Web security:

SQL Injection

GRUPO 2 [Marcos Rojas Pacheco - Daniel Ruiz Raposo - Álvaro Ramos Albertos - Francisco Javier García Cordero]

¿Qué es una inyección SQL?

Una inyección SQL se realiza cuando los inputs no están controlados o validados, pudiendo ejecutar código SQL a la base de datos directamente a través de una página web que la use dando acceso a datos confidenciales de la empresa.

¿Cuáles son los daños que puede causar?

Si no reparamos el problema con las `inyecciones SQL`, dejaremos expuesta información de la compañía la cual va a poder ser extraída, modificada e inclusive tener ingreso completo al sistema, llegando a perjudicar toda la red empresarial si esto no se previene.

¿Como evitar o prevenir la inyección sql?

- Escaneos regulares utilizando `Acunetix` u otro software de escaneado de vulnerabilidades.
- Entrenar y concienciar a los implicados en la creación d la web
- Utilizar listas blancas en vez de negras para la entrada de usuarios en la base de datos
- En cuanto a la programacion en sí:
  - Escapar los caracteres especiales utilizados en consultas sql
  - Delimitar los valores de las consultas
  - Verificar los datos introducidos por los usuarios.
  - Mostrar solo mensajes de error genéricos.
- Asignar correctamente los privilegios a los usuarios que se conecten a la base de datos.

Ejemplo de una vulnerabilidad similar[CVE-2021-24762]

Descripción ☐

El plugin para wordpress `The Perfect Survey` para versiones anteriores a la 1.5.2 no valida el parámetro `GET question_id` antes de usarlo en la declaración SQL, específicamente en la acción AJAX `get_question`, lo que permite a los usuarios no autenticados realizar una inyección SQL.

CVSS SCORE	IMPACTO SOBRE LA CONFIDENCIALIDAD	IMPACTO SOBRE LA INTEGRIAD	IMPACTO SOBRE LA VIABILIDAD	COMPLEJIDAD EN EL ACCESO	AUTENTICACIÓN	OBTENCIÓN DE ACCESO	TIPO DE VULNERABILIDAD
7.5	*PARCIAL*	*PARCIAL*	*PARCIAL*	*BAJA*	*NO REQUERIDA*	*NO*	*SQL INJECTION*

Tipo de vulnerabilidad

Inyección SQL

Se hace una vez que los inputs no permanecen controlados o validados, logrando llevar a cabo código SQL a la base de datos de manera directa por medio de una página web que la utilice dando ingreso a datos confidenciales de la compañía.

Tipo de Exploit

El exploit se llama:

- WordPress Plugin Perfect Survey - 1.5.1 - SQLi (Unauthenticated)

Efectos del Exploit

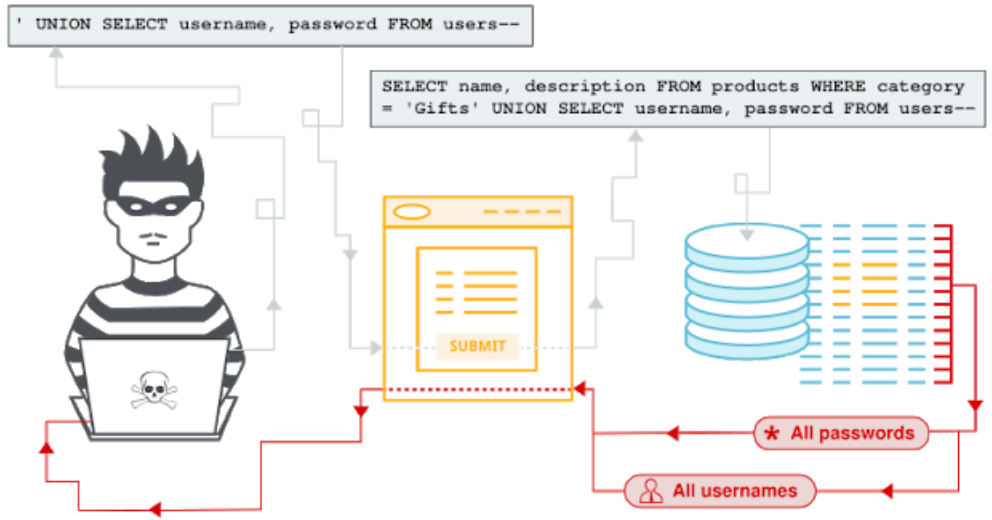
El mal que causa este exploit justamente es la entrada completo tanto a las tablas, columnas y base de datos de SQL, logrando además crear copias de la información almacenada en la máquina local del agresor, ocasionando una fuga de información confidencial tanto de los usuarios como de los administradores del servidor.

