DS DATA

Security Consulting

웹 취약점 진단

INDEX

01. 웹 취약점 개요

도입 배경 ▶ 관련 법령 및 가이드

정보통신기반 보호법

[법률 제18870호, 2022. 6. 10]

제9조(취약점의 분석 · 평가)

① 관리기관의 장은 대통령령으로 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석 · 평가하여야 한다.

행정 · 공공기관 웹사이트 구축 · 운영 가이드

[2021년 3월, 행정안전부]

3.2 운영활동 수행

□ 보안 관리

○ 웹서버 등 공개서버 보안 관리

- 웹서버의 사이버 침해 및 관리 소홀로 인한 정보 유출 및 변조 등을 방지하기 위한 기술적·관리적 보호조치 현황과 보안취약점 등을 정기적으로 점검하고 개선

○ 웹 보안 취약점 점검 및 대응

- 행정기관 등이 제공하는 웹서비스의 안정성 및 신뢰성을 확보하기 위하여 웹사이트의 웹 보안 취약점에 대한 상시대응 체계 마련

01. 웹 취약점 개요

도입 배경 ▶ 관련 법령 및 가이드

행정기관 및 공공기관 정보시스템 구축·운영 지침

[행정안전부고시 제2022-31호]

제50조(소프트웨어 개발보안 원칙)

① 행정기관등이 영 제71조제1항에 해당하는 정보시스템 사업을 추진할 때에는 별표 3의 소프트웨어 보안약점이 없도록 소프트웨어를 개발 또는 변경하여야 한다. 다만, 영 제71조제1항에 해당하지 않는 정보시스템 사업도 소프트웨어 개발보안을 적용할 수 있다.

[별표 3] 소프트웨어 보안약점 기준

번호	보안약점	설 명
1	SQL 삽입	SQL 질의문을 생성할 때 검증되지 않은 외부 입력값을 허용하여 악의적인 질의문이 실행가능한 보안약점
2	코드 삽입	프로세스가 외부 입력 값을 코드(명령어)로 해석·실행할 수 있고 프로세스에 검증되지 않은 외부 입력값을 허용한 경우 악의적인 코드가 실행 가능한 보안약점
3	경로 조작 및 자원 삽입	시스템 자원 접근경로 또는 자원제어 명령어에 검증되지 않은 외부 입력값을 허용하여 시스템 자원에 무단 접근 및 악의적인 행위가 가능한 보안약점
4	크로스사이트 스크립트	사용자 브라우저에 검증되지 않은 외부 입력값을 허용하여 악의적인 스크립트가 실행 가능한 보안약점
5	운영체제 명령어 삽입	운영체제 명령어를 생성할 때 검증되지 않은 외부 입력값을 허용하여 악의적인 명령어가 실행 가능한 보안약점
6	위험한 형식 파일 업로드	파일의 확장자 등 파일형식에 대한 검증없이 파일 업로드를 허용하여 공격이 가능한 보안약점
7	신뢰되지 않는 URL 주소로 자동접속 연결	URL 링크 생성에 검증되지 않은 외부 입력값을 허용하여 악의적인 사이트로 자동 접속 가능한 보안약점
8	부적절한 XML 외부 개체 참조	임의로 조작된 XML 외부개체에 대한 적절한 검증없이 참조를 허용하여 공격이 가능한 보안약점
9	XML 삽입	XQuery, XPath 질의문을 생성할 때 검증되지 않은 외부 입력값을 허용하여 악의적인 질의문이 실행가능한 보안약점
10	LDAP 삽입	LDAP 명령문을 생성할 때 검증되지 않은 외부 입력 값을 허용하여 악의적인 명령어가 실행가능한 보안약점
11	크로스사이트 요청 위조	사용자 브라우저에 검증되지 않은 외부 입력 값을 허용하여 사용자 본인의 의지와는 무관하게 공격자가 의도한 행위가 실행 가능한 보안약점

〈소프트웨어 보안약점 기준〉 일부 발췌

01. 웹 취약점 개요

도입 배경 ▶ 관련 법령 및 가이드

전자금융거래법

[법률 제17354호, 2020. 6. 9]

제21조의3(전자금융기반시설 취약점 분석 · 평가)

① 금융회사 및 전자금융업자는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자금융기반시설에 대한 다음 각 호의 사항을 분석 · 평가하고 그 결과(「정보통신기반 보호법」 제9조에 따른 취약점 분석 · 평가를 한 경우에는 그 결과를 말한다)를 금융위원회에 보고하여야 한다.

② 금융회사 및 전자금융업자는 제1항에 따른 전자금융기반시설의 취약점 분석 · 평가 결과에 따른 필요한 보완조치의 이행계획을 수립 · 시행하여야 한다.

