**上海市第一人民医院**

**体检中心系统**

**渗透测试报告**

**密 级：**商业机密

**版本编号：**V1.0

**编写时间：**2025年05月12日

目录

[一 .摘要 3](#_Toc22533)

[二 .服务概述 4](#_Toc26277)

[2.1 测试流程 4](#_Toc23616)

[2.2 风险管理及规避 4](#_Toc3116)

[2.3 参考依据 5](#_Toc10911)

[2.4 预期收益 6](#_Toc25423)

[三 .测试服务说明 7](#_Toc24853)

[3.1 测试环境 7](#_Toc1134)

[3.2 测试人员 7](#_Toc18388)

[四 .测试结果和建议 8](#_Toc11007)

[4.1 测试结果详情 8](#_Toc6236)

[4.1.1 敏感信息get方式展现【中危】 8](#_Toc28375)

[4.1.2 巡检账号弱密码【高危】 9](#_Toc9759)

[4.1.3 版本信息泄露【低危】 11](#_Toc19665)

[4.1.4 注册处手机号可重复注册【中危】 12](#_Toc15628)

[4.1.5 Js文件token泄露【低危】 15](#_Toc8594)

[4.2 其他建议 16](#_Toc28106)

[五 .致谢 17](#_Toc3958)

[附录A 安全等级评定 18](#_Toc31845)

[附录B WASC威胁分类 19](#_Toc20721)

1. .摘要

经上海市第一人民医院授权，上海鑫炙智能科技有限公司渗透测试团队于2025年5月7日-2025年5月9日，对授权系统进行渗透测试工作。

|  |  |  |  |
| --- | --- | --- | --- |
| **系统名称** | **目标地址** | **ip** | **安全等级** |
| 体检中心系统 | https://jkgl.shgh.cn:8001/ |  | 不安全 |

测试结果汇总：

详情汇总如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **测试目标** | **漏洞等级** | **漏洞名称** | **数量** |
| 体检中心系统 | 高危漏洞 | 1. 巡检账号弱密码 | 1个 |
| 中危漏洞 | 1. 注册处手机号可重复注册 2. 敏感信息get方式展现 | 2个 |
| 低危漏洞 | 1. 版本信息泄露 2. Js文件token泄露 | 2个 |

1. .服务概述
   1. 测试流程

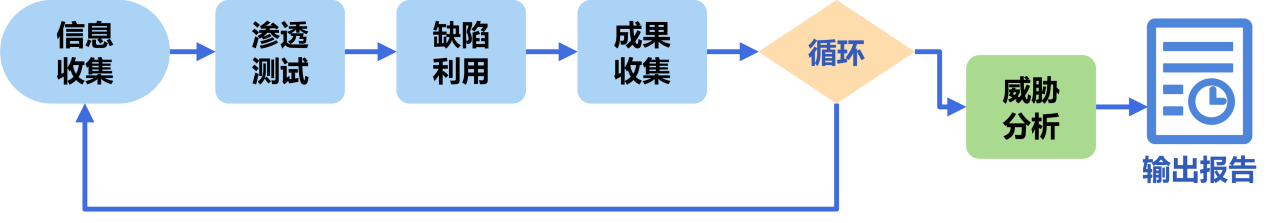


图2-1：测试流程

1. 信息收集：本阶段，上海鑫炙智能科技有限公司测试人员进行必要的信息收集，如 IP 地址、DNS 记录、软件版本信息、IP 段、Google中的公开信息等。
2. 渗透测试：本阶段，上海鑫炙智能科技有限公司测试人员根据第一阶段获得的信息对网络、系统进行渗透测试。此阶段如果成功的话，可能获得普通权限。
3. 缺陷利用：本阶段，上海鑫炙智能科技有限公司测试人员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。
4. 成果收集：本阶段，上海鑫炙智能科技有限公司测试人员对前期收集的各类弱点、漏洞等问题进行分类整理，集中展示。
5. 威胁分析：本阶段，上海鑫炙智能科技有限公司测试人员对发现的上述问题进行威胁分类和分析其影响。
6. 输出报告：本阶段，上海鑫炙智能科技有限公司测试人员根据测试和分析的结果编写直观的渗透测试服务报告。
   1. 风险管理及规避

为保障客户系统在渗透测试过程中稳定、安全的运转，我们将提供以下多种方式建议来进行风险规避。

**对象的选择**

为更大程度的避免风险的产生，渗透测试还可选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

**时间的控制**

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

**技术手段**

上海鑫炙智能科技有限公司的渗透测试人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

**监控措施**

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

**工具使用**

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

* 1. 参考依据

为了保证此次渗透测试的先进性、完备性、规范性，上海鑫炙智能科技有限公司渗透工程师将参考下列国内、国际与渗透测试有关的标准进行工作。

**国内可参考的标准、指南或规范**

* ISO/IEC 27001:2005信息技术-安全技术-信息系统规范与使用指南
* ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
* ISO/IEC TR 15443-1: 2005 信息技术安全保障框架
* ISO/IEC PDTR 19791: 2004 信息技术 安全技术 运行系统安全评估
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 19715.1-2005 信息技术-信息技术安全管理指南
* GB/T 19716-2005 信息技术-信息安全管理实用规则
* GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
* GB/T17859-1999 计算机信息系统安全保护等级划分准则
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 20988-2007信息系统灾难恢复规范
* GB/Z 20986-2007信息安全事件分类分级指南
* 上海鑫炙智能科技有限公司渗透测试最佳实践
* 上海鑫炙智能科技有限公司安全服务工作规范、渗透测试实施规范
* ……

**国际可参考的标准、指南或规范**

* 信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
* 信息系统审计标准（ISACA）G7 应有的职业谨慎
* 信息系统审计标准（ISACA）G9 不正当行为的审计考虑
* 信息系统审计标准（ISACA）G18 信息系统管理
* 信息系统审计标准（ISACA）G19 不正当及非法行为
* 信息系统审计标准（ISACA）G33 对网络使用的总体考虑
* CESG (CHECK) IT Health Check方法
* OWASP OWASP\_Testing\_Guide\_v3
* OWASP OWASP\_Development\_Guide\_2005
* OWASP OWASP\_Top\_10\_2010\_Chinese\_V1.0
* OWASP OWASP\_Top\_10\_2013-Chinese-V1.2
* OWASP OWASP\_Top\_10\_2017\_RC1\_V1.0
* OSSTMM OSSTMM\_Web\_App\_Alpha
* Web应用安全委员会（WASC）WASC Threat Classification v2
* ……
  1. 预期收益

通过实施渗透测试服务，可对授权测试网站系统起到如下推进作用：

**明确安全隐患**

渗透测试是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此明确整体系统中的安全隐患点。

**提高安全意识**

如上所述，任何的隐患在渗透测试服务中都可能造成“千里之堤溃于蚁穴”的效果，因此渗透测试服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

**提高安全技能**

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的渗透测试报告，也能为用户提供当前流行安全问题的参考。

1. .测试服务说明
   1. 测试环境

|  |  |  |
| --- | --- | --- |
| **测试账号** | **密码** | **备注** |
| / | / | / |

上海鑫炙智能科技有限公司测试团队使用的测试IP地址如下：

|  |  |
| --- | --- |
| **IP地址** | 203.156.231.100 |

* 1. 测试人员

本次上海鑫炙智能科技有限公司测试团队参与渗透测试人员，如下所示：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **测试人员名单** | | | | | |
| **姓名** | 孙杰 | **所属部门** | 上海安全服务部门 | **联系方式** | jie.sun@sh-xinzhizn.com |
| **姓名** | 李好 | **所属部门** | 上海安全服务部门 | **联系方式** | hao.li@sh-xinzhizn.com |

