四叶草安全
CloverSec

唤醒乙方安全服务的力量

speaker: 残废

chaihao@seclover.com

四叶草安全
CloverSec

About Me

残废

四叶草安全CloverSec实验室

擅长领域：渗透测试　Web前端安全

Mail：chaihao@seclover.com

复杂的人性

脆弱的应用

文件上传 表单破解
CMS识别 注入 跨站
子域名 目录遍历 后台猜解
服务识别
任意url跳转 报错信息抓取
端口扫描
任意文件包含\下载

snmp rsync memcache smb socks5 nfs进行弱口令爆破和漏洞扫描

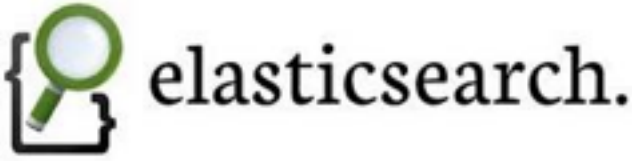

NGINX


Windows
IIS
Internet
Information
Services


php


JBoss


ThinkPHP


elasticsearch.

struts2


WordPress


phpMyAdmin


ECSHOP

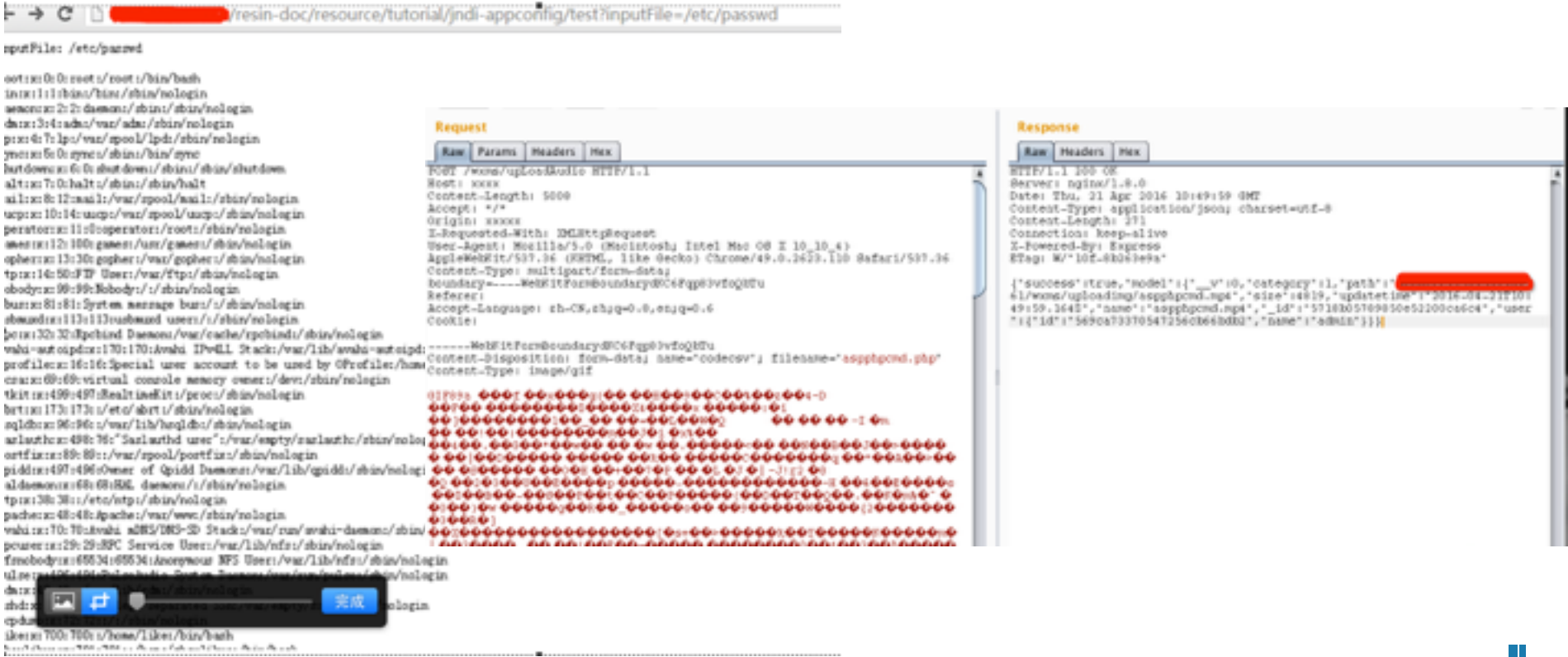

社区动力
DISCUZ!

