Building a pen-test system for web security

Penetration testing

- Ethical hacking for finding security vulnerabilities

- Practice of simple testing : computer system, network or web application

- Pen- testing can be automated with software applications or performed manually

Pen-test process

1. Design pen-test system structure

2. Install pen-test program

3. Test run under pen-test system

[STEP1] Design pen-test system structure

Case1	Case2	Case3
New home page	Sharing current home page	No home page

[STEP1] Design pen-test system structure

	Case1	Case2	Case3
Home page type	New home page	Sharing current home page	No home page
System type	Client- server full system	Client- server full system	Server local test
Connection route (developing)	Client-server-web appl.-DB server-DB	Client-server-web appl.-DB server-DB	Server-web appl.-DB server-DB
Server	Apache	Apache	Apache
Web appl.	PHP	PHP	PHP
DB server	My SQL	My SQL	My SQL
System location	One server in class	Current server	Each PC in class
Client	Each PC in class	Each PC in class	No home page log in client screen

[STEP1] Design pen-test system structure

Case1:

New web site development on one PC in class => web server, web appl, SQLserver, Data table, Client log in screen

Case2:

On current web site => web server, web appl, SQL server, Data table, Client log in screen

Case3:

Local server => web server, web appl, SQL server, Data table (just coding and test on each PC)

(Case1) Design pen-test system structure

- Usage: for web security practice by students
- Test items: SQL injection login, XSS attack
- Location: in class server
- Capacity: 100 sessions simultaneously
- Screen lay ouy : log in, bu/lletin board, advertisement, popup, information sharing space
- Access: wired network system

(Case1) Requirement for home page

- Hardware resource
- Login screen design and development
- Menu function design and development
- Interlocking function design and development
- Database table design and data creating

[STEP2] Install pen-test program

- Select your software combination type

=>Apache PHP MySQL, IIS ASP MsSQL

- Design your **pen-test** process

⇒Follow the basic & common steps as next page process

⇒Search your own procedure and design

Required Resource

Resource	Hardware	Description
OS	OS in class	CentOS 7, Ubuntu , Windows 10
Client	PC in class	• Type and version of Browser • Program Language • Script(CSS:java script, HTML) • IP address
Web Server	Server in class	• Type and version of Web Server • Web Application(SSS) • Program Language • URL, IP address • ODBC(SSS-DB connection)
DB Server	Share with Web Server or different one	• Type and version of DB • Type and version of File
Others	Home page	• URL • site for sign up, log in, bulletien board test

[STEP2] Install pen-test program (Case1)

New home page
Cliect- server full system
Client-server-web appl.-DB server-DB
Apache
PHP
My SQL
One server in class
Each PC in class

1. Apache web server package installation
2. MySQL Server Installation
3. PHP installation
4. Create DB Table
5. Design and install log-in screen on client
6. MySQL connection with PHP

[STEP2] Install pen-test program (Case1)

- Preparing a home page system for test
- Design pen-test system

  =>client – server – web application – SQL server – DB
- Install one web server (Apache, IIS) in class
- Develop web app(PHP, ASP, JSP) and install it on web server
- Install DB server(My SQL,MS SQL) in server in class
- Set and install SQL data table
- Create sign up data
- Design and install log-in screen on client
- Connect from client to web server and DB server

[STEP2] Install pen-test program (Case2)

Sharing current home page
Clisct- server full system
Client-server-web appl.-DB server-DB
Apache
PHP
My SQL
Current server
Each PC in class

1. Apache web server package installation
2. MySQL Server Installation
3. PHP installation
4. Create DB Table
5. Design and install log-in screen on client
6. Mysql connection with PHP

[STEP2] Install pen-test program (Case3)

No home page
Local test
server-web appl.-DB server-DB
Apache
PHP
My SQL
Each PC in class
No client

1. Apache2 web server package installation
2. MySQL Server Installation
3. PHP installation
4. Create DB Table
5. Mysql connection with PHP

[STEP2] Install pen-test program

- Select your model for designing
pen – test system

- Design pen-test system using experience and google searching

- The design method can be different depending on the ideas of each student.

