Desarrollo seguro de Aplicaciones Web basado en OWASP

Por: Carlos Carreño,

OCP, ScrumMaster, Solution Architect

Email: ccarrenovi@Gmail.com

Unidad 5 Seguridad en la codificación de software

- Vulnerabilidades más comunes. ¿Cómo prevenirlas?
- SQL Injection & Command Injection
- XSS, CSRF
- Vulnerabilidades del ranking OWASP Top 10
- Otras vulnerabilidades
- Errores de Canonización
- Information disclosure
- Phishing Vector
- Recursos de OWASP para seguridad en la codificación

Autor: ccarrenovi@Gmail.com

Vulnerabilidades más comunes. ¿Cómo prevenirlas?

- Vulnerabilidades mas comunes en las aplicaciones web

A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	∪	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	∪	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

Autor: ccarrenovi@Gmail.com

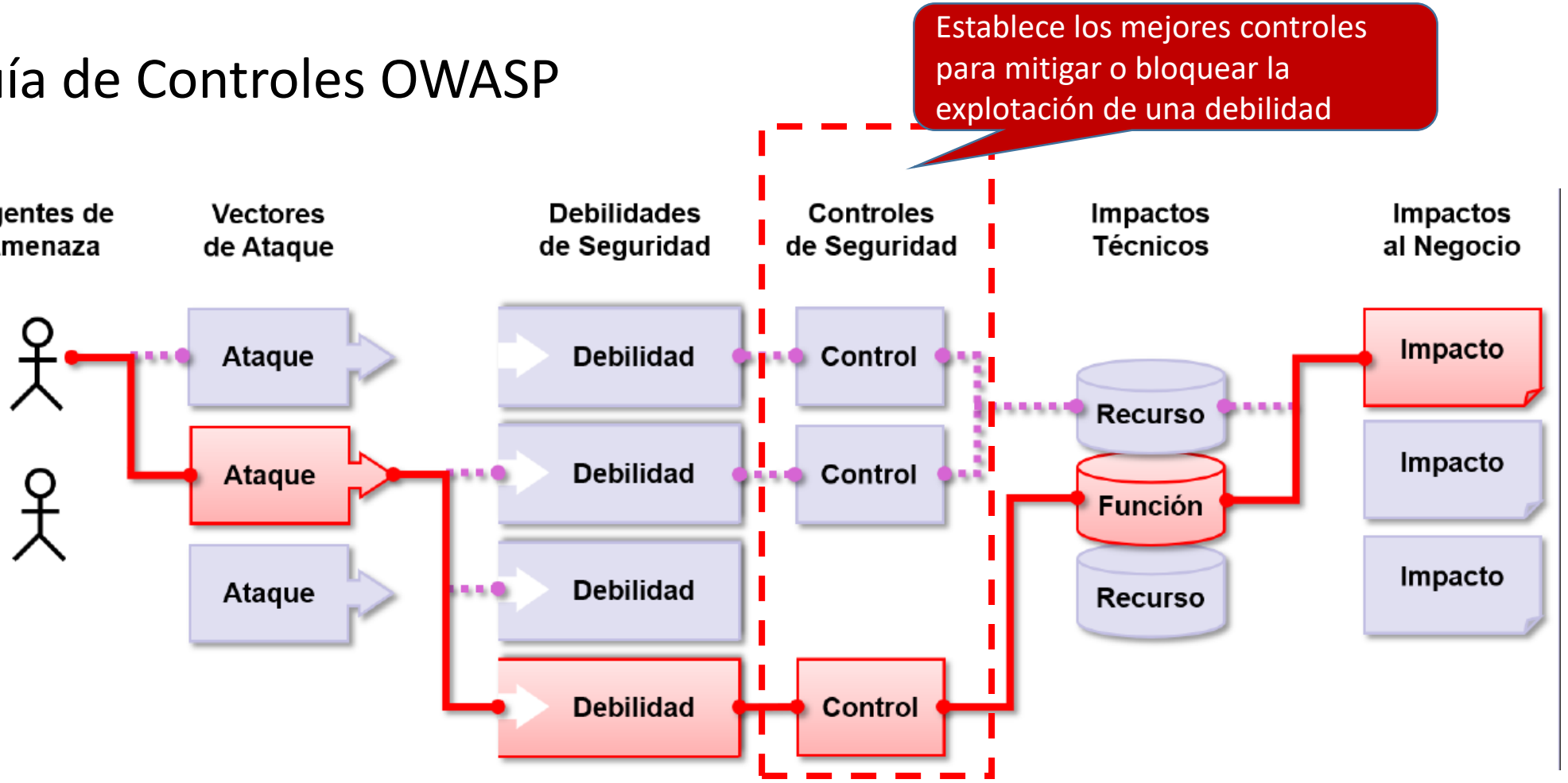
Vulnerabilidades: ¿Cómo prevenirlas?

