光大国际环保监测平台

渗透测试报告



|  |  |  |  |
| --- | --- | --- | --- |
| **文件类型** | **项目文档** | **密级** | **商业秘密** |
| **编 制 人** | **连岳钦** | **版本** | **V1.0** |
| **审核人** | **朱奕森** | **审批日期** | **2019年10月8日** |
| **批准人** | **朱奕森** | **批准日期** | **2019年10月8日** |

**北京天融信网络安全技术有限公司**

**2019年10月8日**

**文档修订**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **日期** | **修改人员** | **描述** | **审核人员** |
| 1.0 | 2019年10月8日 | 连岳钦 | 创建 |  |
|  |  |  |  |  |

**版权说明**

本文件中出现的全部内容,除另有特别注明,版权均属**北京天融信网络安全技术有限公司**所有。任何个人、机构未经北京天融信网络安全技术有限公司书面授权许可,不得以任何方式复制或引用文件的任何片断。

**保密申明**

本文件包含了来自**北京天融信网络安全技术有限公司**的可靠、权威的信息,以及被检测单位信息系统的敏感信息,接受这份文件表示同意对其内容保密并且未经**北京天融信网络安全技术有限公司**书面请求和书面认可,不得复制,泄露或散布这份文件。如果你不是有意接受者,请注意对这份文件内容的任何形式的泄露、复制或散布都是被禁止的。

**摘要**

本文件是北京天融信网络安全技术有限公司对光大国际环保监测平台进行安全渗透的测试报告。这里对本次渗透测试结果所得出的整体安全情况作概括描述,文件正文为全面的分析。

本次渗透测试主要采用专家人工测试的方法,采用了部分工具作为辅助。在渗透测试中我们发现：光大国际环保监测平台在前台应用层存在一定的安全问题。

结论：整体而言,光大国际环保监测平台在本次渗透测试实施期间的安全风险状况为“**预警状态**”。(系统安全风险状况等级的含义及说明详见附录A)。

**目录**

[第一章 项目信息 5](#_Toc21425233)

[1.1 委托单位信息 5](#_Toc21425234)

[1.2 测试单位信息 5](#_Toc21425235)

[第二章 项目概述 6](#_Toc21425236)

[2.1 测试目的 6](#_Toc21425237)

[2.2 测试范围 6](#_Toc21425238)

[2.3 测试过程 6](#_Toc21425239)

[第三章 安全漏洞归纳 7](#_Toc21425240)

[3.1 XSS跨站脚本执行漏洞 7](#_Toc21425241)

[3.2 信息泄露 8](#_Toc21425242)

[3.3 物理路径泄露 8](#_Toc21425243)

[第四章 综合分析 10](#_Toc21425244)

[4.1 安全概况 10](#_Toc21425245)

[4.2 整体安全建议 10](#_Toc21425246)

[4.3 下一步工作 11](#_Toc21425247)

[附录A. 安全风险状况等级说明 12](#_Toc21425248)

# 第一章 项目信息

## 1.1 委托单位信息

|  |  |  |  |
| --- | --- | --- | --- |
| **单位名称** |  | | |
| **委托项目名称** |  | | |
| **单位地址** |  | | |
| **邮政编码** |  | | |
| **联系人** |  | **联系电话** |  |
| **联系人EMAIL** |  | | |

## 1.2 测试单位信息

|  |  |  |  |
| --- | --- | --- | --- |
| **单位名称** | 北京天融信网络安全技术有限公司 | | |
| **单位地址** | 北京市海淀区上地东路一号华控大厦2层 | | |
| **单位网址** | www.topsec.com.cn | | |
| **邮政编码** | 100085 | | |
| **联系人** |  | **联系电话** |  |
| **联系人EMAIL** |  | | |
| **参与本次测试成员: 连岳钦** | | | |

# 第二章 项目概述

## 2.1 测试目的

通过本项目的成功实施，在坚持科学、客观、公正原则的基础上，全面、完整地了解当前光大国际环保监测平台系统的安全状况，分析系统所面临的各种风险，模拟攻击者可能利用的漏洞，根据测试结果发现系统存在的安全问题，并对严重的问题提出加固的建议。