1. .测试结果和建议
   1. 测试结果详情
      1. 敏感信息get方式展现【中危】

**问题描述**：

登录处账号、密码、手机号以get方式展现在url中。

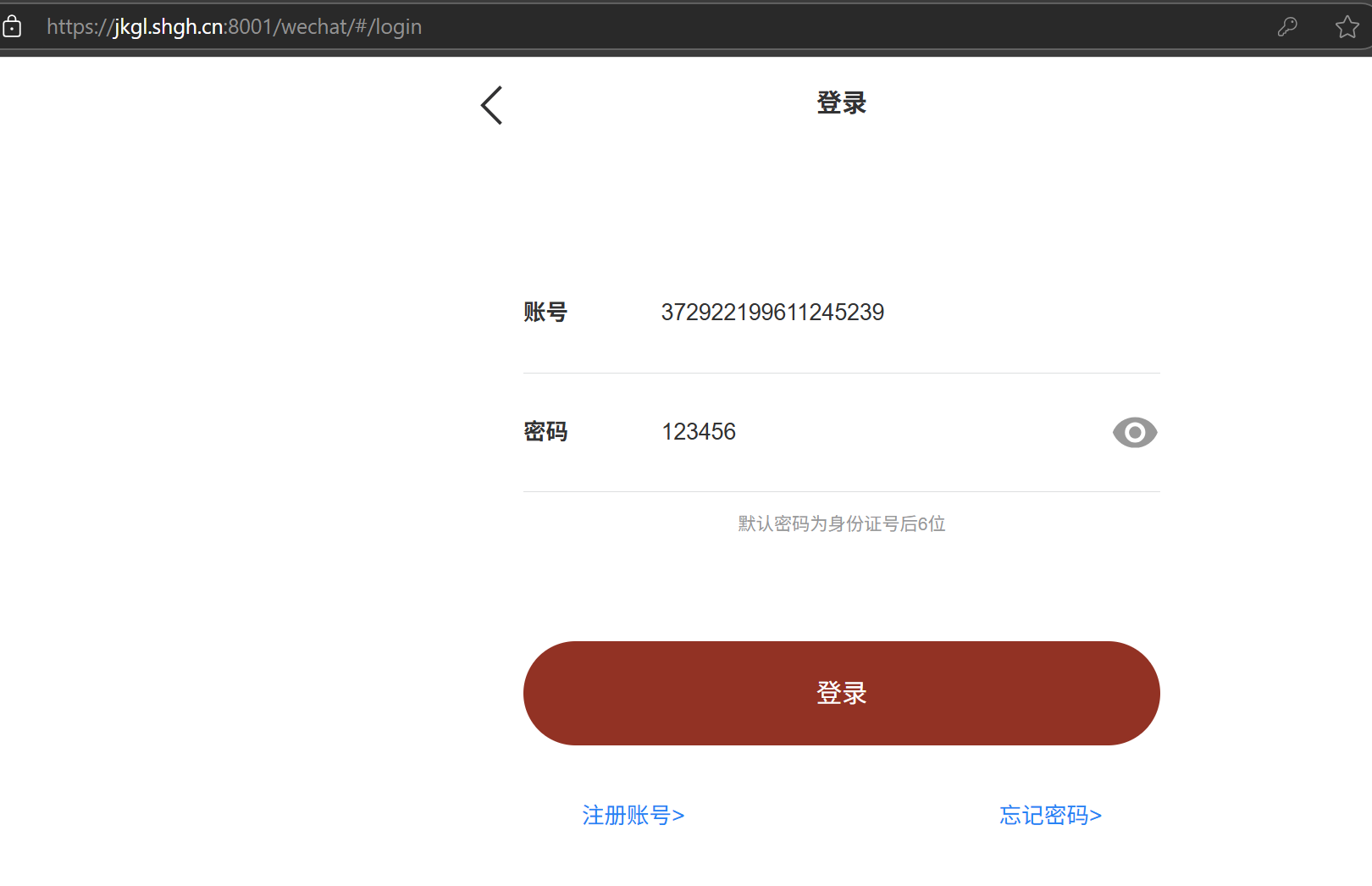
**测试地址：**

[https://jkgl.shgh.cn:8001/wechat/#/login](https://jkgl.shgh.cn:8001/wechat/#/index)

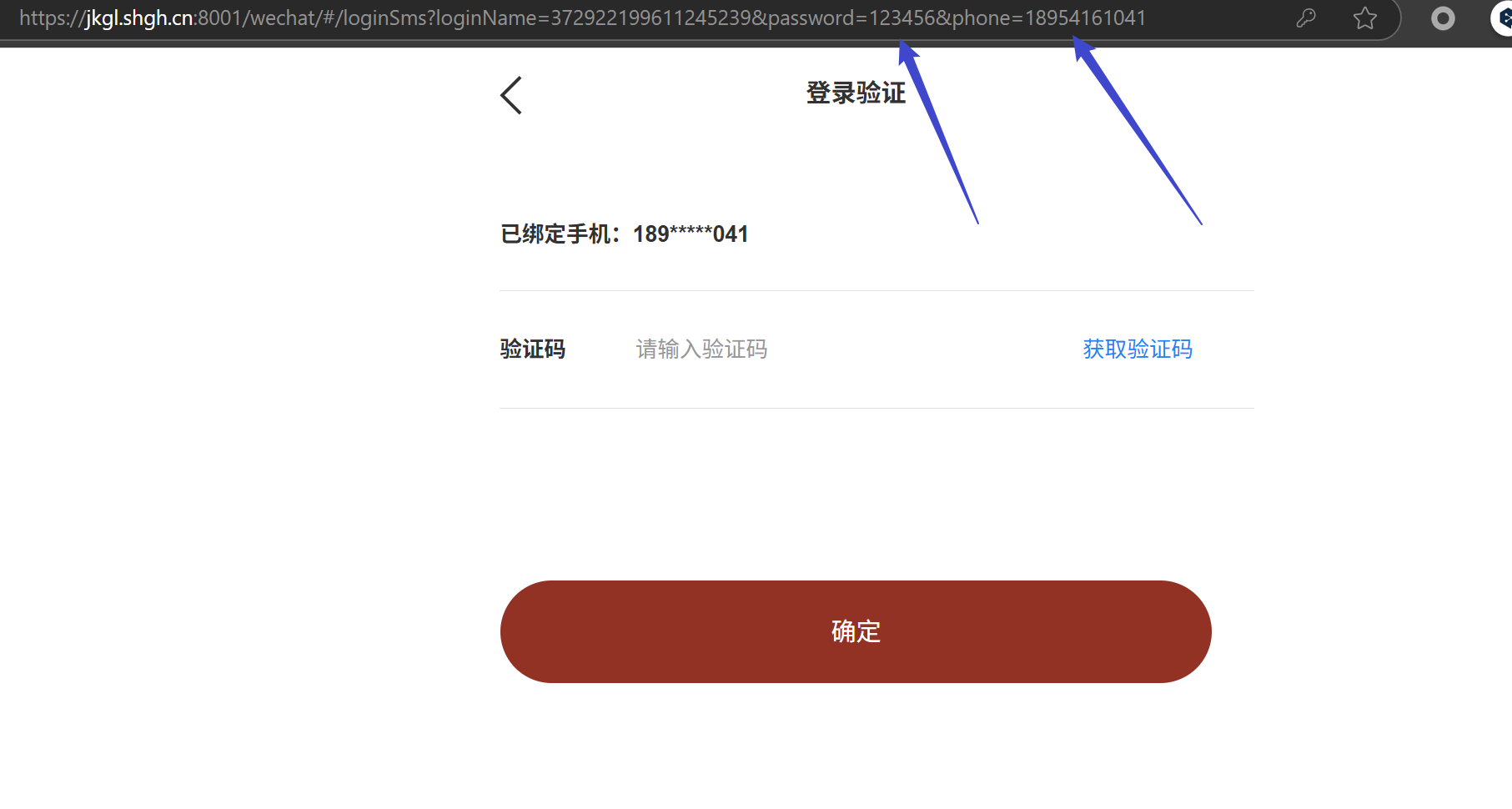
**测试过程：**

1. 访问：[https://jkgl.shgh.cn:8001/wechat/#/login](https://jkgl.shgh.cn:8001/wechat/#/index)

