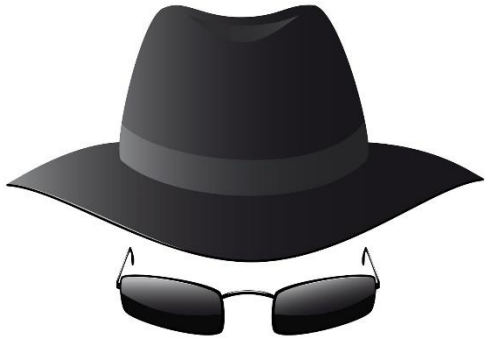
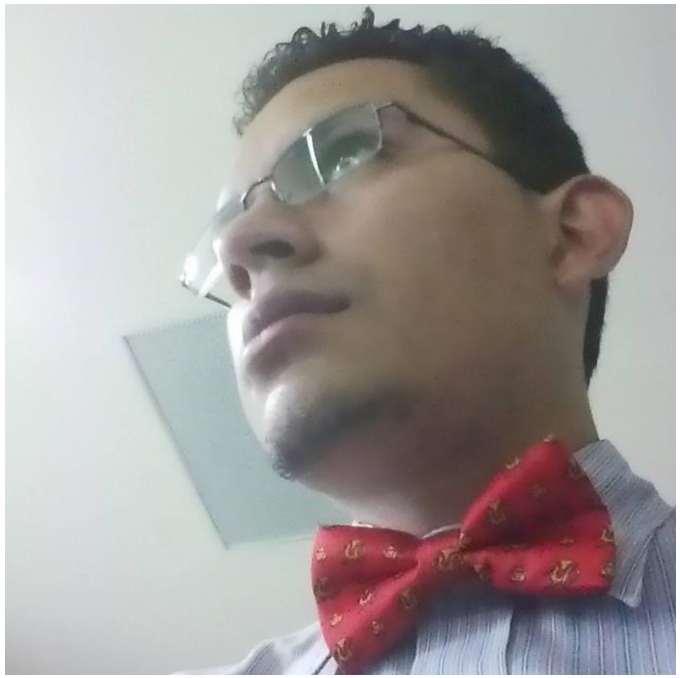


HACKING 101

Técnicas básicas de ataque y Defensa

¿ Quien ?



Jorge Alejandro Cajas Mota

jac.mota@gmail.com

@cajasmota

Contenido

Temas

- ¿Hacker?
  - Definición
  - Tipos
- ¿Por donde empiezo?
  - Herramientas
  - Reconocimiento
  - Vulnerabilidades
  - Pruebas
  - ¡ Lotería !
- Vulnerabilidades comunes
  - XSS
  - SQL Injection
  - Web Services
- Bonus

¿Hacker?

Definición

- Es un Experto en una Ciencia
- Le apasiona el conocimiento
- Se divierte aprendiendo cosas nuevas
- Le gustan los retos difíciles.
- Es revolucionario, comparte su conocimiento

- NO es un pirata informático
- NO es un criminal
- NO es un intruso en sistemas ajenos

¿Hacker?

Tipos

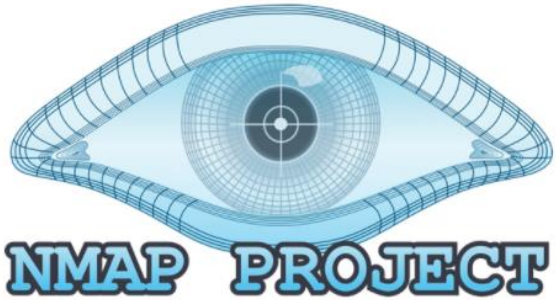
¿Hacker?

Tipos

¿Por donde empiezo?

Herramientas

Webscarab



¿Por donde empiezo?

Herramientas

Google

¿Por donde empiezo?

Reconocimiento

- ¿Quién es la Víctima?
- ¿Qué protocolos de comunicación utiliza?
- ¿Están usando algún framework?
- ¿Tienen alguna vulnerabilidad común?
- ¿Qué espero obtener?

ANONIMATO

¿Por donde empiezo?

Vulnerabilidades

- OWASP Vulnerabilities List
- Exploit DB
- Mala Configuración
- Malas practicas de programación
- Ingeniería Social
- Exposición de datos sensibles

¿Por donde empiezo?

Pruebas

- No dejemos un rastro, puede ser problemático.
- No violemos la ley, también es problemático.
- Usemos las herramientas adecuadas
- Muchas pruebas se pueden hacer 1 sola vez

ANONIMATO

¿Por donde empiezo?

¡ Lotería !

Vulnerabilidades Comunes

XSS

Cross Site Scripting:

Es un vector de ataque que intenta inyectar código malicioso en nuestros sitios web.

Normalmente se produce por malas prácticas de programación o desconocimiento del vector de ataque.

