University
Carlos III of Madrid

Distributed Systems Security

Lab Assignments
Module 3: Fakebook part II (c)
IT Security Group

Guillermo Suárez de Tangil
(guillermo.suarez.tangil@uc3m.es)

Remembering last session…

- **Web Server** (Apache-Tomcat)
  - Fakebook should be accessible for any user
  - Tomcat's configuration should allow the correct operation of the web application
  - Not reveal any critical information
  - SSL
- **Data Base** (MySQL)
  - Accessible only from the local machine
  - Web admin only tables related to the web

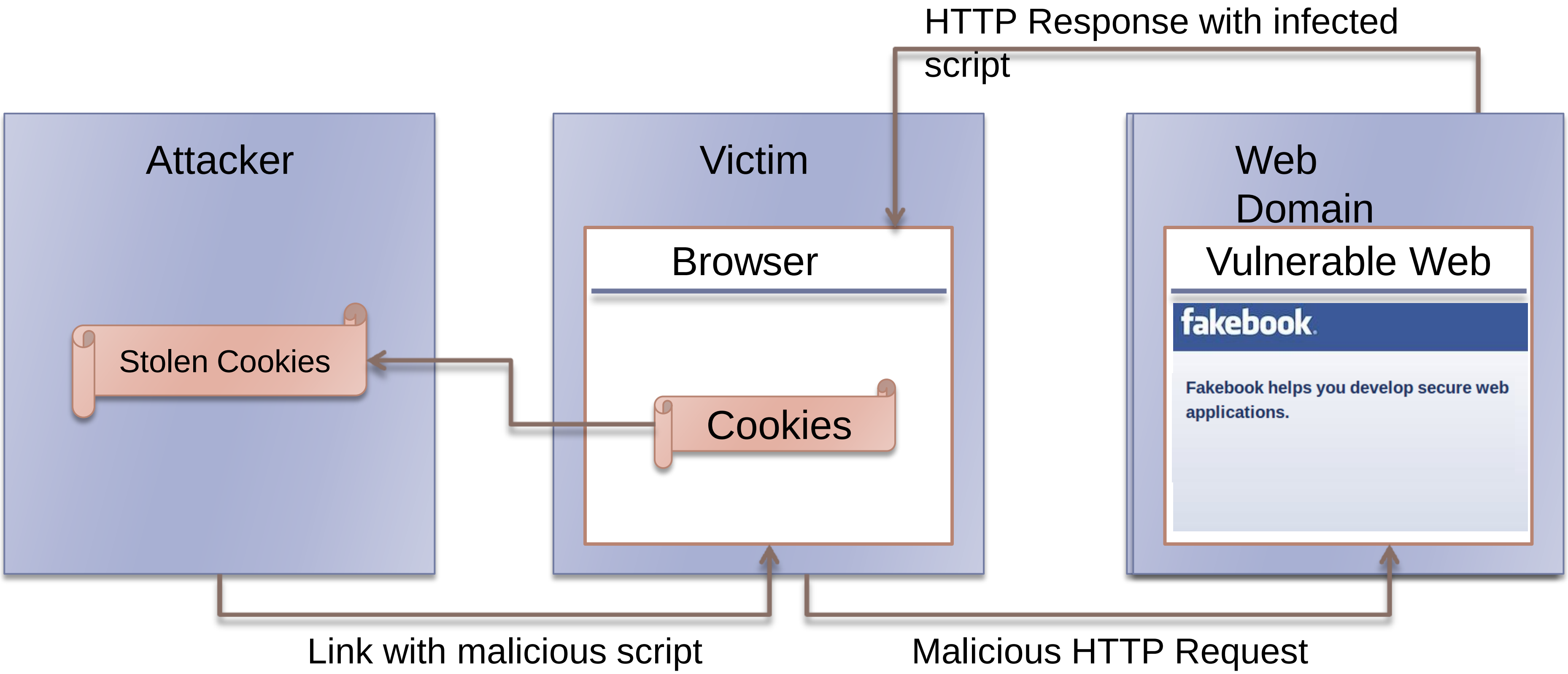
Remembering last session…

- **JSP Files**
  - Any user can enroll in Fakebook
  - Input parameters must be specially treated
    - SQL Injection
    - XSS
    - Control Input parameters (forms & database)
  - Errors/Anomalies Control
  - Access Control
  - Identity Theft
  - Protection of Personal Information
- Optional
  - Profile Image
  - Privacy Control -> Friends

Cross Site Scripting

- Affects the Web Application
- Code injection technique
  - Generally *JavaScript*
- Exploits server’s vulnerabilities, but **affects the client.**
- Consequences:
  - Steal of
    - Credentials
    - Private information
  - Identity theft
  - …

