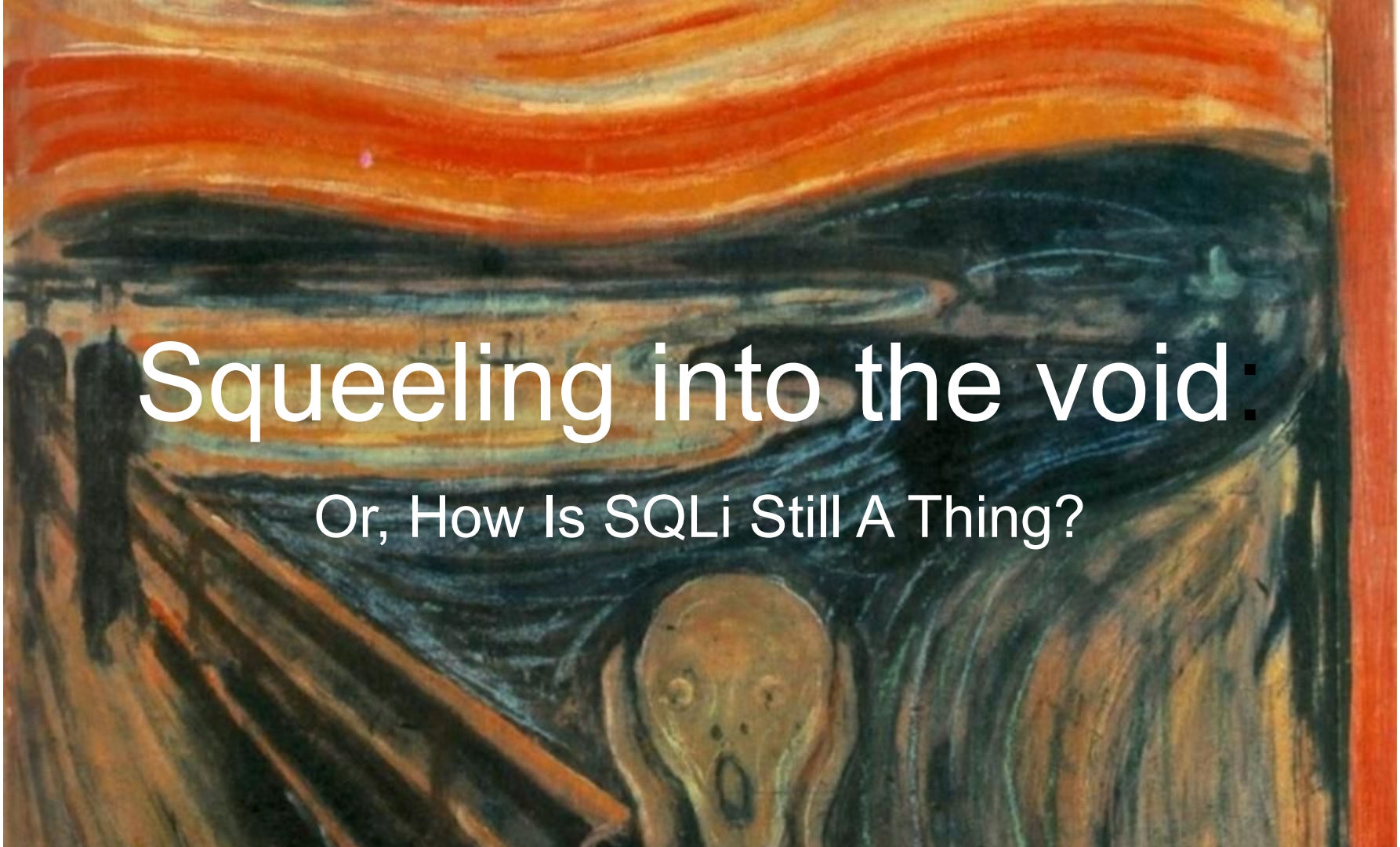

Squeeling into the void:
Or, How Is SQLi Still A Thing?