Vulnerabilidades Comunes

XSS

Vulnerabilidades Comunes

XSS

- Nunca confiemos en la Data que escribe el usuario.
- Escapemos los caracteres, ejemplo “<“ → “<”
- Nunca renderizemos la data del usuario directamente

```
echo “Results for" . $_GET[‘search'];

echo “Results for" . Htmlspecialchars($_GET[‘search']);
```

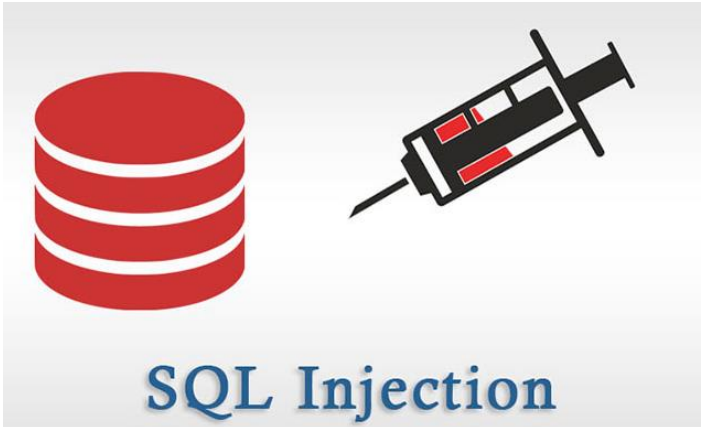
Vulnerabilidades Comunes

SQL Injection

SQL Injection:

Es un vector de ataque que intenta inyectar código SQL en nuestras consultas del servidor hacia la Base de Datos para obtener más información de la que se le permite o destruir nuestros datos

Normalmente se produce por malas prácticas de programación o desconocimiento del vector de ataque.



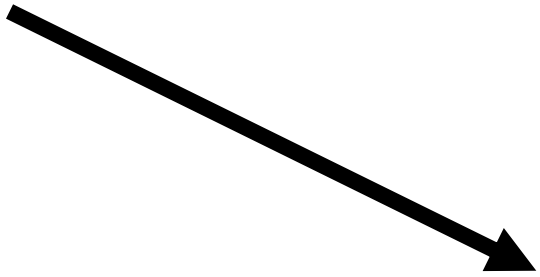
Vulnerabilidades Comunes

SQL Injection

Enter your last name: Smith Go!

```
SELECT * FROM user_data WHERE last_name = ?
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
102	John	Smith	2435600002222	MC		0
102	John	Smith	4352209902222	AMEX		0



Enter your last name: Smith' OR 1=1 -- Go!

```
SELECT * FROM user_data WHERE last_name = 'Smith' OR 1=1 --'
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COU
101	Joe	Snow	987654321	VISA		0
101	Joe	Snow	2234200065411	MC		0
102	John	Smith	2435600002222	MC		0
102	John	Smith	4352209902222	AMEX		0

Vulnerabilidades Comunes

SQL Injection

- Nunca confiemos en la Data que escribe el usuario.
- Sanitizemos nuestros campos
- Usemos parámetros de SQL en lugar de concatenar la data en un solo String.

```
// prepare and bind
$stmt = $conn->prepare("INSERT INTO MyGuests (firstname, lastname, email) VALUES (?, ?, ?)");
$stmt->bind_param("sss", $firstname, $lastname, $email);
```

Vulnerabilidades Comunes

Web Services

Autenticación

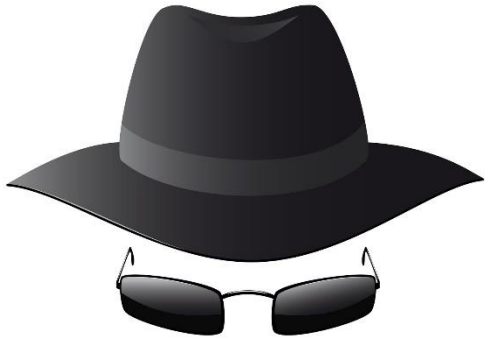
Estamos en la era de los Servicios WEB, ya sean SOAP o REST

Si no somos cuidadosos con nuestros servicios podemos exponer más datos de los deseados, por lo que debemos de manejar protocolos de autenticación y autorización.

No debemos publicar o exponer a internet más de la cuenta

Bonus

WebGoat



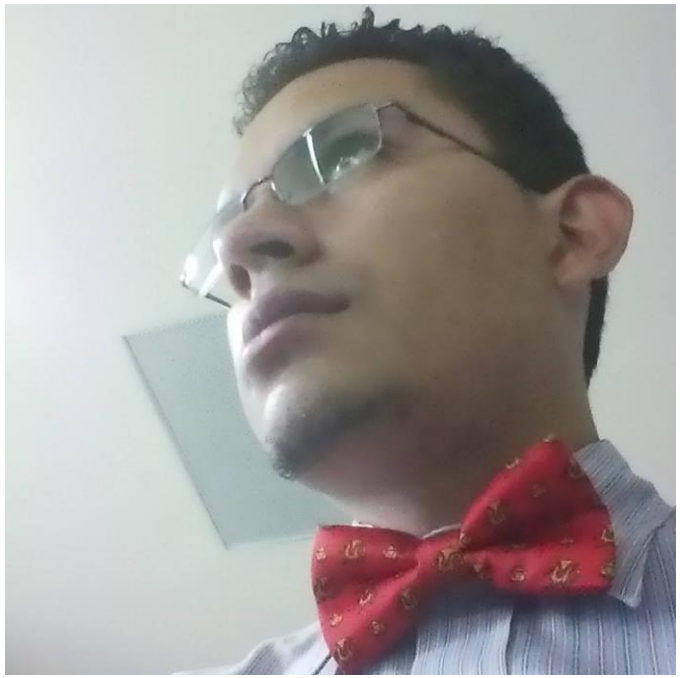
HACKING 101

¿Preguntas?

Devs+ 502

INVERSIONES INTELECTUALES

¡ Muchas Gracias !



Jorge Alejandro Cajas Mota

jac.mota@gmail.com

@cajasmota