填写验证账号信息



1. 点击“登录”跳转到下一流程即可再url中获取到输入的敏感信息及 被隐藏的手机号信息



**风险分析：**

可导致敏感信息泄露。

**安全建议：**

1. 禁止敏感信息以明文方式及GET方式展示在url中。
   * 1. 巡检账号弱密码【高危】

**问题描述**：

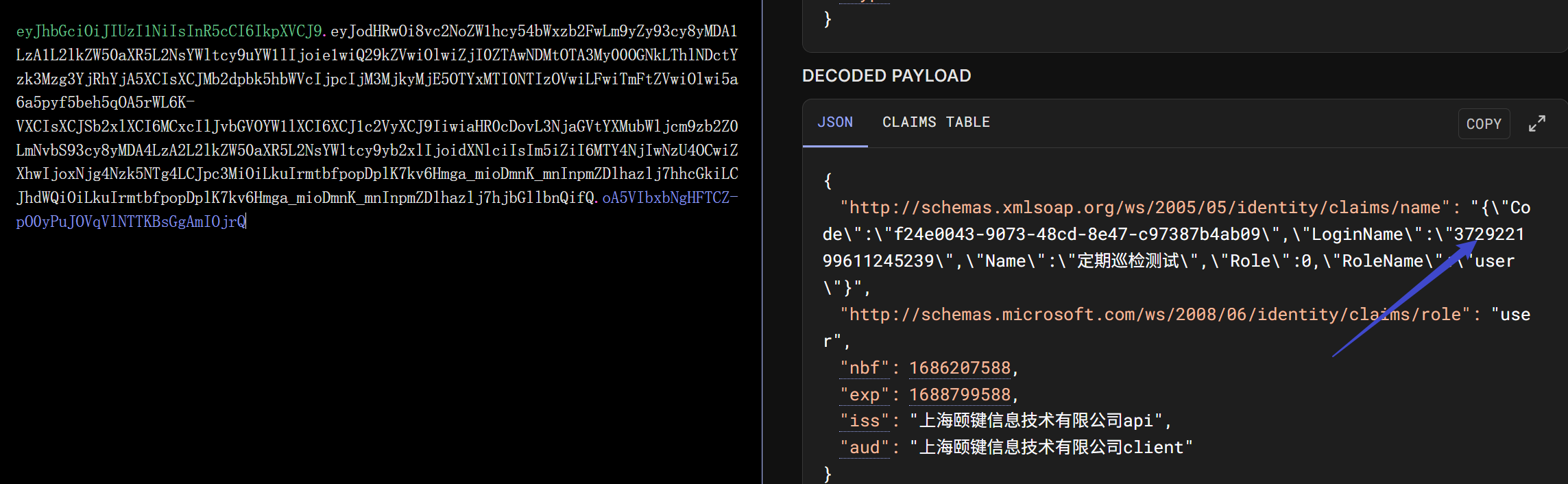
账号弱密码。

**测试地址：**

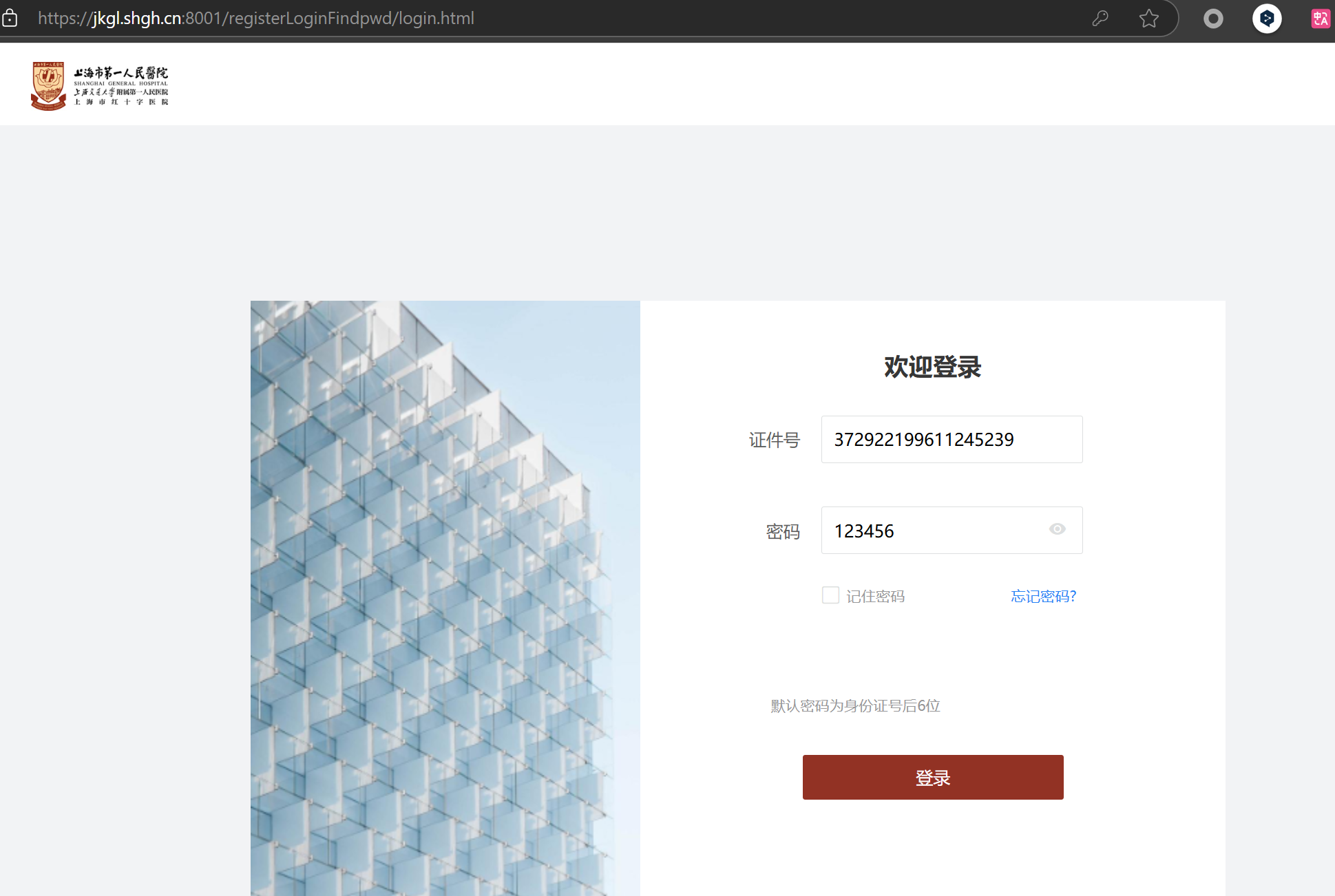
<https://jkgl.shgh.cn:8001/registerLoginFindpwd/login.html>

**测试过程：**

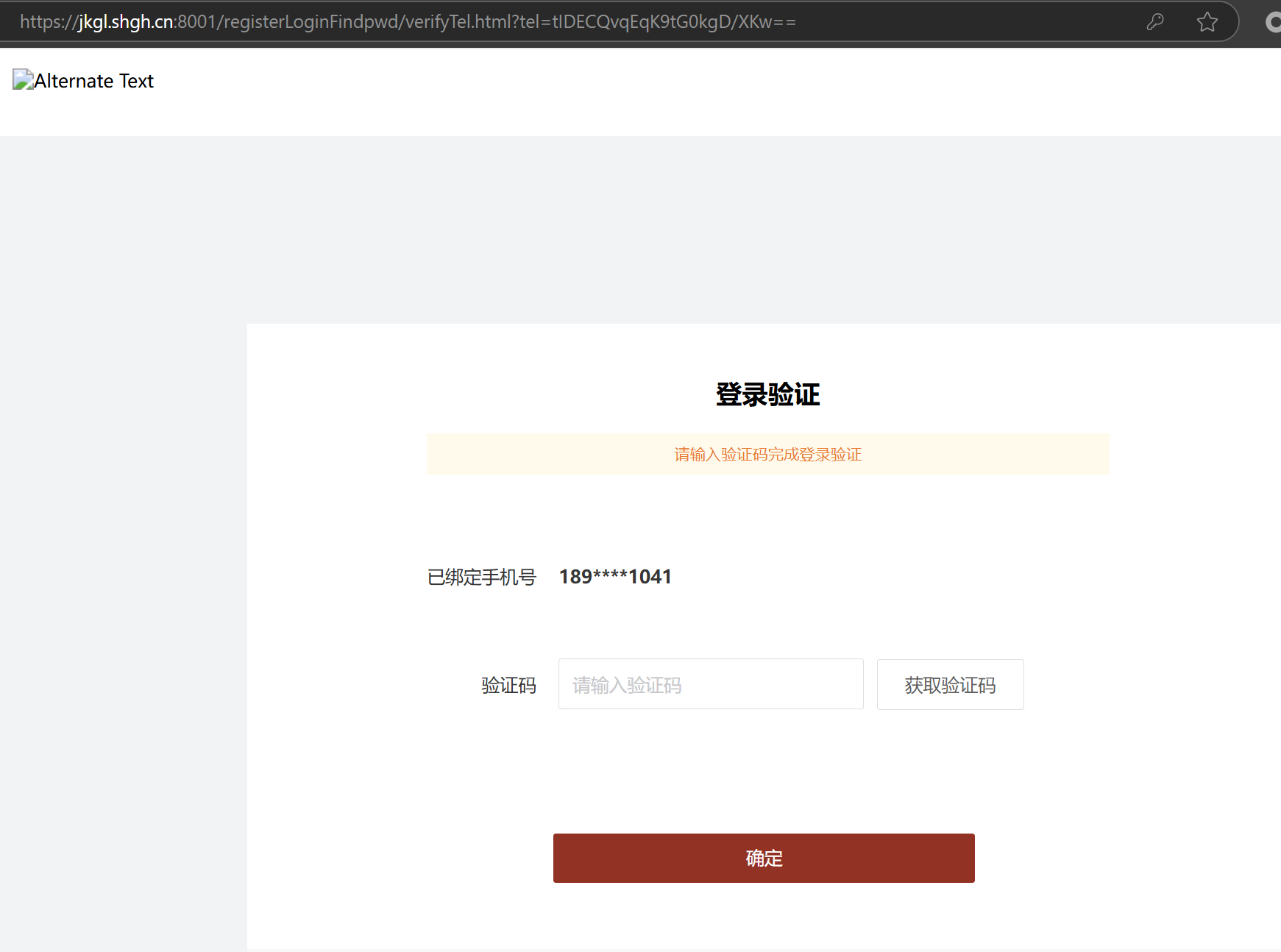
1. <https://jkgl.shgh.cn:8001/wechat/static/js/app.879cd354f183e52fc5761687158540803.js>文件中解密jwt token值获取登录账号



