SQLi, XSS, CSRF: niektóre z podatności występujących w aplikacjach webowych

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie
AGH University of Science and Technology

Dominik Czarnota, Magdalena Jaroszyńska

23.05.2016

SQLi – SQL Injection

- Brak odpowiedniego sprawdzenia (walidacji) parametru przekazanego przez użytkownika, który jest przekazywany bezpośrednio do zapytania SQL
- Przykład:

```
query = "SELECT col FROM table WHERE param='"
      + param + "'";
connection.execute(query);
```

SQLi – wykorzystanie

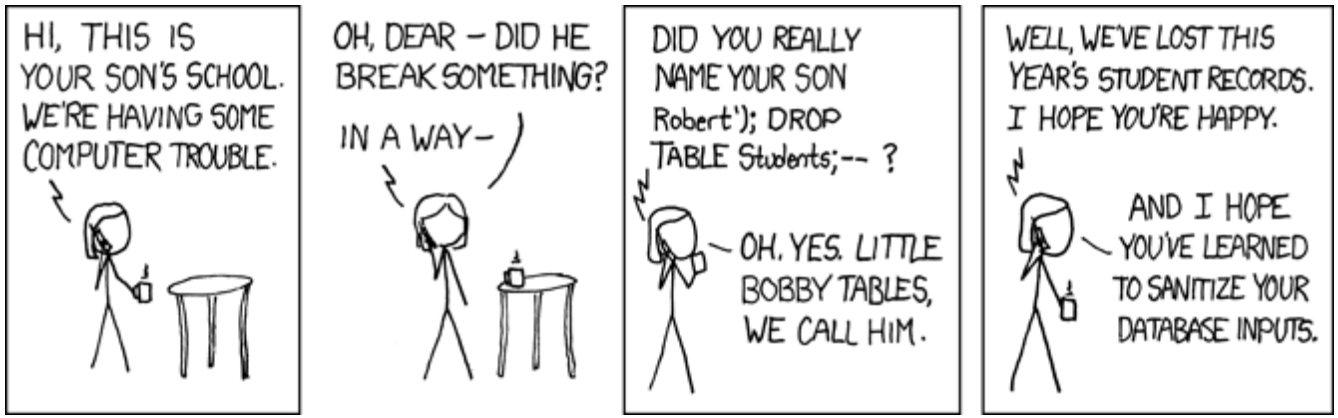
[sqlmap: automatic SQL injection and database takeover tool]

» Przykład – aplikacja napisana w Pythonie.

SQLi – metody

```
query = "SELECT col FROM table WHERE param='" + param + "'";
```

- Stacked queries: `'; SELECT col2 FROM table2 WHERE 'a' = 'a`
- UNION query-based: `' UNION SELECT col2 FROM table2 WHERE 'a' = 'a`
- Boolean-based blind: `SELECT 1 FROM table …`
- Time-based blind
- Error-based



Źródło: https://github.com/sqlmapproject/sqlmap/wiki/Techniques

SQLi – zapobieganie

- Primary Defenses:
  - Use of Prepared Statements (Parameterized Queries)
  - Use of Stored Procedures
  - Escaping all User Supplied Input

Używanie ORMów*

- Additional Defenses:
  - Also Enforce: Least Privilege
  - Also Perform: White List Input Validation

Źródło:
https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

XSS – Cross Site Scripting

- Atak na klienta korzystającego z podatnej webaplikacji
- Wstrzyknięcie do przeglądarki ofiary fragmentu kodu, który może być uruchomiony w przeglądarce (Javascript, VBScript)
- Rodzaje:
  - **Persistent/stored** – umieszczenie na serwerze kodu, który jest wyświetlany użytkownikowi

    <Przykład w Pythonie>
  - **Reflected** – kod Javascript zaszyty w linku

    ```
    /image?src=cat.img"><script>alert("XSS")</script>
    ```
  - **DOM Based**

XSS – zapobieganie

- Enkodowanie encji html:
  - & ⟶ &
  - < ⟶ <
  - > ⟶ >
  - " ⟶ "
  - ' ⟶ '
  - / ⟶ /
- Escape'owanie danych, które pochodzą od użytkownika i są przekazywane do Javascripta

CSRF – Cross Site Request Forgery

- Atak polegający na zmuszeniu przeglądarki ofiary do wykonania pewnej nieautoryzowanej akcji (wysłania żądania HTTP)
- Zapobieganie:
  - Sprawdzanie nagłówków HTTP – czy żądanie pochodzi z tej samej strony (nagłówków Origin/Referer)
  - CSRF token – dodanie ukrytego pola do renderowanego formularza, zawierającego losowy token, którego poprawność sprawdzimy po stronie serwera

Dziękujemy za uwagę