116: SQL Injection

⓪ Lindsay Verola, MSFT

① Ubuntu VM to download; use for a2

② Last class: XSS; how to steal cookies from an XSS-vulnerable site

③ SQL basics at SQL Zoo (www.sqlzoo.net)

④ SQL injection

The idea: twist SQL queries via input data

⇓

Access or modify data you should not have access to

Where: web app w/ database

The culprit: the ' (single quote)

⑤ Prevention:
- Filter out special chars
- Limit data and privileges that a database user has access to ⇒ least privilege
- Use prepared statements. They bind variables using "?" as placeholder

⑥ Exercise: http://67.23.79.113
↓
Find FLAG: