CTFweb中常用套路

原创

Flemington、 于 2017-05-10 18:05:10 发布
分类专栏： web 文章标签： web CTF

0x.前言

最近忙着上课，忙着考试，刷题少着可怜，今天碰巧看到之前长亭科技某ppt中某大佬简单说了一些web方面的套路，才决定结合自己状况，来写一写。方便以后做题嘛

1x.正文

0.常用爆破，其中就有MD5，验证码识别，爆破随机数。

1.绕WAF，花式绕Mysql，绕文件读取关键字检测之类的拦截。

2.几个常见的php特性，其中就有弱类型，反序列化+destruct，\0截断，iconv截断。（最近在学php，等熟练一波后，再补一篇）

3.密码题中就包括hash长度扩展，异或，移位加密的变形，32位随机数过小，随机数种子可预测。

4.各种找源码的技巧，git，svn，xxx，php.swp，*www*...（zip|tar.gz|rar|7z），xxx.php.bak。

5.文件上传，其中就有文件的后缀，php345.inc.phtml.phpt.phps，各种文件内容检测<?php<?<%<script language=php>,花式解析漏洞。

6.Mysql类型差异，包括和php弱类型类似的特性，0x，0b，0e之类，varchar和integar相互转换，非strict模式截断等。

7.open_basedir，diable_functions花式绕过技巧，包括dl，mail，imagick，bash漏洞，Directorylterator及各种二进制选手插足的方法。

8.条件竞争，包括竞争删除前生成shell，竞争数据库无锁多扣线。

9.社工，花式查社工库，微博，qq签名，whois。

10.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。

11.SSRF，花式探测端口，302跳转，花式协议利用，gophar直接取shell等。

12.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。

13.XXE，各种XML存在地方（rss/word/流媒体），各种XEE利用方法（SSRF，文件读取）。

14.协议，花式IP伪造X-Forwarded-For/X-Client-IP/X-Real-IP/CDN-Src-IP,花式改UA，花式藏FLAG，花式分析数据包。

==========

CTF中web比分比较多，相比其他的PWN，MISC,REVESE,CRYPTO都是稳扎稳打的题型 WEB更需要技巧，WEB要学习和了解的东西也很多。

既然选择了CTF，就慢慢的学习 ↖(^ω^)↗加油~推荐白帽子讲web安全等书籍~