目录

一、题目

1、源码

```php
extract($_POST);
function goAway() {
    error_log("Hacking attempt.");
    header('Location: /error/');
}

if (!isset($pi) || !is_numeric($pi)) {
    goAway();
}

if (!assert("(int)$pi == 3")) {
    echo "This is not pi.";
}
else {
    echo "This might be pi.";
}
```

2、知识点

知识点	说明
error_log()	向服务器错误记录、文件或远程目标发送一个错误
extract()	使用数组键名作为变量名，使用数组键值作为变量值
is_numeric()	用于检测变量是否为数字或数字字符串
assert()	断言，在程序中的某个特定点视表达式值为真；如果该表达式为假，就中断操作

3、解读

1）第1行，接收POST方法传入的数据，并将键作为变量名，值作为变量值。
2）第7行，如果POST数据中没有参数pi，或者没有pi不是数字，就调用函数goAway()。
3）第2行，函数goAway()中，输出错误信息。
4）第11行，如果POST数据中参数pi不等于3，就输出一条语句，否则输出另一条语句。

4、分析

1）POST传入的参数和值会被转换成变量名和变量值，也就意味着变量可控。
2）在第7行，对POST数据中的变量进行了判断和处理，也就是说如果参数为pi，就会被调用并处理，并且在第一个判断完之后，并没有进行exit退出操作，程序会继续向下执行。
3）此时POST传入pi参数，并指定要执行的命令。程序首先会进行第7行的if判断，没问题之后走向函数goAway()，但goAway()出来之后，还会继续执行下一个判断，也就是pi的值会被调用并执行。

5、利用

```
pi=phpinfo()
```

二、CMS

1、源码-FengCMS 1.32

```php
if(file_exists(ROOT_PATH.'/upload/INSTALL')){
  echo '<script type="text/javascript">alert("系统已安装，如需要
        重新安装，请手工删除upload目录下的INSTALL文件！");</script>';
  echo '<meta http-equiv="refresh" content="0;url=/">';
}

switch($_GET['step']){

    case '1': //安装许可协议
        include ABS_PATH."/step/step1.php";
    break;

    case '2': //检查安装环境是否满足要求
        ......
    break;

    case '3': //填写数据库信息

        include ABS_PATH."/step/step3.php";

    break;

    case '4': //正在安装
        ......
    case '5': //安装完成
        include ABS_PATH."/step/step5.php";
        $in = fopen(ROOT_PATH.'/upload/INSTALL','w');
        fclose ($in);
    break;
}
```

2、知识点

```
Null
```

3、解读

```
1）第1行，如果根目录下的/upload/INSTALL文件存在，就输出提示。
2）第7行，根据传入的step参数，进入安装流程，并在安装完成后生成/upload/INSTALL文件。
```

4、分析

```
1）首次安装完成后，会在根目录下生成/upload/INSTALL文件。
2）再次访问/upload/INSTALL文件时，系统会提示已经安装过了，但是代码会继续向下执行，再次进入安装流程，也就导致了网站重装漏洞。
```

5、利用

```
直接访问/install（这里访问upload/install好像不太对）文件，无视提示，继续访问，就会进入重装环节。
```

6、修复方案

```
在检查到非法操作的时候，添加退出函数，避免代码继续执行，造成漏洞。
```

7、参考链接

```
https://github.com/hongriSec/PHP-Audit-Labs/blob/master/Part1/Day10/files/README.md
```