data amplified™

PARIS 2017

THE **FUTURE** OF BUSINESS REPORTING

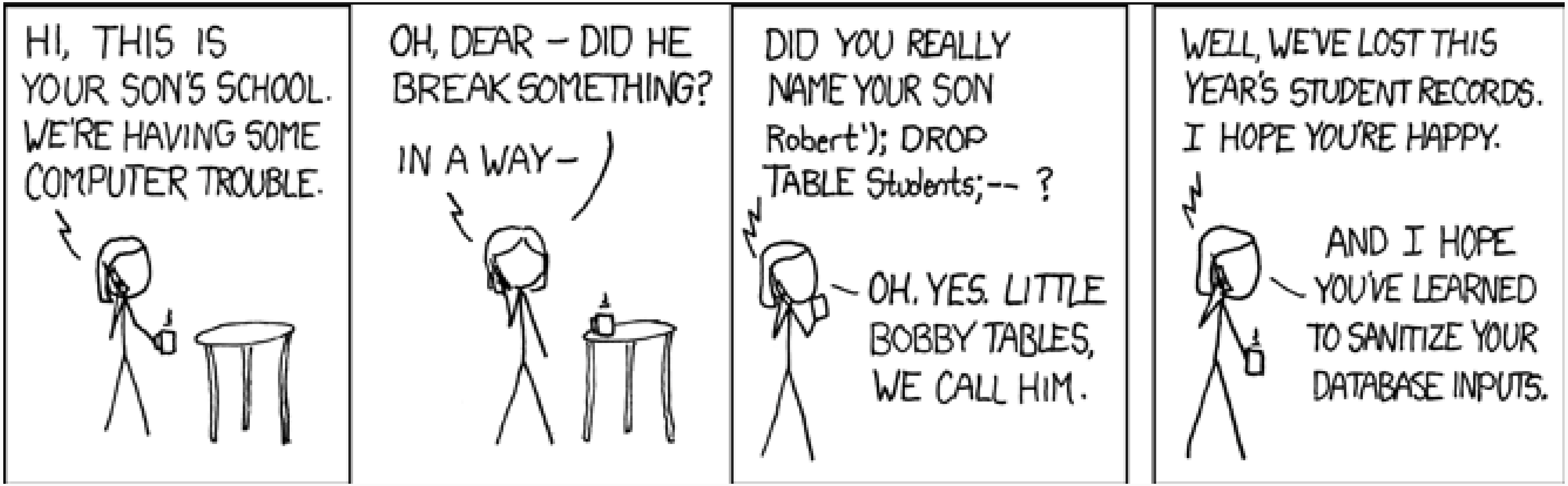
XBRL & Cybersecurity

Paul Warren

