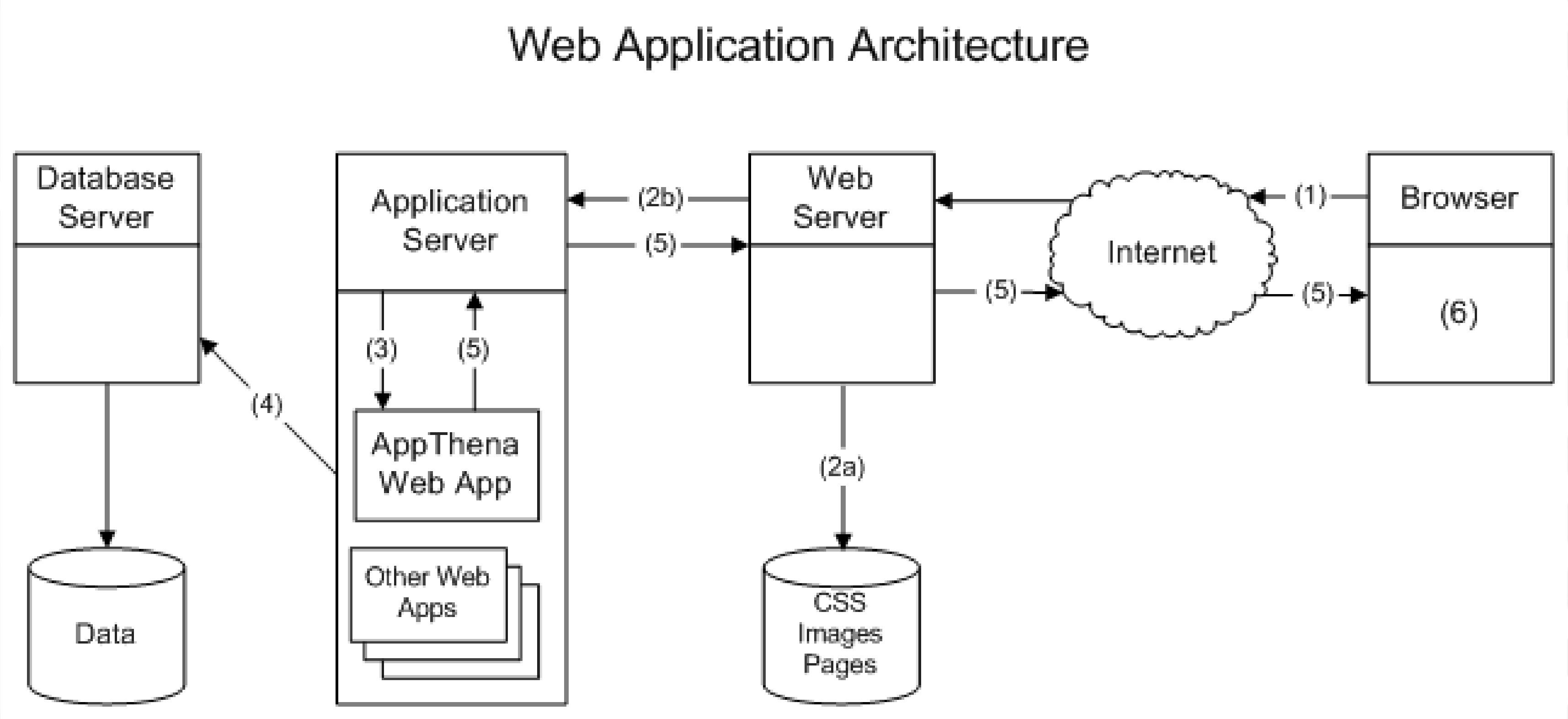
The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