Solución o parche que se publicó

La solución que optaron por tomar los creadores del plugin `Perfect Survey` fue quitarlo de wordpress para que los usuarios no descargaran una versión vulnerable y dejar de darle mantenimiento en vez de validar el parámetro `GET question_id` antes de usarlo en la acción AJAX `get_question` para que no fuese vulnerable ante inyecciones SQL .

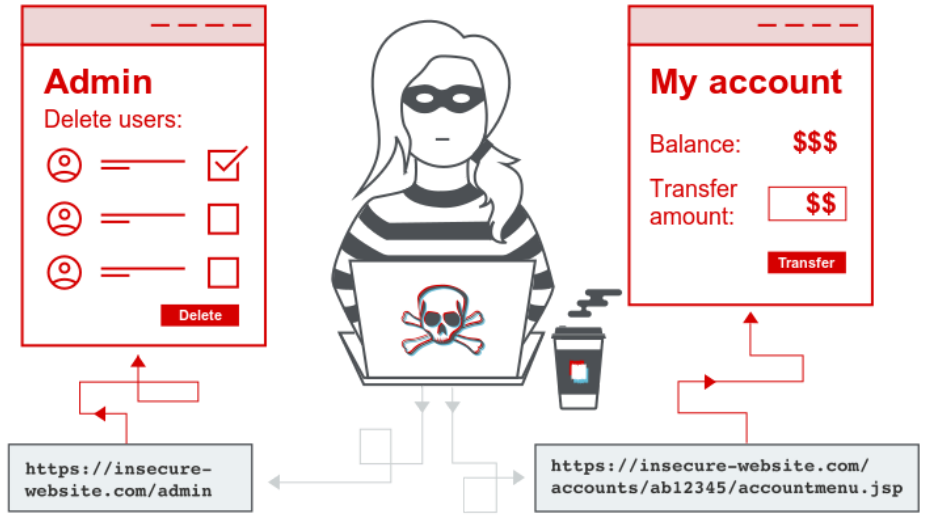
Los 10 ciberataques más comunes en empresas

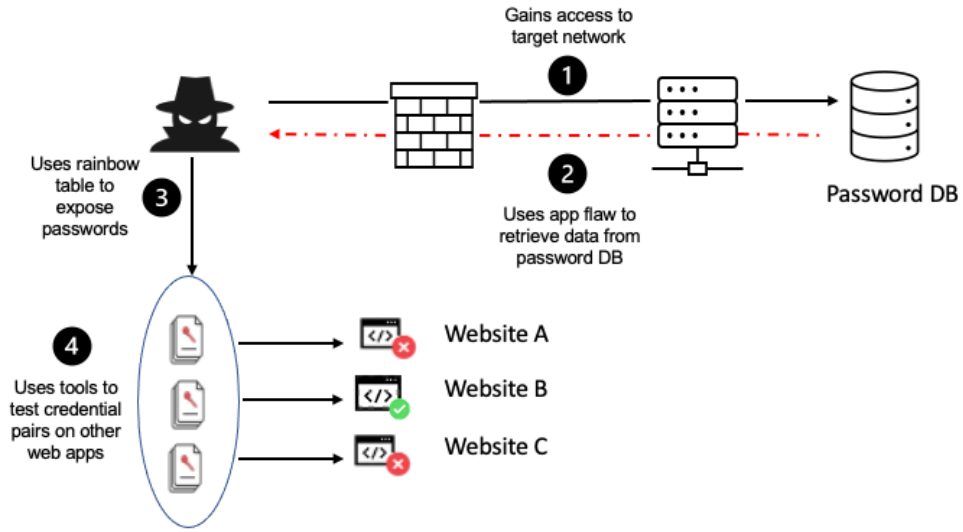
1. Broken Access Control
2. Cryptographics Failures
3. SQL Injections
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server Side Request Forgery



Broken Access Control

La política del control de acceso no permite a los usuarios actuar fuera de sus permisos previstos. Las fallas generalmente conducen a la divulgación, modificación o destrucción no autorizada de todos los datos o a la realización de una función comercial fuera de los límites del usuario.



