OWASP
Open Web Application
Security Project

Hacking OWASP

OWASP
Chapter República Dominicana

whoami /all

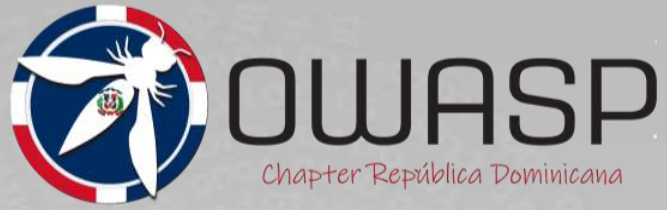
Julio Ureña / PlainText

- Twitter: @JulioUrena
- Blog: https://plaintext.do
- YouTube: https://www.youtube.com/c/JulioUreña
- Experiencia Profesional (Publico/Privado/Local/Internacional)
- Cristiano / Esposo / Padre / Amigo
- Ingeniero en Sistemas
- OSCP

Agenda

- OWASP Top 10
- Juice Shop un lugar Seguro para practicar
- Hacking Demo
  - SQL Injection
  - Combinando multiples bugs
- Defensas
- Preguntas y Respuestas

OWASP Top 10



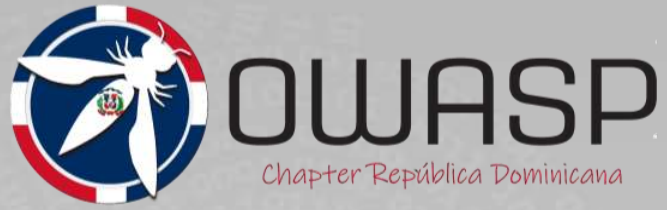
OWASP Top 10 es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la organización OWASP (Open Web Application Security Project). Esta lista se publica y actualiza cada tres años.

El objetivo de este proyecto, es crear conciencia acerca de la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones.

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Juice Shop

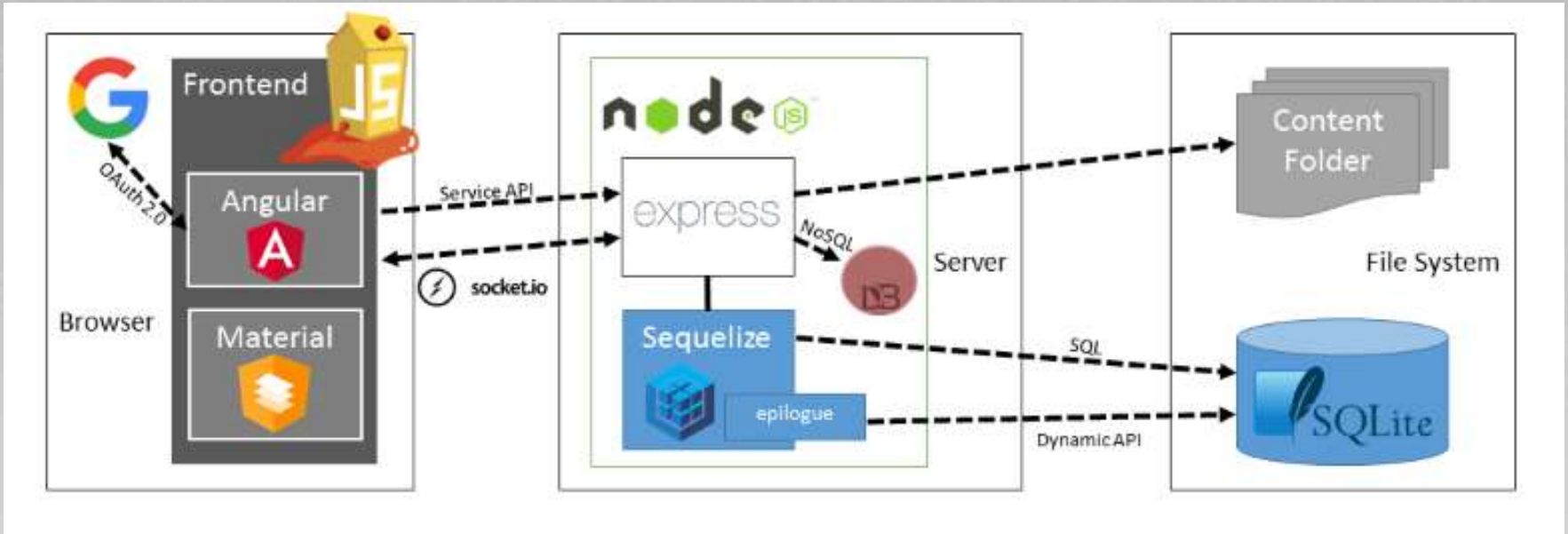


¡**OWASP Juice Shop** es probablemente la aplicación web insegura más moderna y sofisticada! ¡Se puede utilizar en entrenamientos de seguridad, demostraciones de conciencia, CTF y como conejillo de indias para herramientas de seguridad!

¡Juice Shop incluye vulnerabilidades de todo el OWASP Top 10 junto con muchas otras fallas de seguridad encontradas en aplicaciones del mundo real!

https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

Juice Shop

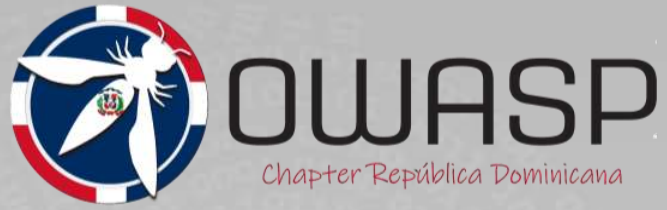


https://github.com/bkimminich/juice-shop

Vision General
Juice Shop

DEMO

Hacking Demo



Historia de un atacante. Nuestro objetivo es conseguir acceso de Administrador en la tienda. Que haremos:

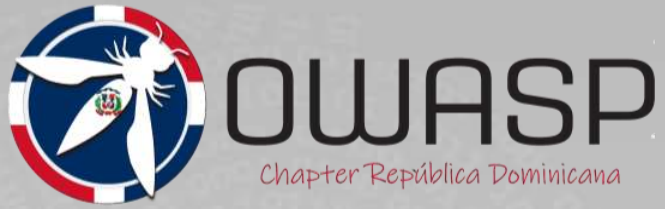
1. Uso de la pagina web.
2. Enumeración (Manual / Automática)
3. Acceso FTP (Documentos confidenciales) – (A3 / A6)
4. Identificar componentes vulnerables - (A9)
5. Obtener las credenciales de Administrador (A7)

Hacking Juice Shop

OWASP
Chapter República Dominicana

DEMO

Defensas



Opciones para establecer defensas:

- **OWASP - Documentación / Proyectos**
- **Web Application Firewalls (WAF)**
- **Análisis de Código Fuente**
- **Monitoreo de Aplicaciones**
- **Pentesting**

Gracias!

Preguntas?

Contactos: Twitter o juliourena@plaintext.do

OWASP

Chapter República Dominicana