CROSS SITE SCRIPTING (XSS)

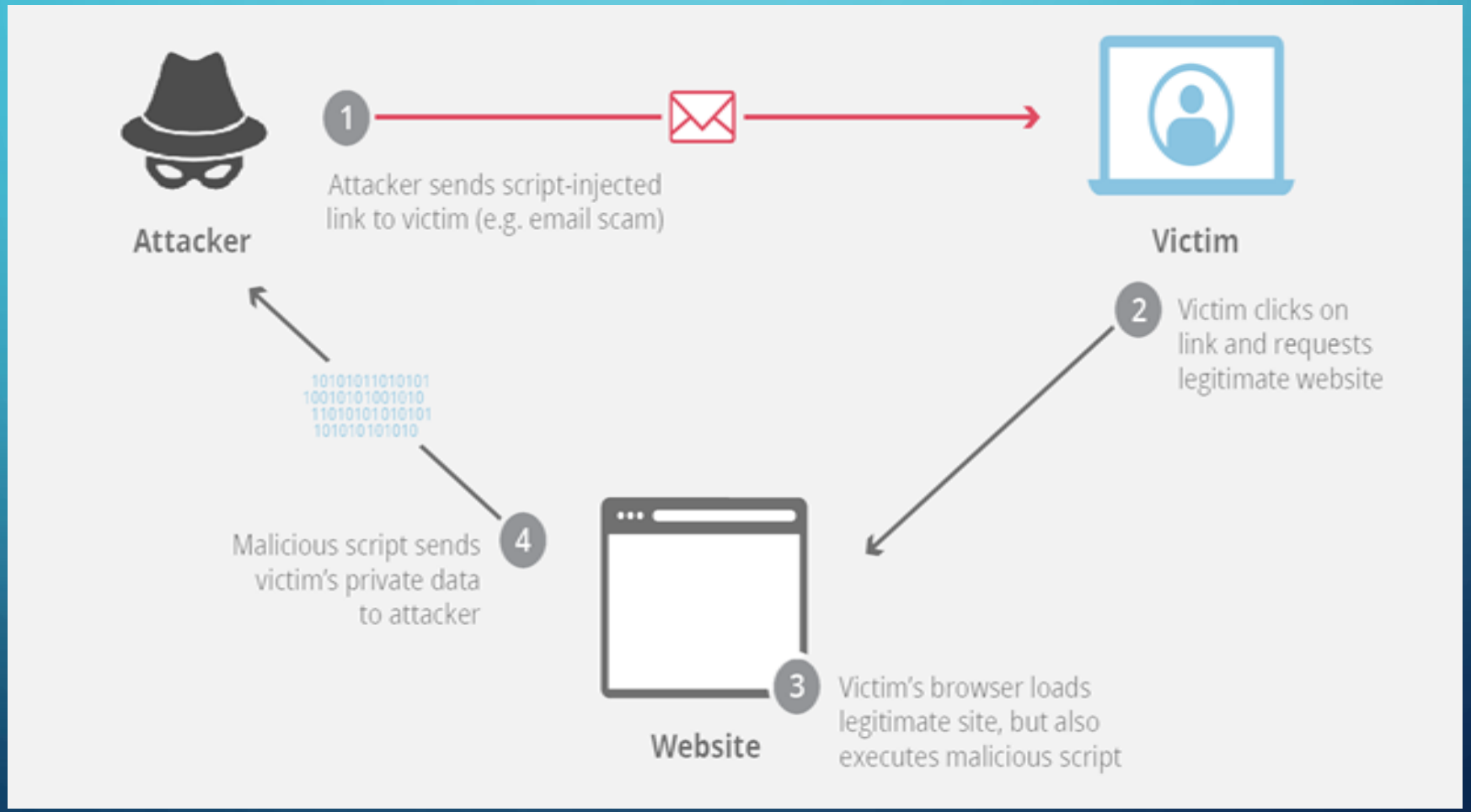
AGENDA

- Introduction of Cross site Scripting.
- How Cross Site Scripting is executed.
- How to fix Cross Site Scripting.
- Impacts of Cross Site Scripting.

1) INTRODUCTION OF XSS

- Cross-site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website.
- Types:
    1. Stored XSS (injected script is permanently stored in target server).
    2. Reflected XSS (injected script is reflected off a web application and directly onto user's browser).
    3. DOM based XSS (script manipulates the DOM to execute within user's browser).

2) EXECUTION OF XSS



3) FIXING OF XSS

- Validate all the Input data before served.
- Output Encoding.
- Use a trusted HTML sanitizer library.
- Use Security Headers.
- Patch and Update of Browser.

4) IMPACTS OF XSS

1. DATA THEAFT.
2. SESSION HIJACKING.
3. MALWARE DISTRIBUTION.
4. PHISING.

THANK YOU