[STEP3] Test run pen-test system

(based on case)

(Environment)

- Web server : select one among IIS, Apache
- Web application : select one among ASP, PHP, JSP
- SQL server : select one among MS SQL, My SQL

(Program coding)

- Client : log in module using CSS (if necessary)
- Web application : log in module, SQL calling routine
- SQL server : table format creation, table data creation

[STEP4] Test run pen-test system

(based on case)

(SQL injection)

- Find the attacking type from references
- Code PHP conditional statement to call SQL server with injection mode

(xss)

- Find the attacking type from references
- Code XSS conditional statement to web page

=> enters a malicious script into a web page that stores the data on the server

Code & Install (based on case)

1. **Install** Apache web server

Confirm installation

Run web browser on Ubuntu(firefox)

Enter web address => **localhost** or server IP

Use ifconfig from terminal

Code & Install (based on case)

2. Install MySQL server

Multi users can access DB

3. Install PHP

Web server supports SSS

For web developing script language

Dynamic web page creation, View or edit that HTML can not

Code & Install (based on case)

4. Confirm

- Run web browser
- Enter web ip => **localhost/info.php** or server ip/info.php

5. Creat DB table for ID,PW test

Code & Install (based on case)

6. Connect mysql with PHP

- The mysql_ * functions are replaced in PHP 7.X.
- When connecting to a database, connect using mysqli or PDO instead of mysql_conncet.
- Example-> mysqli_connect ('hostname', 'username', 'password', 'database');

7. Connect DB

Install Apache, PHP, MySQL on VM, Ubuntu

1. Install web server Apache package
2. Install MySQL server
3. Install PHP
4. Creat DB table(for ID,PW checking)
5. Connect PHP to MySQL
6. Check ID,PW with wrong ones

Install APM on VM, Ubuntu

1. Install Apache web server

- Confirm installation
- Run web browser on Ubuntu(firefox)
- Enter web address => **localhost** or server IP
- Use ifconfig from terminal