1. 输入登录账号及密码信息



1. 跳转到如下可证明密码正确



**风险分析：**

弱密码可增加攻击面，扩展攻击思路，在特定条件下可导致信息泄露等 严重问题。

**安全建议：**

1. 在不影响业务的前提下删除js中的token信息。
2. 强制密码设置为多重组合形式的强密码。
   * 1. **版本信息泄露【低危】**

**问题描述：**

服务端响应头中返回版本号信息。

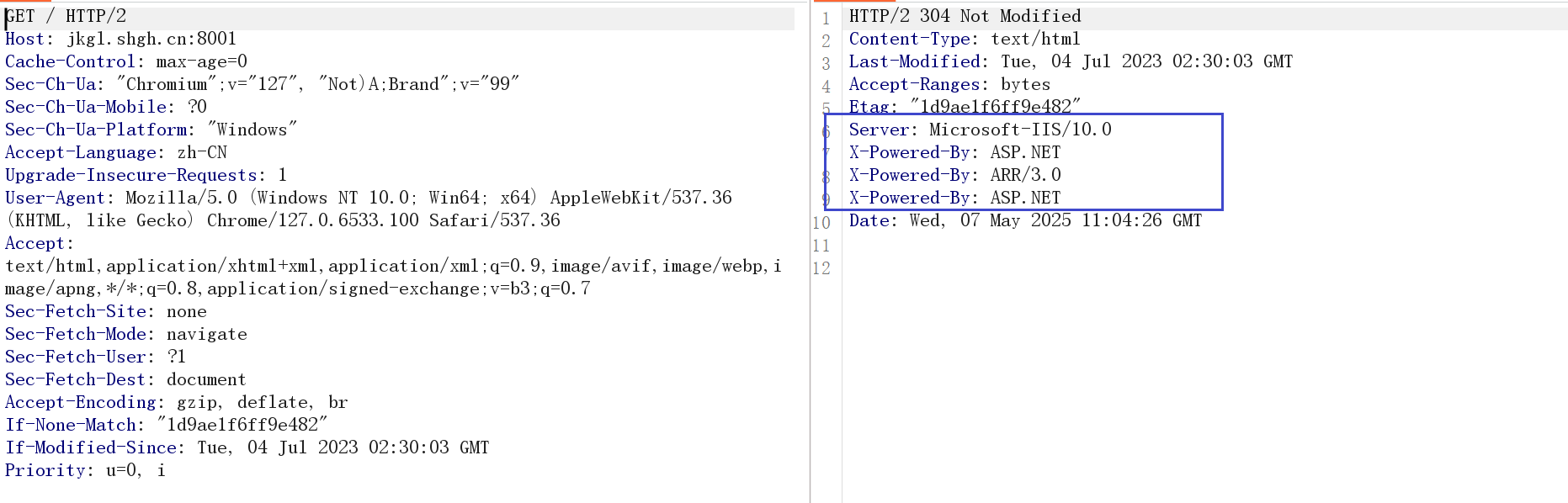
**测试地址：**

<https://jkgl.shgh.cn:8001/>

**测试过程：**

访问：<https://jkgl.shgh.cn:8001/>

服务端返回版本信息



**风险分析：**

组件版本信息泄露可能使攻击者识别出系统中的已知漏洞，增加被攻击 的风险。

**安全建议：**

1. 移除或隐藏版本信息：在生产环境中移除或隐藏系统组件的版本信 息，以防止攻击者获取这些信息。
2. 访问权限限制：限制对系统组件的访问权限，确保只有授权用户可 以获取组件版本信息，例如通过使用访问控制列表（ACL）或网络安全组等 机制。
3. 定期更新和漏洞修复：及时更新系统中使用的组件，并定期进行漏 洞扫描和修复，以确保已知漏洞得到及时修复，减少攻击面。
   * 1. **注册处手机号可重复注册**【中危】

**问题描述**：

注册账号处，同一手机号可绑定不同的新注册账号。

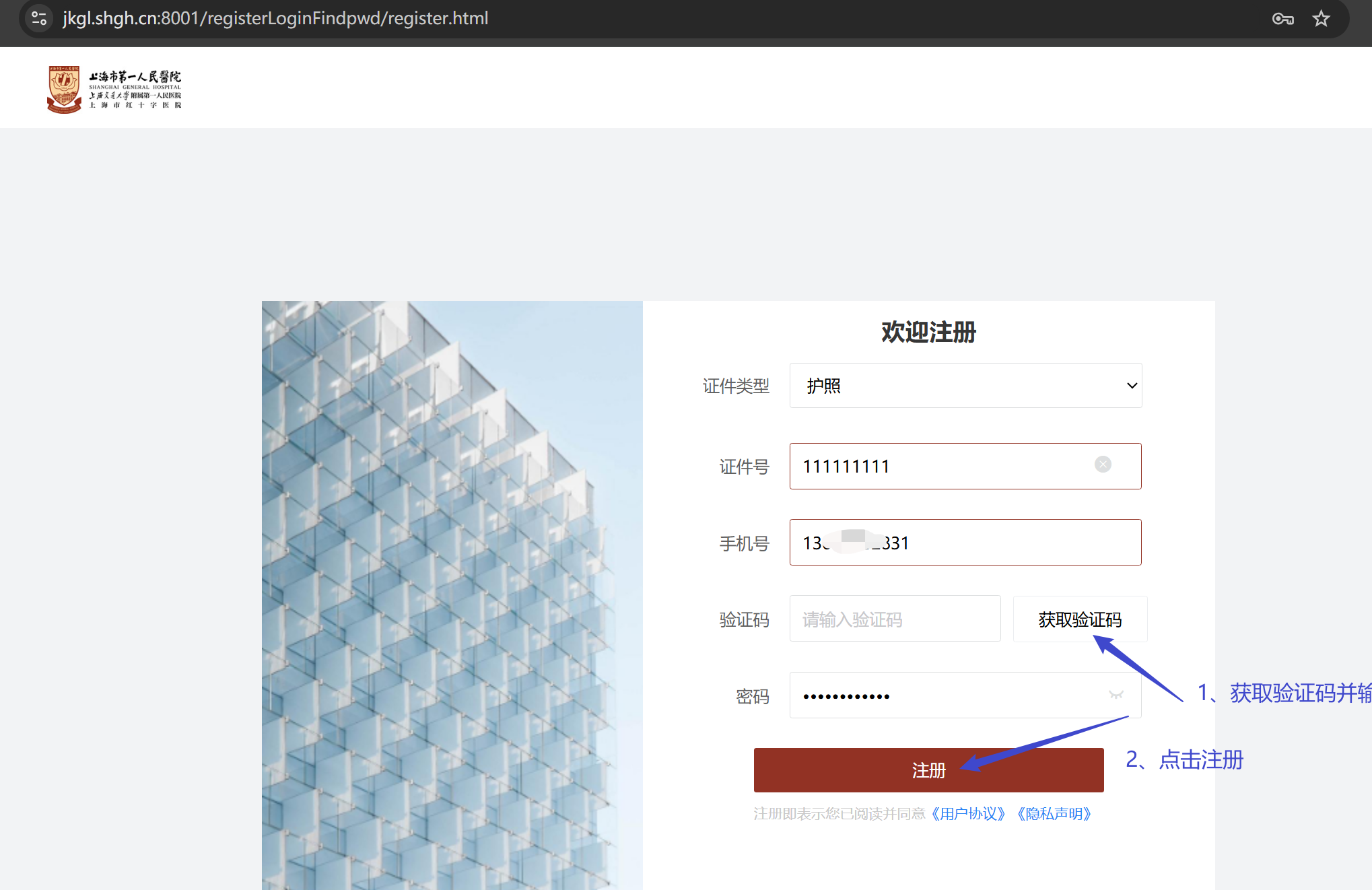
**测试地址：**

[https://jkgl.shgh.cn:8001/registerLoginFindpwd/register.html](https://www.tdrc.org.cn/jkzx/admin/login)

