

홈페이지 개인정보 노출예방 교육



CONTENT

I. 개 요

II. 개인정보 노출 사례 및 긴급 조치

III. 개인정보 노출 예방





I. 개 요

- 1 개인정보 “노출”과 “유출”의 차이
- 2 개인정보 노출의 문제점
- 3 개인정보 노출관련 제재
- 4 개인정보 노출 모니터링





“개인정보” 『유출』 이란?

정보주체의 “개인정보”에 대하여 개인정보처리자가 통제를 **상실**하거나 또는 **권한 없는 자**의 접근을 허용한 경우 (고의+과실+부주의)

- “개인정보 노출”은 유출의 한 부분



게시판 상담요청 및 처리 시, **개인정보가 포함된 내용을 그대로 답변 등으로 게시**할 경우



검색엔진 등을 통한 사이트 내에 개인정보가 수집/저장되어 일반인이 **노출된 개인정보에 접근**하게 하는 경우



개인정보가 저장된 DB 등 개인정보처리시스템에 정상적인 **권한이 없는 자가 접근**한 경우



개인정보처리자의 **고의 또는 과실**로 인해 개인정보가 포함된 파일, 문서, 저장매체 등이 **잘못 전달**된 경우

개인정보 “유출”과 “노출”의 차이 (Ⅱ)



홈페이지를 통한 “개인정보” 『노출』 이란?

홈페이지 이용자가 해킹 등 특별한 방법을 사용하지 않고, 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 인터넷 상에서 관련 『정보가 방치』된 상태
- 주로 과실, 부주의로 발생



※ 노출되면 안 되는
고유식별정보

- + 운전면허번호
- + 외국인등록번호...



고유식별정보 등 사생활 침해가 우려되는 정보가 노출

노출되어서는 안 되는 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인 등록번호), 신용카드번호, 계좌번호, 바이오정보 등

- 노출시 법적 제재의 대상이 될 수 있음



홈페이지에 노출된 개인정보는 구글 등 검색엔진에 2차 노출

홈페이지에 노출된 개인정보를 신속히 삭제하지 않을 경우, 구글 등 검색엔진에 의해 노출이 확산되거나, 제3자에 의해 수집됨

- 개인은 명의도용, 보이스피싱 등 범죄에 악용, 대량 스팸 수신 등 피해
 - * 노출된 정보는 수집되어 **개인을 분석하는 자료로 활용**(프라이버시 침해)
- 기업은 이미지 실추, 다수 피해자에 의한 손해배상 소송 제기



검색엔진(구글, 네이버, 다음 등)의 크롤러(수집기)는 홈페이지의 **모든 정보**를 수집하여 검색엔진 DB에 저장
- 이 과정에서 개인정보나 비공개 자료도 포함



검색엔진은 홈페이지에 노출된 **정보** 외에 SNS, 일정관리 등을 종합적으로 수집 분석하여 특화된 서비스 제공

검색엔진 이해 (2)



홈페이지에 노출된 개인정보를 삭제했더라도, 검색엔진은 삭제하기 이전의 홈페이지 정보(캐시)를 저장하고 있음
=> 구글 등 검색엔진에 별도로 삭제를 요청하여야 함

한국인터넷진흥원

www.kisa.or.kr

한국인터넷진흥원 사이트

클릭시 메뉴표시됨

한국인터넷진흥원
www.kisa.or.kr

한국인터넷진흥원
학부의 정보시스템

저장된 페이지
유사한 페이지

환영합니다.본 페이지는 WCAG2.0,KWCAG2.0 및 미래창조과학부의 지침을 준수하여 제작...

세금납부 현황 < 재무·회계 < 사전정보공표 < 정보공개 < 정부 3.0 정보 ...
https://www.kisa.or.kr/disclosure/process03_0006.jsp

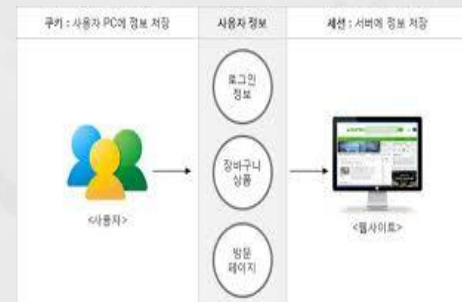
세금납부 현황 목록. 번호, 제목, 게시일, 조회, 첨부, 2015년 세금납부 현황, 2016-02-11, 204, 첨부파일 2, 2014년 세금납부 현황, 2015-02-06, 723, 첨부파일 1.

현재 페이지

저장된 페이지



"구글 등 검색엔진에 남아 있음"



안전조치 의무

- 개인정보 또는 **고유식별정보**가 분실·도난·유출·변조·훼손되지 않도록 안전성 확보에 필요한 기술적·관리적·물리적 조치 이행 (개인정보보호법 제24조제4항, 제29조)

안전성 확보 조치

- 안전성 확보조치에 필요한 세부사항은 행정안전부장관이 지침으로 정하여 고시

번호	고시 조항	조치할 사항	비고
①	고시 제6조 제3항	○ 취급중인 개인정보가 인터넷 홈페이지 , P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개 되거나 유출되지 않도록 접근 통제 등에 관한 조치 시행	
②	고시 제6조 제4항	○ 인터넷 홈페이지를 통해 고유식별정보 가 유출, 변조, 훼손되지 않도록 연 1회 이상 취약점을 점검 하고 필요한 보완조치 시행	
③	고시 제7조 제1항	○ 고유식별정보, 바이오정보, 비밀번호의 암호화	
④	고시 제7조 제2항	○ 비밀번호 및 바이오정보 암호화 (단, 비밀번호는 단방향 처리)	
⑤	고시 제7조 제3항	○ 인터넷 구간 및 인터넷 구간과 DMZ 구간의 고유식별정보의 암호화	

처벌 규정

- 미이행 시, 3천만원 이하의 과태료
- 미이행으로 인한 유출 시, 2년 이하 징역 또는 1천만원 이하 벌금

※ 정보통신망법 “개인정보 기술적 관리적 보호조치 기준”에서는 **고유식별정보 외에 신용카드번호, 계좌번호, 바이오정보를 암호화하도록 규정**



개인정보 노출시 경우에 따라 정보주체에게 통지 의무

유출사고
발생

“정보주체”에게 통지

- 후속 피해의 최소화 및 예방
- 피해구제

[통지 시기]

사고 발생 후, 사건경위 및
잠정적 원인 등을 파악 후, 통지

[통지 내용]

- 유출된 개인정보의 항목
- 유출된 시점과 그 경위
- 유출로 인한 피해 최소화를 위한 방법
- 개인정보처리자의 대응조치 및 피해 구제절차
- 피해 접수 위한 담당부서 및 연락처

[대책 마련]

- 유출사고 원인 분석
- 기술지원 의뢰 및 복구
- 직원 징계, 사법조치 의뢰
- 유사사고 재발 방지대책 수립

[통지 방법]

- 웹사이트 첫 화면 게재
- 전화
- 이메일 등



[법 제34조]