2. Install MySQL server

- Multi users can access DB

Install APM on VM, Ubuntu

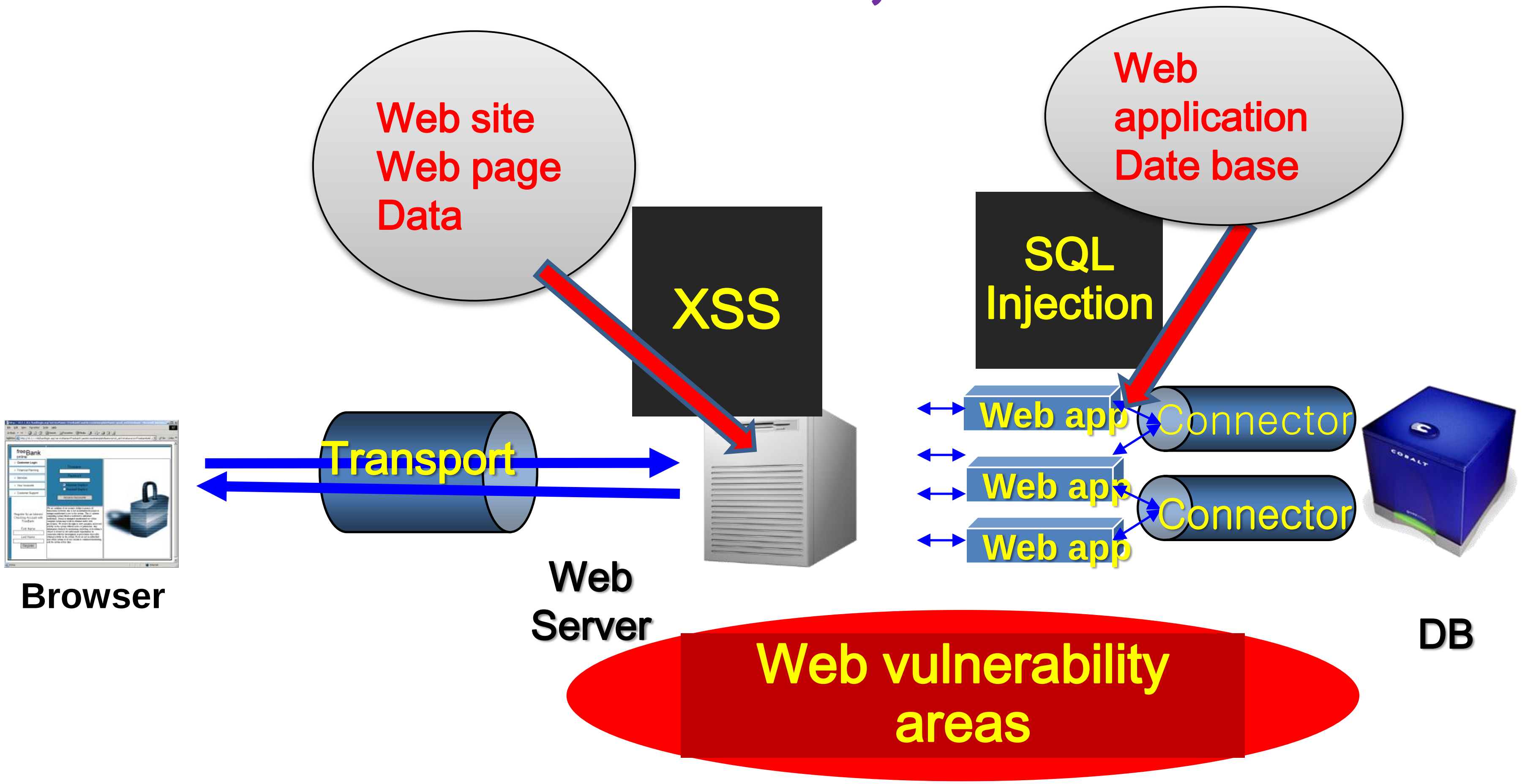
3. Install PHP

For web developing dynamic web page creation, view or edit that HTML can not

4. Creat DB table for ID,PW test

5. Connect mysql with PHP

Vital Threats to Web, OWASP 10



Web site
Web page
Data

Web
application
Date base

XSS

SQL
Injection

Transport

Browser

Web
Server

Web app

Web app

Web app

Connector

Connector

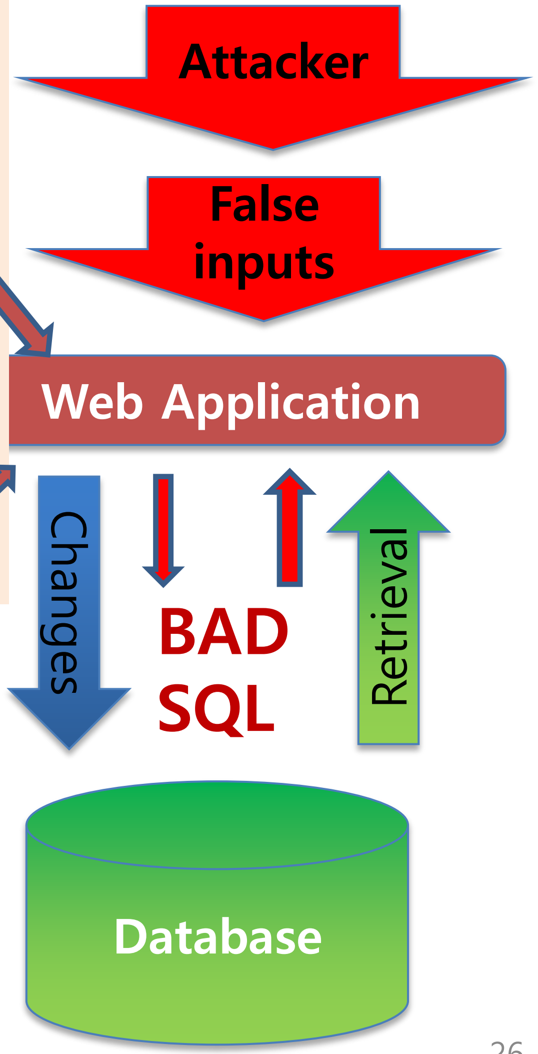
DB

Web vulnerability
areas

SQLI senario

Attacker inserts inputs to change the SQL statements
instead of original values

Statements made to do unintended things, using full permissions of the application



concept
https://www.youtube.com/watch?v=wcaiKgQU6VE
example
https://www.youtube.com/watch?v=FwIUkAwKzG8

