Web Security and the OWASP Top 10: The Big Picture

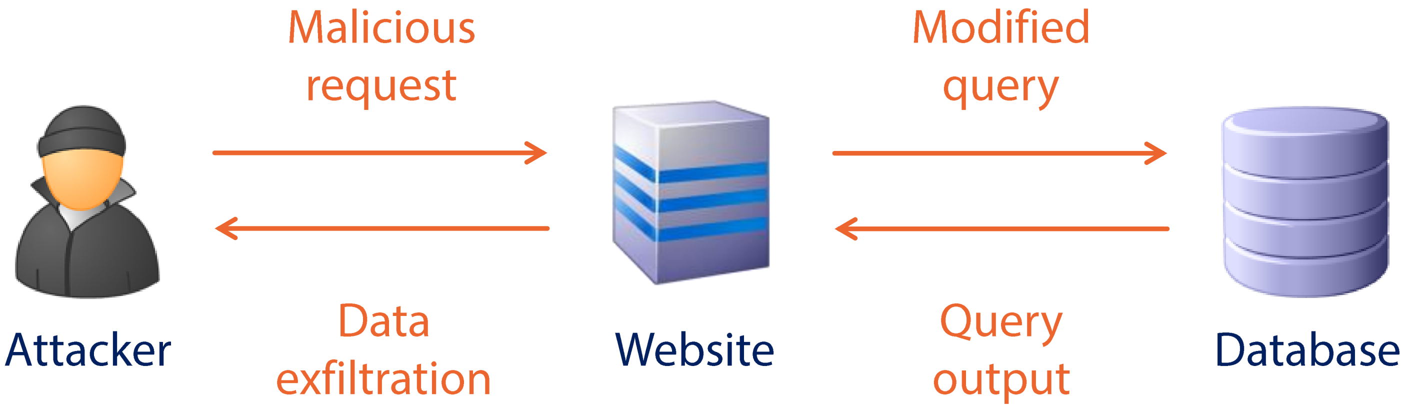
Injection

Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Injection Overview

Attack Vectors	Security Weaknesses		Technical Impacts
Exploitability Easy	Prevalence Common	Detectability Average	Impact Severe



Malicious request

Modified query

Attacker

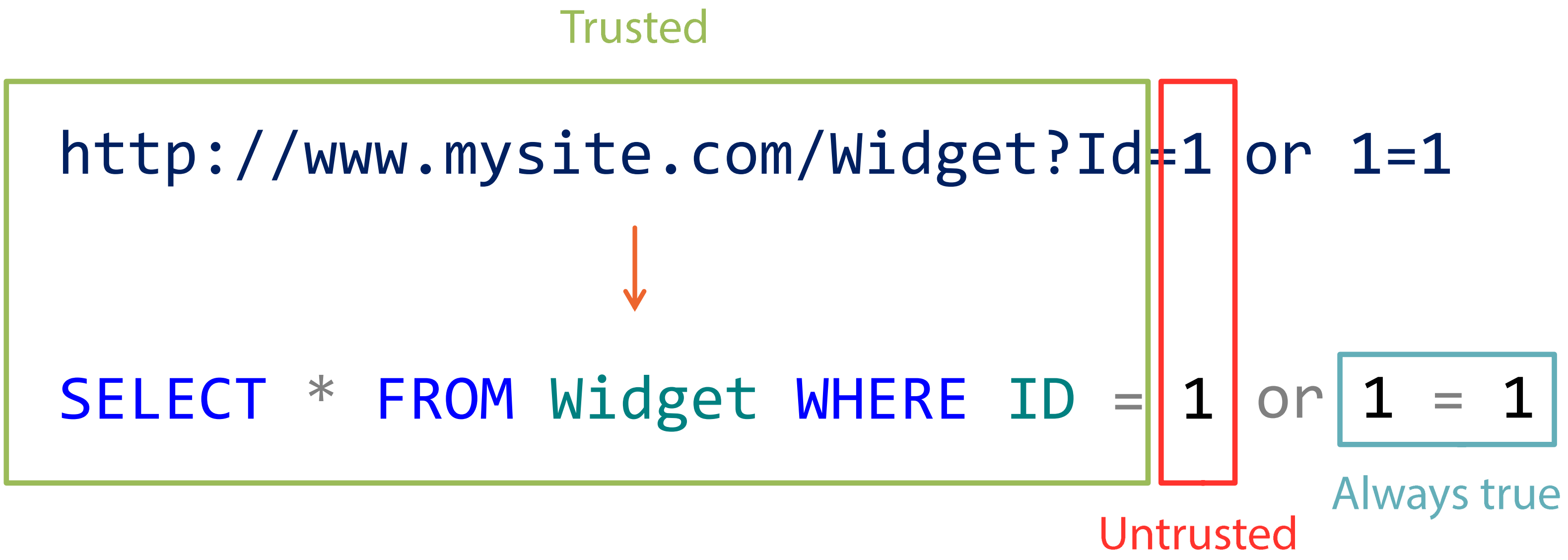
Data exfiltration

Website

Query output

Database

Understanding SQL Injection



Trusted

```
http://www.mysite.com/Widget?Id=1 or 1=1

SELECT * FROM Widget WHERE ID = 1 or 1 = 1
```

Untrusted

Always true

Common Defences Against Injection Attacks

Whitelist
untrusted data

- What input do we *trust?*
- Does it adhere to expected patterns?

