XSecurity Project
- OWASP XSSER
- OWASP Zezengorri Code Project
- OWASP ZSC Tool Project
- OWASP中文项目

P

- OWASP Passw3rd Project
- OWASP Portuguese Language Project
- Project Information:template Vicnum Project
- Project Online Resources
- Project Reviews Guideline
- *Projects Reboot 2012*
- OWASP Spanish

T

- OWASP Testing Project
- OWASP Threat Modelling Project
- OWASP Tiger
- Top 10 2004
- GPC Project Details/OWASP Top10

U

- OWASP Uniform Reporting Guidelines

V

- OWASP VFW Project
- GPC Project Details/OWASP Vicnum Project

W

- WASC OWASP Web Application Firewall Evaluation Criteria Project
- OWASP Web Application Security Accessibility Project
- OWASP Web Service Attack Community Project
- WebGoatPHP
- OWASP WebScarab NG Project
- Proyecto WebScarab OWASP
- OWASP WhatTheFuzz Project
- OWASP Web Testing Environment Project

X

- OWASP Fiddler Addons for Security Testing Project
- OWASP Xenotix XSS Exploit Framework

Z

- OWASP SAMM Project
- OWASP Zed Attack Proxy Project

真实项目：安全运维标准化-ITOP

为什么选择开源

1、厂商产品价格昂贵且无法贴合实际需求；
2、涉密信息无法确保安全性；
3、员工参与开源项目，提升能力；

开源带来的益处

深入了解ITLE标准化管理体系，全方位参与事件管理、问题管理、配置管理、变更管理、发布管理等

根据企业自身情况深度定制，包括 CMDB 功能、CMDB管理流程、知识共享库、发布管理、模块之间关联性等消除了技术绑定并完全符合企业需求。

员工提升了代码水平，交流了思想，提升了发现问题、解决问题的能力。

01 我对信息安全的理解

02 甲方安全与开源技术

03 OWASP项目分享

OWASP Juice Shop Tool Project

简介

Juice Shop是用Node.js，Express和Angular编写的。这是第一个完全用OWASP VWA目录中列出的JavaScript编写的应用程序。
该应用程序包含大量针对不同难度的黑客攻击，用户应该利用潜在的漏洞。在记分板上跟踪黑客攻击进度。
除了黑客和意识培训用例之外，测试代理或安全扫描程序可以使用Juice Shop作为“豚鼠”应用程序来检查他们的工具如何更好地处理JavaScript繁重的应用程序前端和REST API。

主要卖点

免费和开源：根据MIT许可证获得许可，无隐藏费用或警告
易于安装：在Windows / Mac / Linux上运行node.js，Docker和Vagrant之间进行选择
自我修复：在每个服务器启动时，从头开始擦除并重新填充简单的SQLite和MarsDB数据库
游戏化：应用程序通知您已解决的挑战并跟踪记分板上成功利用的漏洞
品牌重塑：完全可根据您的企业或客户要求定制商业环境和外观
CTF支持：可与其他开源CTF结合

