南京微盟电子有限公司

渗透测试报告

中电长城网际系统应用有限公司

2020 年 07 月 30 日

中电长城网际
CYBERSPACE GREAT WALL

文档信息

项目名称			
文档名称	南京微盟电子有限公司渗透测试报告		
文档编号			
文件类型	项目文档		
创 建 人	芦佳	**版本**	1.2
审 核 人	印钰	**审核日期**	2020-07-29
批 准 人		**批准日期**	2020-07-30
接 收 方		**接收日期**	

文档修订

版本	日期	修改人员	描述	审核人员
1.0	2020-07-28	芦佳	创建	
1.2	2020-07-30	印钰	修订	

目　　录

一. 综述

经南京微盟电子有限公司授权，中电长城网际系统应用有限公司于 2020-07-28 至 2020-07-30 对南京微盟电子有限公司进行了安全渗透测试。

本次测试发现南京微盟电子有限公司门户网站在当前安全防护体系下共存在 2 个 Web 应用漏洞和 3 个业务逻辑漏洞。

漏洞汇总如下:

漏洞级别	数量（个）	漏洞类型
高危漏洞	2	WEB 应用漏洞
	3	业务逻辑漏洞

整体而言，系统在本次渗透测试实施期间的安全风险状况为“紧急状态”。(系统安全风险状况等级的含义及说明详见附录 A)。详细测试结果如下:

测试分类	测试项	测试结果
业务逻辑漏洞	验证码缺陷	未检出
	用户名枚举	未检出
	暴力破解风险	未检出
	用户弱口令	未检出
	用户登录绕过	存在
	会话标志固定攻击	未检出
	平行越权访问	未检出

	垂直越权访问	未检出
	未授权访问	未检出
	业务逻辑漏洞	未检出
	短信炸弹	未检出
	任意用户密码修改/重置	存在
	管理后台泄露	存在
	备份文件	未检出
	内网 IP 泄露	未检出
网络漏洞	域传送漏洞	未检出
	SNMP 使用默认团体字	未检出
	DNS 服务允许递归查询	未检出
	存在可被反射式拒绝服务攻击利用的服务	未检出
系统漏洞	Heartbleed'心脏出血'漏洞	未检出
	MS08-067 漏洞	未检出
	MS17-010 漏洞	未检出
	CVE-2019-0708 Windows RDP 服务高 RCE 漏洞	未检出
	CVE-2020-1350 Windows DNS 服务器 RCE 漏洞	未检出
	其他 Windows 操作系统漏洞	未检出
	Linux Dirtycow'脏牛'本地提取漏洞	未检出
	Linux Shellshock'破壳'远程执行漏洞	未检出
	CVE-2017-7494 Samba 远程执行漏洞	未检出
	远程桌面弱口令	未检出
	FTP 匿名登录/弱口令	未检出
	SSH 服务弱口令	未检出
	VNC 服务弱口令	未检出
	TELNET 弱口令	未检出
中间件漏洞	中间件后台暴露	未检出
	中间件后台弱口令	未检出
	Websphere 反序列化命令执行	未检出

	Weblogic 反序列化命令执行	未检出
	Jenkins 远程命令执行	未检出
	JBoss 远程代码执行	未检出
	PHP 文件解析代码执行	未检出
	HTTP.sys 远程代码执行漏洞	未检出
	Apache Struts2 远程命令执行	未检出
	Apache Shiro 反序列化漏洞	未检出
	Hadoop Yarn REST API 未授权漏洞	未检出
	Zookeeper 未授权访问	未检出
	Spring 框架远程执行漏洞	未检出
	PHP 版本过低导致多个漏洞	未检出
	Flash 跨域漏洞	未检出
	Flash 未混淆导致反编译	未检出
	IIS 短文件名泄露	未检出
	Apache Tomcat 示例目录漏洞	未检出
	调试模式已启用	存在
	SSL/TLS 存在 Bar Mitzvah Attack 漏洞（RC4 密码套件）	未检出
	SSL/TLS 存在 FREAK 攻击漏洞（CVE-2015-0204）	未检出
	SSL 3.0 POODLE 攻击信息泄露漏洞(CVE-2014-3566)	未检出
	不安全的 HTTP 方法	未检出
数据库漏洞	数据库弱口令	未检出
	Redis 未授权访问	未检出
	MongoDB 未授权访问	未检出
	Elasticsearch 服务未授权访问	未检出
	MYSQL 登录绕过	未检出
WEB 应用漏洞	SQL 注入漏洞	存在
	存储型跨站脚本攻击(XSS)	未检出