전자금융거래법 시행령

[대통령령 제33112호, 2022. 12. 20]

제11조의5(전자금융기반시설 취약점 분석 · 평가의 절차 및 방법 등)

① 금융회사 및 전자금융업자는 법 제21조의3제1항에 따라 전자금융기반시설의 취약점 분석 · 평가를 하려는 경우에는 자체전담반을 구성하여 실시하거나 전문성을 갖춘 외부 기관에 의뢰하여 실시하여야 한다. 이 경우 자체전담반의 구성기준과 의뢰할 수 있는 외부 기관의 기준은 금융위원회가 정하여 고시한다.

01. 웹 취약점 개요

도입 배경 ▶ 금융부문 관련 정책 강화

보 도 자 료			
보도	2022. 4. 11.(월) 조간	배포	2022. 4. 8.(금)
담당부서	IT검사국	장성욱 국장 (3145-7420), 위충기 팀 장 (3145-7415)	

제 목 : 2022년도 IT리스크 상시감시 및 검사업무 운영방향

◈ 금융감독원은 **금융상품의 복잡화·다양화**로 인한 **전자금융거래의 안전성 확보** 및 **소비자 피해 예방**을 위하여 **금융부문 IT업무 전반**에 대한 「**IT 리스크 상시감시 및 검사업무 운영방향**」을 마련하였습니다.

1 추진 배경

□ 금융감독원은 2016년부터 「IT리스크 계량평가 제도」 도입하여 자산규모 2조원 이상인 **대형 금융회사**에 대하여 IT 인프라 운영상의 **주요 리스크**를 **정기적**으로 **점검**하고 있으나,

○ 최근 중소형 금융회사 및 전자금융업자가 **디지털 기반**의 **금융상품** 및 **신규서비스 출시**를 **확대**하면서

○ 대형 금융회사에 비해 **IT 인프라·정보보호 기반**이 **열악**한 **중소형 금융회사 등**의 **IT 리스크**가 **증가**할 것으로 예상됩니다.

□ 이에 **금융감독원**은 전자금융업무를 수행하는 **모든 금융회사 및 전자금융업자**의 **IT 리스크**에 **선제적 대응**이 가능하도록 **상시감시** 및 **검사 업무**를 **운영**해 나갈 계획입니다.

금융감독원 IT리스크 상시평가 강화

IT리스크를 상시 평가하여 자체감사 활동 및 선제적 대응
→ **핵심·취약 부문에 대한 사전예방적 검사를 강화**

① IT리스크에 대한 상시평가 기능 강화
- 모든 금융회사 및 전자금융업자에 대해 IT리스크 계량평가를 실시

② 자체감사 등을 통한 자율규제 기능 강화
- IT리스크 상시평가 등급이 일정기준 이하인 경우 자체감사 활동을 통해 취약점을 자율시정하도록 유도
  ※ 자체감사 결과는 IT검사국 담당 검사팀에서 '적정성 검토'를 실시하고, 개선 등의 조치가 '부적정'한 것으로 판단되는 경우에는 필요시 금융감독원이 직접 검사 실시

③ IT부문에 대한 사전예방적 검사 강화
- 금융회사의 특성 별 2~5년 주기로 IT부문에 대한 정기검사를 실시
- IT 업무 전반에 대한 '실태평가'와 함께 '상시평가' 결과 확인된 취약점 및 미흡사항에 대해서도 중점 검사
- IT사고로 소비자 피해 발생하였거나, 내부통제가 취약한 금융회사 등을 대상으로 테마검사를 강화(수시검사)

〈보도자료〉 일부 발췌

01. 웹 취약점 개요

정보보안 이슈 ▶ SQL Injection 을 활용한 해킹 수법

대규모 SQL Injection 공격으로 무작위 해킹

[긴급] 대규모 SQL 인젝션 공격으로 국내 웹사이트 무작위 해킹

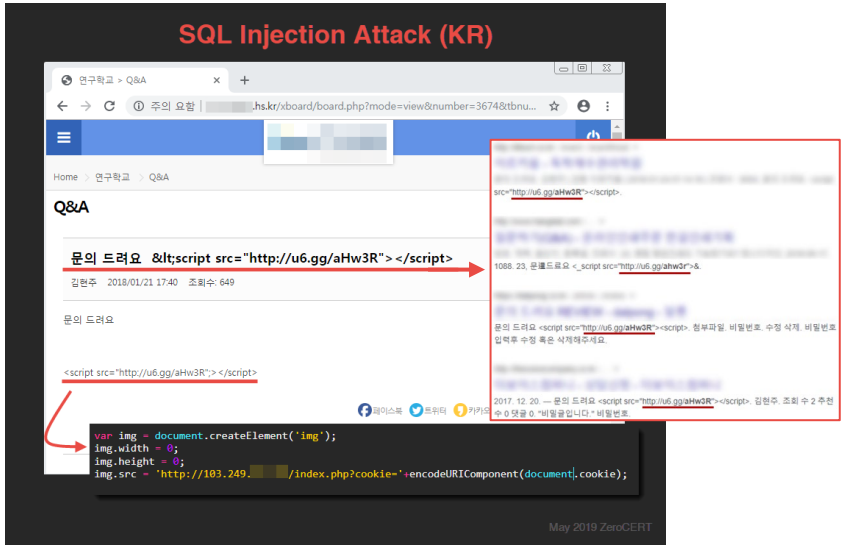
특정 게시판 취약점 악용해 공격…DB 탈취 가능성도 배제 못해
SQL 인젝션 공격 예방 위해선 모든 입력값에 대한 적절한 검증절차 설계·구현