“개인정보 유출사실 통지 의무화”



미통지 시,
과태료 3천만원



정기적인 개인정보 노출 여부 모니터링 실시

- 시행주체 : 행정안전부, 한국인터넷진흥원
- 모니터링 대상
 - 홈페이지 : 20만여개 공공기관, 비영리단체 등
 - 검색엔진 : 구글, 네이버 등 검색엔진
- 대상 정보
 - 홈페이지 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
 - 검색엔진 : 고유식별정보, 신용카드번호, 키워드(번호, 이력서 등) 등



노출 기관에 대한 조치

- 개인정보가 노출된 기관에 삭제 등 조치하도록 통보
 - 공공기관의 경우, 상급 기관에 통보
- 행정안전부의 “개인정보 관리실태 특별점검” 대상에 포함
- 노출된 기관의 담당자에게 “개인정보 노출 재발방지” 교육 실시(필수)

Ⅱ . 개인정보 노출 사례 및 조치





약 59%

(126,035건)
증가

스포츠월드
뉴스 인쇄
해정문서 관리 허점.. 개인정보
줄줄 (16.10)

개인정보 뒤져,
탈퇴 종용
이정보 보호 'F학점'

스마트폰 개인정보 ‘술술’

말을 종합하면, 지난 2월부터 심평원 누리집을 통해 건강보험
민원인 3300여명의 주민등록번호와 요양기관, 본인부담금 액수
여 동안 노출됐다. 이들의 개인정보는 검색엔진 '구글'을 통해 노
...보험업체의 신고를 받고 나서야 이런 사실을 파악해 구
...를 강화했다. 신아무개(51)씨의 경우, 주민번호
...의 본인부담금이 537만원이라는 내

주민등록

미술대회 접수자
개인정보 대거 유출

[illegible]



홈페이지 노출 정보가 검색엔진에 저장 및 재노출

[단독] 구글神 때문에...공무원 개인정보 및 관리자 페이지 대거 노출

입력날짜 : 2017-03-06 15:50

스크랩 프린트하기 목록

좋아요 273 트윗



구글 색인기능으로 로그인된 관리자 페이지 무방비 노출

정부산하기관 및 지자체 GIS 시스템 구축기업 등에서 공무원 개인정보 열람 가능
검색엔진 배제 표준이나 관리자 페이지 세션처리 등으로 검색 안 되도록 해야

[보안뉴스 원병철 기자] 지난 3월 3일 본지는 구글 검색에 의한 개인정보 노출의 심각성에 대해 문제를 제기한 바 있다. 너무나 열심히 일하는(?) 구글 봇 때문에 다음의 한 카페에 올라온 회원 주소록이 별도의 로그인 없이도 그대로 노출된 사건이었다. 해당 기사가 나간 후 구글의 검색기능으로 꽤나 많은 홈페이지들의 관리자 페이지에 접속할 수 있으며, 관리자 권한으로 회원 등의 개인정보를 그대로 검색할 수 있다는 제보가 들어왔다.

Google **intitle / inurl:admin**

전체 동영상 이미지 뉴스 지도 더보기 설정 도구

한국어 웹 모든 날짜 모든 결과 초기화

- 쇼핑몰 관리자 로그인
getmallskin.getmall.kr/admin/
- 관리자 모드 - 한국교회연합
www.ccik.kr/admin/
- 관리자모드 로그인 - 소셜미디어구입구 - CAPE INDUSTRIES LTD
cape.co.kr/admin/login.html
- 관리자 데모 - 베스트상품 베스트상품을 소개합니다. - 쓰리웨이
demoshop.web2002.co.kr/admin/
- 관리자페이지입니다.
www.wj-enertec.co.kr/admin/login.htm
- 쇼핑몰+홈페이지 통합솔루션 센스콤비 v1.0 사이트 관리자 페이지
combi21.e-sens.co.kr/admin/
- 관리자 :: 이루온
www.eluon.com/admin/member
- 관리자 로그인 - admin/index.asp
www.hosiden.co.kr/admin/index.asp
- HAPDONG 관리자 로그인 - 합동택배
www.hdexp.co.kr/admin/
- ADMIN - 관리자 모드
www.appleden.com/admin/

관리자 페이지 대거 노출

개인정보 취급자 부주의



- 개인정보가 포함된 첨부파일 업로드

홈페이지 이용자 부주의



- 게시글 또는 댓글에 개인정보 포함



홈페이지 설계 및 관리 미흡



< 홈페이지 설계 오류 >

- URL 내, 개인정보 노출
- 소스코드 내, 개인정보 노출
- 게시글 작성 중, 임시 저장 페이지 노출
- 디렉터리 리스팅

< 관리미흡 >

- 관리자 페이지 접근제어 미흡



2016년도 홈페이지 노출 유형 Top 3



1. 첨부파일 노출 (42.7%)
2. 홈페이지 이용자 부주의 (33.6%)
3. 관리자 페이지 접근제어 미흡 (14.1%)



첨부 파일 노출 유형

노출 빈도 1위 엑셀파일



2016년 첨부파일 노출 TOP 3

1. 엑셀파일(.xls, 95.45%)
2. 한글파일(.hwp, 4.30%)
3. 이미지파일(***, 0.25%)

1. Sheet 숨기기 처리
2. 함수 치환 처리
3. 행/열 숨기기
4. Sheet 보호 처리
5. 글자색을 배경색과 같게 처리
6. 메모에 "개인정보" 입력
7. "개인정보"가 포함된 개체 삽입 (OLE개체)
8. 한글파일 (서식)에서 노출된 "개인정보"
9. 이미지 파일에 "개인정보" 포함

편리하게 주어진 "기능"과 "옵션"을 통해 노출이 되고 있음. 그리고 일부 "잘못된 사용"...