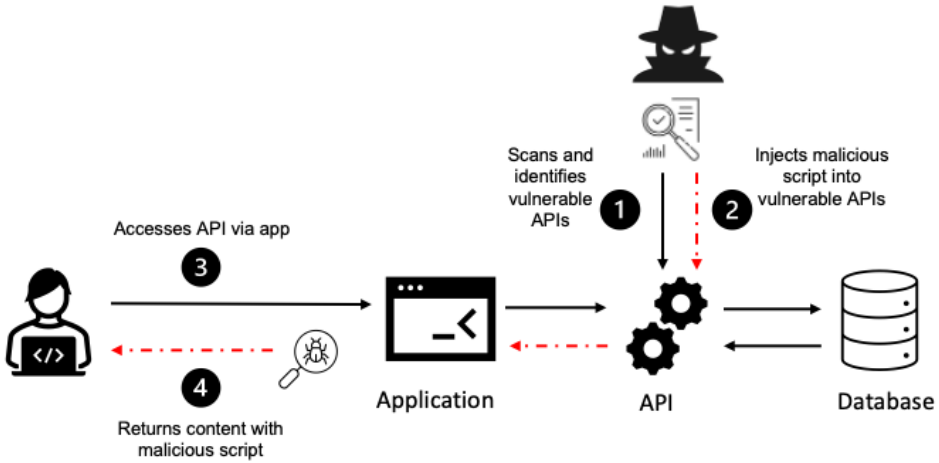


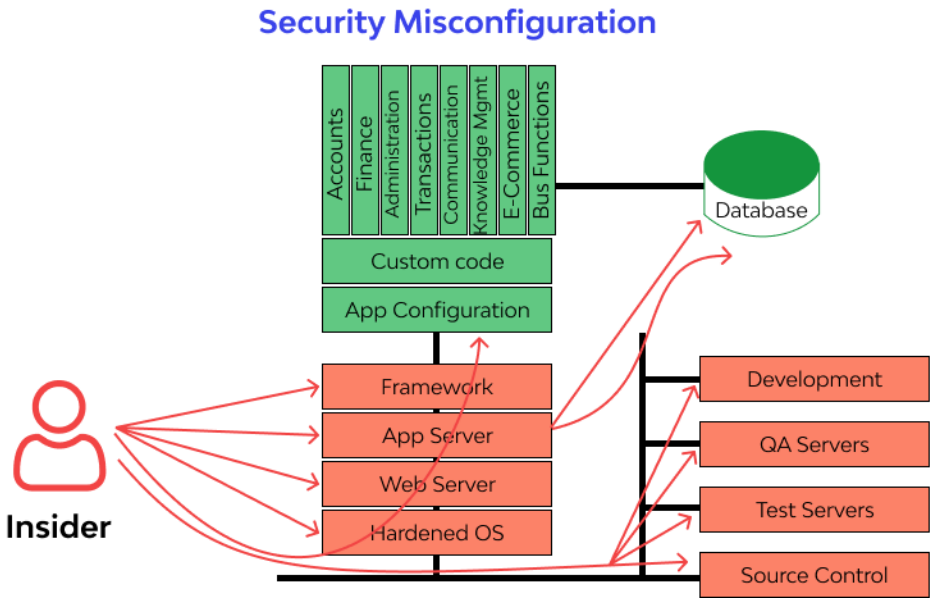
Cryptographic Failures

Vulnerabilidad crítica de seguridad de la aplicación web que expone datos confidenciales de la aplicación en un algoritmo criptográfico débil o inexistente. Pueden ser contraseñas, registros de salud de pacientes, secretos comerciales, información de tarjetas de crédito, direcciones de correo electrónico u otra información personal del usuario.

Insecure Design

El diseño inseguro surge cuando los desarrolladores no anticipan la seguridad ni evalúan las amenazas durante el diseño del código, también ocurren por el incumplimiento de las prácticas de seguridad al crear las aplicaciones, algunos ejemplos de esto son el almacenamiento desprotegido de credenciales, generación de mensajes de error que contienen información confidencial, compartimentación inadecuada, etc...



