首轮测试后，统计测试结果，并填写以下表格：

1. **渗透测试问题统计**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **测试对象** | **超危** | **高危** | **中危** | **低危** |
| 国家重点污染源核心应用软件 | 0 | 2 | 2 | 0 |
| **合计** | **0** | **2** | **2** | **0** |

回归测试后，统计测试结果，并填写以下表格：

1. 渗透测试结果统计

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **测试对象** | **首轮测试结果** | | | | **回归测试结果** | | | |
| **超危** | **高危** | **中危** | **低危** | **超危** | **高危** | **中危** | **低危** |
| 国家重点污染源核心应用软件 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 |
| **合计** | **0** | **2** | **2** | **0** | **0** | **0** | **0** | **0** |

（1）【国家重点污染源核心应用软件-未授权访问漏洞】

|  |  |  |  |
| --- | --- | --- | --- |
| **被测对象** | 国家重点污染源核心应用软件 | **漏洞报告单编号** |  |
| **POC** | http://19.15.16.158:8080/jointframe/dwr/test/AlarmMessagePush | | |
| **漏洞类型** | 未授权访问漏洞 | | |
| **漏洞描述** | 由于没有对网站敏感页面进行登录状态、访问权限的检查，导致攻击者可未授权访问，获取敏感信息及进行未授权操作。。 | | |
| **漏洞等级** | 超危 高危 中危 低危 | | |
| **风险评估** | 攻击者可未授权访问，可能获取敏感信息及进行未授权操作. | | |
| **整改建议** | 1、页面进行严格的访问权限的控制以及对访问角色进行权限检查。  2、可以使用session对用户的身份进行判断和控制。 | | |
| **整改结果** |  | | |
| **漏洞证明** | | | |
| 1. 使用浏览器直接访问URL: http://19.15.16.158:8080/jointframe/dwr/test/AlarmMessagePush | | | |
| **整改情况记录** | | | |

（2）【国家重点污染源核心应用软件-明文传输漏洞】

|  |  |  |  |
| --- | --- | --- | --- |
| **被测对象** | 国家重点污染源核心应用软件 | **漏洞报告单编号** |  |
| **POC** | POST /jointframe/app/sso/login?service=http://19.15.16.158:8080/jointframe/app/sso/j\_sso\_spring\_security\_check HTTP/1.1  Host: 19.15.16.158:8080  User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0  Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/webp,\*/\*;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  Content-Type: application/x-www-form-urlencoded  Content-Length: 148  Origin: http://19.15.16.158:8080  Connection: close  Referer: http://19.15.16.158:8080/jointframe/app/sso/login?service=http://19.15.16.158:8080/jointframe/app/sso/j\_sso\_spring\_security\_check  Cookie: JSESSIONID=9B283592D9A4BACD862A6319556E4009; DWRSESSIONID=TjHc49AJrMTgwaKoqm\*tTVF6Wmn; UserName=zhonghailin; StylePath=../../Themes/LightBlue/LightBlue.swf; ASP.NET\_SessionId=kiphfl4sr322f1w3udbk4xur  Upgrade-Insecure-Requests: 1  username=zhonghailin&password=zhl1983&password\_show2=&password\_show1=zhl1983&lt=LT-660-Of6mCQLj1haala5Qfsb0eNQlP9svsp&execution=e2s1&\_eventId=submit | | |
| **漏洞类型** | 明文传输漏洞 | | |
| **漏洞描述** | 用户登录过程中使用明文传输用户登录信息，若用户遭受中间人攻击时，攻击者可直接获取该用户登录账户，从而进行进一步渗透. | | |
| **漏洞等级** | 超危 高危 中危 低危 | | |
| **风险评估** | 若用户遭受中间人攻击时，攻击者可直接获取该用户登录账户。 | | |
| **整改建议** | 1、用户登录信息使用加密传输，如密码在传输前使用安全的算法加密后传输，可采用的算法包括：不可逆hash算法加盐（4位及以上随机数，由服务器端产生）；安全对称加密算法，如AES(128、192、256位)，且必须保证客户端密钥安全，不可被破解或读出；非对称加密算法，如RSA(不低于1024位)、SM2等。  2、使用https来保证传输的安全。 | | |
| **整改结果** |  | | |
| **漏洞证明** | | | |
| 1.访问http://19.15.16.158:8080/jointframe/app，输入账号及密码，点击登录，抓包分析，发现密码明文传输。 | | | |
| **整改情况记录** | | | |
|  | | | |