OWASP
Open Web Application Security Project

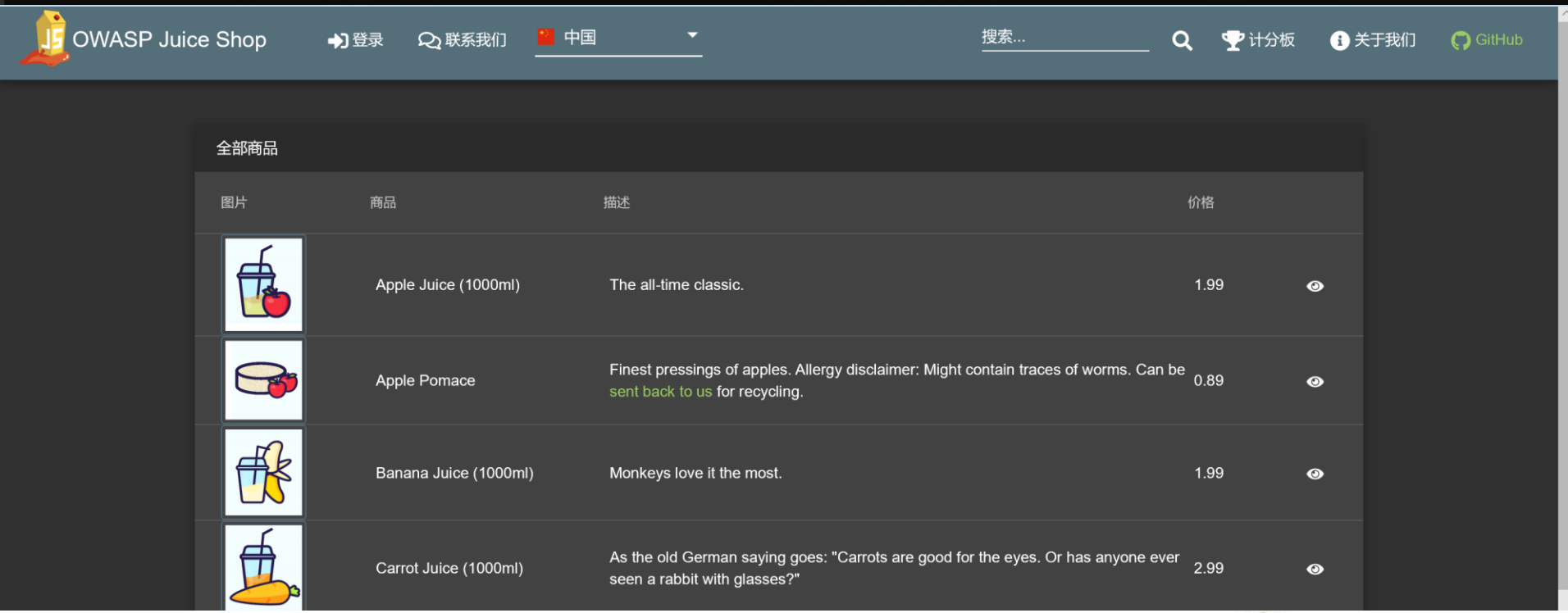
```
C:\juice-shop-8.2.0_node10_windows_x64\juice-shop_8.2.0>npm start

> juice-shop@8.2.0 start C:\juice-shop-8.2.0_node10_windows_x64\juice-shop_8.2.0
> node app

Detected Node.js version v10.15.0 (OK)
Configuration default validated (OK)

Server listening on port 3000

Solved challenge Score Board (Find the carefully hidden 'Score Board' page.)
Solved challenge XSS Tier 1 (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.)
```



OWASP Juice Shop 登录 联系我们 中国 "javascript:alert(`xss`)">. 计分板 关于我们 GitHub

你成功地解决了一项挑战： XSS Tier 1 (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.) X

计分板 1%

难度系数

1 1/8 | 2 0/8 | 3 0/18 | 4 0/16 | 5 0/14 | 6 0/10 | 显示已解决的问题

Broken Access Control | Broken Authentication | Forgotten Content | Improper Input Validation | Injection | Insecure Deserialization | Race Condition | Roll your own Security | Security Misconfiguration | Security through Obscurity | Sensitive Data Exposure | Vulnerable Components | XSS | XXE

★ 入门 挑战

名称	描述	状态
Admin Section	Access the administration section of the store.	未解决

OWASP Open Web Application Security Project

Type to search

Pwning OWASP Juice Shop

PREFACE

Introduction

Why OWASP Juice Shop exists

Architecture overview

PART I - HACKING PREPARATIONS

Hacking preparations

Running OWASP Juice Shop

Vulnerability categories

Challenge tracking

Hacking exercise rules

Walking the "happy path"

Customization

Hosting a CTF event

PART II - CHALLENGE HUNTING

Challenge hunting

Finding the Score Board

Star 1,596

Forgotten content

The challenges in this chapter are all about files or features that were simply forgotten and are completely unprotected against access.