## 2.2 测试范围

本次渗透测试的范围如下

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **备注** |
| 1 | 光大国际环保监测平台 | http://10.10.52.124:13298/jointos/app/AppMain!index.page |

## 2.3 测试过程

2019年10月6日至2019年10月7日，进行渗透测试；

2019年10月8日进行报告撰写。

# 第三章 安全漏洞归纳

## 3.1 XSS跨站脚本执行漏洞

**漏洞位置**

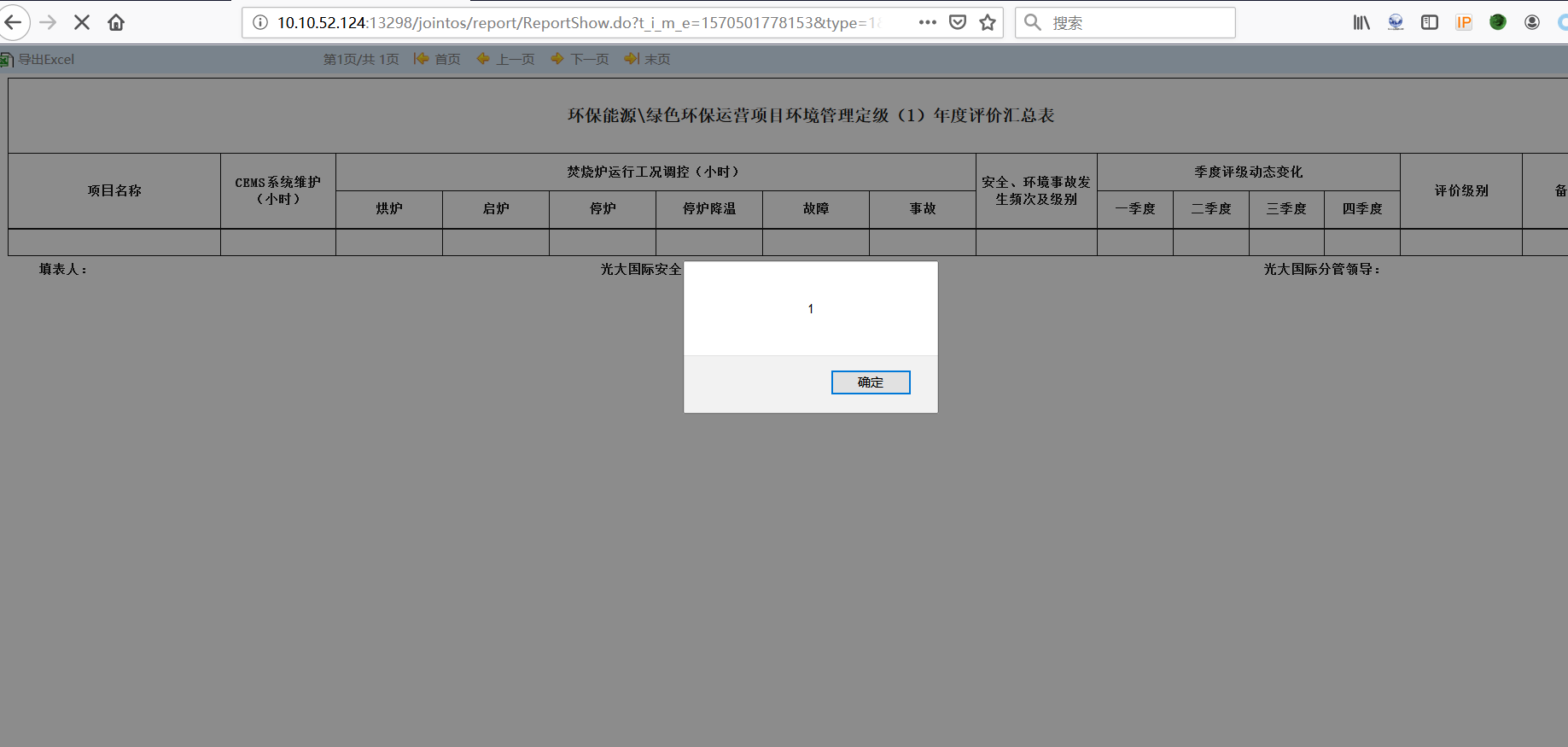
http://10.10.52.124:13298/jointos/report/ReportShow.do?t\_i\_m\_e=1570501778153&type=1&retype=1&report=report5.raq&psPlateCode=&psModuleCode=%22%3e%3csvg%2fonload%3dalert%281%29%3e&psId=&year=1&\_\_beanName=1570501777847\_reportBean&report1\_currPage=1&report1\_cachedId=A\_1059%27

