# 目录



# WEB 解题思路

首先附上 P 牛总结的 WEB 解题思路汇总

==========思路==========

一、爆破，包括 md5、爆破随机数、验证码识别等

二、绕 WAF，包括花式绕 Mysql、绕文件读取关键词检测之类拦截

三、花式玩弄几个 PHP 特性，包括弱类型，strpos 和===，反序列化+destruct、\0 截断、iconv 截断、各种协议流

四、密码题，包括 hash 长度扩展、异或、移位加密各种变形、32 位随机数过小

五、各种找源码技巧，包括 git、svn、xxx.php.swp、*www*.(zip|tar.gz|rar|7z)、xxx.php.bak、xxx.php~

六、文件上传，包括花式文件后缀 .php345 .inc .phtml .phpt .phps、各种文件内容检测<?php <? <% <script language=php>、花式解析漏洞、ffmpeg-avi-m3u-xbin

七、Mysql 类型差异，包括和 PHP 弱类型类似的特性,0x、0b、1e 之类，varchar 和 integer 相互转换

八、open_basedir、disable_functions 花式绕过技巧，包括 dl、mail、imagick、bash 漏洞、DirectoryIterator 及各种二进制选手插足的方法

九、条件竞争，包括竞争删除前生成 shell、竞争数据库无锁多扣钱

十、社工，包括花式查社工库、微博、QQ 签名、whois

十一、windows 特性，包括短文件名、IIS 解析漏洞、NTFS 文件系统通配符、::$DATA，冒号截断

十二、SSRF，包括花式探测端口，302 跳转、花式协议利用、gophar 直接取 shell 等

十三、XSS，各种浏览器 auditor 绕过、富文本过滤黑白名单绕过、flash xss、CSP 绕过
十四、XXE，各种 XML 存在地方（rss/word/流媒体）、各种 XXE 利用方法（SSRF、文件读取）
十五、协议，花式 IP 伪造 X-Forwarded-For/Client-IP/X-Real-IP/CDN-Src-IP、花式改 UA，花式藏 FLAG、花式分析数据包
十六、逻辑错误（用户注册、已存在、长度）
十七、ssrf python-django-directory 比如直接 127.0.0.1/../../etc/passwd

# 来几个栗子

### 命令执行技巧

绕过空格
%%0909 代替 空格 $IFS <> 都能来代替空格
我们知道 linux 多命令执行使用 &；等符号 &在 url 传值是需要 url 编码一下

### SQL 注入

一般题目会出现两种情况，一种是简单的 web 页面，另一种是附带登录、注册等功能的页面，简单的就直接上我整理好的 sql.txt 一般都能出结果，除非是盲注。
功能相对多一些的，先整体看处理逻辑功能，然后在逐一测试参数，细心一点，在手工判断的时候注意页面内容的相关变化，比如 2017 国赛的 web300，细心一点你能发现当附带 sql 语句进行注册之后登录，买 key 钱会有相关的变化，成功减少说明 sql 语句执行成功。
还有一些偏脑洞的就是上传文件 filename 值是 sql 注入。
相关的 sql 注入总结可以看 sql 注入总结.doc.
就拿这两个栗子说话吧。
附几个脚本
备份文件扫描
SourceLeakHackerFor.py
反弹 shell 脚本

# 攻防模式一。沙盒模式

题型 ：贴近实际的目标网站，隐含着花样的拓扑结构，flag 不止一个 ，各个沙盒有可能有关联。

入手点：一。实际的网站一般会是通用的开源框架，需要掌握流行开源框架的利用的 exploit。

快速的定位漏洞的位置。

一未果的话，快速扫描目录，是否有信息泄漏，和铭感文件。然后就是定位到后台地址，猜用户名和密码，弱口令是关键。还有待扩思路。

进入后台之后的思路就是先 getshell ，getshell 的思路就是后台的上传漏洞，一般是后台的编辑插件，比如 fuck edit ...绕过这些插件的过滤，再者是数据库备份，数据库命令执行等等。

提权: 这里如果是 window 提权首先如果是 IIS+2003 使用菜刀+pr 或者就是大马+15051exp 来提权。如果有防护，使用组建或者免杀等方法提权。

