



唤醒乙方安全服务的力量

speaker: 残废

chaihao@seclover.com

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



elasticsearch.

struts2



ECShop

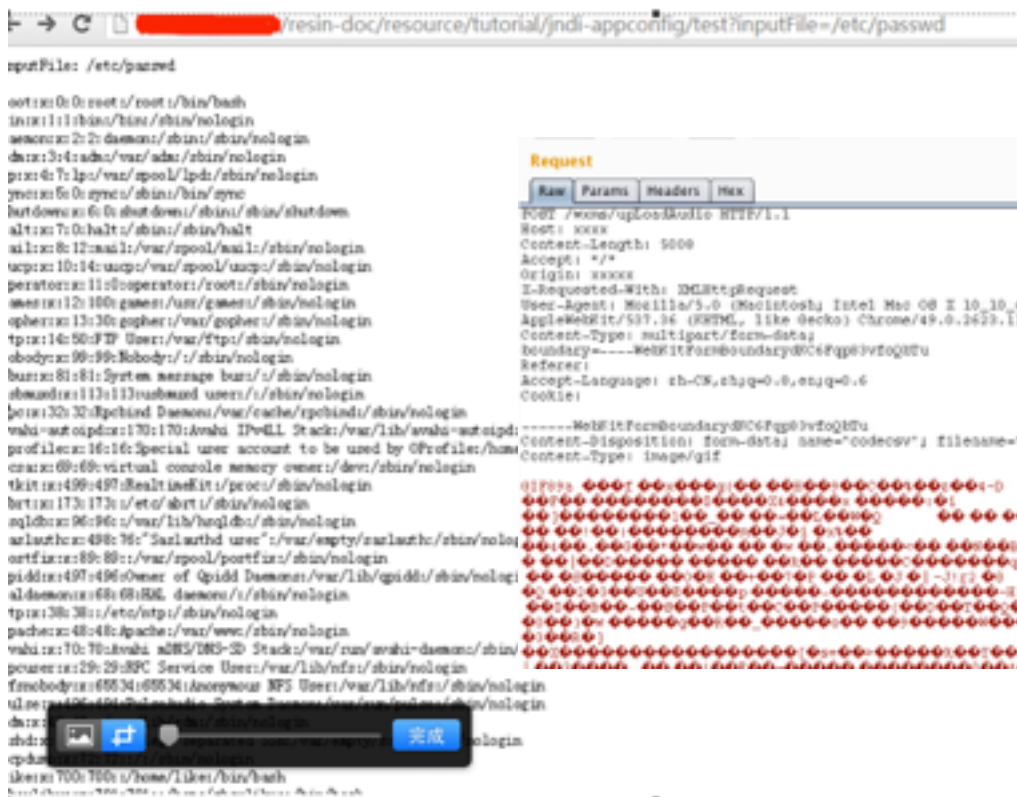


DEDECMS

数据的操作



文件传输

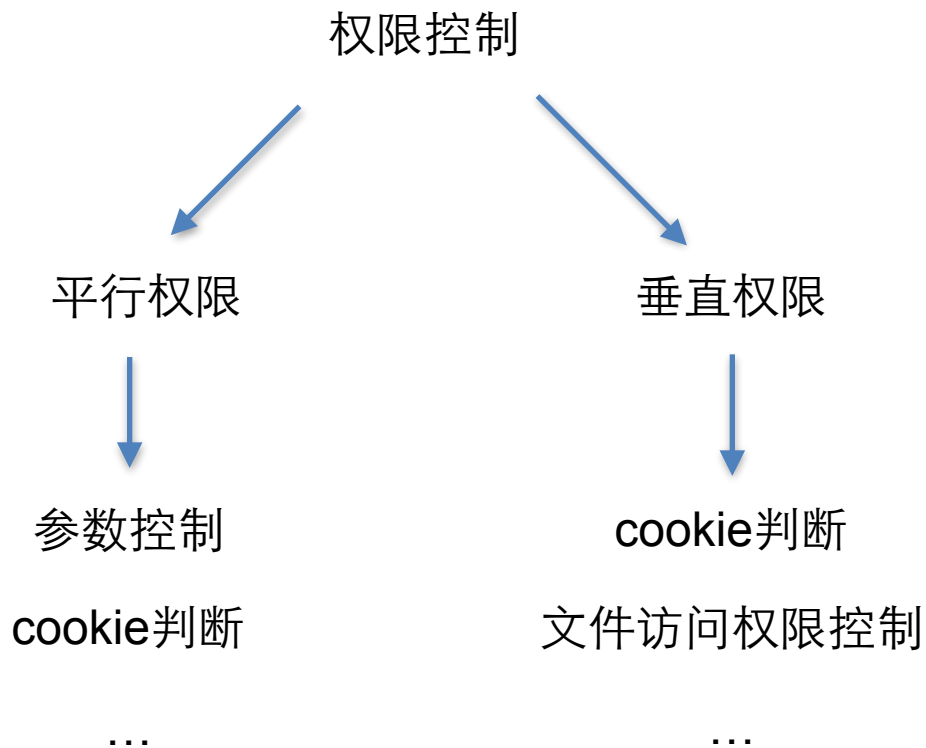


Request

Raw	Params	Headers	Hex
POST /www/upload.php HTTP/1.1 Host: xxxxx Content-Length: 5000 Accept: */* Origin: xxxxx X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2629.110 Safari/537.36 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryd0C6Fpp3vfoQltu Referer: Accept-Language: zh-CN,zh;q=0.8,en;q=0.6 Cookie:			
-----WebKitFormBoundaryd0C6Fpp3vfoQltu Content-Disposition: form-data; name="codecsv"; filename="asppcmd.php" Content-Type: image/gif			

Response

Raw	Headers	Hex
HTTP/1.1 200 OK Server: nginx/1.8.0 Date: Thu, 21 Apr 2016 10:49:59 GMT Content-Type: application/json; charset=utf-8 Content-Length: 271 Connection: keep-alive X-Powered-By: Express ETag: W/"10f-8b08e9a"		
<pre> {"success":true,"model":{"_v":0,"category":"path","path":"/www/upload/asppcmd.php","size":4819,"updateTime":"2016-04-21T10:49:59.364Z","name":"asppcmd.php","id":"5718305769850e51200c6c4","user":{"id":"5690a73370547256c064b8d2","name":"admin"}}} </pre>		