存在问题参数：report、psPlateCode、psModuleCode

**漏洞描述**

渗透测试人员发现，通过插入xss代码，访问以下链接，成功执行

http://10.10.52.124:13298/jointos/report/ReportShow.do?t\_i\_m\_e=1570501778153&type=1&retype=1&report=report5.raq&psPlateCode=&psModuleCode=%22%3e%3csvg%2fonload%3dalert%281%29%3e&psId=&year=1&\_\_beanName=1570501777847\_reportBean&report1\_currPage=1&report1\_cachedId=A\_1059%27



**漏洞建议**

对所有用户提交内容进行可靠的输入验证，包括对URL、查询关键字、HTTP头、REFERER、POST数据等，仅接受 指定长度范围内、采用适当格式、采用所预期的字符的内容提交，对其他的一律过滤。尽量采用POST 而非GET 提交表单；对"<"，">",";","'"，"javascript"，"jscript"，"vbscript"等字符做过滤。

1.在HTML/XML中显示"用户可控数据"前，应该进行html escape转义。

2.在javascript内容中输出的"用户可控数据"，需要做javascript escape转义。

3.对输出到富文本中的"用户可控数据"，做富文本安全过滤（允许用户输出HTML的情况）。

4.输出在url中的数据，做url安全输出。

**脆弱性评价：**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 严重程度 | 高 |  | **中** | **■** | 低 |  |

## 3.2 信息泄露

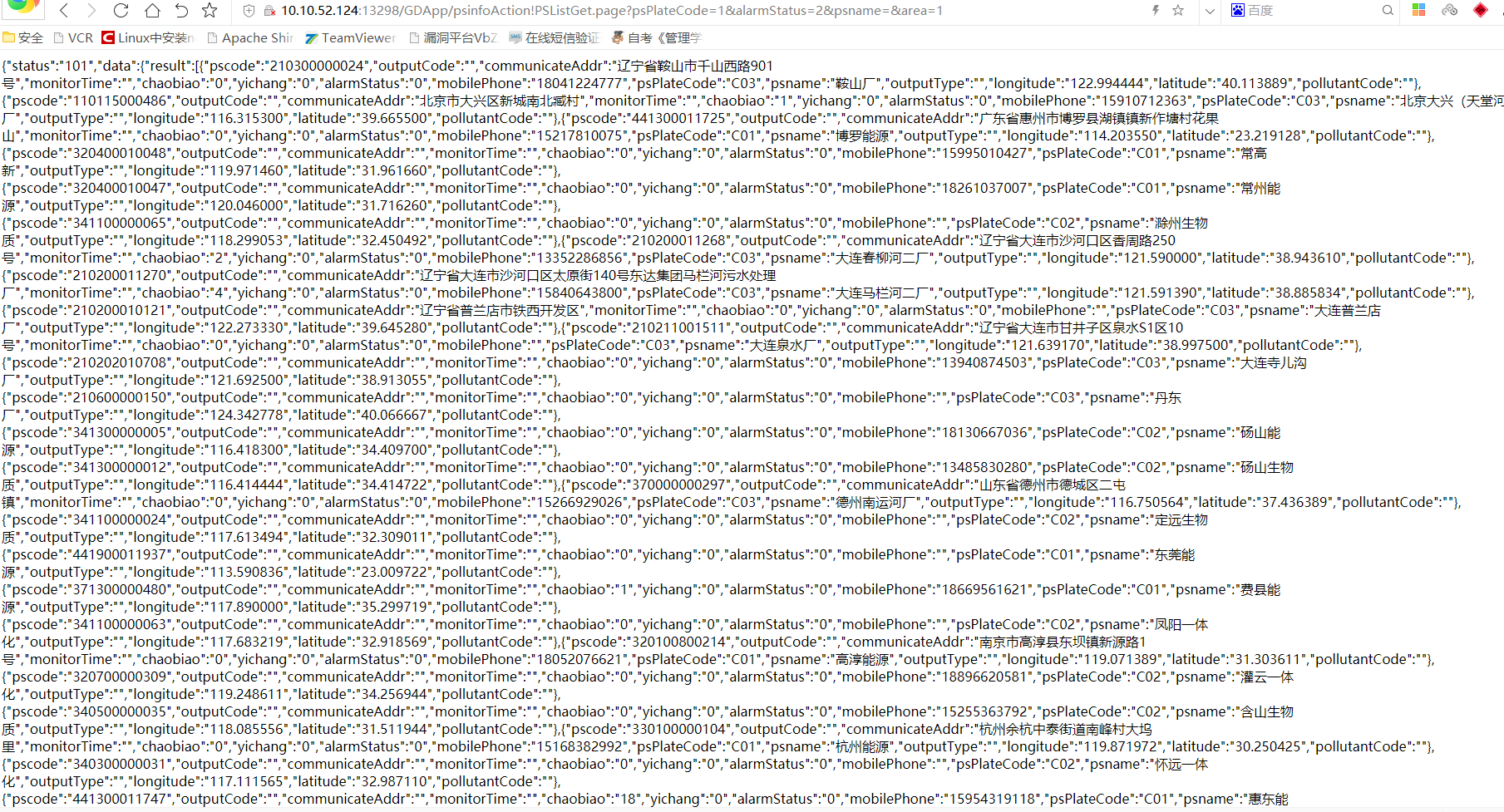
**漏洞位置**

<http://10.10.52.124:13298/GDApp/psinfoAction!PSListGet.page?psPlateCode=1&alarmStatus=2&psname=&area=1>

**漏洞描述**

渗透测试人员发现，无需登录系统，即可访问此url出现系统内部信息

<http://10.10.52.124:13298/GDApp/psinfoAction!PSListGet.page?psPlateCode=1&alarmStatus=2&psname=&area=1>