- Estable una metodología de evaluación del riesgo.
- Modelado de Amenazas y riesgos

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

Vulnerabilidades: ¿Cómo prevenirlas?

- Guía de Controles OWASP



Autor: ccarrenovi@Gmail.com

Injection

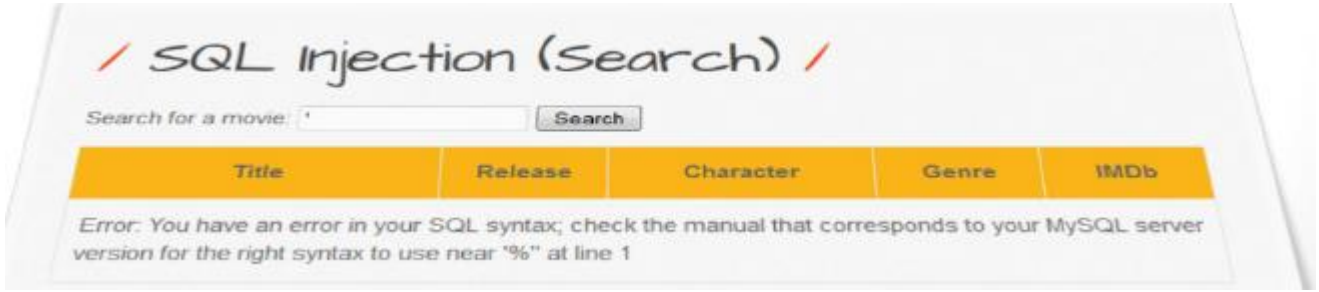
- Los defectos de inyección ocurren cuando una aplicación envía datos no confiables a un intérprete
- A menudo se encuentran en SQL, comandos del sistema operativo, XPath, Analizadores XML, encabezados SMTP, argumentos de programa, etc.
- Fácil de descubrir al examinar el código, pero más bien difícil de descubrir a través del pentesting!
- Los escáneres y difusores ayudan a encontrar fallas de inyección

Injection

- Los ataques de inyección pueden resultar en:
  - Perdida de datos o corrupción
  - Desfiguración del sitio web
  - Denegación de acceso
  - Perdida del control del host

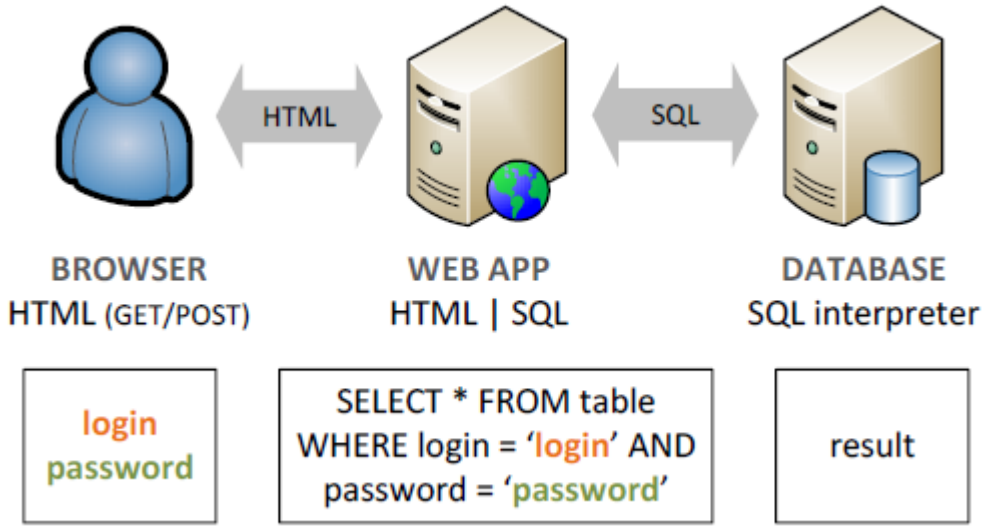
SQL Injection

- La inyección SQL es muy común en aplicaciones web.
- Ocurre cuando la entrada del usuario se envía a un intérprete de SQL como parte de una consulta
- El atacante engaña al intérprete para que ejecute consultas SQL no deseadas



