TỔNG QUAN VỀ OWASP TOP 10- 2013

Trình bày: Khổng Văn Cường

Email: cuongkv@fpt.com.vn

Đơn vị tổ chức:

Đơn vị tài trợ:

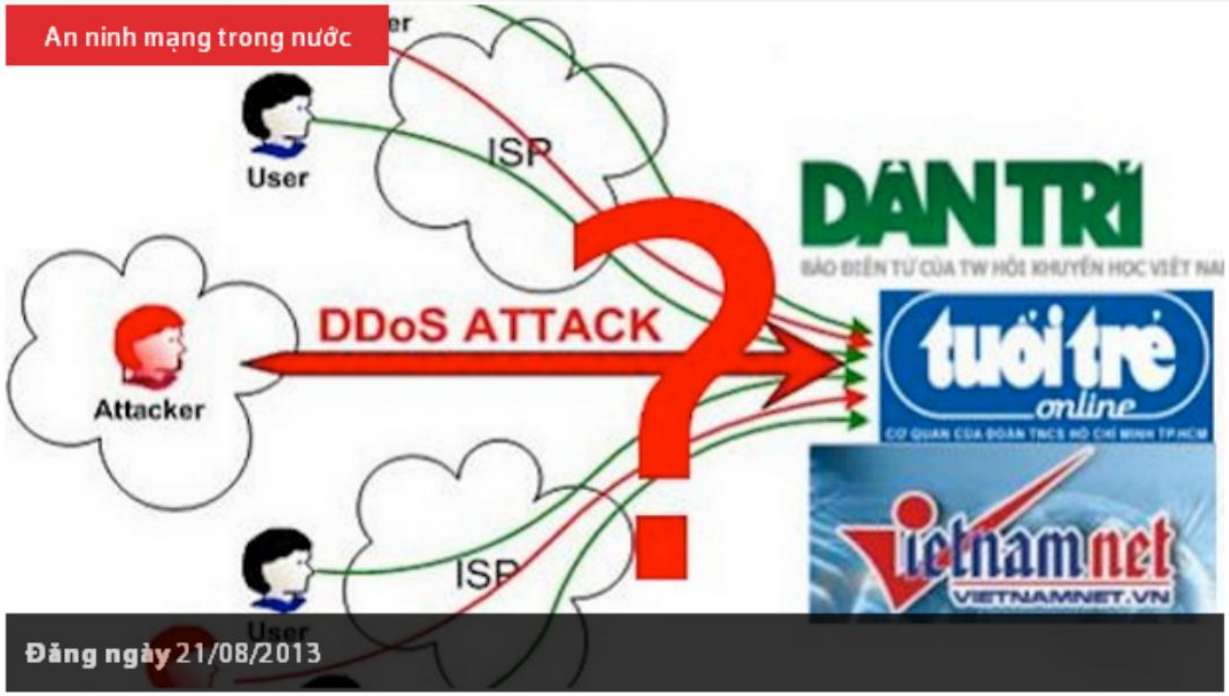
Nội dung

- Hiện trạng
- Giải pháp
- Giới thiệu tổng quan về PENTEST và chuẩn OWASP TOP 10 phiên bản 2013.
- Các nhóm lỗi trong OWASP TOP 10 phiên bản 2013.
- Case Study : File Upload

Hiện trạng


owasp1.pez
File Edit Language Account Help
An ninh mạng trong nước
Tấn công từ chối dịch vụ - Botnet
Máy chủ điều khiển
(C&C Server)
Website bị tấn công
Hacker
Đăng ngày 24/08/2013
Prezi
VietNamNet thiệt hại 1 tỷ đồng/tuần trong vụ tấn công DDoS
9:52 AM
10/21/2013

