WEB后端强制访问控制规则

适用于web后端的RBAC角色访问控制规则,用途为抵御nginx和php程序里面的0day漏洞，阻止webshell上传和运行，阻止被控制为肉鸡攻击其他机器，尽最大可能保障web程序按照预期设计的方式工作。

警告：此类规则仅为整个安全体系一部分，系统访问控制并不能阻止sql注入和XSS攻击

本文仅涉及业务相关访问控制规则，业务无关程序/用户完全禁止访问

关键技术：使用grsecurity内核的Linux，启用RBAC（角色访问控制）规则

规则描述：

1. Ngnix 提供静态文件服务

文件访问规则: /data/web 所有文件只读访问

网络访问规则: 仅允许监听项目指定的端口，不允许监听其他端口

允许反向代理访问

禁止对外发起连接

1. php5-fpm php动态服务

文件访问规则: /data/web 只读访问，禁止写入\*.php,彻底阻止webshell上传

/data/web/项目/logs 可以写入log文件，禁止写入\*.php

/data/log 可以写入log文件, 禁止写入\*.php

/srv 图片上传目录 仅允许写入指定格式文件，禁止写入\*.php，

网络访问规则: 禁止监听端口（配置为unix socket）

对外发起连接，web仅允许连接指定IP（移动流量查询，短信发送，支付宝接口，微信接口,业务接口）

对外发起连接，内网redis

对外发起连接，内网mysql

对外发起连接，内网dns

其他对外连接完全禁止

1. rsync 网站源码更新

文件访问规则: /data/web 可以写入覆盖任何文件

网络访问规则: 仅允许监听内网873端口

允许内网代码更新机器连接，其他阻止

禁止对外发起连接

1. cron定时任务，脚本curl访问

文件访问规则: /data/scripts 仅读和执行

网络访问规则: 禁止监听端口

对外发起连接，web仅允许连接指定IP

其他对外连接完全禁止

保障系统正常运行与sshd远程管理相关访问控制规则略

本规则实现了仅有rsync 可以修改网站源码，非业务相关程序例如vi之类编辑器，以及系统中其他程序都无法修改网站源码。

这是操作系统范围内的白名单规则，因此规则尽可能的少，尽可能的严格，刚好满足业务程序正常运行，其他利用漏洞进行命令注入、远程/本地提权等都不是规则允许范围的行为，还有各种超出想象（预期）的未知行为，完全禁止，这就具备了对抗0day漏洞，木马，后门等的能力。