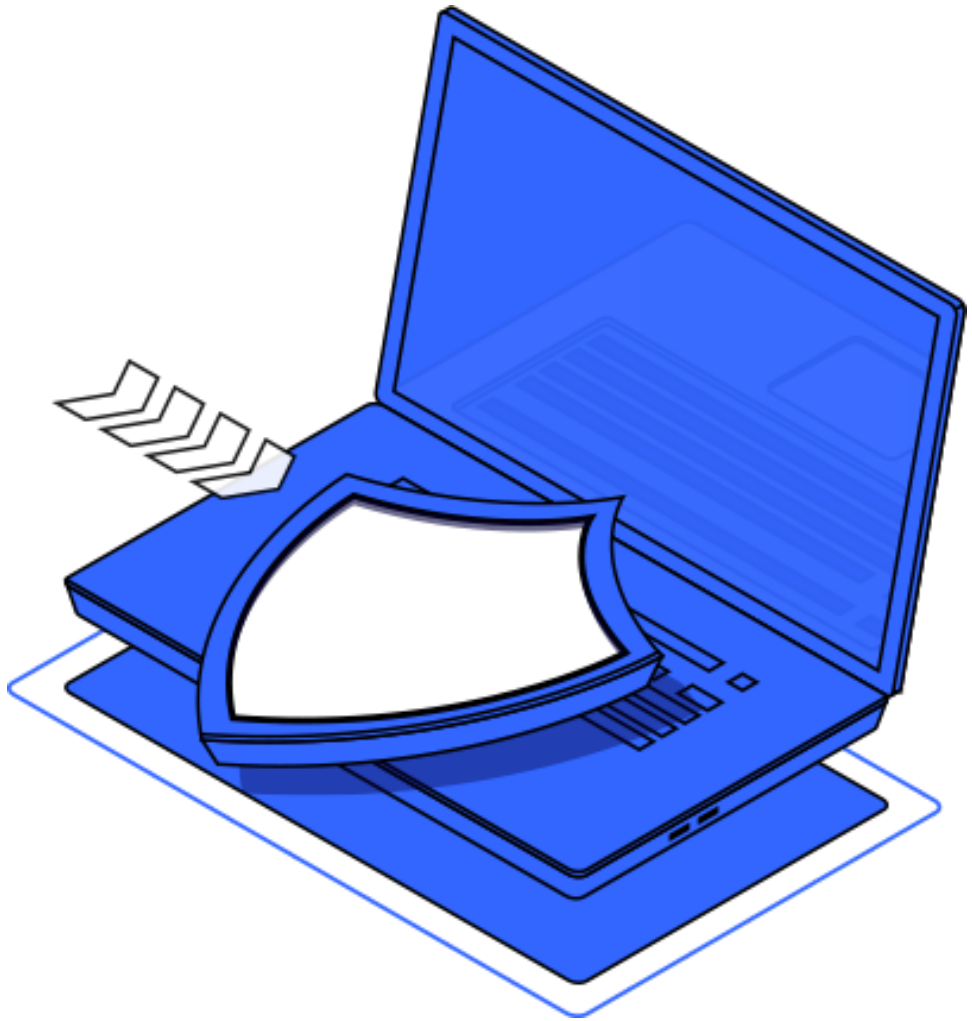
Web Application Pentesting

IES Rafael Alberti

Manuel Rivas (@0xmrivas)



Contenido

- **Técnicas de Pentesting** : Information gathering, scanning and enumeration, explotation, manteining access, and cleanup
- **Herramientas**:Burp _Suite, Nikto, Dirbuster, curl, sublist4r, nmap, WPScan...
- **Principales vulnerabidades**: OWASP To 10 y algunas otras...
- **Otros**: Documentación, recursos, ...

Recursos

- **Juice Shop** :
  - https://github.com/juice-shop/juice-shop#setup
  - https://pwning.owasp-juice.shop/
- **OWASP Testing Guides** :
  - https://owasp.org/www-project-web-security-testing-guide/v41/
  - https://github.com/tanprathan/OWASP-Testing-Checklist
- **Bug Bounties** :
  - https://github.com/tanprathan/OWASP-Testing-Checklist
  - https://www.hackerone.com/
  - https://www.synack.com/red-team/
  - https://www.guru99.com/bug-bounty-programs.html
- **Education** :
  - https://portswigger.net/web-security
  - https://www.giac.org/certifications/web-application-penetration-tester-gwapt/
  - https://www.offensive-security.com/courses-and-certifications/
  - https://www.amazon.es/Web-Application-Hackers-Handbook-Discovering/dp/1118026470

The Five stages of Ethical Hacking

Reconnaissance

Scanning and Enumeration

Gaining Access

Maintaining Access

Covering Tracks

Reconnaissance

Passive OSINT

Reconnaissance

Passive OSINT

Target Validation	Finding Subdomains	Fingerprinting	Data Breaches
• WHOIS, nslookup, dnsrecon	• Google Fu, dig, Nmap, Sublist3r, Bluto, crt.sh, etc.	• Nmap, Wappalyzer, WhatWeb, BuiltWith, Netcat	• HaveIBeenPwned and similar lists

Ejemplo

Tarea

```
Buscar información sobre la compañía XXXX.
Echemos un ojo a que información nos dan algunas de las herramientas.
```

Happy Hacking! ✌

by Manuel Rivas ([@0xmrivas][0xmrivas])