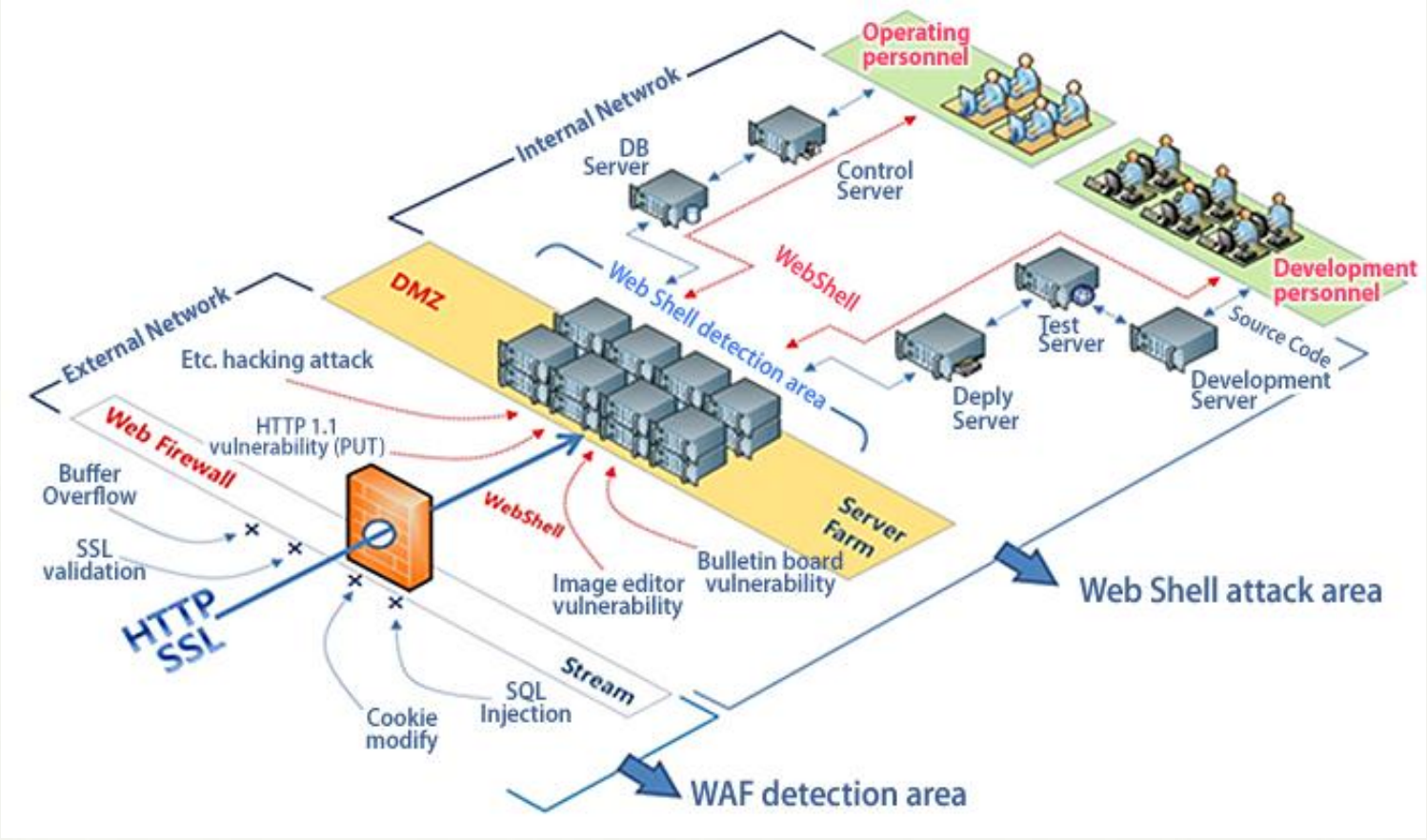
Hiện trạng



Tin tặc tấn công hàng trăm trang web Việt trong 30 ngày qua

Công ty an ninh mạng Bkav ngày 20/08 cho biết, trong 30 ngày qua có 437 trang web của các cơ quan, doanh nghiệp tại Việt Nam bị tin tặc xâm nhập; trong đó có 16 trường hợp gây ra bởi tin tặc

BẠN THẬT SỰ ĐÃ ĐƯỢC BẢO VỆ?

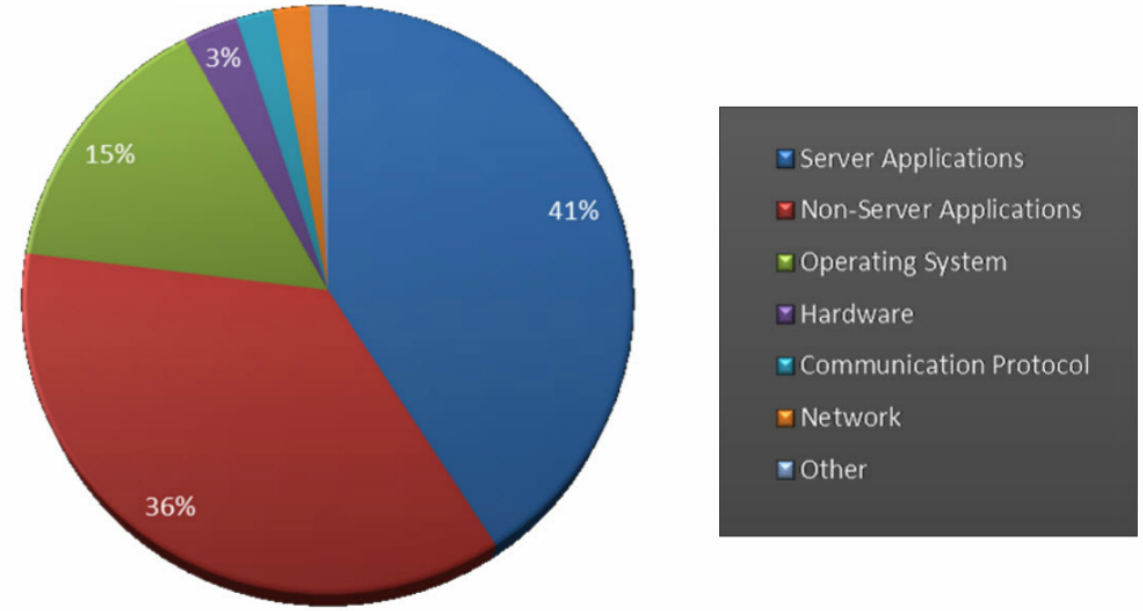


BẠN THẬT SỰ ĐÃ ĐƯỢC BẢO VỆ?

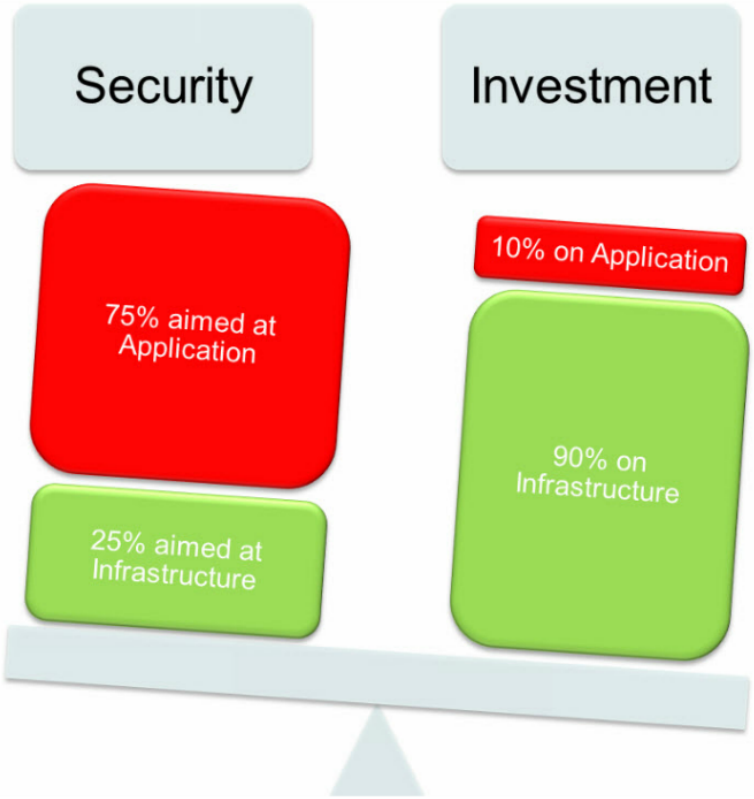
Network Firewall
Web Application Firewall
IDS/IPS/HIDS
Antivirus

BẠN THẬT SỰ ĐÃ ĐƯỢC BẢO VỆ?