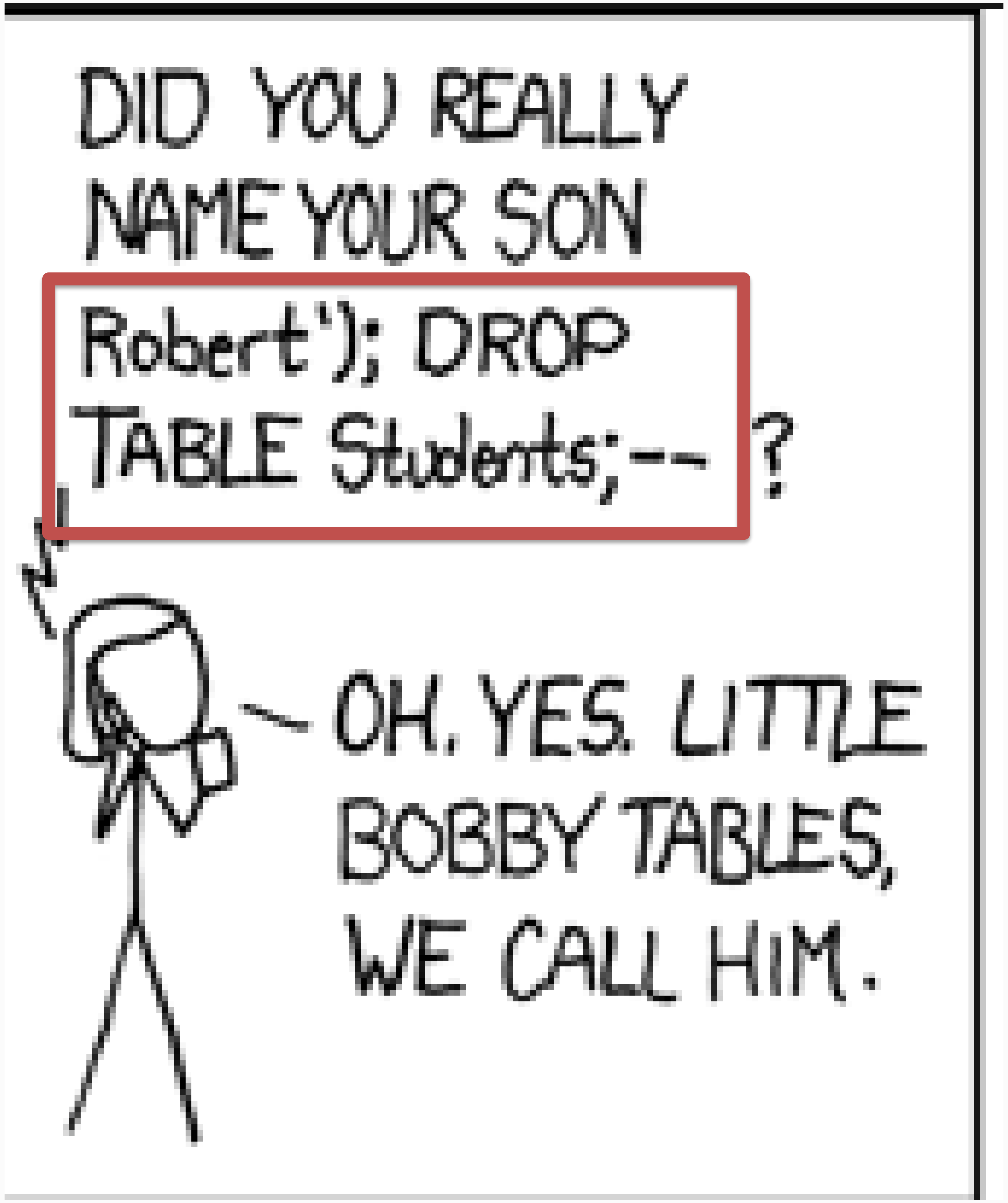
Technical Director
XBRL International

Anatomy of a security vulnerability

What does an exploit look like?