Challenges covered in this chapter

Challenge	Difficulty
Let us redirect you to a donation site that went out of business.	★
Use a deprecated B2B interface that was not properly shut down.	★★
Retrieve the language file that never made it into production.	★★★★★
Deprive the shop of earnings by downloading the blueprint for one of its products.	★★★★★

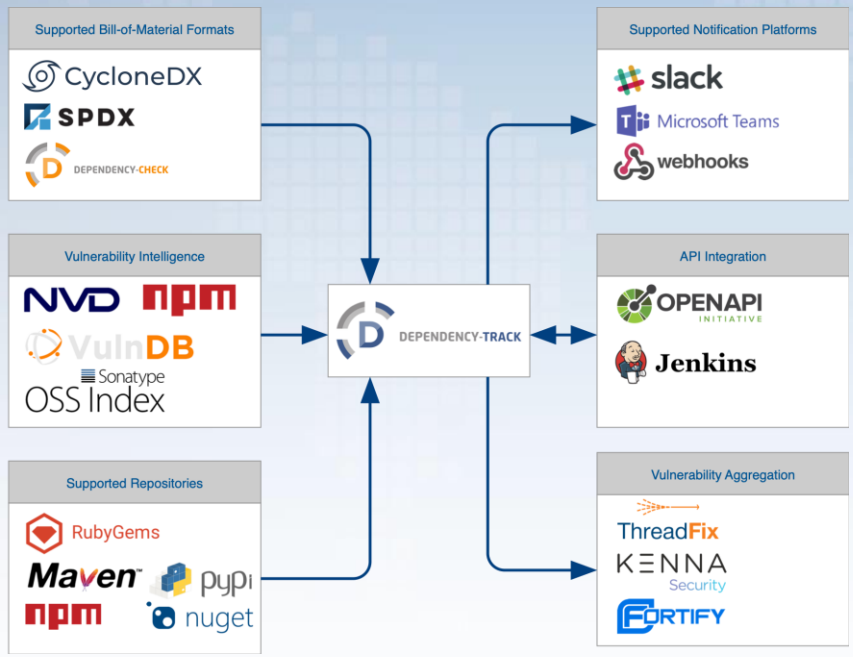
Let us redirect you to a donation site that went out of business

One of the sites that the Juice Shop accepted donations from went out of business end of 2017.

Hints

OWASP Open Web Application Security Project

OWASP DependencyTrack



简介

Dependency-Track是一个软件组合分析（SCA）平台，用于跟踪组织创建或使用的所有应用程序中使用的所有第三方组件。它集成了多个漏洞数据库，包括国家漏洞数据库（NVD），NPM公众公告， Sonatype的OSS指数，并VulnDB从基于风险的安全性。Dependency-Track监控其产品组合中的所有应用程序，以便主动识别使你的应用程序面临风险的组件中的漏洞。

