**PHP代码审计流程分析法**

1. 思路
2. 分析每一个函数。
3. 标记出危险的函数。
4. 通过手工输入，通过程序梳理全部的流程。
5. 人工判断每个流程是否危险。
6. 详细设计
   1. 流程设计
      1. 源代码基础信息输入（ok）
7. 输入文件路径，选择文件，上传。
8. 输入点的数据：文件路径、行号（从0开始）、级别（自动判断，默认为null）、位置（是否为入口或结束，默认为NULL）、行的内容。
9. 插入数据库。
   * 1. 源代码基础信息完善
10. 选择路径、文件。
11. 列出文件未完善基础信息的行。（级别和位置为NULL值的）
12. 添加变量。（添加到temp表中）
13. 选择变量，输入线。（1、需要校验线的终点是否已经添加。2、变量从temp表中取）
14. 输入：级别、位置。
    * 1. 类的输入

***注释：类中函数的输入最好一次输入完。***

1. 选择添加类。
2. 输入类名、文件名（包含路径）
3. 插入数据库。
   * 1. 类中函数的输入
4. 选择类。
5. 添加函数。
6. 输入函数名、访问权限、是否危险、函数内容。
7. 插入数据库。
   * 1. 普通函数的输入
8. 选择添加函数
9. 输入文件名、函数名、访问权限、是否危险、函数内容。
10. 插入数据库。
    * 1. 单独添加线
11. 选择目录、选择文件；
12. 选择线头；
13. 输入线尾所在文件和行；或输入线尾所在文件和函数名，有类名可以输入类名
14. 输入说明(备注)，这条线可行吗？。
15. 选择变量（这个一定要写清楚。）；
16. 插入数据库。
    * 1. 路径计算算法
17. 找出所有的起点，start数组。
18. 从start里提取第一个数组。
19. 数组所有的线。没有线返回。
20. 提取一根线，以终点为开始。
21. 如果为终点为结束点，结束。否则回到2。
    * 1. 代码合并
22. 点击与上一行合并，当前代码行与上一行合并。
23. 将当前代码行标记为不判断。。
    * 1. 其它说明

1、是否危险的判断标准：

* 1. 源代码基础信息完善
     1. Points

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| id | file | line\_number | level | start | content |  |
| 1 | / index.php | 10 | 0 | 1 | … |  |
| 2 | / index.php | 11 | 0 | 0 | … |  |
| 3 | / index.php | 12 | 0 | 0 | … |  |
| 4 | / index.php | 120 | 0 | 0 |  |  |
| 5 | / index.php |  |  |  |  |  |
| 6 | / index.php |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* + 1. variables

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| id | Points\_id | variable | value |  |
| 1 | 2 | $\_SERVER[‘QUERY\_STRING’] | is\_numeric($\_SERVER[‘QUERY\_STRING’]) |  |
| 2 | 3 | $\_ENV[‘curapp’] | ‘Home’’ |  |
| 3 | 4 | $\_GET[‘mod’] | ‘space’ |  |
| 4 | 4 | $\_GET[‘uid’] | $\_SERVER[‘QUERY\_STRING’] |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. Lines

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| id | point\_u\_id | point\_v\_id | variables\_ids |  |
| 1 | 1 | 2 | 1 |  |
| 2 | 2 | 3 | 2 |  |
| 3 | 3 | 4 | 3#4 |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. Functions

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| id | function\_name | file | class\_name | start | end | level | function\_start |  |
| 1 | null | / index.php | null | 1 | 119 | 0 | 1 |  |
| 2 | null | / index.php | null | 120 | 130 | 1 | 0 |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