没有黑客进不去的内网
因为你有脆弱的边界

Step 3 攻击者通过数据库



四叶草安全
CloverSec

Internet

服务器



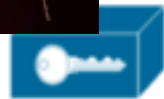
管理员



员工



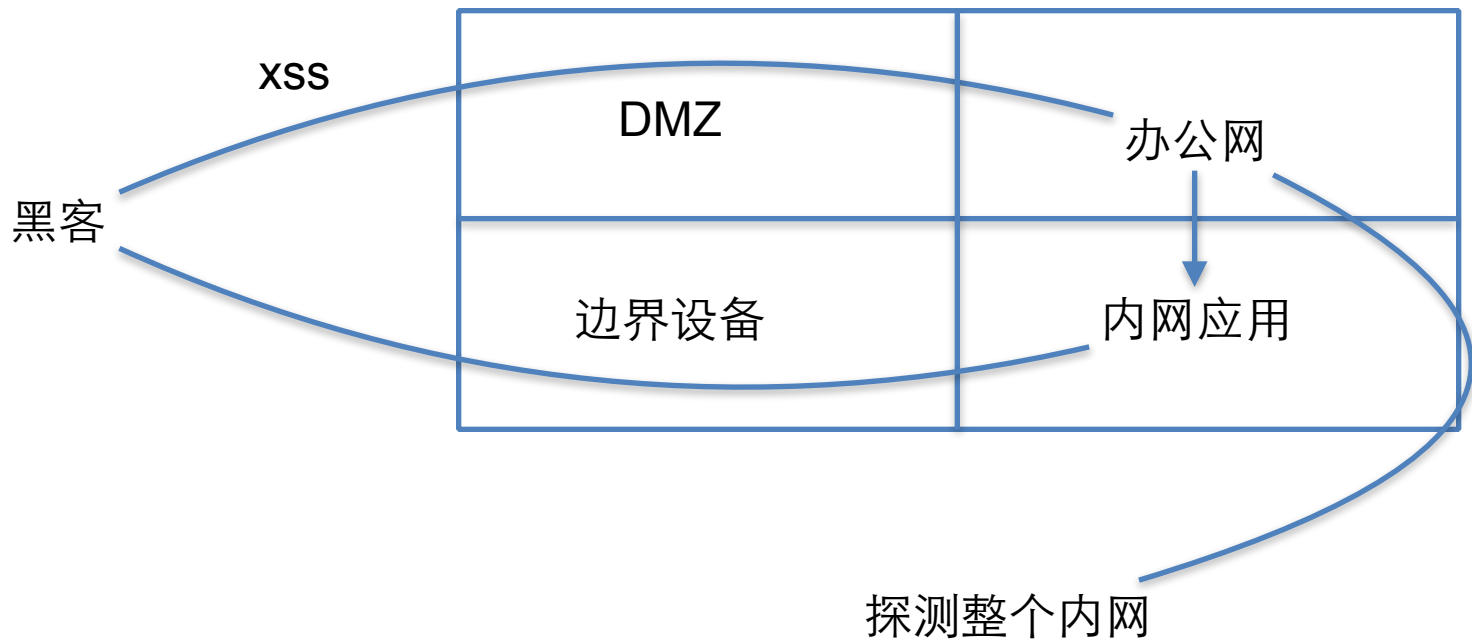
摄像头