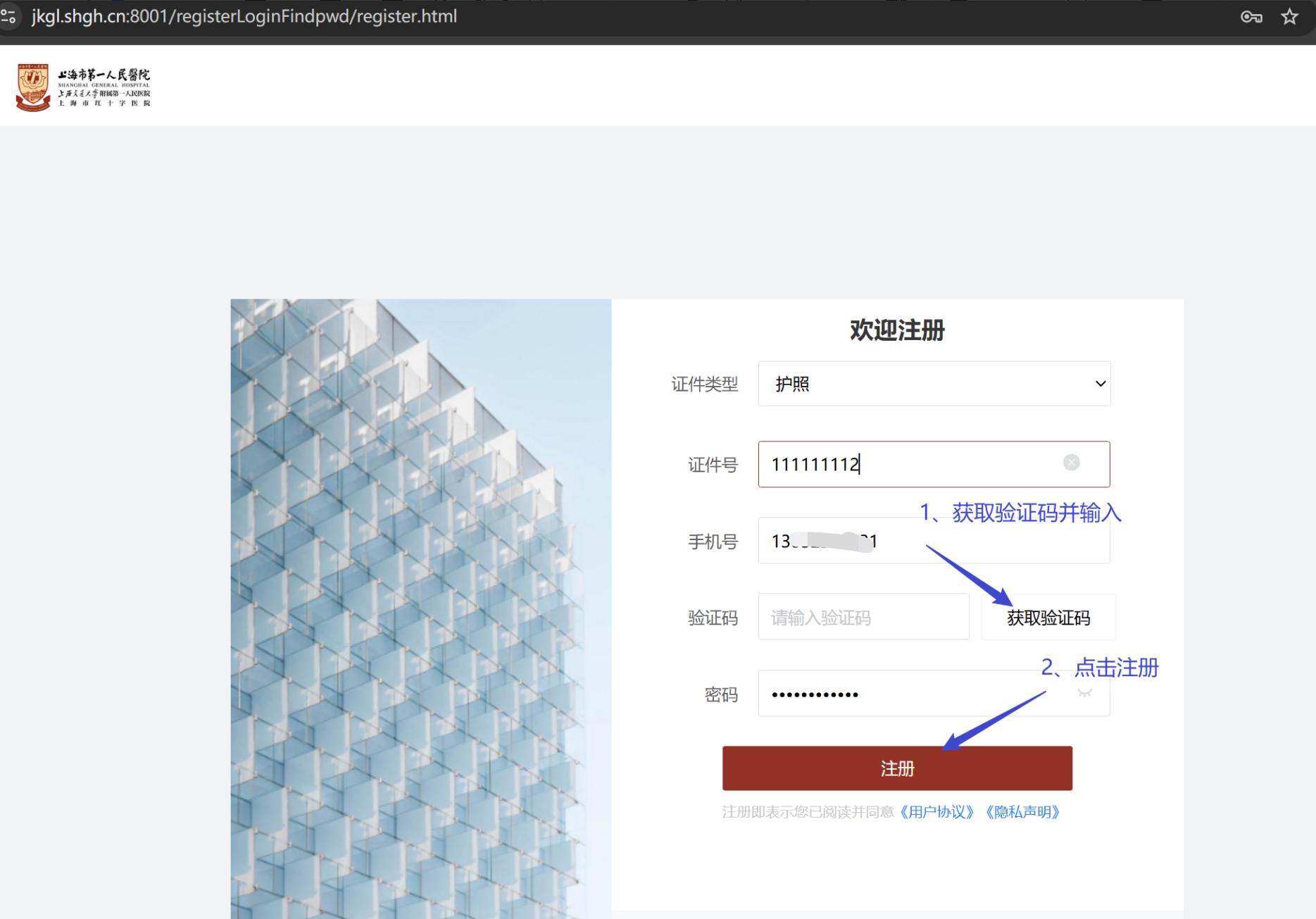
**测试过程：**

1. 注册处选择证件类型为“护照”并按要求填写注册信息

注册账号：111111111

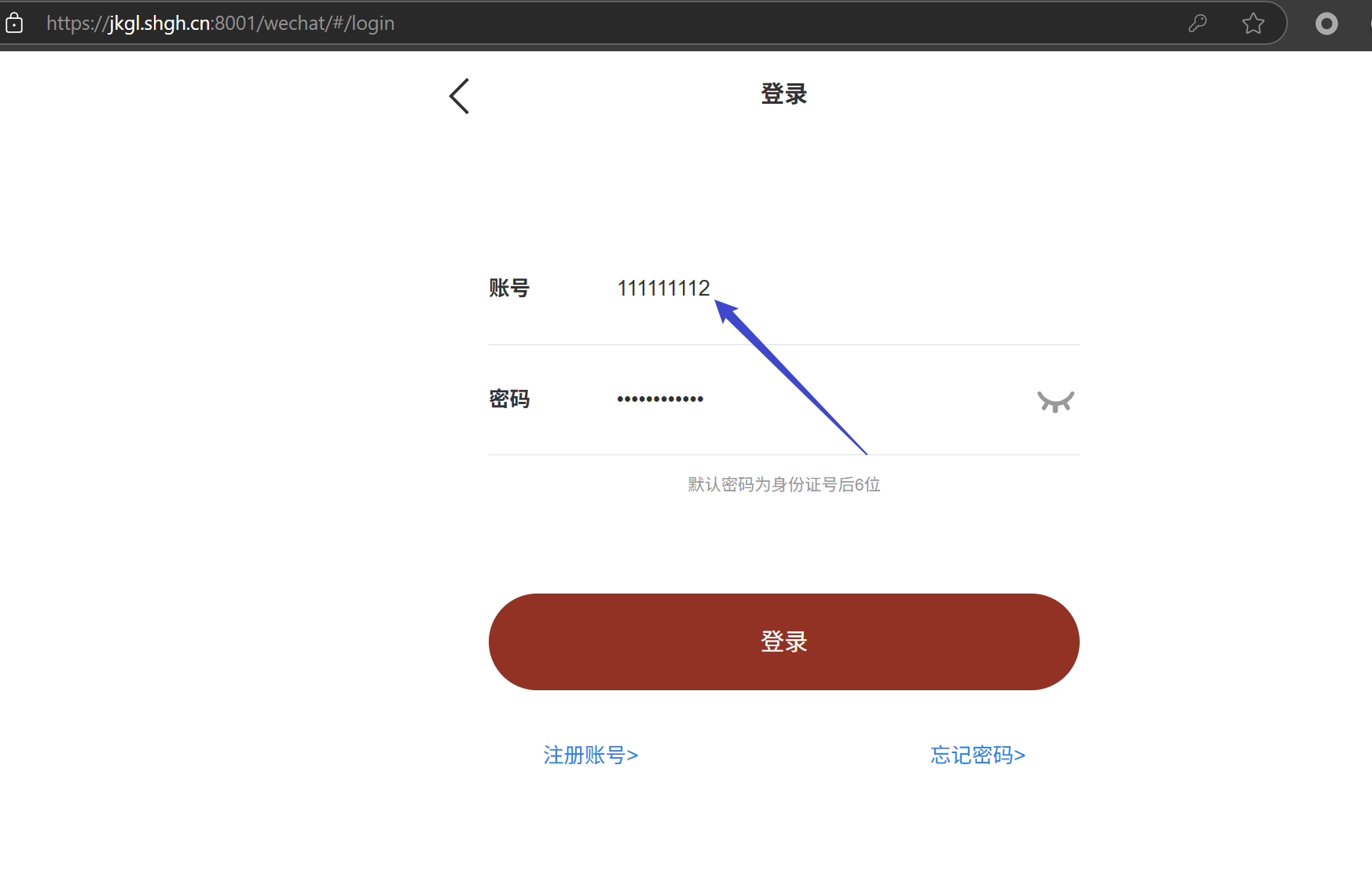


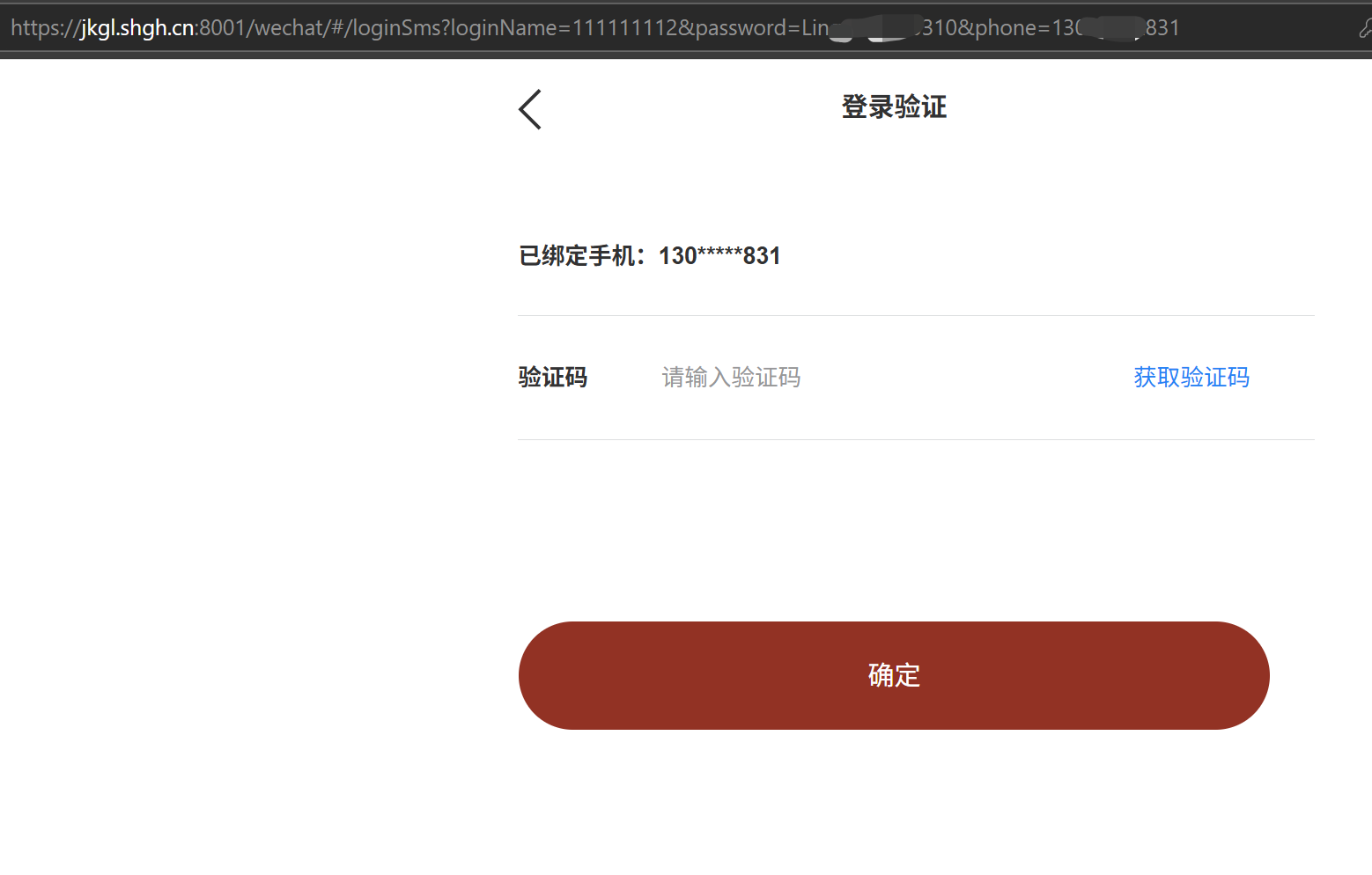
注册账号：111111112，填写同上手机号