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

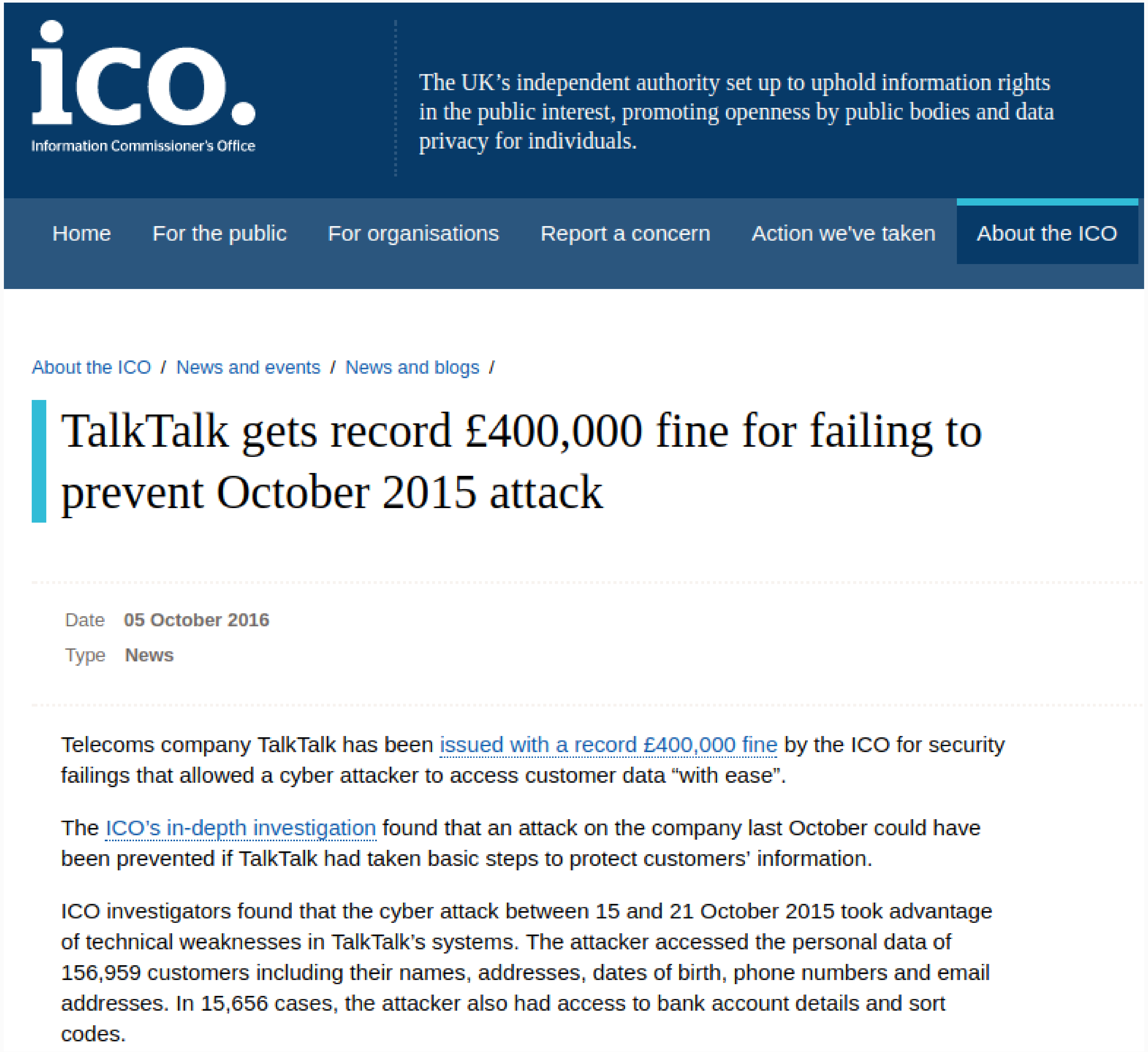
https://xkcd.com/327/


DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.