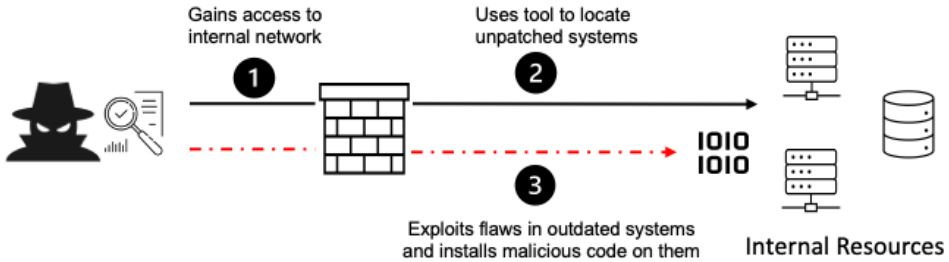


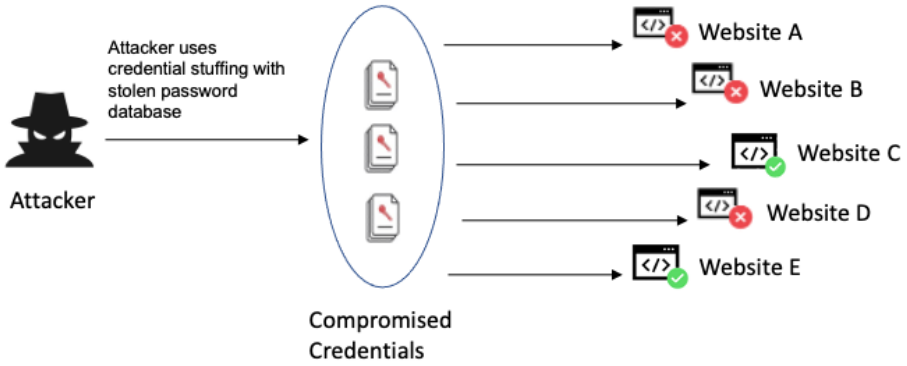
Security Misconfiguration

Este ataque se presenta cuando se ha realizado mal la configuración en las aplicaciones, en los servidores, en las bases de datos o en el sistema operativo. Generalmente se producen cuando existen páginas sin uso, fallas sin el parche correspondiente, archivos y directorios sin protección.

Vulnerable and Outdated Components

Un componente de software es parte de un sistema o aplicación que amplía la funcionalidad de la aplicación, como un módulo, un paquete de software o una API. Las vulnerabilidades basadas en componentes ocurren cuando un componente de software no es compatible, está desactualizado o es vulnerable a un exploit conocido.