	反射型跨站脚本攻击(XSS)	未检出
	XML 外部实体(XXE)注入	未检出
	跨站点伪造请求(CSRF)	未检出
	服务器端请求伪造(SSRF)	未检出
	发现 WEBSHELL	未检出
	任意文件下载	未检出
	任意文件删除	未检出
	本地/远程文件包含	未检出
	URL 重定向	未检出
	文件上传漏洞	未检出
	目录遍历	未检出
	.svn/.git 源代码泄露	未检出
	. DS_Store 文件泄漏	未检出
	. idea 目录信息泄露	未检出
	WEB-INF/web.xml 泄露	未检出
	CRLF 注入	未检出
	命令执行注入	未检出
	框架注入漏洞	未检出
	链接注入漏洞	未检出
	JsonP 劫持	未检出
	第三方组件漏洞	未检出
	缺少“X-XSS-Protection”头	未检出
	HTML 表单无 CSRF 保护	未检出
	使用 GET 方式进行用户名密码传输	未检出
	X-Frame-Options Header 未配置	未检出
	绝对路径泄露	未检出
	未设置 HTTPONLY	未检出
	X-Forwarded-For 伪造	未检出
	用户凭据明文传输	未检出

	PHPINFO 页面泄露	未检出
	敏感信息泄露	未检出

二. 项目信息

2.1 委托单位信息

单位名称	南京微盟电子有限公司		
委托项目名称			
单位地址			
邮政编码		**传真**	
联系人	余强	**联系电话**	18626455710
联系人 E-MAIL			

2.2 测试单位信息

单位名称	中电长城网际系统应用有限公司		
单位地址	北京市海淀区昆明湖南路 51 号中关村军民融合产业园 B 栋 111		
单位网址	https://www.cecgw.cn		
邮政编码	100015	**传真**	
联系人	赵唯乐	**联系电话**	13911259492
联系人 E-MAIL	zhaoweile@cecgw.cn		
参与本次测试小组成员有：芦佳、刘博			

三. 项目概述

3.1 测试目的

通过渗透测试，全面、完整地了解南京微盟电子有限公司主站当前的安全状况，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。

3.2 测试范围

本次渗透测试的范围如下：

序 号	名 称	备 注
1	南京微盟电子有限公司主站	

3.3 测试依据

安全测试服务将参考下列规范进行工作。

- 信息安全技术 信息安全风险评估规范（GB/T 20984-2007）
- 信息技术 信息安全管理实用规则（GB/T 19716-2005)(ISO/IEC 17799:2000)
- 信息技术 安全技术 信息安全管理实用规则（GB/T 22081-2016 ）
- GB T 31509-2015 信息安全技术 信息安全风险评估实施指南
- 信息系统审计标准（ISACA）
- OWASP OWASP_Testing_Guide_v3
- OWASP OWASP_Development_Guide_2005
- OWASP OWASP_Top_10_2010_Chinese_V1.0

3.4 测试工具

- ◆ 网络分析工具：Traceroute、Nslookup 等
- ◆ 自动化扫描工具：Nessus、AIScanner 等
- ◆ 端口扫描、服务检测：Nmap、Masscan 等
- ◆ 漏洞利用工具：Metasploit Framework 等
- ◆ 应用缺陷分析工具：Burp Professional、SQLMAP 等