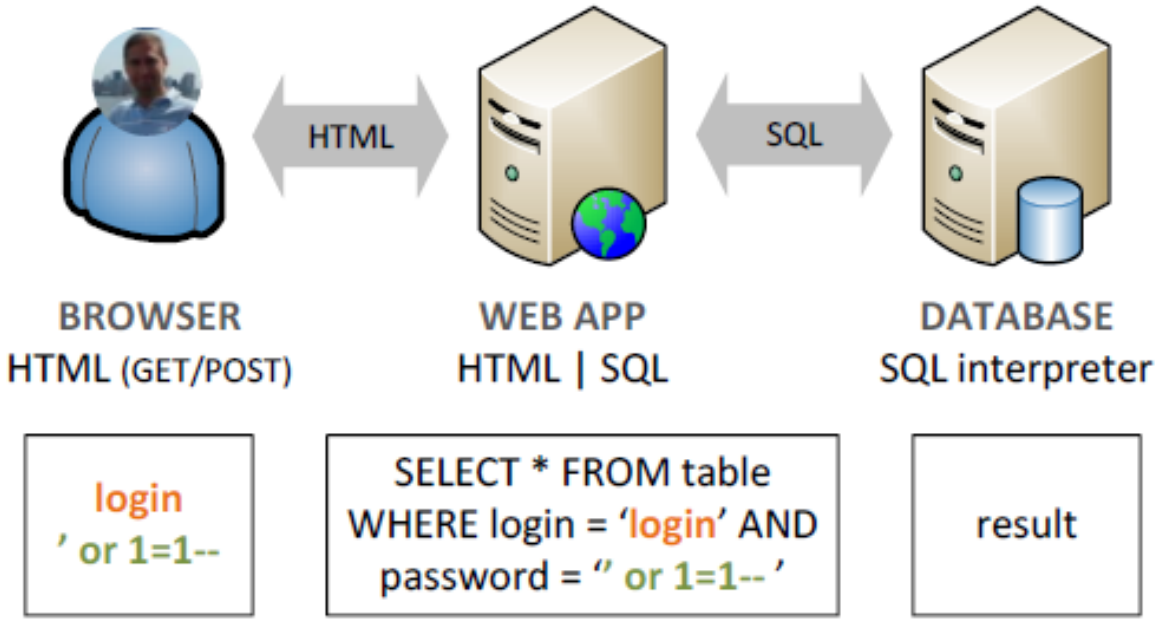
SQL Injection

- Operación normal



SQL Injection

- Operación anormal



Autor: ccarrenovi@Gmail.com

SQL Injection

- Ejemplo:

PHP code

- SELECT * FROM table WHERE username='. $login .' AND password='. $password .'

Expected input

- SELECT * FROM table WHERE username='alice' AND password='loveZombies'

But what if the person injected

- SELECT * FROM table WHERE username='alice' AND password='' or 1=1 --

SQL Injection

- Inyecciones Simples
  - '--
  - ' or 'a'='a
  - ' or 'a'='a'--
  - ' or '1'='1
  - ' or 1=1--

SQL Injection

- Ejemplos:

  Union injections

  - ' UNION SELECT field1, field2 FROM table--
  - ' UNION SELECT table_name FROM
    INFORMATION_SCHEMA.TABLES
    WHERE table_schema=database()--

  Stacked queries

  - '; DROP TABLE table;--

Blind SQL Injection

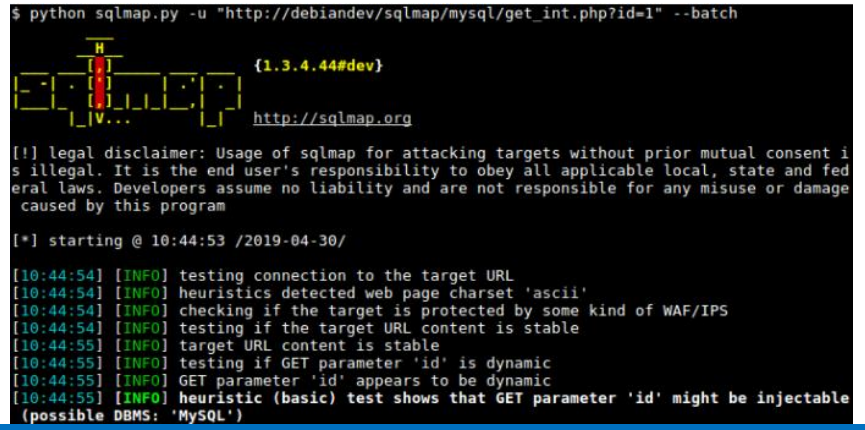
- La inyección SQL ciega es un tipo de ataque de inyección SQL que hace preguntas verdaderas o falsas a la base de datos
- Se utiliza a menudo cuando la aplicación web está configurada para mostrar mensajes genéricos
  - No se muestra el código vulnerable a la inyección de SQL
  - La base de datos no envía datos a la página web
- Casi idéntica a la inyección SQL normal, la forma en que los datos se recupera de la base de datos es diferente ...

