웹 취약점 진단 보고서(샘플)

Monthly Scan Report

- 2015년 02월 -

사이트 명	www.security-server.co.kr		
사이트 분류	일반기업/정보보안		
관 리 부 서	보안사업본부	담 당 자	OOO
전 화	02)449-6261	이 메 일	master@bugbounty.co.kr

본 보고서는 정보시스템의 취약점에 관련된 내용이 기술되어 있으므로, 본 문서를 열람할 권한이 없는 사람에게 공개되어서는 안됩니다..

『웹 버그 바운티』 서비스 소개 및 유의사항 안내

한국버그바운티㈜가 제공하는 Web Bug Bounty(웹 버그 바운티)서비스는 사업자 회원님께 **고객사 인터넷서비스의 노출된 취약점을 이용한 해킹 등 정보침해 위험으로 피해를 최소화** 하기 위해 **3중 보안 시스템**으로 운영됩니다.

- 본 보고서는 웹 버그 바운티 서비스 가입 기업에게 제공되는 웹 사이트 취약점 진단 보고서 입니다.
- 웹 사이트 취약점 진단 보고서는 월 1회 정기적으로 제공되는 보고서이며, 고객사 웹 서비스의 중대한 보안 취약점이 화이트해커로부터 제보 됐을 때 비정기적으로 버그 바운티 보고서가 추가로 제공됩니다.
- 웹 버그 바운티 서비스는 일반형과 고급형 상품이 있으며 고급형 신청고객은 본 보고서 이외에도 서비스 가입과 동시에 모의해킹를 진단하고 결과보고서가 함께 제공됩니다.
- 본 보고서의 제공 목적은 해킹 등의 외부 침입에 대비한 사이트의 취약점 진단과 개선 조치 지원에 있습니다.
- 발견된 취약점에 대한 전달을 통하여, 회사별 정책에 따라 적극적인 대응을 권장합니다.
- 본 서비스를 통해 발견되지 않는 취약점이 있을 수 있으며, 이에 대한 책임을 지지 않습니다.
- 본 보고서는 고객사 정보시스템의 기밀사항이 포함되어 있으므로 고객사의 정보보안 담당자 및 승인 받은 인가자에 한하여 열람이 가능하도록 관리하여 주시기 바랍니다.
- 한국버그바운티는 고객사의 동의 및 승인 없이 본 보고서의 내용을 보관 또는 활용하지 않을 것을 약속 드립니다.
- 한국버그바운티 고객센터는 주중(토, 일, 공휴일 휴무) 10시부터 18시까지 운영됩니다.
- 자세한 문의사항은 홈페이지나 아래 연락처를 참조하시기 바랍니다.

한국버그바운티 고객센터
http://www.bugbounty.co.kr
(E-mail: master@bugbounty.co.kr / ☎ 02-449-6261)

웹 취약점 진단 항목

No	구 분	설 명	선 정기준
1	File Upload	JSP, ASP, PHP 파일을 Upload하여 System 권한 획득	OWASP/금감원
2	File Download	Download 인자 값을 조작하여 System 파일 공격	금감원/국정원
3	SQL Injecttion	로그인 폼 및 변수 값에 SQL Query를 입력하여 우회 및 DB 접근	OWASP/금감원
4	URL Parameter 조작	Parameter 조작을 통하여 인증 없는 페이지에 접속하거나 서버전송시 조작하는 공격	OWASP
5	부적절한 암호화 사용	취약한 암호화 방식을 사용하는 ID 및 중요정보 복호화 공격	OWASP
6	Directory Indexing	/admin/과 같은 디렉토리의 파일 목록 노출	OWASP/금감원
7	관리자 Page 노출	/admin.jsp 등의 URL 추측을 통해 관리자페이지 공격	OWASP/금감원
8	취약한 ID/Password	취약한 ID/Password 를 유추하는 공격	OWASP
9	Cookie Manipulation	Cookie 조작 및 도용으로 타 사용자 위장 공격	OWASP
10	Hidden 필드 조작	Hidden Field를 통해 중요정보를 서버로 전송시 조작 공격	OWASP/금감원
11	XSS(Cross Site Script)	게시판 및 URL 인자 값에 특정 Java Script를 입력하여 Client측에 공격	OWASP/금감원
12	부적절한 Error 처리	Error Page내에서 노출되는 System 정보를 획득하는 공격	OWASP
13	중요정보노출	HTML 소스코드, 주석에 포함된 중요정보 노출 ID/Password 평문전송시 스니핑과 같은 공격	OWASP
14	Backup File	Server내 백업, 압축파일 존재와 다운로드 가능여부	OWASP
15	Default Page	제품 Install 및 개발 당시의 Test Page를 통해 정보 획득	KISA
16	결제금액 변조	Form Field 및 주요 Parameter의 결제정보를 조작하여 금액을 변조하는 공격	KISA
17	악성코드 유포지 확인	HTML내에 삽입된 악성코드 배포 및 경유지 존재 여부 확인	

