一月月赛出题过程记录

原创

youGuess28 于 2019-01-20 10:02:13 发布 379 收藏 3
分类专栏： 出题 文章标签： Web安全 ctf

记我第一次出月赛题

出题思路

刚听说要试着出个题目的时候...emmm...心方方，不知道要出什么，觉得自己没什么想法，首先给自己定位，难肯定是难不到大佬们的，就是个锻炼过程，`take easy` 。
我就开始想啊，我这一个学期都看了些啥。

1. 想到最开始`ECShop`那个`sql`注入利用链，很长一串，我感觉出不出来，利用都要那么长，我编那么长的代码应该很费劲吧...而且出这种大概是要把`cms`源码搬上来吧？
2. 之前调的`Orange`大大的`CVE-2018-5711`，通过构造一个图片来让服务器宕机。嗯？？服务器宕机？？都宕机了，还可以做题目嘛？？？
3. 在简书上看到的一个`php7`的小`bug`，可以用在本地文件包含上面，这个可以考虑，留着了，最后出题也用上了。

我好像就想了这几个，`sql`注入没想着出，感觉不知道怎么写...虽然最后还是出了`sql`注入。

之前做过安恒杯十月的月赛，就想着看看，有没有可以借鉴的想法，然后翻网上的`writeup`，就决定用 利用子查询来在不知道字段名的情况下`sql`注入。其实大佬肯定方法论一下，卡卡两下都做出来了...emm...但是这也不能不让我出它吧？？

初步的想法定为：最初始的界面是一个类似于搜索框的东西，在里面查询，进行`sql`注入。注入成功，数据库给写文件权限，通过写入一句话木马，`getshell`。哈哈，多么友好的一道题。

后面在出的过程中，想着还是再用一个文件包含吧，在数据库中提示存在本地文件包含漏洞的`php`文件名称，然后包含通过`sql`写的文件，当然这个文件就不允许写到`web`目录下了，只能通过文件包含来执行其中的指令。

然后，又突然想到了上面提到的`php7`的小`bug`，试了一下在我用的`docker`里是存在的哎，那正好，就把这个用进来吧。

所以，**最终**的题目是：

1. 进行`sql`注入，拿到数据库中存着的可以包含文件的`php`文件名(接下来就叫它`include.php`)以及对应提示；
2. 使`include.php`包含自身，造成崩溃，同时，`post`文件内容为一句话木马的文件，由于`php`崩溃，来不及删掉被上传的临时文件，我们就可以成功上传文件到临时文件目录，默认是`/tmp`
3. 之后就是爆破我们上传的一句话木马的文件名了，这个要爆破好长时间了...看运气吧。

对于第`2`点，我关掉了默认开启的`session.upload_progress`，这个是今年`hitcon`的那个题目的做法，emm...关掉应该就可以了吧。我后面也没测试过哎。(又测试了一下，关掉就没事啦，不会记录下来`session`文件了，o98k)

现在还不知道可能有哪些非预期的做法，或者是我没考虑到的地方，等月赛结束了，我会再回来补一下的。

出题过程

接下来就是出题过程了。

Web界面

我在网上找了一下搜索框的`html`模版，看到一个满意的，但是要钱...很绝望，然后突然灵机一动，`css`那些不都是可以看到的嘛？？我可以`ctrl+c ctrl+v`呀。然后就`F12`，不道德地拿到了我想要的那个模版的所有源码，再按照我的要求改改，完美。（还有，在找模版的网站竟然有错误信息回显，emm，`mark`一下，之后可以看一下能不能复现，有没有问题）

数据库配置

以前用数据库就只用过`select` `union select`这些最基础的，没有新建过用户，没有给过用户权限这样的，这些都接触了一下，虽然很简单哈。

`get`到几个知识点：

1. 默认安装后，`mysql`是没有密码，直接可以登录的，要修改一下`root`用户的密码，我的`mysql`版本试`5.7`，因为`user`表变了，所以更新语句也有些不同：
   `update user set authentication_string = password('root'), password_expired = 'N', password_last_changed = now() where user = 'root';`
2. 刚开始是想给新建的用户读写文件权限的，然后一直配置不成功，在网上找，发现：
   `file 作为一种管理权限，要赋予用户时，只能*.*`解决问题，当然，后来我又把这个权限给`revoke`了。记得要执行这个语句：
   `flush privileges;`

