Asegure su Aplicación Web a través de una perspectiva hacker

Kenneth Webb Vargas

OWASP

The Open Web Application Security Project

Kenneth Webb V.

OWASP
The Open Web Application Security Project

- 12+ años de experiencia en desarrollo de software para Bancos, Aerolíneas, Juegos en Línea, Procesos de Manufactura y Seguridad de Información.

@KWSecDev

https://cr.linkedin.com/in/kwebbv

GIAC WEB APP PEN TESTER
GWAPT

Universidad de Costa Rica
Lucem Aspicio

Microsoft
CERTIFIED
Professional

Microsoft
CERTIFIED
Professional Developer
Web Developer

CloudSchool.com™
CLOUD CERTIFIED
Technology Professional

Scrum Alliance
CSM
CERTIFIED

Microsoft
CERTIFIED
Application Developer
Microsoft .NET

Microsoft
CERTIFIED
Technology Specialist
.NET Framework 2.0
Distributed Applications

CloudSchool.com™
CLOUD CERTIFIED
Professional

CIA

OWASP
The Open Web Application Security Project

- Pilares básicos de seguridad de la información por sus siglas en Ingles:
  - Confidentiality
  - Integrity
  - Availability

Hacker

- Pasado

- Presente

Verizon Data Breach 2017

OWASP
The Open Web Application Security Project

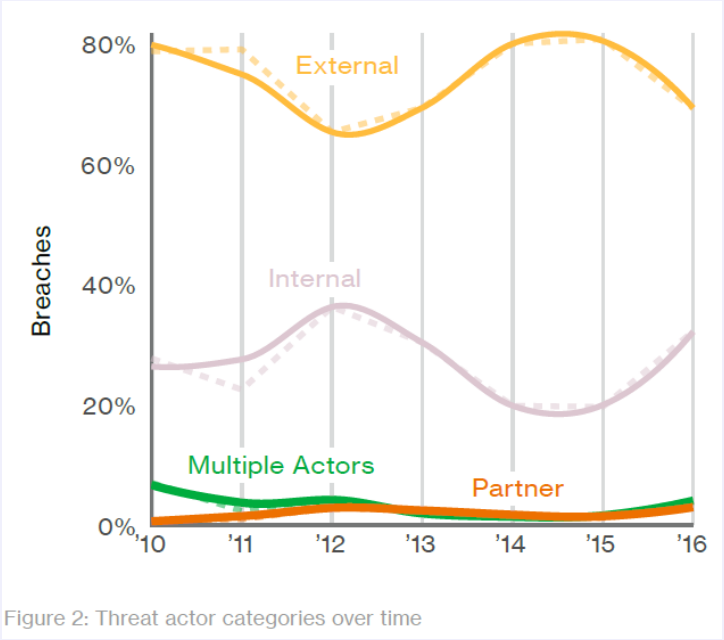


Figure 2: Threat actor categories over time

