[happyctf]部分writeup

转载

weixin_30597269 于 2017-07-10 22:26:00 发布 197 收藏
原文链接：http://www.cnblogs.com/deen-/p/7148071.html

题目名称：sqltest所属：MISC考察点：盲注 眼力 耐心（好吧是废话）

附件下载下来，到手一个流量包，用wireshark打开，大致浏览了一下，抓的应该是盲注的数据流量。

这里有一个经验问题，一般的数据流量包，这样的杂项题，二话不说，直接导出，选择导出http对象，save all。

导出后的截图如下。

不知道你们的是怎样的，我的windows7，默认按“名称”排列。

这是一个盲注，我们现在要找的就是从这些这么多语句当中找出盲注当中True和False那一个临界。这里使用的ascii，我们要做的就是把那些按顺序记下来。

打开这些文件分析，比较可得以下：

1.真值为true时候 文件内容中 有“version” 这个关键词。

2.真值为true时，文件大小为780字节。

这里也就有两个思路，一个是写个脚本把包含version的文件挑出来，还有一个就是利用大小判断，进行筛选。

这里我选择后者，比较快，让文件按大小排列，找到780字节的地方，然后找到是查看flag的盲注语句。这里很巧的一点是按大小排列之后 还按了名称顺序排列，所以，直接照着顺序记下来就可，可得如下结果。

后面圈起来的就是我们要的ascii的值。

题目名称：包罗万象所属：web考察点：文件包含

这题比较简单，这提示得太明显了，“包罗万象”，一个文件包含的题目。

访问靶场，发现有个url是index.php?url=upload

进一步探索题目，发现存在flag.php，那就没什么好说的了。

换成，这直接访问，并没有什么，转一个弯，加一个伪协议。

Base64解密，出flag。

给一个伪协议介绍传送门：

http://blog.csdn.net/Ni9htMar3/article/details/69812306?locationNum=2&fps=1

感谢大佬。

题目名称：我的博客所属：web考察点：文件泄露 代码审计 文件包含

看题，如果不是太简单的题的话，个人做题一般都是先分析一遍题目，看我们能得到哪些有用的信息，**还要一个关键点就是搞明白flag在哪，我们要怎样做才能出flag.**

分析得到的信息如下：

1.Flag在/key/flag.php源码里面

2.标题：备份是个好习惯。

第二个是很明显的一个提示，我们访问blog/www.zip

就把源码下载下来了。

接下来就是代码审计的问题了。

在post.php

图中圈圈是我本地搭建添加的，看到参数的输出，便与调试。

然后我们的目标就是访问flag.php了。

可得结果如下：

查看源码，看源码。

题目名称：login所属：web考察点：文件泄露

这题打开是一个登录界面，如图

尝试输入爆破均无效。实现想不出来了。

回到原题题干，提示是用txt写的。

很明显，这是提示编辑器啊。txt会残留的备份文件的后缀是.bak，

访问check.php.bak。

去登录，拿到flag.

题目名称：留言板投诉所属：web考察点：报错注入，sqlmap

打开界面如图所示：

各种尝试无果，抓包分析

抓包改参数，在class这里发现了端倪，详情如下。

开了gpc，普通的注入是无效的，想到了报错注入，大概是姿势的问题。

卡了一会，直接上sqlmap。

题目名称：新闻所属：web考察点：盲注注入，sqlmap

手工测试了一波，发现是注入点是：

viewId.do?Idid=0||1

1处就是我们的盲注点。

一般盲注题目都会有过滤，所以，我fuzz一下，发现过滤了如下关键字：

And,or,Select ,for ,from ,where等，但是这里比较简单，可以大小写绕过。解题的时候我用的是自己一个写的可以复用型的脚本，这里我想用sqlmap跑一下。

这里用到的是sqlmap的tamper脚本：

randomcase.py随机大小写

我加了两个脚本，

andreplace.py替换and为&&；orreplace.py替换or为||

参数截图如下：

测试了一下，加了happyctf脚本，强制把ORD换成oRd，绕过or过滤。

这里给几个sqlmap深入学习的传送门：

用户手册：http://www.cnblogs.com/hongfei/p/3872156.html

进阶使用：http://www.tuicool.com/articles/BFVbqe

Sqlmap前世今生part1：http://www.2cto.com/article/201509/442345.html

Slqmap绕过脚本整理：http://blog.csdn.net/whatday/article/details/54774043

工欲善其事必先利其器，欲利器，必先知器。

感谢以上文章的大佬们！

还有几题没搞清楚，后面更新

2017 7 10 更新

题目名称：register 所属：web 考察点：代码审计

这题是真的没想到，只能喊666

转载于:https://www.cnblogs.com/deen-/p/7148071.html