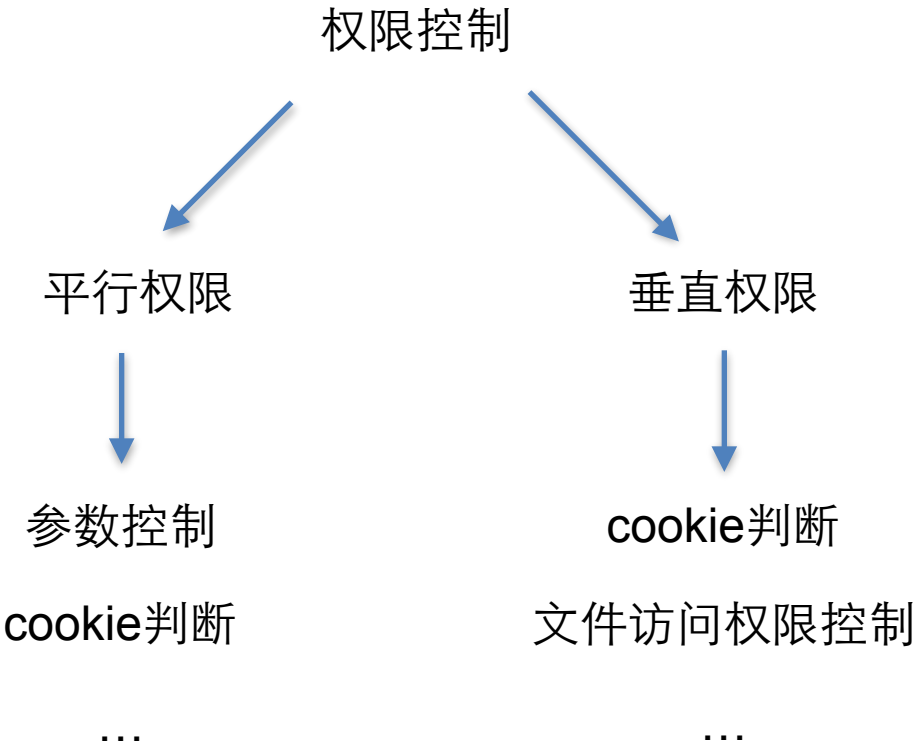

DEDECMS

数据的操作

四叶草安全 CloverSec

文件传输




权限控制
平行权限
垂直权限
参数控制
cookie判断
…
cookie判断
文件访问权限控制
…

没有黑客进不去的内网

因为你有脆弱的边界

服务器

Internet

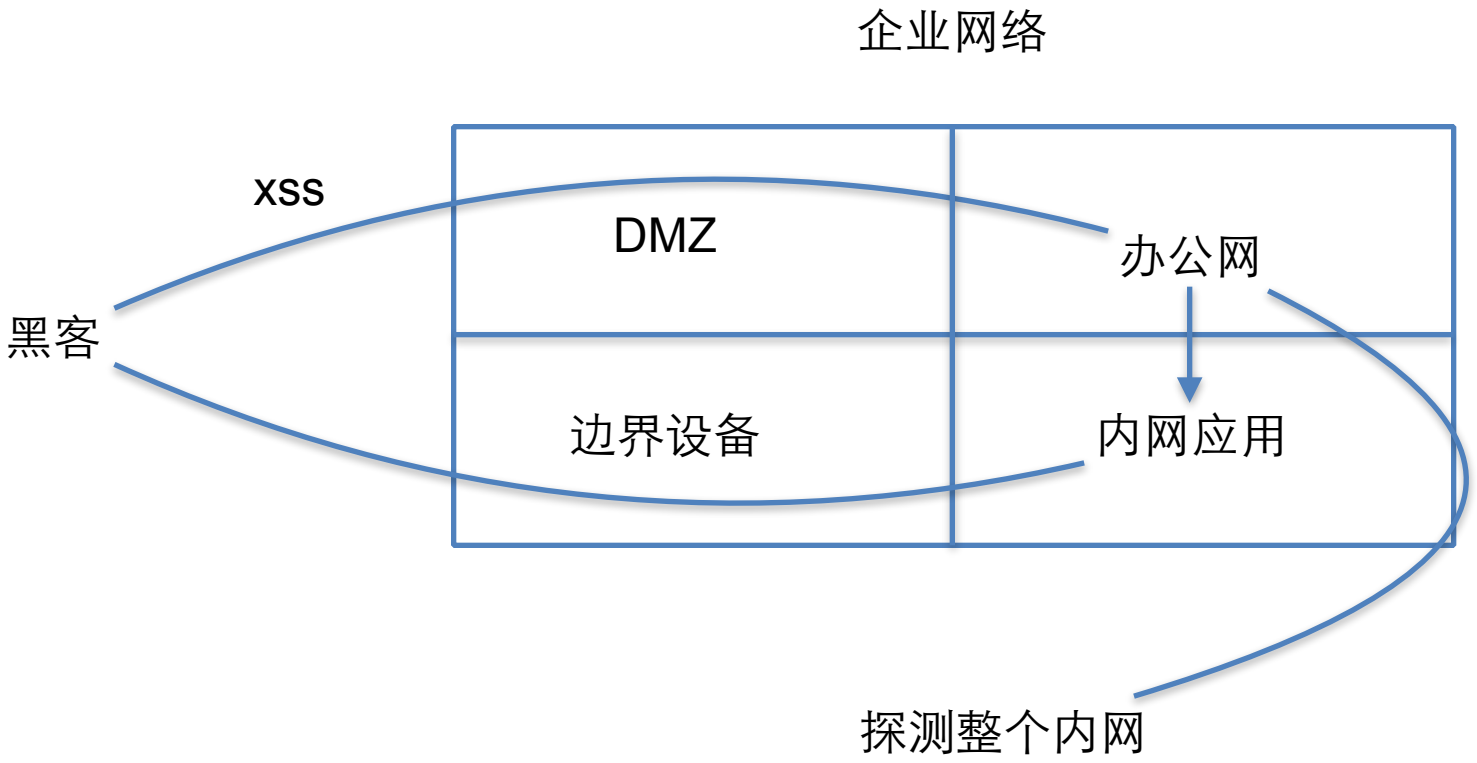
管理员

员工

