肥东县机械行业协会

网站安全风险评估报告

（2020 年 07 月 22 日 13:25—2020 年 07 月 22 日 16:18）

技术支持单位：安徽七禾页信息技术有限公司

扫描全能王 创建

目录:

扫描全能王 创建

1 网站检查基本信息

网站等级：安全

肥东机械行业协会网站检查情况(https://www.fdjxxh.com)

1.1 漏洞统计

网站地址	高	中	低	总计
https://www.fdjxxh.com	0	0	0	0
总计	0	0	0	0

1.2 结果:

2020 年 07 月 22 日 10:18:39 至 2020 年 07 月 23 日 13:04:21，针对该网站进行了安全监测，发现安全隐患 0 个。存在漏洞 0 个，验证通过 0 个（其中紧急漏洞 0 个、高危漏洞 0 个，中危漏洞 0 个，低危漏洞 0 个），误报 0 个，未验证漏洞 0 个；存在其它隐患 0 个，验证通过 0 个，误报 0 个，未验证 0 个。

备注：低危漏洞包括信息类漏洞。

名称：肥东机械行业协会

网站联系人：罗晓虎

联系方式/邮箱：1641534611@qq.com

单位负责人：包训权

安全事件数：0

本次网站安全检查是完全站在攻击者角度，模拟黑客可能使用的攻击技术和漏洞发现技术进行的安全性测试，通过结合多方面的攻击技术进行测试，不存在任何安全漏洞，非常安全！

扫描全能王 创建

2　安全评估方式

安全评估主要依据联想网御安全工程师已经掌握的安全漏洞和安全检测工具，采用工具扫描 + 手工验证的方式。模拟黑客的攻击方法在客户的授权和监督下对客户的系统和网络进行非破坏性质的攻击性测试。

3　安全评估的必要性

安全评估利用网络安全扫描器、专用安全测试工具和富有经验的安全工程师的人工经验对授权测试环境中的核心服务器及重要的网络设备，包括服务器、防火墙等进行非破坏性质的模拟黑客攻击，目的是侵入系统并获取机密信息并将入侵的过程和细节产生报告给用户。

安全评估和工具扫描可以很好的互相补充。工具扫描具有很好的效率和速度，但是存在一定的误报率和漏报率，并且不能发现高层次、复杂、并且相互关联的安全问题；安全评估需要投入的人力资源较大、对测试者的专业技能要求很高（安全评估报告的价值直接依赖于测试者的专业技能），但是非常准确，可以发现逻辑性更强、更深层次的弱点。

此次安全评估的范围：

扫描全能王 创建

4 安全评估方法

4.1 信息收集

信息收集分析几乎是所有入侵攻击的前提/前奏/基础。“知己知彼，百战不殆”，信息收集分析就是完成的这个任务。通过信息收集分析，攻击者（测试者）可以相应地、有针对性地制定入侵攻击的计划，提高入侵的成功率、减小暴露或被发现的几率。

本次评估主要是启用网络漏洞扫描工具，通过网络爬虫测试网站安全、检测流行的攻击 、如交叉站点脚本、SQL 注入等。

4.2 权限提升

通过收集信息和分析，存在两种可能性，其一是目标系统存在重大弱点：测试者可以直接控制目标系统，这时测试者可以直接调查目标系统中的弱点分布、原因，形成最终的测试报告；其二是目标系统没有远程重大弱点，但是可以获得远程普通权限，这时测试者可以通过该普通权限进一步收集目标系统信息。接下来，尽最大努力获取本地权限，收集本地资料信息，寻求本地权限升级的机会。这些不停的信息收集分析、权限升级的结果构成了整个安全评估过程的输出。

4.3 溢出测试

当无法直接利用帐户口令登陆系统时，也会采用系统溢出的方法直接获得系统控制权限，此方法有时会导致系统死机或从新启动，但不会导致系统数据丢失，如出现死机等故障，只要将系统从新启动并开启原有服务即可。

4.4 SQL 注入攻击

SQL 注入常见于那些应用了 SQL 数据库后端的网站服务器，黑客通过向提交某些特殊 SQL 语句，最终可能获取、篡改、控制网站 服务器端数据库中的内容。此类漏洞是黑客最常用的入侵方式之一。

扫描全能王 创建

4.5 检测页面隐藏字段

网站应用系统常采用隐藏字段存储信息。许多基于网站的电子商务应用程序用隐藏字段来存储商品价格、用户名、密码等敏感内容，心存恶意的用户，通过操作隐藏字段内容，达到恶意交易和窃取信息等行为，是一种非常危险的漏洞。