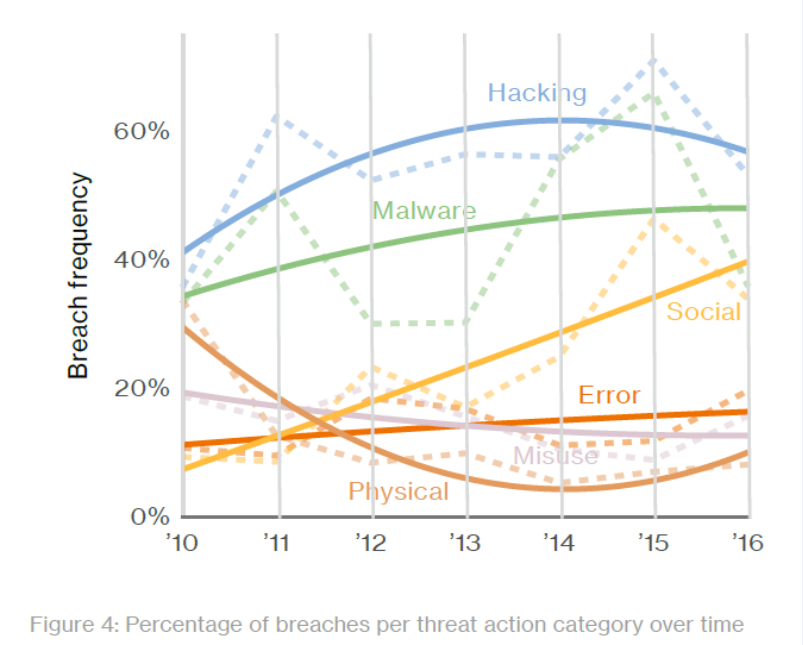


Figure 4: Percentage of breaches per threat action category over time

Fuente:
http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

Verizon Data Breach 2017

OWASP
The Open Web Application Security Project

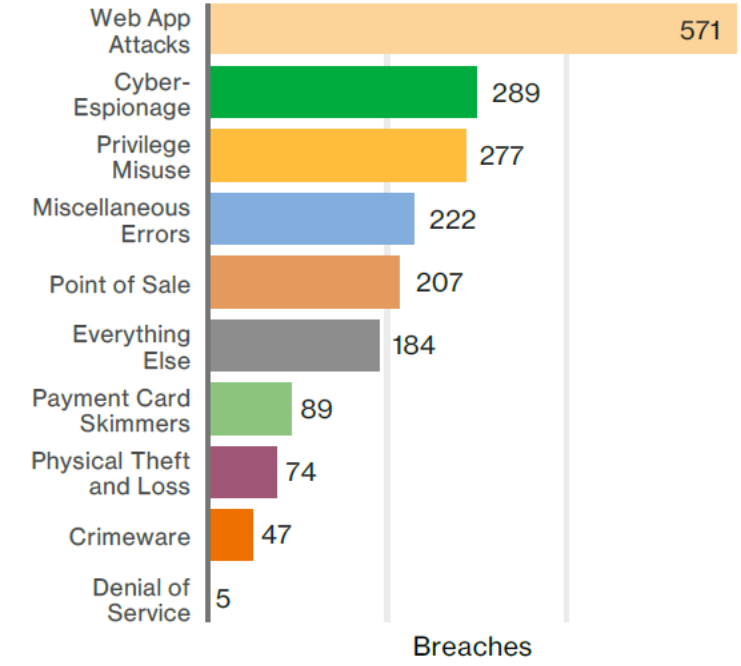


Figure 33: Percentage and count of breaches per pattern (n=1,935)

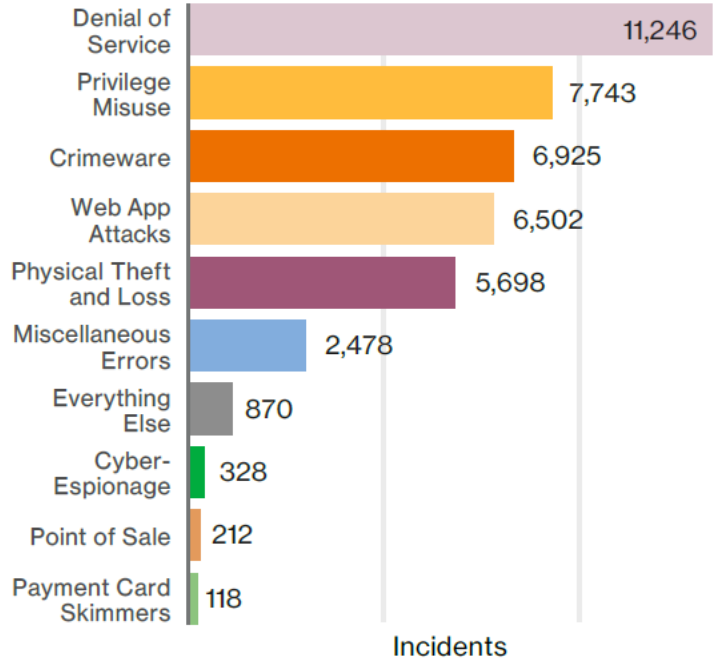


Figure 34: Percentage and count of incidents per pattern (n=42,068)

Fuente:
http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

OWASP
The Open Web Application Security Project

IMPORTANTE

El proceso que se describe a continuación es con fines didácticos para entender el pensamiento de un Hacker y de esta manera asegurar las aplicaciones web.

EL USO DE LAS HERRAMIENTAS LISTADAS A CONTINUACIÓN SIN AUTORIZACIÓN EN APLICACIONES WEB PUEDE GENERAR ACCIONES LEGALES!

OWASP
The Open Web Application Security Project

- Fases:
  - Planeamiento
  - Reconocimiento
  - Mapeo de la Aplicación Web
  - Análisis de Vulnerabilidades
  - Explotar Vulnerabilidades

  Otras como:
  - Limpieza de Rastro

PLANEAMIENTO

Planeamiento

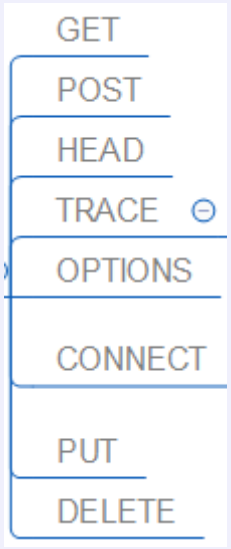
OWASP
The Open Web Application Security Project

