INSTITUTE : UIE
DEPARTMENT : CSE

Bachelor of Engineering (Computer Science & Engineering)

WEB AND MOBILE SECURITY (Professional Elective-I)

(20CST/IT-333)

TOPIC OF PRESENTATION:

Introduction to web applications, Web application hacking

DISCOVER . LEARN . EMPOWER

Lecture Objectives

In this lecture, we will discuss:
• Introduction to Introduction to web applications, Web application hacking
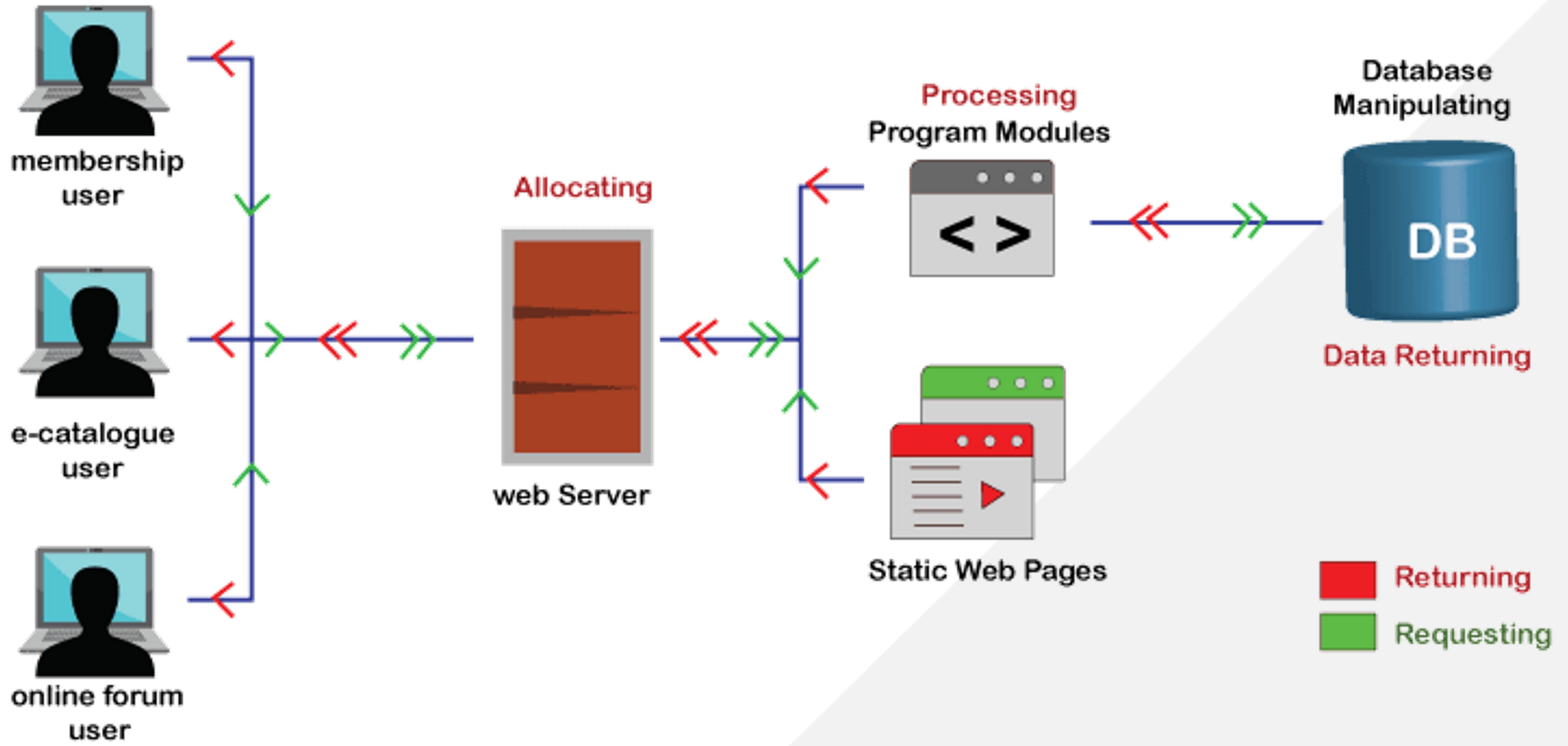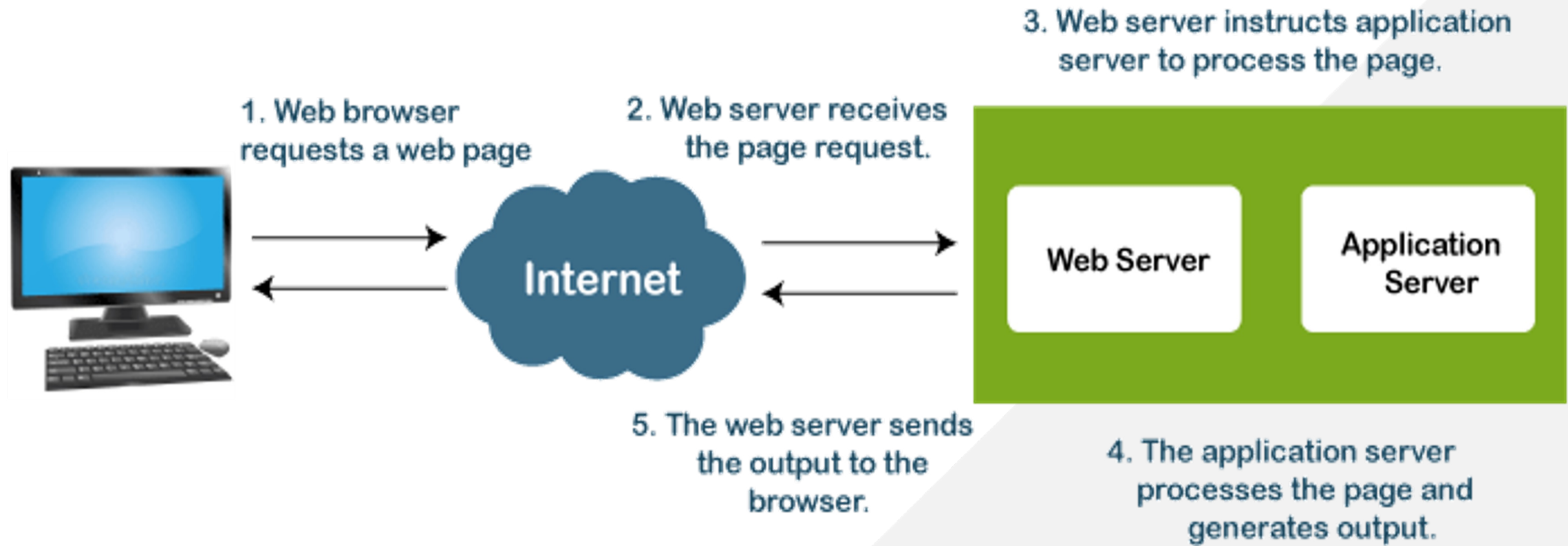
Web-application