把数据弄好，好像就再没其他的了。

代码编写

代码其实很简单，就是过滤用户传递的字符串，然后连接数据库，放到数据库中去查询，相应提示，完事~

好像就卡了一下吧：
`preg_match("/information|union select|,|/i", $id);`
我刚开始把正则匹配表达式写成这样了，导致不管怎么样，都会匹配到一个空，把最后一个竖线去掉就好了。

Dockerfile编写

最后一步了。好像因为不舒服花了很多时间来着。以前都是直接在`docker`里面改，改完`commit push`到`docker hub`上的，然后这次试一下写`Dockerfile`，之前简单写过几次，这次用的更多一点?，虽然还是很简单，又`get`到一些新的知识点。

如果`docker run`之后，想`docker exec`到`docker`内部去操作，发现提示`docker`并没有在运行，那就说明启动失败，失败原因可能是遇到了执行错误，然后进程直接关掉了，导致`docker`运行结束。可以通过指令`docker logs container_name`来查看日志信息。

学会查看各种日志信息真的很重要啊，让自己做事情的效率可以高很多，要不然就只能瞎试。这个问题我其实见过很多次，到这次才真正明白原因。

另外，我们每次执行这个指令`docker run -id --name xxx -p xxx:xxx xxx /bin/bash`，我其实以前一直都不知道后面的`/bin/bash`是什么意思，它代表着`container`起来以后，要一直运行这个指令，这是一个主进程，只要这个主进程没有结束，`container`就一直处于运行状态，否则就会`Exited`。还可以指定`container`起来之后运行的`shell`脚本，就比如`docker run -id -name xxx -p xxx:xxx xxx /bin/bash setup.sh`这样，当然`setup.sh`里需要有一个死循环，保证该进程不会结束，而且`setup.sh`是指`container`里的`setup.sh`，所以路径要写对。`docker run`指令里指定的`container`起来之后运行的指令，会将`Dockerfile`里的`CMD`指令顶替掉，`docker run`指令里指定了之后，`CMD`指令就不会再执行了，要注意一下，另外`CMD`指令在`Dockerfile`里只会执行一个，如果有多个，就只执行第一个。（这些其实看相关文档，很简单就直接知道了，但是以前用着一直没出错，所以就没有仔细去查，老毛病?）

查资料的时候发现说`Dockerfile`中的`RUN`指令执行一条就会建一个镜像，所以如果有多个指令，没有特殊需求的话，最好写到一条`RUN`中，用`&&`连接（刚开始用`&`连接来着，emmm，眼睛是个好东西，希望自己有），否则会使得镜像太过臃肿，体积过大。