（3）【国家重点污染源核心应用软件-XSS漏洞】

|  |  |  |  |
| --- | --- | --- | --- |
| **被测对象** | 国家重点污染源核心应用软件 | **漏洞报告单编号** |  |
| **POC** | POST /jointframe/app/org/AppPosition!save.page HTTP/1.1  Host: 19.15.16.158:8080  User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0  Accept: \*/\*  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  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  X-Requested-With: XMLHttpRequest  Content-Length: 357  Origin: http://19.15.16.158:8080  Connection: close  Referer: http://19.15.16.158:8080/jointframe/app/org/AppPosition!input.page?menuId=40288617495fd1a201495fd1c9a70001&t=20603&id=2c9ad89f75b6601b0175bb789d070000  Cookie: SSOTGC=TGT-12-mS4dupNgGCeWWRdCsYhhrQoYAnD29L3xMQHSvTWpU3AqZ5gMHe-jointframe; JSESSIONID=653157FC2E3D8613A8CB54D911CCCFC9; DWRSESSIONID=TjHc49AJrMTgwaKoqm\*tTVF6Wmn; UserName=zhonghailin; StylePath=..%2f..%2fThemes%2fLightBlue%2fLightBlue.swf; ASP.NET\_SessionId=kiphfl4sr322f1w3udbk4xur  id=2c9ad89f75b6601b0175bb789d070000&oldPositionName=111&parentId=2c95018f46b731850146d5d0e8eb0017&regionCode=445300000&createTime=2020-11-12+04%3A00%3A45&oldStatus=1&status=1&createPlatformCode=1001&oldSyncType=1&parentName=%E4%BA%91%E6%B5%AE%E5%B8%82%E7%8E%AF%E4%BF%9D%E5%B1%80&name=111&duty=11111<script>alert(/XSS/)</script>1111&displayOrder=1&syncType=1 | | |
| **漏洞类型** | XSS漏洞 | | |
| **漏洞描述** | 1、Web程序代码中对用户提交的参数未做过滤或过滤不严，导致参数中的特殊字符破坏了HTML页面的原有逻辑，攻击者可以利用该漏洞执行恶意HTML/JS代码、构造蠕虫、篡改页面实施钓鱼攻击、以及诱导用户再次登录，然后获取其登录凭证等。  2、XSS攻击对Web服务器本身虽无直接危害，但是它借助网站进行传播，对网站用户进行攻击，窃取网站用户账号身份信息等，从而也会对网站产生较严重的威胁 | | |
| **漏洞等级** | 超危 高危 中危 低危 | | |
| **风险评估** | 攻击者可以利用该漏洞执行恶意HTML/JS代码、构造蠕虫、篡改页面实施钓鱼攻击、以及诱导用户再次登录，然后获取其登录凭证等。 | | |
| **整改建议** | xss漏洞本质上是一种html注入，也就是将html代码注入到网页中。那么其防御的根本就是在将用户提交的代码显示到页面上时做好一系列的过滤与转义  　　（1）过滤输入的数据，对例如：“ ‘ ”，“ “ ”，” < “，” > “，” on\* “，script、iframe等危险字符进行严格的检查。这里的输入不仅仅是用户可以直接交互的输入接口，也包括HTTP请求中的Cookie中的变量，HTTP请求头部中的变量等。  　　（2）不仅验证数据的类型，还要验证其格式、长度、范围和内容。  　　（3）不仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。  　　（4）对输出到页面的数据进行相应的编码转换，如HTML实体编码、JS编码等。对输出的数据也要检查，数据库里的值有可能会在一个大网站的多处都有输出，即使在输入做了编码等操作，在各处的输出点时也要进行检查。 | | |
| **整改结果** |  | | |
| **漏洞证明** | | | |
| 1. 登录账号：zhonghailin密码：zhl1983，访问URL【http://19.15.16.158:8080/jointframe/app/AppMain!index.page】,在组织机构管理—岗位列表—编辑信息 2. 插入payload: <script>alert(/XSS/)</script>     3.刷新，成功触发XSS漏洞  。 | | | |
| **整改情况记录** | | | |
|  | | | |