四. 测试详情

4.1 业务逻辑漏洞

4.1.1 管理后台泄露

4.1.1.1 漏洞概述

WEB 系统后台暴露在互联网上，攻击者可以如果掌握管理员密码或者绕过登录认证，可以直接访问系统后台，对系统进行篡改。

4.1.1.2 测试结果

1、发现后台管理员登陆页面

http://www.microne.com.cn/admin/Login.aspx

2、登录可以绕过


后台登陆界面
/*'or'='or'*/
确 定
取 消


南京微盟电子有限公司- 后台管理
不安全 | microne.com.cn/admin/Indexs.aspx
南京微盟电子有限公司
内容管理
产品介绍
应用与方案
质量检测
招聘列表
会员列表
订单列表
网站设置
我的桌面
欢迎使用玛迪科技后台管理

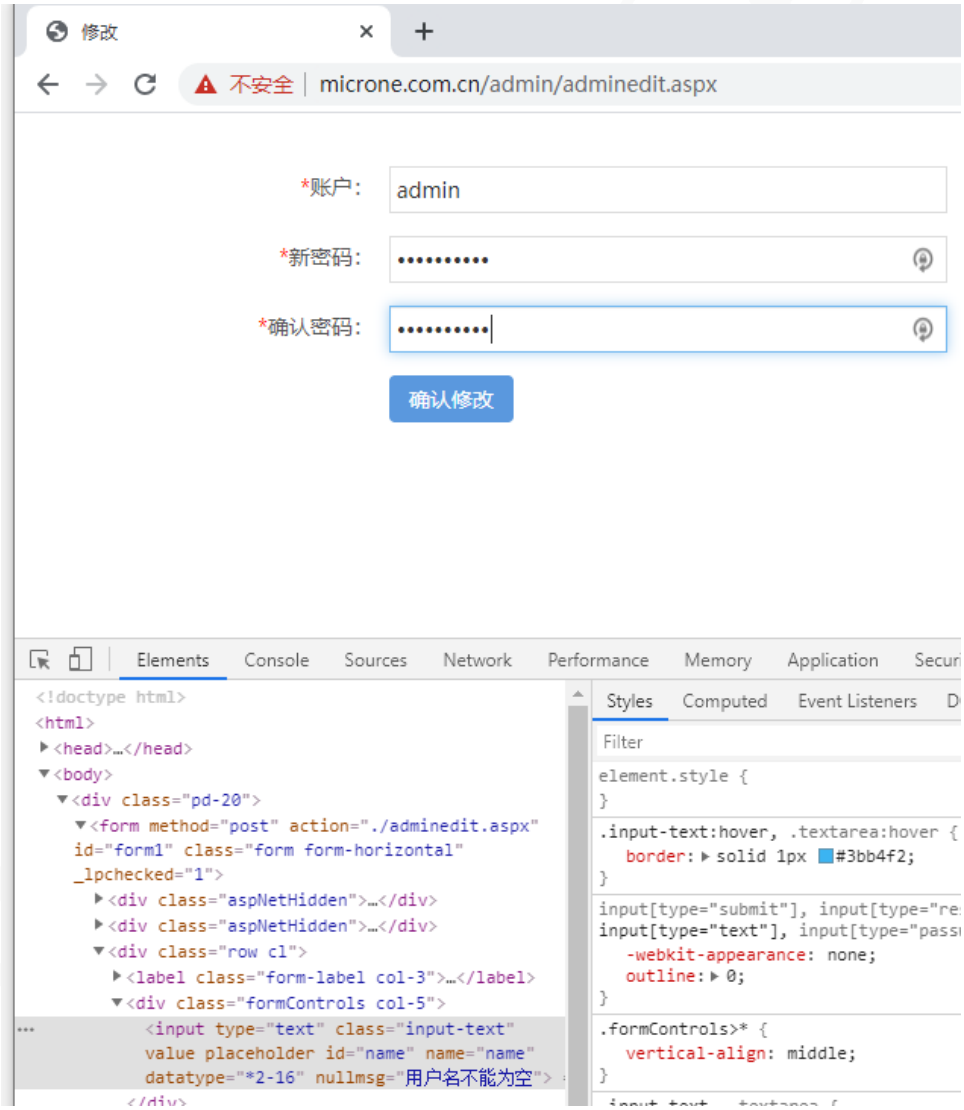
4.1.2 任意用户密码修改/重置

4.1.2.1 漏洞概述

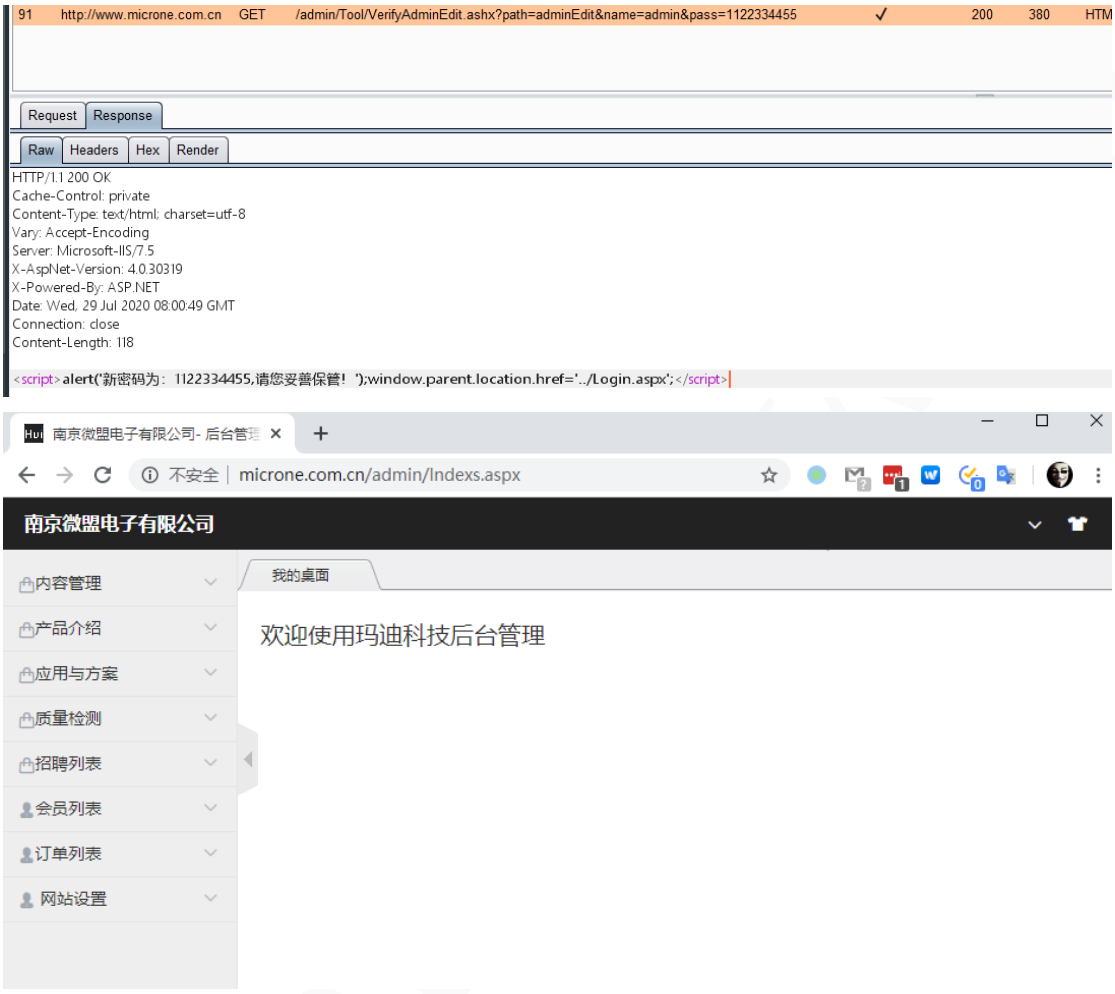
密码重置功能存在逻辑漏洞，没有有效校验用户身份，可导致任意用户重置其他用户的密码，从而登录进入系统。