첨부 파일에 노출된 형태



개인정보가 포함된 엑셀 파일을 첨부하여 게시판에 게시

행정정보 시고시

홈 > 행정정보 > 알림마당

정보공개 > 공고 > 전주시보

통합검색

공개개방 전자민원 참여소통 알림마당 소개 분야별정보

알림마당

시정소식

고시공고

알림마당 > 시정소

『농업진흥지역 변경(해제) 계획(안)』열람 공고

고시공고구분	공고(일반공고)	게제제호
고시공고번호	공고 제2016-855호	등록일
담당부서	농업정책과	

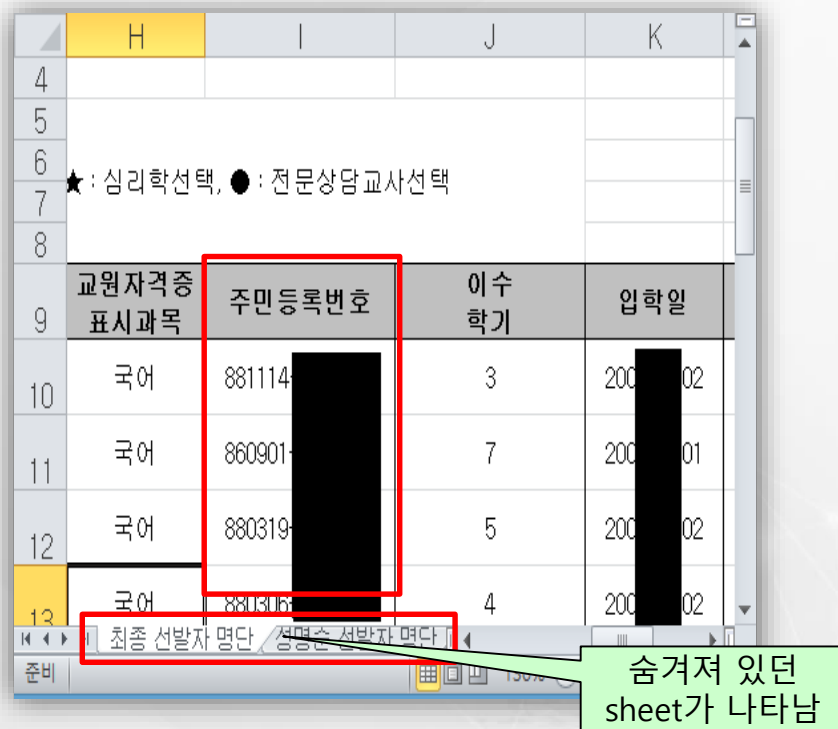
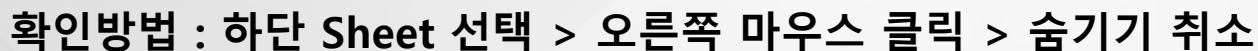
첨부파일

- 시보 제8 호.hwp(7.0MB)
- 시고시 제201 호 불임.xlsx(1.0MB)

클릭하면, "저장"까지 됨

eminwon. 의 농업진흥지역 변경(해제)계획 열람공고(안).hwp(15.5KB)를 열거나 저장하시겠습니까?

열기(O) 저장(S) 취소(C)



<Sheet 숨기기 취소한 파일>

Step 1. 게시물을 비공개로 전환
Step 2. 숨겨진 Sheet 삭제
Step 3. 검색엔진에 저장된 페이지 삭제

첨부 엑셀 파일에 노출 > 행/열 [숨기기] 처리



확인방법 : 열(A,B...) 또는 행(1,2...) 전체선택 > 오른쪽 마우스 클릭 > 숨기기 취소



대형폐기물스티커 판매소 현황

판매소명	주인명	주민등록번호
AA 마트	SS시 AA구 BB동	440227
BB 타운	SS시 ZZ구 QQ동	621013
NN 마트	SS시 AS구 EB동	561230
HH 슈퍼	SS시 AW구 CF동	550424
YY 철물	SS시 AZ구 QB동	
SS 슈퍼	SS시 AX구 CV동	
LL 마트	SS시 BA구 BB동	
AB 등점	SS시 AA구 BB동	780822
BC 상회	SS시 ZZ구 QQ동	630417
SF 슈퍼	SS시 AS구 EB동	691110
CZ 유통	SS시 AW구 CF동	750126
QW 슈퍼	SS시 AZ구 QB동	
BD 점	SS시 AX구 CV동	720125
ASE 점	SS시 BA구 BB동	

숨기기 취소

대형폐기물스티커 판매소 현황

판매소명	주인명	주민등록번호
AA 마트	SS시 AA구 BB동	440227
BB 타운	SS시 ZZ구 QQ동	621013
NN 마트	SS시 AS구 EB동	561230
HH 슈퍼	SS시 AW구 CF동	550424
YY 철물	SS시 AZ구 QB동	
SS 슈퍼	SS시 AX구 CV동	
LL 마트	SS시 BA구 BB동	
AB 등점	SS시 AA구 BB동	780822
BC 상회	SS시 ZZ구 QQ동	630417
SF 슈퍼	SS시 AS구 EB동	691110
CZ 유통	SS시 AW구 CF동	750126
QW 슈퍼	SS시 AZ구 QB동	
BD 점	SS시 AX구 CV동	720125
ASE 점	SS시 BA구 BB동	

<행/열 숨기기 처리>

<행/열 숨기기 취소>

조치

Step 1. 게시물을 비공개로 전환

Step 2. 숨겨진 "행/열" 숨기기 취소, "행/열"에 기록된 개인정보 삭제

Step 3. 검색엔진에 저장된 페이지 삭제

첨부 엑셀 파일에 노출 > 치환함수



확인방법 : 마스킹 된 부분을 마우스로 클릭+드래그하여 "함수" 해제 후, 육안 확인



D3 fx =LEFT(C3,6)&"-*****"

B 다음 D ?

연번	성명	주민등록번호	체납건수	체납액
1	조00	740912-*****	10	000,000,000
2	신00	661002-*****	13	000,000,000
3	남00	500609-*****	7,772,222,570	
4	이00	730730-*****	14	000,000,000
5	엄00	401231-*****	14	000,000,000
6	김00	760305-*****	18	000,000,000
7	손00	500506-*****	22	000,000,000
8	최00	480607-*****	11	000,000,000

마스킹 취소

<개인정보를 치환 함수로 마스킹>

성명	주민등록번호	주민등록번호	체
조00	740912-00000000	740912-*****	
신00	661002-00000000	661002-*****	
남00	500609-00000000	500609-*****	
이00	730730-00000000	730730-*****	
엄00	401231-00000000	*****	
김00	760305-00000000	760305-*****	
손00	500506-00000000	500506-*****	
최00	480607-00000000	480607-*****	