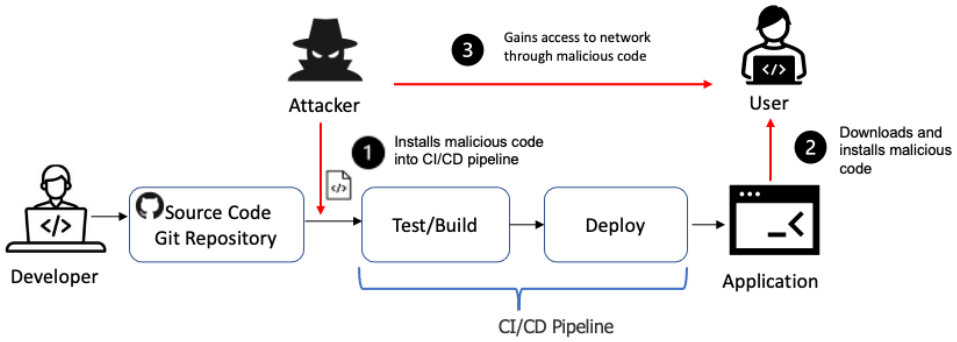


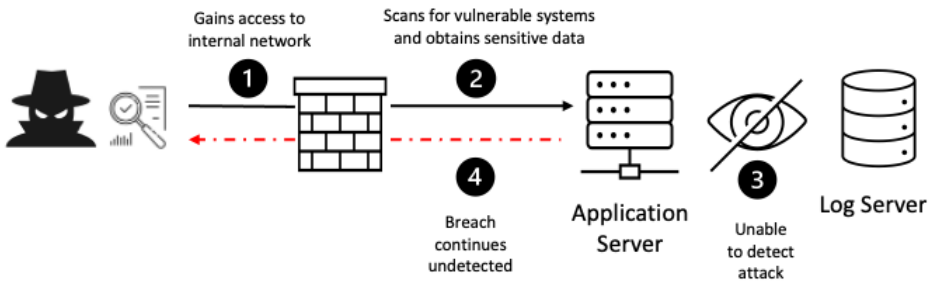
Identification and Authentication Failures

Estas fallas ocurren cuando las funciones relacionadas con la identidad, la autenticación o la administración de sesiones de un usuario no se implementan correctamente o no están adecuadamente protegidas por una aplicación. Los atacantes pueden explotar las fallas de identificación y autenticación al comprometer contraseñas o tokens de sesión. Para realizar estos ataques los cibercriminales utilizan ataques de fuerza bruta, secuestro de sesión, falsificación de solicitudes entre sitios, etc...

Software and Data Integrity Failures

En ausencia de una validación adecuada cuando se agregan actualizaciones de software y datos críticos a la canalización de entrega, las fallas en la integridad del software y los datos hacen que las aplicaciones sean susceptibles a la divulgación de información no autorizada, el compromiso de sistema o la inserción de código malicioso. Esto da como resultado que las cargas corruptas se implementen y se ejecuten directamente en las instalaciones de las aplicaciones.



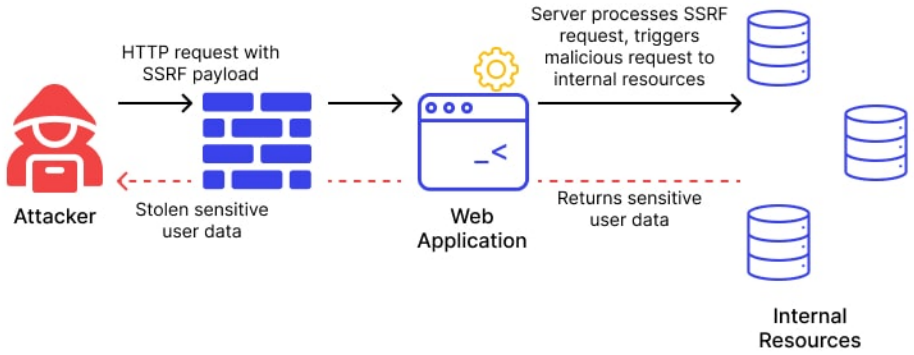


Security Logging and Monitoring Failures

Si no se registran, supervisan o informan suficientemente los eventos de seguridad, como los intentos de inicio de sesión, el comportamiento sospechoso es difícil de detectar y aumenta significativamente la probabilidad de que un atacante pueda aprovechar su aplicación.

Server-Side Request Forgery

Es la falsificación de solicitudes del lado del servidor que es un tipo de explotación en la que un atacante abusa de la funcionalidad de un servidor y hace que acceda o manipule información en el ámbito de ese servidor que, de otro modo, no sería directamente accesible para el atacante.



Fases de un ataque informático

- Reconocimiento y comprobación
- Enumeración
- Explotación
- Escalada de privilegios / persistencia
- Informe

Reconocimiento / Comprobación

Una vez que el ciberdelincuente observa los detalles que el usuario publica y busca información sobre la tecnología que utiliza, analiza los métodos de ataque. Por ello, para evitar que el ciberdelincuente disponga de la información que requiere para empezar el robo, es fundamental que los usuarios cuenten con estrategias de cuidado y resguardo de la información que hacen pública, así como las empresas y organizaciones limitando la información que se comparte en la web y en las redes sociales, o imponiendo información inaccesible.
Herramientas de reconocimiento / comprobación:

- **Shodan**: Es un motor de búsqueda que permite buscar por filtros equipos que estén conectados a Internet.
- **Google**: Es un motor de búsqueda de lo más utilizado globalmente para buscar información en Internet.