4.1.2.2 测试结果

http://www.microne.com.cn/admin/adminedit.aspx



可以直接设置管理员密码并且进行登录



4.1.3 用户登录绕过

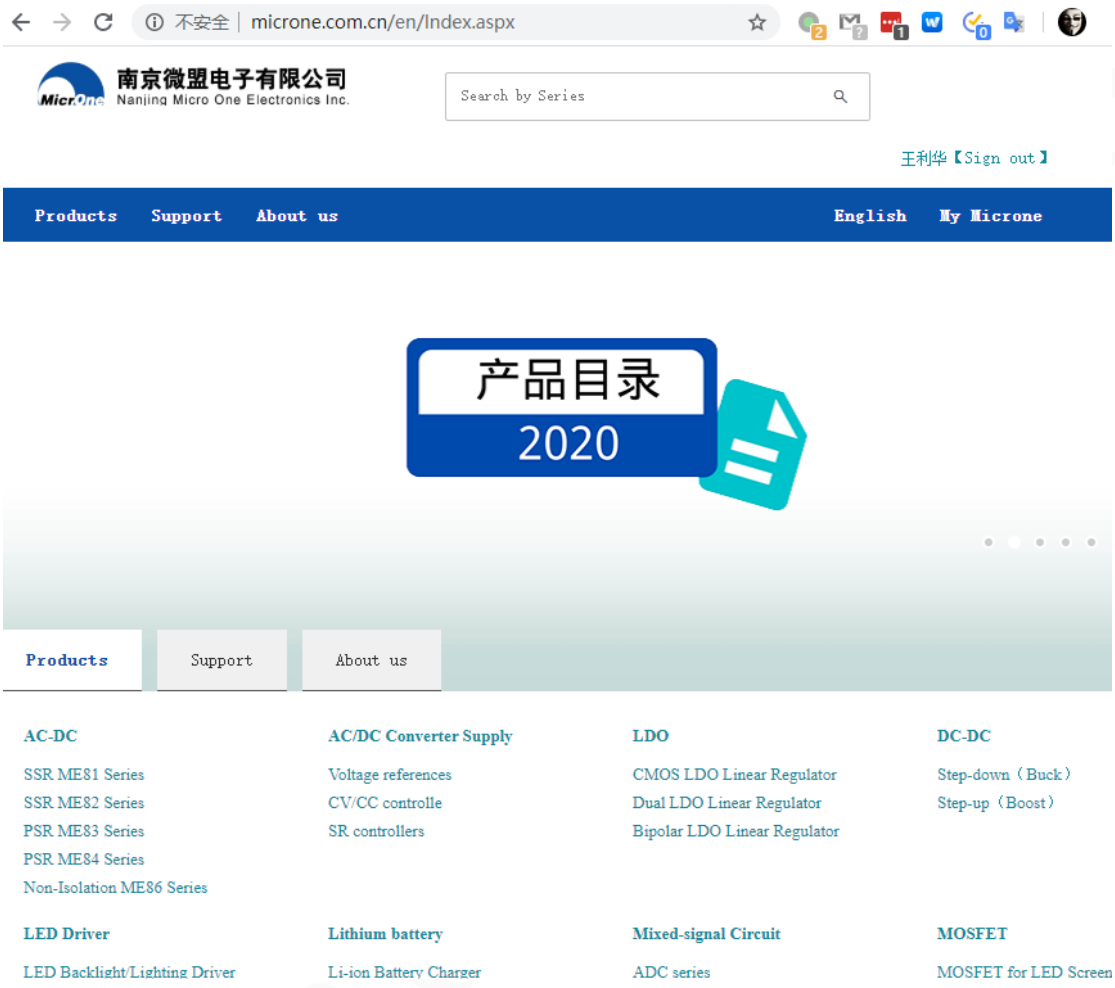
4.1.3.1 漏洞概述

系统在用户登录处验证条件不严格，未能有效鉴别用户身份，导致非法用可以登录进入系统，进行其他操作。

4.1.3.2 测试结果

http://www.microne.com.cn/en/Login.aspx

'or'='or'



