SQL Injection

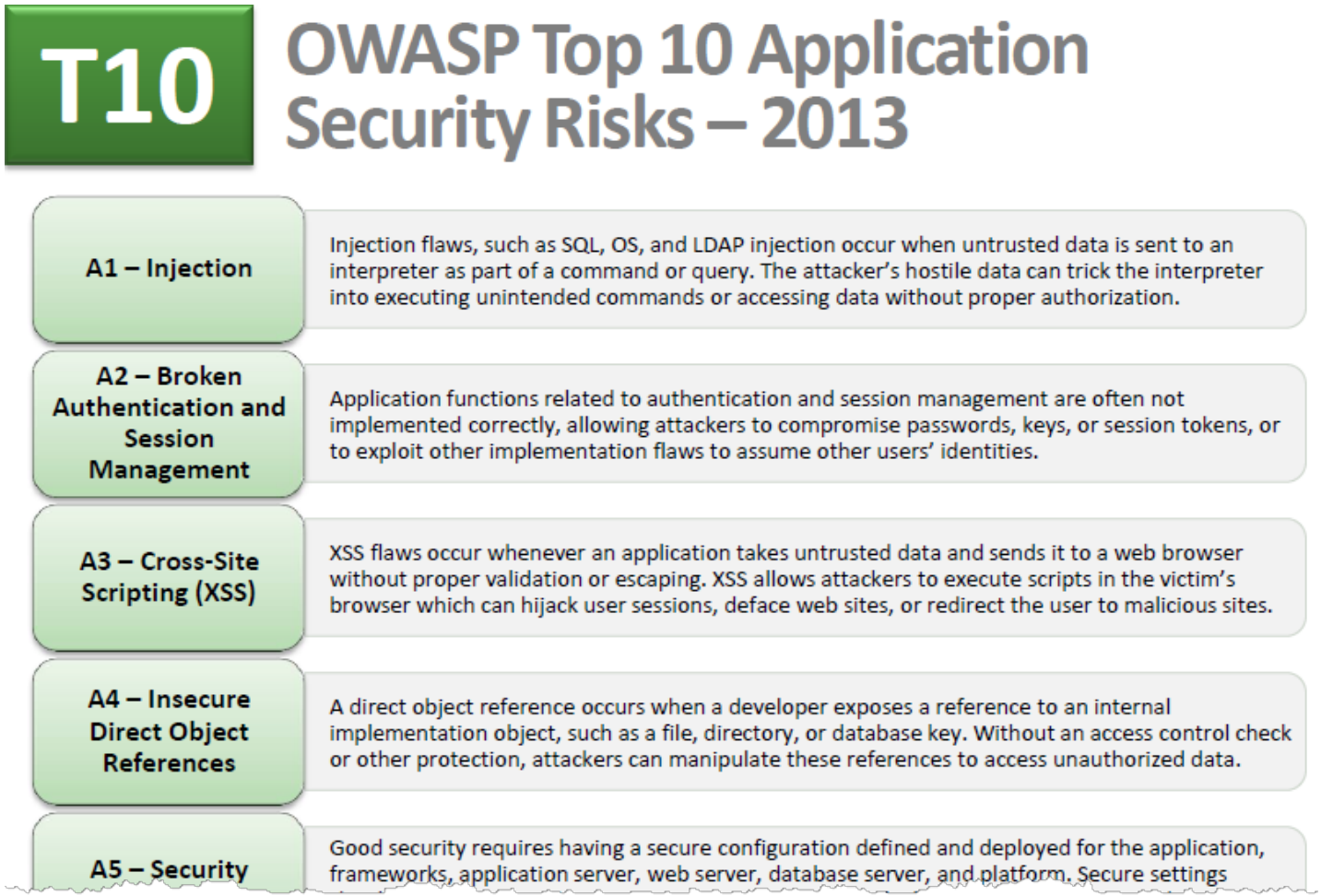
Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Outline

- Understanding SQL injection
- Testing for injection risks
- Discovering database structure via injection
- Harvesting data via injection
- Automating attacks with Havij
- Blind SQL injection
- Secure app patterns

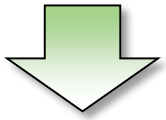
The significance of SQL injection



Understanding SQL injection

Trusted

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

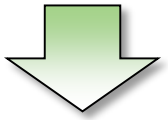


```
SELECT * FROM Widget WHERE ID = 1
```

Untrusted

Breaking out of the data context

```
/Widget?Id=1 or 1=1
```



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

Types of SQL injection attack

- **Explicit**
  - Union-based: append a result set that's rendered to the markup
  - Error-based: disclose information in an unhandled exception
- **Implicit (blind)**
  - Boolean-based: test if a particular condition is true
  - Time-based: cause the response to be delayed in response to a test

Summary

- **SQL injection risks exploit the ability to break out of the data context and enter the query context**
  - Remember untrusted data – here it is again!
- **Once a risk is established, a creative attacker may exploit it to discover the internal database structure and then extract data**
  - Table names
  - Column names
- **It could go even further than that – the account the web app is using may be able to drop or create objects in the database**
- **SQL injection is a repeatable pattern that's frequently automated with tools like Havij**
- **Even with no *explicit* feedback, "blind" injection can still be leveraged**
- **Always check for parameterisation and whitelisting of untrusted data**