SQL injection attack

XKCD 327 has just had its 10th anniversary

SQL injection remains depressingly fashionable…



The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack

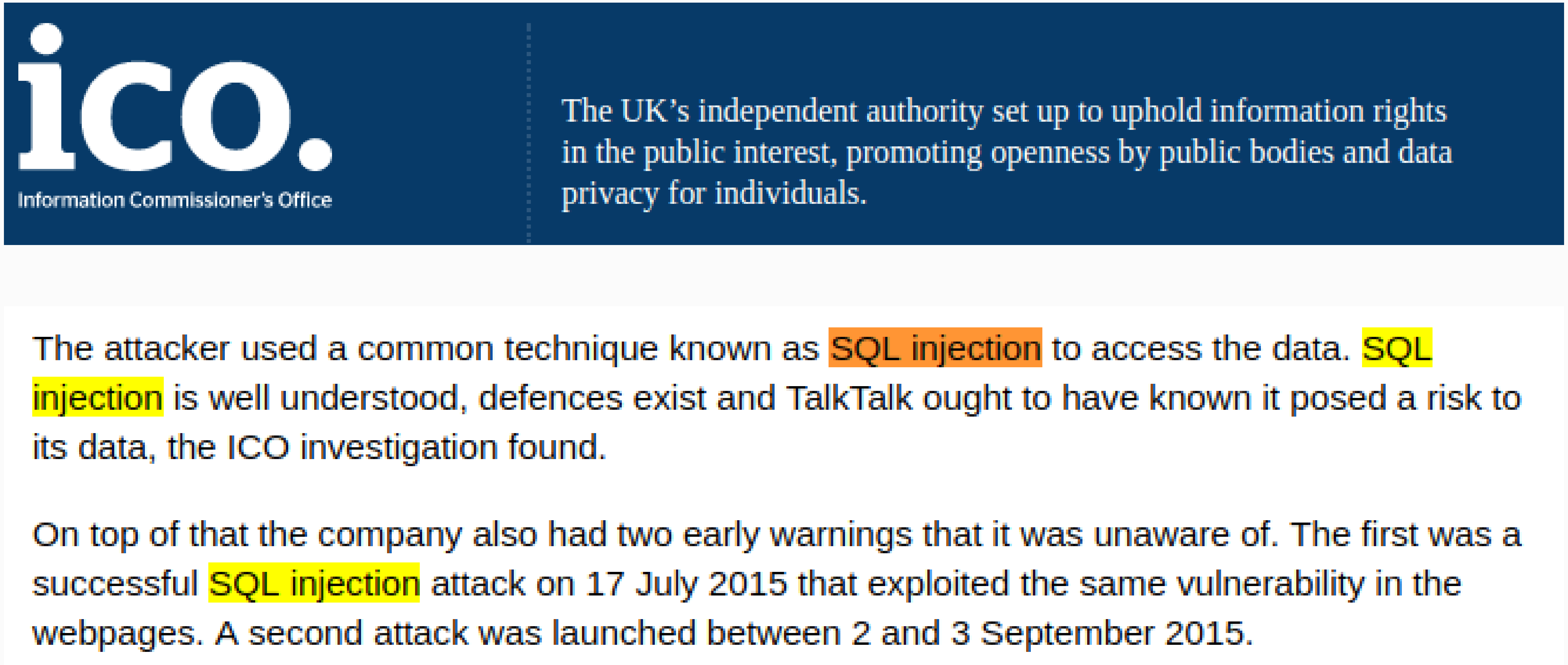
Date **05 October 2016**

Type **News**

Telecoms company TalkTalk has been issued with a record £400,000 fine by the ICO for security failings that allowed a cyber attacker to access customer data "with ease".

The ICO's in-depth investigation found that an attack on the company last October could have been prevented if TalkTalk had taken basic steps to protect customers' information.

ICO investigators found that the cyber attack between 15 and 21 October 2015 took advantage of technical weaknesses in TalkTalk's systems. The attacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers and email addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes.



ico.

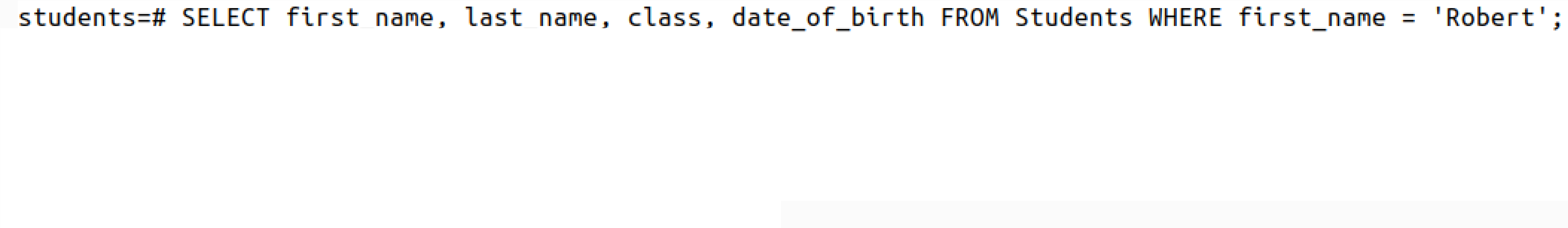
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The attacker used a common technique known as SQL injection to access the data. SQL injection is well understood, defences exist and TalkTalk ought to have known it posed a risk to its data, the ICO investigation found.

On top of that the company also had two early warnings that it was unaware of. The first was a successful SQL injection attack on 17 July 2015 that exploited the same vulnerability in the webpages. A second attack was launched between 2 and 3 September 2015.

So what is it?



```
students=# SELECT first_name, last_name, class, date_of_birth FROM Students WHERE first_name = 'Robert';
```

Dynamic queries

Little Bobby Tables

```
$first_name = "Robert";; DROP TABLE Students; -- ";
```

```
SELECT first_name, last_name, class, date_of_birth FROM Students WHERE first_name = '$first_name';
```

