目录

管理扫描IP

本文介绍了使用本产品对您资产进行漏洞扫描的操作流程。

开启扫描任务

前提条件

1. 您已购买公网弹性IP。
2. 已开启漏洞扫描的弹性IP少于5个。

操作步骤

1. 登录漏洞扫描控制台。
2. 选择要扫描的弹性IP，点击上侧操作栏中的**开启**按钮。
3. 在**开启漏洞扫描**对话框中点击**确定**。
4. 弹性IP的扫描状态显示为**开启**，操作完成。

   说明：同个账号下只可同时开启5个弹性IP的漏洞扫描。

关闭扫描任务

前提条件

存在已开启扫描任务的弹性IP。

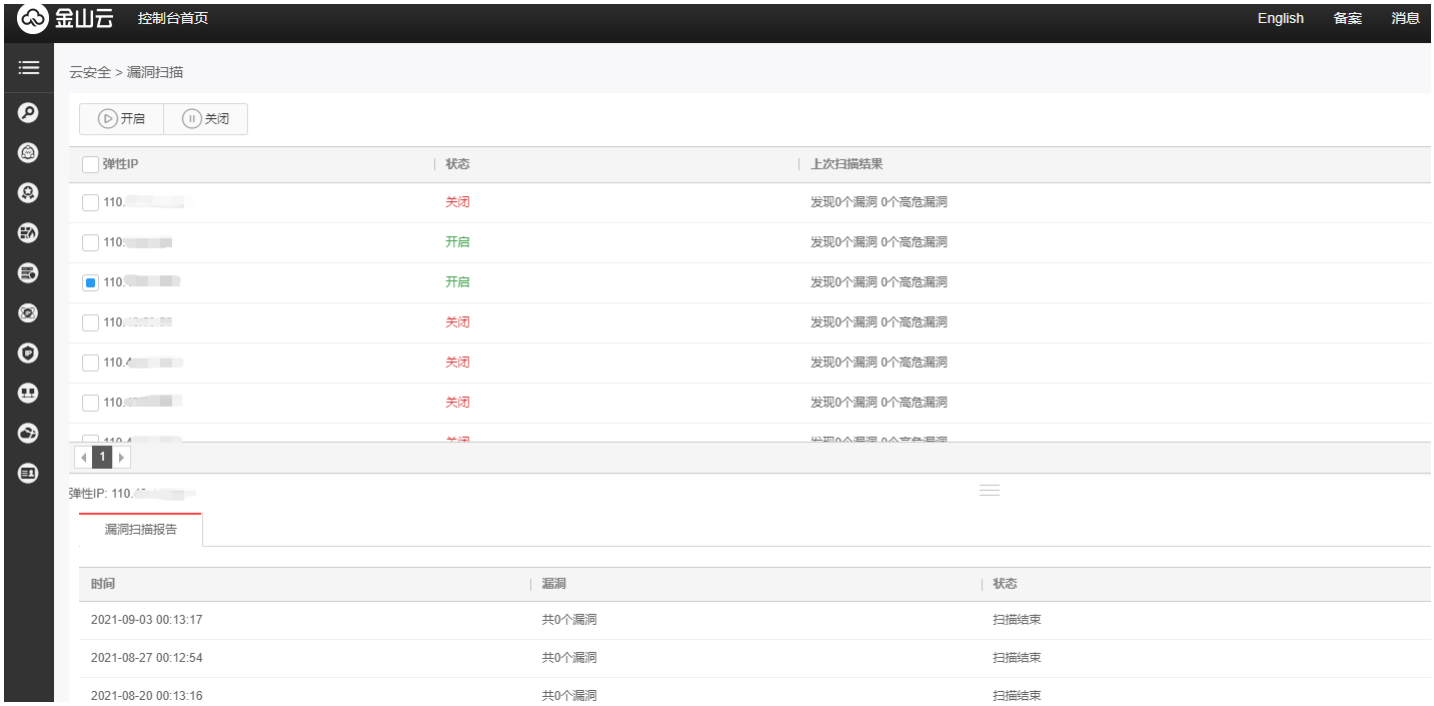
操作步骤

1. 登录漏洞扫描控制台。
2. 选择要扫描的弹性IP，点击上侧操作栏中的**关闭**按钮。
3. 在**关闭漏洞扫描**对话框中点击**确定**。

查看扫描报告

查看历史扫描报告

1. 登录漏洞扫描控制台。
2. 选择弹性IP，在下侧弹出的面板中查看历史扫描报告。

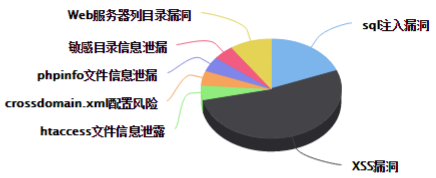


3. 在下侧的历史报告中点击**点击查看详细报告**，可查看每次扫描的具体信息。

漏洞扫描体检报告

报告时间	2016-09-26 15:37:37
弹性IP	120[redacted]
扫描状态	扫描结束
扫描结果	高危
爬虫抓取总数	16 查看爬虫抓取链接
网站应用	php[redacted],ngin[redacted]

漏洞类型数据统计



服务器漏洞

端口	服务	应用	版本	漏洞名称	危险等级
/(ToT)/~~ 没有找到亲要的数据哦~					

Web漏洞

URL	请求方式	漏洞名称	修复建议	危险等级
http://120.[redacted]	GET	sql注入漏洞	点击查看	高危

1. 解决SQL注入漏洞的关键是对所有来自用户输入的数据进行严格检查、对数据库配置使用最小权限原则
2. 所有的查询语句都使用数据库提供的参数化查询接口，参数化的语句使用参数而不是将用户输入变量嵌入到SQL语句中。
3. 对进入数据库的特殊字符（'"<>&*;等）进行转义处理，或编码转换。
4. 确认每种数据的类型，比如数字型的数据就必须是数字，数据库中的存储字段必须对应为int型。
5. 数据长度应该严格规定，能在一定程度上防止比较长的SQL注入语句无法正确执行。
6. 网站每个数据层的编码统一，建议全部使用UTF-8编码，上下层编码不一致有可能导致一些过滤模型被绕过。