[보안뉴스 권 준 기자] 최근 특정 게시판 취약점을 악용한 대규모 SQL 인젝션(injection) 공격이 발생해 국내 수많은 웹사이트가 피해를 입은 것으로 드러났다. 더욱이 현재까지 공격이 진행 중인 것으로 알려졌다.

[이미지=idickart]

〈출처: 보안뉴스, 2019.05.23〉

SQL Injection 무작위 해킹 공격 분석



〈출처: zerocert.org〉

- ✓ 특정 게시판 취약점을 악용해 불특정 다수에게 공격
- ✓ 단축 URL을 통해 정보 수집 및 악성 스크립트 배포
- ✓ SQL Injection과 XSS를 활용한 공격 방식

01. 웹 취약점 개요

정보보안 이슈 ▶ SQL Injection 을 활용한 해킹 수법

숙박 예약사이트 4000여건 고객정보 유출

'여기어때' 고객정보유출…"'SQL인젝션' 공격 흔적, 금전 협박"

BY 이유지 on 2017년 3월 24일 · 💬(0)

숙박 O2O(Online to Offline) 서비스 '여기어때'에서 해킹으로 고객정보가 대량 유출됐다. 최근 '여기어때'를 이용한 고객들에게 불쾌한 내용의 문자 메시지가 대량 발송됐다. 확인된 고객 수만 4000여건이다.

흔히 사용되는 웹 취약점 공격 수법인 'SQL인젝션(Injection)'에 의해 고객 개인정보가 저장된 데이터베이스(DB)가 뚫린 것으로 보인다. 현재 경찰과 한국인터넷진흥원(KISA), 미래창조과학부, 방송

이메일, 연락처, 이름 등 중요 개인정보 유출

방통위, 과징금 3억100만원과 과태료 2500만원을 부과

책임자 징계를 권고

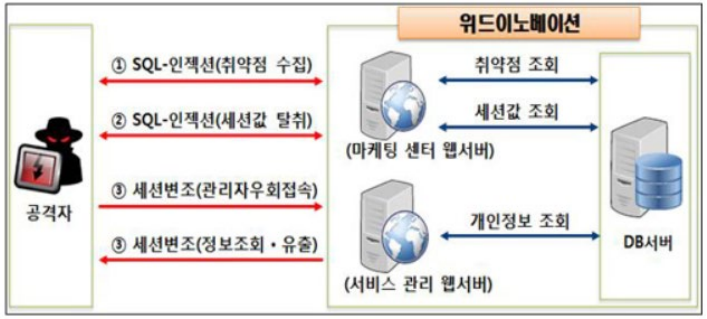
위드이노베이션에 따르면, 유출이 확인된 고객정보는 4000여건이다. 침해된 고객정보는 이메일, 연락처, 이름 등이다. 하지만 더 많은 고객정보가 유출됐을 가능성도 배제할 수는 없는 상태다.

고객정보 유출 사실은 '여기어때'를 이용한 고객들이 불쾌한 문자를 받으면서 인지한 것으로 보인다. '여기어때'는 해커로부터 비트코인으로 금전을 요구하는 협박메일도 받았다.

해커는 문자 대량 발송 서비스를 이용해 두 차례에 걸쳐 고객들에게 문자 메시지를 무단 전송했다. 모르는 번호로 불쾌감을 유발할 수 있는 문자를 받은 고객은 KISA 개인정보침해신고센터에 신고했다.