获取 flag：搜索 flag 文件，一般是在管理员的桌面。

最后扩大战果：

快速的分析此网站所在的网络环境，是否与其他题有关联，是否还存在内网环境等。信息收集的快速定位与扩大化。

这次比赛的总结：

开始 2 个小时的沙盒模式，沙盒 1------→192.168.199.101 提示 don'tscan，没有任何 的思路。

沙盒 2-----→102 是一个 java 的题很像线上的比赛题，这里不是很懂 javaweb 的参数问题就是没有后缀名的内部传参 比如 102/order 显示信息 102/oreder/17 显示 id 为是 17 的信息，这里不熟悉参数的问题。(赛后才知道貌似是 s2 漏洞)

沙盒 3----→103 是一个家具站点，asp+iis+2003，从后台弱口令 admim admin 进入之后就是上传一个图片马，然后数据库备份，getshell 菜刀连接 不能执行 cmd，上传一个 cmd 执行命令，不是 system 权限，使用菜刀+cmd+pr 提权添加用户，3389 连接之后搜索 flag ，最后主办方的提示：沙盒 3 有沙盒 1 的入口信息，到第二天的直接放出了沙盒 1 的入口点，是一个菜刀，需要你 re 一下，检测一下这菜刀的行为，怎么执行的。只 get 一个 flag，并没有做更大化的信息收集，和后续的拓扑扫描。（不足点:后台备份 getshell 不是很熟，提权也出了一些问题）

http://mycms7.cn.adminftp.com/ 沙盒 3 测试环境地址

沙盒 4---→eshop 一个开源的网店系统 3.0 版本，follow.php 注入漏洞未能触发注入，这里也忘记测试后台是否有弱口令了，经验不足。

# 攻防模式二：web+pwn 服务器的组合。

环境说明 web 服务 首先是一个/home/user1/wwwroot 目录下有 flag 文件

Web 目录权限是 777 没有 root 权限 mysql 也是 user1 权限

Web 先说一下一开始的环境， php+mysql 权限都是 r_x 权限 目录在 /home/user1/wwwroot/ 一开始 web 我们就掉了 2 次分。首先搜索连接数据库的配置文件，进入数据库，修改后台的默认密码，删除其他必要的用户。然后进入 web 目录下，修改目

录权限。然后就坐等了一天，竟然 web 就再没有掉分，我也很奇怪，人品爆发了。
后来听到别人的思路就是一开始，上来，猜出了 mysqlroot 的弱口令，udf 提权成功了(不是很清楚)，
直接就 2000 分到手，我很想和师傅们聊聊人生。细节有待实现。
正确的思路是：一开始可以先拼一波手速，破解默认的 admin 密码，直接去后台上传文件，先 getshell 再说。实际是是说 web 至少有 5 个以上的漏洞，师傅们的思路是，注入到管理员的 md5，进后台，上传文件 然后包含 getshell。获取权限持续得分。
正常的策略是 tar 打包 web 目录的文件到/tmp 目录下然后 scp 下载下来，审计测试。

Pwn 不会 一直掉分，第一天没有跌机 掉分相对来说比较少，人品。

######################权限问题和脚本####################

Wwwroot 目录 的权限 没有摸的很清楚，

```
[user1@199-205-GameBox-05]: /home/user1/wwwroot
➜  l                                                                    [2
total 76K
dr-x------ 7 user1 user1 4.0K Jul 21 22:38 .
drwx------ 4 user1 user1 4.0K Jul 21 22:46 ..
-r--r--r-- 1 user1 user1 2.7K Apr 25 16:03 about.php
dr-xr-xr-x 4 user1 user1 4.0K Jul 21 22:40 Admin
-r--r--r-- 1 user1 user1 2.7K Apr 25 16:03 contact.php
dr-xr-xr-x 6 user1 user1 4.0K Apr 25 15:41 Edit
-r--r--r-- 1 user1 user1  333 Apr 25 16:03 .htaccess
dr-xr-xr-x 7 user1 user1 4.0K Apr 25 15:41 Images
dr-xr-xr-x 2 user1 user1 4.0K Jul 16 02:11 Include
-r--r--r-- 1 user1 user1 4.5K Apr 25 16:03 index.php
-r--r--r-- 1 user1 user1 3.4K Apr 25 16:03 info.php
-r--r--r-- 1 user1 user1 3.3K Apr 25 16:03 news.php
-r--r--r-- 1 user1 user1 3.7K Apr 25 16:03 product.php
-r--r--r-- 1 user1 user1 3.2K Apr 25 16:03 search.php
dr-xr-xr-x 3 user1 user1 4.0K Apr 26 11:06 Templete
-r--r--r-- 1 user1 user1 7.1K Apr 25 16:03 view.php
-r--r--r-- 1 user1 user1  359 Apr 26 09:57 使用说明.txt
```

