# CROSS-SITE SCRIPTING

Made by: Me

# INTRODUCTION

- Cross-site scripting is hacking technique that leverages vulnerabilities in the code of a web application to allow an attacker to send malicious content from an end-user and collect some type of data from the victim.

- Attacker sends text-based attack scripts that exploit the interpreter in the browser. Almost any source of data can be an attack vector, including internal sources such as data from the database.

# EXPLOITABILITY - AVERAGE

# PREVALENCE - VERY WIDE SPREAD

- XSS is the most prevalent web application security flaw. XSS flaws occur when an application includes user supplied data in a page sent to the browser without properly validating or escaping that content. There are three known types of XSS flaws:
  - Stored,
  - Reflected
  - DOM based XSS.

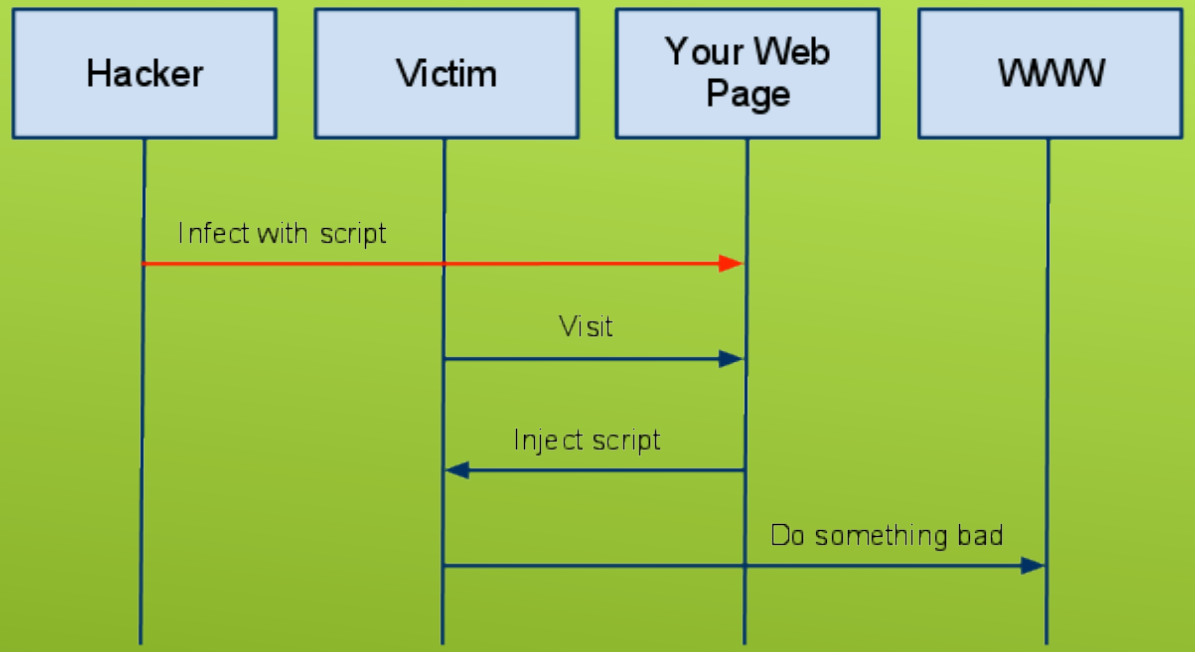
# DETECTABILITY - EASY

- Detection of most XSS flaws is fairly easy via testing or code analysis.

# IMPACT - MODERATE

- Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc.

# SEQUENCE DIAGRAM




A High Level View of a typical XSS Attack