Exploiting Vulnerabilities: SQLi, XSS, XXE, File Injection

January 2019

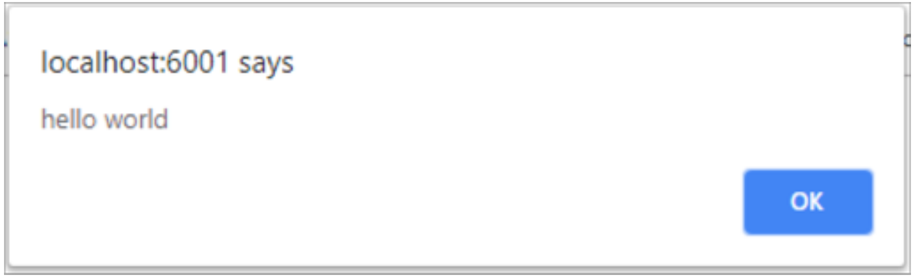
Pushpay

Ko Ranginui kei runga
Ko Papatuanuku kei raro
Ko nga tangata kei waenganui
Tihei wā Mauri Ora!

Ranginui (Sky Father) is above
Papatuanuku (Earth Mother) is below
Their children in between (That’s us)
I sneeze to life! (Behold there is life)

Ko Rangitoto te Maunga	Rangitoto is the mountain
Ko Motuihunga te Motu	Motuihe is the island
Ko Hauraki te Moana	The Hauraki Gulf is the sea
Ko Pupuke te Roto	Lake Pupuke is the lake
Ko Burman te Waka	I arrived on the Burman
Ko Ngati Pakeha te Iwi	My iwi (tribe) is pakeha
Ko Wakanui te Marae	My gathering place is Wakanui
Nō Pushpay ahau	I am part of Pushpay
Ko David ahau	I am David
Tēnā koutou,	Greetings to you
Tēnā koutou,	Greetings to you
Tēnā tātou katoa,	Greetings to us all

XSS



localhost:6001 says

hello world

XSS

Where user data is echoed verbatim on a page

What if the user data includes content such as

```
<script>alert(‘hello world’)</script>
```

Persistent XSS

DEMO

Persistent XSS

Modern frameworks make it *quite difficult* to output verbatim (`Html.Raw`, `dangerouslySetInnerHTML`, etc)

Make sure when using these methods that they don’t contain user data

Persistent XSS

XSS Mitigations

- Context sensitive auto escaping
- Strict Content Security Policy (CSP)

CSRF

Browsers send Cookies

Cookies control Authentication

If we can trick the browser into sending a request, it will include the authentication cookie

CSRF

DEMO

CSRF

Requires active mitigation

Usually through a form value (token) that must also be present for data-manipulation requests

Modern frameworks will come with a built-in way to do this

CSRF

You also need to protect Ajax endpoints

Reflected XSS + CSRF

Combining Multiple Low Severity Issues gives high severity issues

Reflected XSS + CSRF

DEMO

Reflected XSS + CSRF

XSS Mitigations

- Context sensitive auto escaping
- Strict Content Security Policy

CSRF Mitigations

- Token Based

XXE

- Xml eXternal Entity

XXE

DEMO

XXE

XXE Mitigations

- Disable DTD

File Injection

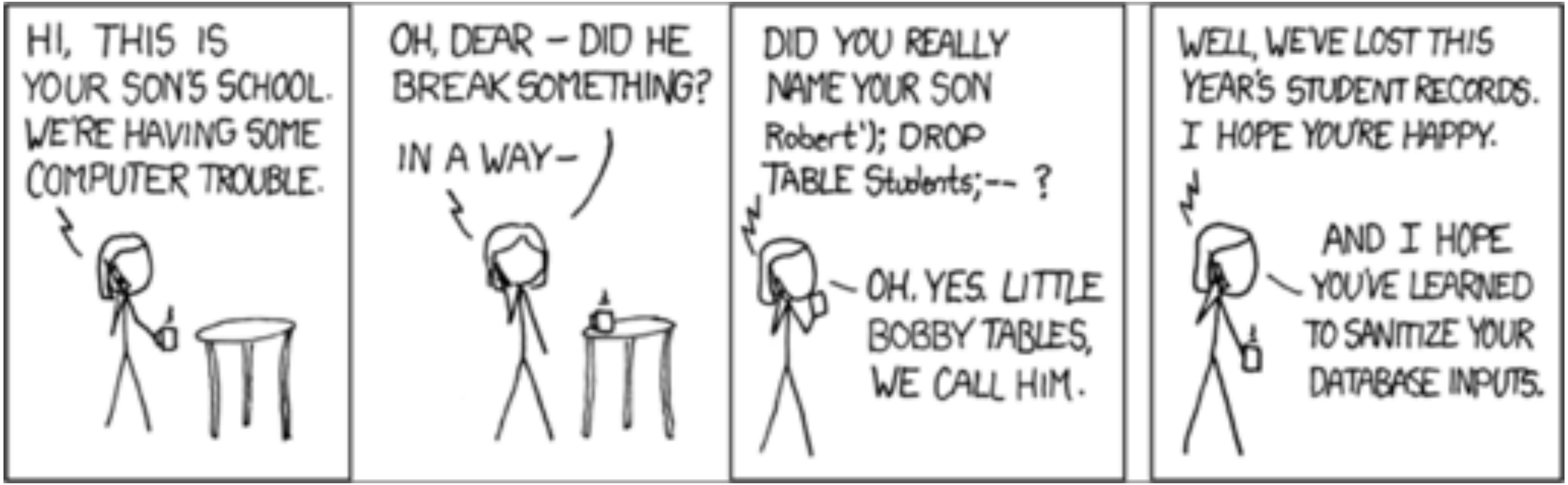
File Injection

DEMO

File Injection - Mitigation

- Don’t persist user supplied name
- Don’t serve directly
- Do serve off alternate domain