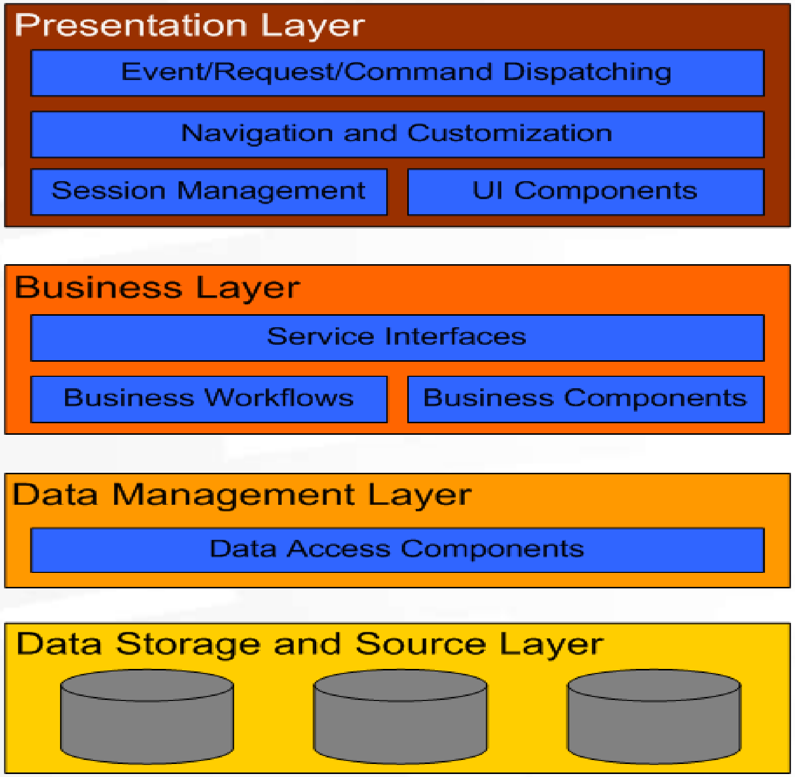
Module 4. Vulnerability Analysis for Web-applications