92% lỗ hổng bảo mật nằm trong lớp ứng dụng - không nằm tại hạ tầng mạng



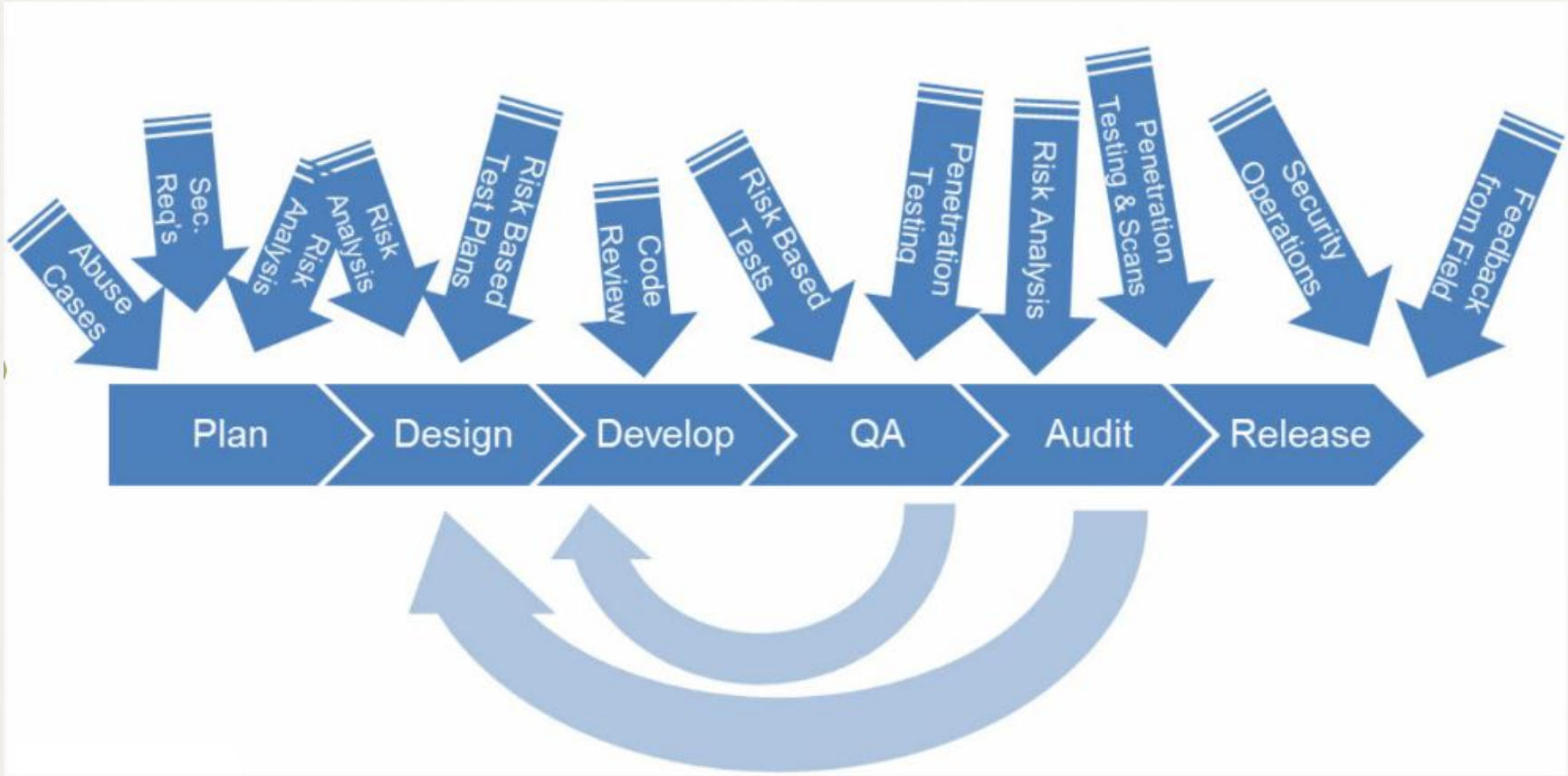
BẠN THẬT SỰ ĐÃ ĐƯỢC BẢO VỆ?



90% ngân sách đầu tư vào cơ sở hạ tầng

75% các cuộc tấn công tập trung vào lớp ứng dụng

SOLUTION?


Abuse Cases
Sec. Req's
Risk Analysis
Risk Analysis
Risk Based Test Plans
Code Review
Risk Based Tests
Penetration Testing
Risk Analysis
Penetration Testing & Scans
Security Operations
Feedback from Field
Plan
Design
Develop
QA
Audit
Release

Tổng Quan Về PENTEST

- Pentest là gì ?
- Các phương pháp sử dụng trong pentest:
  - Hộp đen (Black box)
  - Hộp trắng (White box)
  - Hộp xám (Gray box)

Tổng Quan Về PENTEST

- Phạm vi trong Pentest ?
  - Network Penetration Test
  - Web Application Penetration Test
  - Wireless Network Penetration Test
  - Physical Penetration Test
-

Tổng Quan Về PENTEST

- Tiêu chuẩn để thực hiện Pentest là gì?
  - Đánh giá ứng dụng Web – OWASP (Open-source Web Application Security Project)

Tổng Quan Về PENTEST

- Tiêu chuẩn để thực hiện Pentest là gì?
  - Đánh giá ứng dụng Web – OWASP (Open-source Web Application Security Project)
  - Đánh giá mạng và hệ thống – OSSTMM (Open Source Security Testing Methodology Manual)

OWASP là gì?

Ở OWASP bạn sẽ được cung cấp miễn phí và mở :

- Các công cụ và các tiêu chuẩn về an toàn thông tin
- Tài liệu về kiểm tra bảo mật ứng dụng, lập trình an toàn và kiểm định mã nguồn
- Thư viện và các tiêu chuẩn điều khiển an ninh thông tin
- Các chi nhánh của hội ở khắp thế giới
- Các nghiên cứu mới nhất
- Các buổi hội thảo toàn cầu
- Maillist chung

OWASP TOP 10 phiên bản 2013

OWASP Top 10 – 2010 (old)	OWASP Top 10 – 2013 (New)
2010-A1 – Injection	2013-A1 – Injection
2010-A2 – Cross Site Scripting (XSS)	2013-A2 – Broken Authentication and Session Management
2010-A3 – Broken Authentication and Session Management	2013-A3 – Cross Site Scripting (XSS)
2010-A4 – Insecure Direct Object References	2013-A4 – Insecure Direct Object References
2010-A5 – Cross Site Request Forgery (CSRF)	2013-A5 – Security Misconfiguration
2010-A6 – Security Misconfiguration	2013-A6 – Sensitive Data Exposure
2010-A7 – Insecure Cryptographic Storage	2013-A7 – Missing Function Level Access Control
2010-A8 – Failure to Restrict URL Access	2013-A8 – Cross-Site Request Forgery (CSRF)
2010-A9 – Insufficient Transport Layer Protection	2013-A9 – Using Known Vulnerable Components (NEW)
2010-A10 – Unvalidated Redirects and Forwards (NEW)	2013-A10 – Unvalidated Redirects and Forwards
3 Primary Changes:	▪ Merged: 2010-A7 and 2010-A9 -> 2013-A6
▪ Added New 2013-A9: Using Known Vulnerable Components	▪ 2010-A8 broadened to 2013-A7

A1: Injection

- Nguyên nhân: Các truy vấn đầu vào tại ứng dụng bị chèn thêm dữ liệu không an toàn dẫn đến mã lệnh được gởi tới máy chủ cơ sở dữ liệu.

A1: Injection

- Nguyên nhân: Các truy vấn đầu vào tại ứng dụng bị chèn thêm dữ liệu không an toàn dẫn đến mã lệnh được gởi tới máy chủ cơ sở dữ liệu.