Wwwroot 权限是 7 子目录文件是 r 权限
测试 udf 提权(赛后问了一下大家都没有 root)
定制脚本优化一下
这里修补漏洞的方式：
系统防护
Netstat kill 进程
自动化脚本
暴力删除 敏感文件

首先备份网站目录， 后续的做 diff 命令比对，是否被写后门 shel 了没有 l
首先我们写一个脚本
把我们防护的脚本包含到 php 文件中进行防护

然后可以写一个定时删除 shell 文件的脚本，不允许在文件夹中写入文件

一：不知道漏洞首先包含 php 脚本到 web 文件中做 url 参数获取日志后续在分析
二：包含 waf.php 文件做 sql 注入 xss、srf 等漏洞的通用防护(做全局变量的防护)
三：审计代码发现已知漏洞，做代码上的修补
四：做流量的混淆，防止被人流量重放。
五：包含自动删除 shell 脚本
六：总结的思路，首先我们可以抓取别人的流量 然后利用别人留下的密码什么
比如丝绸杯 我们当时发现我们的 admin 表中被添加了用户
我们可以用他这用户登录别人的服务器后台，然后再上传 shell 什么的

# 攻防脚本

1. 线下比赛记实

http://mp.weixin.qq.com/s?__biz=MzIyNTA1NzAxOA==&mid=2650473772&idx=1&sn=383dd055f2fb51326ebd280c64cd0481&scene=23&srcid=0727uXSMW2H22z3M9GtVcmXH#rd 线下比赛纪实

http://mp.weixin.qq.com/s?__biz=MzI0NTA3NzQ2MQ==&mid=400219727&idx=1&sn=ef52130e5abe78231fc7ecb52dfab30d&scene=23&srcid=0727mNmx7vUY433OxmmAA4qZ#rd

http://mp.weixin.qq.com/s?__biz=MjM5NjkyMTk5Mg==&mid=200915617&idx=2&sn=50fb575f04e3c5b1acea6dbaf594a0d0&scene=23&srcid=07277VWPlLebnsrF3tO5fBrO#rd

http://5alt.me/posts/2014/10/AliCTF2014%E5%86%B3%E8%B5%9B%E8%AE%B0%E5%BD%95.html

http://mp.weixin.qq.com/s?__biz=MjM5NTU2MTQwNA==&mid=2650652095&idx=2&sn=ba608435b3f215e8c93e58556caa1df3&scene=23&srcid=072784JTwY6uY8ww7yoeU701#rd linux 脚本维护系统

http://weibo.com/p/1001603847172578749357?mod=zwenzhang

这里猥琐的不死马和进程后门

http://byd.dropsec.xyz/2017/05/16/CTF%E7%BA%BF%E4%B8%8B%E8%B5%9B%E7%9B%B8%E5%85%B3%E5%B7%A5%E5%85%B7/

http://bobao.360.cn/ctf/detail/169.html

https://blog.rexskz.info/index.php/2016-nationwide-ctf-final-writeup.html

http://rcoil.me/2017/06/CTF%E7%BA%BF%E4%B8%8B%E8%B5%9B%E6%80%BB%E7%BB%93/

2. 实时监控 cms 的脚本

源码的修改进行加固操作

fork 炸弹 https://linux.cn/article-5685-1-rss.html

比赛开始之前准备好各种自动化脚本，例如常见 Cms 漏洞 exp、批量获取 shell 自动化脚本、

# 来俩案例

案例一： 2016 年丝绸杯
web 文件源码 和批量 getshell 脚本

有附件

案例二：第三届网络空间大赛
Web 文件 和批量 getshell 脚本

有附件

# Web 防护加固实现

## 1.有 root、administrator 权限的防护

首先环境是 phpweb 防护，首先直接修改 php.ini 修改 设置为安全模式然后直接禁止大小马的函数，

disable_functions =
passthru,exec,system,chroot,scandir,chgrp,chown,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server
然后再开启安全模式
`pcntl_exec()` 可以绕过
http://security.ctocio.com.cn/tips/5/7764505_5.shtml
全部禁止