Non-Persistent XSS



HTTP Response with infected script

Attacker

Stolen Cookies

Victim

Browser

Cookies

Web Domain

Vulnerable Web

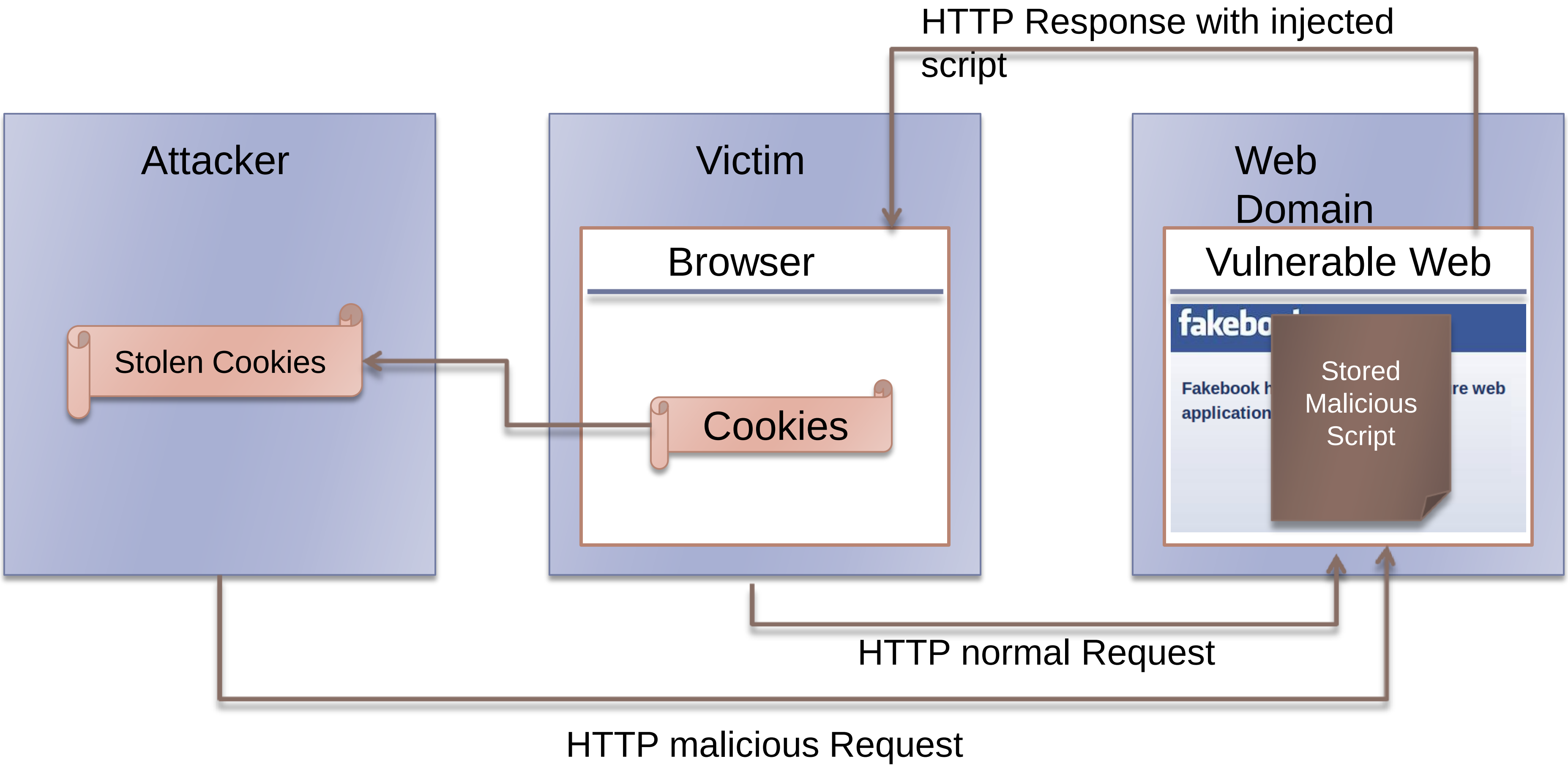
fakebook.

Fakebook helps you develop secure web applications.

Link with malicious script

Malicious HTTP Request

Persistent XSS



HTTP Response with injected script

Attacker

Stolen Cookies

Victim

Browser

Cookies

Web Domain

Vulnerable Web

Stored Malicious Script

HTTP normal Request

HTTP malicious Request

How to avoid XSS

- Find all application’s input variables
- Analyze their use in the application
- Analyze the consequences of their modification
- Implement filter mechanisms
  - Define possible values for the inputs
    - Whitelist
    - Blacklist
  - Filter and/or scape the rest of the characters
  - Careful with the codification of the characters