SQL Injection	Xpath Injection
NoSQL Injection	XML Injection
LDAP Injection	Command Injection

A1: Injection

- Nguy cơ:
  - Truy cập dữ liệu bất hợp pháp.
  - Insert/update dữ liệu vào DB.
  - Thực hiện một số tấn công từ chối dịch vụ (refref, benchmark …)

DEMO

Demo SQL Injection

A2: Broken Authentication and Session Management

- Điểm yếu: Cho phép hacker từ bên ngoài có thể truy cập vào những tài nguyên nội bộ trái phép (admin page, inside, control page …)

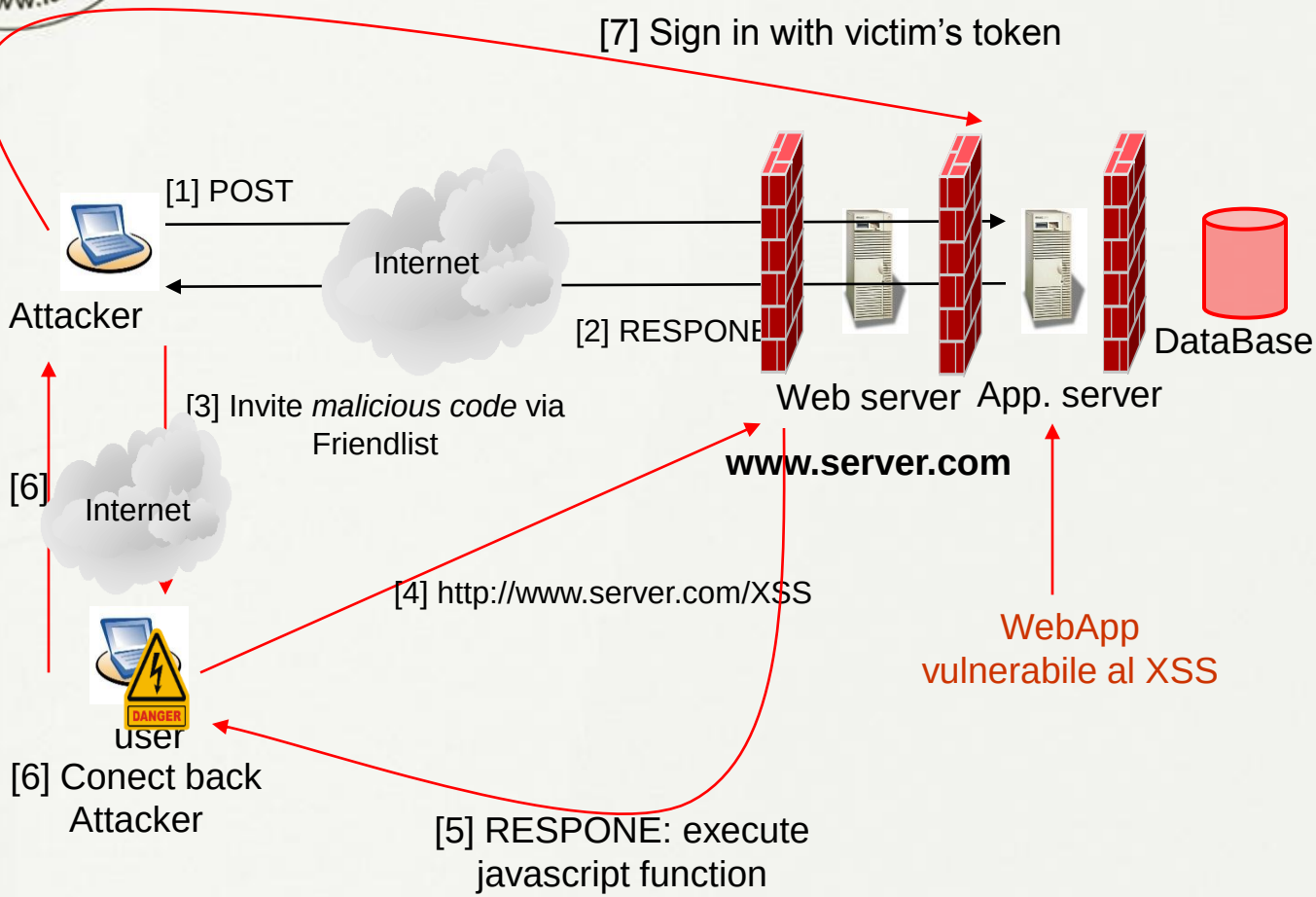
A2: Broken Authentication and Session Management

- Điểm yếu: Cho phép hacker từ bên ngoài có thể truy cập vào những tài nguyên nội bộ trái phép (admin page, inside, control page …)
- Ngoài ra hacker còn có thể thực hiện các hành vi nâng quyền quản trị hoặc tấn công dựa vào các dạng như session fixation …

A3: Cross-Site Scripting(XSS)

- Điểm yếu: Cho phép thực thi mã độc tại máy nạn nhân (client side)
- Nguy cơ:
  - Đánh cắp cookie/session
  - Phát tán mã độc

A3: Cross-Site Scripting(XSS)

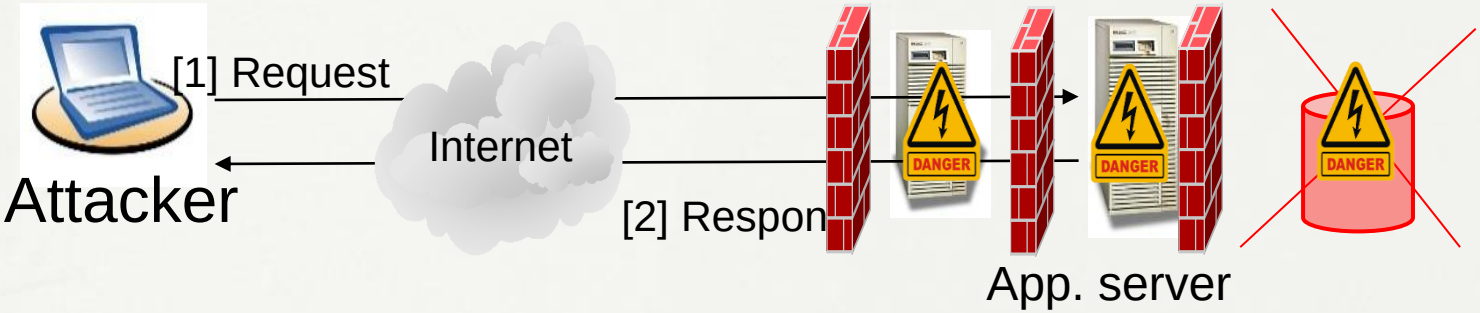


A4: Insecure Direct Object References

- Điểm yếu: Việc phân quyền yếu (weak authorization) cho phép người dùng có thể truy cập dữ liệu của người dùng khác. Trong những trường hợp hacker có thể xác định được chính xác cấu trúc truy vấn gởi đến server, hacker có thể nhanh chóng thu thập dữ liệu như Credit Card, mã khách hàng, thông tin cá nhân…

A4: Insecure Direct Object References

http://www.server.com/app/accountInfo?acct=notmyacct
http://www.server.com/app/download.php?file=../../../../etc/passwd



A5: Security Misconfiguration

- Việc thắt chặt các cấu hình bảo mật tại các tầng trong kiến trúc web là cần thiết: platform, OS, web server, database, framework... nhằm tránh những nguy cơ có thể bị khai thác vào ứng dụng.