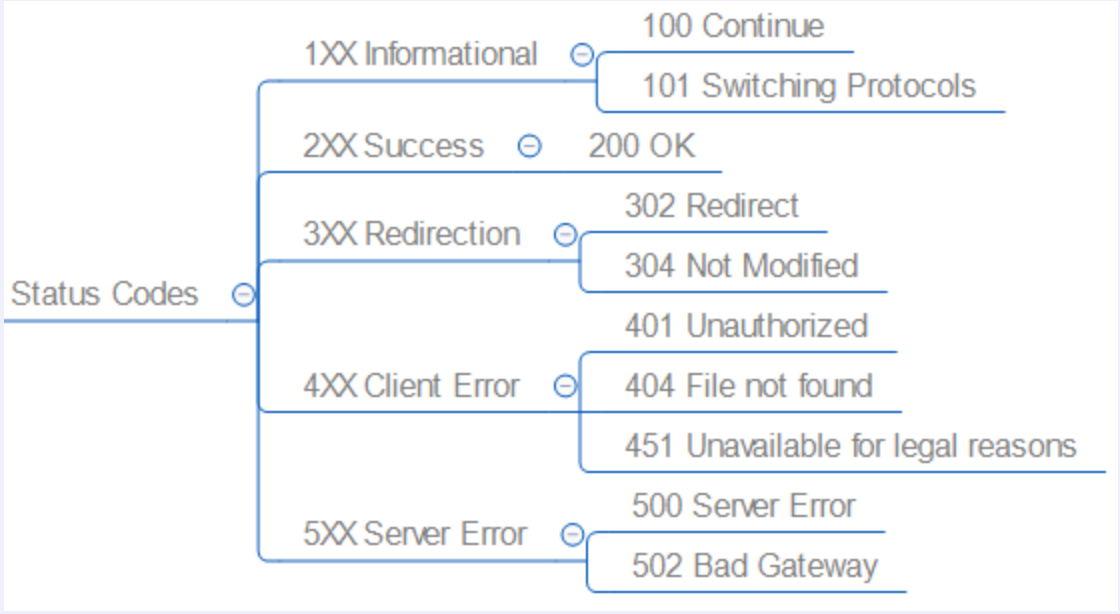
- Plataforma de Ataque (Kali, Windows, SamuraiWTF)
- Web Application Security Scanner (ZAP, Burp, etc.)
- Browser (Mozilla, Chrome)

Planeamiento

OWASP
The Open Web Application Security Project

- Protocolo HTTP
- Métodos





OWASP
The Open Web Application Security Project

User Agent:

Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;rv:11.0) like Gecko

Asegure su aplicacion

OWASP
The Open Web Application Security Project

- Conozca los detalles de las plataformas utilizadas, el protocol HTTP y los diferentes User Agent para identificar amenazas en su aplicacion web.

OWASP
The Open Web Application Security Project

RECONOCIMIENTO

Informacion de DNS y WHOIS

OWASP
The Open Web Application Security Project

- WHOIS

```
[~]$ dig demo.testfire.net

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> demo.testfire.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27858
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;demo.testfire.net.             IN      A

;; ANSWER SECTION:
demo.testfire.net.      15998   IN      A       65.61.137.117

;; Query time: 85 msec
;; SERVER: 10.248.2.1#53(10.248.2.1)
;; WHEN: Wed Apr 18 09:15:39 PDT 2018
;; MSG SIZE  rcvd: 62
```

Informacion de DNS y WHOIS

OWASP
The Open Web Application Security Project

- DNS
  - **Transferencia de zona:** dig demo.testfire.net –t axfr
  - **Reverse DNS**: dnsrecon.py -r 10.248.2.0/24
  - Nslookup:

```
[~]$ nslookup demo.testfire.net
Server:         10.248.2.1
Address:        10.248.2.1#53

Non-authoritative answer:
Name:   demo.testfire.net
Address: 65.61.137.117
```

Mas informacion…

OWASP
The Open Web Application Security Project

- Buscadores
  - DuckDuckGo
  - Google
  - Yahoo
  - Bing
- Social Networks
- Shodan
- FOCA

Otras herramientas…

OWASP
The Open Web Application Security Project

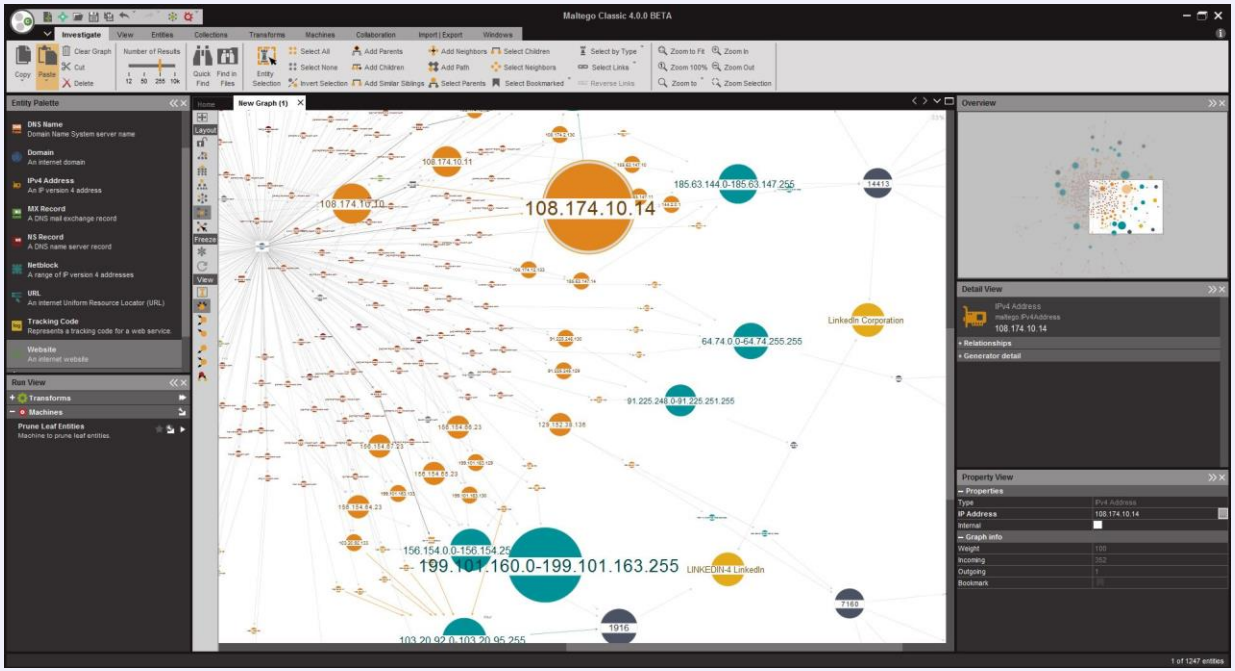
- theHarverster

```
[~]$ theHarvester -d demo.testfire.net -b all


*******************************************************************
*                                                                 *
* | |_| |__   ___      /\  /\__ _ _ ____   _____  ___| |_ ___ _ __   *
* | __| '_ \ / _ \    / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|  *
* | |_| | | |  __/   / __  / (_| | |   \ V /  __/\__ \ ||  __/ |     *
*  \__|_| |_|\___|   \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* TheHarvester Ver. 2.3                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Full Search:
[-] Searching Google:
```