Little Bobby Tables

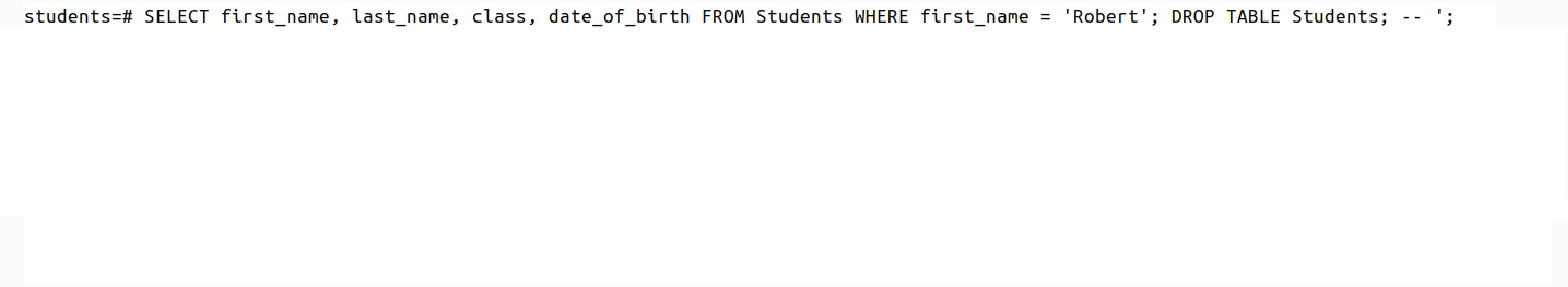
```
$first_name = "Robert' ; DROP TABLE Students; -- ";
```

```
SELECT first_name, last_name, class, date_of_birth FROM Students WHERE first_name = 'Robert'; DROP TABLE Students; -- ';
```

Little Bobby Tables

```
$first_name = "Robert' ; DROP TABLE Students; -- ";
```

```
SELECT first_name, last_name, class, date_of_birth FROM Students WHERE first_name = 'Robert';
DROP TABLE Students;
-- ';
```

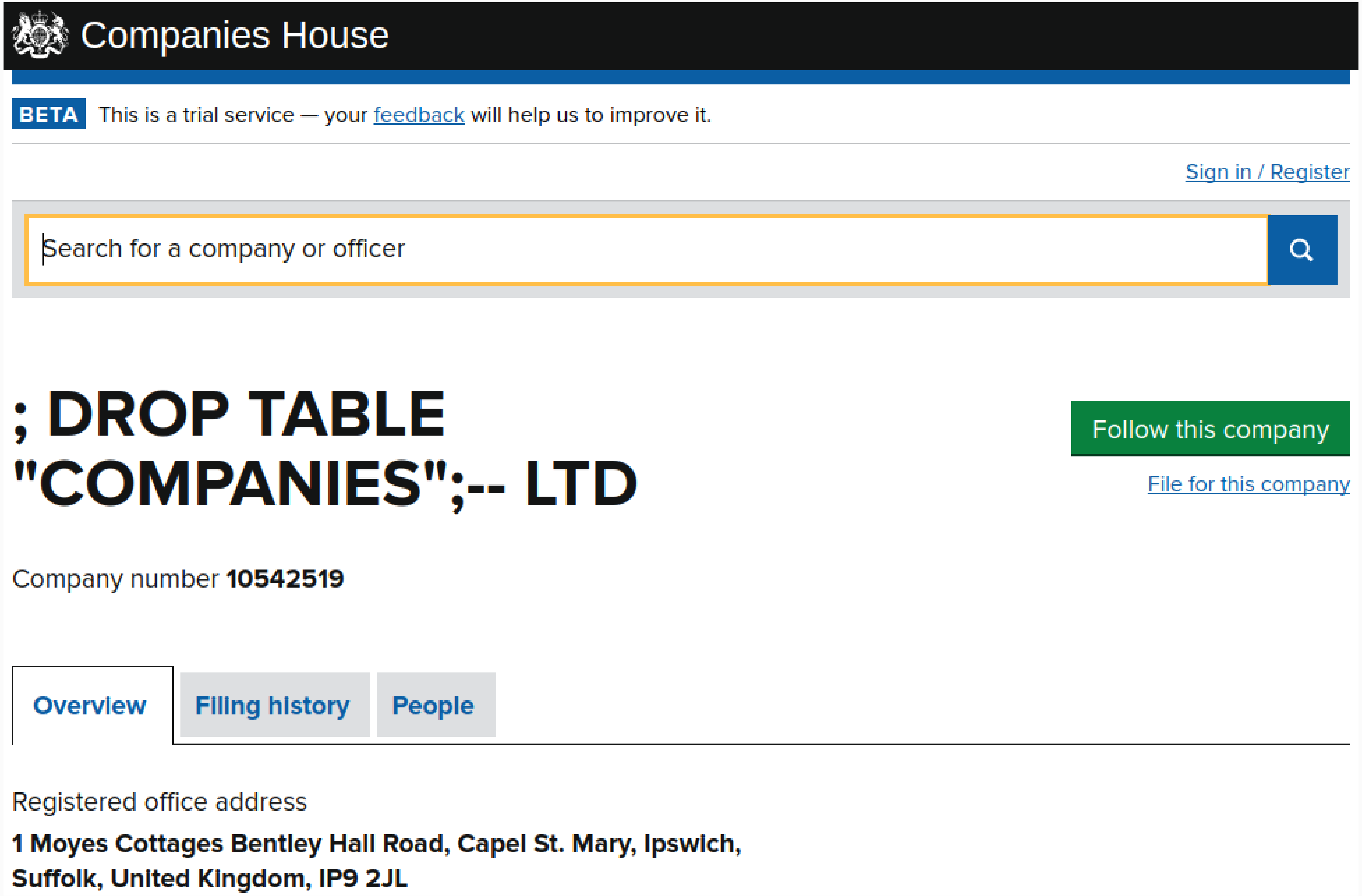


```
students=# SELECT first_name, last_name, class, date_of_birth FROM Students WHERE first_name = 'Robert'; DROP TABLE Students; -- ';
```