主要卖点

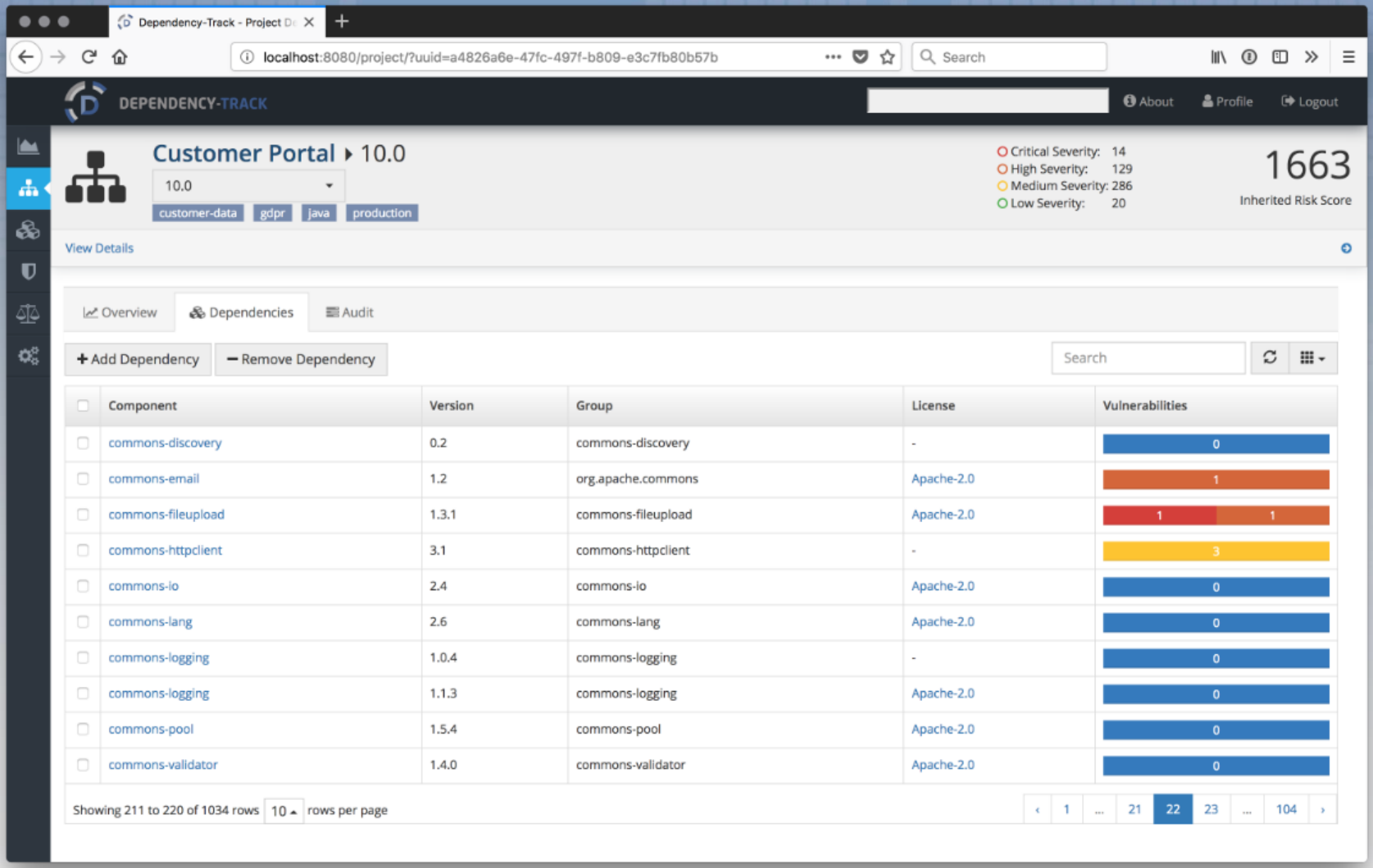
提高对易受攻击和过时组件使用的可见性
灵活的数据模型，支持无限数量的项目和组件
支持Slack，Microsoft Teams，Webhooks和Email的可配置通知
API优先设计便于与其他系统轻松集成
支持内部管理的用户，Active Directory / LDAP和API密钥
易于安装和配置。只需几分钟即可启动并运行