웹 취약점 진단 사용도구

구 분	설 명
Paros	프록시(Proxy)및 웹 취약점 분석 툴
Bit Finder	악성코드(Malware) 유포 및 경유지 확인

웹 취약점 진단 보고서

1 진단 사이트 개요

진단 호스트	www.security-server.co.kr
진단 시작시간	2015-02-15 12:20:20
진단 종료시간	2015-02-15 14:20:20

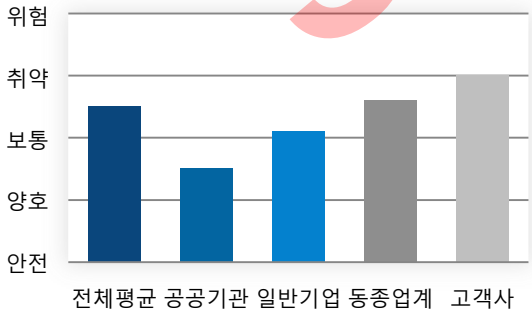
웹 취약점 진단은 평균적으로 약 2시간 정도가 소요되며, 고객사의 사이트에 영향이 없도록 심야 시간을 활용하여 진행합니다. 단, 진단 소요시간은 사이트 및 서버의 규모에 따라 달라질 수 있습니다.

2 진단 결과 요약

진단 평가 등급 : 4등급 (취약)

해킹에 필요한 중요정보가 노출돼 있고 실제 공격이 가능한 등급입니다. 높은 수준의 주의가 요구되니 상세 진단결과를 참고하시고 취약점에 대한 보안패치를 진행하시기 바랍니다.

1등급 (안전)	비교적 안전한 시스템으로 판단됩니다.
2등급 (양호)	전체적으로 양호하나 일부 상세 진단 내역의 확인이 필요합니다.
3등급 (보통)	서버의 중요 정보가 노출되거나 각종 취약점에 노출 가능성이 있고 주의가 필요합니다. 상세 진단결과를 참고하시고 취약점에 대한 보안패치를 진행하시기 바랍니다.
4등급 (취약)	해킹에 필요한 중요정보가 노출돼 있고 실제 공격이 가능한 등급입니다. 높은 수준의 주의가 요구되니 상세 진단결과를 참고하시고 취약점에 대한 보안패치를 진행하시기 바랍니다.
5등급 (위험)	해킹 당할 수 있는 매우 위험한 상태입니다. 즉시 상세 진단결과를 참고하여 취약점에 대한 수정 작업을 진행하시기 바랍니다.

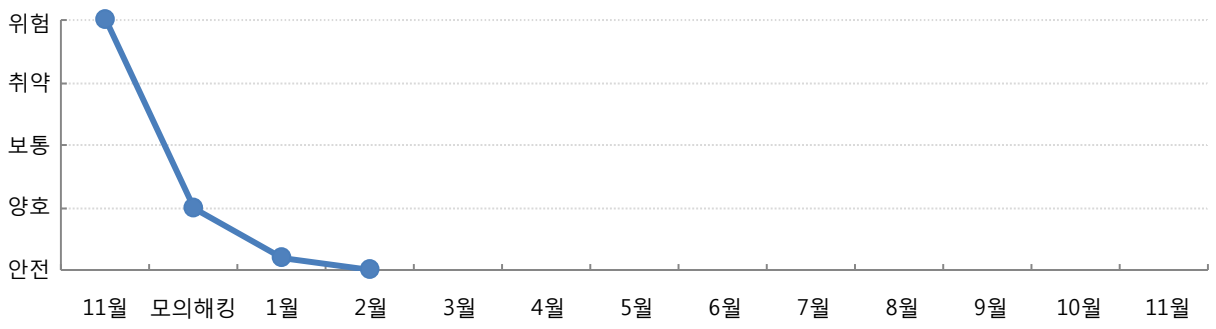


왼쪽 그래프는 타 평가대상 등급 평균과 귀사의 진단 평가등급을 비교한 자료입니다. 귀사 사이트의 진단평가등급은 전체 및 업종 평균 대비 위험도가 다소 높은 수준을 보이고 있습니다. 자체적인 개선 작업과 함께, 필요 시 모의해킹 등의 부가적인 노력을 통하여 취약점을 지속적으로 관리하여 외부침입에 대비하여 정보유출 위험도를 낮추기를 권장합니다.