숨어있던 C열 확인 가능

해제

직접 치환

<치환된 필드를 해제 / 취소한 경우>

조치

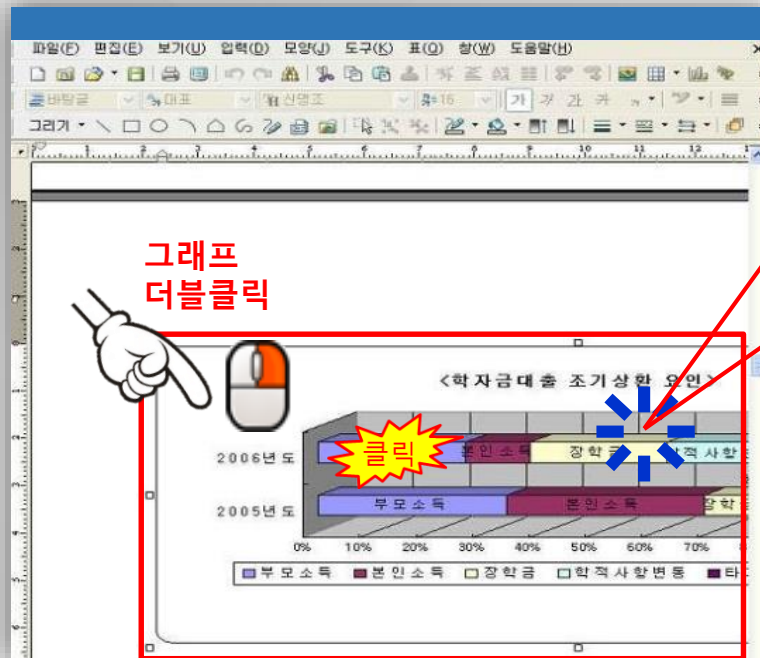
Step 1. 게시물을 비공개로 전환

Step 2. 노출된 개인정보 삭제 혹은 "직접치환(마스킹)" 처리

Step 3. 검색엔진에 저장된 페이지 삭제



확인방법 : 문서 내의 “표” 클릭 > OLE 객체 내 “개인정보” 포함 여부 확인



<OLE 객체가 삽입된 파일>

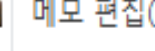
개인정보 발견

1	A	B	C	D	E	F
	년도	은행	계좌번호	출생년도	주민등록번호	핸드폰번호
2	2005	민	94521	81	81	01
3	2005	리	12018	80	80	01
4	2005	나	93046	49	49	01
5	2005	협	00019	77	77	01
6	2005	흥	93604	85	85	01
7	2005	나	48941	67	67	01
8	2005	협	48932	55	55	01
9	2006	리	36841	79	79	01
10	2006	나	00481			
11	2006	민	01478			
12	2006	리	85548			
13	2006	나	00548			
14	2006	협	52233	79	79	01
15	2006	흥	11147	77	77	01
16	2006	나	99467	85	85	01
17	2006	협	16579	67	67	01

<OLE 객체에 포함되어 있던 엑셀시트>

조치

- Step 1. 게시물을 비공개로 전환
- Step 2. 문서 내, “표” 더블 클릭 후, OLE 객체(엑셀시트)에 나타난 개인정보 삭제
- Step 3. 검색엔진에 저장된 페이지 삭제



머모표人

숨겨진 메모는 셀 모서리에
빨간색 표식이 있음

주민등록번호
760419-1

“메모”에
기록된
개인정보

숨겨진 메모는 셀 모서리에
빨간색 표식이 있음

주민등록번호
760419-1

“메모”에
기록된
개인정보

Step 1. 게시물을 비공개로 전환
Step 2. Sheet의 “메모표식” 확인 후 메모에 포함된 “개인정보” 삭제
Step 3. 검색엔진에 저장된 페이지 삭제

첨부 엑셀 파일에 노출 > 배경색과 글자색 동일



확인방법 : Sheet의 “셀 전체 선택” > 글자색을 검은색으로 바꿈



내용 없음

성명	성별	학과(전공)	연락처
손	남	영어영문	016
양	남	정치외교	011
김	여	사회환경시스템	011
조	여	교육공학	010
김	여	부동산	010
이	남	건축공학	010
이	여	행정	010
김	여	영어영문	010
모	여	국제무역	016
박	여	건축	010

<배경색과 동일하게 설정된 글자색>

배경색 전환

개인정보 발견

성명	성별	학과(전공)	연락처
손	남	영어영문	016
양	남	정치외교	011
김	여	사회환경시스템	011
조	여	교육공학	010
김	여	부동산	010
이	남	건축공학	010
이	여	행정	010
김	여	영어영문	010
모	여	국제무역	016
박	여	건축	010

< 글자색을 검은색으로 전환 >

조치

- Step 1. 게시물을 비공개로 전환
- Step 2. 글자색 변경 후 나타난 “개인정보” 삭제 또는 마스킹 처리
- Step 3. 검색엔진에 저장된 페이지 삭제



첨부된 한글 문서에 개인정보가 포함

이 력 서

성명	장 [redacted] (인)	주민등록번호	860902-[redacted]
생년월일	1986년 09월 02일생 (만 25세) 연락처: 010-7711-[redacted]		
주소	경기도 용인시 수지구 동천동 [redacted]		
호적관계	호주와의 관계	년	호주성명 장 [redacted]
년월일	학 력 및 경 력 사 항		
2005. 2	[redacted] 고등학교졸업		
2005. 13	[redacted] 학교 스포츠학과 재즈댄스전공 입학 졸업		

<개인정보가 포함된 한글문서>

게시물

2. 대표자: 김철우(070725-1-****)3: 영업소소재지

게시물 상세 내용

1. 업체명: (주)그린텔

2. 대표자: 김철우(090529-*)

3. 영업소재지: 경기도 수원시 오정구 삼정동 364 (전화: 032-234-1000)

4. 업종 및 등록번호: 수질오염 방지시설업 제57호

5. 등록번호: 자전번호

6. 등록주소일자: 2003년11월27일

2003년12월 2 일

경인지방환경청장

환경기술개발및지원제한법시행규칙 제32조의 규정에 의거 방치시설업 등록취소를 다음과 고합니다.

2003년12월 2 일

경인지방환경청장

1. 업체명: (주)성원인터내셔널

2. 대표자: 박영희(070630-*)

3. 영업소재지: 서울시 강남구 논현동 56 금곡빌딩 501호

4. 업종: 수질오염방지시설업

5. 등록번호: 제 893 호

6. 등록일자: 2003년11월27일

7. 전화번호: 02-514-8280

2003-31호

수로시설등록사항변경공고

환경기술개발및지원제한법 제33조의 규정에 의거 등록사항변경사항을 다음과 같이 공고합니다.

2003년12월 2 일

수로시설등록사항변경공고

수로시설업 제26호 및 같은법시행규칙 15조 규정

<개인정보를 배경색 처리한 한글문서>

조치

Step 1. 게시물을 비공개로 전환

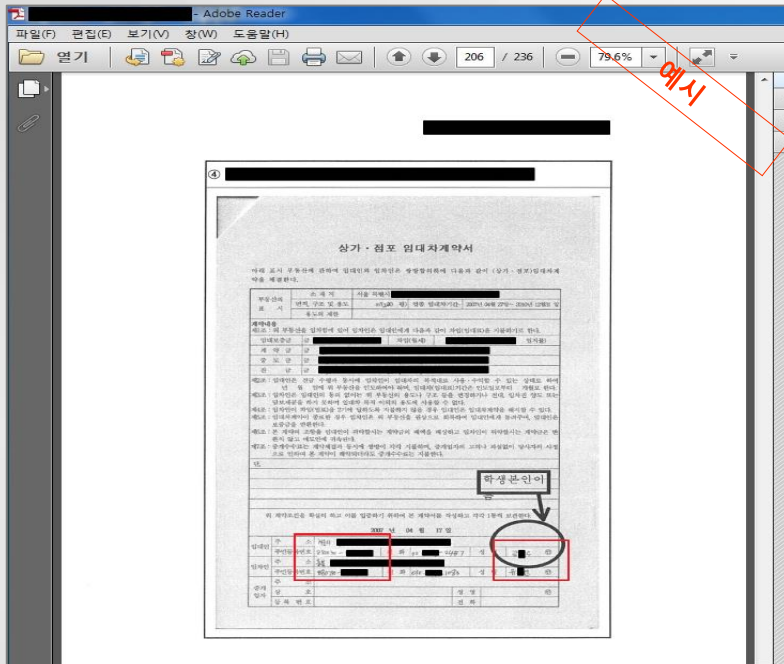
Step 2. 문서에 포함된 “개인정보” 삭제 또는 마스킹 처리

Step 3. 검색엔진에 저장된 페이지 삭제

첨부 이미지 파일에 노출



첨부된 이미지 파일(PDF, JPG 등)에 개인정보 포함



<개인정보가 포함된 PDF 이미지>



<개인정보가 포함된 이미지>

조치

Step 1. 게시물을 비공개로 전환

Step 2. 이미지 파일 삭제 또는 필요시 개인정보 부분을 마스킹 처리하고 업로드

Step 3. 검색엔진에 저장된 페이지 삭제

여행 상담, 자격증 재발급 요청 등을 하면서 개인정보 노출

Q&A

제 목	[] 재발급 요청
작성자	이 []

안녕하세요

[] 재발급을 요청드립니다.

