# Auditoría de Seguridad

## Autor: Maximiliano Dariel Altamirano

### 1. Ámbito y alcance de la auditoría

El objetivo de la autoría fue lograr un acercamiento, en un entorno controlado y guiado, a las funciones de un pentesting. Abordamos la plataforma Webgoat como sitio para trabajar.

Exploramos la plataforma, identificamos luego de una explicación breve las vulnerabilidades y ensayamos un ataque controlado con una pequeña reseña de lo que sucedió.

### 2. Informe ejecutivo

a. Procesos realizados.

Partiendo de la metodología OWASP, exploramos e identificamos las vulnerabilidades más frecuentes y de mayor impacto (criticidad), articulamos un ataque guiado y revisamos las consecuencias.

b. Vulnerabilidades destacadas

* [A3 Injection - SQL Injection](?tab=t.bq3gcyj59pxm)

Se identifica una vulnerabilidad de confidencialidad en el campo “Authentication TAN”

Impacto: "Inyección" de código malicioso a través de la entrada de consulta SQL del cliente.

Recomendaciones: Se sugiere implementar el uso de sentencias preparadas (con consultas parametrizadas), comparto el siguiente [enlace](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html) con más procedimientos a revisar.

* [A3 Injection - Cross Site Scripting](?tab=t.nv6nxvwso5z3)

Se encontró una vulnerabilidad XSS en el campo “Enter your credit card number:” de la plataforma.

Impacto: Se ejecuta script malicioso en el campo mencionado identificando la posibilidad de acceso no autorizado a información sensible.

Recomendaciones: Todas las variables de una aplicación web deben estar protegidas para garantizar que todas las variables pasen por la validación, comparto el siguiente [enlace](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html#xss-defense-philosophy) con más procedimientos a revisar.

* [A5 Security Misconfiguration](?tab=t.kug6j65jjb43)

Se identifica una vulnerabilidad en el posteo de una imagen de un usuario desde la entrada de comentarios con XML.

Impacto: “Inyección” de código malicioso desde una entrada XML con una referencia a una entidad externa. Este ataque puede conducir a la divulgación de datos confidenciales, denegación de servicio, falsificación de solicitud del lado del servidor.

Recomendaciones: El procesador XML debe ser configurado para usar una DTD estática local y no permitir ninguna DTD declarada incluido en el documento XML, comparto el siguiente [enlace](https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing) con más procedimientos a revisar.

* [A6 Vuln & outdated Components](?tab=t.u5cfovbpjyvq)

Se identifica una vulnerabilidad Exploiting CVE-2013-7285.

Impacto: Se puede utilizar para la ejecución remota de código

Recomendaciones: Los usuarios pueden registrar un convertidor propio para proxies dinámicos, del tipo java.beans.EventHandler o para el tipo java.lang.ProcessBuilder, comparto el siguiente [enlace](https://x-stream.github.io/CVE-2013-7285.html#workaround) con más procedimientos a revisar.

* [A7 Identity & Auth Failure - Secure Passwords](?tab=t.24rzpq57sozv)

Identificamos como gestionar una password/credencial de forma correcta siguiendo las normas del NIST

Impacto: El aplicación se puede utilizar como un oráculo de contraseñas para determinar si el las credenciales son válidas

Recomendaciones: Disponer de la siguiente [documentación](https://pages.nist.gov/800-63-3/sp800-63b.html) para generar de forma integral contraseñas según valoraciones de NIST.

c. Conclusiones

Abordamos una plataforma deliberadamente insegura para probar vulnerabilidades,y conocer los peligros de que una persona sin autorización manipule datos confidenciales riempiendo su integridad y disponibilidad. Comenzamos a desarrollar un criterio más amplio con respecto a los niveles de vulnerabilidad de nuestros datos en la red.

d. Recomendaciones  
  
Acompañamiento constante a los desarrolladores de BBDD, aplicativos, web, etc. desde un perfil preventivo. Formando e informando nuevas normas y metodologías de seguridad y prevención en el momento de desarrollo e implementación de proyectos digitales (entre otros).

### 3. Descripción del proceso de auditoría

a. Reconocimiento/Information gathering

Se identificaron los puertos que utiliza la plataforma de manera local, lenguaje de programación y reseñas en foros orientados en hacking ético.

b. Explotación de vulnerabilidades detectadas, post-exploración, posibles mitigaciones.

Informo a partir de un índice como he explorado y confirmado las diferentes vulnerabilidades de la plataforma.

e. Herramientas utilizadas

Nmap: Para la revisión y escaneo de los puertos y servicios.

Wappalyzer: Para identificar las tecnologías utilizadas en la plataforma.

Burp/Zap: Para pruebas de seguridad en el entorno web.