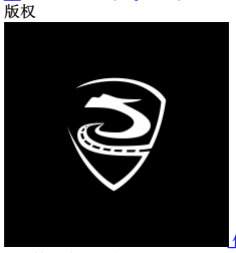
CTF初识与深入

转载

myh0st@信安之路 于 2022-04-10 19:46:13 发布 21 收藏
分类专栏： 信安之路 文章标签： web安全
原文链接：https://mp.weixin.qq.com/s?__biz=MzI5MDQ2NjExOQ==&mid=2247484446&idx=1&sn=21f929d5f230c41dc70a3120d7dba9d4&chksm=ec1e3436db69bd20cd2ac8a711edf2d1ebd8b0d83b0694a2e5d57eb2c79bf6c6315c891d2317&token=2038700666&
版权



这段时间一直在忙活CTF相关的东西，从参赛者到出题人，刷过一些题，也初步了解了出题人的逻辑；这篇文章就简单地讲一下CTF如何入门以及如何深入的学习、利用CTF这个训练、学习平台。

文章里会涉及的一些资源：http://pan.baidu.com/s/1jlDpV8q

CTF认知

CTF可以理解成一种锻炼和学习信息安全技术的训练场，具体的解释在百度以及这篇安全维基~上都有，就不再赘述了。而CTF对信安人员的意义，在我看来，是扩宽我们的安全知识面，以及实战式应用我们学到的安全知识。随着《网络安全法》的公布，以及企业安全意识的增长，信安领域刚入门的小白越来越难找到真实、合法的环境来训练自己的技能。而CTF的出现，弥补了这个空白。

如何入门CTF

CTF分为Web、Reverse、Pwn、Crypto、Mobile、Misc六大类，我是走web方向的，偶尔也做一下misc。在这篇文章里，就以web为切入点，讲解一下如何开始，以及ctf学习带给我web技术那些启示与收获。

没有接触过ctf的小伙伴可以先看看这个

```
https://ctf-wiki.github.io/ctf-wiki/#/introduction
```

里面对ctf的介绍。

要开始ctf生涯，刷题是第一步，在这里贴一下精灵大大的ctf训练场集合：

```
https://www.zhihu.com/question/30505597
```

总结得非常全，对于web方向，重点强调一下bugku这个平台，真的很不错，题目很经典，只有两三个脑洞比较大，体验不是很好。想要学知识的可以先把bugku刷上一遍。

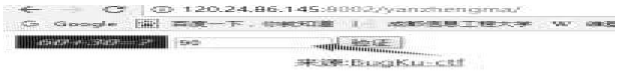
当然，刷题也有刷题的方法，那就是必须要搞清楚题目背后的知识点点原理。不然即使你似懂非懂地拿到了flag，对于个人的成长也是无济于事。一道题扣一天，搞懂了原理不是浪费时间；照着write up刷了一遍，背后原理啥都不懂才是真的浪费时间。

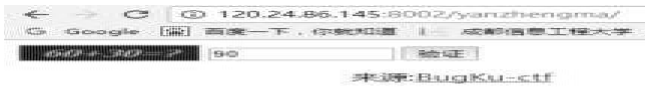
在这段事件的学习之中有几个知识点，让我受益颇多，贴出来给大家分享一下。会尽量找一些可以复原环境的题目，供大家测试。

PS：由于我在写文章的时候bugku平台正在维护，所以可能题目链接之后会换，如果链接失效的话，大家可以去搜一下bugku的入口，题目名称是对应的。

1、Bugku——计算题（http://120.24.86.145:8002/yanzhengma/）

这道题很简单，在HTML里限制了输入数字的长度，所以通过快捷键F12，Element处修改长度限制，然后输入90，getflag就行~





之所以把这么简单的题目贴出来，是想要强调一下，浏览器的调试功能，就像这道题里的可以修改HTML代码一样，JavaScript代码以及CSS代码都是可控的。在实战过程中程序员将过滤函数或者重要数据写到了HTML或者JavaScript里面，我们就可以轻松获取。控制台也可以执行我们的JavaScript代码，实现一些mazing的功能。比如在真实场景就遇到一个，某刷题网站（高中题），是通过js发送成绩数据输入进数据库的。这么一来完全可以拦截下请求，修改数据，分分钟一百分。

