pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

Introduction to: SQL Injection

by Paul Ritchie, @cornerpirate

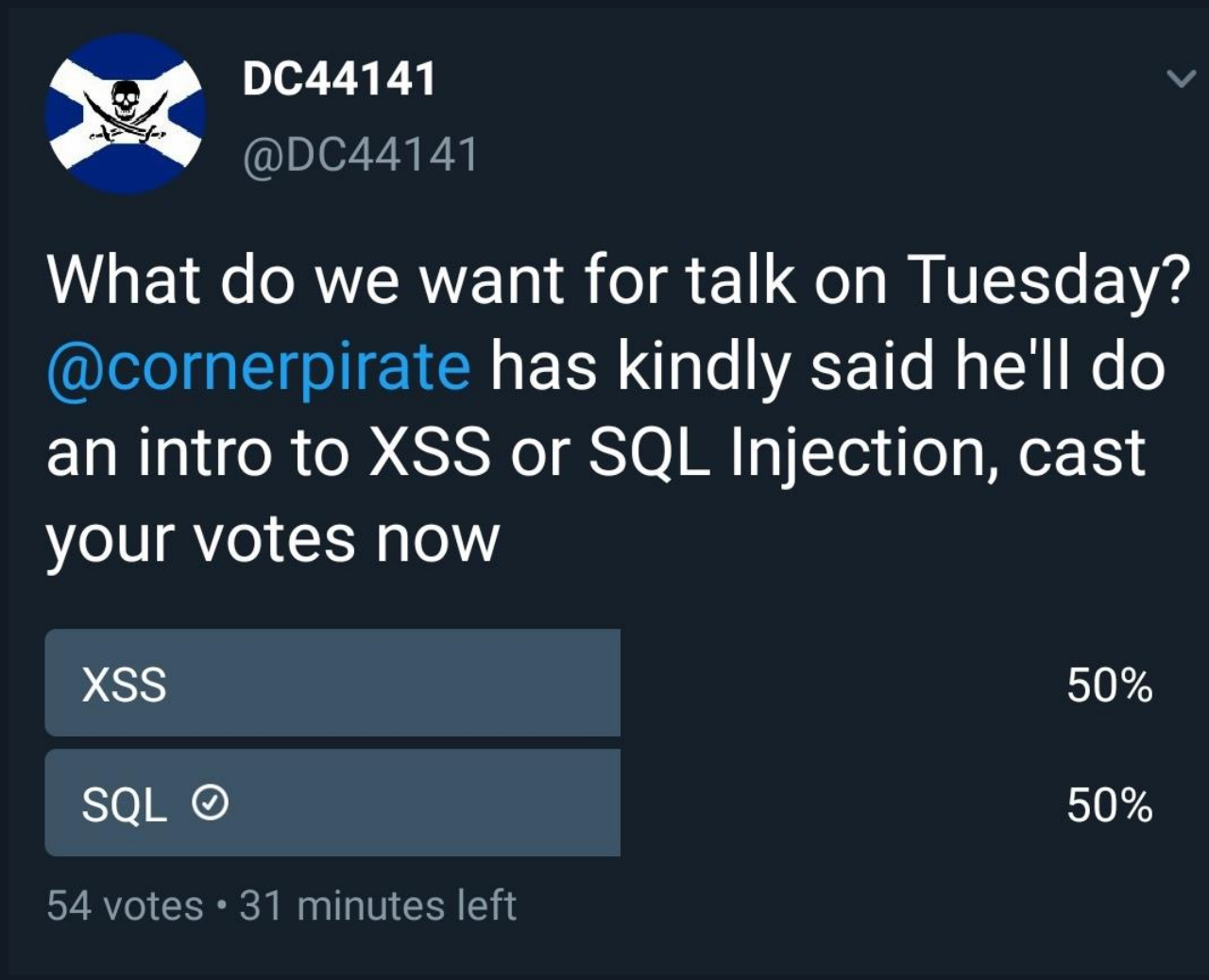
pentest.co.uk

Democracy-ish

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

Boaty mcBoatface 2.0!

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company



What is SQL?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- 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.
- 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!

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

Oh look it crawls!

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- SELECT * FROM People WHERE age<40;

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
3	Lila Shirley	25

Baby's first steps!