〈출처: 2017.03.24, 바이라인네트워크〉

숙박 예약사이트 4000여건 고객정보 유출 분석



▲ 해킹 과정 개요[제공: 방통위, 미래부]

〈출처: 보안뉴스 2017.04.26 〉

- ✓ 비정상적인 DB 질의에 대한 검증 절차가 없어 SQL 인젝션 공격에 취약한 웹페이지가 존재
- ✓ 탈취된 관리자 세션 값을 통한 우회 접속(세션 변조 공격)을 탐지·차단하는 체계가 없는 것으로 확인

01. 웹 취약점 개요

정보보안 이슈 ▶ SQL Injection 을 활용한 해킹 수법

개인정보 유출에 대한 소송제기

- ✓ ‘위드이노베이션’ 상대로 손해배상소송 제기
- ✓ ‘여기어때’ 개인정보 유출 피해자 회사 대표 형사 고소

〈 2017.09.11 여해법률사무소 〉

‘정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정통망법)’에서 법정손해배상제도 관련 조항이 신설됨에 따라
개인정보 유출 피해자들은 피해액에 대한 구체적인 입증이 없어도 300만 원 이하의 범위에서 손해배상을 청구할 수 있게 됐다.

⚠ 참고: SQL Injection

데이터베이스에 대한 질의값(SQL 구문)을 조작해 정상적인 자료 이외에 공격자가 원하는 자료까지 데이터베이스로부터 유출 가능한 공격 기법

전산 담당자의 고민

전산담당자는 누구보다도 정보보안의 중요성을 알지만

다음과 같은 이유로 보안 취약점 및 개인정보를 관리하고자 할 때 고민이 생깁니다.

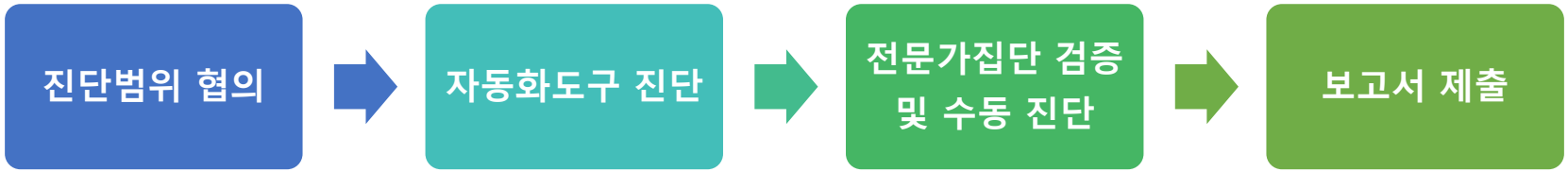
Security Consulting은 별도의 관리 인력 및 구축형 솔루션 없이도 우수한 제품으로

보안취약점 조치 및 정보보호컨설팅을 할 수 있게 결과를 제공합니다

02. 웹 취약점 진단

진단 절차 및 일정

웹 취약점 진단은 다음 절차에 따라 수행합니다.



웹 취약점 진단 시 예상 일정은 다음과 같습니다. (진단 범위에 따라 상이)

구분	예상 일정
진단범위 협의 및 수행계획서 작성	3일
자동화도구 진단 수행	2주
전문가집단 검증 및 수동 진단	3주
보고서 작성 (주요 취약점 및 개선안)	7일

02. 웹 취약점 진단

서비스 소개

웹 취약점 진단 서비스를 통해 가장 복합한 Application들의 보안홀까지도 발견할 수 있습니다.

보안 자문 서비스

보안 향상을 가속화 시킬 수 있습니다

위협 노출 관리

위험 확률을 감소시킬 수 있습니다

사고 탐지 및 응답

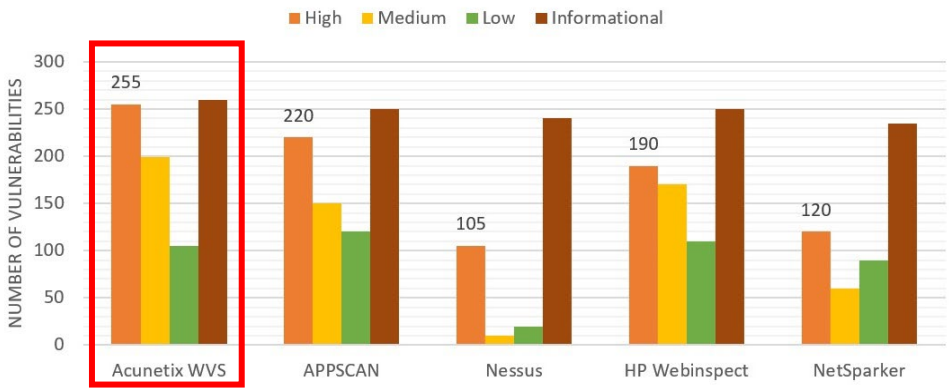
이미 놓친 공격도 찾을 수 있습니다

02. 웹 취약점 진단

서비스 소개

웹 취약점 진단 도구 중 가장 탐지력이 뛰어나고 미탐 및 오탐율이 낮은 도구를 활용하여 진단하므로 보다 정확한 결과값을 토대로 조치 방안을 제시합니다.