**漏洞建议**

如无必要，进行屏蔽，或者校验是否登录账号才能进行访问

**脆弱性评价：**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 严重程度 | 高 |  | **中** | **■** | 低 |  |

## 3.3 物理路径泄露

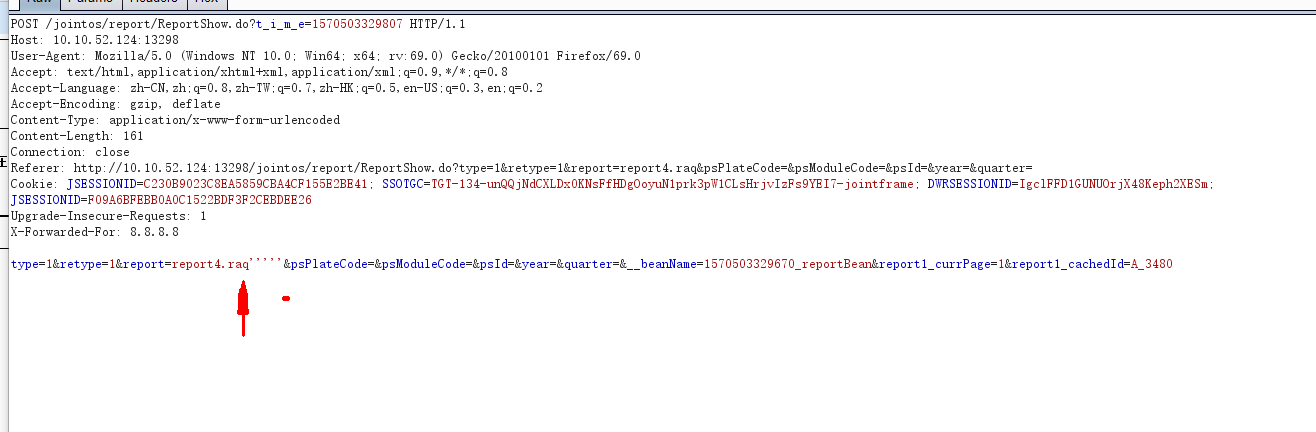
**漏洞位置**

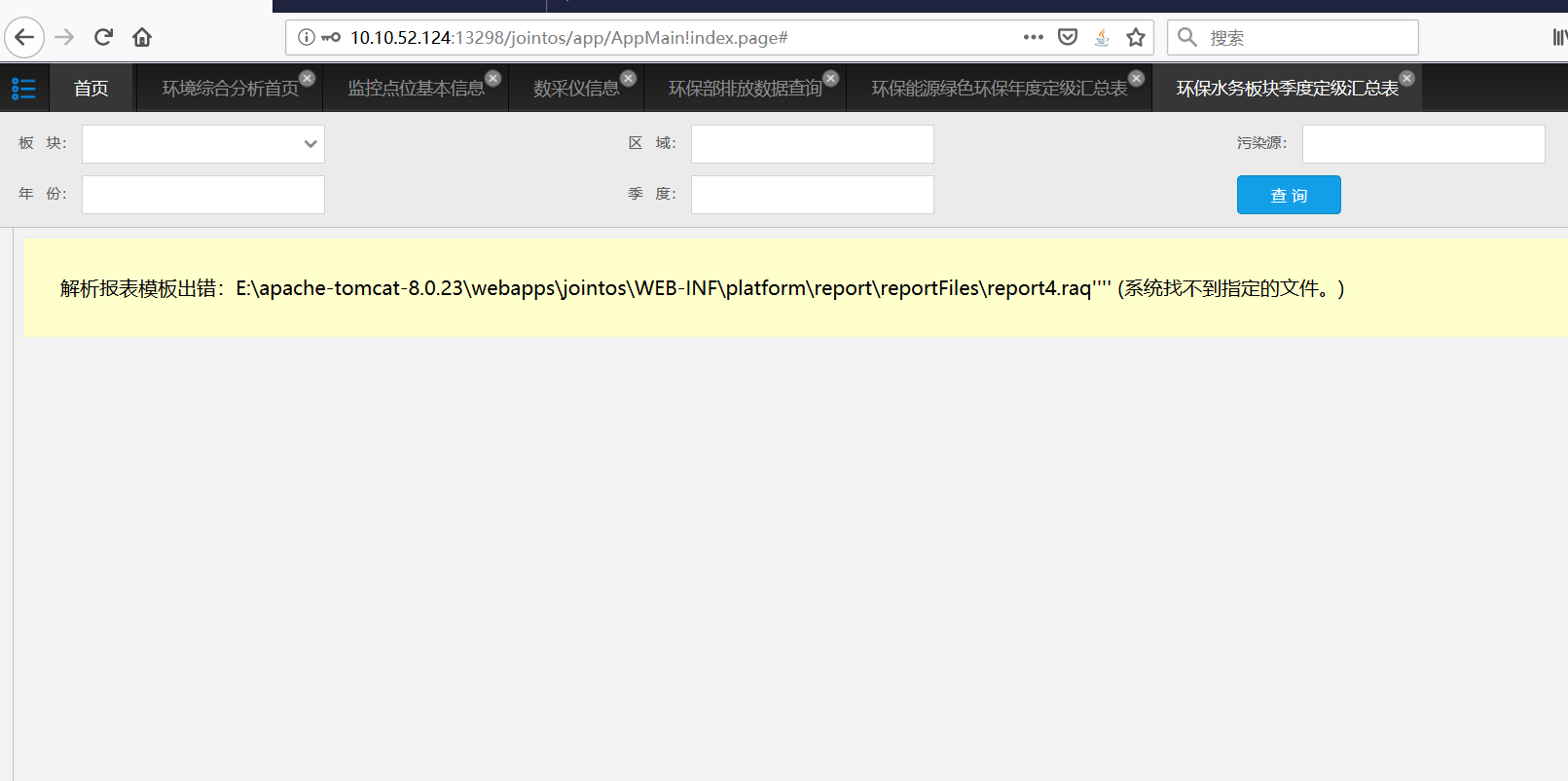
http://10.10.52.124:13298/jointos/report/ReportShow.do?t\_i\_m\_e=1570503329807