Penetration testing course

Architecture of Web-application

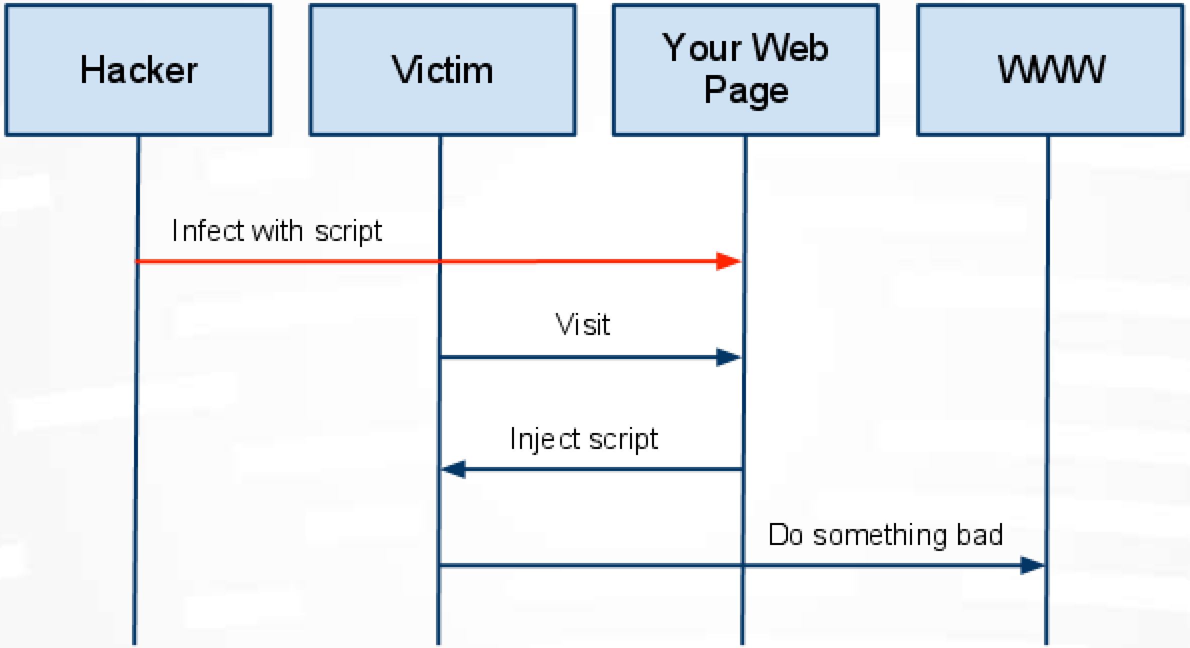


Web-application layers



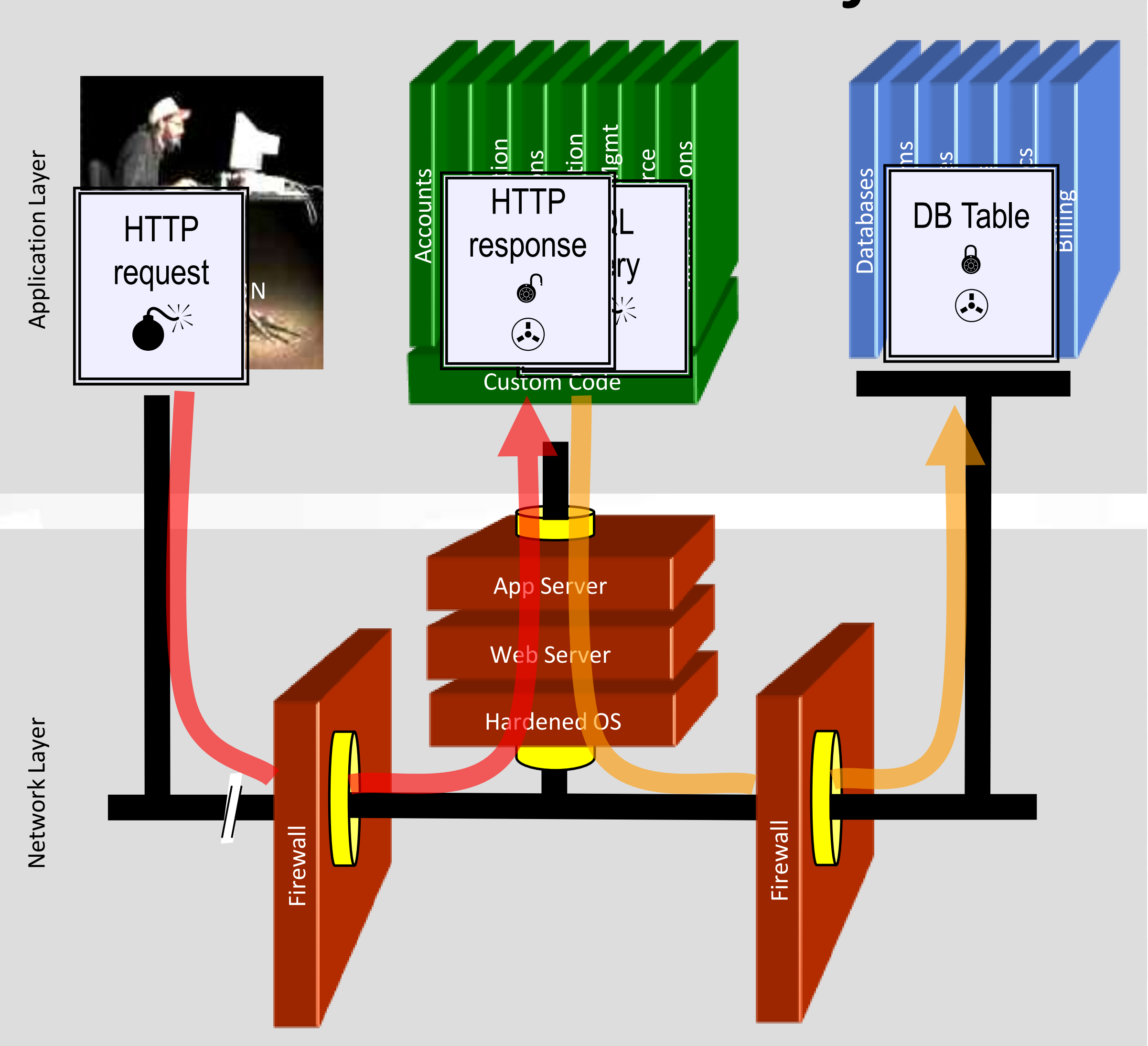
Use of layers allows to divide logics of application. Lack of layers and data controls lead to different vulnerabilities in Web-applications.