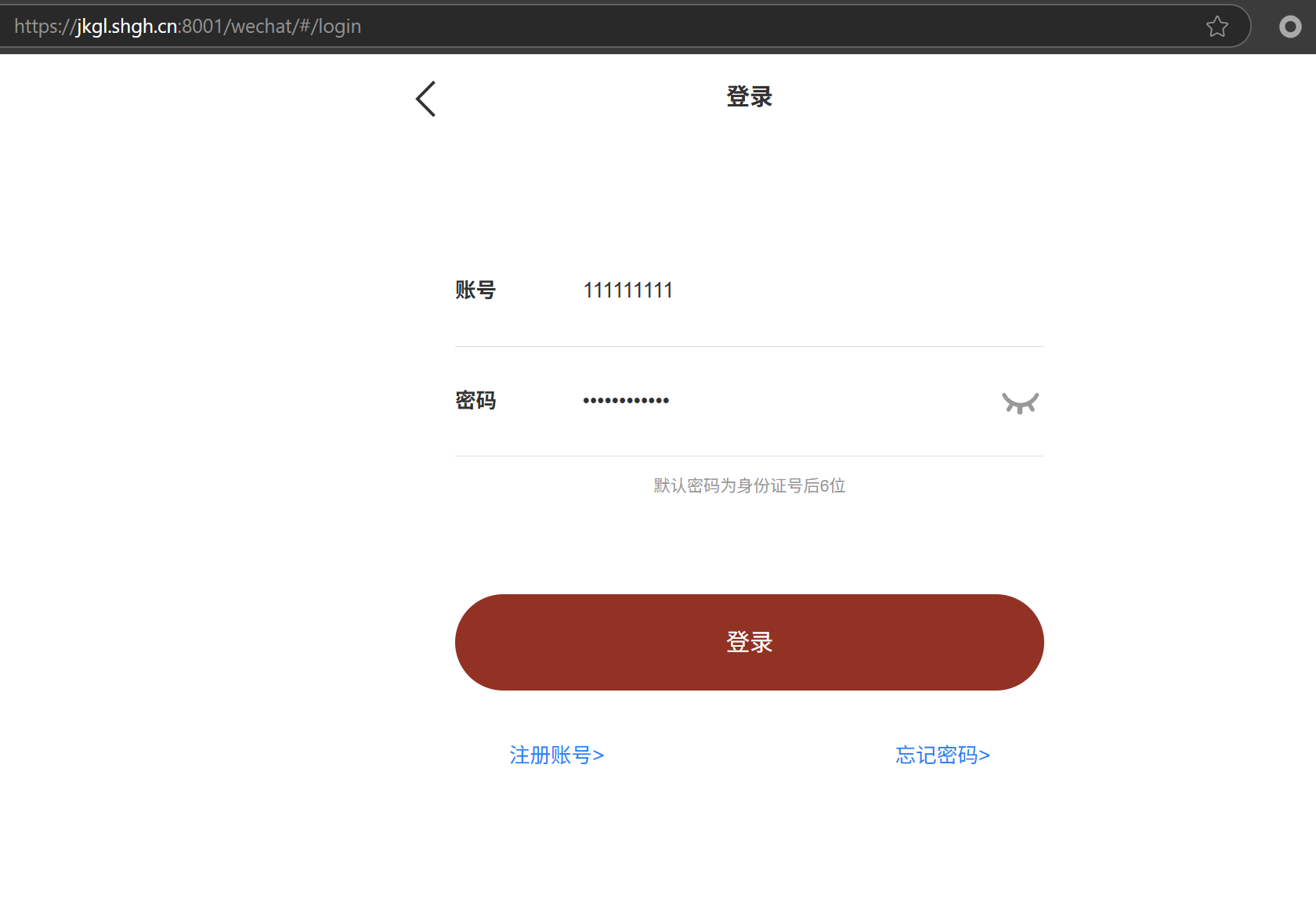
1. 登录验证

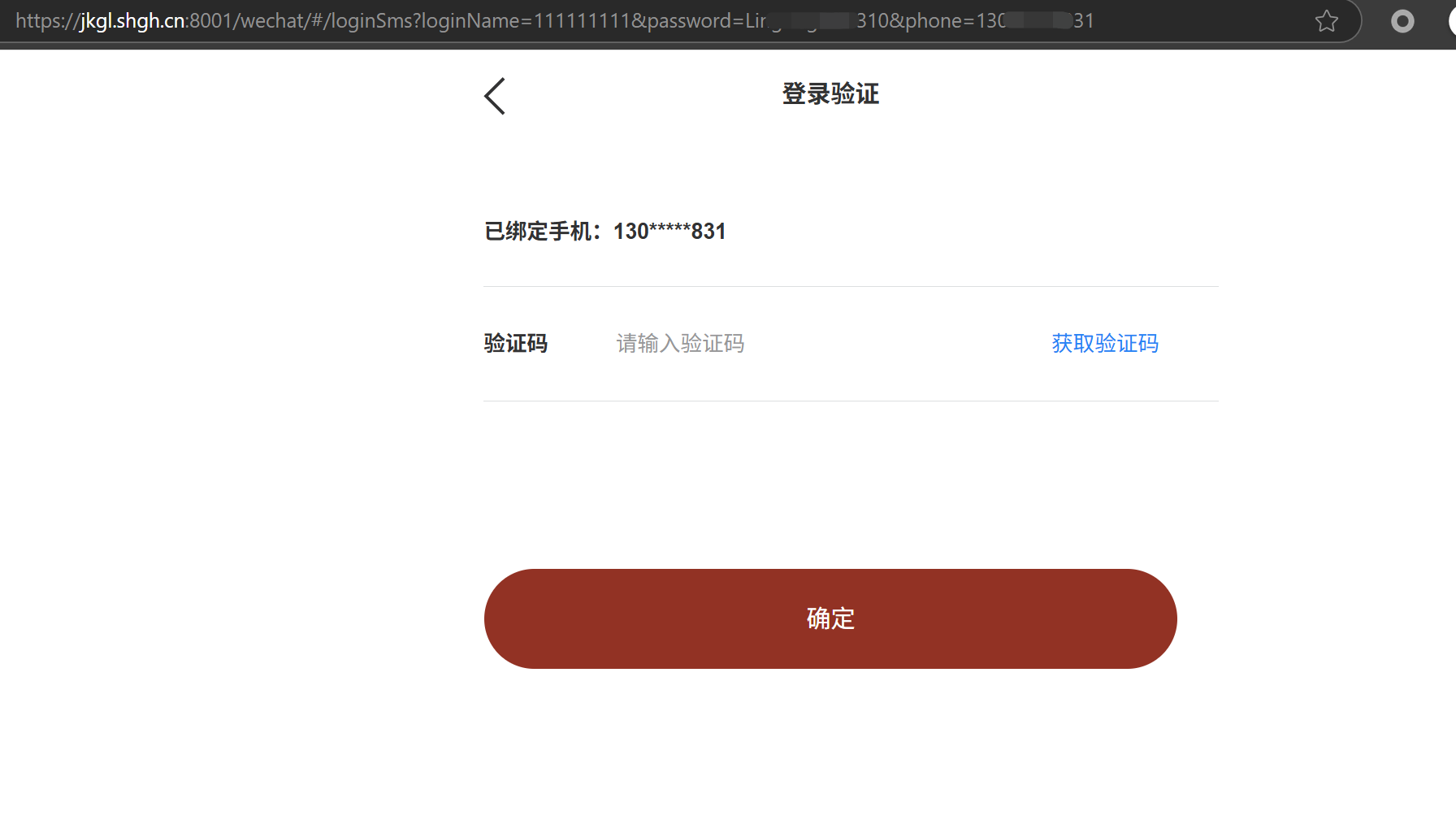
111111112账号：





111111111账号：





**风险分析：**

可导致恶意注册账号、捆绑已注册绑定用户的手机号。

**安全建议：**

1. 增加逻辑验证，校验手机号是否已注册

已注册的情况下禁止重复绑定。