* Source : Frein, SQL Injection

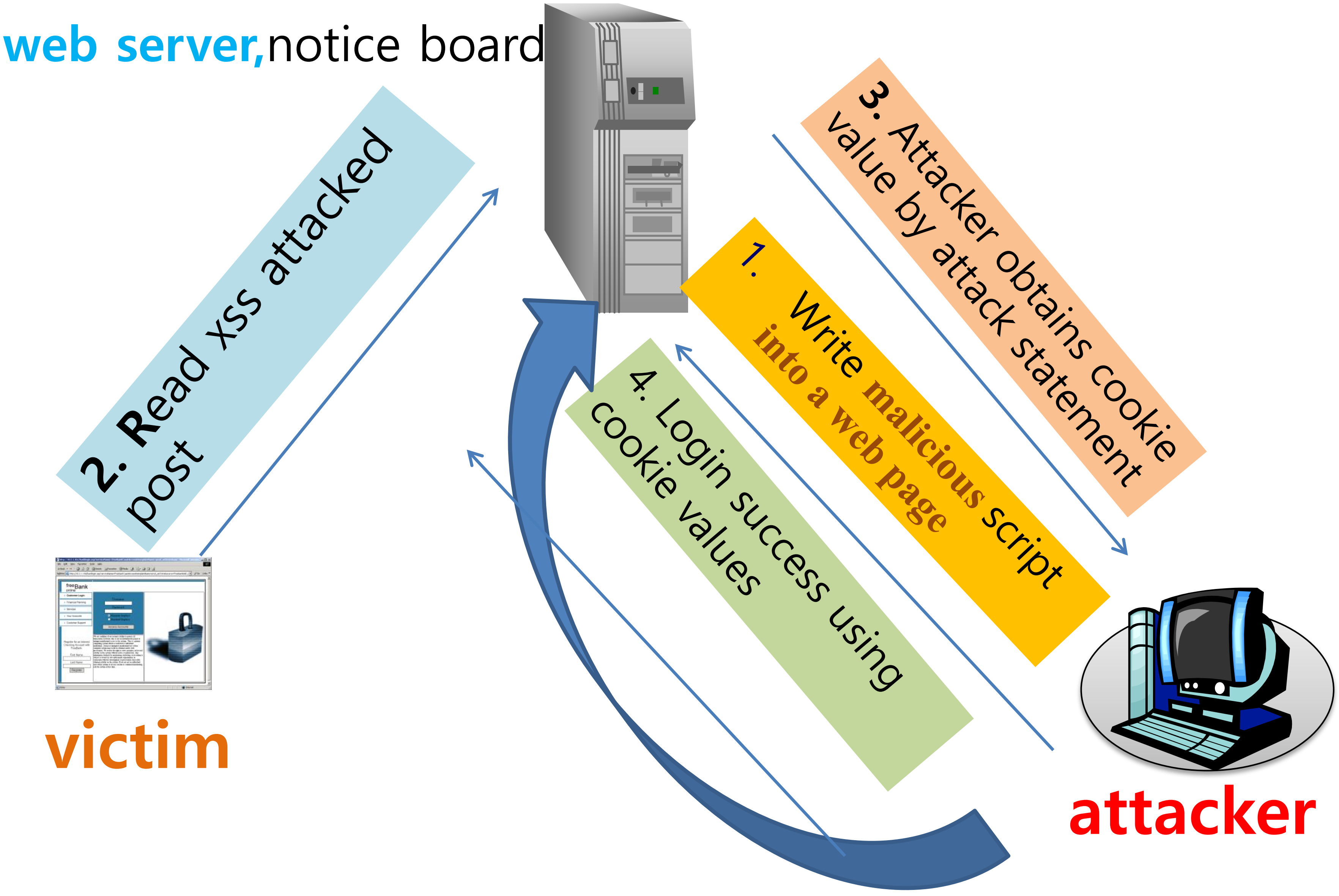
SQLI senario

- Attacker attacks web application code
  => Inserts inputs to change the SQL statements instead of original values