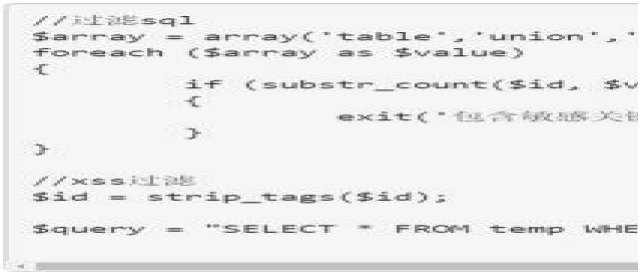
浏览器的调试功能很强大，Chrome的自带F12就基本够用，火狐的Firebug插件也很牛。如果想进一步学习可以看下面的两个连接：

```
http://wiki.jikexueyuan.com/project/chrome-devtools/

http://www.runoob.com/firebug/firebug-tutorial.html
```

无论是对CTF还是实战都非常有用，再次强调，打CTF是为了获取知识。

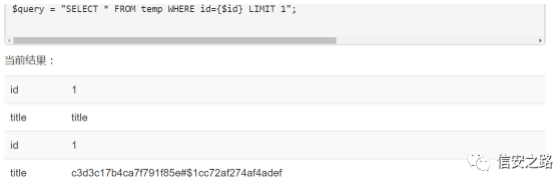
2、Bugku——SQL注入1（http://103.238.227.13:10087/）



过滤了几乎所有的关键字，尝试绕过无果之后发现，下面有个xss过滤代码。经搜索得该函数会去掉所有的html标签，所以向注入关键字中插入<>，就可以不被检测到，并成功注入；

Demo

```
http://103.238.227.13:10087/?id=1%20uni%3Chtml%3Eon%20sel%3Chtml%3Eect%20%201,hash%20fr%3C%3Eom%20sql3.key%20w%3C%3Ehere%20id=1--+
```



Get flag！

这道题并不难，但想要强调的是这种白盒审计的思路。有幸认识一个审计超神的大佬，听他讲审计的时候，就经常见到类似这种情况，本来两个过滤都很严实，但放到一起时，就可以用前一个过滤函数去绕过后一个过滤。这是程序员在写程序时常犯的毛病，指的Mark一下。

3、Bugku——Flag在index里（http://120.24.86.145:8005/post/）

进入题目发现有一个file参数，查看源码，发现该参数可以包含php文件，并且题目提示，flag在index.php里，所以想到可以用php协议来获取index.php的源码。

构造payload：

```
http://120.24.86.145:8005/post/index.php?file=php://filter/convert.base64-encode/resource=index.php
```

获得经过base64编码后的源码，放到hackbar里解码一下得：

Getflag~

这道题需要注意两点，第一就是php协议，在这个文件包含的点使用php协议就可以读取任何文件源码，类似地还有data协议，file协议。web协议的种类多，利用方法也多，可谓是实战中的一大利器。在CTF线上赛中也经常用到，比如上次CUIT校赛以及西安的那个XCTF比赛中就用到了phar://协议。

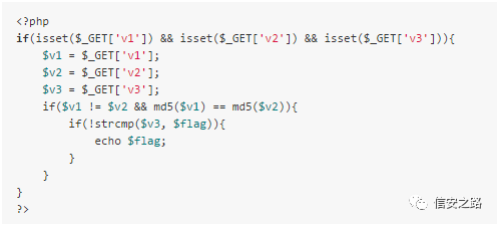
想要仔细了解的伙伴可看一下：

```
http://php.net/manual/zh/wrappers.php
```

