

系统安全实验八

Julius Karl

2024 年 6 月 26 日

1 XSS 漏洞分析

XSS（跨站脚本攻击）是一种常见的网络应用安全漏洞，允许攻击者将恶意脚本注入到网页中，进而由受害者的浏览器执行。这些脚本可以窃取用户的会话凭证、篡改网页内容、重定向用户至恶意站点，甚至进行钓鱼攻击。

XSS 漏洞主要分为以下几种类型：

1.1 反射型（非持久型）：

攻击是一次性的，受害者点击了包含恶意 JavaScript 脚本的 URL。恶意代码并没有保存在目标网站，而 Web 应用程序只是不加处理地将该恶意脚本“反射”回受害者的浏览器，使其执行相应的脚本。

1.2 存储型（持久型）：

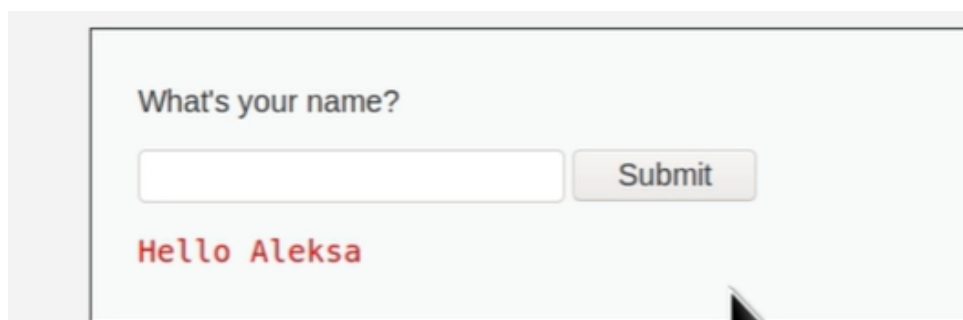
应用程序通过 Web 请求获取不可信赖的数据，并将其存入数据库。当下一次从数据库中获取该数据时，程序未对其进行过滤，页面再次执行 XSS 代码，持续攻击用户。常出现在留言板、评论区等用户提交内容的地方。

1.3 DOM 型（非持久型）：

恶意代码直接影响浏览器的 DOM 结构，而不是服务器端。攻击不需要数据存储，直接在浏览器中执行。

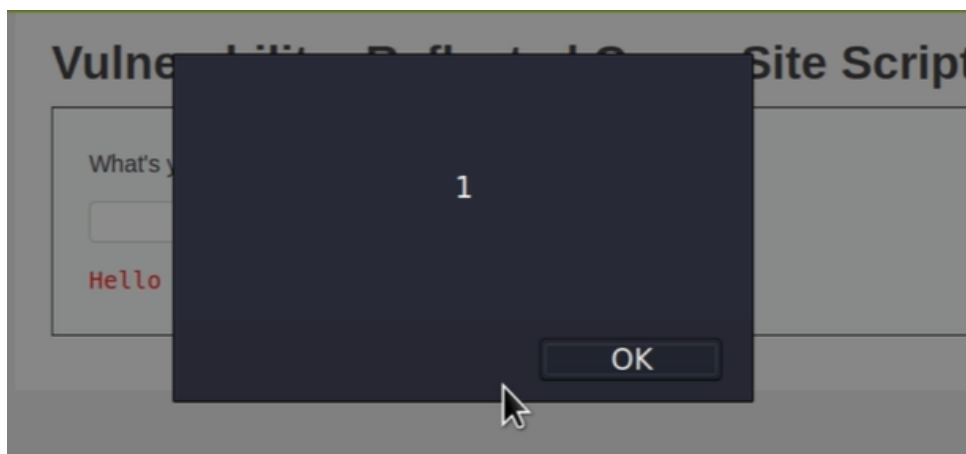
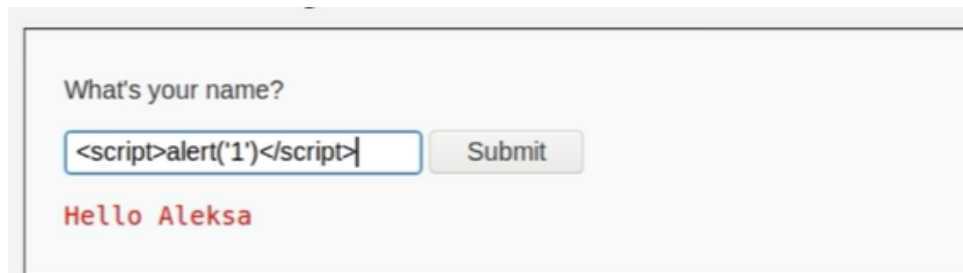
2 反射型：

