电子病历渗透测试报告

版本说明

修订人	修订内容	修订时间	版本号	审阅人

文档信息

文档名称	文档版本	文档编号	保密级别
xxx 渗透测试报告	V1.1	XXXX-ST-20180627	项目组公开

目录

1. 综述 1

1.1. 测试方案 1

1.2. 测试范围 1

1.3. 测试内容 2

1.4. 测试流程 4

2. 内网漏洞汇总 5

2.1. 漏洞等级分布 5

2.2. 漏洞类型分布 5

2.3. 漏洞结果列表 6

3. 渗透测试结果分析 7

3.1. 生产服务器区 7

3.1.1. 服务器存在弱口令可直接登录域控服务器【严重】 7

3.1.2. 数据库存在弱口令【严重】 12

3.1.3. FTP 存在弱口令【高危】 15

3.2. B/S 应用区 17

3.2.1. 电子病历查询系统存在 SQL 注入【严重】 17

3.2.2. 网强系统存在 S2-016 远程代码执行漏洞【严重】 20

3.2.3. 盈高管理系统越权登录【高危】 21

3.3. C/S 应用区 22

3.3.1. 维护工具代码未加壳【中危】 22

3.3.2. 虚拟平台存在弱口令【高危】 23

4. 附录 A：漏洞风险评级标准 24

5. 附录 B：应用系统风险评级标准 25

6. 附录 D：漏洞测试工具简介 25

6.1. Sqlmap 注入工具 25

6.2. BurpSuite 代理工具 25

6.3. Firefox hackbar 插件 25

6.4. WebSOC 网站安全立体监控系统.....26
6.5. Pocsuite 开源远程漏洞测试框架 26
6.6. 渗透测试人员专用工具包.....26
7. 附录 E 研发技能表 v3.0 26

1. 综述

本次报告有效测试时间是从 2018 年 6 月 14 日开始到 2018 年 6 月 29 日结束，在此期间针对 xxx 的安全性和完整性进行测试并以此作为报告统计依据。

本次对 xxx 进行安全测试，总共发现问题 49 个，其中**严重问题 4 个**，**高危问题 3 个**，**中危漏洞 1 个**，**低危漏洞 0 个**。这些问题导致攻击者可轻易从通过破解 wifi 密码连接到内网系统，导致服务器个人电脑被入侵，最终渗透到核心服务器。因此，此次对 xxx 测试结论是**严重-不安全系统**。

由于本次测试过程中为生产系统,采用保守测试方法,生产环境评估为高风险操作的的功能,均与 xxx 相关接口人进行沟通,并在操作风险可控的情况下进行相关测试操作,以规避测试过程中的生产运营风险。

1.1. 测试方案

抵达客户现场，利用访客 wifi 渗透进办公区网络，并在该办公网络中收集 ip 资产、拓扑信息、其他数字信息等，挖掘资产漏洞，然后绕过防火墙限制，最终实现对内网服务器进行控制。

1.2. 测试范围

此次安全测试包含 xxx 节点，如下图所示。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。

如要下载或阅读全文，请访问：

https://d.book118.com/575040243333011303