Mas herramientas…

OWASP
The Open Web Application Security Project

- Maltego
- Recon-ng
- nmap



Que otras acciones?

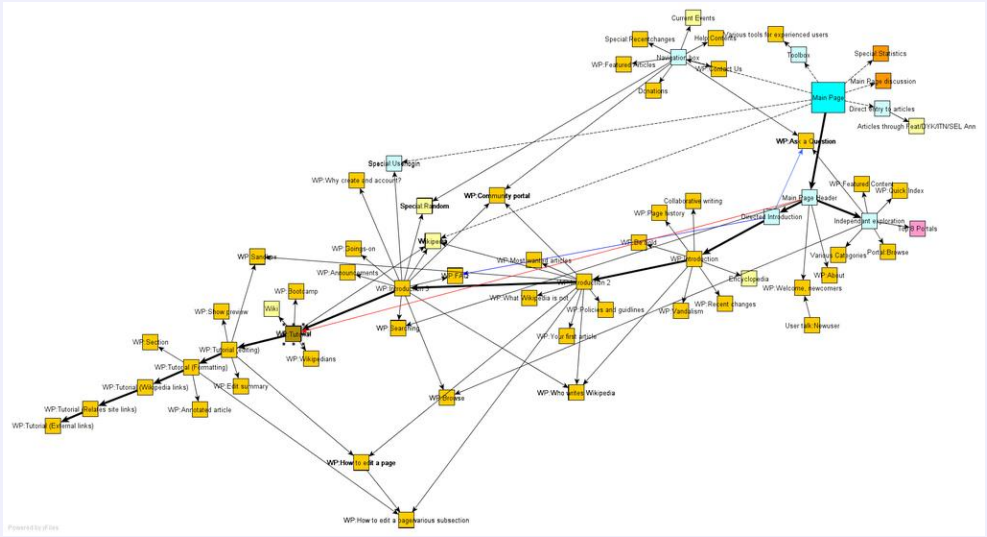
OWASP
The Open Web Application Security Project

- Ademas en esta fase los hackers prueban:
  - Weak Ciphers (SSL Certificates)
  - Heartbleed
  - Server Profiling

Asegure su aplicacion

OWASP
The Open Web Application Security Project

- Ejecute estas acciones en sitios web de su empresa (con permiso firmado para hacerlo) y valide que informacion, su aplicacion web y sus colaboradores, estan divulgando al mundo.

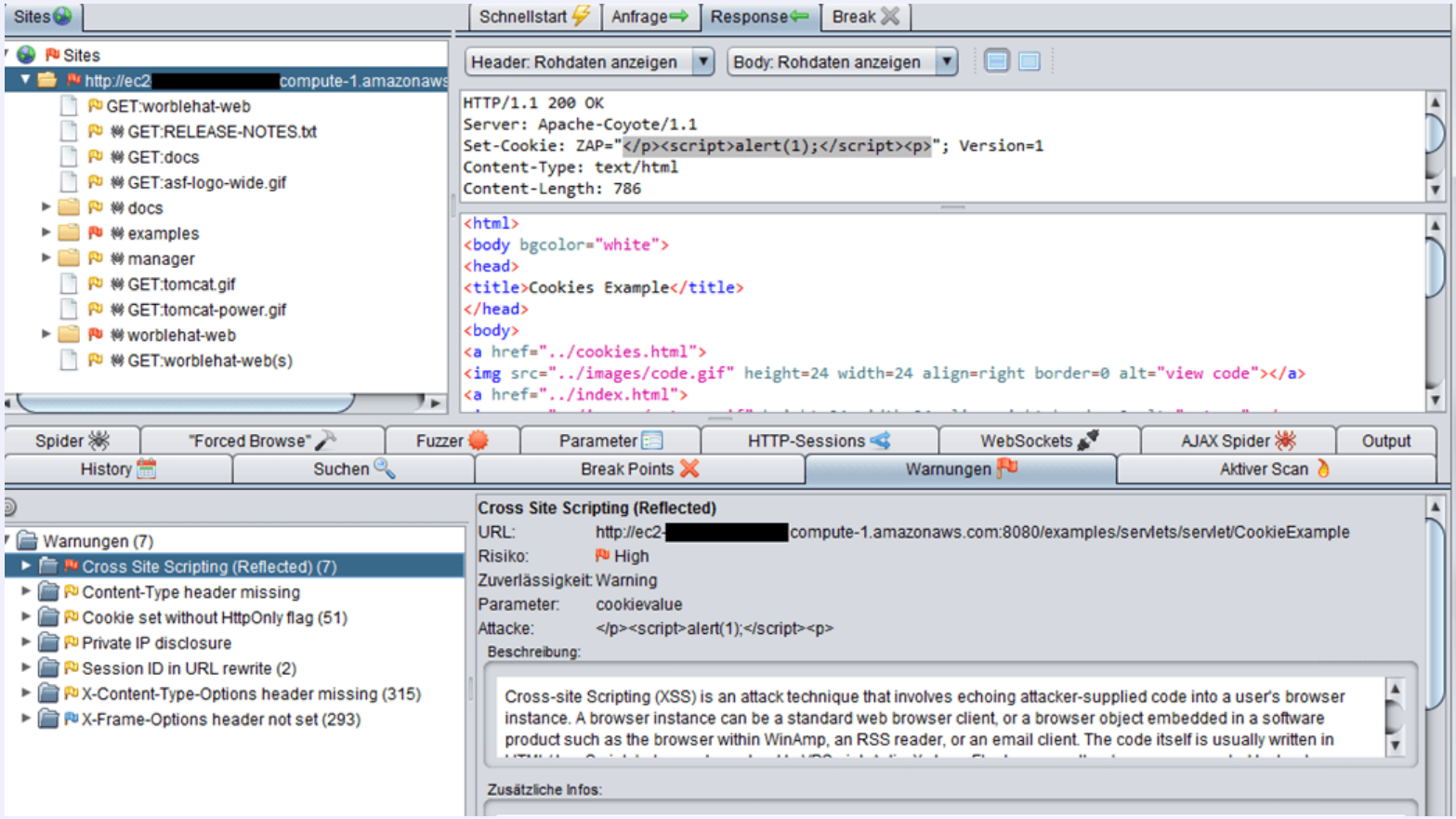

Current Events
Special Recentchanges
Help Contents
Various tools for experienced users
Toolbox
Special Statistics
Donations
Contact Us
Main Page discussion
Main Page
Direct Entry to articles
Articles through Search
WP:Ask a Question
Special Random
WP:Community portal
Collaborative writing
WP:Page history
Directed Introduction
Independent exploration
Portal Portals
Various Categories
Portal Browse
WP:Introduction
WP:About
WP:Welcome, newcomers
WP:Recent changes
WP:Vandalism
User talk:Newuser
WP:Most wanted articles
WP:What Wikipedia is not
WP:Policies and guidlines
WP:Your first article
WP:Who edits Wikipedia
WP:Browse
WP:How to edit a page
WP:How to edit a page:various subsection
WP:Sandbox
WP:Show preview
WP:Section
WP:Tutorial (Formatting)
WP:Tutorial (Wikipedia links)
WP:Tutorial (Relative site links)
WP:Tutorial (External links)
WP:Edit summary
WP:Annotated article
WP:Wikipedians
WP:Learning
WP:Same-on
WP:Accounts

MAPEO

Tecnicas Utilizadas

OWASP
The Open Web Application Security Project

- Spidering o Crawling



Pruebas sobre el sitio web

OWASP
The Open Web Application Security Project

- Fuzzing
- Busqueda de divulgacion de informacion (Information Leakage)
  - OTG-CONFIG-004 (Owasp test)
  - Herramientas:
    - Nikto
    - ZAP (Forced browse)
    - Metasploit’s WMAP

Pruebas sobre el sitio web

OWASP
The Open Web Application Security Project

- Que autenticación utiliza?
  - Basic
  - Digest
  - Integrated Windows
  - Form Based
  - OAuth

OWASP
The Open Web Application Security Project

- Username Harversting!!!
  - Tenemos toda la informacion de la fase de reconocimiento de incluso personas, intentemos adivinar usuarios
  - OWASP Test: OTG-IDENT-004-Testing for Account Enumeration