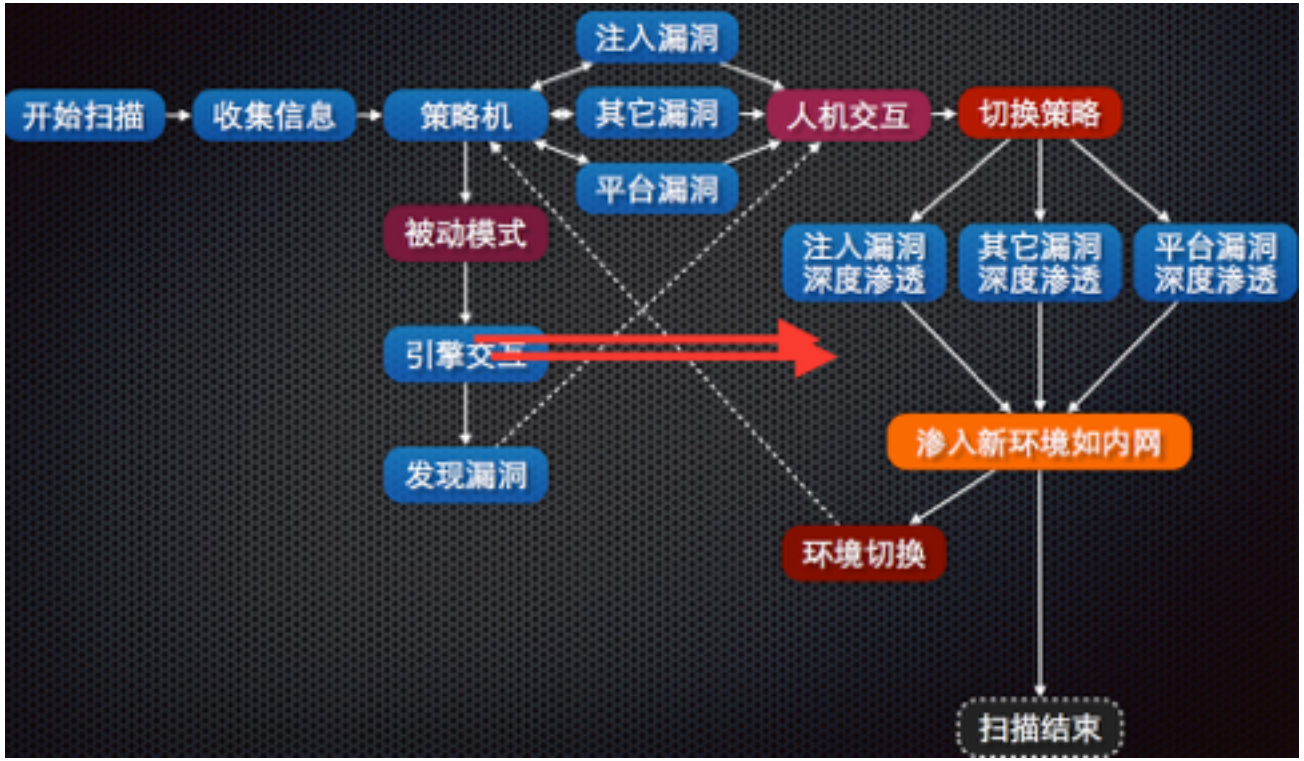
摄像头

没有黑客进不去的内网

因为你有脆弱的应用


企业网络
XSS
DMZ
办公网
黑客
边界设备
内网应用
探测整个内网

感动—Bugfeel（全时自动风险感知平台）



bugscan圈子

q.bugscan.net

bugfeel

www.bugfeel.net

四叶草安全
CloverSec

谢谢

speaker: 残废

chaihao@seclover.com