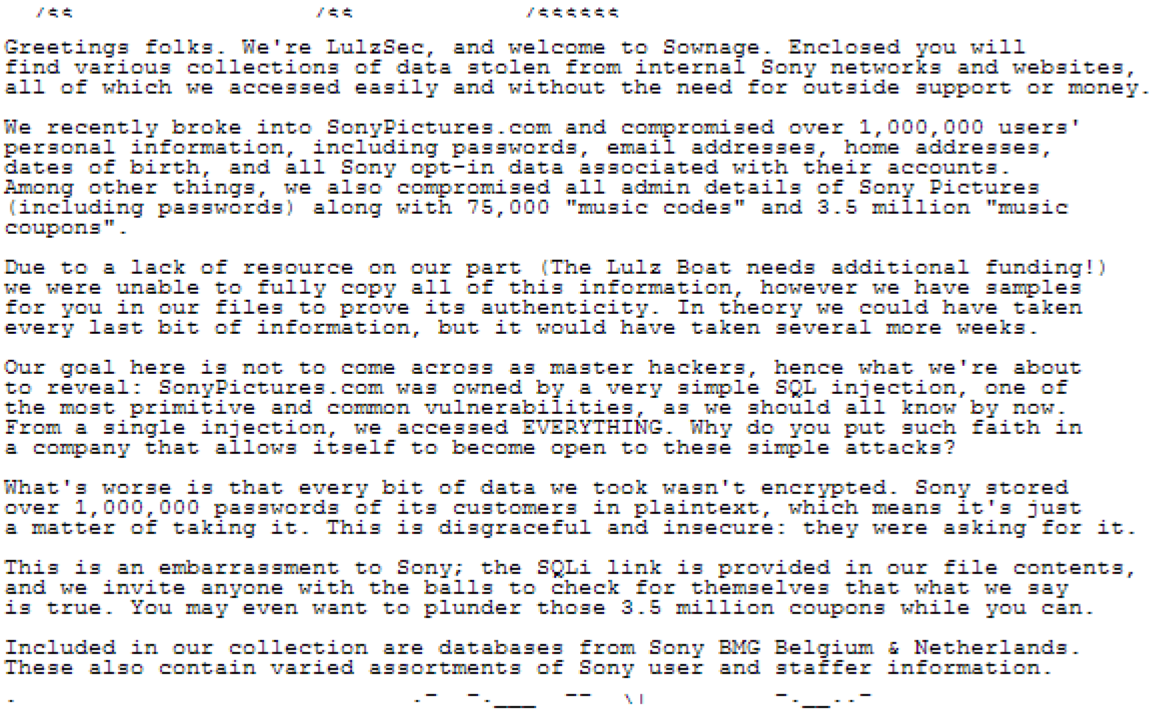
Parameterise
SQL statements

- Separate the query from the input data
- Type cast each parameter

Fine tune DB
permissions

- Segment accounts for admin and public
- Apply the "principle of least privilege"

Injection in the Wild – Sony Hack



```
  /$$                   /$$             /$$$$$$
```

Greetings folks. We're LulzSec, and welcome to Sownage. Enclosed you will find various collections of data stolen from internal Sony networks and websites, all of which we accessed easily and without the need for outside support or money.

We recently broke into SonyPictures.com and compromised over 1,000,000 users' personal information, including passwords, email addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts. Among other things, we also compromised all admin details of Sony Pictures (including passwords) along with 75,000 "music codes" and 3.5 million "music coupons".

Due to a lack of resource on our part (The Lulz Boat needs additional funding!) we were unable to fully copy all of this information, however we have samples for you in our files to prove its authenticity. In theory we could have taken every last bit of information, but it would have taken several more weeks.

Our goal here is not to come across as master hackers, hence what we're about to reveal: SonyPictures.com was owned by a very simple SQL injection, one of the most primitive and common vulnerabilities, as we should all know by now. From a single injection, we accessed EVERYTHING. Why do you put such faith in a company that allows itself to become open to these simple attacks?

What's worse is that every bit of data we took wasn't encrypted. Sony stored over 1,000,000 passwords of its customers in plaintext, which means it's just a matter of taking it. This is disgraceful and insecure: they were asking for it.

This is an embarrassment to Sony; the SQLi link is provided in our file contents, and we invite anyone with the balls to check for themselves that what we say is true. You may even want to plunder those 3.5 million coupons while you can.

Included in our collection are databases from Sony BMG Belgium & Netherlands. These also contain varied assortments of Sony user and staffer information.

```
.                            .-  -.___  --  \|          -.__..-
```