- DB query statements are changed to malicious query

- For pen test every student needs to prepare his/her own web application code

XSS senario



web server,notice board

1. Write **malicious** script **into a web page**

2. **R**ead xss attacked post

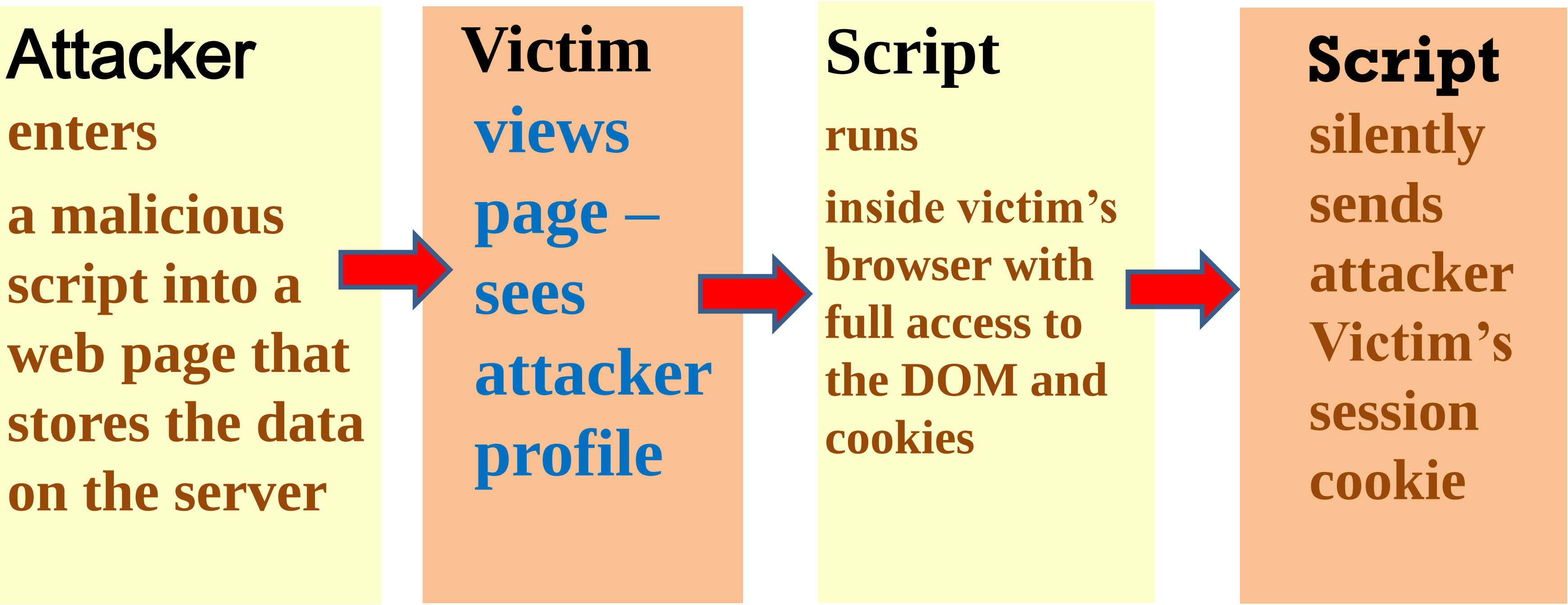
3. Attacker obtains cookie value by attack statement

4. Login success using cookie values

victim

attacker

XSS senario



Attacker enters a malicious script into a web page that stores the data on the server