4、Bugku——前女友（http://47.93.190.246:49162/）

点开源码发现一个txt文件

访问得到部分源码:



总共考察两个php弱类型的知识点:

第一个是md5双等号相等: md5('240610708') == md5('QNKCDZO')

第二个是数组和字符串进行strcmp返回0

所以payload:

```
http://47.93.190.246:49162/?v1=240610708&v2=QNKCDZO&v3[]=123
```

分类情况，以及少数的几个知识点~审计相关，以及join，就BUG库的提醒进行介绍。 Php弱类型算是PHP语言的一大特色了，在CTF中经常遇到，实际的白盒审计中也很常见。 详细可参见:

```
https://www.dexcoder.com/RAnders00/article/4602
```

5、 Bugku——login1

SQL约束性攻击，在检测用户是否已存在的问题上把控不严。介绍文章：

```
http://www.freebuf.com/articles/web/124537.html
```

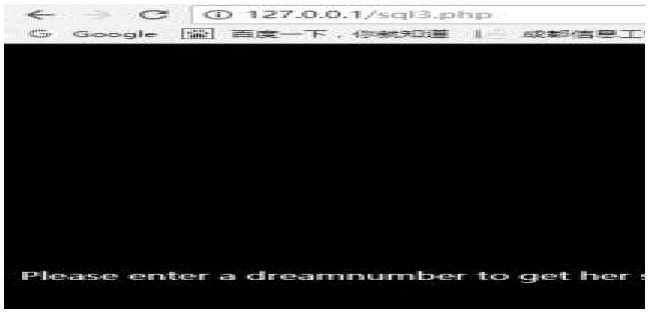
注册的时候多留几个空格就可以更改admin的密码了~

具体原理已经在上面的链接中介绍得很清楚了，就不再赘述了。

CUIT实验班考核——SQL2

源码在压缩包里，可自行搭环境测试，过滤了逗号和空格。以下是我写的writeup：

拿到题后发现:



发现提示里说，女神喜欢饼干（COOKIE）所以猜测为COOKIE注入。这时就需要工具了，最方便的是用BurpSuite抓包送到Repeater，然后在原有Cookie后面加上分号

拿到题后，先测闭合情况，找一下原语句是用什么闭合的，单引号？双引号？括号？最常见的就是单引号。

测试的方法就是挨个用(1 -1 1’ -1’ 1# -1# 1’# -1’#)来测。本题是用 ’ 闭合的。

然后开始测试段数，使用order by 无回显后，可以用

```
-1’ union select 1,2,3……n
```

来测，测到回显位显示出我们的数字即可。但这道题在尝试的时候会报“what are you doing”，应该是某个关键词被过滤掉了。所以在源语句的基础上依次删掉某个词，每次只删一个，如果都不行，就一次删两个。最后测出来是空格和逗号被过滤了~

空格很好绕过，可以用//来绕，检测是否绕过成功可以用and//1=1#和and/**/1=0#来测。逗号在尝试编码绕过无果之后，去网上找到了:

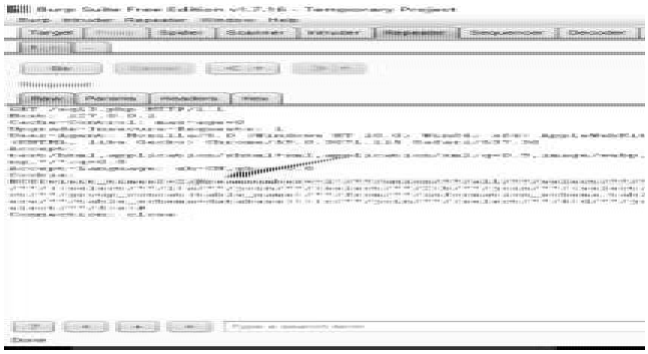
```
http://drops.blbana.cc/2017/05/20/SQLi-%E2%80%94%E2%80%94-%E9%80%97%E5%8F%B7%EF%BC%8C%E7%A9%BA%E6%A0%BC%EF%BC%8C%E5%AD%97%E6%AE%B5%E5%90%8D%E8%BF%87%E6%BB%A4%E7%AA%81%E7%A0%B
```