취약점 탐지 성능



〈웹 취약점 진단 도구에서 탐지된 취약점 수〉

진단 도구 신뢰도

Table 5. Precision rate of evaluated scanners.

Evaluated Scanner	CSS		SQLI		Precision
	TP	FP	TP	FP	
Acunetix	139	0	66	0	100%
IBM APPSCAN	6	5	49	0	84%
Nessus	200	21	43	5	90.88%
BurpSuite	136	3	62	0	98.5%
Wapiti	11	7	4	6	53%
Arachni	136	5	60	0	81.32%
WebInspect	8	7	11	17	44.1%
Nikto	9	2	11	6	71.4%
Netsparker	136	3	64	0	98.5%

〈웹 취약점 진단 도구의 정밀도 비율〉

〈출처 : Shahid J, Hameed MK, Javed IT, Qureshi KN, Ali M, Crespi N.
A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions.
Applied Sciences. 2022; 12(8):4077.〉

02. 웹 취약점 진단

서비스 소개 ▶ 진단 항목(1/3)

OWASP Top 10 항목, KISA 홈페이지 취약점 진단제거 가이드, 국정원에서 발표한 8대 취약점 중 중요 항목을 선별하여 진단을 수행하고 조치 방안을 안내합니다.

단계	코드	취약점 항목	공격 피해
웹 어플리케이션	OC	운영체제 명령 실행	시스템 장악
	SI	SQL 인젝션	DB 정보 유출
	XI	Xpath 인젝션	사용자 인증 우회
	IL	정보누출	서버 정보 노출
	CS	악성콘텐츠	악성코드 감염
	XS	크로스 사이트 스크립트(XSS)	세션하이재킹 악성코드 전파
	BF	약한 문자열 강도	사용자 계정 탈취
	IN	불충분한 인증 및 인가	관리자 권한 탈취
	PR	취약한 패스워드 복구	사용자 계정 탈취
	SM	불충분한 세션 관리	사용자 권한 탈취
	CF	크로스 사이트 리퀘스트 변조(CSRF)	사용자 권한 탈취

[표 2-1] KISA 가이드 기준 웹 취약점 진단 항목

02. 웹 취약점 진단

서비스 소개 ▶ 진단 항목(2/3)

OWASP Top 10 항목, KISA 홈페이지 취약점 진단제거 가이드, 국정원에서 발표한 8대 취약점 중 중요 항목을 선별하여 진단을 수행하고 조치 방안을 안내합니다.

단계	코드	취약점 항목	공격 피해
웹 어플리케이션	AU	자동화 공격	시스템 과부하
	FU	파일 업로드	시스템 장악
	FD	경로추적 및 파일 다운로드	웹 서버 정보 노출
	SN	데이터 평문 전송	중요 정보 노출
	CC	쿠키 변조	사용자 권한 탈취
	UP	URL/파라미터 변조	사용자 권한 탈취
웹 서버	DI	디렉터리 인덱싱	시스템 파일 노출
	AE	관리자페이지 노출	웹 사이트 정보 노출
	PL	위치공개	웹 사이트 정보 노출
	MS	웹 서비스 메소드 설정 공격	시스템 장악

[표 2-2] KISA 가이드 기준 웹 취약점 진단 항목

02. 웹 취약점 진단

서비스 소개 ▶ 진단 항목(3/3)

A - E

- Apache Struts 2 Framework Checks
- Apache Struts Detection
- Arbitrary File Upload
- Autocomplete attribute
- Blind SQL (improved)
- Brute Force (Form Auth)
- Brute Force (HTTP Auth)
- Business logic abuse attacks
- Cookie attributes
- Credentials stored in clear text in a cookie
- Cross-Site Request Forgery (CSRF)
- Cross-site scripting (XSS), DOM based
- Cross-site scripting (XSS), reflected
- Cross-site tracing (XST)
- Directory Indexing
- Email Disclosure

F - R

- Forced Browsing
- Form Session Strength
- HTTP Response Splitting
- HTTP Strict Transport Security
- HTTPS Downgrade
- Information Disclosure
- Information Leakage
- Java Grinder
- OS Commanding
- Parameter Fuzzing
- Predictable Resource Location
- Privacy Disclosure
- Profanity
- Reflection
- Remote File Include (RFI)
- Reverse Proxy

S - Z

- Secure and non-secure content mix
- Server Configuration
- Session Fixation
- Session Strength
- Source Code Disclosure
- SQL Injection
- SQL injection Auth Bypass
- SSL Strength
- Unvalidated Redirect
- URL rewriting
- Web Beacon
- Web Service Parameter Fuzzing
- X-Frame-Options missing HTTP header
- X-XSS-Protection missing HTTP header
- Z-Customer created attack