Uh oh.

How is this relevant to the world of business reporting?

UK Company number 10542519



This is a trial service — your feedback will help us to improve it.

; DROP TABLE "COMPANIES";-- LTD

Company number **10542519**

Registered office address

1 Moyes Cottages Bentley Hall Road, Capel St. Mary, Ipswich, Suffolk, United Kingdom, IP9 2JL

Is cyber security an issue for XBRL implementations?

Cross Site Scripting

(XSS)

Cross-site scripting (XSS)

- Typical log-in process:

  1. Website (e.g. yourbank.com) ask for username & password
  2. You provide username and password to website
  3. Website checks credentials, and if valid, gives you a token (a cookie)
  4. Your browser provides that cookie on future requests during that session

Anyone who has the cookie can get access to the site

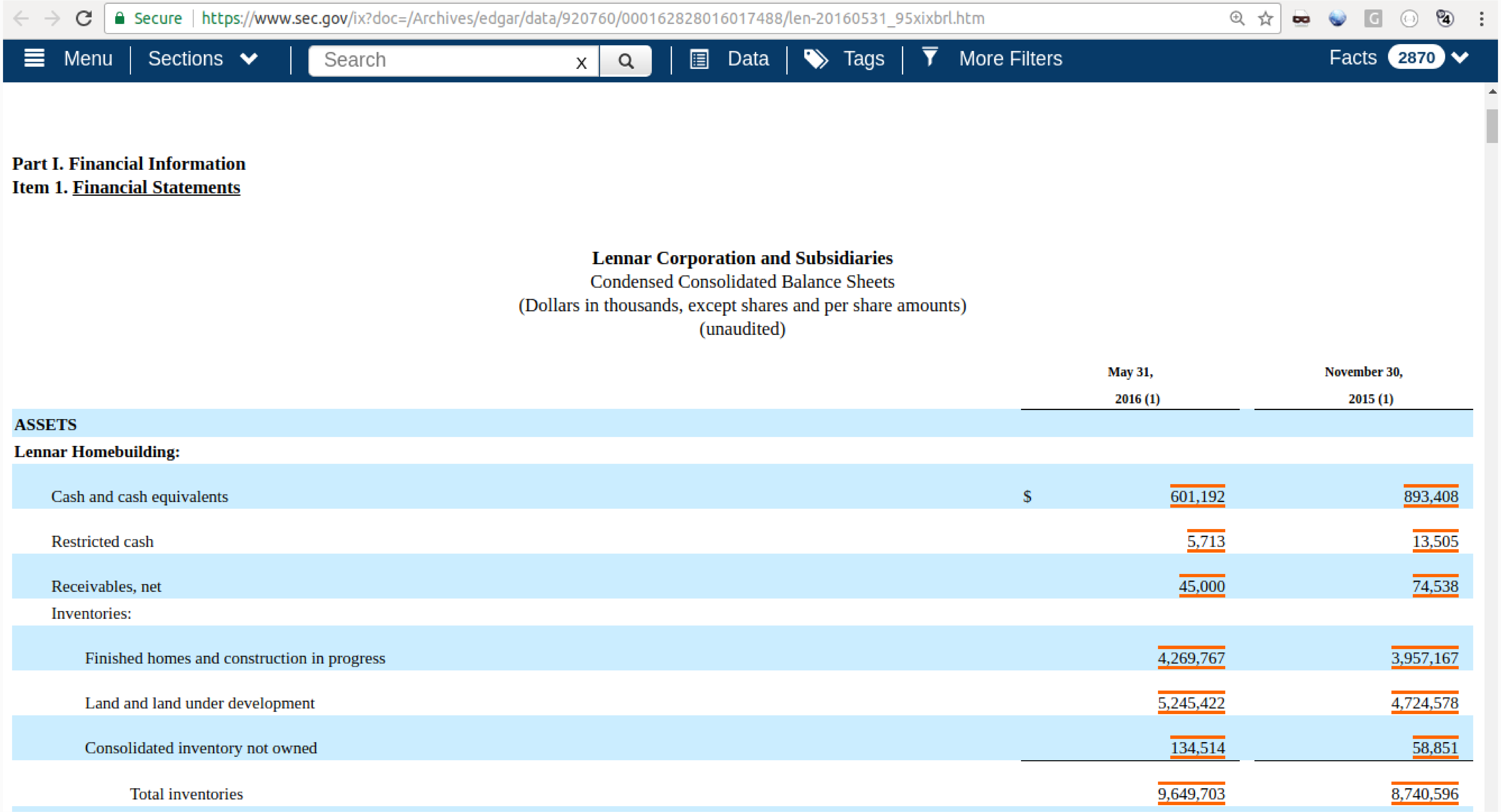
Your browser will only give the cookie to the right site (https://www.yourbank.com)