발급연도는 20[]년 인지 20[]년 물중에 한 해이고,
 [] 대학교 [] 재학시에 학교에서 시험보고 났으며,
 주민등록번호는 820126-[] 이고,
 연락처는 010-9[]-7[]입니다.

<개인정보가 포함된 상담 글>

글쓰기 답글

리장 출 [] 착 기차표예매요~~ | 예약] 중국기차표예매

진시황 | 조회 89 | 추천 0 | 2017,02,27, 16:36

4월26일 [] 리장 22시50분출발
 4월27일 윤남 [] 09시 01분 도착
 폭신한 침대로 4명 예약문의 드립니다
 HWUNG []
 M038E[]
 KIM []
 M4629[]
 YUN []
 M855 []
 LIM []
 M325 []

<개인정보가 포함된 게시글>

조치

Step 1. 콘텐츠 내, “**개인정보**” 포함 확인

Step 3. 게시글에 포함된 “**개인정보**” 삭제 또는 마스킹 처리, 비공개 게시판으로 전환

Step 3. 검색엔진에 저장된 페이지 삭제



여행 상담, 자격증 재발급 요청 등을 하면서 개인정보 노출



또한 예약시, 영문성함, 나이, 성별, 여권번호, 전화번호, 이메일주소 등이 필요하므로 댓글로 달아주시면 확인 후 안내사항을 전달해드리도록 하겠습니다.

감사합니다.

할공 송 0 421 / 428-7 @hanmail.net

<개인정보가 포함된 상담 글>

<개인정보가 포함된 게시물>

조치

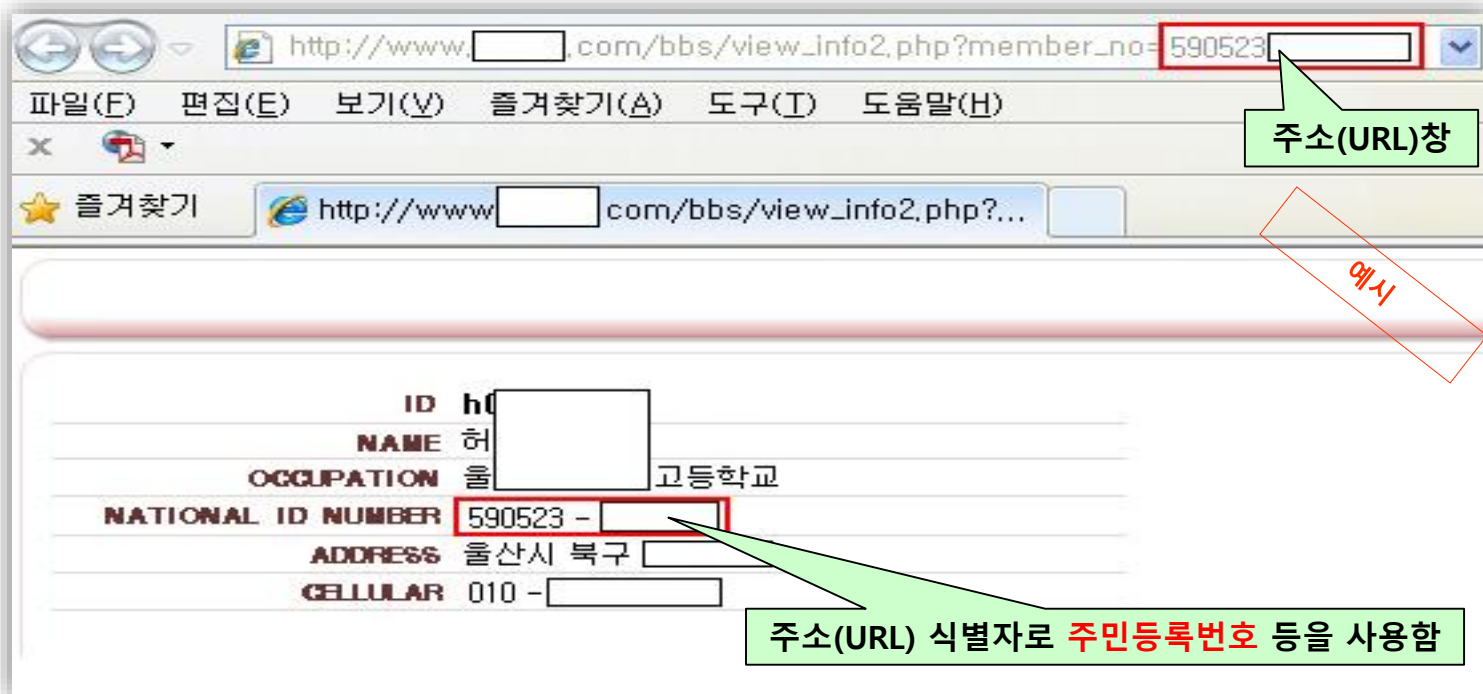
Step 1. 콘텐츠 내, “**개인정보**” 포함 확인

Step 3. 댓글에 포함된 “**개인정보**” 삭제 또는 마스킹 처리, 비공개 게시판으로 전환

Step 3. 검색엔진에 저장된 페이지 삭제



홈페이지 설계 오류로 URL에 개인정보 노출



조치

- ✓ Step 1. URL에 개인정보 노출여부 확인
- ✓ Step 2. 웹브라우저 주소URL(창)에 파라미터 값이 보이지 않도록 작성
URL에 개인을 구분할 수 있는 다른 값을 정의
- ✓ Step 3. 검색엔진에 저장된 페이지 삭제



- ✓ Step 1. 인터넷 브라우저에서 소스코드를 통해 개인정보가 있는지 확인
- ✓ Step 2. 불필요한 개인정보는 프로그램에서 삭제하고 꼭 필요한 정보는 암호화하거나 개인 식별용 구분자 변경
- ✓ Step 3. 검색엔진에 저장된 페이지 삭제



홈페이지 설계 오류로 임시 저장 페이지의 개인정보 노출

온라인상담

이름	김주
비밀번호	*****
이메일	
홈페이지	
제목	일본 여행 문의

<p>여권이 이제 나와서 여권번호랑 여행자보험 때문에 주민등록번호랑
올릴게요 ^^

처음 일본 여행이라 모르는게 많아 전화 자주 드리는데 항상 친절하게 답
변해주셔서 감사합니다 !!