진단 결과 평가 등급은 1등급(안전), 2등급(양호), 3등급(보통), 4등급(취약), 5등급(위험) 단계로 분류되며, 국제 웹 표준 및 보안 관련 각종 가이드를 참조하여, 한국버그바운티㈜에서 분석 결과를 제공합니다.

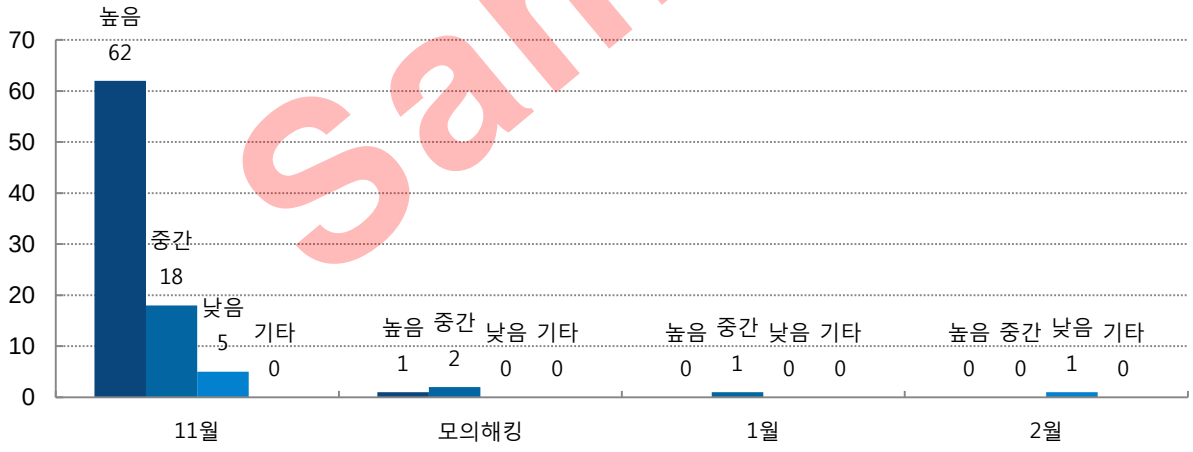
3 취약점 진단 통계

3.1 진단 평가등급 누적 통계 (서비스가입기간 : 2014년 11월 ~ 2015년 02월)



웹 버그 바운티 서비스 가입기간 동안 귀사 웹 서비스의 취약점 진단과 모의해킹을 통해 산출된 평가 등급 추이를 나타낸 누적 통계 그래프입니다.

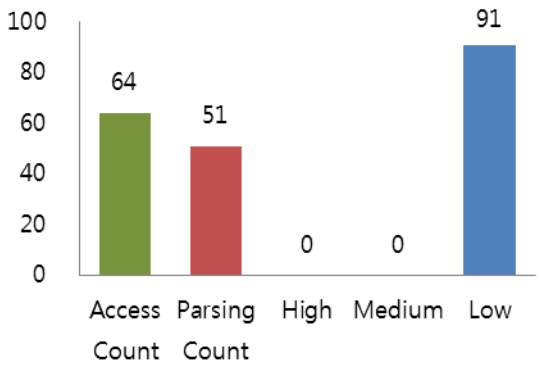
3.2 발견된 취약점 누적 통계 (최근 4개월)



웹 버그바운티 서비스 가입기간 동안 귀사 웹 서비스의 취약점 진단과 모의해킹을 통해 검출된 취약점의 누적 통계 추이를 나타낸 그래프입니다.

4 악성코드 진단 결과

4.1 악성코드(Malware) 유포 및 경유지 분석결과 요약



HTML 소스분석결과 악성코드 유포 및 경유지로 이용된 흔적이 없습니다.