02. 웹 취약점 진단

웹 취약점 검증 프로세스

자동화 진단 도구에서 발견된 취약점을 바탕으로 해당 취약점을 재 검증하여 최종 결과 보고서를 작성 합니다

1 웹 취약점 진단 도구 실행 (보고서 생성)

▼

2 검증 수행

 Burp suite	• PC에서 외부로 나가는 패킷과 외부에서 PC로 들어오는 패킷을 제어할 수 있는 proxy tool • 웹 취약점 검증 시 클라이언트와 웹 서버 간의 요청/응답 패킷을 변조하여 검증 함 • **XSS, SQL injection 등**을 검증
 Wireshark	• 네트워크 패킷을 캡처하여 분석 할 수 있는 도구 • **데이터 평문 전송**을 검증
 RESTClient	• URL 입력 후 접속 시 Response 헤더정보 확인 • **서버 타입 정보 누출**을 검증

▼

3 결과보고서 작성

02. 웹 취약점 진단

보고서 제공

OWASP Top 10 항목, KISA 홈페이지 취약점 진단제거 가이드, 국정원에서 발표한 8대 취약점을 기준으로 진단한 결과 값에 대한 리포트 및 해결 방안을 제시합니다.

웹 취약점 진단 결과 보고서 목차

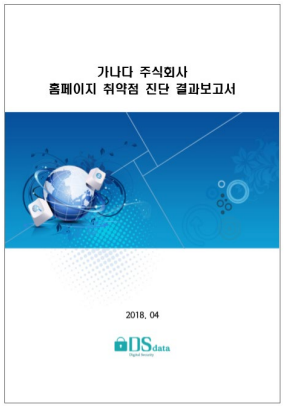
진단 개요	진단방법 및 진단대상	진단 결과
● 진단목적	● 진단 절차	● 총평
● 수행 담당자	● 진단 도구	● 진단 결과 상세 현황
● 진단일정	● 진단 항목	
	● 진단 대상	

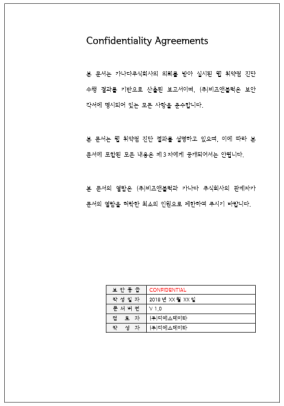
02. 웹 취약점 진단

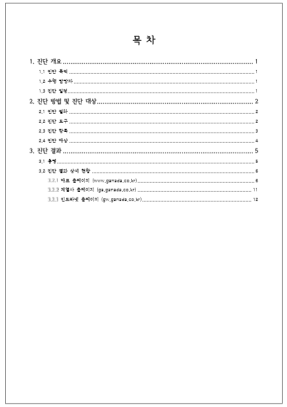
보고서 제공

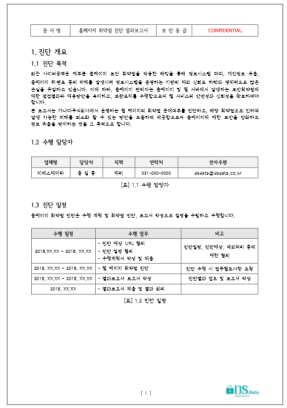
OWASP Top 10 항목, KISA 홈페이지 취약점 진단제거 가이드, 국정원에서 발표한 8대 취약점을 기준으로 진단한 결과 값에 대한 리포트 및 해결 방안을 제시합니다.