**漏洞描述**

渗透测试人员发现，通过使网站报错，出现了网站的物理路径泄露

http://10.10.52.124:13298/jointos/report/ReportShow.do?t\_i\_m\_e=1570503329807





**漏洞建议**

屏蔽物理路径

**脆弱性评价：**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 严重程度 | 高 |  | 中 |  | **低** | **■** |

# 第四章 综合分析

在测试过程中，通过对网站、应用的远程信息收集，风险和漏洞的分析，发现光大国际环保监测平台目前的应用和管理存在着一些风险，对于发现的具体问题，已经在前面的相应章节进行了详细的描述，并针对具体问题提出了初步建议，在此不再赘述。

针对渗透过程中发现的问题，项目组对主要的安全风险进行了分类总结。对于所识别出的各类安全风险，处理方式有四种，即预防、避免、降低、转移和接受，但对于整个系统而言，风险不可能完全被消灭。在风险识别后，应按照风险程度的轻重缓急、机构安全需求、机构自身的发展需要、安全测试的结果等众多因素，实施处理风险的各类措施。控制措施的选择应兼顾技术，并考虑发展战略、人员素质，并特别关注成本与风险的平衡。

## 4.1 安全概况

**总体安全状态：预警状态**

**总体风险描述：**

通过本次规范性测试可以看到，光大国际环保监测平台采取了一定的防护措施，但是依旧存在一定的安全问题。

因此，我们认为在渗透测试期间，光大国际环保监测平台的总体安全状态为**预警状态**，建议立刻采取措施。

## 4.2 整体安全建议

⚫ 对内网各种服务的弱口令现象进行排查。

⚫ 对所有中间件进行降权处理，避免使用管理员等高权限账号启动。

⚫ 对所有用户提交的变量进行严格的SQL、XSS、XXE等漏洞关键字过滤。

⚫ 严格检查Apache、Tomcat、Weblogic、IIS等中间件的配置。

⚫ 升级中间件、服务器应用软件为较新版本、及时更新补丁。

⚫ 增强敏感信息的安全防护以及安全加密方式。

⚫ 对所有用户的操作进行Session身份验证。

⚫ 对所有用户的URL进行Token、Referer头校验，防止CSRF。

⚫ 尽量启用HTTPS传输敏感信息。

⚫ 用户所有的提交一律经过WEB应用的软WAF过滤，或者加一道防火墙。

⚫ 及时停止掉不常用的、过时的业务系统。

⚫ 进一步加强管理人员安全意识，防止人为操作原因导致的安全隐患

## 4.3 下一步工作

安全问题日新月异，为了应对这种高频率的变化及威胁，我们建议建立起科学规范的信息安全体系，包括全面的安全管理体系建设以及专业的信息安全服务，周期性的进行安全评估、安全培训以及安全审计，使用更新更有效的安全产品，这样才能与时俱进的做好信息安全防范工作，建立更完善的信息安全防护体系结构，为将来的业务发展打造良好的基础。

# 附录A. 安全风险状况等级说明

| **安全风险状况说明** | |
| --- | --- |
| **1** | **良好状态**  信息系统处于良好运行状态，没有发现或只存在零星的低风险安全问题，此时只要保持现有安全策略就满足了本系统的安全等级要求。 |
| **2** | **预警状态**  信息系统中存在一些漏洞或安全隐患，此时需根据评估中发现的网络、主机、应用和管理等方面的问题对进行有针对性的加固或改进。 |
| **3** | **严重状态**  信息系统中发现存在严重漏洞或可能严重威胁到系统正常运行的安全问题，此时需要立刻采取措施，例如安装补丁或重新部署安全系统进行防护等等。 |
| **4** | **紧急状态**  信息系统面临严峻的网络安全态势，对组织的重大经济利益或政治利益可能造成严重损害。此时需要与其他安全部门通力协作采取紧急防御措施。 |