A5: Security Misconfiguration

```
.228 www.[redacted].com GET /api/imx/1.0/report?_=1311023064402&itemId=179222&type=game
.240 www.[redacted].com GET /dynamo/video/configuration.jhtml?uri=mgid%3Acms%3Aitem%3An
.236 www.[redacted].com GET /sbcom/data/profile/[redacted]/shows_paginated.jhtml?callback=NIC
.232 www.[redacted].com GET /club/mall/clothing-boutique.html HTTP/1.1
.234 www.[redacted].com GET /games/data/brainsurge/[redacted]/assets/xml/confi
.233 www.[redacted].com GET /games/data/[redacted]/assets/characters/bra
.244 www.[redacted].com GET /common/login/check.jhtml?password=MOMMY&callback=[redacted].re
.236 www.[redacted].com GET /api/imx/1.0/put?callback=[redacted].request.lstnrs[\"apiimx10put1
.231 www.[redacted].com GET /movies HTTP/1.1
.242 www.[redacted].com GET /games/data/[redacted]/data/characters/sheen.x
.249 www.[redacted].com GET /sbcom/data/games/achievements-config.jhtml?game=[redacted]-
.234 www.[redacted].com GET /AdSettings/adSnippet.jhtml?site=[redacted]&uri=/movies HTTP
.248 www.[redacted].com POST /common/login/check.jhtml HTTP/1.1
.234 www.[redacted].com GET /games/data/[redacted]Wrappe
.231 www.[redacted].com GET /ajax/celebrity/?_=1311023063235&memberName_t=_Taylor_Gray_
.227 www.[redacted].com POST /common/login/check.jhtml HTTP/1.1
.237 www.[redacted].com GET /AdSettings/adSnippet.jhtml?site=site-parentsconnect&uri=/g
.247 www.[redacted].com GET /sbcom/data/profile/[redacted]/shows_paginated.jhtml?callback=NIC
```

A6: Sensitive Data Exposure

- Các dữ liệu nhạy cảm được lưu trữ không an toàn có thể gây ra những ảnh hưởng to lớn cho hệ thống máy chủ, cũng như cho khách hàng.

A6: Sensitive Data Exposure

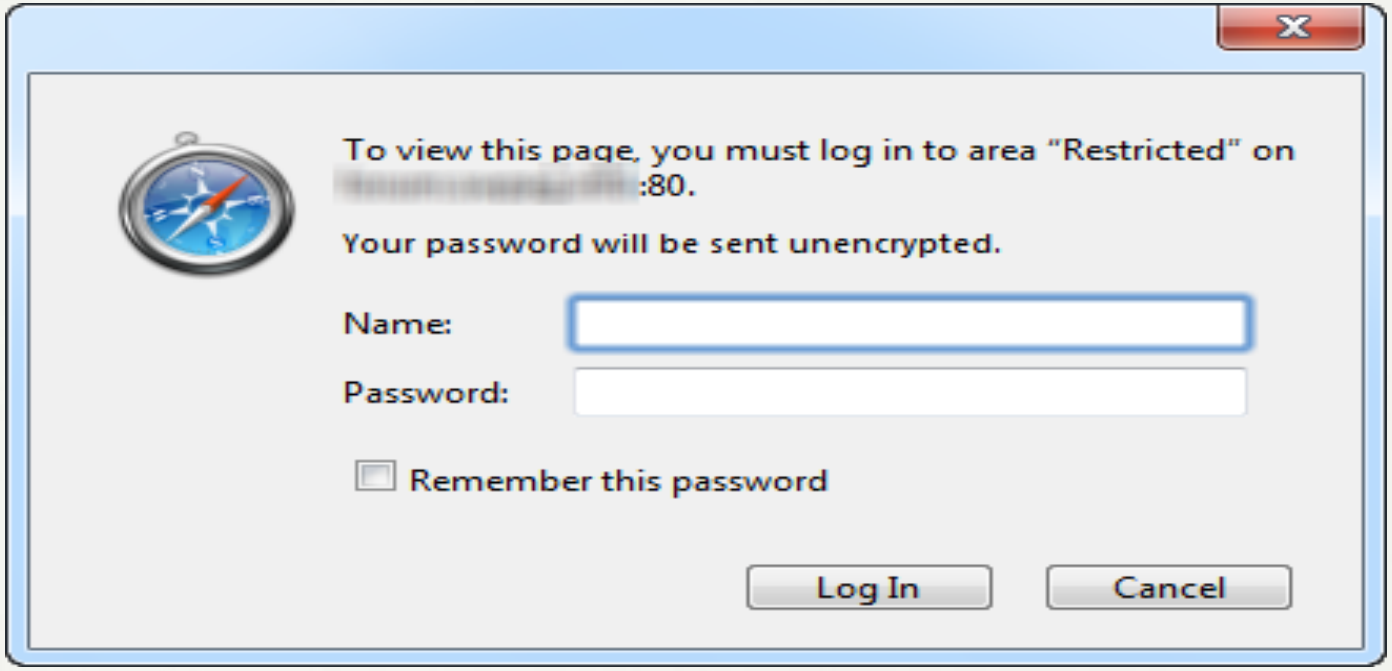
- Tình huống 1: Thẻ tín dụng/Tài khoản đăng nhập được lưu trữ cleartext.

