Lista de verificación de recompensas por errores para aplicaciones web

> Esta lista de verificación puede ayudarte a tener una buena metodología para la búsqueda de recompensas por errores. Cuando hayas realizado una acción, no olvides verificarla;)
> Feliz cacería !

Tabla de contenido

Recon en dominio comodín

- [] Correr en masa
- [] Ejecutar subbuscador
- [] Ejecutar buscador de activos
- [] Ejecute dnsgen
- [] Ejecutar massdns
- [] Utilice httprobe
- [] Ejecute aquatone (captura de pantalla del host activo)

Dominio único

Exploración

- [] Escaneo de Nmap
- [ ] Rastreador de
- eructos [ ] ffuf (difusión de directorios y
- archivos) [ ] hakrawler/gau/paramspider
- [ ] Buscador de enlaces
- [] URL con aplicación de Android

Comprobación manual

- [] Shodan
- [] Censys
- [] idiotas de Google
- [] Pastebin
- [] Github
- [ ] OSINT

Recopilación de información

- [] Explorar manualmente el sitio
- [] Búsqueda/rastreo de contenido perdido u oculto
- [] Busque archivos que expongan contenido, como robots.txt, sitemap.xml, .DS_Store
- [] Verifique los cachés de los principales motores de búsqueda para sitios de acceso público
- [] Verifique las diferencias en el contenido según el agente de usuario (por ejemplo, sitios móviles, acceso como motor de búsqueda). Tractor)
- [ ] Realizar huellas dactilares de aplicaciones web [ ]
- Identificar tecnologías utilizadas [ ]
- Identificar roles de usuario
- [ ] Identificar puntos de entrada de aplicaciones
- [ ] Identificar código del lado del
- cliente [ ] Identificar múltiples versiones/canales (por ejemplo, web, web móvil, aplicación móvil, servicios web)
- [ ] Identificar aplicaciones coalojadas y relacionadas [ ]
- Identificar todos los nombres de host y puertos
- [ ] Identificar contenido alojado por terceros

- [] Identificar los parámetros de depuración

Gestión de configuración

- [] Verifique las URL administrativas y de aplicaciones de uso común
- [] Compruebe si hay archivos antiguos, de copia de seguridad y sin referencia
- [] Verifique los métodos HTTP admitidos y el seguimiento entre sitios (XST)
- [ ] Pruebe el manejo de extensiones de archivos
- [ ] Pruebe la seguridad de los encabezados HTTP (por ejemplo, CSP, X-Frame-Options, HSTS)
- [] Prueba de políticas (por ejemplo, Flash, Silverlight, robots)
- [] Prueba de datos que no son de producción en un entorno real y viceversa
- [] Verifique datos confidenciales en el código del lado del cliente (por ejemplo, claves API, credenciales)

Transmisión segura

- [] Verifique la versión de SSL, los algoritmos y la longitud de la clave
- [ ] Verificación de Validez del Certificado Digital (Duración, Firma y CN)
- [] Verifique las credenciales enviadas solo a través de HTTPS
- [] Verifique que el formulario de inicio de sesión se entregue a través de HTTPS
- [] Verifique los tokens de sesión solo entregados a través de HTTPS
- [] Compruebe si se utiliza la seguridad de transporte estricta HTTP (HSTS)

Autenticación

- [] Prueba de enumeración de usuarios
- [] Prueba de omisión de autenticación
- [] Prueba de protección de fuerza bruta
- [] Probar las reglas de calidad de la contraseña
- [] Prueba la funcionalidad recordarme
- [] Prueba de autocompletar en formularios/entrada de contraseña
- [] Prueba de restablecimiento y/o recuperación de contraseña
- [] Probar el proceso de cambio de contraseña
- [] Prueba CAPTCHA
- [] Pruebe la autenticación multifactor
- [] Prueba de presencia de la funcionalidad de cierre de sesión
- [] Prueba de gestión de caché en HTTP (por ejemplo, Pragma, Expires, Max-age)
- [] Prueba de inicios de sesión predeterminados

- [] Prueba del historial de autenticación accesible al usuario
- [] Prueba de notificación fuera del canal sobre bloqueos de cuentas y cambios de contraseña exitosos
- [] Pruebe la autenticación coherente en todas las aplicaciones con esquema de autenticación compartido/SSO

Gestión de sesiones

- [] Establecer cómo se maneja la gestión de sesiones en la aplicación (por ejemplo, tokens en cookies, token en URL)
- [] Verifique los tokens de sesión para detectar indicadores de cookies (solo http y seguro)
- [] Verifique el alcance de las cookies de sesión (ruta y dominio)
- [] Verifique la duración de las cookies de la sesión (caduca y tiene una edad máxima)
- [] Verifique la terminación de la sesión después de una vida útil máxima
- [] Verificar la finalización de la sesión después del tiempo de espera relativo
- [] Verificar la finalización de la sesión después de cerrar sesión
- [] Pruebe para ver si los usuarios pueden tener varias sesiones simultáneas
- [] Cookies de sesión de prueba para aleatoriedad
- [] Confirme que se emitan nuevos tokens de sesión al iniciar sesión, cambiar de rol y cerrar sesión
- [] Pruebe la gestión de sesiones coherente en todas las aplicaciones con gestión de sesiones compartida
- [] Prueba de desconcierto de sesión
- [] Prueba de CSRF y clickjacking

