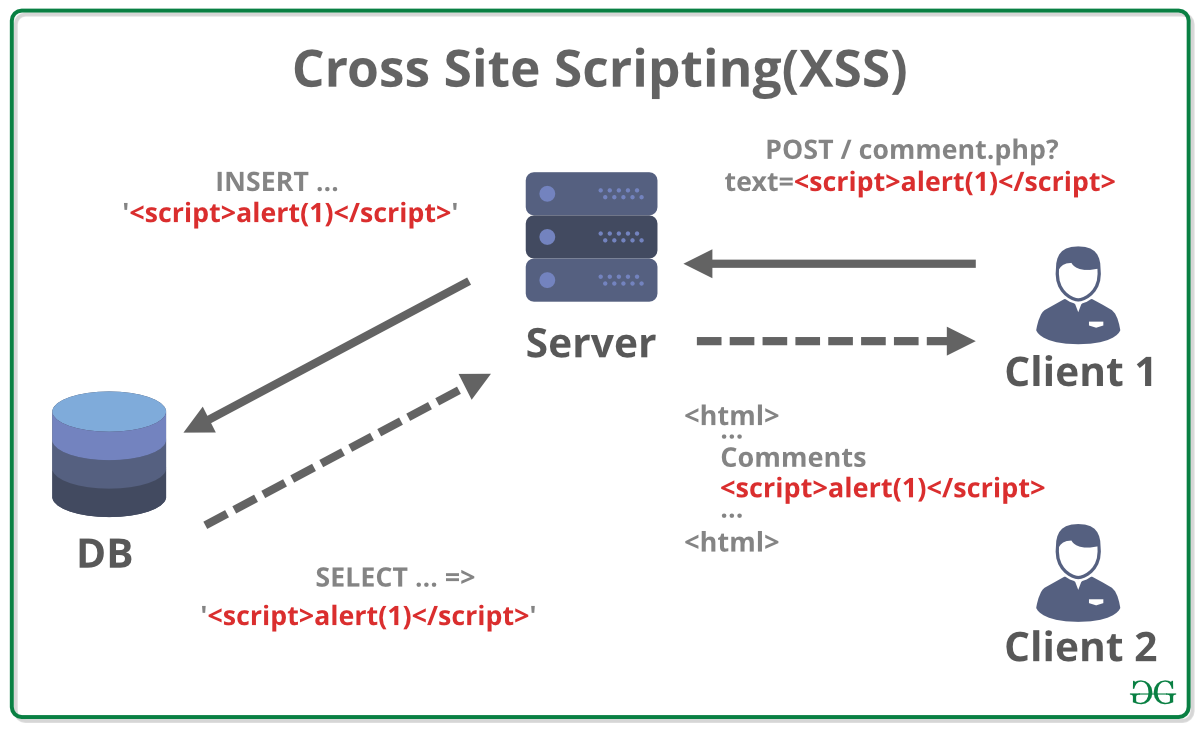
**CTF Challenge: Exploiting XSS Vulnerabilities**



**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.

**5. Let's Begin the Challenge**

**Step 1: Navigate to the Target Site**

Open your web browser and go to <http://testphp.vulnweb.com/>

**Step 2: Find a Vulnerable Input Field**

Look for an input field that might reflect user input in the webpage. A good starting point is the search bar.

**Step 3: Inject the Payload**

Enter “**<script>alert('XSS');</script>**” into the search bar and submit.

**Question**

Flag 1: What input field did you find to be vulnerable?

Answer: search bar

Flag Captured.

Flag 2:What payload did you use to exploit the XSS vulnerability?

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

Flag Captured.

Flag 3: What was the result of the payload injection?

Answer: XSS

Flag Captured.

**Hint**