Asegure su aplicacion

OWASP
The Open Web Application Security Project

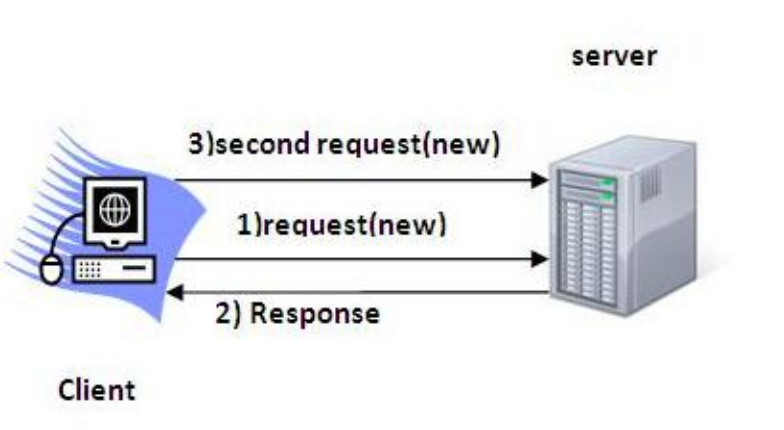
- Haga un mapeo de sus aplicaciones web:
  - ¿Qué archivos, directorios y links tienen?
  - ¿Qué información hay en esos archivos? Credenciales en comentarios?
  - ¿Qué tipo de autenticación utiliza? ¿Utiliza autenticación de dos pasos o mas?
  - Ejecute las pruebas de OWASP sobre sus aplicaciones web

OWASP
The Open Web Application Security Project

ANALISIS DE VULNERABILIDADES

Session Tracking

- Tipos de Sesión:
  - Cliente
  - Server
- Formas de tracking:
  - Cookies
  - Parámetros en el URI
  - Campos escondidos
- Herramientas de ataque:
  - Proxies como ZAP o Burp
  - Scripts de fuerza bruta



Session Fixation

OWASP
The Open Web Application Security Project

- Herramientas:
  - Burp Sequencer Session Analysis

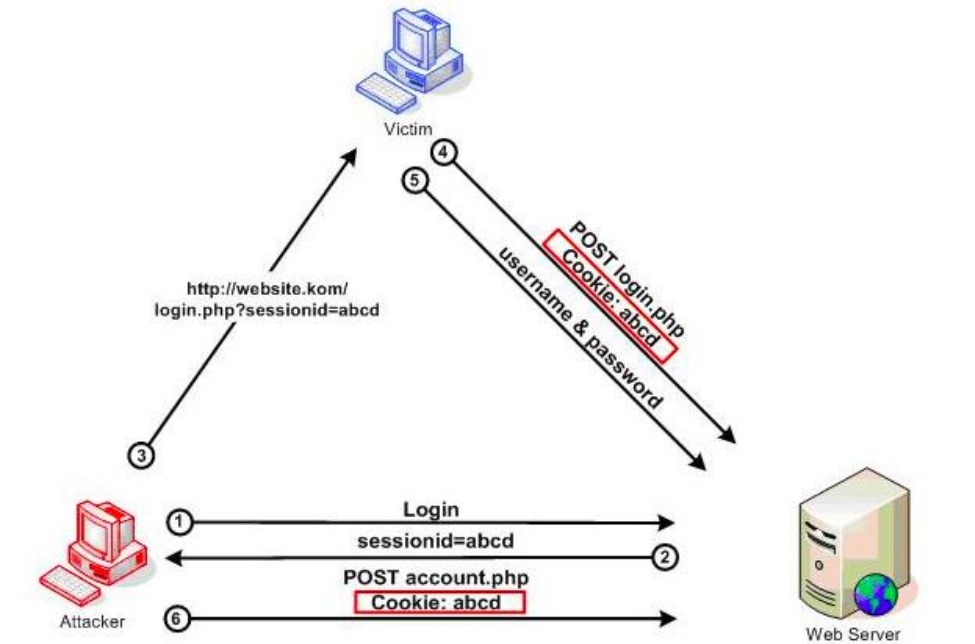


Figure 1. Simple example of Session Fixation attack.

Sobrepasar Autenticación

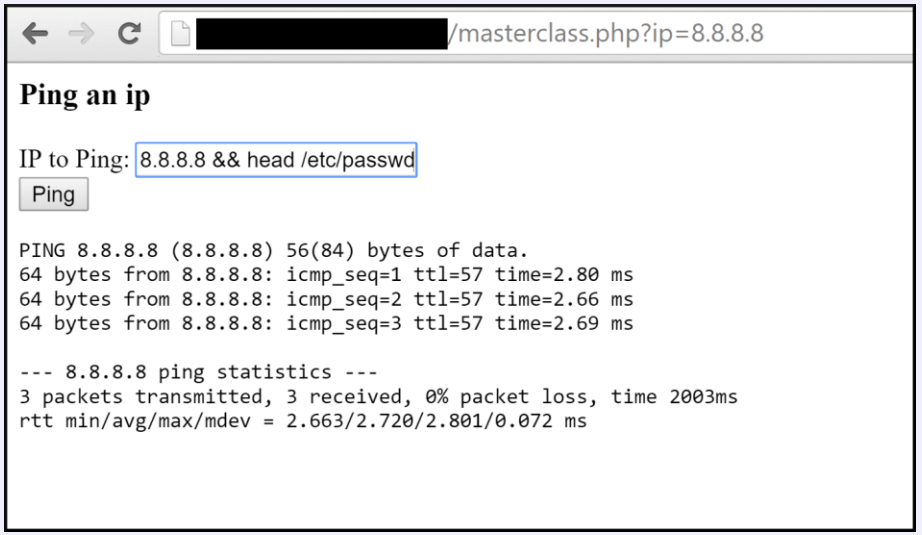
OWASP
The Open Web Application Security Project