（4）【国家重点污染源核心应用软件-存储型XSS漏洞】

|  |  |  |  |
| --- | --- | --- | --- |
| **被测对象** | 省生态环境厅国家重点污染源核心应用软件 | **漏洞报告单编号** |  |
| **POC** | POST /jointframe/app/authorize/AppRole!save.page HTTP/1.1  Host: 19.15.16.158:8080  Content-Length: 268  Accept: \*/\*  Origin: http://19.15.16.158:8080  X-Requested-With: XMLHttpRequest  User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36 SE 2.X MetaSr 1.0  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Referer: http://19.15.16.158:8080/jointframe/app/authorize/AppRole!input.page?menuId=40288617495fd1a201495fd1c9a70000&t=19203&id=2c9ad89f75b63ae40175b654cba10000  Accept-Encoding: gzip, deflate  Accept-Language: zh-CN,zh;q=0.9  Cookie: widgetState0=%5B%5D; SSOTGC=TGT-13-bRGIftGVWBvCcdYj5gv5DqeiaTidZzBJwIUhWYkBCD0g5SjX9O-jointframe; DWRSESSIONID=WYI61PfyN6Pa27WGJJVRNp$dXmn; JSESSIONID=6353C81ED7ED4F6595085329CCD724DE; UserName=zhonghailin; ASP.NET\_SessionId=lcsa0nbux25t0wuy00m415kc  Connection: close  id=2c9ad89f75b63ae40175b654cba10000&isConsole=0&createUserId=2c9598e54114f95f01412b2f61530002&oldIsConsole=0&isSuperRole=0&parentId=4028861649e521190149e5236cae0000&name=%E6%B5%8B%E8%AF%95%E7%94%A8%E6%88%B7&status=1&describe=%3Cscript%3Ealert(%2Fxss%2F)%3C%2Fscript%3E | | |
| **漏洞类型** | XSS漏洞 | | |
| **漏洞描述** | 1、Web程序代码中对用户提交的参数未做过滤或过滤不严，导致参数中的特殊字符破坏了HTML页面的原有逻辑，攻击者可以利用该漏洞执行恶意HTML/JS代码、构造蠕虫、篡改页面实施钓鱼攻击、以及诱导用户再次登录，然后获取其登录凭证等。  2、XSS攻击对Web服务器本身虽无直接危害，但是它借助网站进行传播，对网站用户进行攻击，窃取网站用户账号身份信息等，从而也会对网站产生较严重的威胁。 | | |
| **漏洞等级** | 超危 高危 中危 低危 | | |
| **风险评估** | 攻击者可以利用该漏洞执行恶意HTML/JS代码、构造蠕虫、篡改页面实施钓鱼攻击、以及诱导用户再次登录，然后获取其登录凭证等。 | | |
| **整改建议** | xss漏洞本质上是一种html注入，也就是将html代码注入到网页中。那么其防御的根本就是在将用户提交的代码显示到页面上时做好一系列的过滤与转义  （1）过滤输入的数据，对例如：“ ‘ ”，“ “ ”，” < “，” > “，” on\* “，script、iframe等危险字符进行严格的检查。这里的输入不仅仅是用户可以直接交互的输入接口，也包括HTTP请求中的Cookie中的变量，HTTP请求头部中的变量等。  　　（2）不仅验证数据的类型，还要验证其格式、长度、范围和内容。  　　（3）不仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。  （4）对输出到页面的数据进行相应的编码转换，如HTML实体编码、JS编码等。对输出的数据也要检查，数据库里的值有可能会在一个大网站的多处都有输出，即使在输入做了编码等操作，在各处的输出点时也要进行检查。  （5）修复时过滤方案全局覆盖 | | |
| **整改结果** |  | | |
| **漏洞证明** | | | |
| 1、访问http://19.15.16.158:8080/jointframe/app/AppMain!index.page  登录账号：zhonghailin密码：zhl1983  2、在角色管理-修改。    3、点击修改，修改数据包，插入payload：<script>alert(/XSS/)</script>    4、成功触发存储型XSS漏洞    5、全局存在XSS，修复时过滤方案全局覆盖 | | | |
| **整改情况记录** | | | |
|  | | | |