* + 1. Parameters

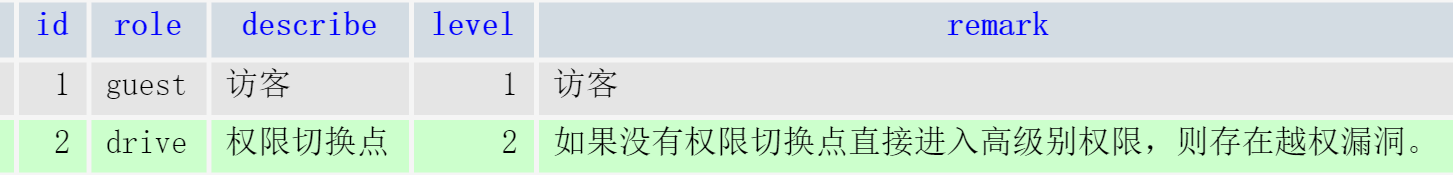
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| id | lines\_id | parameter | value |  |
| 1 | 1 | $\_SERVER[‘QUERY\_STRING’] | is\_numeric() |  |
| 2 | 1 | $\_ENV[‘curapp’] | ‘Home’’ |  |
| 3 | 1 | $\_GET[‘mod’] | ‘space’ |  |
| 4 | 1 | $\_GET[‘uid’] | $\_SERVER[‘QUERY\_STRING’] |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. 数据库设计
   1. role

角色中一定要有两个权限设置。

guest ：访客

drive ：权限切换点，如果没有权限切换点直接进入高级别权限，则存在越权漏洞。



* 1. Points

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **类型** | **长度** | **备注** |
| id | Int |  | 自增长 |
| file | Text |  | 路径和文件名，以“/”为根目录 |
| line\_number | int |  | 行号 |
| level | Int |  | 是否危险，1代表危险，0代表不危险。-2代表不判断。 |
| Position | int |  | 是否是入口行，1代表是，0代表不是,-1代表结束行。-2代表不判断。 |
| Content | text |  | 行的内容 |

* 1. Lines

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **类型** | **长度** | **备注** |
| id | Int |  | 自增长 |
| point\_u\_id | Int |  | 函数ID，没有为null |
| point\_v\_id | int |  | 函数ID，没有为null |
| variables\_ids | text |  | 这条路径所需要variables的ID，使用  Addslashes serialize |

* 1. variables

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **类型** | **长度** | **备注** |
| id | Int |  | 自增长 |
| variable | text |  | 变量名 |
| value | text |  | 值 |
| Remark | Text |  | 变量说明 |

* 1. Paths

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **类型** | **长度** | **备注** |
| id | Int |  | 自增长 |
| points\_id | text |  | Functions的ID，使用“#”分隔 |
| Lines\_id | text |  | Lines\_id的ID，使用“#”分隔 |
| Check | Int |  | 是否检查过流程是否有问题，1代表是，0代表不是，-2代表这条路径不可能存在。 |

* 1. class

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **类型** | **长度** | **备注** |
| id | Int |  | 自增长 |
| file |  |  |  |
| Class\_name |  |  |  |
| Function\_name |  |  |  |
| Function\_type |  |  |  |
| content | text |  |  |
| remark | Text |  |  |

* 1. temp

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **类型** | **长度** | **备注** |
| id | Int |  | 自增长 |
| name | Int |  | 临时的字段 |
| content | text |  | 临时的内容 |

* 1. Functions

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **类型** | **长度** | **备注** |
| id | Int |  | 自增长 |
| function\_name | Text |  | 函数名，没有为null |
| file | Text |  | 路径和文件名，以“/”为根目录 |
| class\_name | text |  | 类名，没有为null |
| start | int |  | 开始的行数 |
| end | int |  | 结束的行数 |
| level | Int |  | 是否危险，1代表危险，0代表不危险。 |
| function\_start | int |  | 是否是入口函数，1代表是，0代表不是。 |

* 1. Parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **类型** | **长度** | **备注** |
| id | Int |  | 自增长 |
| lines\_id | Int |  | Lines的ID，使用外键 |
| parameter | text |  | 参数名 |
| value | text |  | 值 |