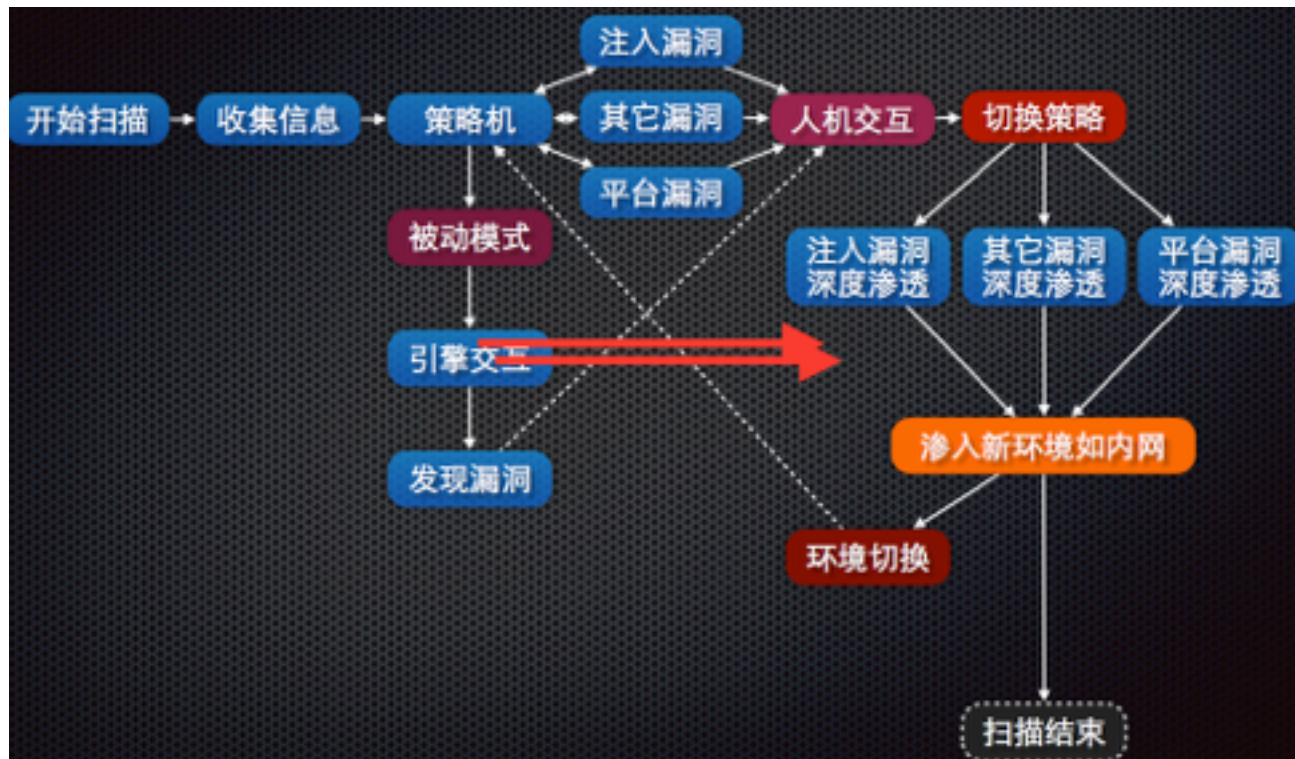
没有黑客进不去的内网

因为你有脆弱的应用

企业网络



感动—Bugfeel（全时自动风险感知平台）



bugscan圈子

q.bugscan.net

bugfeel

www.bugfeel.net



谢谢

speaker: 残废

chaihao@seclover.com