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

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

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?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

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

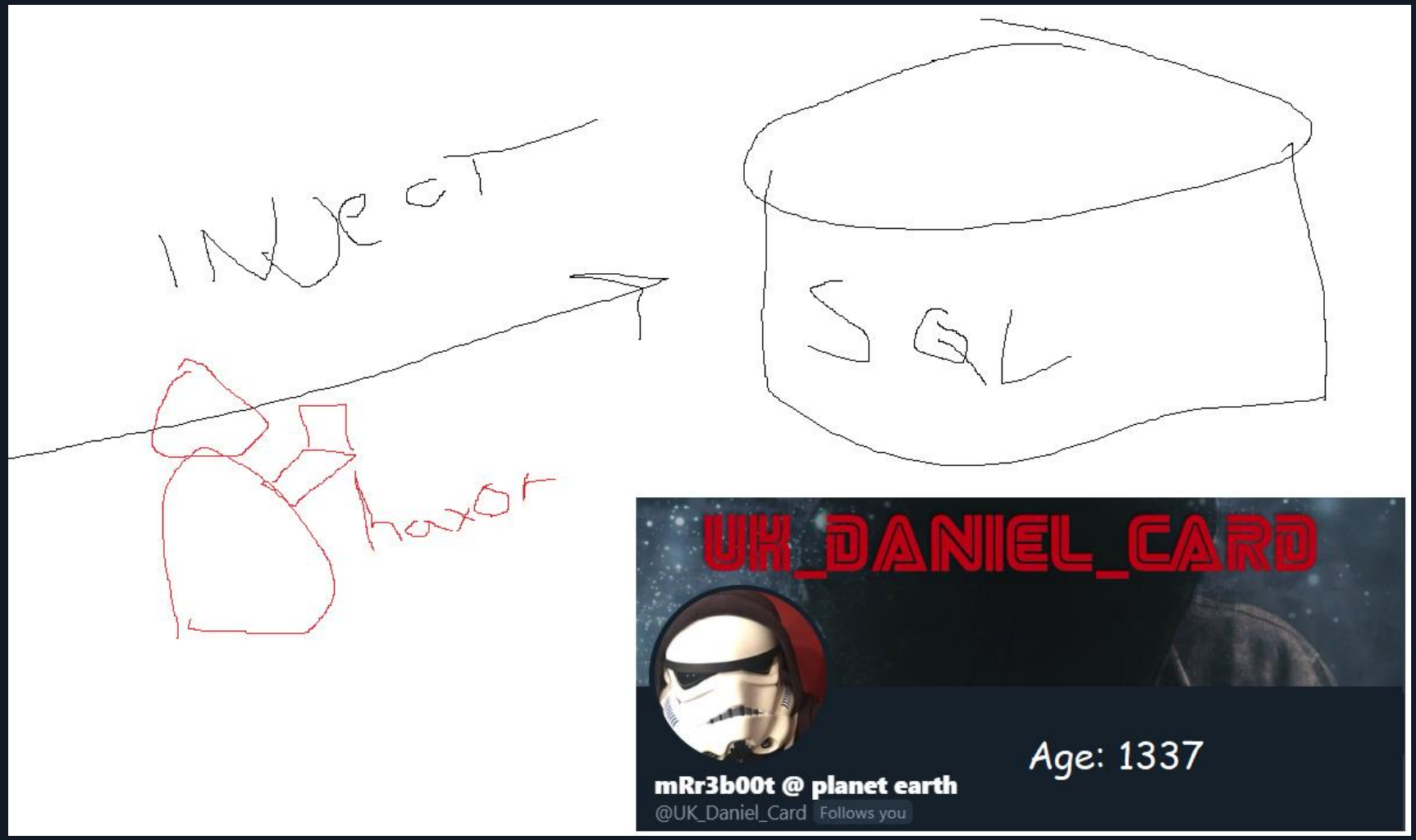
```
$sql = “SELECT * FROM People WHERE age<” + $_GET[“age"];
```

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

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

What is it though?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company



#1 – Injection into String Field

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Strings in SQL are wrapped in single-quotes.

```
mysql> select 'DC44141';
+----------+
| DC44141 |
+----------+
| DC44141 |
+----------+
1 row in set (0.00 sec)
```

#1 – Injection into String Field

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Suspect SQL Injection into a string field?
- You will need to:
  - Break out of the original string (using single-quote character)
  - Supply new logic.
  - End the remaining query ensuring it is valid SQL:

a’ NEW LOGIC OR ‘1’=‘1
a’ NEW LOGIC --
a’; ENTIRELY NEW SQL QUERY; --

#1 – Injection into String Field

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- DEMO GODS BE PRAISED.