Victim views page – sees attacker profile

Script runs inside victim’s browser with full access to the DOM and cookies

Script silently sends attacker Victim’s session cookie

Application with stored XSS vulnerability

XSS **senario**

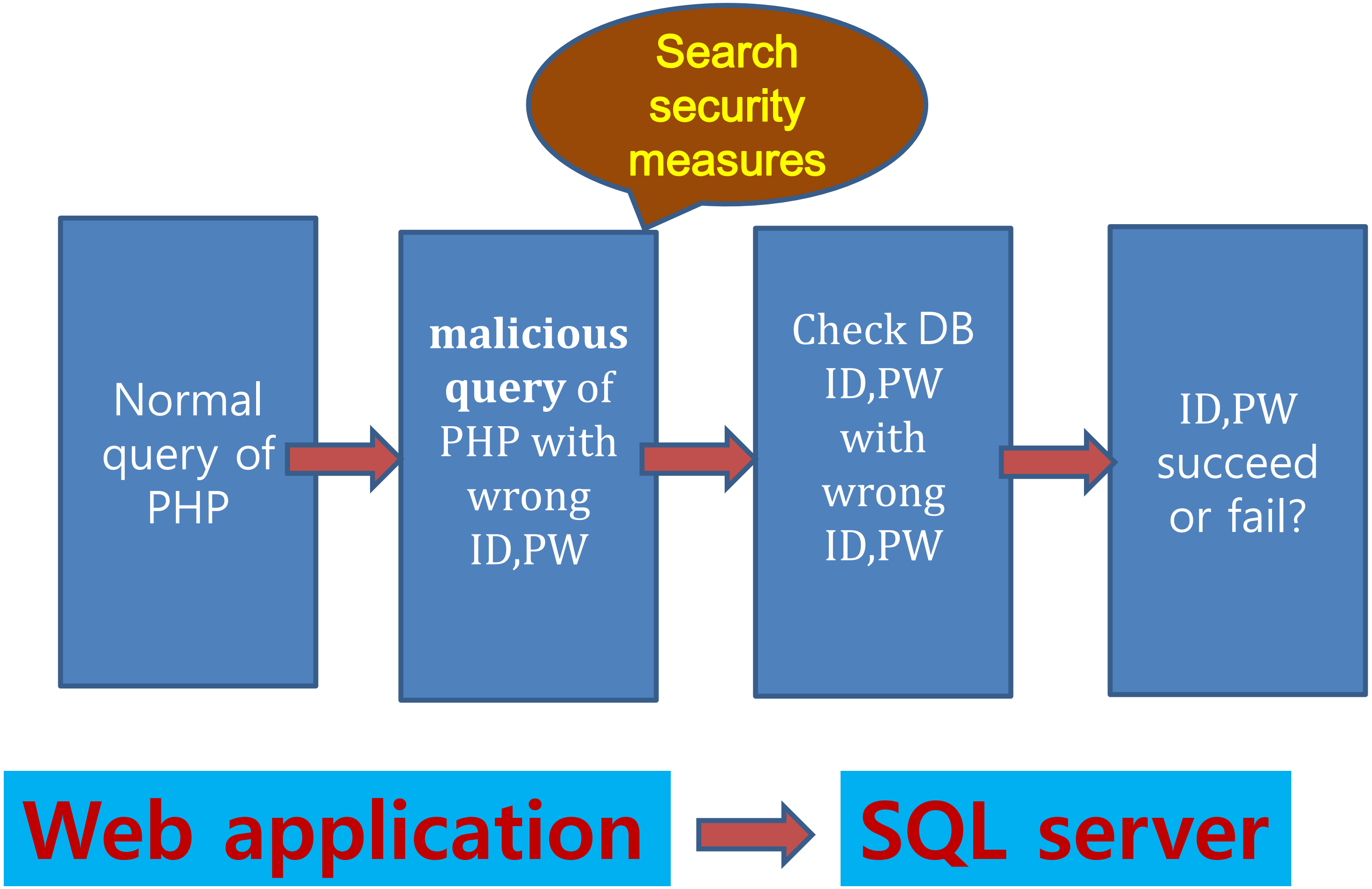
- Attacker attacks data on web pages

=> Inserts malicious script into a web page to abuse the victim`s views

- Malicious script are prepared to runs inside victim’s browser with full access to the cookies

- For pen test every student needs to prepare his/her own code for malicious script writing and use

Web appl.for security measures



Search security measures

Normal query of PHP

malicious query of PHP with wrong ID,PW

Check DB ID,PW with wrong ID,PW

ID,PW succeed or fail?

Web application → SQL server