OWASP
Open Web Application Security Project

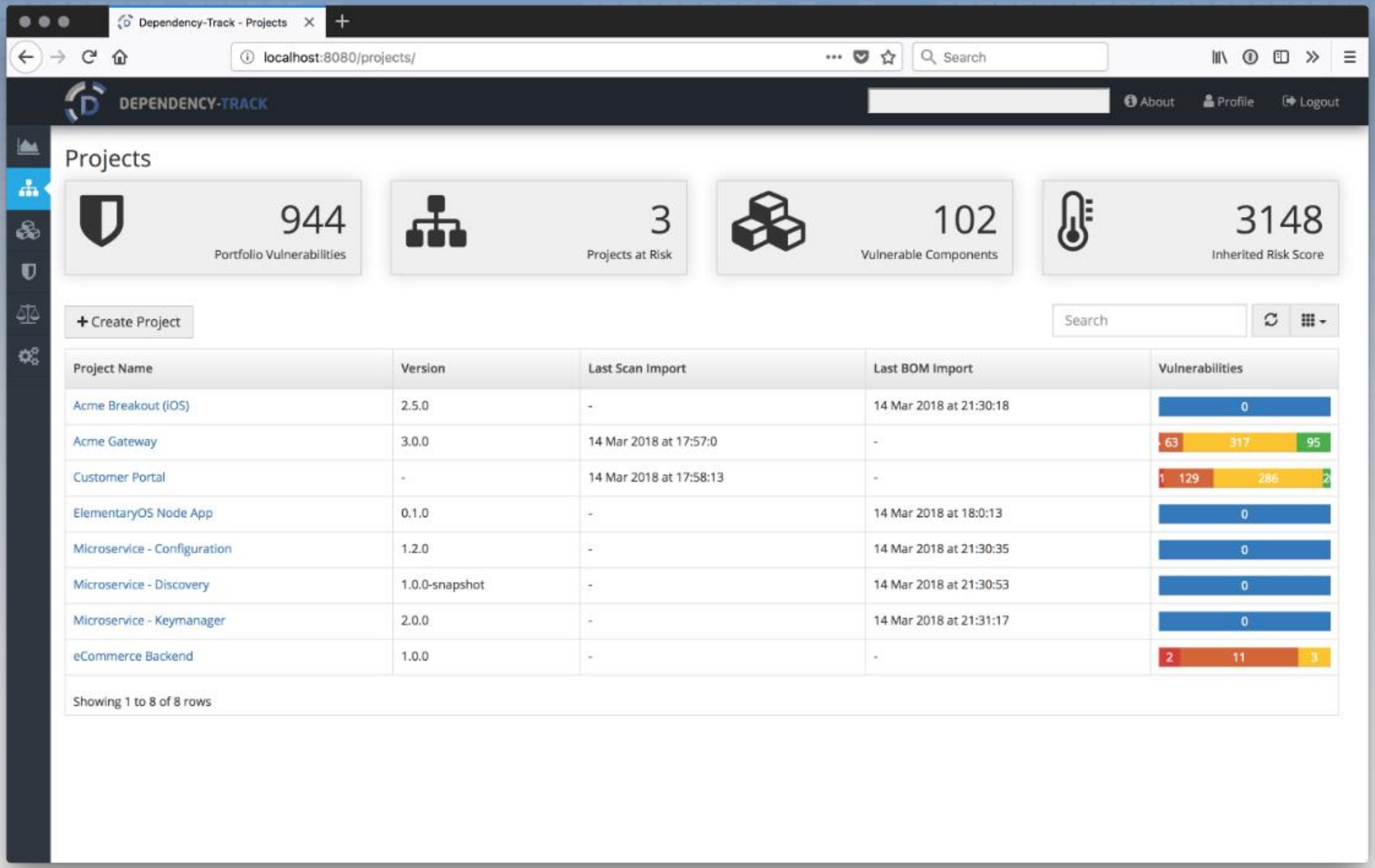
```
bogon:amass ds$ docker pull owasp/dependency-track
Using default tag: latest
latest: Pulling from owasp/dependency-track
4fe2ade4980c: Pull complete
6fc58a8d4ae4: Pull complete
819f4a45746c: Pull complete
38d737d7cef3: Pull complete
fff11c748c70: Pull complete
a67d1e63eaf1: Pull complete
944004fb7575: Pull complete
7ef76b418a87: Pull complete
acf819e564e4: Pull complete
1d9fd15b4575: Pull complete
1cd0dc7b0580: Pull complete
Digest: sha256:08c9e4b804e47ad45828128f2e261c5a7dee4840baafba669db7be427873fd2b
Status: Downloaded newer image for owasp/dependency-track:latest
```

```
bogon:amass ds$ docker volume create --name dependency-track
dependency-track
```