A6: Sensitive Data Exposure

- Tình huống 1: Thẻ tín dụng/Tài khoản đăng nhập được lưu trữ cleartext.
- Tình huống 2: Kênh truyền HTTPS bị hacker nghe lén và dữ liệu được giải mã thông qua lỗ hổng CRIME

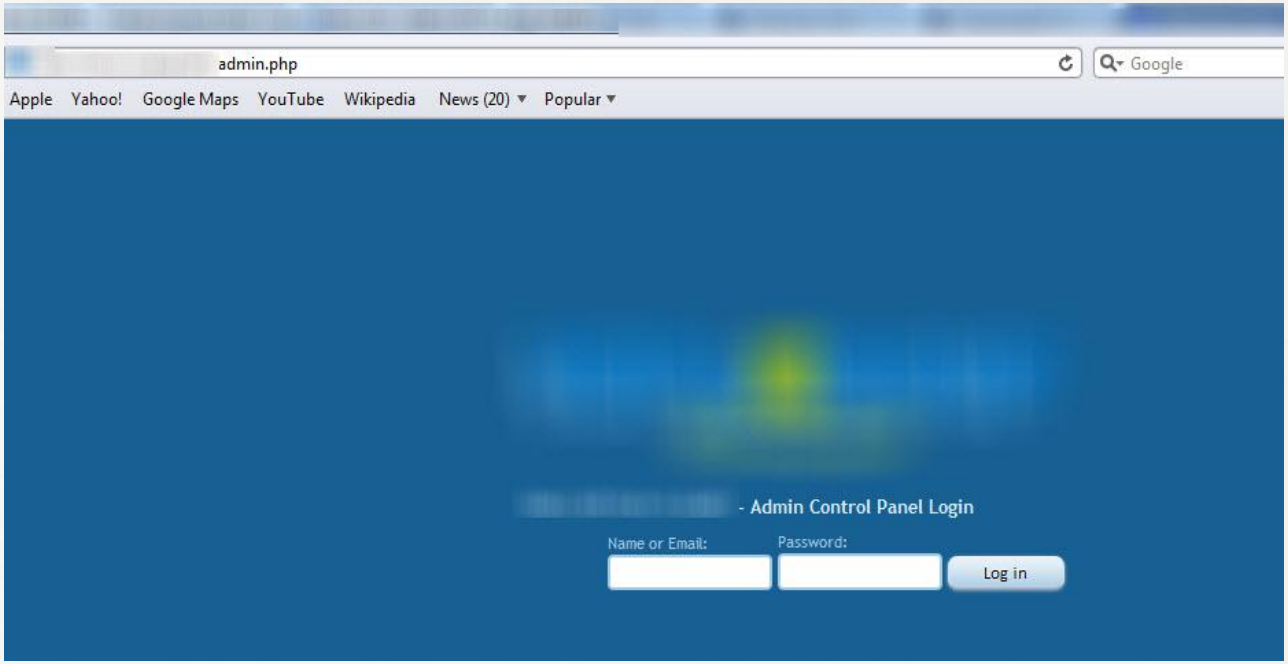
A7: Missing Function Level Access Control

http://admin.server.com/



A7: Missing Function Level Access Control

http://admin.server.com/admin.php

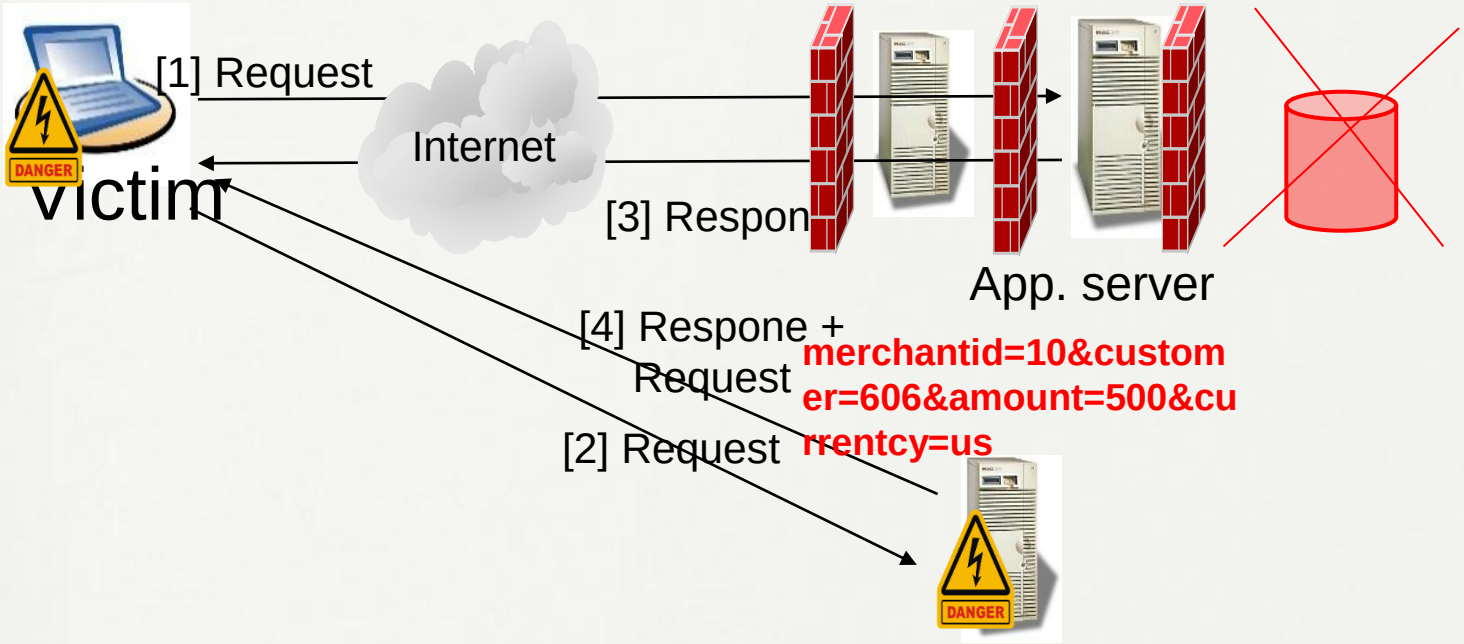


A8: Cross-Site Request Forgery

- Với những hệ thống thanh toán không kiểm tra tính hợp lệ của token/Session/Domain... thì nguy cơ người dùng bị mất tiền do bị lừa thực hiện các mã kịch bản không mong muốn từ các site lừa đảo.

A8: Cross-Site Request Forgery

http://www.server.com/app/checkout.php?
merchantid=10&customer=541&amount=500&currentcy=us



A9: Using Components with Known Vulnerabilities

- Điểm yếu: Việc sử dụng các lỗ hổng bảo mật trong các thư viện, plugin, module, ứng dụng... được công khai trong cộng đồng giúp hacker nhanh chóng khai thác các lỗ hổng bảo mật.