Blind SQL Injection

- El resultado de la inyección SQL se determina en función de las respuestas de la aplicación
  - Basado en booleano o basado en tiempo
- Explotar la vulnerabilidad es más difícil y más lento que la inyección SQL tradicional ... ¡pero no imposible!
- El uso de herramientas automatizadas es imprescindible

Inyección SQL automatizada

- sqlmap
  - Herramienta de prueba de penetración de código abierto
  - Automatiza el proceso de detección y explotación de la inyección SQL
  - Desarrollado en Python, desde julio de 2006
  - Soporte completo para MS SQL, MySQL, Oracle, PostgreSQL,…
  - Soporte completo para varias técnicas de inyección SQL
  - Sitio: http://sqlmap.org/



HTML Injection

- La inyección de HTML se produce cuando un usuario inserta código HTML a través de un campo de entrada o parámetro específico
- Validación insuficiente de los datos proporcionados por el usuario
- ¡Peligroso cuando se almacena permanentemente!
- Las inyecciones de HTML pueden provocar
  - Deformaciones del sitio web
  - Ataques de phishing
  - Explotación del lado del cliente

Command Injection or SSI Injection

- Lado del servidor incluye inyección o inyección SSI
- Un ataque SSI permite la explotación inyectando scripts en Páginas HTML y ejecución del código arbitrario.
- Muy similar a HTML / inyección de comandos y XSS
- Las inyecciones de SSI pueden provocar
  - Deformaciones del sitio web
  - Completar el control del host
  - Ataques de phishing

SSI Injection

SSI Injections

- <!--#exec cmd="ls -l" -->
- <!--#exec cmd="cat /etc/passwd" -->
- <!--#exec cmd="echo 'Bugged!' > /var/www/index.htm" -->
- <!--#include file="AAAA[...]AA" -->

Autor: ccarrenovi@Gmail.com

SSI Injection

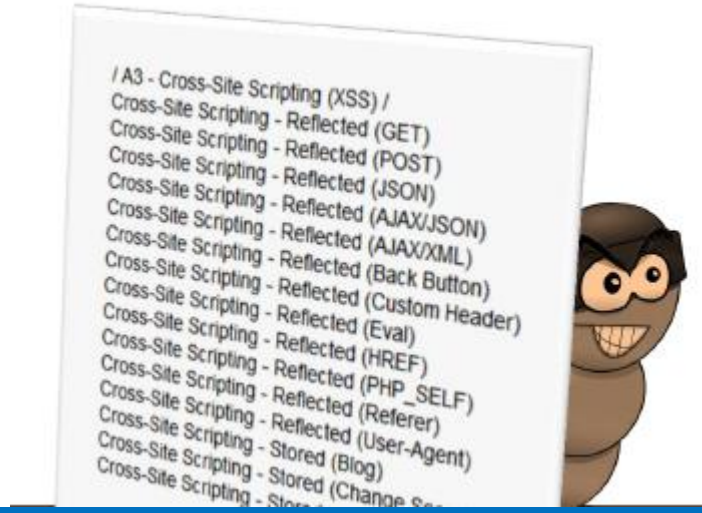
- Vulnerabilidad de escalamiento de privilegios SSI
  - Una vulnerabilidad anterior en IIS 4.0 y 5.0 permite a un atacante obtener privilegios del sistema! (CVE-2001-0506 / MS01-044)
  - Desbordamiento de búfer en una biblioteca de vínculos dinámicos (ssinc.dll)
  - Explotado creando una página maliciosa que contiene el código SSI a continuación y obligando a la aplicación a cargar la página
    - <! - # include file = "AAAA [...] AA" ->
    - El número de A debe ser superior a 2049

XSS, CSRF

- Cross-Site Scripting, o XSS, ocurre cuando un atacante inyecta un script del navegador en una aplicación web
  - El script no se ejecuta en el sitio web, sino en el navegador de la víctima.
  - El sitio web envía el script al navegador de la víctima.
- Validación insuficiente de los datos proporcionados por el usuario (~ inyección HTML)
- Normalmente JavaScript, pero también puede incluir HTML, Flash, o cualquier otro tipo de código que pueda ejecutar el navegador