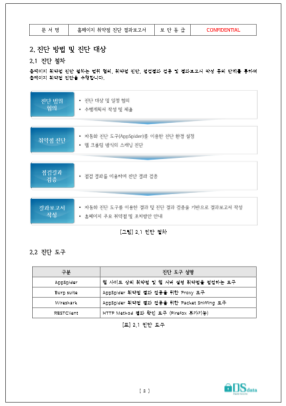
웹 취약점 진단 결과 보고서

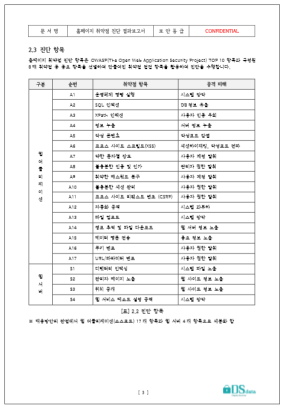


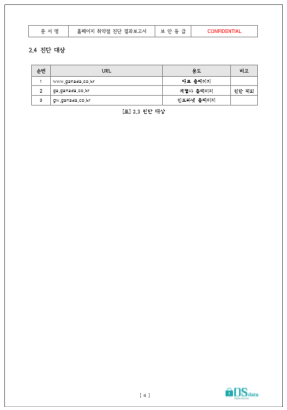


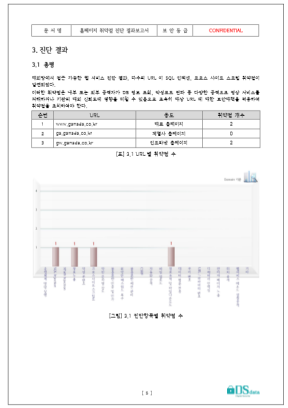


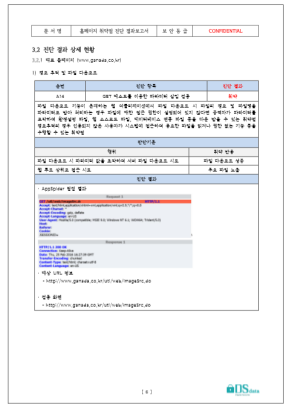


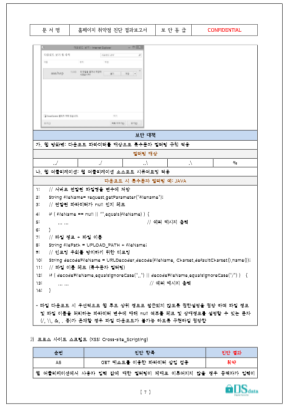












03. 특장점 및 기대효과

특장점

웹 페이지 관리자는 웹 페이지 및 웹 서버에서 발생하는 보안취약점에 대한 점검결과와 대응방안을 숙지하고, 보완 조치를 수행함으로써 웹 서비스의 안전성과 신뢰성을 확보하여야 합니다.

글로벌 3대 진단도구

acunetix

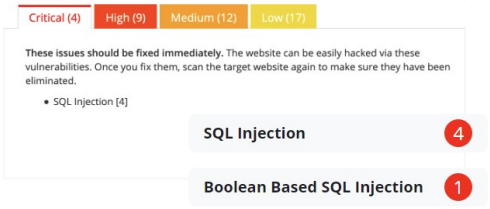
appspider

AppScan

IBM Security

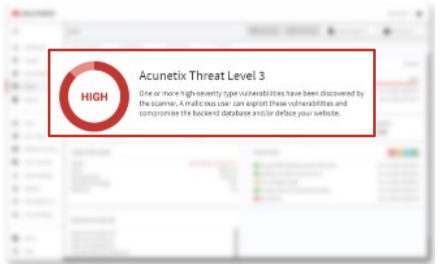
- 경쟁도구 대비 10~20배의 취약점을 찾아냄
- 가장 낮은 오탐률을 가진 진단 툴을 활용하여 자동화 진단 실시