SQLi


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/

SQLi

Injection

Where a command is built by interpolating user data

SQL Injection

Where a SQL query is built by interpolating user data

SQLi

eg

```
var query = $“SELECT id, name FROM USERS
WHERE name LIKE ‘%{ username }%’”;
```

SQLi

You’d know if someone dropped your database…

SQLi

DEMO

SQLi

This made use of the error page

Even without an error page, SQLMAP can use timing to extract data

SQLi

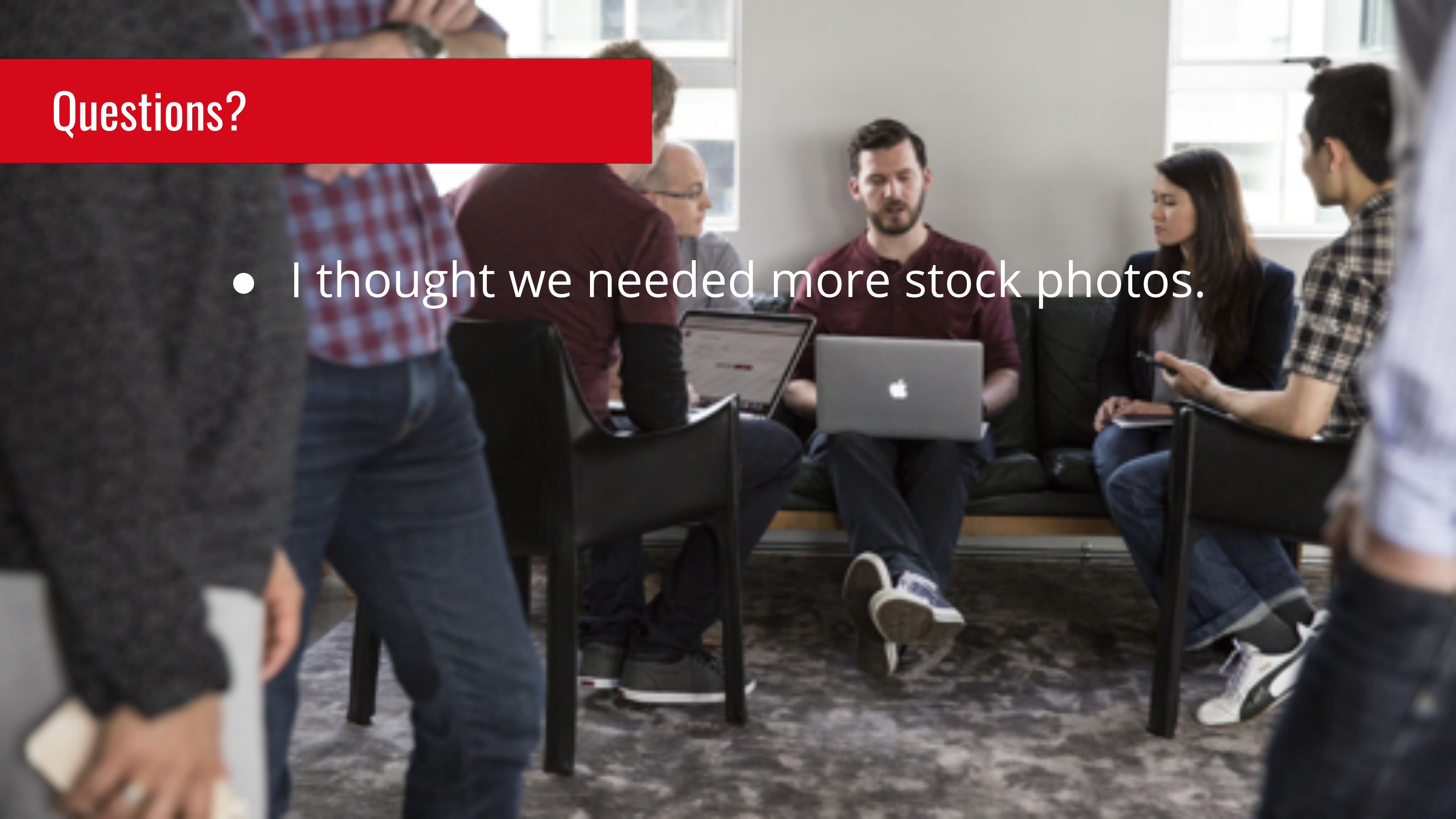
Would you know if it happened to you?

SQLi

Modern ORMs will mostly protect you from this

When you need to run direct SQL queries, parameterize

Questions?



- I thought we needed more stock photos.