4.2 WEB 应用漏洞

4.2.1 SQL 注入漏洞

4.2.1.1 漏洞概述

WEB 程序在处理用户输入时，过滤不严谨，恶意攻击者可以将精心构造的 sql 语句传递给 WEB 程序，导致程序执行其他操作。

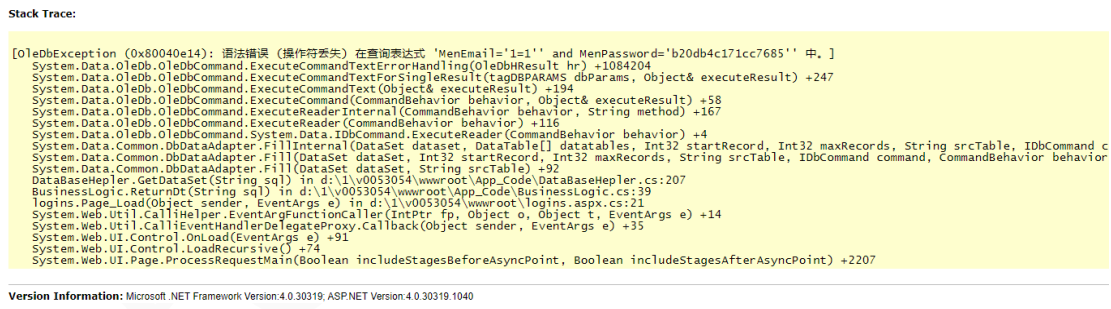
4.2.1.2 测试结果

4.2.2 开启调试模式

4.2.2.1 漏洞概述

WEB 服务器开启了调试模式，可以显示详细的错误信息，攻击者可以利用这些信息进行进一步测试。

4.2.2.2 测试结果



五. 安全风险总结

此次安全检查中发现存多个严重和高危漏洞，需要开发人员及时进行漏洞修复。因此，我们认为南京微盟电子

有限公司网站总体安全状态为“紧急状态”，建议在特殊时期关闭，待整改加固完毕后再上线。

附录A 安全风险状况等级说明

安全风险状况说明	
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。
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。
高危状态	信息系统中发现存在高危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。
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。

附录B 漏洞等级状况说明

安全风险状况说明	
低危漏洞	对系统造成较小的影响，攻击成本高，攻击场景较为苛刻，不会直接影响到系统的正常运行，攻击者可能无法通过该漏洞获得权限。
中危漏洞	对系统造成一般的影响，攻击成本一般，在特定场景下将可影响系统的正常运行，攻击者需要配合其他安全漏洞方可间接获得权限。
高危漏洞	对系统造成严重的影响，攻击成本低，一般情况下可直接利用而无需特定场景和要求，攻击者可直接利用该漏洞获得权限。

附录C 渗透测试授权书

验证测试基本信息表

（一）单位基本情况

单位名称	南京微盟电子有限公司	责任部门	行政部
单位性质	国有控股	所属行业	电子信息
联系人	余强	联系电话	18626455710

（二）互联网信息系统基本情况

系统名称	www.microne.com.cn	互联网IP	/
系统描述	南京微盟电子有限公司官网		
URL和端口	http://www.microne.com.cn/admin/Indexs.aspx 80		

提供互联网登录功能的URL、IP和端口	用户列表（用于口令猜测）	普通权限用户测试账号（用于深度测

测试时间要求	两天
其他要求	

注：测试账号用于深度测试，提供普通权限用户即可，测试完成后请删除相关账户

（三）其他互联网信息系统（合同以外）基本情况

单位其他系统URL、IP	是否提供登录功能	备注

确认信息：
1、上述验证测试基本信息表中填写内容正确且完整；
2、授权方已了解安全测评对信息系统可能会带来的如下影响：
a）对被测网络设备或主机造成异常运行或停机的可能；
b）对被测主机上的各种系统服务和应用程序造成异常运行或终止运行的可能；
c）测评期间，被测主机上的各种服务的运行速度可能会减慢；
d）测评期间，网络的处理能力和传输速度可能会减慢。
3、授权方在测评时段之前针对测评可能对系统带来的影响和后果已做好充分应对准备和采取适当措施（特别是测评前已做好系统的全面备份）
4、仅针对表格中的内容开展安全性测试，其他未提供部分不在测评范围。

确认人	余强	确认时间	22.7.29