Cross-Site Scripting

- Tipos de fallas de XSS
  - Reflexibilidad de XSS
  - Almacenamiento de XSS



Autor: ccarrenovi@Gmail.com

Vulnerabilidades del ranking OWASP Top 10

- A1 - Inyección
- A2 - Falla de autenticación
- A3 – Exposición de datos sensibles
- A4 – XML External Entities
- A5 – Ausencia de control de acceso
- A6 – Configuraciones por defecto
- A7 – Cross-site scripting
- A8 – Deserialización insegura
- A9 - Utilización de componentes con vuln. conocidas
- A10 – Falta de registros y monitoreo

Autor: ccarrenovi@Gmail.com

Vulnerabilidades del ranking OWASP Top 10

A1:2017 Inyección	Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.
A2:2017 Pérdida de Autenticación	Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).
A3:201 Exposición de datos sensibles	Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.

Vulnerabilidades del ranking OWASP Top 10

A4:2017 **Entidades Externas XML (XXE)**	Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).
A5:2017 **Pérdida de Control de Acceso**	Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.
A6:2017 **Configuración de Seguridad Incorrecta**	La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, *ad hoc* o por omisión (o directamente por la falta de configuración). Son ejemplos: *S3 buckets* abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, *frameworks,* dependencias y componentes desactualizados, etc.

Vulnerabilidades del ranking OWASP Top 10

A7:2017 **Secuencia de Comandos en Sitios Cruzados (XSS)**	Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta *JavaScript* en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar (*defacement*) los sitios web, o redireccionar al usuario hacia un sitio malicioso.
A8:2017 **Deserialización Insegura**	Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.
A9:2017 **Componentes con vulnerabilidades conocidas**	Los componentes como bibliotecas, *frameworks* y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.

Vulnerabilidades del ranking OWASP Top 10

A10:2017 **Registro y Monitoreo Insuficientes**	El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos

Otras vulnerabilidades

- Errores de Canonización
- Information disclosure
- Phishing Vector

Errores de Canonización

- Los valores de entrada deben ser **decodificados y canonizados** a la representación interna de la aplicación antes de ser validados.
- Asegurarse que la aplicación no decodifique la misma entrada dos veces.
- Tales errores pueden ser usados para evadir los esquemas de listas blancas "**whitelists**" introduciendo entradas peligrosas luego de haber sido controladas.
- Una **lista blanca** (en inglés, *whitelist*) es una lista o registro de entidades que, por una razón u otra, pueden obtener algún privilegio particular, servicio, movilidad, acceso o reconocimiento. Por el contrario la lista negra es la compilación que identifica a quienes serán denegados, no reconocidos u obstaculizados.

Information disclosure

- La divulgación de información, también conocida como fuga de información, es cuando un sitio web revela involuntariamente información confidencial a sus usuarios. Dependiendo del contexto, los sitios web pueden filtrar todo tipo de información a un atacante potencial, incluidos:
  - Datos sobre otros usuarios, como nombres de usuario o información financiera
  - Datos comerciales o empresariales sensibles
  - Detalles técnicos sobre el sitio web y su infraestructura

Autor: ccarrenovi@Gmail.com

Phishing Vector

- El phishing es el vector de ataque más popular y potente y se clasifica como un ataque de ingeniería social que a menudo se usa para robar datos de usuarios, incluidas las credenciales de inicio de sesión y los números de tarjetas de crédito.
- El objetivo del phishing a través de la ingeniería social es engañar a la víctima haciéndole creer que el mensaje que recibe del perpetrador del phishing contiene algo que quiere o necesita (una solicitud de su banco, por ejemplo, o una nota de alguien dentro de su empresa) y haga clic en un enlace o descargue un archivo adjunto.
- Phishing por correo electrónico
- Phishing de almacenamiento en la nube
- Phishing Móvil

Recursos de OWASP para seguridad en la codificación

OWASP Code Review Guide

Main

Thank you for visiting OWASP.org. We recently migrated our community to a new web platform and regretably the content for this page needed to be programmatically ported from its previous wiki page. There's still some work to be done. The historical content can be found here.

Please visit our Page Migration Guide for more information about updating pages for the new website as well as examples of github markdown.

The current PDF version can be found here

Laboratorio

- Lab 3 Resolver los ejercicios de SQL Injection