Cross-site scripting (XSS)

Your browser will only give the cookie to the right site (https://www.yourbank.com)

If an attacker can get their own HTML tags (including <script> tags) displayed on a https://www.yourbank.com page and can get you to look at it, they can steal your cookie.

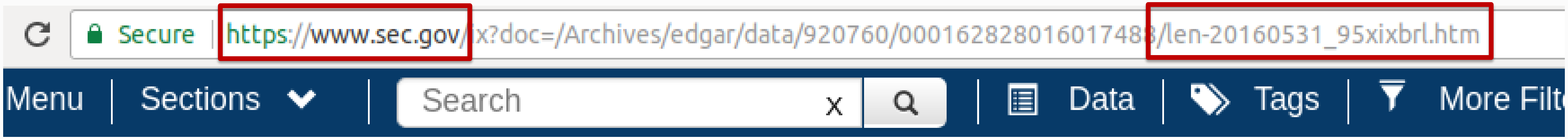
The goal of an XSS attack is to get **your HTML** displayed on **someone else's site**


Secure
https://www.sec.gov/ix?doc=/Archives/edgar/data/920760/000162828016017488/len-20160531_95xixbrl.htm
Menu
Sections
Search
X
Data
Tags
More Filters
Facts 2870

Part I. Financial Information
Item 1. Financial Statements

Lennar Corporation and Subsidiaries
Condensed Consolidated Balance Sheets
(Dollars in thousands, except shares and per share amounts)
(unaudited)

		May 31, 2016 (1)	November 30, 2015 (1)
ASSETS			
Lennar Homebuilding:			
Cash and cash equivalents	$	601,192	893,408
Restricted cash		5,713	13,505
Receivables, net		45,000	74,538
Inventories:			
Finished homes and construction in progress		4,269,767	3,957,167
Land and land under development		5,245,422	4,724,578
Consolidated inventory not owned		134,514	58,851
Total inventories		9,649,703	8,740,596


Secure https://www.sec.gov/ix?doc=/Archives/edgar/data/920760/000162828016017488/len-20160531_95xixbrl.htm

The goal of an XSS attack is to get **your HTML** displayed on **someone else's site**…

Is cyber security an issue of XBRL implementations?

Is cyber security an issue of XBRL implementations?

Yes!

Don't panic. Sanitise your inputs.