김주

주민등록번호 791224-

여권번호 M8-

기간만료일 05 JAN 2020

☒ 글올리기 ☐ 취소

<p>여권이 이제 나와서 여권번호랑 여행자보험 때문에 주민등록번호랑
올릴게요 ^^

처음 일본 여행이라 모르는게 많아 전화 자주 드리는데 항상 친절하게 답
변해주셔서 감사합니다 !!

김주

주민등록번호 791224-

여권번호 M8-

기간만료일 05 JAN 2020

임시저장 페이지에 개인정보 노출

조치

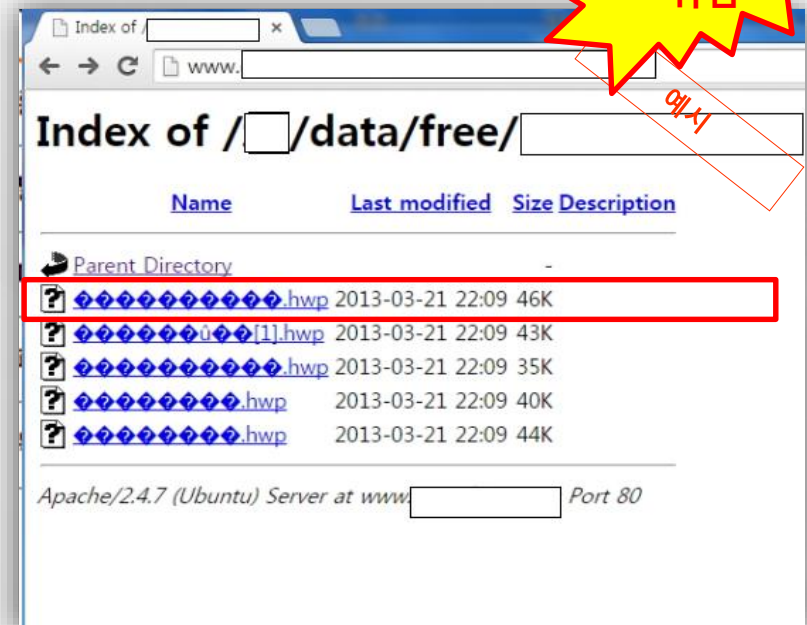
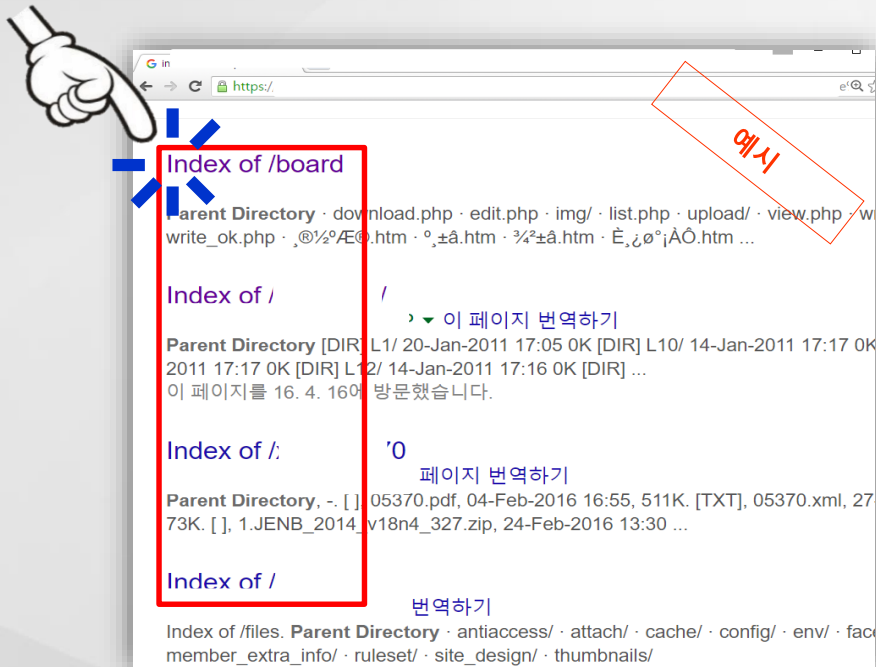
- ✓ Step 1. 인터넷 브라우저 “도구” 탭에서 “임시 저장 페이지” 삭제 조치
작성 완료 / 취소 시, 일정 시간 경과 시, 저장내용 삭제
- ✓ Step 2. 검색엔진에 저장된 페이지 삭제

디렉토리 리스팅 취약점으로 노출 (1)

홈페이지 설계 오류인 디렉터리 리스팅 취약점으로 인해 노출

- ➡ 서버관리자가 사이트 테스트 목적으로 사용하는 설정으로 브라우징하는 모든 디렉토리를 볼 수 있음
- ➡ 웹 서버의 URL로 “도메인 네임 + 디렉터리” 경로를 입력 했을 때, 웹 브라우저에 해당 디렉터리 내, 모든 파일 목록이 노출되는 보안 취약점

개인정보
대량 노출
위험

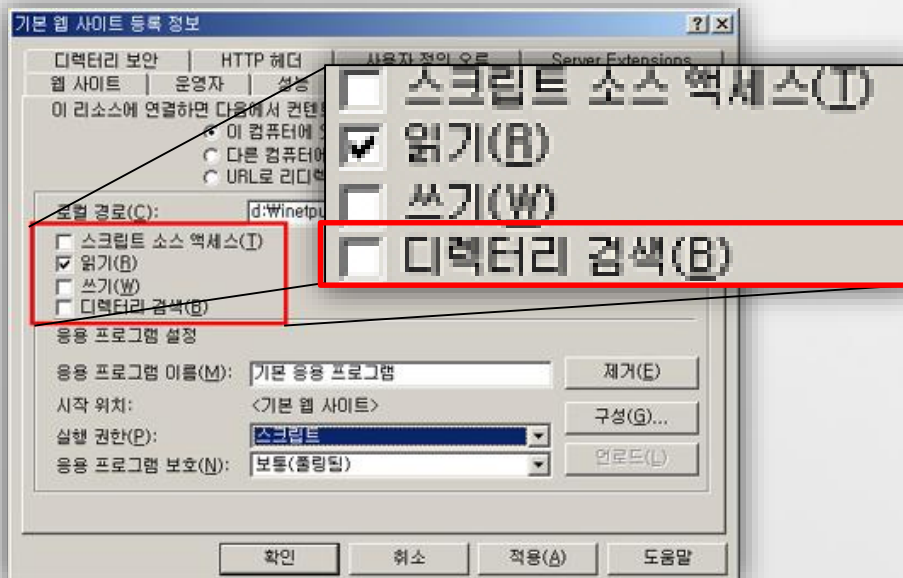


[디렉토리 리스팅 취약점이 있는 홈페이지 검색(예시)]