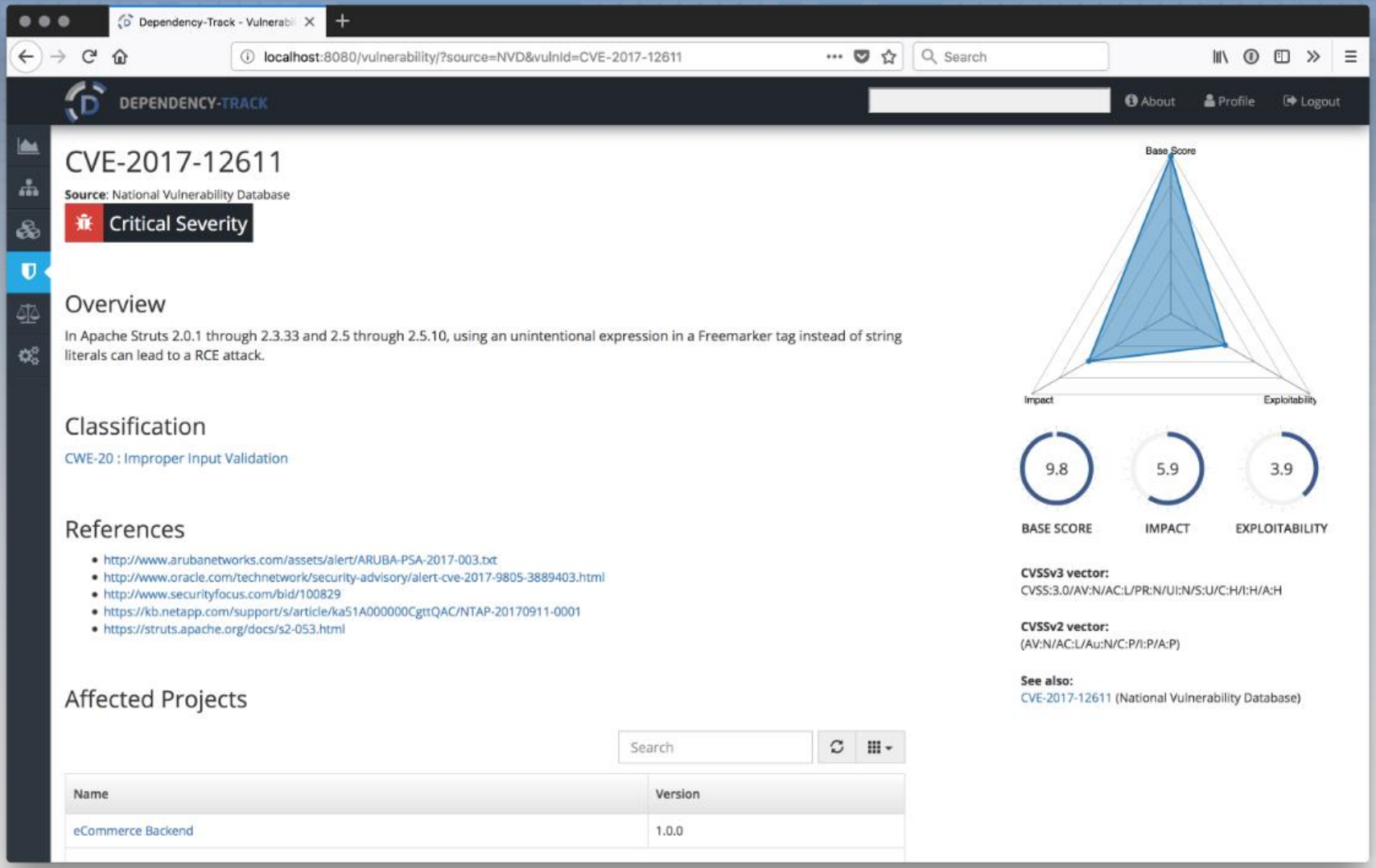
```
bogon:amass ds$ docker run -d -p 8080:8080 --name dependency-track -v dependency
-track:/data owasp/dependency-track
900bfb9359f1d68a6d4db9bdf2fd737924e67af092e7a7d7524eb005ee6d7e61
```