4.6 跨站攻击

攻击者可以借助网站来攻击访问此网站的终端用户，来获得用户口令或使用站点挂马来控制客户端。

4.7 第三方软件误配置

第三方软件的错误设置可能导致黑客利用该漏洞构造不同类型的入侵攻击。

4.8 Cookie 利用

网站应用系统常使用 cookies 机制在客户端主机上保存某些信息，例如用户 ID、口令、时间戳等。黑客可能通过篡改 cookies 内容，获取用户的账号，导致严重的后果。

4.9 后门程序检查

系统开发过程中遗留的后门和调试选项可能被黑客所利用，导致黑客轻易地从捷径实施攻击。

4.10 其他测试

在安全评估中还需要借助暴力破解、网络嗅探等其他方法，目的也是为获取用户名及密码。

扫描全能王 创建

5 安全隐患说明

5.1 安全隐患: SQL 注入漏洞 经检查未发现此类漏洞

5.2 安全隐患: XSS（跨脚本攻击） 经检查未发现存在脚本攻击

6 通用安全建议

6.1 SQL 注入类

没有被授权的恶意攻击者可以在有该漏洞的系统上任意执行 SQL 命令，这将威胁到数据库的安全，并且会泄漏敏感信息。

针对 SQL 注入，目前的解决办法是：

1、在程序中限制用户提交数据的长度。

2、对用户输入的数据进行合法性检查，只允许合法字符通过检测。对于非字符串类型的，强制检查类型；字符串类型的，过滤单引号。

3、WEB 程序调动低权限的 sql 用户连接，勿用类似于 dbo 高权限的 sql 账号。细化 Sql 用户权限，限定用户仅对自身数据库的访问控制权限。

4、使用具备拦截 SQL 注入攻击能力（专门算法）的 IPS（入侵防御设备）来保护网站系统。

6.2 跨站脚本类

1、在程序中限制用户提交数据的长度。

2、对用户输入的数据进行合法性检查，只允许合法字符通过检测。

3、使用具备拦截跨站脚本攻击能力（专门算法）的 IPS（入侵防御设备）来保护网站系统。

6.3 密码泄漏类

采用 HTTPS 协议，保护登录页面。

扫描全能王 创建

并对用户名密码参数采用密文传输。

6.4 其他类

如上传漏洞修改程序过滤恶意文件；证书错误修改证书；链接错误修改错误链接，开放不安全端口等。

6.5 服务最小化

对系统主机的服务进行确认关闭一些无用的服务或端口，确保主机安全。对数据库的一些端口建议对端口进行做防火墙连接限制，保证不能让外界主机对数据库进行管理。

6.6 配置权限

将网站的各个目录（包括子目录）尽量减小权限，需要用什么权限开什么权限，其他的权限全部删除。

6.7 配置日志

对访问网站的 URL 动作进行记录全部日志，以便日后的审计和检查。

7 附录

7.1 Web 应用漏洞原理

7.1.1 WEB 漏洞的定义

WEB 程序语言，无论是 ASP、PHP、JSP 或者 perl 等等，都遵循一个基本的接口规范，那就是 CGI（Common Gaterway Interface），这也就使得 WEB 漏洞具有很多相通的地方，但是由于各种实现语言有自己的特点，所以 WEB 漏洞体现在各种语言方面又有很多不同的地方，WEB 漏洞就是指在 WEB 程序设计开发的过程中，由于各

扫描全能王 创建

种原因所导致的安全问题，这可能包括设计缺陷，编程错误或者是配置问题等。

7.1.2 WEB 漏洞的特点

WEB 漏洞包括四大特点，即普遍存在、后果严重、容易利用和容易隐藏。普遍存在是因为 WEB 应用广泛以及 WEB 程序员普遍不懂安全知识导致的；后果严重是因为 WEB 漏洞可以导致对数据库中的敏感数据的任意增加、篡改和删除，以及执行任意代码或者读、写、删除任意文件；容易利用是因为攻击者不需要任何特殊的工具，只需要一个浏览器就可以完成整个攻击的过程；容易隐藏则是由于 HTTP 协议和 WEB 服务器的特点，攻击者可以非常容易的隐藏自己的攻击行为。