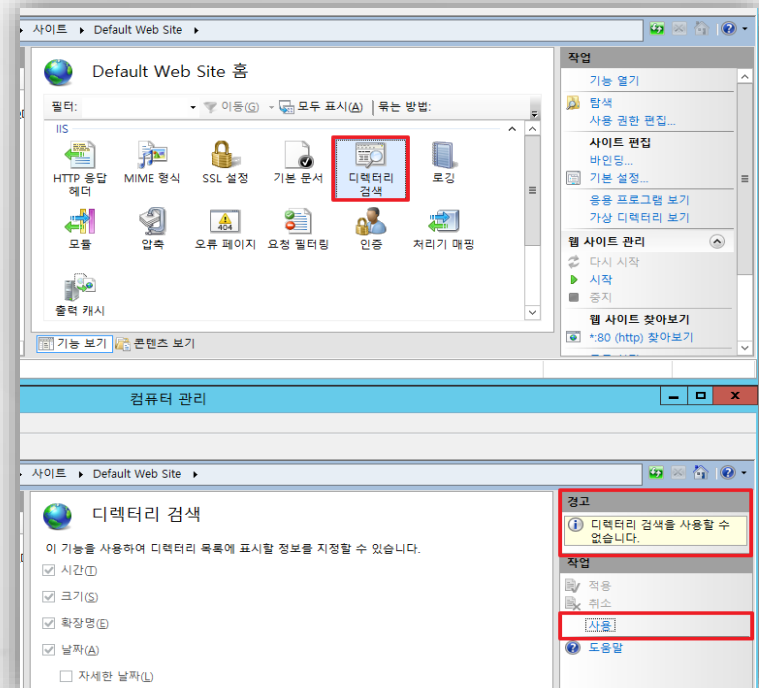
디렉토리 리스팅 취약점으로 노출 (2)

조치 디렉토리 리스팅 올바른 설정 : 윈도우 인터넷 정보서비스(IIS)

- 제어판 > 관리도구 > 인터넷 서비스 관리자 > 기본 웹사이트 속성 정보 수정
- ※ 디렉터리 검색 부분을 비활성화



[IIS 6.0 이하]



[IIS 7.0 이상]

디렉토리 리스팅 취약점으로 노출 (3)

조치 디렉토리 리스팅 올바른 설정 : UNIX / LINUX

- Apache 서버 : Indexes의 "문자열" 제거
- Tomcat 서버 : Param-value의 "False" 설정

The screenshot shows the Apache Tomcat 6.0 documentation page. On the left, the 'User Guide' section lists 14 items, with '5) Manager' highlighted by a red box. The main content area is divided into two sections: 'Apache' and 'Tomcat'. The 'Apache' section has a header 'httpd.conf 파일에서 indexes 문자열 제거' and shows a code snippet for the `<Directory>` block where the `Options` line has `Indexes` highlighted with a red box. A yellow starburst callout points to this with the text 'Indexes 문자열 제거'. The 'Tomcat' section has a header 'web.xml 파일에서 param-value false 설정' and shows a code snippet for the `<Init-param>` block where the `<param-value>` line has `false` highlighted with a red box. A yellow starburst callout points to this with the text 'Param-value False 설정'.

Apache Tomcat 6.0 - Docume... x +

Apache Tomcat

The Apache Software Foundation
http://www.apache.org/

Links

- Docs Home
- FAQ

User Guide

- 1) Introduction
- 2) Setup
- 3) First webapp
- 4) Deployer
- 5) Manager
- 6) Realms and AAA
- 7) Security Manager
- 8) JNDI Resources
- 9) JDBC DataSources
- 10) Classloading
- 11) JSPs
- 12) SSL
- 13) SSI
- 14) CGI

Apache

httpd.conf 파일에서 indexes 문자열 제거

```
<Directory "/user/local/serv
Options Indexes
</Directory>
```

Indexes 문자열 제거

Tomcat

web.xml 파일에서 param-value false 설정

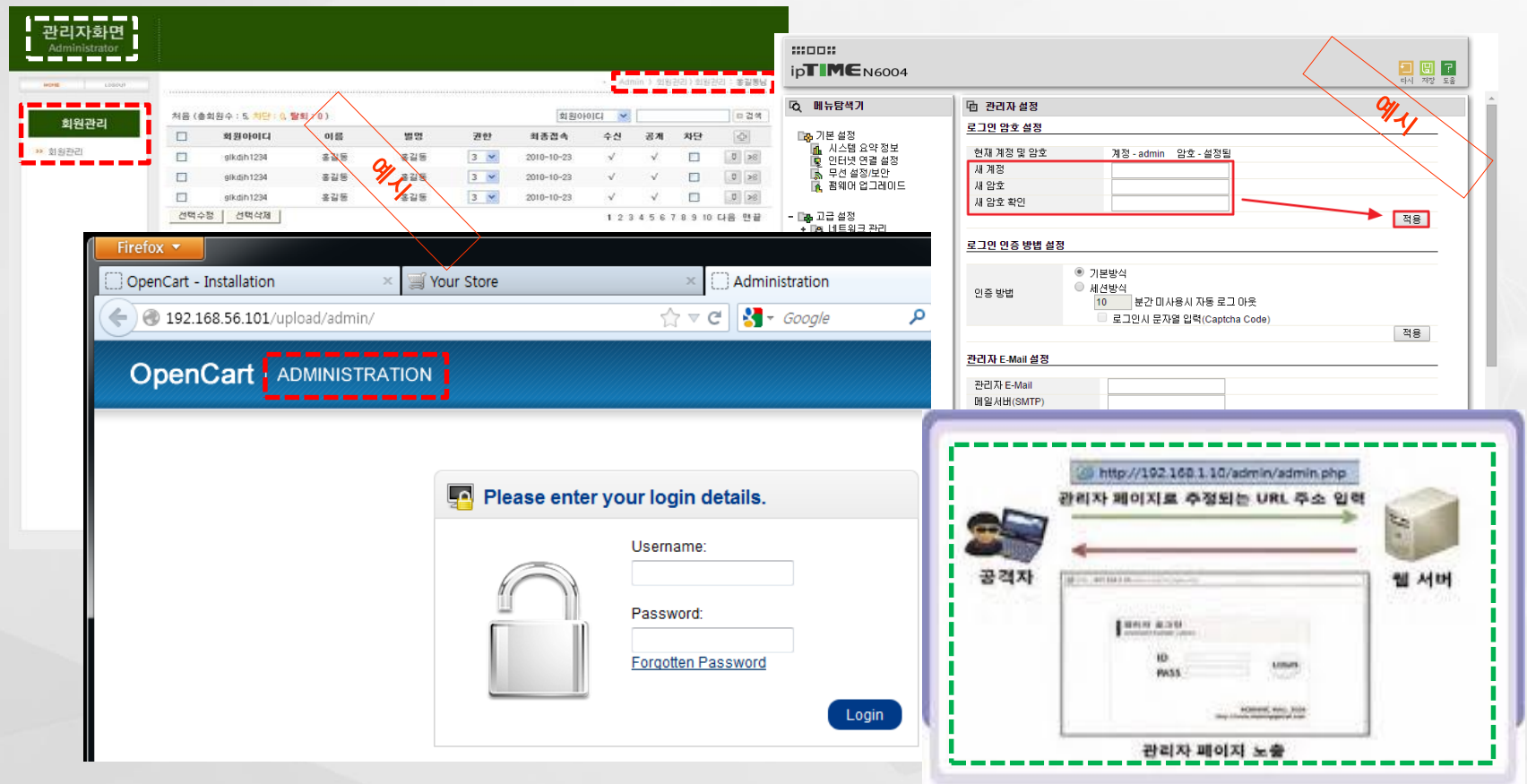
```
<Init-param>
  <param-name>listings</param-na
  <param-value>false</param-t
</Init-param>
```