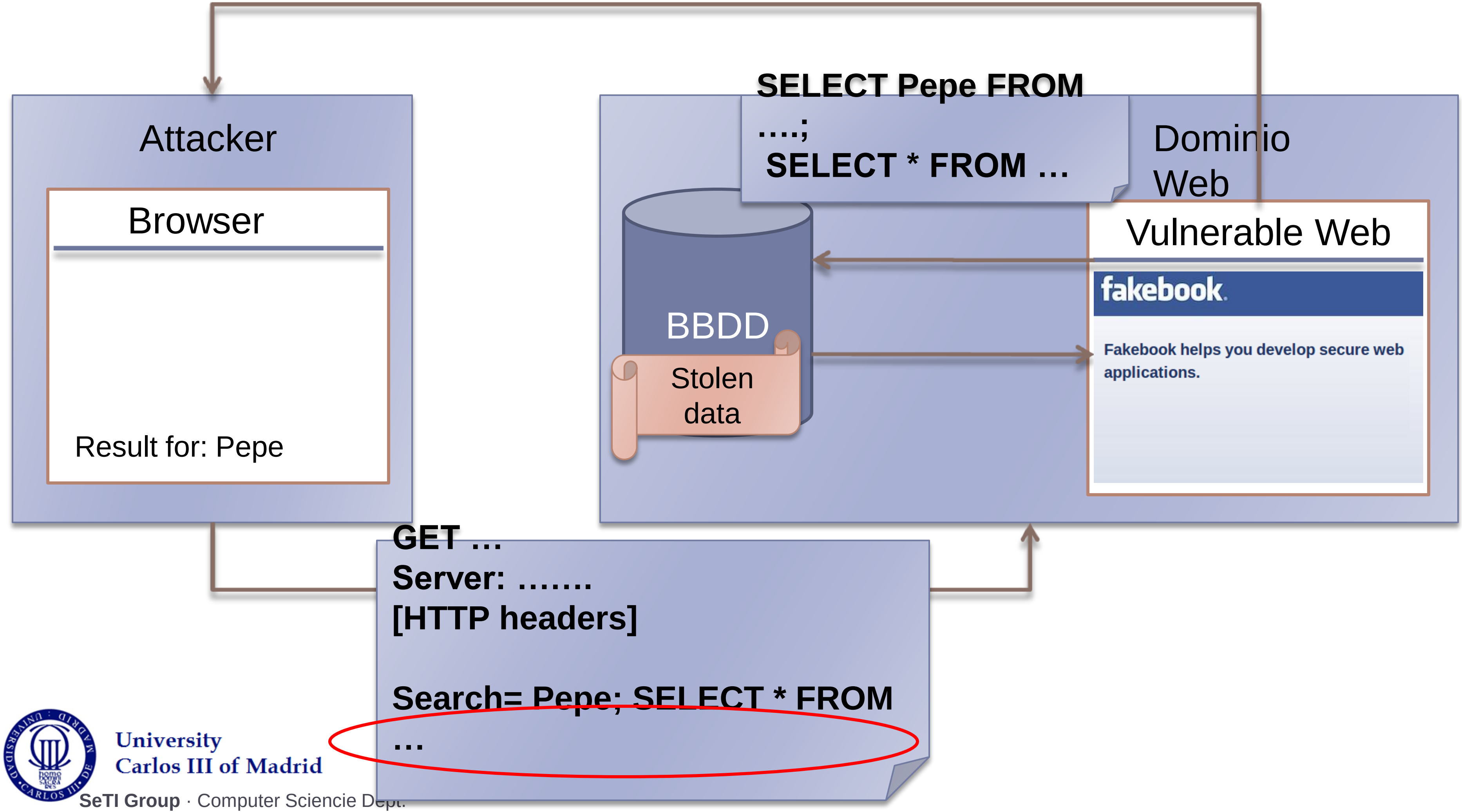
What are we expecting?

- Learn how to take advantage of existing errors
  - Explaining how are produced
  - Example
- Justification of the risk of each threat
- Solution to the threat
  - Complete/Partial
  - Justification

SQL Injection

- Affects to the data base
  - Both the server
  - And the client
- It is achieved by means of malicious SQL queries
- Consequences:
  - Steal of
    - Credentials
    - Private information
  - Identity theft
  - …
- Violates confidentiality, integrity and authenticity.

Typical SQL-attack



SELECT Pepe FROM ….;
SELECT * FROM …

GET …
Server: …….
[HTTP headers]

Search= Pepe; SELECT * FROM …

Other attacks

- In general, it can be done anything that could be done with SQL
  - Delete tables
  - Insert new rows
  - Modify tables
  - …
- Other related attacks
  - LDAP Injection

How to avoid SQL-Injection

- Find all application’s input variables
- Analyze their use as SQL sentences in the source code
- Analyze output information retrieved from the data base.
- Implement filter mechanisms and/or scape characters
- Administrate the data base
  - Table’s privileges
  - Handle sensible information

What are we expecting?

- Learn how to take advantage of existing errors
  - Explaining how are produced
  - Example
- Justification of the risk of each threat
- Solution to the threat
  - Complete/Partial
  - Justification

Tips and Useful Advises (I/II)

- Analyze and understand how the Web application operates
- Identify variables that take its value from user input.
  - *Matching* and *storage* **database**
  - **HTML code**
- Analyze the mechanisms used to store personal information of the user
- Perform additional modifications to improve the security of the Web application, always considering the established requirements

Tips and Useful Advises (II/II)

- Divide and conquer
  - Break the module down (smallest work scopes)
- Before implementing, **abstraction**!
  - Textual description of the changes to tackle
- Backup copies
- Criticize your own decisions
- Discuss in with other pairs
  - **Do not plagiarize! (Knowledge assessment)**

References

- Assignment description
- XSS and SQL Injection
  - On the Internet, *and*
  - At the laboratory.

More Information

- Microsoft
- XSSED
- OWASP
- Google