Dom.php

* **总漏洞数**: 2

1. **漏洞类型**: 反射型跨站脚本攻击 (Reflected Cross-Site Scripting, XSS)
   * **CWE 标号**: CWE-79
   * **描述**: 未对用户输入的 name 参数进行适当的转义和验证，直接输出到 HTML 中，可能导致跨站脚本攻击（XSS）。
   * **修复建议**: 对用户输入的数据进行适当的转义和验证，防止 XSS 攻击。
2. **漏洞类型**: DOM型跨站脚本攻击 (DOM-based Cross-Site Scripting, XSS)
   * **CWE 标号**: CWE-79
   * **描述**: 在 JavaScript 中使用用户可控的对象属性来动态加载脚本，存在 DOM 型 XSS 攻击的风险。
   * **修复建议**: 避免使用用户可控的对象属性直接操作 DOM，或者对其进行严格的验证和转义。

Example.php

* **总漏洞数**: 1

1. **漏洞类型**: 反射型跨站脚本攻击 (Reflected Cross-Site Scripting, XSS)
   * **CWE 标号**: CWE-79
   * **描述**: 未对用户输入的 name 参数进行适当的转义和验证，直接输出到 HTML 中，可能导致跨站脚本攻击（XSS）。
   * **修复建议**: 对用户输入的数据进行适当的转义和验证，防止 XSS 攻击。

Express.js

* **总漏洞数**: 1

1. **漏洞类型**: 反射型跨站脚本攻击 (Reflected Cross-Site Scripting, XSS)
   * **CWE 标号**: CWE-79
   * **描述**: 未对用户输入的 name 参数进行适当的转义和验证，直接输出到 HTML 中，可能导致跨站脚本攻击（XSS）。
   * **修复建议**: 对用户输入的数据进行适当的转义和验证，防止 XSS 攻击。

Sc.cs

* **总漏洞数**: 1

1. **漏洞类型**: 不安全的 Cookie 设置 (Insecure Cookie Setting)
   * **CWE 标号**: CWE-614
   * **描述**: 在不安全的上下文中设置了敏感信息的 Cookie，未对 Cookie 属性进行适当配置，可能导致 Cookie 被窃取或篡改。
   * **修复建议**: 确保在安全的上下文中设置敏感信息的 Cookie，并设置适当的属性，如 Secure 和 HttpOnly。

Sc2.cs

**总结**

* **总漏洞数**: 1

1. **漏洞类型**: 不安全的 Cookie 设置 (Insecure Cookie Setting)
   * **CWE 标号**: CWE-614
   * **描述**: 在不安全的上下文中设置了敏感信息的 Cookie，未对 Cookie 属性进行适当配置，可能导致 Cookie 被窃取或篡改。
   * **修复建议**: 确保在安全的上下文中设置敏感信息的 Cookie，并设置适当的属性，如 Secure 和 HttpOnly。

Spring.java

* **总漏洞数**: 1

1. **漏洞类型**: 反射型跨站脚本攻击 (Reflected Cross-Site Scripting, XSS)
   * **CWE 标号**: CWE-79
   * **描述**: 未对用户输入的 name 参数进行适当的转义和验证，直接输出到 HTML 中，可能导致跨站脚本攻击（XSS）。
   * **修复建议**: 对用户输入的数据进行适当的转义和验证，防止 XSS 攻击。

Xss.cs

* **总漏洞数**: 1

1. **漏洞类型**: 反射型跨站脚本攻击 (Reflected Cross-Site Scripting, XSS)
   * **CWE 标号**: CWE-79
   * **描述**: 未对用户输入的 userInfo 参数进行适当的转义和验证，直接输出到 HTML 中，可能导致跨站脚本攻击（XSS）。
   * **修复建议**: 对用户输入的数据进行适当的转义和验证，防止 XSS 攻击。