【原创】bashshell实现自动检查网站敏感信息泄露

种田 / 2016-11-23 09:10:31 / 浏览数 8062 安全工具 工具 顶(0) 踩(0)

bash shell实现自动检查网站敏感信息泄露

一、用途

1.研发人员在网站目录下生成带有敏感内容的log文件；
2.运维人员修改配置文件后生成.bak的文件；
3.代码压缩文件上传更新后未及时删除；
4.内部系统附件下载未添加权限校验；
.....

本程序实现：

通过批量自动化的方式检查web服务器代码目录敏感文件泄露，并通过web展示。

二、思路

1.因为网站服务器较多，首先要实现批量管理Linux,远程调用，推荐使用ansible；
2.通过bash shell（当然你也可以用python）获取网站目录所有文件列表（或指定类型文件，可排除图片、JS、CSS文件等），写入数据库供web展示，；
3.如果你的网站服务器部署没有规范化，站点目录不是固定的，需要一个配置平台。

三、实现

1. web配置

用于配置服务器IP、IP对应域名（后面用得上）、网站目录、排除文件类型规则。
如图：

2.检查脚本

关键脚本如下：
变量设置：

生成文件列表：
使用for循环是因为支持多个网站目录地址。

写入数据库：
这里循环文件列表分别写入数据库，如果文件多的话，多台服务器同时运行文件会对数据库有性能要求，如果你有更好的方法可以讨论。数据库中一个文件 一条记录是为了

3.每天定时批量调用

只需要在ansible控制端执行，ansible可以设置并发数，只有脚本文件变更了，才会重新上传至网站服务器。
主要命令：

```
#更新脚本文件
ansible ${ip} -m copy -a "src=${file_shell_default} dest=${file_shell}"
#设置执行权限
ansible ${ip} -m file -a "dest=${file_shell} mode=755"
#获取文件列表
ansible ${ip} -m raw -a "cd /script/checkfile/;./getfile.sh ${ip}"
```

4.web展示

1.如果前面配置了IP对应的域名，程序自动从公网请求判断该文件是否未授权访问。
2.常见类型的敏感文件：
[压缩文件] [日志文件] [phpinfo文件] [备份文件] [数据文件] [配置文件] [脚本文件] [OFFICE文件] [源码文件] [系统文件]
后台展示如图：

上一篇：Search-guard 在 El... 下一篇：1

1. 8 条回复


紫霞仙子 2016-11-23 09:14:42

种田大师傅

0 回复Ta


种田 2016-11-23 09:15:57

献丑了。

0 回复Ta


helloworld 2016-11-23 10:58:41

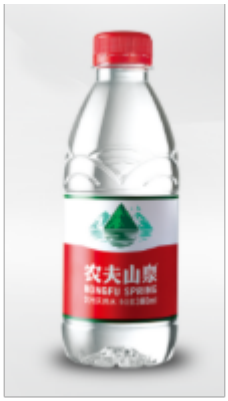
种田大师傅好

0 回复Ta


笑然 2016-11-24 02:21:27

学习

0 回复Ta



anx1ang 2016-12-01 06:11:14

0 回复Ta


yosebiubius 2016-12-20 05:44:43

感谢！学习了

0 回复Ta


sec_jack 2016-12-22 06:54:43

干货中的战斗机

0 回复Ta


sec_m0ker 2016-12-30 06:51:54

学习

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板