# 2.非 root 权限的防护

http://blog.csdn.net/andy1219111/article/details/9054277
打包 web 目录文件
下载保存扫描是否有内置后门
常规的修改默认的用户名和密码

1. 首先去查看 web 目录下链接 sql 的配置文件，获取数据库的密码，然后登陆数据库修改网站的默认后台密码。是否有 file 权限
2. 修改 web 目录下文件的权限，设置 600，指定目录的权限设置 400 等，具体的文件具体设置，或者直接设置 upload 文件权限为 chmod 000
3. 写一个自动删除 shell 的 php 脚本，白名单，自动删除目录下多出来的 php 文件
   Watch –n 1 rm –rf uploads　每 1 秒定时删除 uploads 文件
4. 加载防护 waf safe 等 php 的脚本，抓取流量或者写脚本动态监控 脚本请参考<攻防脚本中的连接地址>
5. 对特定的漏洞进行代码上的修改补上漏洞。
6. 如果手速慢了被植入了内存马，一种是分析 php-fmp 进行进行查看，申请重启服务
   另一种是，内存马判断文件，可以手动添加一个文件，内容可以随意了，只要存在此文件名的文件就可以了

7.如果主办方 check 的不严就直接删服务
8.赛后向主办方申请要自己服务的日志，一定要做赛后总结，日志分析

# 动态监控踩点防护

1. 使用 server.php 抓取 get,post,request 等数据包
2. Py 实施 md5 检测目录，是否有新增、改动、减少等文件
3. 手动检测本地测试

具体办法：
首先，php 文件内容头批量先导入抓数据包的 php 脚本和 waf 脚本
然后实施动态监控
这里功能可以预先集成在一个 py 脚本中
具体方法和脚本在【加固脚本】文件夹中

# 漏洞查找

1. 首先扫描 web 文件，是否含有主办方隐藏的后门 附脚本：查找后门木马

```
文件位置:  html\phpcms\modules\admin\functions\admin.func.php
base64_decode('PHNjcmlwdCB0eXBlPSJ0ZXh0L2phdmFzY3JpcHQiPiQoIiNtYWluX2ZyYW1laWQiKS5yZW1vdmVDbGFzcygiZ --------->The code in 32 line
```

Opensns 这里就印证了主办方留有后门

直接

```
url = "http://40.10.10.%s/index.php?s=/weibo/index/index.html" % (num)
print url
data={
    "welcome":"system('cat /home/flag');"
}
```

可以直接刷 flag

2. 再一系列的防护之后，代码审计是否有包含 命令执行漏洞
3. 确认有漏洞上传的 shell 到 uoload 文件
   一般 upload 文件是 777 权限 所以我们可以
   Watch –n 1 rm –rf upload 每隔 1 秒 删除 upload 文件
4. 内存马的使用，第三届网络空间大赛中学习到使用内存马+手速的模式，然后使用批量的脚本，感觉很无解
5. 加载防护日志，抓取流量或者从别人的服务上分析 shell 使用别人的 shell 进行批量
6. 应对备份查找后门，我们可以上传一个具有上传功能的 upload.php,再使用内存马来进行隐藏
7. 高一点的赛事，可能网上难以搜索到现成的 exp、poc 这时就需要审计代码，一般持续的时间相对比较久。

附一下一些通用漏洞

**列表**

memcache 未授权访问 java 反序列(struts2 可以细分) jenkis jenkis 配置不当 心脏出血 nosql 未授权 glashfish 任意文件读 ms10-070 padding orcles jdwp 调试漏洞 mogodb 未授权 iis put 解析漏洞 svn 信息泄露 redis 未授权 域传送 iis 短文件名 ElasticSearch 漏洞..... 后待续

一定好多动手复现，比赛的时候才能拼手速。

最后复现 P 牛的这个漏洞库

https://github.com/phith0n/vulhub/

最后欢迎大家来搞基

**Author:Seck https://github.com/Huseck**