chulelita demasiada rica todo owasp pdf : https://owasp.org/www-pdf-archive/

top 10 web

2023
top 10
A01: autorización a nivel de objeto roto
A02: autenticación rota
A03: autorización de nivel de propiedad de objeto roto
A04: Consumo de recursos sin restricciones
A05: Autorización de nivel de función rota
A06: acceso sin restricciones a flujos comerciales confidenciales
A07: Falsificación de solicitudes del lado del servidor
A08: configuración incorrecta de seguridad
A09: Gestión inadecuada del inventario
A10: Consumo inseguro de API
https://owasp.org/API-Security/editions/2023/en/0x11-t10/

2021
top 10
A01: Broken Access Control
A02: Fallos criptográficos
A03: La inyección se
A04: Diseño inseguro
A05: La configuración incorrecta de seguridad
A06: Componentes vulnerables y obsoletos
A07: Identification and Authentication Failures
A08: Software and Data Integrity Failures
A09: Security Logging and Monitoring Failures
R10: falsificación de solicitudes del lado del servidor 2021
A10: Falsificación de solicitudes del lado del servidor (SSRF)

.....

2020
top 10
10- Técnicas de evasión WAF
9 - Atacar las interfaces web de MS Exchange
8- ImageMagick - Inyección de shell mediante contraseña PDF
7 - RCE no autenticado en MobileIron MDM
6 - Contrabando de encabezados HTTP a través de proxies inversos

5 - NAT Slipstreaming
4 - Cuando TLS te piratea
3 - Atacar contextos secundarios en aplicaciones web
2 - ExFiltración de datos portátil: XSS para PDF
1 - Contrabando de H2C: Solicitar contrabando a través de HTTP / 2 Texto sin cifrar

.....
.....

2019

top 10

10.Aprovechamiento del desbordamiento del búfer de bytes nulos para obtener una recompensa de $ 40,000
9. Microsoft Edge (Chromium) - EoP a RCE potencial
8. Infiltrarse en una intranet corporativa como la NSA: RCE previo a la autenticación en las principales VPN SSL
7. Explorando los servicios de CI como un cazarrecompensas de errores
6. Todo lo que llega a .NET es XSS
5. Búsqueda de Google XSS
4. Abuso de la metaprogramación para RCE no autenticado
3. Poseer la Falsificación a través de la Falsificación de Solicitudes del lado del Servidor
2. Fugas entre sitios
1. En caché y confuso: el engaño de la caché web en la naturaleza

.....
.....

2018

top 10

10. XS-Searching en el rastreador de errores de Google para descubrir el código fuente vulnerable
9. Exfiltración de datos mediante inyección de fórmula
8. Prepare (): Introducción de nuevas técnicas de explotación en WordPress
7. Explotación de XXE con archivos DTD locales
6. Es una vulnerabilidad de no serialización de PHP Jim, pero no como la conocemos
5. Atacar las tecnologías web "modernas"
4. Prototipo de ataques de contaminación en aplicaciones NodeJS
3. Más allá de XSS : el lado del borde incluye inyección
2. Envenenamiento práctico de caché web: redefinición de "no explotable"
1. Rompiendo la lógica del analizador: ¡Elimine la normalización de su ruta y salga de 0 días!

.....
.....

2017

top 10

10. Webshell binario a través de OPcache en PHP 7
9. Informe técnico de seguridad del navegador Cure53

8. Solicite la codificación para evitar los firewalls de las aplicaciones web.
7. Profundización en los controles de acceso de AWS S3
6. Vulnerabilidades avanzadas de Flash
5. Cloudbleed
4. Viernes 13 de ataques JSON
3. Truco de entradas
2. Engaño de la caché web
1. Una nueva era de la SSRF

.....
.....
Tema owasp para practicar
.....
.....
Contrabando de solicitudes HTTP
Falsificación de solicitudes del lado del servidor (SSRF)
Uso compartido de recursos de origen cruzado (CORS)
Clickjacking (reparación de la interfaz de usuario)
Inyección de entidad externa XML (XXE)
Falsificación de solicitudes entre sitios (CSRF)
Secuencias de comandos entre sitios
inyección SQL
Envenenamiento de caché web
Vulnerabilidades de la lógica empresarial
Ataques de encabezado de host HTTP
Vulnerabilidades de autenticación de OAuth 2.0
Inyección de comandos del sistema operativo
Inyección de plantillas del lado del servidor
Deserialización insegura
Cruce de directorio
Vulnerabilidades de control de acceso y escalada de privilegios
Vulnerabilidades de autenticación
Prueba de vulnerabilidades de seguridad de WebSockets
Vulnerabilidades basadas en DOM
Vulnerabilidades de divulgación de información
cryptografia debil hash-identifider
Web socket
Vulnerabilidades de divulgación de información

CMS:
wordpress
aws
joomla
Drupal