某项目(实际的项目/系统名称)

安全测试报告

作者：[贰拾壹](https://github.com/er10yi)

二〇二〇年八月二十二日

目 录

[1 漏洞分类：从分类及名称文档的分类中选择一个，没有则新增（不需要修改） 1](#_Toc49029994)

[**1.1** **漏洞名称：**从分类及名称文档的漏洞名称选择一个，按实际修改名称 1](#_Toc49029995)

[2 漏洞分类：跨站脚本攻击（XSS） 3](#_Toc49029996)

[**2.1** **漏洞名称：**XSS演示页面反射型XSS 3](#_Toc49029997)

1. **漏洞分类：**从分类及名称文档的分类中选择一个，没有则新增（不需要修改）
   1. **漏洞名称：**从分类及名称文档的漏洞名称选择一个，按实际修改名称

|  |  |  |
| --- | --- | --- |
| **风险等级** | | |
| 严重，高危，中危，低危，信息（五选一） | | |
| **影响范围（可以设置多个，下面加新行即可）** | | |
| **位置** | **链接（不能插入超链接，否则脚本识别不到）** | **参数** |
| 首页-登录 | http://www.test.com | username、password |
| 位置2 | 链接2 | 参数2 |
| **描述及证明** | | |
| 漏洞复现步骤，相应的请求与响应（参数、payload等标记），证明截图等  复现步骤   |  | | --- | | Request  xxxxx | | Response  xxxx |   证明截图（如有，图片贴在画布里） | | |
| **修复方案** | | |
| 1. 修复1（行尾没有句号） 2. 修复2（行尾没有句号） | | |
| **发现时间** | | |
| 20200822 | | |
| **复测结果** | | |
| 记录复测过程，包括修复的方式，聊天截图，代码等都需要记下来，已修复或未修复，格式如下（日期加已修复证明/未修复证明）  **20200822已修复证明：**  xxx代码，或者修复截图（如有，图片贴在画布里）  或者**20200822未修复证明：** | | |

（以下是示例）

1. **漏洞分类：跨站脚本攻击（XSS）**
   1. **漏洞名称：**XSS演示页面反射型XSS

|  |  |  |
| --- | --- | --- |
| **风险等级** | | |
| 中危 | | |
| **影响范围** | | |
| **位置** | **链接** | **参数** |
| 首页-登录 | http://127.0.0.1:8080/VulnWeb/xss.jsp | username、password、resume |
| **描述及证明** | | |
| 提交<script>alert(1)</script>，发现输出结果被替换成空白，换成<svg onload=alert(1)>，输出结果为<svg alert(1)>，猜测XSS防护采用的是黑名单方式，使用<svg onclick=alert(1)>，提交后单击成功弹窗。  resume参数请求响应与触发弹窗如下   |  | | --- | | Request  POST /VulnWeb/XSSServlet HTTP/1.1  Host: 127.0.0.1:8080  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:63.0) Gecko/20100101 Firefox/63.0  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  Accept-Encoding: gzip, deflate  Referer: http://127.0.0.1:8080/VulnWeb/xss.jsp  Content-Type: application/x-www-form-urlencoded  Content-Length: 57  Connection: close  Cookie: JSESSIONID=FE12A598ACAF711E9908DED9D5D214FE  Upgrade-Insecure-Requests: 1  username=user&password=pass&resume=<svg onclick=alert(1)> | | Response  HTTP/1.1 200  Content-Type: text/html;charset=UTF-8  Content-Length: 648  Date: Mon, 31 Dec 2018 16:07:18 GMT  Connection: close  <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">  <html>  <head>  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">  <style type="text/css">  body {  text-align: center;  margin: 0px;  padding: 0px;  }  </style>  <title>show1</title>  </head>  <body>  <table border="1" cellspacing="1" width="20%">    <tr>    <td>username</td>  <td>user</td>  </tr>    <tr>    <td>password</td>  <td>pass</td>  </tr>    <tr>    <td>resume</td>  <td><svg onclick=alert(1)></td>  </tr>    </table>  </body>  </html> |   证明截图 | | |
| **修复方案** | | |
| 1. 根据不同的场景采用输出编码，此处为HTML实体，所以采用HTML实体输出编码 2. 使用黑名单作为辅助方案，将触发弹窗的标签加入黑名单 3. 严格校验数据合法性 | | |
| **发现时间** | | |
| 20200822 | | |
| **复测结果** | | |
| **20200822已修复证明：**  已增加输出编码 | | |