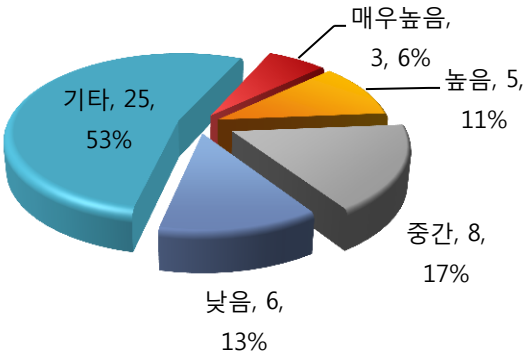
Access Count	64
Parsing Count	51
External link suspicion of first-order	**0**
External link suspicion of second-order	**0**

▶ 검출된 외부 링크 목록

No	OutLink URL	No	OutLink URL	No	OutLink URL	No	OutLink URL
1	www.aaa.co.kr	26	www.naver.com	51	www.aaa.co.kr	76	www.naver.com
2	www.bbb.co.kr	27	www.daum.net	52	www.bbb.co.kr	77	www.daum.net
3	www.ccc.co.kr	28	www.google.co.kr	53	www.ccc.co.kr	78	www.google.co.kr
4	www.ddd.co.kr	29	www.bugbounty.co.kr	54	www.ddd.co.kr	79	www.bugbounty.co.kr
5	www.eee.co.kr	30	www.test-server.co.kr	55	www.eee.co.kr	80	www.test-server.co.kr
6	www.naver.com	31	www.aaa.co.kr	56	www.naver.com	81	www.aaa.co.kr
7	www.daum.net	32	www.bbb.co.kr	57	www.daum.net	82	www.bbb.co.kr
8	www.google.co.kr	33	www.ccc.co.kr	58	www.google.co.kr	83	www.ccc.co.kr
9	www.bugbounty.co.kr	34	www.ddd.co.kr	59	www.bugbounty.co.kr	84	www.ddd.co.kr
10	www.test-server.co.kr	35	www.eee.co.kr	60	www.test-server.co.kr	85	www.eee.co.kr
11	www.aaa.co.kr	36	www.naver.com	61	www.aaa.co.kr	86	www.naver.com
12	www.bbb.co.kr	37	www.daum.net	62	www.bbb.co.kr	87	www.daum.net
13	www.ccc.co.kr	38	www.google.co.kr	63	www.ccc.co.kr	88	www.google.co.kr
14	www.ddd.co.kr	39	www.bugbounty.co.kr	64	www.ddd.co.kr	89	www.bugbounty.co.kr
15	www.eee.co.kr	40	www.test-server.co.kr	65	www.eee.co.kr	90	www.test-server.co.kr
16	www.naver.com	41	www.aaa.co.kr	66	www.naver.com	91	www.aaa.co.kr
17	www.daum.net	42	www.bbb.co.kr	67	www.daum.net		
18	www.google.co.kr	43	www.ccc.co.kr	68	www.google.co.kr		
19	www.bugbounty.co.kr	44	www.ddd.co.kr	69	www.bugbounty.co.kr		
20	www.test-server.co.kr	45	www.eee.co.kr	70	www.test-server.co.kr		
21	www.aaa.co.kr	46	www.naver.com	71	www.aaa.co.kr		
22	www.bbb.co.kr	47	www.daum.net	72	www.bbb.co.kr		
23	www.ccc.co.kr	48	www.google.co.kr	73	www.ccc.co.kr		
24	www.ddd.co.kr	49	www.bugbounty.co.kr	74	www.ddd.co.kr		
25	www.eee.co.kr	50	www.test-server.co.kr	75	www.eee.co.kr		

▪ 외부 링크가 악성코드의 유포지 및 경유지로 판명 될 경우 붉은색으로 표시됩니다.