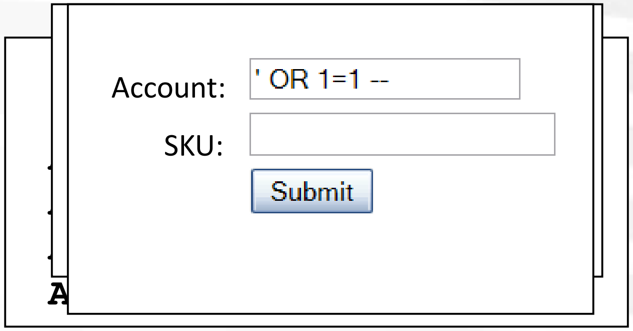
XSS-attacks



A High Level View of a typical XSS Attack

SQL-injection




Account: ' OR 1=1 --

SKU:

1. Application presents a form to the attacker

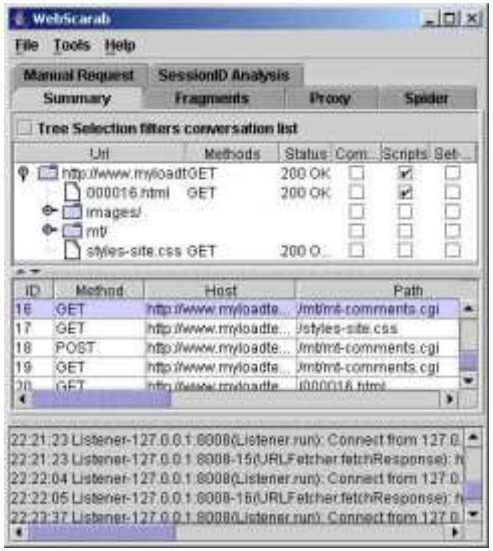
2. Attacker sends an attack in the form data

3. Application forwards attack to the database in a SQL query

4. Database runs query containing attack and sends encrypted results back to application

5. Application decrypts data as normal and sends results to the user

Use of local proxies



Url	Methods	Status	Com...	Scripts	Set-...
http://www.myloadt	GET	200 OK	□	☑	□
000016.html	GET	200 OK	□	☑	□
images/			□	□	□
mt/			□	□	□
styles-site.css	GET	200 O...	□	□	□

ID	Method	Host	Path
16	GET	http://www.myloadte...	/mt/mt-comments.cgi
17	GET	http://www.myloadte...	/styles-site.css
18	POST	http://www.myloadte...	/mt/mt-comments.cgi
19	GET	http://www.myloadte...	/mt/mt-comments.cgi
20	GET	http://www.myloadte...	/000016.html

```
22:21:23 Listener-127.0.0.1:8008(Listener.run): Connect from 127.0.
22:21:23 Listener-127.0.0.1:8008-15(URLFetcher.fetchResponse): h
22:22:04 Listener-127.0.0.1:8008(Listener.run): Connect from 127.0.
22:22:05 Listener-127.0.0.1:8008-16(URLFetcher.fetchResponse): h
22:23:37 Listener-127.0.0.1:8008(Listener.run): Connect from 127.0.
```

Web-application security testing

OWASP Open Web Application Security Project | Testing Guide 4.0

)release(

Project Leaders: Matteo Meucci and Andrew Muller

Creative Commons (CC) Attribution Share-Alike

Free version at http://www.owasp.org

https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf

OWASP testing guide

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for weak Cryptography
- Business Logic Testing
- Client Side Testing