

**API Penetration Testing Report Of VAmPI For Open**

**Web Application Security Project (OWASP)**

tabla de contenido

3 Resumen del proyecto

# Detalles de las vulnerabilidades

# Resumen Ejecutivo

Hacking Mind Corp se realizó una evaluación de seguridad integral de Open Web Application Security Project (OWASP) para determinar las vulnerabilidades existentes y establecer el nivel actual de riesgo de seguridad asociado con el entorno y las tecnologías en uso. Esta evaluación aprovechó las pruebas de penetración y las redes sociales, técnicas de ingeniería para proporcionar a la gerencia de Open Web Application Security Project (OWASP) una comprensión de los riesgos y postura de seguridad de su entorno corporativo.

# Detalles del proyecto

Este compromiso se llevó a cabo para evaluar la postura de seguridad de los objetivos de alto valor mencionados por nuestro cliente Open Web Application Security Project (OWASP). Hemos revisado VAmPI API Penetration Testing según el marco de las metodologias OWASP

Resumen del proyecto

# Alcance

**Alcance Tipo de alcance Fecha de inicio Fecha de finalización**

http://localhost:5000/api/v1 API Penetration Testing Oct. 17, 2022 Nov. 1, 2022

Descripción

prueba de seguridad al microservicio VAmPI

# Involucrados en el proyecto

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Email Address** | **Phone** | **Company** |
| Prueba prueba | test@owasp.org | +150239133111 | Open Web Application Security Project (OWASP) |

Jeremy jeremy2212landa@gmail.com 584120977285 Hacking Mind Corp

Detalles de las vulnerabilidades

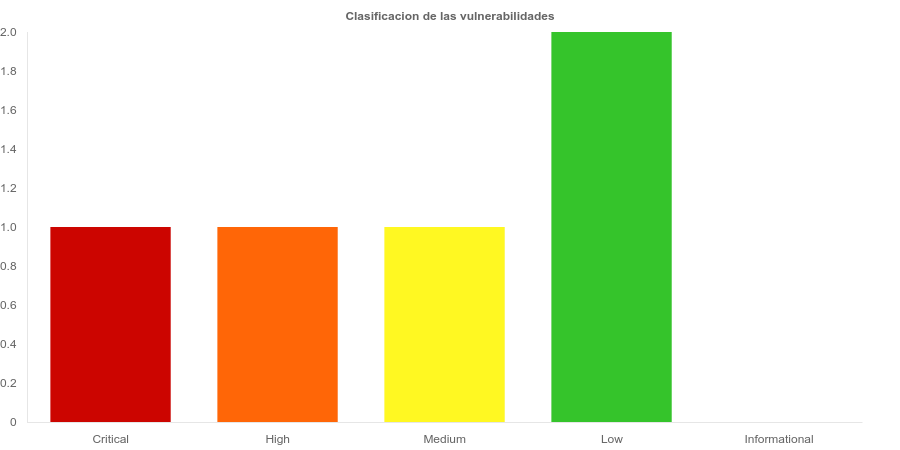
# Clasificación

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr** | **Nombre** | **Severidad** | **Status** |
| 1 | Inyección SQL | **Critical** | Vulnerable |
| 2 | Cross-Site Scripting (XSS) Reflejado | **High** | Vulnerable |
| 3 | Ausencia de fichas (tokens) Anti-CSRF | **Medium** | Vulnerable |
| 4 | Divulgación de direcciones IP Privadas | **Low** | Vulnerable |

5 Cookie sin el atributo “SameSite” Vulnerable



**Low**



# Inyección SQL

## Vulnerable

**Critical**

**CVSS Score -** 10.0

**CVSS Vector -** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Descripción**

Se detecta la presencia de una inyeccion de comandos sql

**Evidencia**

prueba

**Solucion**

Es recomendable filtrar las entradas de usuario mediante listas blancas en lugar de listas negras.

### Referencias

[Inyeccion SQL w3School](https://www.w3schools.com/sql/sql_injection.asp)

[OWASP](https://owasp.org/www-community/attacks/SQL_Injection)

[Portswigger](https://portswigger.net/web-security/sql-injection)

ID OWASP TOP 10 WEB: A03

ID OWASP TOP 10 API: API08

### Instancias vulnerables

**URL Parametro**

http://localhost:5000/api/v1

# Cross-Site Scripting (XSS) Reflejado

## Vulnerable



**High**

**CVSS Score -** 7.7

**CVSS Vector -** CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

### Descripción

Se detecta la presencia de un XSS de tipo reflejado en el cliente

Cross Site Scripting es una tecnica de ataque que comprende hacer eco de codigo dentro de las entradas de datos

### Evidencia Solucion

Al realizar la validacion de entrada, usted debe considerar todas las propiedades potencialmente destacadas, incluida la longitud, el tipo de entrada, el rango completo de valores aceptables

### Referencias

[Cross-Site-Scripting](http://projects.webappsec.org/Cross-Site-Scripting)

[Mitre CWE-79](http://cwe.mitre.org/data/definitions/79.html)

ID OWASP TOP 10 WEB: A03

ID OWASP TOP 10 API: API8

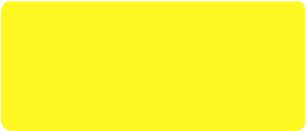
### Instancias vulnerables

**URL Parametro**

http:localhost:5000/api/v1

# Ausencia de fichas (tokens) Anti-CSRF

## Vulnerable

**Medium**

**CVSS Score -** 4.0

**CVSS Vector -** CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**Descripción**

No se encontraron fichas (tokens) Anti-CSRF en un formulario HTML.

**Evidencia**

esta es una prueba

### Solucion

Implementar tokens anti-CSRF en los diferentes formularios HTML

Utilice una biblioteca o marco comprobado que no acepte que ocura esta debilidad o que

### Referencias

http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html

Clasificacion OWASP top 10 A01- CONTROL DE ACCESO ROTO

### Instancias vulnerables

**URL Parametro**

http://localhost:9090/api/v1 http://localhost:9090/api/v1

# Divulgación de direcciones IP Privadas

## Vulnerable



**Low**

**CVSS Score -** 2.4

**CVSS Vector -** CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**Descripción**

Una IP privada se ha encontrado en el cuerpo de la respuesta HTTP

**Evidencia**

esta es una prueba

**Solucion**

Eliminar las direcciones IP privadas del cuerpo de la respuesta HTTP.

### Referencias

<https://tools.ietf.org/html/rfc1918>

CLASIFICACION OWASP TOP 10 A01- CONTROL DE ACCESO ROTO

### Instancias vulnerables

**URL Parametro**

http://localhost:9090/api/v1 http://localhost:9090/api/v1