Enumeración

La enumeración es el proceso de extraer nombres de usuario, máquinas, recursos de red, recursos compartidos y servicios de un sistema o red. La información recopilada permite al atacante identificar puntos débiles de un sistema.

Herramientas de enumeración:

- **Nmap**: Es un programa que sirve para rastrear puertos, descubrir servidores, determinar servicios que se están ejecutando, etc...
- **Gobuster**: Es una herramienta utilizada para realizar ataques de diccionario a URL, subdominios DNS y nombres de hosts en servidores web.

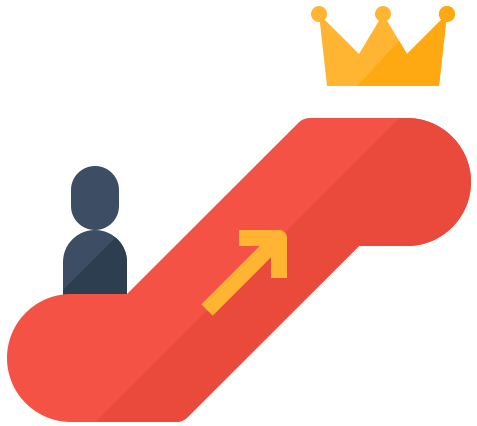
Explotación

Esta fase implica la detonación del ataque, comprometiendo al equipo objetivo y a la red a la que pertenezca. Por este motivo, es muy importante disponer de soluciones de seguridad y mantener todos los sistemas, incluido el antivirus, actualizado a su última versión.

Herramientas explotación:

- **Metasploit Framework**: conjunto de herramientas de explotación de vulnerabilidades que reúne miles de programas capaces de aprovechar fallos informáticos.
- **Meterpreter**: herramienta que se usa a través de Metasploit para ejecutar todo tipo de tareas en el ordenador de una víctima.

Escalada privilegios / persistencia



Un ataque de escalada de privilegios es aquel que busca o consigue acceso a un usuario con permisos de administrador `root` en el sistema de una organización. Esto se logra a partir de la explotación de vulnerabilidades, que el atacante debe primero encontrar a través de una recopilación de información sobre su objetivo.
Una amenaza persistente es un ciberataque prolongado y dirigido en el que un intruso obtiene acceso a una red y permanece sin ser detectado por un largo periodo de tiempo.
Herramientas de escalada de privilegios / persistencia:

- **GTFOBins**: Es una página web donde enlistan archivos de Unix que se utilizan para eludir las restricciones de seguridad locales en sistemas mal configurados.

Informe

Los puntos de vista vulnerables y las exposiciones usuales (CVE) componen una lista de fallas de estabilidad informática que está disponible al público. Un CVE tiene relación con una vulnerabilidad a la cual se le asignó un número de identificación.
El estudio perimetral es un informe que creamos una vez se ha explotado la vulnerabilidad para ver el alcance que ha tenido aquel ataque, y ver las secuelas que ha tenido la compañía.

Herramientas de informe:

- **Notion**: Es un programa de gestión de proyectos y para tomar notas.
- **Cherrytree**: Es un gestor de notas gratuito que tiene un esquema jerárquico en la estructuración de la información

Referencias

WEBGRAFICA

- https://www.getperfectsurvey.com/
- https://wpscan.com/vulnerability/c1620905-7c31-4e62-80f5-1d9635be11ad
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24762
- https://www.exploit-db.com/exploits/50766
- https://github.com/Hacker5preme/Exploits/blob/main/Wordpress/CVE-2021-24762/README.md
- https://www.getperfectsurvey.com/
- https://web.archive.org/web/20210817031040/https://downloads.wordpress.org/plugin/perfect-survey.1.5.1.zip
- https://nvd.nist.gov/vuln/detail/CVE-2021-24762

Referencias

WEBGRAFICA

- https://creantelab.co/fases-de-un-ciberataque-y-como-evitarlo/
- https://keepcoding.io/blog/herramientas-de-postexplotacion/
- https://keepcoding.io/blog/que-es-la-escalada-de-privilegios/
- https://www.computerweekly.com/es/definicion/Amenaza-persistente-avanzada-o-APT
- https://gtfobins.github.io/
- https://www.redhat.com/es/topics/security/what-is-cve
- https://owasp.org/www-project-top-ten/