这篇文章，根据文章的内容再去查一下join的语法，再按照SQL注入的常规流程（不清楚的话建议刷一遍sqli）就可以构造出payload。

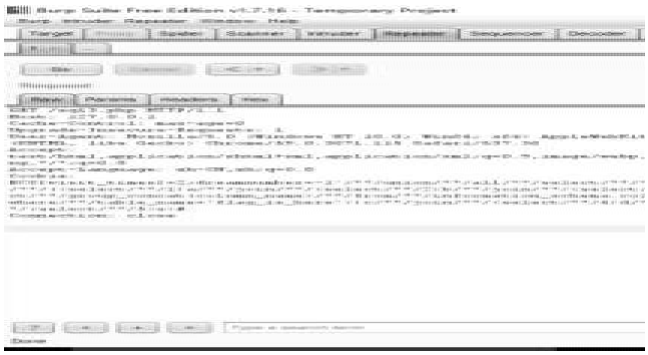
Payload截图如下：

爆库名：

爆表名：



爆列名:



爆FLAG~

小密圈——Mysql字符集问题

这个点非常棒，P师傅（这个博客必须收藏啊~有没有）已经讲的很清楚了：

```
https://www.leavesongs.com/PENETRATION/mysql-charset-trick.html
```

8、php4fun——全部

Php4fun原来是一个练习代码审计的一套小程序，但后面下线了，需要自己搭环境。本来想把几个知识点在这里阐述一下，但发现已经有很详细的writeup了，再写就是浪费时间。所以我把wp和源码都放到了压缩包里，可以自己搭环境玩一玩儿。

小总结

这段时间还做了，“网络安全实验室”，“XSS Challenges”，和WeChall里的一些题，但因为我做得很零碎，并且现在还没有写writeup，所以相关知识点就不列在这里了。确实感觉从CTF中学到了很多很多~有个想法：在博客上连载各大训练平台的Writeup，算是为大家服务，如果开始做了的话，会在下一篇CTF文章中，贴出链接的，敬请期待。

在压缩包里还有一个p师傅的PPT，关于CTF技巧的，安利一波~

因为我只是一只web狗，所以其它题型也讲不出什么好东西来~在这里贴一个之前出现过的链接

```
https://ctf-wiki.github.io/ctf-wiki/#/introduction
```

真的是个好东西。

充分利用上面的一些资源，入门绝对不是问题啦~

哦，对了，做笔记是个很好的习惯，我用印象笔记，听说国内的为知笔记也不错~

如何进阶CTF

讲完了入门的问题，再讲讲进阶，可能讲得不好毕竟我是菜鸟

刷完一套bugku就可以尝试着打打线上赛了

每年都会有各种各样的比赛，而且感觉会越来越多~

可以在这里找到最近的一些比赛，取得名次还有有奖励岂不爽滋滋

```
https://ctftime.org/
```

如果因为时间安排，以及其它不可抗因素错过了某些比赛，可以看官方的writeup来弥补一下。看到精彩处可以尝试联系出题人，要一下题目的源码出题人虽然经常被‘追杀’，但人还是很好的除了一些敏感的东西，一般都会给你~

CUIT校赛经验

下面就我CUIT的校赛，简单说一下正规线上赛的难度系数与形式。

这场比赛，有两个大三的学长带，打起来虽不能说轻松，但也算是有惊无险~

我做了杂项和web，杂项在这里就不说了。感觉考的是加解密的知识储备以及运气，对了，还遇到了个离散数学的题，妈妈诶，大一的萌新瑟瑟发抖~

Web部分我感觉题出的非常棒，官方的Writeup很详细（萌新我还有地方没搞懂啊）在这里只是简单介绍下题目的难度系数

比如，第一题“山水集团”，是一道SQL的题，一上来进行简单的黑盒测试，然后想办法绕过过滤，最后的解决为盲注写脚本。爆出账号密码后，又有一个Mysql字符编码的绕过（就是上面说的那一点），进后台之后是无回显命令执行。