* + 1. Js文件token泄露**【低危】**

**问题描述：**

Js文件中泄露了jwt token信息，可解密后获取账号信息。

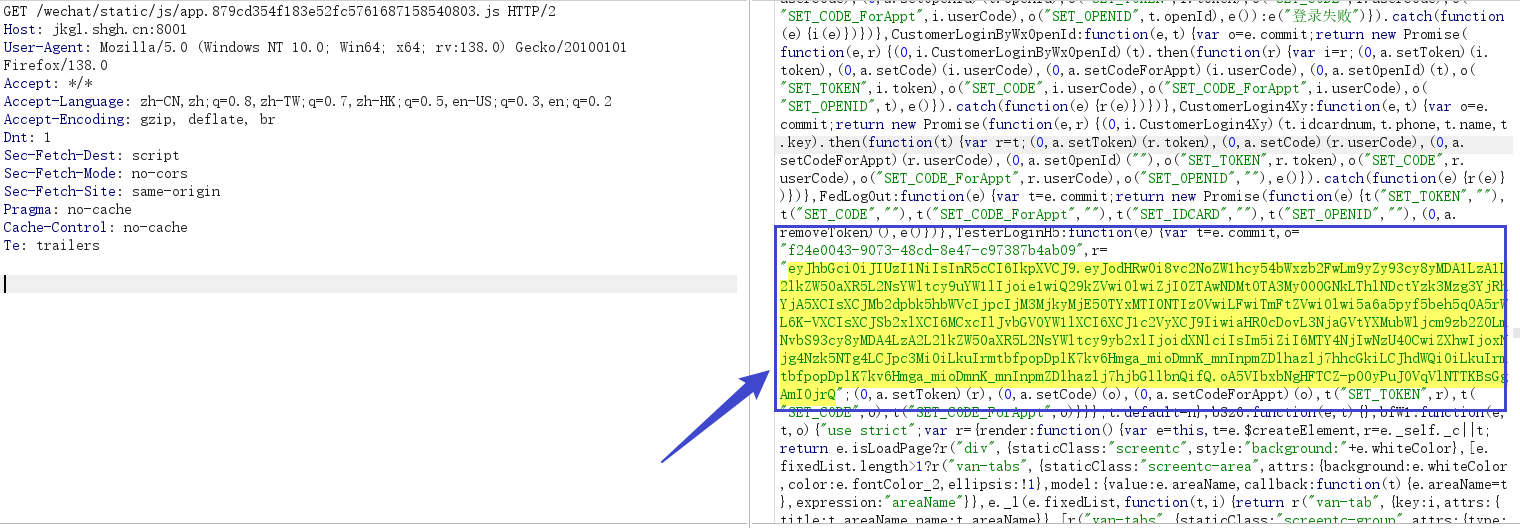
**测试地址：**

<https://jkgl.shgh.cn:8001/wechat/static/js/app.879cd354f183e52fc5761687158540803.js>