7.2 典型漏洞介绍

7.3 XSS 跨站脚本攻击

- 漏洞成因

  是因为WEB程序没有对用户提交的变量中的HTML代码进行过滤或转换。

- 漏洞形式

  这里所说的形式，实际上是指 WEB 输入的形式，主要分为两种：

  1. 显示输入
  2. 隐式输入

  其中显示输入明确要求用户输入数据，而隐式输入则本来并不要求用户输入数据，但是用户却可以通过输入数据来进行干涉。

  显示输入又可以分为两种：

  1. 输入完成立刻输出结果
  2. 输入完成先存储在文本文件或数据库中，然后再输出结果

  注意：后者可能会让你的网站面目全非！

  而隐式输入除了一些正常的情况外，还可以利用服务器或 WEB 程序处理错误信息的方式来实施。

- 漏洞危害

扫描全能王 创建

比较典型的危害包括但不限于：

1. 获取其他用户 Cookie 中的敏感数据
2. 屏蔽页面特定信息
3. 伪造页面信息
4. 拒绝服务攻击
5. 突破外网内网不同安全设置
6. 与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等
7. 其它

一般来说，上面的危害还经常伴随着页面变形的情况。而所谓跨站脚本执行漏洞，也就是通过别人的网站达到攻击的效果，也就是说，这种攻击能在一定程度上隐藏身份。

7.4 SQL INJECTION 数据库注入攻击

- SQL Injection 定义

  所谓 SQL Injection ，就是通过向有 SQL 查询的 WEB 程序提交一个精心构造的请求，从而突破了最初的 SQL 查询限制，实现了未授权的访问或存取。

- SQL Injection 原理

  随着 WEB 应用的复杂化，多数 WEB 应用都使用数据库作为后台，WEB 程序接受用户参数作为查询条件，即用户可以在某种程度上控制查询的结果，如果 WEB 程序对用户输入过滤的比较少，那么入侵者就可能提交一些特殊的参数，而这些参数可以使该查询语句按照自己的意图来运行，这往往是一些未授权的操作，这样只要组合后的查询语句在语法上没有错误，那么就会被执行。

- SQL Injection 危害

  SQL Injection 的危害主要包括：

  1. 露敏感信息
  2. 提升 WEB 应用程序权限

扫描全能王 创建

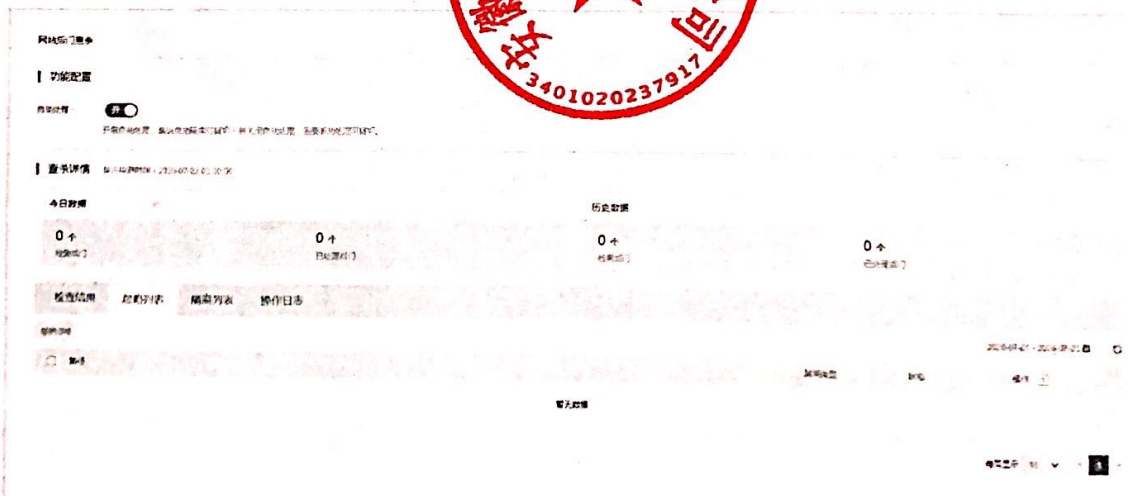
3. 操作任意文件
4. 执行任意命令

- SQL Injection 技巧

利用 SQL Injection 的攻击技巧主要有如下几种：

1. 逻辑组合法：通过组合多种逻辑查询语句，获得所需要的查询结果。
2. 错误信息法：通过精心构造某些查询语句，使数据库运行出错，错误信息中包含了敏感信息。
3. 有限穷举法：通过精心构造查询语句，可以快速穷举出数据库中的任意信息。
4. 移花接木法：利用数据库已有资源，结合其特性立刻获得所需信息。

7.5 木马自动查杀结果：未发现存在木马病毒



扫描全能王 创建