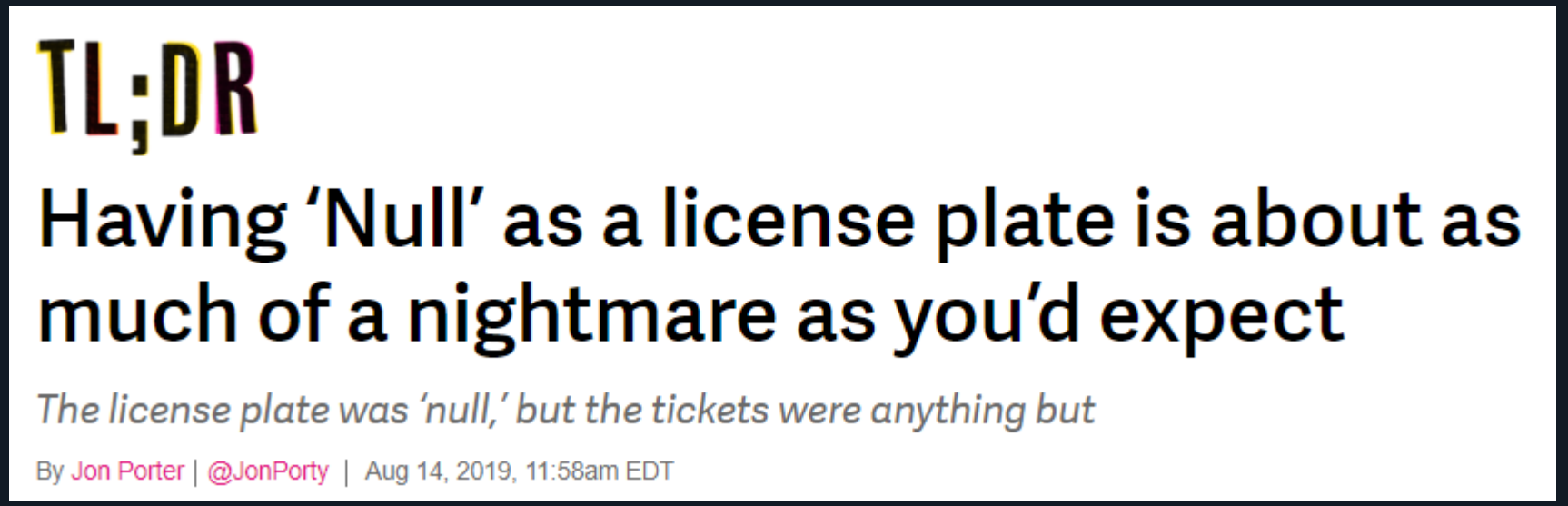
Getting Something out of it

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Finding the number columns in query with "ORDER BY N"
- Using "UNION SELECT" with the "null" data type
- Extraction of something an attacker did not know before:
  - @@version - in MYSQL

null never hurt anyone!

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company



TL;DR

Having 'Null' as a license plate is about as much of a nightmare as you'd expect

The license plate was 'null,' but the tickets were anything but

By Jon Porter | @JonPorty | Aug 14, 2019, 11:58am EDT

- Registered personal number plate 'null'
- Racked up a bill of $12,049.

Source: https://www.theverge.com/tldr/2019/8/14/20805543/null-license-plate-california-parking-tickets-violations-void-programming-bug

#2 – Injection into Numeric Field

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Numeric fields are NOT wrapped in single-quotes.

```
mysql> select 123;
+-----+
| 123 |
+-----+
| 123 |
+-----+
1 row in set (0.00 sec)
```

#2 – Injection into Numeric Field

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- DEMO GODS BE PRAISED.

Data from another table

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- We showed enumerating table names
  - Querying INFORMATION_SCHEMA.TABLES
- Then column names for those tables.
  - Querying INFORMATION_SCHEMA.COLUMNS
- Finally, we got some secrets out of another table.

#3 – Authentication Bypass

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- DEMO GODS BE DAMNED!

How did that work?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Intended Query:

```
SELECT * FROM users
WHERE username='<x>' AND password ='<y>'
```

- By controlling "username" we executed:

```
SELECT * FROM users
WHERE username='a' OR 1=1 -- AND password ='<y>'
```

OR Truth Table

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

Pizza	Chips	Answer
False	False	False
True	False	True
False	True	True
True	True	True

But why were we admin?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

```
mysql> select * from users;
+----+----------+-----------+
| id | username | password  |
+----+----------+-----------+
|  1 | admin    | secureguy |
|  2 | aaa      | aaaaaa    |
|  3 | bbb      | bbbbbb    |
|  4 | ccc      | cccccc    |
+----+----------+-----------+
4 rows in set (0.00 sec)

mysql> select * from users where username='a' or 1=1-- and username='b'
    -> ;
+----+----------+-----------+
| id | username | password  |
+----+----------+-----------+
|  1 | admin    | secureguy |
|  2 | aaa      | aaaaaa    |
|  3 | bbb      | bbbbbb    |
|  4 | ccc      | cccccc    |
+----+----------+-----------+
4 rows in set (0.00 sec)
```

STOP - what about impact?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

Confidentiality

- Attacker will have access to data that they should not.
- A data breach may result in industry or legal fines.