- El atacante utiliza el mapeo para acceder recursos directamente que no estén protegidos por seguridad.
- Se utilizan scripts para automatizar este proceso

Command Injection

OWASP
The Open Web Application Security Project

- Caracteres amigos para esta vulnerabilidad:
  - &
  - &&
  - ||
  - >
  - <
  - ;



- OTG-INPVAL-013 - Testing for Command Injection

File Inclusion/Directory Traversal

OWASP
The Open Web Application Security Project

OTG-INPVAL-012 - Testing for Code Injection (LFI/RFI)

Request del sitio web:

GET http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1
Host: test.webarticles.com

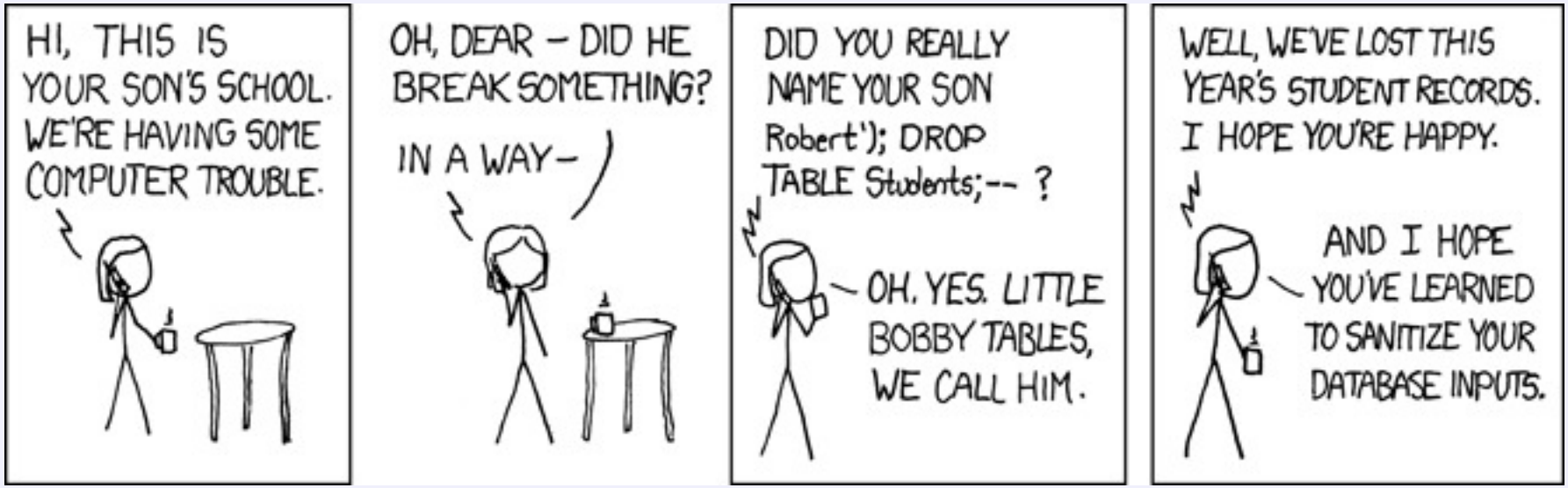
Request de prueba:

GET http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1
Host: test.webarticles.com

SQL Injection

OWASP
The Open Web Application Security Project

- Campos de entrada de datos en las paginas
- ‘ or 1=1; -- **(Payload ☺)**



XSS

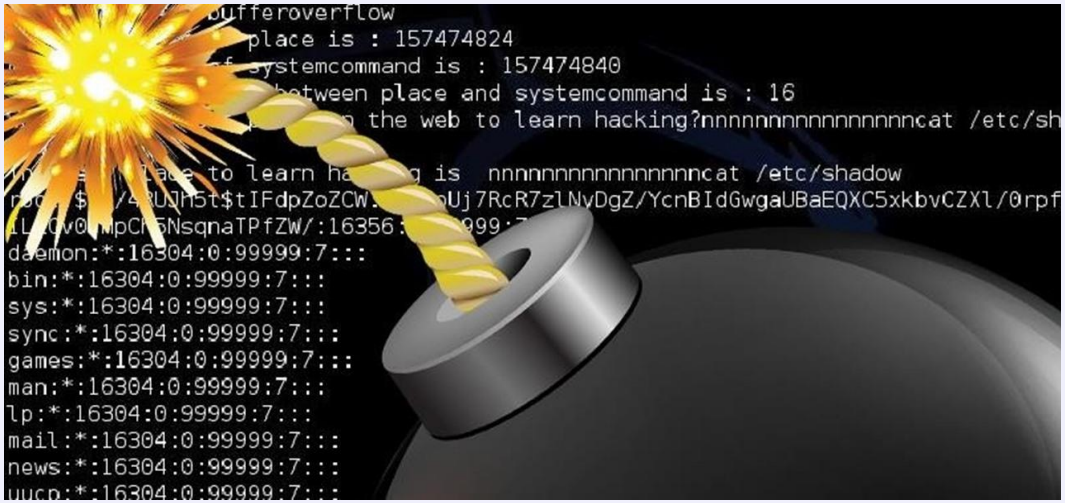
OWASP
The Open Web Application Security Project