这道题是300分，比赛的时候没做出来，看wp的时候就感觉师傅们真厉害其它的题目的难度在这道题的上下浮动，具体的可以看一下压缩包里的官方wp，（PS：“短域名“里的那个dict协议真是厉害）

因为是在自己的学校办的，并且队伍里有两个大三的学长带，所以有幸通过了线上选拔，参加了线下赛。

线下赛的比赛规则大概是，每个队伍分一台服务器（给你SSH的密码）。服务器上的配置都一样，每支队伍都需要审计自己服务器上的代码，找出漏洞，去打其它的队伍。从早上9点到下午5点，共8个小时，中午管盒饭和饮料。每隔10分钟会在服务器的固定位置，刷新flag文件，拿到flag提交，就可以给自己的队伍加分，被打的队伍减分。

感觉线下赛主要打以下几点：

1、快速白盒审计，发现并补上自己的洞

2、自动化攻击，利用发现的洞攻击其它队伍的洞，用Python实现半自动化。

3、种不死马，因为没有提权，所以只能上马来收割flag，一般的马很容易被删，所以可以根据下面的代码，来编写一个自己的不死马，其实就是无限循环生成，并且密码加密的一个马，但这种马只要重启一下服务就可以杀掉。还有一个更厉害的姿势，目前还没有杀掉的方法，等省赛过后再和大家分享吧~

4、审查日志，可以在服务器上放个记录访问日志的脚本，然后根据其它队伍打你的payload找到漏洞的位置，还可以拿这个payload去打其它队伍。（PS：比赛的时候发现了其它队伍的上传到我们服务器上的马，然后我们就很无耻地爆破出了密码，只有三位数。然后借刀杀人，拿到了7/8台服务器，刷了一下午哈）

关于线下赛，这里有两个链接讲得还不错，可以学习一波不死马可以把两个文章的代码结合起来，自己写一个

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

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/index.html
```

防范思维CTF化

无疑，打CTF是有助于我们技术的提升的，对于学生而言，一个重量级CTF奖状也将是你入职的敲门砖。

但打比赛与技术水平的高低倒还真没有必然的联系，想要打比赛需要长时间的投入，需要了解出题人的套路，认识很多不喜欢打比赛但很厉害的大佬。而比赛毕竟只是比赛，不是100%的真实环境，多多少少有些出入之处。

所以不要只满足于拿flag的快感，把从比赛获得的知识应用到实战上，拿个站、写个外挂、审审代码什么的。学，然后用，我认为这才是CTF的正确打开姿势。

出题人的一点想法

出题人真的挺难做的，既要想办法把题目出得有内涵，又要考虑预期之外的解法，还要防“搅屎”（在此为南邮以及bugku里被搅屎挂掉的几道getshell题目默哀3分钟）。

当然，就像p师傅说的，能成功地搅屎，也是一种能力体现。而能防止别人搅屎，是出题人能力的体现。

在这里贴上一篇“搅屎”教程，和p师傅的Freebuf上的搅屎攻略：

```
http://www.freebuf.com/articles/web/118149.html
```

以及P师傅防搅屎攻略：

```
http://hack.hk.cn/2016/04/22/ctf%E4%B8%BB%E5%8A%9E%E6%96%B9%E6%8C%87%E5%8D%97%E4%B9%8B%E5%AF%B9%E6%8A%97%E6%90%85%E5%B1%8E%E6%A3%8D/
```

希望大家能够从中学到些东西（反正我学到了~嘻嘻）