- A web-application is an application program that is usually stored on a remote server, and users can access it through the use of **Software** known as **web-browser.**

- In general, a web application can contain online shops (or we can also say them e-commerce shops), webmail's, calculators, social media platforms, etc. There is also some kind of web application that usually requires a special kind of web browser to access them.

- We cannot access those kinds of web applications by using regular web-browsers. However, most of the web applications available on the internet can be accessed using a standard web browser.

How does a web- application work?

- A web application are generally coded using the languages supported by almost every web-browsers such as HTML, JavaScript because these are the languages that rely on the web browsers to render the program executable.

- Some of the web applications are entirely static due to which they not required any processing on the server at all while, on the other hand, some web applications are dynamic and require server-side processing.

- To operate a web- application, we usually required a web server (or we can say some space on the web-server for our programs/application's code) to manage the clients' upcoming requests and required an application server.

- The application server performs the task that requested by the clients, which also may need a database to store the information sometimes. Application server technologies range from **ASP.NET**, **ASP**, and **ColdFusion to PHP and JSP**.

1. Web browser requests a web page

2. Web server receives the page request.

3. Web server instructs application server to process the page.

Internet

Web Server

Application Server

5. The web server sends the output to the browser.

4. The application server processes the page and generates output.

Hacking web applications

- Some of the most common forms of attacks:
- Cross site scripting (XSS) — This vulnerability allows the attacker to target other users on the application to gain their user data or perform unauthorised actions on their behalf.
- Cross site request forgery (CSRF) — Is an attack that forces a user to perform an unintended action. E.g. get them to change their password or transfer funds to the attackers account.
- Information Leakage — As the name suggests this vulnerability allows the attacker gain information about an application or its underlying data. This could be from developers leaving comments in the source code or through poor error handling.
- https://www.knowledgehut.com/blog/security/hacking-web-applications

Introduction to hacking web applications

- Broken access controls — Is where the web application fails to protect its data or functionality held for admin users enabling an attacker to access data it shouldn't be allowed to.

- Broken authentication — This includes vulnerabilities that allow users to set weak passwords, have weak or easily guessable recovery password questions, allowing brute force login attempts.

- SQL injection — The popularity of this attack has fallen in recent years due to new functions and libraries that can help developers protect their application. Increased awareness of SQL injection taught in schools and throughout university means that even junior developers are aware of the potential implications of not sanitising user inputs that form part of the SQL query string.

Security mechanisms

- The web application uses the below security mechanisms:
- Authentication
- Session management
- Access control

References:

Books:
1. Web Design With HTML, CSS, JavaScript and jQuery Set, 1st Edition, by Jon Duckett.
2. Hacking Exposed Web Applications, 3rd edition, Joel Scambray, Vincent Liu, Caleb Sima, Released October 2010, Publisher(s): McGraw-Hill
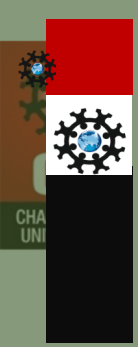
Relevant Videos:
1. https://www.youtube.com/watch?v=24fHLWXGS-M
2. https://www.youtube.com/watch?v=X4eRbHgRawI

Reference Links:
1. https://www.knowledgehut.com/blog/security/hacking-web-applications
2. https://medium.com/@dandobusiness/introduction-to-hacking-web-applications-d72e52b247b2

THANK YOU