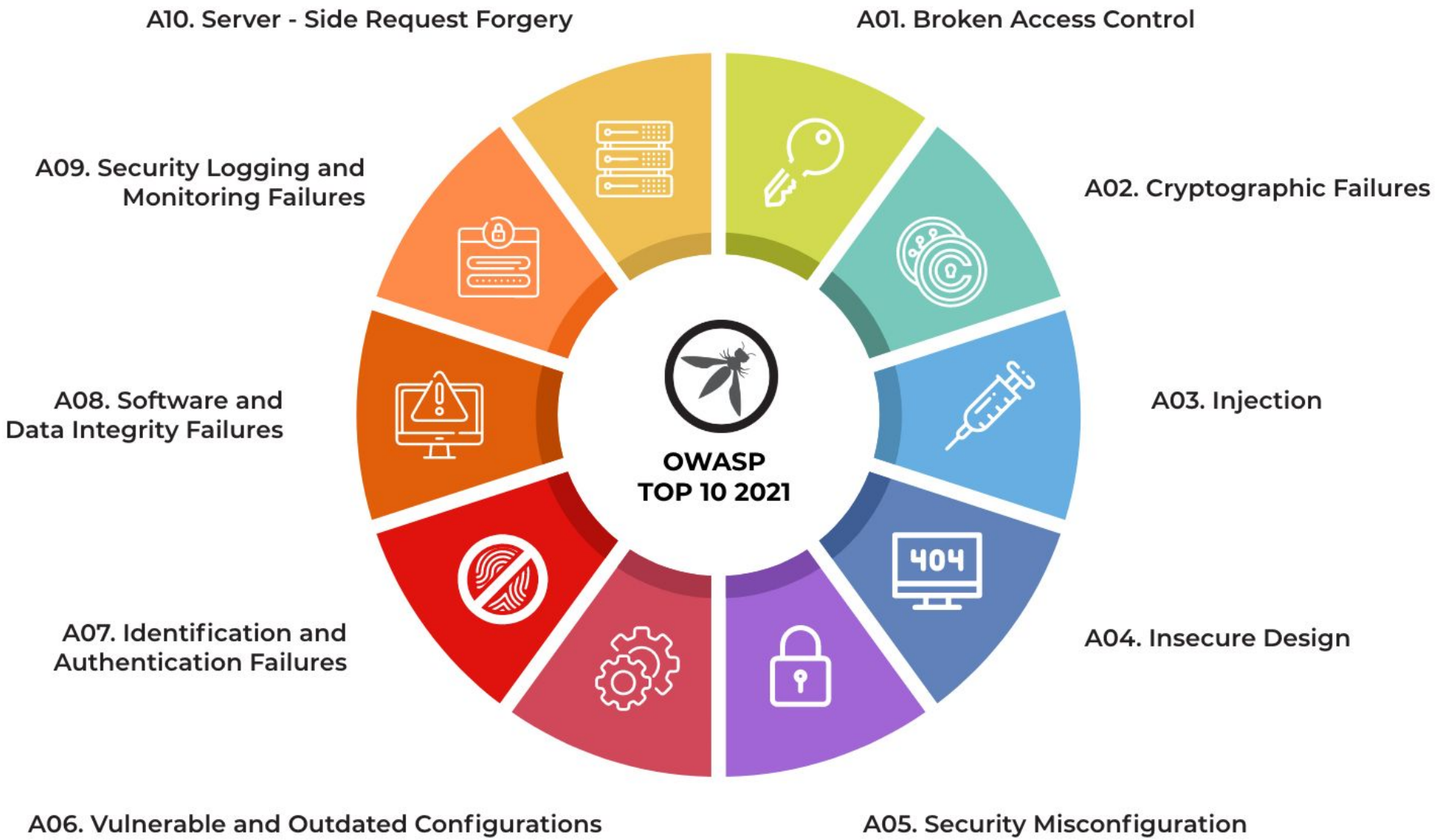
Curso de

Hacking de Aplicaciones Web: Server-Side

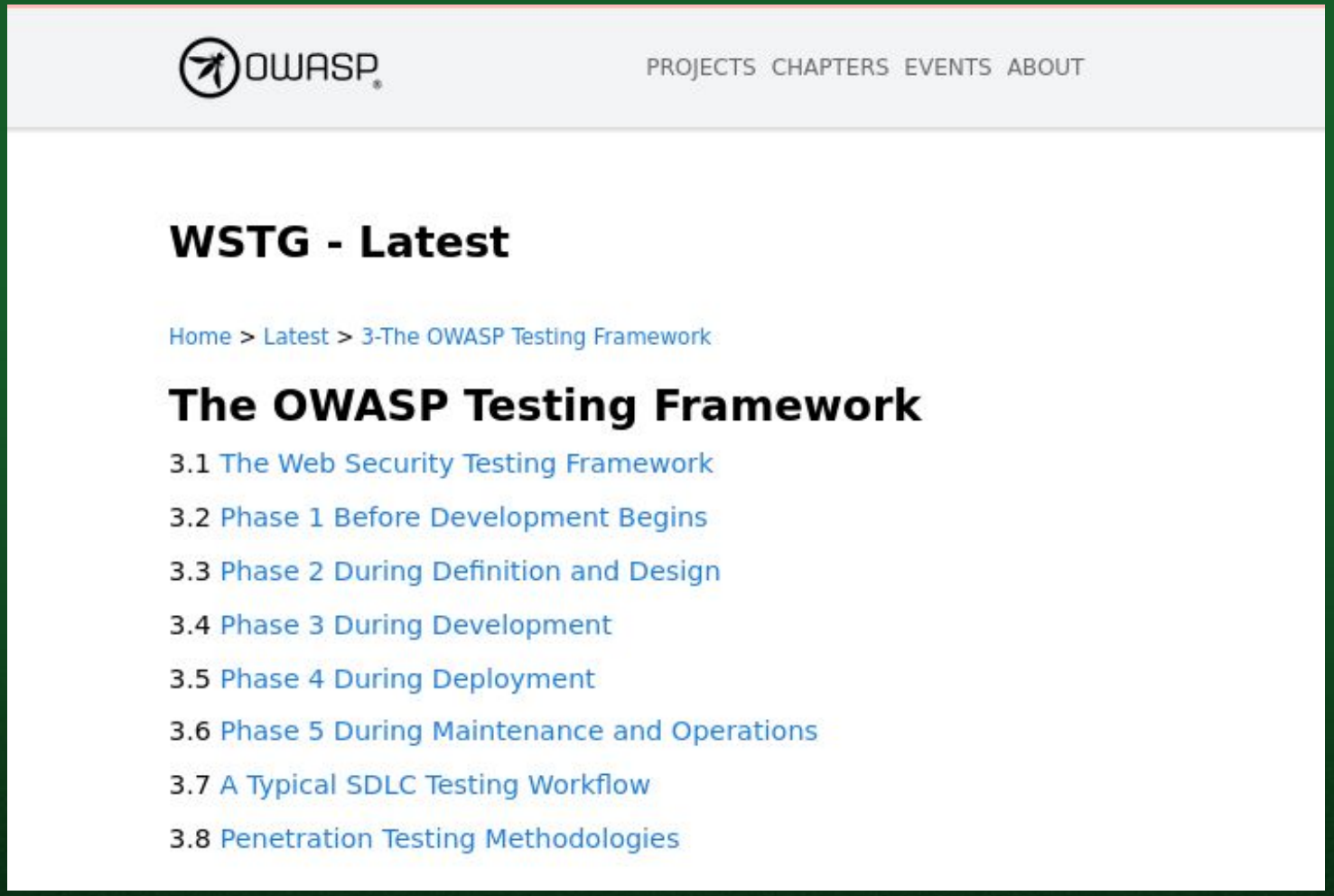
Daniel Carvajal

¿Qué es la OWASP?

Open Web Application Security Project.


A10. Server - Side Request Forgery
A01. Broken Access Control
A09. Security Logging and Monitoring Failures
A02. Cryptographic Failures
A08. Software and Data Integrity Failures
A03. Injection
OWASP TOP 10 2021
A07. Identification and Authentication Failures
A04. Insecure Design
A06. Vulnerable and Outdated Configurations
A05. Security Misconfiguration

OWASP Testing Guide



Burpsuite: Análisis de solicitudes HTTP

¿Qué es HTTP?