손 쉬운 취약점 조치



- 검증 결과 제공: 손쉬운 취약점 확인 및 취약점 교정
- 우선 순위 제공: 중요 사항부터 우선순위화 하여 결과 제공

안정적인 진단



- 실제 서비스를 제공하는 서버에 사용할 수 있도록 안전하게 설계

03. 특장점 및 기대효과

기대효과

관리의 편리성

별도의 관리자 및 Agent 없이 진단을 실시하고 그 결과를 확인할 수 있습니다

합리적인 비용

초기 도입비용 없이 합리적인 가격으로 양질의 서비스를 받을 수 있습니다

보안 감사 대비

상위기관에서 실시하는 정보보안 감사에 대비할 수 있습니다

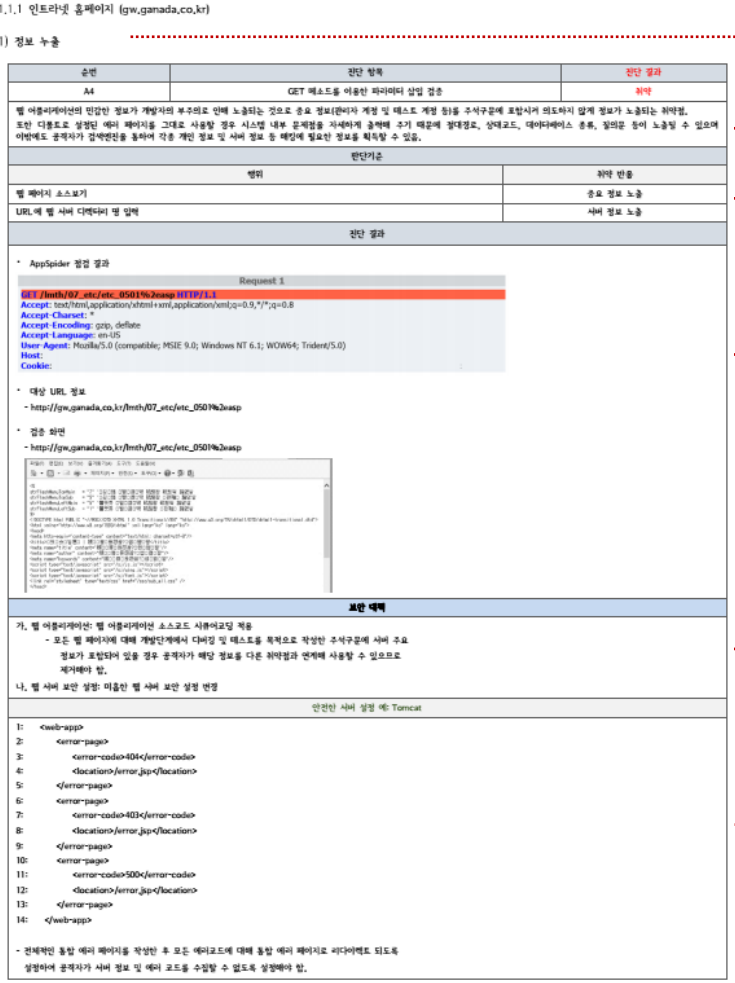
보안 정책 수립

취약성이 높은 것부터 우선 조치하고 이를 기반으로 보안 정책 수립이 가능합니다

04. 웹 취약점 산출물

웹 취약점 결과 보고서

웹 취약점 진단 도구로부터 생성된 보고서를 바탕으로 발견된 취약점을 URL(홈페이지)기반으로 결과 보고서 작성



1.1.1 인트라넷 홈페이지 (gw.ganada.co.kr)

1) 정보 누출

순번	진단 항목	진단 결과
A4	GET 메소드를 이용한 파라미터 삽입 검증	취약

웹 어플리케이션의 민감한 정보가 개발자의 부주의로 인해 노출되는 것으로 중요 정보(관리자 계정 및 테스트 계정 등)를 주석구문에 포함시켜 의도하지 않게 정보가 노출되는 취약점.
또한 디폴트로 설정된 에러 페이지를 그대로 사용할 경우 시스템 내부 문제점을 자세하게 출력해 주기 때문에 절대경로, 상대코드, 데이터베이스 종류, 질의문 등이 노출될 수 있으며 이밖에도 공격자가 검색엔진을 통하여 각종 개인 정보 및 서버 정보 등 해킹에 필요한 정보를 획득할 수 있음.

판단기준	
범위	취약 반응
웹 페이지 소스보기	중요 정보 노출
URL에 웹 서버 디렉터리 명 입력	서버 정보 노출

진단 결과

- AppSpider 점검 결과

Request 1

```
GET /lmth/07_etc/etc_0501%2easp HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Charset: *
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host:
Cookie:
```

- 대상 URL 정보
  - http://gw.ganada.co.kr/lmth/07_etc/etc_0501%2easp
- 검증 화면
  - http://gw.ganada.co.kr/lmth/07_etc/etc_0501%2easp

보안 대책

가. 웹 어플리케이션: 웹 어플리케이션 소스코드 사용여부 적용
- 모든 웹 페이지에 대해 개발단계에서 디버깅 및 테스트를 목적으로 작성한 주석구문에 서버 주요 정보가 포함되어 있을 경우 공격자가 해당 정보를 다른 취약점과 연계해 사용할 수 있으므로 제거해야 함.

나. 웹 서버 보안 설정: 미흡한 웹 서버 보안 설정 변경

안전한 서버 설정 예: Tomcat

```
1:  <web-app>
2:      <error-page>
3:          <error-code>404</error-code>
4:          <location>/error.jsp</location>
5:      </error-page>
6:      <error-page>
7:          <error-code>403</error-code>
8:          <location>/error.jsp</location>
9:      </error-page>
10:     <error-page>
11:         <error-code>500</error-code>
12:         <location>/error.jsp</location>
13:     </error-page>
14: </web-app>
```

- 전체적인 통합 에러 페이지를 작성한 후 모든 에러코드에 대해 통합 에러 페이지로 리다이렉트 되도록 설정하여 공격자가 서버 정보 및 에러 코드를 수집할 수 없도록 설정해야 함.

홈페이지별 취약점

진단항목 및 취약점 설명

취약 판단 근거

① 점검결과: 자동화 진단 도구에서 생성된 보고서 화면

② 대상 URL 정보: 해당 취약점을 가지고 있는 URL 목록 작성

③ 검증화면: 취약점 검증한 URL 및 취약한 검증 화면

취약점 보안대책 설명

설정 방법의 예시

감사합니다

DS data
Digital Security

Contact us.

Homepage :
https://www.dsdata.co.kr

Email :
sales@dsdata.co.kr

Tel :
031-698-2066