A9: Using Components with Known Vulnerabilities

A9: Using Components with Known Vulnerabilities

A9: Using Components with Known Vulnerabilities

A9: Using Components with Known Vulnerabilities

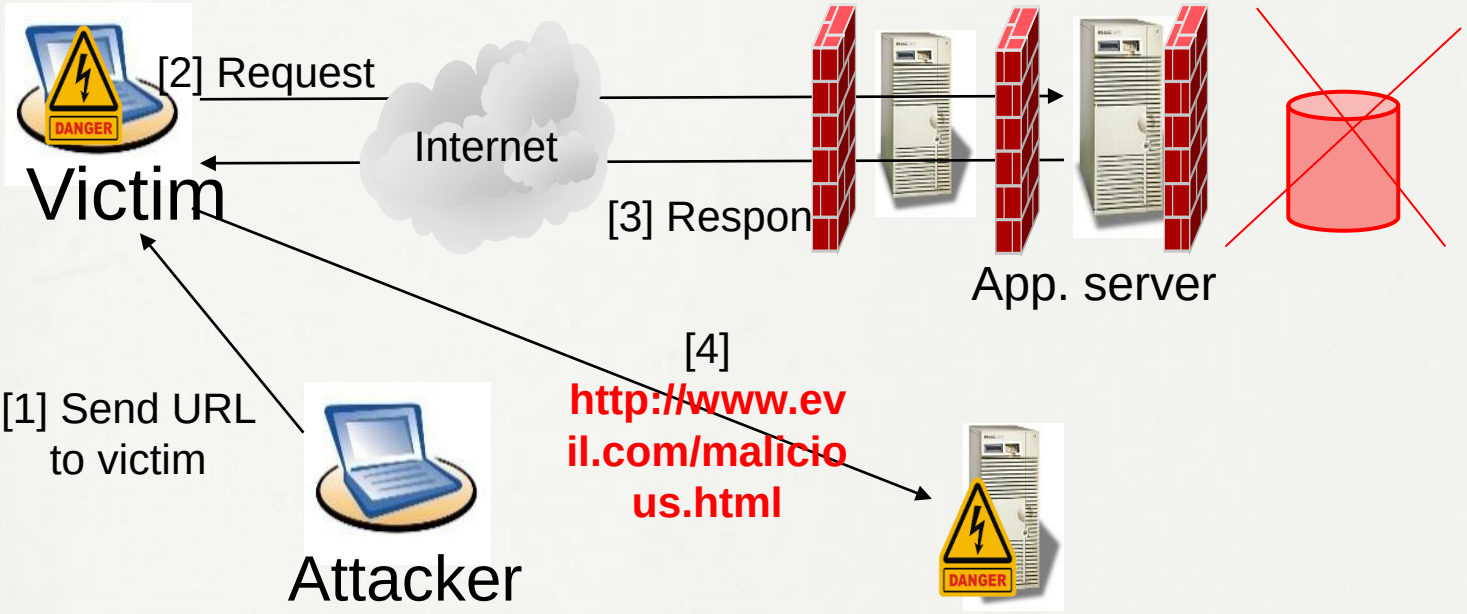
- Khuyến cáo: Các bản vá bảo mật từ nhà phát triển ứng dụng sẽ giúp ứng dụng giảm thiểu các rủi ro khai thác.

A10: Unvalidated Redirects and Forwards

- Việc chuyển hướng không an toàn người dùng đến một đường dẫn bên ngoài trang có thể tạo nguy cơ người dùng truy cập đến những trang chứa mã độc nhằm đánh cắp dữ liệu cá nhân.

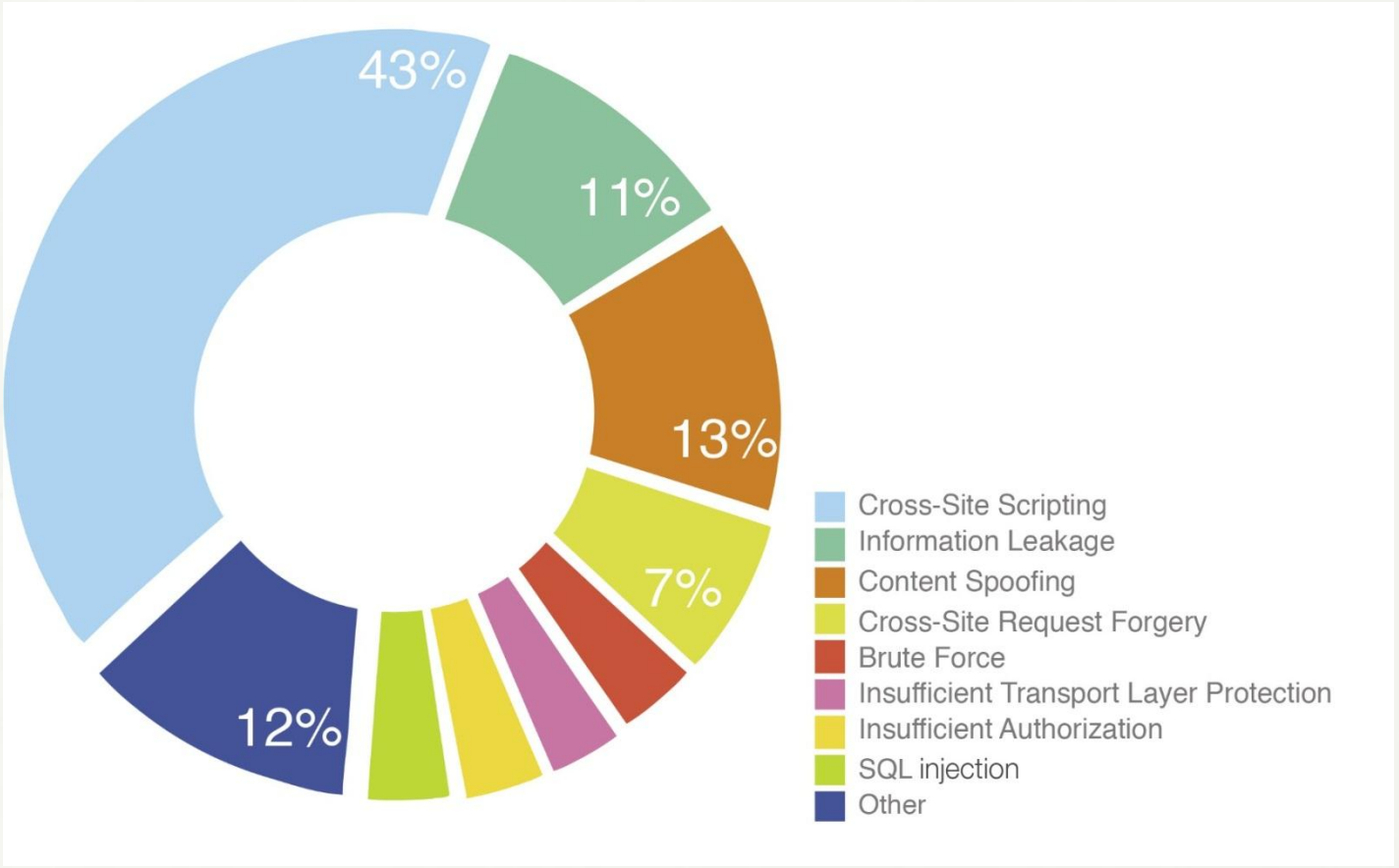
A10: Unvalidated Redirects and Forwards

http://www.server.com/app/redirect.php?url=http://www.evil.com/malicious.ht



Tổng Kết

Tổng kết


43%
11%
13%
7%
12%
Cross-Site Scripting
Information Leakage
Content Spoofing
Cross-Site Request Forgery
Brute Force
Insufficient Transport Layer Protection
Insufficient Authorization
SQL injection
Other