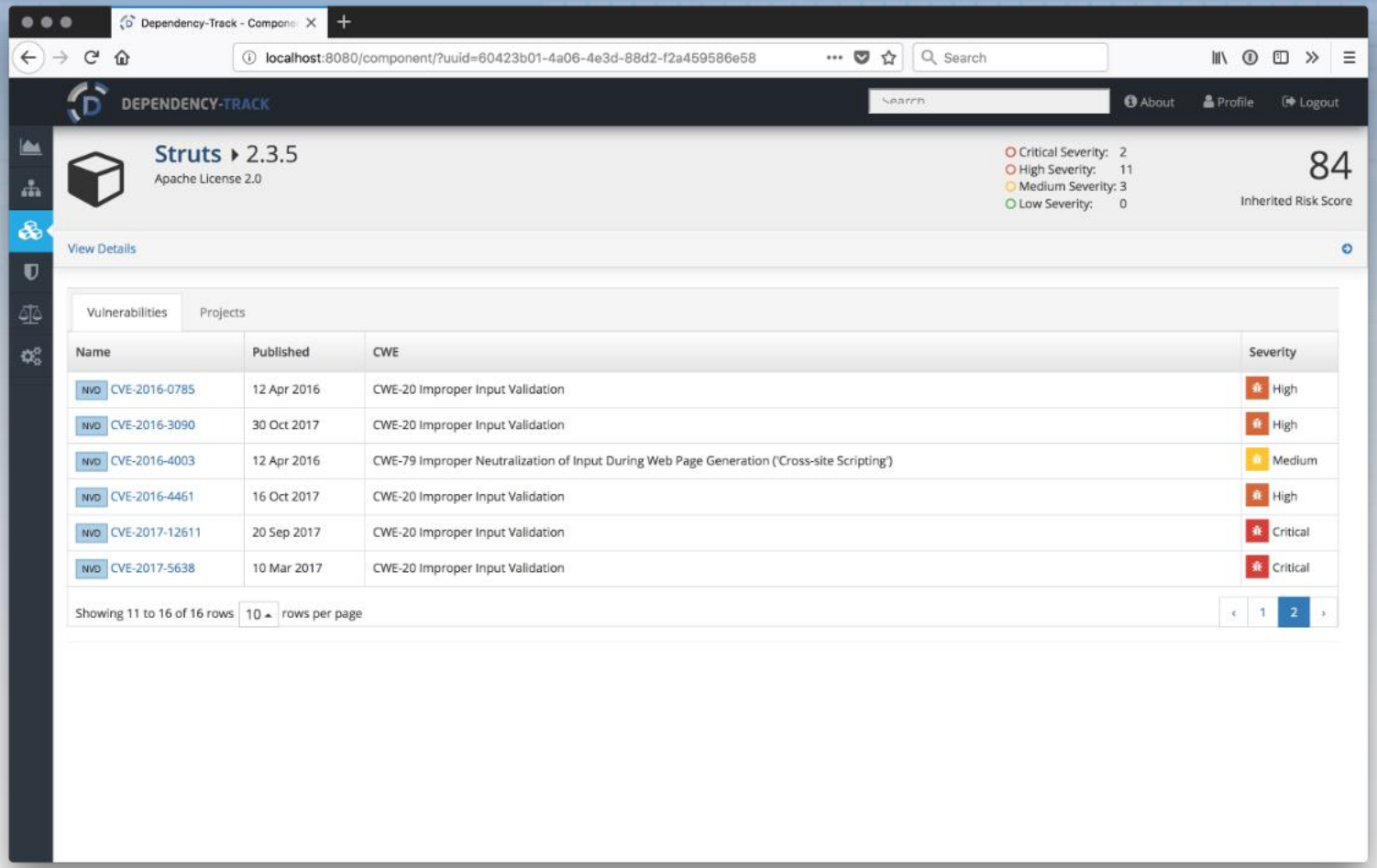
OWASP
Open Web Application Security Project



OWASP
Open Web Application Security Project



OWASP
Open Web Application Security Project



OWASP
Open Web Application Security Project