About me:

Done a bunch of things (I’m old)

RNZ

TE IRI DA

timely

homes.co.nz

Background:

- Used to foolishly tour bands (around 80 of them, 2006-2013).
- Used to be a software developer
- Got tired of the product grind
- Breaking internet things is so much more fun than making them

New to security, but I feel like I've been in tech a thousand years

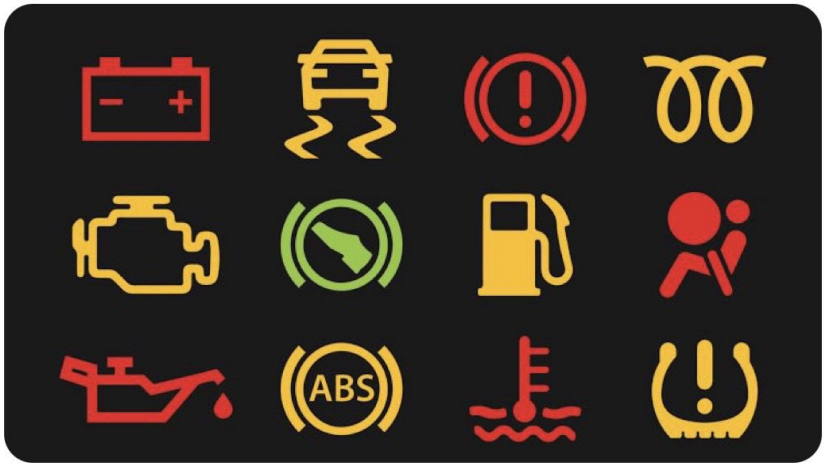
- When I started I was told 'You can look for SQLi, but you probably won't find it'
- I've found it on three in ten jobs.
- This is 2021! The year immediately following 2019, how are we still here and finding squeely?

Squeely: is it still a thing?

- What is it?
- What can it do?
- How it happens?
- What does it look like?
- How do we stop it from happening?

Every tutorial will have you believe that hacking is like this:

the server when I put in one quotey boi



But mostly let’s be real:

me when the server fails to yield to my quotey boi

How have I found it?

- Source code review
- Looking for the oldest bits of the website or endpoints that behave differently from the others.

What is it?

- Client controlled data being passed without sanitisation to SQL queries.
- Generally it looks like this +

What can it do?

- Short answer: it depends
- Mid range answer: Privilege escalation, data retrieval or tampering, denial of service by dropping tables
- The sometimes answer: total compromise

How have I found it (cont)

- Anything to do with reporting, or a high level of...dynamacism? Is that the word?
- If it’s black box testing, running SQL map on EVERYTHING. Honestly. It doesn’t take long.

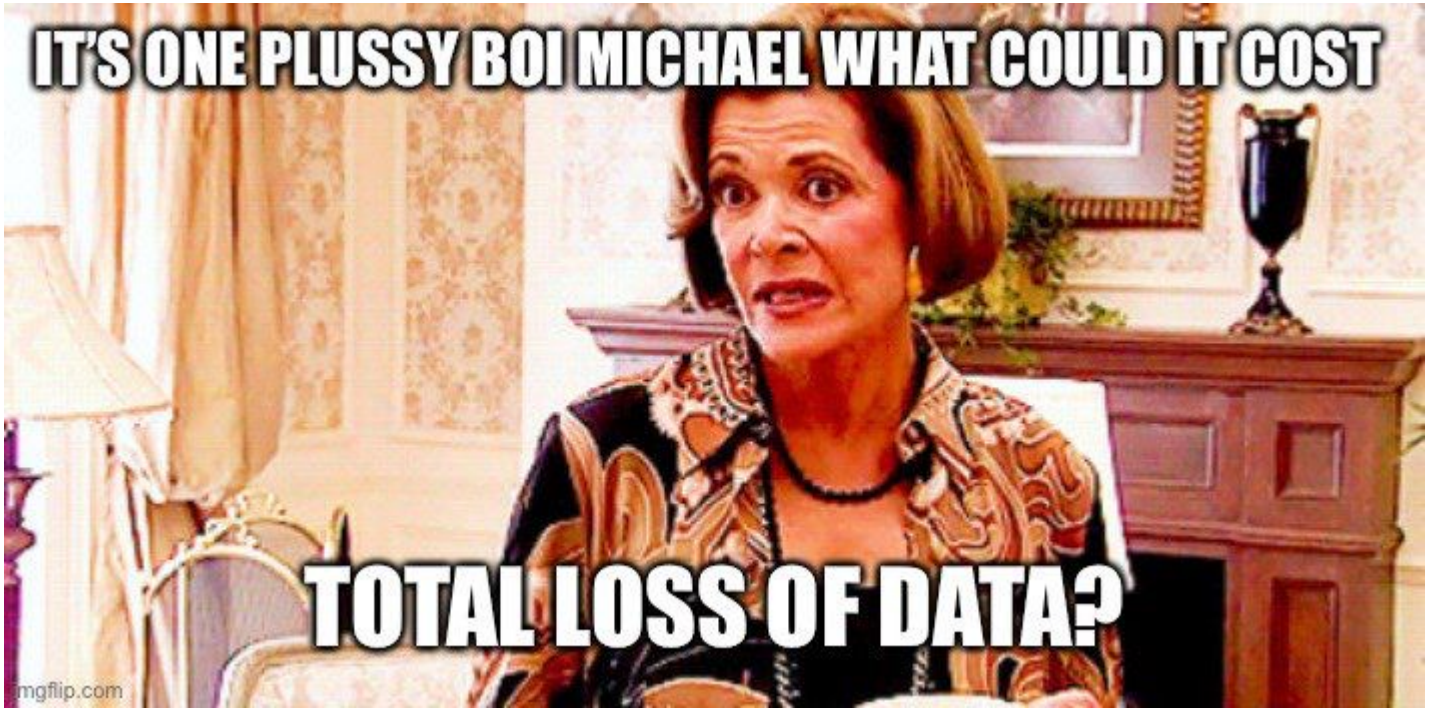
Some heuristics that might help:

- Server info disclosed in headers - educated guess
- Stack traces are your friend.
- XHR requests on the fly that validate things

SQL map:

- Proxy it through burp.
- It can throw up a lot of false positives, running through burp can help you figure out why.

Meme break:


IT'S ONE PLUSSY BOI MICHAEL WHAT COULD IT COST
TOTAL LOSS OF DATA?
imgflip.com

How does it happen? The security consultant view:

- This app is garbage! What a pack of dummies!
- This code is a trash fire!!!
- Your code is dumb and you should feel dumb!
- I haz all ur data now ha ha ha

How does it happen?

- Don’t do this. Aurynn Shaw has talked a lot more eloquently about this.
- We’re here to make things more secure not talk shit about things that people have spent a lot of time working on.

How does it happen? The software developer view

Um we have 17 different ways of accessing the database in this 500k line code base and marketing have promised a custom integration to win over a big client and the senior developer she’s away at the moment and my product manager really wanted me to do this so I raised a jira ticket to come back and address the technical debt that I put into production and it’s just one little plus and a client controlled parameter how bad can it be

meme break

Mmm code.

```
public void CreateDocument(CreateDocument document, Guid user)
    {
        var documentId = Guid.NewGuid();
        var date = DateTime.Now;

        using (var db = _databaseComponent.GetOpenConnection())
        {
            var sql =
                @"INSERT INTO tbl_businessdocuments (businessdocumentID, businessTransactionID, documentTypeID, CompletedByContactID, AssessedByContactID,
                        (@documentId, @transactionId, @type, @user, @user, @date, @sessionId) ";

            {highlight:yellow}foreach{/highlight} (var field in document.Fields)
            {
                sql += $@"INSERT INTO tbl_businessdocumentPropertyData (SessiondocumentID, documentPropertyId, documentPropertyValue)
                          SELECT @documentId, documentPropertyID, '{field.Value}{' FROM tbl_documentPropertyFields WHERE FieldName = '{field.Key}'";
            }

            db.Execute(sql, new { documentId, transactionId = document.TransactionId, type = document.Type, user, sessionId = document.SessionId, date });
        }

    }
```

Mmmm code part 2 - time based blind.

```
public List<ImportantBusinessStuff> getBusinessDetailsOverTime(Long businessID,
    Date startDate,
    Date endDate,
    String shortName) {
    DateFormat df = new SimpleDateFormat("yyyy-MM-dd HH:mm:ss");
    endDate = Utils.getEndDay(endDate);
    Query q = entityManager.createNativeQuery(
        "SELECT   businessID, unitID, effectiveArea,shortname, averageUnits as 'averageValue',
            + businessID + ", '" + df.format(startDate) + "','" + df.format(endDate) + "','"
            + shortName + "')",
        ImportantStuff.class);
    return (List<ImportantBusinessStuff>) q.getResultList();
}
```

How do we stop it from happening?

- Parametised queries
- Sanitise everything
- Use an ORM
- Lock down your databases.
- Don’t do this:

```
[13:17:16] [INFO] testing if current user is DBA
database management system users privileges:
[*] sa (administrator)
```

help jim get his first shell

$1,215 raised of $25,000 goal

6 donors **42** shares **6** followers

Share

Donate now

ss23
$100 · 6 d

See all

jim is organising this on behalf of jim

SHELL SHELL SHELL SHELL (SHELLING INTENSIFIES)

Without whom:

- Thanks to my ZX colleagues for putting up with me pestering them about all this blummun database stuff, looking at u ss23
- Thanks to all the clients for letting me steal their data
- Thank you everyone for coming!