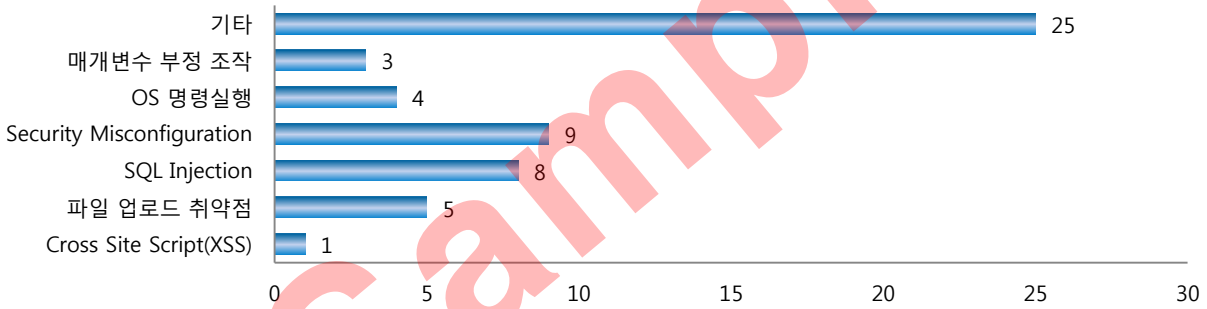
5 취약점 위험도 분포



수집된 URL 수	1,000개	
취약점 총계	47건	
위험도별 검출 수	매우 높음	3건
	높음	5건
	중간	8건
	낮음	6건
	기타	25건

그래프에서 '매우 높음'과 '높음' 위험도가 의미하는 것은 가장 가까운 미래에 해당 취약점에 대한 즉각적이고 시급한(Quick Fix) 대응이 필요함을 의미합니다. 위험도가 높은 취약점의 경우 반드시 즉시 조치하고 그 밖에 취약점 또한 해당 취약점을 활용한 해커의 공격 등이 발생하는 경우에는 위험이 현실화 될 수 있으므로 조치를 권장합니다

6 취약점 분류



7 취약점 상세 목록

- Cross Site Scripting(XSS) 취약점 1건

XSS - CSS (Cross-Site-Scripting)로 알려져 있는 이 취약점은 동적 웹 페이지에서 사용하기 전에, 웹 어플리케이션이 입력값에 대해 적합한 유효성 검사를 하지 않을 때 생깁니다.
악의적인 웹 사이트 운영자가 사용자를 자신의 웹 사이트로 유인할 수 있고, CSS 취약점이 있는 제 3의 웹사이트를 알고 있다면 다른 웹 사이트에서 만들어진 웹 페이지에 스크립트를 삽입하고 이것이 사용자에게 전달되도록 취약점을 악용할 가능성이 있습니다. 최종 결과는 악의적인 운영자의 스크립트가 다른 사이트의 신뢰성을 이용해 사용자의 컴퓨터에서 실행 되게 됩니다.
이 취약점은 웹 서버상에서 실행하고 사용자의 입력을 받아 충분한 유효성 검사 없이 이를 웹 페이지를 생성하는데 사용하는 모든 소프트웨어에 영향을 미칠 수 있습니다.

취약인자	갯수	등급	HIGH
프로토콜	http (결과 200)	메소드	GET
상위 URL	/member/03.jsp		
원본 URL	/join/05_view.jsp? No=1		
변조 URL	/join/05_view.jsp? no=%3Cscript%3EPSScanW3B_43460%3D%22test%22%3C%2Fscript%3E		

HIGH 등급의 일반 CGI 취약점: 일반 1건

취약인자	공격인자가 없는 취약점 입니다.	등급	HIGH
프로토콜	http (결과 200)	메소드	GET
상위 URL	/FCKeditor/editor/filemanager/upload/test.html		
원본 URL	FCKeditor 에디터는 원격 공격자에 의해 파일들이 수정될 수 있습니다.		
변조 URL	FCKeditor 를 최신버전으로 업데이트 해야 합니다.		

- 파일업로드 취약점 2건

File Upload 가능 - 비록 내부 명령을 실행할 수 있는 확장자를 업로드할 수는 없지만, 침입자가 웹 서버에 특정 파일을 업로드 할 수 있는 취약점이 존재한다. 이를 통해서 침입자는 명령 실행을 유도할 수 있으며, 명령 실행이 가능한 확장자들을 유추함으로써 결과적으로 웹 서버 권한을 빼앗길 위험이 있을 수 있다

취약인자	공격인자가 없는 취약점 입니다.	등급	HIGH
프로토콜	http (결과 200)	메소드	GET
상위 URL	/member/03.jsp		
원본 URL	/join/03_write.jsp		
변조 URL	/join/03_write.jsp		

취약인자	공격인자가 없는 취약점 입니다.	등급	HIGH
프로토콜	http (결과 200)	메소드	GET
상위 URL	/member/03.jsp		
원본 URL	/join/03_write.jsp		
변조 URL	/join/03_write.jsp		

중 략