Hypertext Transfer Protocol

Hypertext Transfer Protocol Secure

```
Http://user:password@control.website.com:80/productos/view_products?id=3#Contact

Schema = HTTP, HTTPS, FTP
Autenticación = user:password
Subdominio = control
Host / Dominio = website.com
Puerto = :80, :443, :8080, :8081
Ruta = /products/view_product.php
Parámetros= ?id=3&category=10
Fragmento = #contact
```

HTTP: Métodos y Códigos de Status

Métodos HTTP

- GET
- HEAD
- POST
- PUT
- DELETE

```
GET /courses.php?course=1 HTTP/1.1
Host: platzi.com
User-Agent: Mozilla/5.0 Firefox/87.0
Referrer: https://platzi.com/
```

```
POST /courses.php HTTP/1.1
Host: platzi.com
User-Agent: Mozilla/5.0 Firefox/87.0
Referrer: https://platzi.com/


course=1
```

```
HEAD / HTTP/1.1
Host: platzi.com
User-Agent: Mozilla/5.0 Firefox/87.0
Referrer: https://platzi.com/
```

```
PUT /new.html HTTP/1.1
Host: platzi.com
Content-type: text/html
Content-length: 16

<p>New File</p>
```

```
DELETE /file.html HTTP/1.1
Host: platzi.com
```

Códigos de Status HTTP

200 - OK	The request was completed successfully.
201 - Created	A resource has been created (for example a new user or new blog post).
301 - Permanent Redirect	This redirects the client's browser to a new webpage or tells search engines that the page has moved somewhere else and to look there instead.
302 - Temporary Redirect	Similar to the above permanent redirect, but as the name suggests, this is only a temporary change and it may change again in the near future.
400 - Bad Request	This tells the browser that something was either wrong or missing in their request. This could sometimes be used if the web server resource that is being requested expected a certain parameter that the client didn't send.
401 - Not Authorised	You are not currently allowed to view this resource until you have authorised with the web application, most commonly with a username and password.
403 - Forbidden	You do not have permission to view this resource whether you are logged in or not.
405 - Method Not Allowed	The resource does not allow this method request, for example, you send a GET request to the resource /create-account when it was expecting a POST request instead.
404 - Page Not Found	The page/resource you requested does not exist.
500 - Internal Service Error	The server has encountered some kind of error with your request that it doesn't know how to handle properly.
503 - Service Unavailable	This server cannot handle your request as it's either overloaded or down for maintenance.

Cabeceras HTTP y Cookies

```
GET /licenses HTTP/1.1
Host: enterprise-platform.nordsec.com
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: es-419,es;q=0.9
Connection: close
```

```
GET /licenses HTTP/1.1
Host: enterprise-platform.nordsec.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
S

Content-Length:

Accept-Encoding: gzip, deflate

Accept-Language: es-419,es;q=0.9

Connection: close
Cookie:SSID=AI3jL1cvRnSBmGQ4S;
```

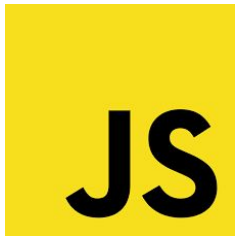
¿Qué son las Cookies?

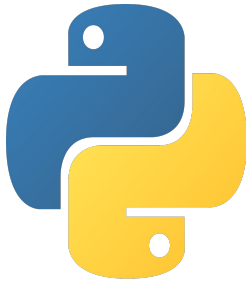
Tipos de Aplicaciones Web y Análisis de sus Tecnologías

Web Estática *vs* Web Dinámica

Vanilla Code

- PHP
- ASP
- Go
- Python
- Ruby
- JavaScript
- SQL





Frameworks

- Laravel (PHP)
- Django (Python)
- Rails (Ruby)
- GIN (Gonic)
- Next.js (JavaScript)

Content Management System

- WordPress
- Joomla
- Drupal
- Magento
- Wix
- Blogger

Defacement: Vulnerabilidad en File Upload

Técnicas de File Inclusion: Local y Remote

Full Path Disclosure y Directory Traversal

Full Path Disclosure

Provocas un error

Obtienes la ruta completa del archivo

Permite reconocer la arquitectura de la aplicación y el sistema de archivos

Directory Traversal

Incluyes archivos locales del sistema

Obtienes información sensible

Command Injection

SQL Injection Manual

SQL Injection Automatizada con SQLMap