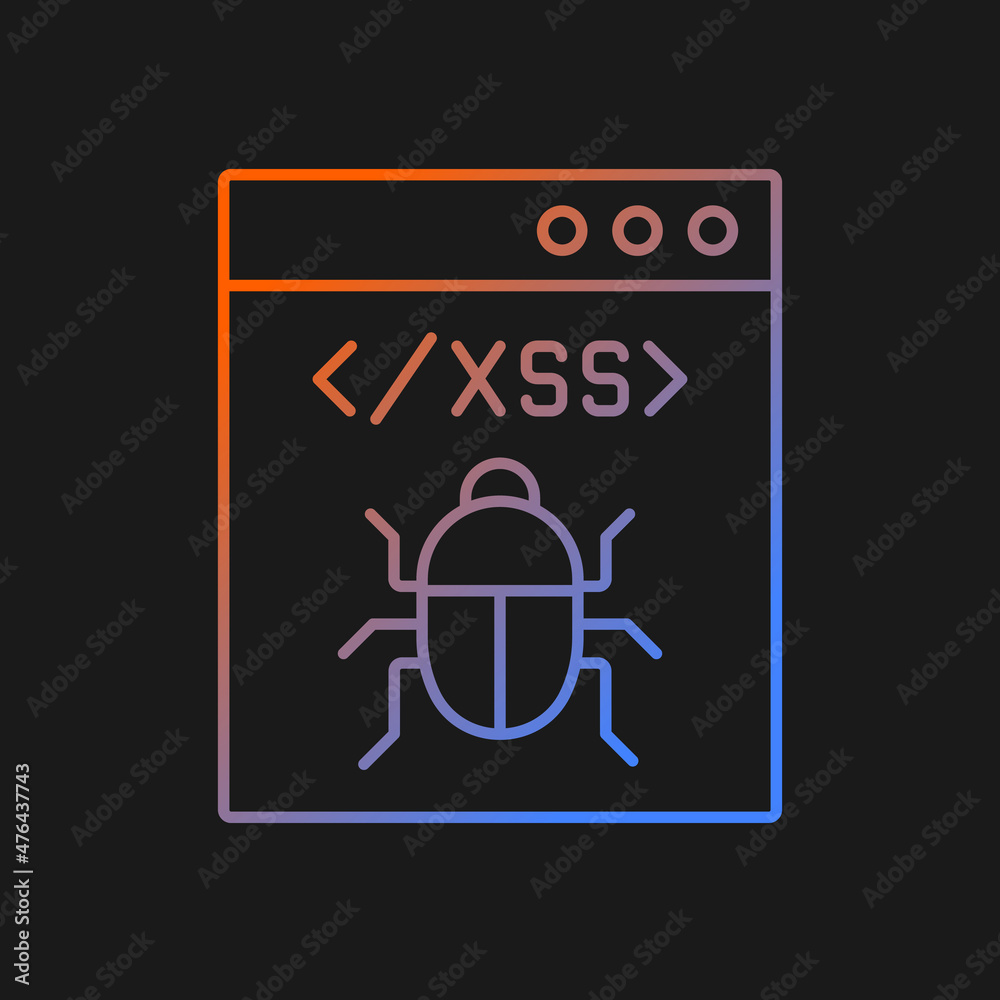
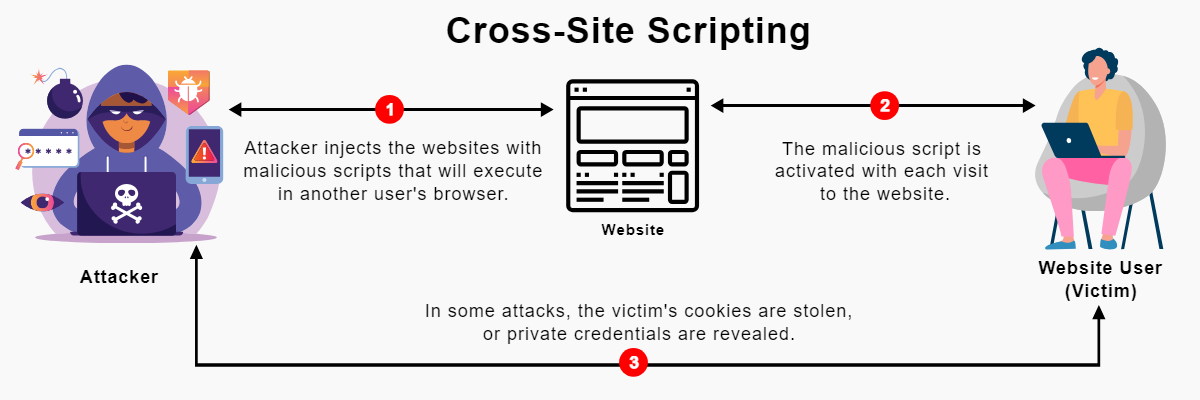
**CTF Challenge: Exploiting XSS Vulnerabilities**

****

**1. Introduction**

****

Cross-site scripting (XSS) is a type of security vulnerability commonly found in web applications. It allows attackers to inject malicious scripts into content from otherwise trusted websites. This guide will walk you through a simple Capture The Flag (CTF) challenge focused on exploiting XSS using a free online website.

**2. Tools and Requirements**

* Web Browser: Any modern web browser (Chrome, Firefox, etc.)

**3. Scenario**

****

You are a security researcher tasked with testing a web application for XSS vulnerabilities. Your goal is to identify an XSS vulnerability and exploit it to display a custom message.

**4. Process to Perform While performing CTF**

Step 1: Go to the website <http://testphp.vulnweb.com/>

Step 2: Put the payload on the `<script>alert('XSS');</script>` on search art which will appear on the top left of the box.

**Question**

Flag 1: What payload did you use to exploit the XSS vulnerability?

Answer: <script>alert('XSS');</script>.

Flag 2: What was the result of the payload injection?

Answer: XSS

Hint:

