OWASP
Open Web Application
Security Project

OWASP Security Shepherd

Aldo Salas
aldo.salas@owasp.org

Agenda

- Intro
- What is Security Shepherd
- Wait, what about WebGoat?
- Demo

About me

- 10+ years of experience in AppSec.
- Currently working for Fortune 500 Company.
- Independent researcher in free time (bug bounty).
- Chapter Leader for Aguascalientes.
- Favorite vulnerability: SQL Injection.
- Proud U.A.A. alumnus.

What is OWASP Security Shepherd?

- Web and mobile application security training platform.

What is OWASP Security Shepherd?

- Designed to foster and improve security awareness among a varied skill-set demographic.

What is NOT Security Shepherd?

- Network penetration training.
- Firewall training.
- Reverse-engineering training.
- Etc.

What does Shepherd include?

- Lots of topics: 70+ levels

- Slow learning curve
- Real world examples
- Scalable: from local to thousand users
- Highly Customizable
- Scoreboard
- Perfect for Classrooms

Topic coverage

- SQL Injection
- Broken Authentication and Session Management
- Cross Site Scripting
- Insecure Direct Object Reference
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross Site Request Forgery
- Unvalidated Redirects and Forwards
- Poor Data Validation
- Insecure Data Storage
- Poor Authentication and Authorization
- Broken crypto

- And more!

Layout options

- CTF Mode
- Open Floor
- Tournament Mode

Installation

- Manual mode:
  - Install dependencies (MySQL, Tomcat, etc.)
  - Deploy WAR
  - Profit!
- VM Mode:
  - Download VM and power it on.

Wait, what about WebGoat?

WebGoat VS Shepherd

WebGoat	Shepherd
Single user	Multiple users
One or two challenges per category	Up to 10 per category
Focuses on first-time users	Challenges experienced users
Easier to deploy	Installation requires more steps
Scorecard	Advanced scorecard
Makes host vulnerable	Safe to run even in production env
No console management	Admin console available
Not configurable	Easily configurable (close challenges)
Lessons included	Lessons included

Demo

Download:

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

Questions?

Thanks!

aldo.salas@owasp.org