- Tipos:
  - Reflejado
  - Persistente
  - Basado en DOM
- Se utilizan campos de entrada de datos así como parámetros en el URL
- Herramientas de análisis:
  - XSSer
  - XSScrapy
  - xssniper

Asegure su aplicacion

OWASP
The Open Web Application Security Project

- Como mínimo pruebe su aplicación con la guía de OWASP Top 10
- Utilice las librerías del lenguaje de programación para limpiar la entrada del usuario.
- Este al tanto también del Top 25 de SANS sobre vulnerabilidades de software



EXPLOTAR VULNERABILIDADES

Explotar Vulnerabilidades

OWASP
The Open Web Application Security Project

- Una vez encontradas las vulnerabilidades el atacante puede realizar ataques manuales o puede utilizar herramientas para mayor efectividad.

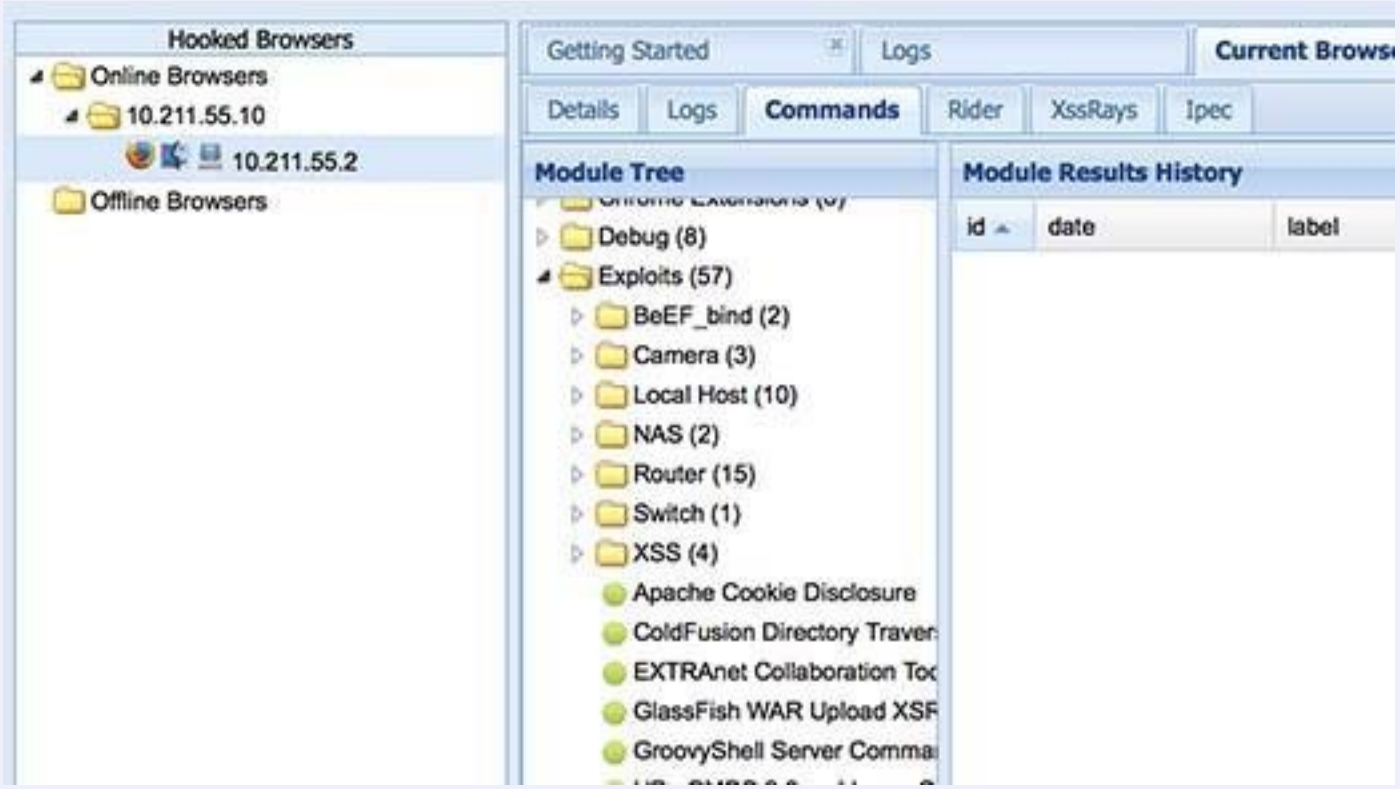
SQL Injection

OWASP
The Open Web Application Security Project

- Sqlmap

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
        _
___ ___| |_____ ___ ___  {1.0.5.63#dev}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
```

BeEF: Browser Exploitation Framework



Asegure su Aplicacion

OWASP
The Open Web Application Security Project

- Pruebe su aplicación: OWASP Testing Guide
- Utilice herramientas de pruebas en su proceso de desarrollo:
  - OWASP ZAP
  - W3af – Web Applications Attack and Audit Framework

OWASP
The Open Web Application Security Project

MUCHAS GRACIAS!