DEMO

Demo Business Logic Testing

Case Study : File Upload

- Protection bằng Content-Type

```
------------boundry123456
Content-Disposition: form-data; name="Filedata"; filename="test.txt"
Content-Type: application/octet-stream

test
```

- Có thể dễ dàng thay đổi “Content-Type”

1. Name and Extension

- File Extension in “test.php.jpg”?

  “.php.jpg”?

  “.jpg”

Bỏ qua Extensions

- Kiểm tra thực thi extensions:
- ".php" thường bị khóa, vậy ".php3", ".php4", ".phtml", thì như thế nào?
- Tương tự cho ".asp" thường bị khóa ➔ ".asa" or ".cer" thì sao?
- Còn client side extensions thì sao?

  .htm, .html, .swf, .jar, …?

2. Double Extensions

- Cấu hình trong Apache
  - "file.php.jpg" served chạy PHP
  - "AddHandler application/x-httpd-php .php"

```
<FilesMatch \.php$>
    SetHandler application/x-httpd-php
</FilesMatch>
```

- Cấu hình trong IIS 6 thì:
  - "file.asp;.jpg" → Chạy file ASP
  - "/folder.asp/file.txt" → Chạy file ASP

DEMO

Demo Remote Code Execution On Nginx Server

3. Case Sensitive Rules

- Ví dụ:
  - Blacklist RegEx: “^\.php$”
    - “file.php” != “file.PhP”
  - “file.php3.jpg” != “file.PHP3.JpG”

4. Windows 8.3

- Ghi đè các file nhạy cảm như:
  - "web.config" == "WEB~1.con"
  - "default.aspx" == "DEFAUL~1.asp"
- Trường hợp không extensions thì có cho phép?
  - ".htaccess" == "HTACCE~1"

5. Windows File System

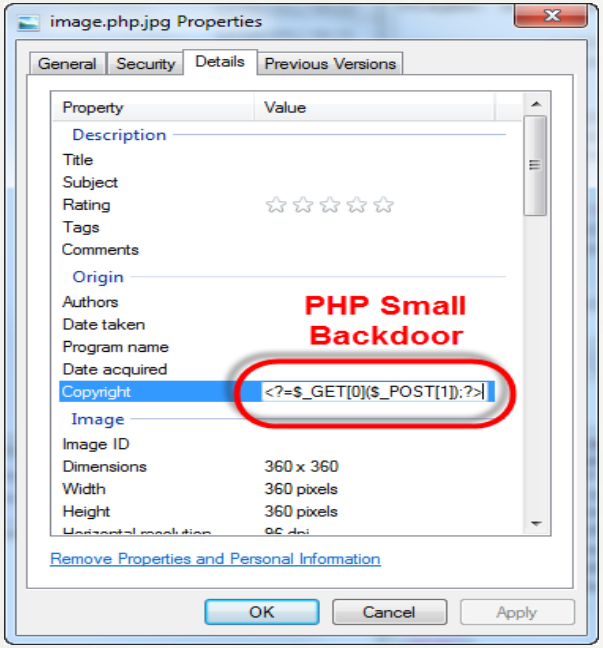
- Cuối tập tin thường bị bỏ qua:
  - Ví dụ dấu chấm và ký tự space
    - “test.asp … . .. .” == “test.asp”
  - Hoặc file:
    - “test.php<>” == “test.php”

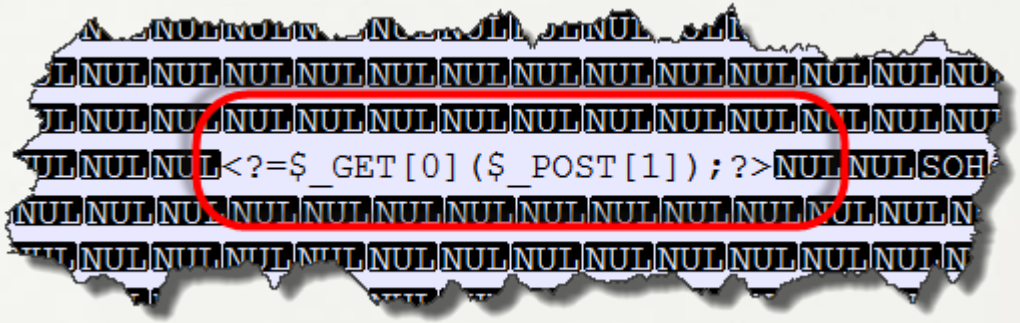
5. Windows File System

- NTFS Alternate Data Streams:
  - "file.asp::$data" == "file.asp"
  - "/folder:$i30:$Index_allocation" == "/folder"
  - ".htaccess:.jpg" → make empty ".htaccess" == "HTACCE~1" …

6. File Type Detector Issues

- Trường hợp Height/Width của file image?
- Ví dụ: Comments trong file jpeg:





7. Null Character

- “file.php%00.jpg”

```
Content-Disposition: form-data; name="myfile"; filename="test.asp.txt"
Content-Type: text/plain
```

Null Character

8. Compression (Image) Issues

Việc nén file .png có thể chứa code php

8. GZIP Compression → PHP Code

- Dữ liệu Text …

```
0   ... ... 9f ... ... 6f ... 24  ... ... ... ... ... ... 6f ...  £ÿgTo,$ + g To
1   ... ... ... ... ... ... ... 6b 6f 5f ... ... -- -- -- --  .) +!g"ko_S
```

- Nén Gzip

```
0   1f ... ... ... ... ... ... 00  ... ... ... ... ... 3f ...  <          c^<?=$
1   5f ... ... ... ... ... ... 28  ... 5f ... 4f ... ... ...  _GET[0]($_POST[1
2   ... ... ... 3f ... ... ... 00  ... ... ... ... ... ... ...  ]);?>X   ï`“
```

- Chúng ta có PHP backdoor:
  - <?=$_GET[0]($_POST[1]);?>

DEMO

DEMO RISKY FUNCTIONALITY FILE UPLOADS

Thank You!

&

Question