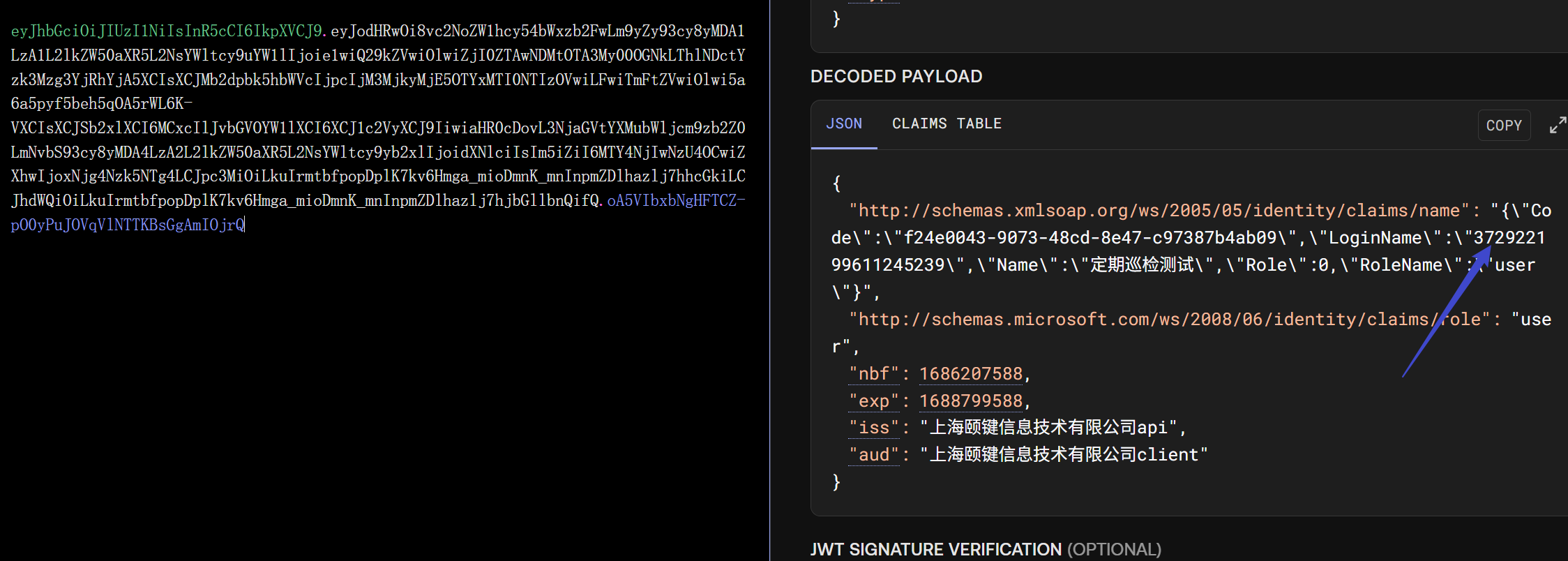
**测试过程：**

访问：

<https://jkgl.shgh.cn:8001/wechat/static/js/app.879cd354f183e52fc5761687158540803.js>



解密后结果：



**风险分析：**

Token泄露，在可解密的情况下可导致敏感信息的泄露，从而导致增加 攻击面。

**安全建议：**

1. 在不影响业务前提下删除js中的token信息。
2. 设置针对js文件的访问控制权限。
   1. 其他建议

针对系统的渗透测试及定期的评估扫描等方式，均以暴露问题为目标，属于被动的安全手段，而这些方式也大大的增加开发和维护的成本。

因此建议针对如客户端程序这类个性化产品开发前就应做好安全的相关工作，建议对定制开发的产品从以下几个方面进行相关的考察和关注：

* + 制定以功能和安全兼顾的产品开发需求
  + 将安全作为产品开发项目中的重要参考指标
  + 产品开发过程中的人员安全意识和技能培训
  + 完善的安全开发手册及通用的安全的代码库
  + 在开发每阶段完成后的定期代码审计和扫描

1. .致谢

本次远程渗透测试过程中，上海鑫炙智能科技有限公司感谢上海市第一人民医院相关人员在渗透测试过程中进行沟通、协调的相关部门和人员的配合，使得我们的工作能够顺利完成。

1. 安全等级评定

|  |  |
| --- | --- |
| **安全等级名称** | **条件描述** |
| 不安全  **（**满足任何一个条件**）** | 1. 存在一个或一个以上严重的安全问题，可直接导致系统受到破坏； 2. 与其他非安全系统连接，同时存在相互信任关系（或帐号互通）的主机； 3. 发现已经被人入侵且留下远程后门的主机； 4. 存在3个以上中等安全问题的主机； 5. 与其他非安全系统在一个共享网络中，同时远程维护明文传输口令； 6. 完全不能抵抗小规模的拒绝服务攻击 |
| 一般安全  **（**满足任何一个条件**）** | 1. 存在一个或一个以上中等安全问题的主机； 2. 开放过多服务，同时可能被利用来进行拒绝服务的主机； 3. 与其他非安全系统直接连接，但暂时不存在直接信任(或帐号互通)关系； 4. 远程维护通过明文的方式传递信息； 5. 存在三个以上轻度安全问题的主机； 6. 只能抵御最低级的拒绝服务攻击； |
| 安全  **（**符合全部条件**）** | 1. 最多存在1-2个轻度安全问题； 2. 远程维护方式安全； 3. 与不安全或一般安全系统相对独立； 4. 能抵挡一定规模的拒绝服务攻击。 |

1. WASC威胁分类

WASC是由专家、行业实践者和组织代表组成的国际性小组，他们提出开放 式源代码以及广泛同意的万维网的最佳做法安全性标准。Web 安全漏洞会持 续影响 Web 站点的风险。确定任何 web 安全漏洞时，执行攻击需要使用至 少若干种应用程序攻击技术之一。这些方法通常称为攻击类（对安全漏洞加 以利用的方式）。

WASC Web 应用程序威胁分类列表：

**功能滥用**：功能滥用是利用 Web 站点自身的特性和功能来使用、欺骗或

阻挠访问控制机制的一种攻击方法。

**暴力**：“暴力”攻击是指猜测个人的用户名、密码、信用卡号或密钥所 使

用的自动化反复试验过程。

**缓冲区溢出**：“缓冲区溢出”利用是指通过覆盖部分内存来改变应用程 序

流的攻击。

**内容电子欺骗**：内容电子欺骗是用于骗取用户相信 Web 站点上出现的某

些内容合法且不是来自外部源的一种攻击方法。

**凭证/会话预测**：凭证/会话预测是一种操纵或假冒 Web 站点用户的方法。

推断或猜测识别特定会话或用户的唯一值，以完成攻击。

**跨站点脚本编制**：跨站点脚本编制 (XSS) 是一种强制 Web 站点回传攻

击者提供的可执行代码（装入在用户浏览器中）的攻击方法。受跨站点

脚本影响的用户的帐户可能会受操纵（cookie 盗用），其浏览器可能会

重定向到其他位置，或者可能显示用户正在访问的 Web 站点所提供的欺

骗性内容。

**拒绝服务**：“拒绝服务”（DoS）攻击技术目的是阻止 Web 站点为一般 用

户活动提供服务。

**目录索引**：“自动目录列表/索引”是 Web 服务器功能，如果未提供常 规

基础文件（index.html/home.html/default.htm），那么该功能会列出 所

请求目录中的所有文件。

**格式字符串攻击**：“格式字符串攻击”通过使用字符串格式化库功能访 问

其他内存空间来修改应用程序流。

**信息泄露**：“信息泄露”指 Web 站点显示可能会协助攻击者攻击系统的

敏感数据（如开发者注释或错误消息）时出现的漏洞。

**不充分反自动化**：不充分反自动化是当 Web 站点允许攻击者将应当仅手

动执行的过程自动化时产生的结果。

**认证不充分**：认证不充分是指 Web 站点允许攻击者访问敏感内容或功能，

而未对其访问许可权进行适当认证时出现的漏洞。

**授权不充分**：授权不充分是指 Web 站点允许访问敏感内容或功能，而这

些内容或功能需要增加访问控制限制时出现的漏洞。

**不充分过程验证**：不充分过程验证是当 Web 站点允许攻击者绕过或规避

应用程序的预期流控制时出现的漏洞。

**会话有效期不足**：会话有效期不足是当 Web 站点允许攻击者复用旧会话

标识进行授权时出现的漏洞。会话有效期不足将增加 Web 站点受攻击

（窃取或假冒其他用户）的可能性。

**LDAP 注入**：LDAP 注入是一种攻击方法，它通过用户提供的输入来构造

轻量级目录访问控制 (LDAP) 语句，从而攻击 Web 站点。

**操作系统命令**：操作系统命令是用于通过操纵应用程序输入来执行操作

系统命令，从而对 Web 站点进行攻击的一种方法。

**路径遍历**：路径遍历攻击方法会强制访问可能位于文档根目录外的文件、

目录和命令。攻击者可能会通过以下方法来操纵 URL：Web 站点将运行

或显示 Web 服务器上任何位置任意文件的内容。

**可预测资源位置**：可预测资源位置是用于显示隐藏 Web 站点内容和功能

的一种攻击方法。通过有根据的猜测，就可以知道攻击是强行搜索，以

查找不打算供公共查看的内容。临时文件、备份文件、配置文件和样本

文件这些示例，都是潜在的剩余文件。

**会话固定**：“会话固定”攻击技术会强制赋予用户的会话标识一个确值。

**SQL 注入**：SQL 注入是一种攻击方法，它通过用户提供的输入来构造 SQL

语句，从而攻击 Web 站点。

**SSI 注入**：SSI 注入（服务器端包含）是一种服务器端攻击方法，该方

法允许攻击者将代码发送到随后将由 Web 服务器在本地执行的应用程

序。

**弱密码恢复验证**：弱密码恢复验证是指当 Web 站点允许攻击者非法获取、

更改或恢复其他用户的密码时出现的漏洞。

**XPath 注入**：XPath 注入是一种攻击方法，它从由用户提供的输入构造

XPath 查询，从而攻击 Web 站点。