2.1 LOW



用户名是通过 name 参数用 GET 方式提交的。

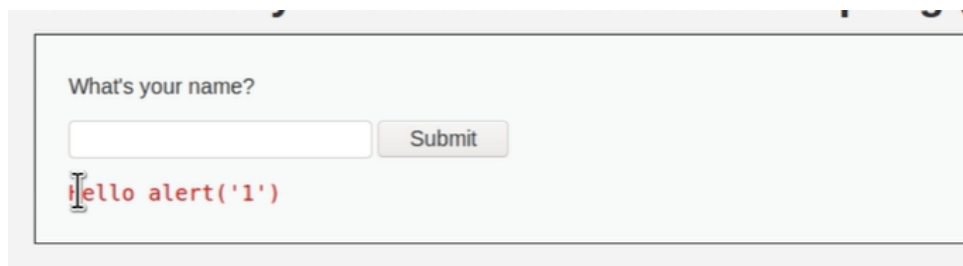
输入 XSS 攻击命令



输入的脚本嵌入到了网页中，此处存在漏洞。

2.2 MEDIUM

对输入进行了过滤



但是可以通过大小写混淆绕过。

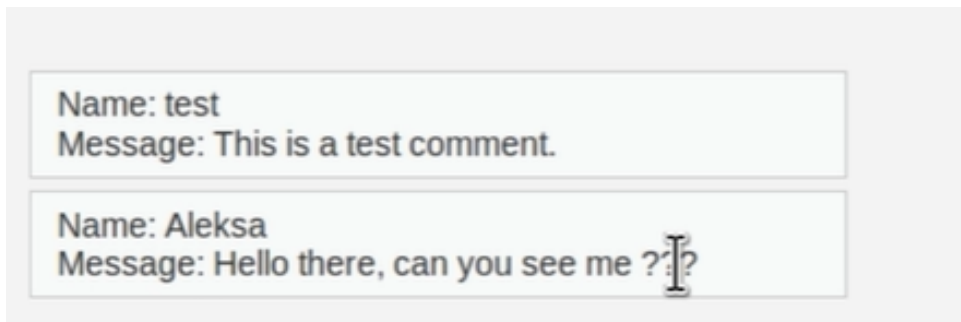


2.3 HIGH

通过 img,body 等 HTML 语言标签的事件注入恶意 js 代码。

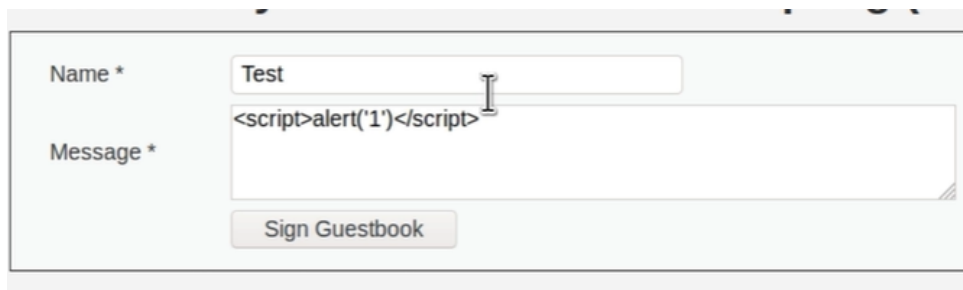
3 存储型

3.1 LOW



Name: test
Message: This is a test comment.

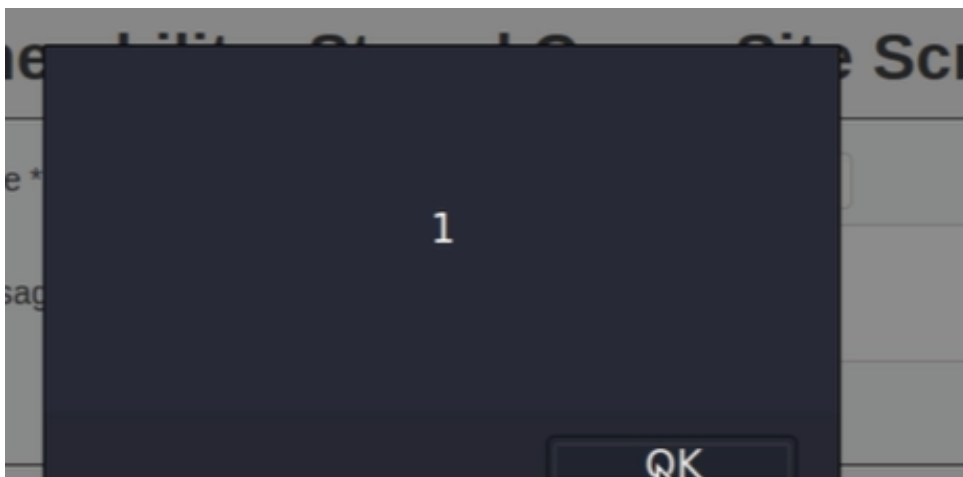
Name: Aleksa
Message: Hello there, can you see me ? :?



Name * Test

Message * `<script>alert('1')</script>`

Sign Guestbook



3.2 MEDIUM

需要通过抓包更改 name 参数，通过大小写混淆或双写绕过。

笔者这里通过 f12 修改限制字符串的长度使能够在 name 中输入。

3.3 HIGH

与反射型相同。