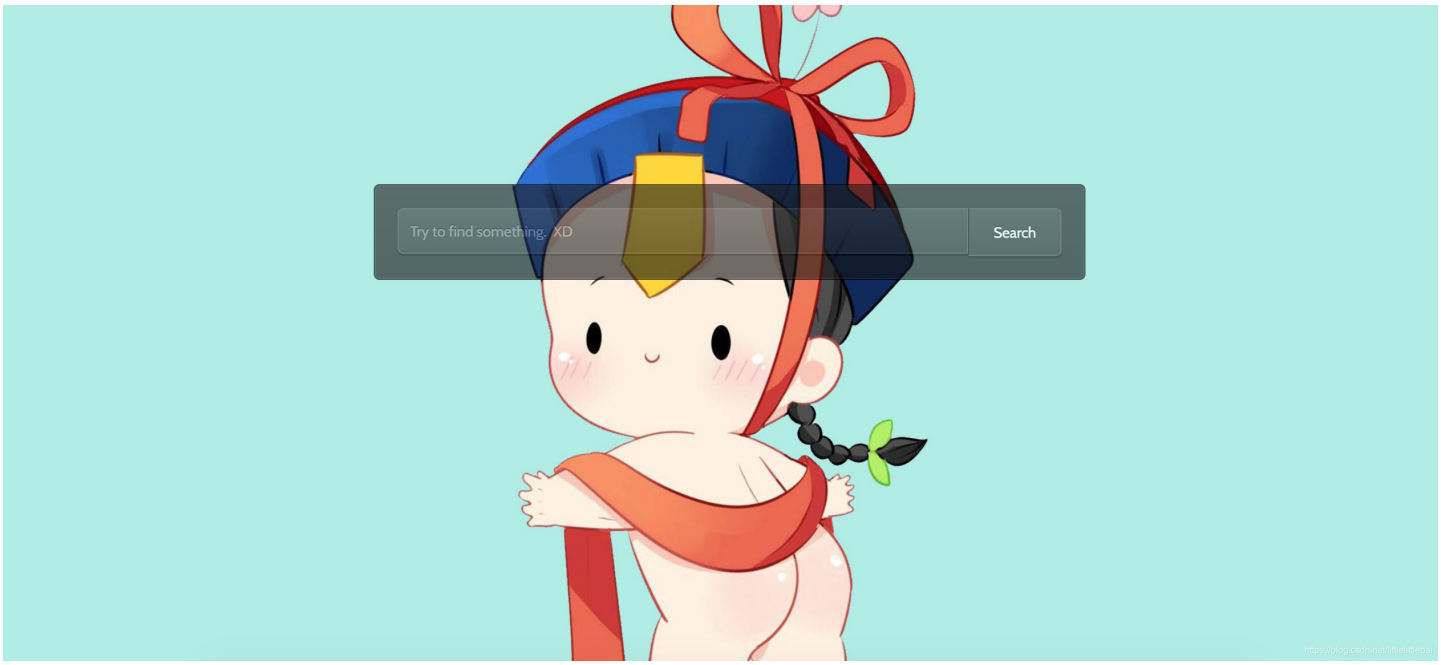
之前有一次弄`docker`时候就发现，进去之后`apache`服务要重启一下才可以用，这次同样问题，所以在执行的启动脚本里，设置重启要用到的服务（`mysql apache`），刚开始因为这个导致数据库里数据一直都装在失败。

另外还有一个使用`nc`指令传文件，可能大家都已经很熟悉了，我是之前有一次要跟同学传文件时候才发现的...很方便。

```
+ nc -l port >file --- nc ip -p <file (方法一)
+ nc -l port <file --- nc ip -p >file (方法二)
+ --> ">"是写入的，就像echo >这样的，"<"是发送
```

好像差不多了。以后做一个东西的时候，可以在做的过程把遇到的问题记到草稿文档里，等到总结的时候就不会错过每个遇到的问题啦。

题目Writeup



哈哈，我喜欢的小僵尸。
写到本地啦。

月赛结束

昨天月赛结束啦，还不错，没有被大佬喷，虽然由于实际布题时候出了点问题，导致`php.ini`没有被正确替换，也就是说`upload_progress`没有被关掉，最后还是通过`hitcon`的`one-line-php`那道题目的方法去做的...不过，正好大佬说我原本的出法通过爆破来得到上传的临时文件名，实在太鸡肋了?，而且这个套路都已经被出烂了...随缘吧，总的来说，第一次出题目，我自己很满意，希望以后在学习的过程中，能多注意到一些细节，可以多留意一些出题的思路。

`sql`注入好像是都过滤全了，没有被非预期，听说师兄还卡住了呢，哈哈哈。

然后之前说是让我学习一下`docker compose`，用这个来写自己的`docker`，我刚开始理解的意思是，后台布所有题目的时候是要用`docker compose`把各个题目的`docker`管理起来的...emmm...原来是说让我把每一个服务，就是`apache` `mysql`这些，都分别起一个`docker`，然后用`docker compose`管理这些，成为一整个题目的环境。?原来是这个意思，学习了。

另外，我还被夸了。总之，这次月赛不管是自己出的这个题目，还是我做的另一个题目，都有很多收获，也更加认识到方法论的重要性，一定要在做题目的过程中运用方法论，指导自己做题思路。
好啦好啦~~开心

弱弱地给一下`docker`：
`docker pull gaoxijiejie/month:latest`