Autorización

- [ ] Prueba de recorrido de ruta [ ]
- Prueba de elusión del esquema de autorización [ ] Prueba de
- problemas de control de acceso vertical (también conocido como escalada de privilegios)
- [] Prueba de problemas de control de acceso horizontal (entre dos usuarios con el mismo nivel de privilegio)
- [] Prueba de autorización faltante

Validación de datos

- [] Prueba de secuencias de comandos reflejadas entre sitios
- [] Prueba de secuencias de comandos entre sitios almacenadas
- [] Prueba de secuencias de comandos entre sitios basadas en DOM
- [] Prueba de flasheo entre sitios
- [] Prueba de inyección HTML
- [] Prueba de inyección SQL

- [] Prueba de inyección LDAP
- [] Prueba de inyección ORM
- [] Prueba de inyección XML
- [] Prueba de inyección XXE
- [] Prueba de inyección SSI
- [] Prueba de inyección XPath
- [] Prueba de inyección XQuery
- [] Prueba de inyección IMAP/SMTP
- [] Prueba de inyección de código
- [] Prueba de inyección de lenguaje de expresión
- [] Prueba de inyección de comando
- [] Prueba de desbordamiento (pila, montón y entero)
- [] Prueba de cadena de formato
- [] Prueba de vulnerabilidades incubadas
- [] Prueba de división/contrabando de HTTP
- [] Prueba de manipulación de verbos HTTP
- [] Prueba de redirección abierta
- [] Prueba de inclusión de archivos locales
- [] Prueba de inclusión remota de archivos
- [] Comparar reglas de validación del lado del cliente y del lado del servidor
- [] Prueba de inyección NoSQL
- [] Prueba de contaminación de parámetros HTTP
- [] Prueba de enlace automático
- [] Prueba de asignación masiva
- [] Prueba de cookie de sesión NULL/no válida

Negación de servicio

- [] Prueba de antiautomatización
- [] Prueba de bloqueo de cuenta
- [] Prueba para el protocolo HTTP DoS
- [] Prueba de DoS comodín SQL

Lógica de negocios

- [] Prueba de uso indebido de funciones

- [ ] Prueba de falta de no repudio
- [] Prueba de relaciones de confianza
- [] Prueba de integridad de los datos
- [ ] Prueba de segregación de funciones

Criptografía

- [] Compruebe si los datos que deben cifrarse no están
- [] Verifique el uso de algoritmos incorrectos según el contexto
- [] Verifique el uso de algoritmos débiles
- [ ] Verificar el uso adecuado de la salazón
- [] Verifique las funciones de aleatoriedad

Funcionalidad riesgosa: carga de archivos

- [ ] Pruebe que los tipos de archivos aceptables estén incluidos en la
- lista blanca [ ] Pruebe que los límites de tamaño de archivo, la frecuencia de carga y el recuento total de archivos estén definidos y se
- apliquen [ ] Pruebe que el contenido del archivo coincida con el tipo de
- archivo definido [ ] Pruebe que todas las cargas de archivos tengan antivirus escaneo en el lugar.
- [] Pruebe que los nombres de archivos inseguros estén desinfectados
- [] Pruebe que los archivos cargados no sean accesibles directamente desde la raíz web
- [] Pruebe que los archivos cargados no se entreguen en el mismo nombre de host/puerto
- [] Pruebe que los archivos y otros medios estén integrados con los esquemas de autenticación y autorización.

Funcionalidad riesgosa: pago con tarjeta

- [] Prueba de vulnerabilidades conocidas y problemas de configuración en el servidor web y la aplicación web
- [] Prueba de contraseña predeterminada o adivinable
- [] Prueba de datos que no son de producción en un entorno real y viceversa
- [] Prueba de vulnerabilidades de inyección
- [] Prueba de desbordamientos del búfer
- [] Prueba de almacenamiento criptográfico inseguro
- [] Prueba de protección insuficiente de la capa de transporte
- [] Prueba de manejo inadecuado de errores
- [] Pruebe todas las vulnerabilidades con una puntuación CVSS v2 > 4,0
- [] Prueba de problemas de autenticación y autorización
- [] Prueba de CSRF

HTML5

- [] Prueba de mensajería web
- [] Prueba de inyección SQL de almacenamiento web
- [] Verifique la implementación de CORS
- [] Verificar aplicación web sin conexión

Fuente:

OWASP