|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **上海市徐汇区中心医院**  **体检健康管理平台**  **安全服务报告**  **2023年9月份**   |  |  | | --- | --- | |  |  | |  |  | |  |  | | 成稿日期 | 2023年9月8日星期五 | |

**目 录**

[1. 概要 3](#_Toc14996)

[1.1 渗透测试必要性 3](#_Toc15078)

[1.2 渗透测试可行性 3](#_Toc16511)

[2. 服务概述 4](#_Toc32247)

[2.1 渗透测试对象 4](#_Toc29947)

[2.2 渗透测试结果 4](#_Toc29461)

[3. 漏洞分析 5](#_Toc15106)

[3.1 体检健康管理平台测试 5](#_Toc6525)

[3.1.1 未使用HTTPS安全协议【低危】 5](#_Toc9339)

[3.1.2 点击劫持【低危】 6](#_Toc29861)

# 概要

通过渗透性测试，发现逻辑性更强、更深层次的漏洞，并直观反映漏洞的潜在危害，了解网络防御系统的安全强度，为预期计划正常运行而提供的一种有效安全机制，提供网络安全状况方面的具体证据。渗透性测试能够制定出切实可行的有效的安全管理制度。因此，徐汇区中心医院授权我公司进行渗透测试安全检查。

* 1. 渗透测试必要性

渗透测试是安全工程师尽可能完整的模拟黑客使用的漏洞发现技术与攻击技术(与黑客攻击相比其结果实可预知性的)，对目标网络、主机、数据库与应用系统的安全性做深入的探测，发现系统薄弱环节的过程。它能够直观的让管理人员知道当前网络、主机、数据库与应用系统存在的安全弱点以及可能造成的影响，以便采取必要的防范措施。我们通过工具扫描、人工评估可以发现网络、系统、数据库与应用存在的安全弱点，但我们并不知道弱点被利用的可能以及被利用后引起的风险大小，甚至可能并没有发现系统真正最薄弱的环节，而渗透测试正好可以弥补这些不足。

* 1. 渗透测试可行性

由于渗透测试是在受测试方监督下进行，使用的渗透测试方法和工具也是非暴力的，测试的结果在测试工程师的可预知范围之内，并且测试只进行到漏洞被利用为止，而不会进行下一步的破坏活动。因此不会导致服务的异常，渗透测试是完全可行的。

# 服务概述

渗透测试服务流程定义为如下阶段：

* **信息收集**

在此阶段必须对所测试的网站进行相关信息收集，为后续的渗透测试工作做好准备。收集的信息包括：网站的域名、IP地址、对外开放端口、网站使用的组件以及目标主机的操作系统版本等等。

* **渗透测试**

此阶段主要根据上一阶段所获得的信息对网站及所在网络进行渗透测试，主要包括工具扫描和手工测试，如果顺利的话可以获取相应的权限。

* **权限提升**

此阶段，渗透测试小组尝试由普通权限提升为管理员权限，获得对系统的完全控制权。在时间许可的情况下，必要时从第一阶段重新进行。

* **后续工作**

清除阶段，渗透测试小组清除中间数据，输出根据测试的结果编写的直观的渗透测试服务报告。

1. 1. 渗透测试对象

|  |  |
| --- | --- |
| **渗透测试目标** | **URL** |
| 体检健康管理平台 | http://phyexam.hospital-cas.cn/ |

* 1. 渗透测试结果

下表列出了包含的安全漏洞以及这些安全漏洞带来的安全风险，检测结果如下：

* 高危漏洞：0个
* 中危漏洞：0个
* 低危漏洞：2个

|  |  |  |
| --- | --- | --- |
| **系统** | **漏洞名称** | **漏洞等级** |
| 体检健康管理平台 | 未使用HTTPS安全协议 | **低危** |
| 体检健康管理平台 | 点击劫持 | **低危** |

# 漏洞分析

1. 1. 体检健康管理平台测试
      1. 未使用HTTPS安全协议【低危】

|  |
| --- |
| **未使用HTTPS安全协议** |
| **漏洞描述** |
| 用户数据以明文方式传输，攻击者可以任意截取，篡改网络传输数据 |
| **漏洞地址** |
| http://phyexam.hospital-cas.cn/ |
| **测试过程** |
|  |
| **修复建议** |
| 建议系统增加HTTPS安全协议。 |

* + 1. 点击劫持【低危】

|  |
| --- |
| **点击劫持** |
| **漏洞描述** |
| 点击劫持 (Clickjacking) 技术又称为界面伪装攻击 (UI redress attack )，是一种视觉上的欺骗手段。攻击者使用一个或多个透明的 iframe 覆盖在一个正常的网页上，然后诱使用户在该网页上进行操作，当用户在不知情的情况下点击透明的 iframe 页面时，用户的操作已经被劫持到攻击者事先设计好的恶意按钮或链接上。攻击者既可以通过点击劫持设计一个独立的恶意网站，执行钓鱼攻击等；也可以与 XSS 和 CSRF 攻击相结合，突破传统的防御措施，提升漏洞的危害程度。 |
| **漏洞地址** |
| http://phyexam.hospital-cas.cn/ |
| **测试过程** |
| <!DOCTYPE html>  <html>  <head lang="en">  <meta charset="UTF-8" >  <title>点击劫持测试</title>  </head>  <body>  <iframe src="http://phyexam.hospital-cas.cn" width="500" height="500" frameborder="10"> </iframe>  </body>  </html> |
| **修复建议** |
| 在response头部设置X-Frame-Options或者Content-Security-Policy 'frame- ancestors' |