# 资产安全管理系统（v2.0）--详细设计文档

巡天鉴Celestial Mirror

### 资源管理

域名--子域名---web地址---web目录---API地址

IP地址---端口---端口服务

维护一个数据库，包括已知资产（定期从云平台更新资产数据，手动上传、录入数据），标记数据来源为内部。然后根据已知资产定期做资产发现，然后标记为三无七边资产，如子域名爆破（被动：subfinder）、目录扫描、IP发现（uncover）、端口扫描（naabu）。

预选项目：

URLFinder 一种用于被动收集 URL 的高速工具，经过优化，无需主动扫描即可高效发现 Web 资产。

<https://github.com/projectdiscovery/uncover> 使用多个搜索引擎快速发现 Internet 上暴露的主机。

<https://github.com/projectdiscovery/notify> 通知

<https://github.com/projectdiscovery/shuffledns> 主动DNS 子域名爆破

<https://github.com/projectdiscovery/cloudlist> 从云上获取资产

<https://github.com/projectdiscovery/wappalyzergo> 指纹识别

<https://github.com/projectdiscovery/cdncheck> 检查给定 IP 是否在 Cloud / CDN / WAF 上运行的帮助程序库

<https://github.com/projectdiscovery/httpx> 存活探测

<https://github.com/projectdiscovery/urlfinder> 被动URL发现

<https://github.com/OJ/gobuster> 主动URL发现

<https://github.com/ffuf/ffuf> 主动URL发现

### 安全扫描

域名、子域名、业务地址、多级目录可以做web扫描，考虑用katana或者rad+xray被动+nuclei主动

IP地址列表做端口扫描和漏洞探测，考虑用naabu+ nuclei

要有扫描任务的管理，主动扫描、定时扫描。

### 三、漏洞管理

要做一个漏洞管理模版，包括新增漏洞，漏洞的状态，漏洞地址，发现时间.

对于扫描出来的安全问题，可以按照漏洞级别进行排序和筛选，并可以标记状态为误报，确认，忽略，已修复，正常。

### 四、定时或者单次任务设计

1. IP地址、端口自动巡检

程序自动对暴露面清单中的IP地址、端口，进行自动化巡检，确保IP、端口和清单内容匹配，程序自动巡检完成后，生成相应巡检日志。如IP和端口和清单不匹配，及时进行预警，模板为：

**XXip，XX端口，开放中/已关闭，和清单不一致，请核实确认。**

**IP地址来源：自己维护的IP列表+阿里云、天翼云的API接口清单**

**每次巡检后要对比IP是否一致、然后对比IP的端口情况。**

1. 对接阿里云域名管理API，程序每周1凌晨6点自动对清单中的域名进行巡检，巡检过程中，需要对以下几点进行系统自动确认。
2. 是否有域名未在清单内，如果有，需要进行邮件告警，告警信息模板为：

**XXX域名，未在域名管理清单内，请核实确认。**

1. 当前域名是否有效，具体手段为：
2. 对域名进行ping测，对ping后返回的ip进行确认，如ip未知或ping测后无ip返回，则可判断为域名已无效。
3. 对域名进行http get请求，如响应状态码不为200，则可判断为该域名已无效。
4. 对无效域名进行告警，模板为：**XXX域名，自动巡检为已失效，请核实**。
5. 巡检完成要对新发现的资产做漏洞扫描。定期对所有资产做漏洞扫描。
6. 对应数据库表设计如下。

**表:IP记录表**

|  |  |  |
| --- | --- | --- |
| **字段** | **类型及长度** | **备注说明** |
| id | 整形，自增 | 表主键 |
| ip\_addr | 字符串类型，50 | 要巡检的ip地址 |
| port\_list | 字符串类型，500 | 多个端口，用|分割存放 |
| location | 整型，2 | IP位置  1：天翼云  2：阿里云  3：北艾机房  4：国脉私有云  5：国脉办公21F  6：金山机房  7：南汇机房  如有新增，持续扩展，这部分数据维护至数据字典表 |
| status | 整形 | 状态  1:正常  -1:IP已下线  -2:暴露端口未授权  -3:授权端口未暴露 |
| business | 字符串类型，200 | 承载业务，手动维护 |
| url | 字符串类型，200 | 核心业务访问地址 |
| create\_time | 时间戳 | 创建时间 |
| update\_time | 时间戳 | 更新时间 |
| admin | 字符串类型，50 | 管理员 |
| op\_user | 字符串类型，50 | 操作员 |

**表:IP巡检日志表**

|  |  |  |
| --- | --- | --- |
| **字段** | **类型及长度** | **备注说明** |
| id | 整形，自增 | 表主键 |
| ip\_addr | 字符串类型，50 | 要巡检的ip地址 |
| port | 整形，10 | 端口 |
| result | 整形，2 | 1:正常  -1:IP已下线  -2:暴露端口未授权  -3:授权端口未暴露 |
| create\_time | 时间戳 | 创建时间 |

**表:域名记录表**

|  |  |  |
| --- | --- | --- |
| **字段** | **类型及长度** | **备注说明** |
| id | 整形，自增 | 表主键 |
| domain\_name | 字符串类型，120 | 要巡检的ip地址 |
| location | 整型，2 | IP位置  1：天翼云  2：阿里云  3：北艾机房  4：国脉私有云  5：国脉办公21F  6：金山机房  7：南汇机房  如有新增，持续扩展，这部分数据维护至数据字典表 |
| type | 整型，2 | 域名类型  1：公有域名  2：私有域名 |
| staus | 整型，2 | 1:正常  -1:域名未授权  -2:域名已下线  -3:域名不活跃  -4:证书已过期 |
| cer | 整型，2 | 证书情况  1：有证书  2：无证书 |
| cer\_exp\_time | 时间戳 | 证书过期时间 |
| business | 字符串类型，200 | 承载业务，手动维护 |
| url | 字符串类型，200 | 核心业务访问地址 |
| create\_time | 时间戳 | 创建时间 |
| update\_time | 时间戳 | 更新时间 |
| admin | 字符串类型，50 | 管理员 |
| op\_user | 字符串类型，50 | 操作员 |

**表:域名巡检日志表**

|  |  |  |
| --- | --- | --- |
| **字段** | **类型及长度** | **备注说明** |
| id | 整形，自增 | 表主键 |
| domain\_name | 字符串类型，120 | 要巡检的ip地址 |
| result | 整形，2 | 1:正常  -1:域名未授权  -2:域名已下线  -3:域名不活跃  -4:证书已过期 -5:403 |
| create\_time | 时间戳 | 创建时间 |

**表:应用资产表**

|  |  |  |
| --- | --- | --- |
| **字段** | **类型及长度** | **备注说明** |
| id | 整形，自增 | 表主键 |
| web\_addr | 字符串类型，120 | 要巡检的web地址 |
| status | 整形，2 | 200:正常  403  404  302 |
| create\_time | 时间戳 | 创建时间 |
| vul\_num | 字符串类型，1000 | 漏洞数量 |

**表:漏洞资产表**

|  |  |  |
| --- | --- | --- |
| **字段** | **类型及长度** | **备注说明** |
| id | 整形，自增 | 表主键 |
| vul\_name | 字符串类型，120 | 漏洞名称 |
| status | 整形，2 | 1：已修复  2：未修复  3：忽略 |
| create\_time | 时间戳 | 创建时间 |
| level |  | 1：高危  2：中危  3：低危  4：信息 |
|  |  |  |