光大环保

信息安全服务项目

web应用安全扫描报告

光大国际网站及环境公示网站



北京天融信网络安全技术有限公司

安全服务部

2019年11月

文档控制

|  |  |  |  |
| --- | --- | --- | --- |
| 框架版本： |  | V0.93 |  |
| 文档创建： | 2019.11.13 | V1.0 |  |
| 文档修订： |  | V1.1 |  |
| 标 准 化： |  |  |  |
| 读 者： |  |

保密申明

这份文档涉及到天融信公司的商业秘密信息。接受这份说明书表示同意对其内容保密，未经书面请求并得到天融信公司的书面认可，不得复制，泄露或散布这份文档。如果你不是有意接受者，请注意对这份文档内容的任何形式的泄露、复制或散布都有可能引起法律纠纷。

目 录

[一、 安全扫描信息 1](#_Toc24646360)

[1.1、 扫描目的 1](#_Toc24646361)

[1.2、 扫描范围 1](#_Toc24646362)

[1.3、 扫描过程 1](#_Toc24646363)

[二、 漏洞详细情况 2](#_Toc24646364)

[2.1、 （高危）Sql注入 2](#_Toc24646365)

1. 安全扫描信息
	1. 扫描目的

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，根据验证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。

* 1. 扫描范围

本次web应用安全扫描的范围如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **内网URL** |
| 1 | 光大国际网站及环境公示网站 | <https://10.10.52.29:8090/EM4/cn/index.php> |

* 1. 扫描过程

2019年11月12日，进行内网web应用扫描；

2019年11月13日进行漏洞验证；

2019年11月13日进行报告撰写。

1. 漏洞详细情况
	1. （高危）Sql注入

**影响页面**

https://10.10.52.29:8090/EM4/cn/index.php?a=index&cid=if(now()=sysdate()%2Csleep(0)%2C0)&m=index

**漏洞描述**

所谓SQL注入，就是通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。具体来说，它是利用现有应用程序，将（恶意）SQL命令注入到后台数据库引擎执行的能力，它可以通过在Web表单中输入（恶意）SQL语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行SQL语句。 造成SQL注入漏洞原因有两个：一个是没有对输入的数据进行过滤（过滤输入），还有一个是没有对发送到数据库的数据进行转义（转义输出）。

https://10.10.52.29:8090/EM4/cn/index.php?a=index&cid=if(now()=sysdate()%2Csleep(10)%2C0)&m=index



**修复建议**

1)对用户输入的特殊字符进行严格过滤，如’、”、<、>、/、\*、;、+、-、&、|、(、)、and、or、select、union。

2)使用参数化查询（PreparedStatement），避免将未经过滤的输入直接拼接到SQL查询语句中。

3)Web应用中用于连接数据库的用户与数据库的系统管理员用户的权限有严格的区分（如不能执行drop等），并设置Web应用中用于连接数据库的用户不允许操作其他数据库。

4)设置Web应用中用于连接数据库的用户对Web目录不允许有写权限。

5)使用Web应用防火墙。