OWASP Comprobación Pruebas

[INFO] RECOPILACIÓN DE INFORMACIÓN

- [ ] INFO-001 Fugas de información indexadas por buscadores
- [ ] INFO-002 Fingerprinting del servidor web
- [ ] INFO-003 Fugas de información sensible en metaficheros del servidor
- [ ] INFO-004 Enumeración de aplicaciones en el servidor web
- [ ] INFO-005 Fugas de información sensible en metadatos y comentarios
- [ ] INFO-006 Identificación de puntos de entrada en la aplicación
- [ ] INFO-007 Mapas de rutas de ejecución a través de la aplicación
- [ ] INFO-008 Fingerprinting del framework de la aplicación web
- [ ] INFO-009 Fingerprinting de la aplicación web
- [ ] INFO-010 Mapa de arquitectura de la aplicación

[CONFIG] GESTIÓN DE CONFIGURACIÓN E IMPLEMENTACIÓN

- [ ] CONFIG-001 Configuración de infraestructura/red
- [ ] CONFIG-002 Configuración de la plataforma de la aplicación
- [ ] CONFIG-003 Fugas de información sensible en el manejo de extensiones de archivos
- [ ] CONFIG-004 Fugas de información sensible en archivos obsoletos, de backup o no referenciados
- [ ] CONFIG-005 Enumeración de infraestructura e interfaces de administración de la aplicación
- [ ] CONFIG-006 Métodos HTTP
- [ ] CONFIG-007 HTTP Strict Transport Security
- [ ] CONFIG-008 Política de dominio cruzado RIA
- [ ] CONFIG-009 Permisos de archivos

[IDENT] GESTIÓN DE IDENTIDADES

- [ ] IDENT-001 Definición de roles
- [ ] IDENT-002 Proceso de registro
- [ ] IDENT-003 Proceso de asignación de cuentas de usuario
- [ ] IDENT-004 Enumeración de cuentas de usuario
- [ ] IDENT-005 Política de nombres de usuario débil

[AUTHN] AUTENTICACIÓN

- [ ] AUTHN-001 Transporte de credenciales por canales cifrados
- [ ] AUTHN-002 Uso de credenciales por defecto

- [ ] AUTHN-003 Debilidades en el mecanismo de bloqueo
- [ ] AUTHN-004 Fallos en el esquema de autenticación
- [ ] AUTHN-005 Sistema recuérdame
- [ ] AUTHN-006 Debilidades en la caché del navegador
- [ ] AUTHN-007 Política de contraseñas débiles
- [ ] AUTHN-008 Debilidades en el sistema de pregunta de seguridad
- [ ] AUTHN-009 Debilidades en las funcionalidades de cambio y reseteo de contraseñas
- [ ] AUTHN-010 Canales alternativos de autenticación

[AUTHZ] AUTORIZACIÓN

- [ ] AUTHZ-001 Política de contraseñas débiles
- [ ] AUTHZ-002 Fallos en el control de acceso a recursos y funcionalidades
- [ ] AUTHZ-003 Escalado de privilegios
- [ ] AUTHZ-004 Referencias directas inseguras a objetos

[SESS] GESTIÓN DE SESIONES**

- [ ] SESS-001 Fallos en el sistema de manejo de sesiones
- [ ] SESS-002 Atributos de las cookies
- [ ] SESS-003 Fijación de sesión
- [ ] SESS-004 Variables de sesión expuestas
- [ ] SESS-005 Cross Site Request Forgery (CSRF)
- [ ] SESS-006 Sistema de cierre de sesión
- [ ] SESS-007 Sistema de timeout (caducidad) de la sesión
- [ ] SESS-008 Sobrecarga de variables de sesión (Session Puzzling)

[INPVAL] VALIDACIÓN DE ENTRADA

- [ ] INPVAL-001 Cross Site Scripting reflejado
- [ ] INPVAL-002 Cross Site Scripting almacenado
- [ ] INPVAL-003 Manipulación de verbos HTTP
- [ ] INPVAL-004 Contaminación de parámetros HTTP
- [ ] INPVAL-005 Inyección SQL
- [ ] INPVAL-006 Inyección LDAP
- [ ] INPVAL-007 Inyección ORM
- [ ] INPVAL-008 Inyección XML
- [ ] INPVAL-009 Inyección SSI
- [ ] INPVAL-010 Inyección Xpath

- [ ] INPVAL-011 Inyección IMAP/SMTP
- [ ] INPVAL-012 Inyección de código
- [ ] INPVAL-013 Inyección de comandos
- [ ] INPVAL-014 Sobrecargas de buffer
- [ ] INPVAL-015 Vulnerabilidades incubadas
- [ ] INPVAL-016 HTTP Splitting/Smuggling
- [ ] INPVAL-017 HTTP solicitudes entrantes

[ERR] MANEJO DE ERRORES

- [ ] ERR-001 Análisis de códigos de error
- [ ] ERR-002 Análisis de trazas de error

[CRYPST] CRIPTOGRAFÍA

- [ ] CRYPST-001 Confidencialidad de la información en tránsito
- [ ] CRYPST-002 Padding Oracle
- [ ] CRYPST-003 Envío de información sensible por canales sin cifrar
- [ ] CRYPST-004 Cifrado débil

[BUSLOGIC] LÓGICA DE NEGOCIO

- [ ] BUSLOGIC-001 Validación de datos de la lógica del negocio
- [ ] BUSLOGIC-002 Habilidad de manipulación consultas
- [ ] BUSLOGIC-003 Comprobación de integridad
- [ ] BUSLOGIC-004 Tiempo de procesamiento
- [ ] BUSLOGIC-005 Límite de veces de uso de una función
- [ ] BUSLOGIC-006 Evasión de los flujos de trabajo
- [ ] BUSLOGIC-007 Defensas contra el mal uso de la aplicación
- [ ] BUSLOGIC-008 Subida de tipos de archivos inesperados
- [ ] BUSLOGIC-009 Subida de archivos maliciosos

[CLIENT] PRUEBAS DEL LADO DEL CLIENTE

- [ ] CLIENT-001 Cross Site Scripting basado en DOM
- [ ] CLIENT-002 Ejecución de JavaScript
- [ ] CLIENT-003 Inyección de HTML
- [ ] CLIENT-004 Redireccionamiento de la URL del lado del cliente
- [ ] CLIENT-005 Pruebas de inyección de CSS
- [ ] CLIENT-006 Pruebas de la manipulación de recursos del lado del cliente

- [ ] CLIENT-007 Intercambio de recursos de origen cruzado
- [ ] CLIENT-008 Pruebas de Cross Site Flashing
- [ ] CLIENT-009 Clickjacking
- [ ] CLIENT-010 WebSockets
- [ ] CLIENT-011 Mensajería web
- [ ] CLIENT-012 Almacenamiento local