Integrity

- Attacker can change data then trust in its integrity is lost.
- Equally if an attacker can execute commands on a compromised computer then it can no longer be trusted.

Availability

- Making a resource inaccessible to legitimate users removes its availability.
- Doing so can prevent companies from trading and result in significant financial and reputational damages.

But what is impacted?

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- The application (what does that mean?)
- The database (all of it? part of it?)
- The operating systems of the app and database servers
- Is a user's PC impacted at all?
- Will a user be the victim of ID theft if exploited?
- What about the business interests or reputation of the application and the company who own it.

Confidentiality

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Most applications are configured with a database user account which has full read access to the data processed by that application.
- Full loss of Confidentiality (for data processed by the application) is almost certain.
- Files stored by the OS can *generally* be read too.
- Security principal of “Least Privilege” may limit impact to one database and prevent file access etc.

Integrity

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Most applications are configured with a database user account which can modify the data processed by that application.
- Full loss of Integrity (for data processed by the application) is almost certain.
- Some databases allow command execution on the OS meaning you can no longer trust the OS!
- Least privilege again *could* limit the impact.

Availability

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- Most applications are configured with a database user account which can delete the data processed by that application.
- Full loss of the Availability (for data processed by the application) is almost certain.

  DROP TABLE people;

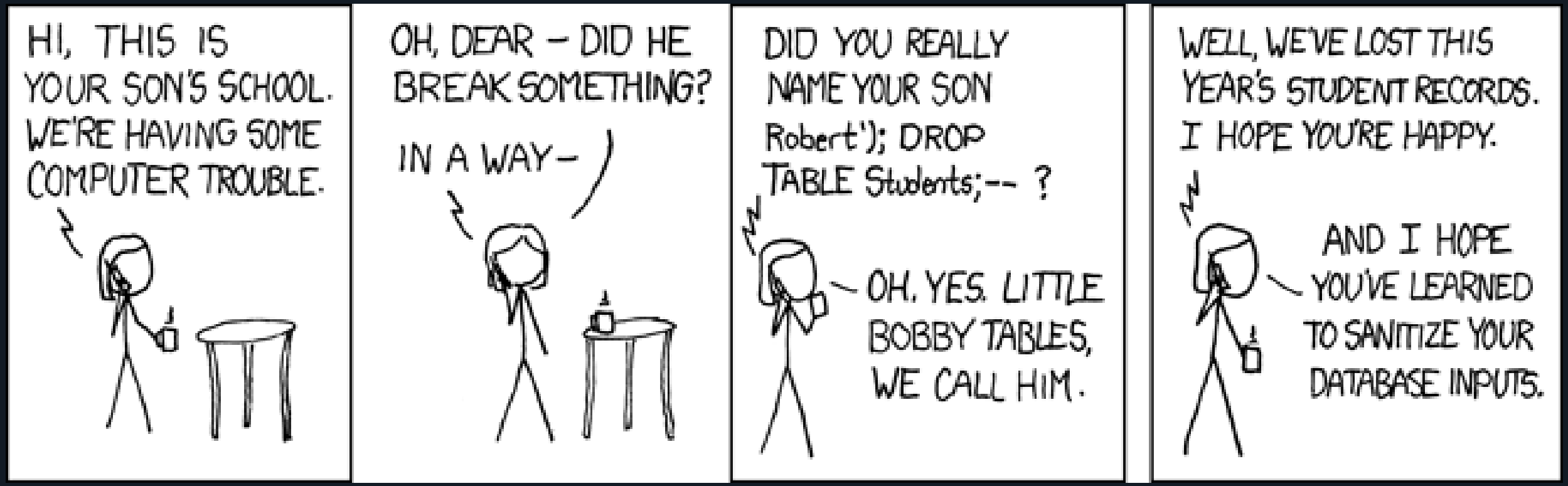
- Injecting into an “UPDATE” or “DELETE” statement without thinking:

  DELETE FROM people WHERE id=1

  DELETE FROM people WHERE *id*=*1 OR 1=1--*

Now you get this!

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company



Source: https://xkcd.com/327 /

Preventing SQL Injection

pentest
INFORMATION SECURITY ASSURANCE
A Shearwater Group plc Company

- 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

- The demo targets will be made available soon.
- Follow me on Twitter @cornerpirate
- I will shout about it there, and also probably stick a recording of this material and the slides out too.
- Intent is to give you time to play with these things before coming back for more advanced SQL Injection next month

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