Param-value False 설정

관리자 페이지 접근제한 미흡으로 노출 (1)

홈페이지 설계 및 관리 미흡 > 관리자 페이지 접근제한 미흡

➡ 관리자만 볼 수 있는 페이지가 인증 과정을 거치지 않고 방치되어 일반 이용자에게 노출되는 유형임

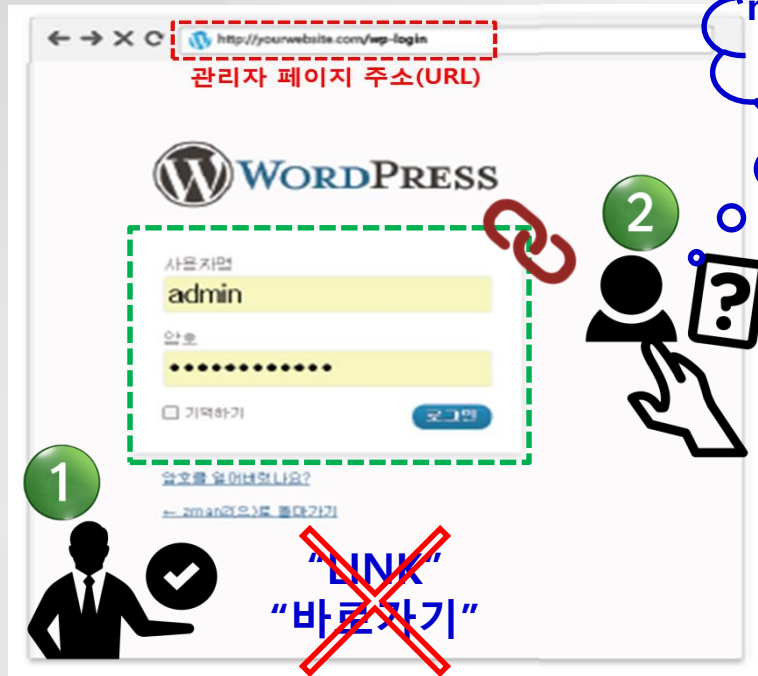


The composite image illustrates security vulnerabilities in the OpenCart administrator interface. It includes three main components:

- Top Left:** A screenshot of the OpenCart administrator interface. A red dashed box highlights the '회원관리' (Member Management) link in the sidebar. Another red dashed box highlights a table of users, with a red arrow pointing to it from the '예시' (Example) label.
- Top Right:** A screenshot of the '관리자 설정' (Administrator Settings) page. A red dashed box highlights the '로그인 암호 설정' (Login Password Settings) section, with a red arrow pointing to it from the '예시' (Example) label.
- Bottom Left:** A screenshot of the OpenCart administrator login page. A red dashed box highlights the 'ADMINISTRATION' link in the header.
- Bottom Right:** A diagram illustrating the unauthorized access process. It shows a '공격자' (Attacker) using a laptop to access the '관리자 페이지' (Administrator Page) via a URL. The URL is shown as 'http://192.168.1.10/admin/admin.php'. The diagram also shows a '웹 서버' (Web Server) and a '관리자 페이지 노출' (Administrator Page Exposure) status.

관리자 페이지 접근제한 미흡으로 노출 (2)

조치 올바른 관리자 페이지 설정

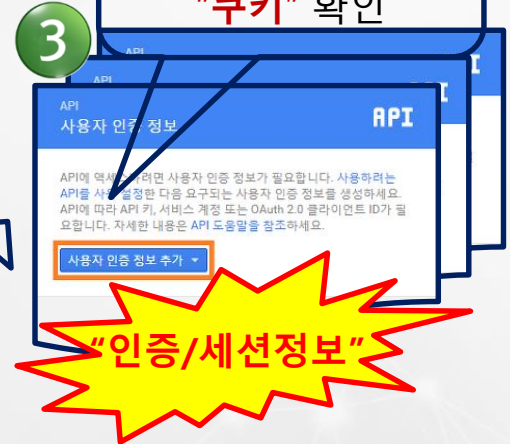


외부망 검색은
"VPN"이나 "전용망"
으로 조치



관리자 페이지는
내부망에서만 검색

작성된 웹페이지마다
관리자 "세션" 및
"쿠키" 확인



✓ Step 1. 올바른 관리자 페이지 설정

- 홈페이지의 각 페이지마다 "세션" 및 "쿠키" 확인 구문 입력
- 비인가자일 경우, 접속시마다 로그인 페이지로 리다이렉트 조치
- 관리자 페이지는 특정 IP 및 인가된 IP만 접근 가능토록 설정
- 관리자 페이지 주소는 추측하기 어려운 명칭으로 작성

✓ Step 2. 검색엔진에 저장된 페이지 삭제



검색엔진에 저장된 페이지 삭제 (1)

조치

- ✓ Step 1. 홈페이지에 노출된 개인정보 페이지를 삭제
- ✓ Step 2. 검색엔진에 홈페이지의 노출 개인정보 URL 또는 노출된 값을 입력하여 검색결과 값 확인
- ✓ Step 3. 검색결과 캐시페이지에 개인정보가 존재할 경우 해당 페이지 **삭제 요청**

구글(Google)에 노출된 개인정보정보 삭제 방법

1

사이트 추가 [삭제대상 사이트 추가]

관리하려는 사이트의 URL을 입력하세요.

www.example.com

계속 취소

2

Google Search Console

Google에 있는 http://www.example.com/ 2013년 5월 13일 15:53:56 GMT에 표시된 페이지와 소문장입니다.

다음 검색어가 강조 표시되어 있습니다: 750020

알고 싶어요

알고 싶어요

공개

이의신청서 인접사항 이름: [] 주민등록번호: 750020-1 [] 차량번호: 1321 [] 등록시간: 2013-03-22, 13:32 위반장소: [] 단속공무원: [] (02-7-) 위반사항: 우측 1개 항목 이상 이의신청 사유: 현재 중대 주안으로써 누구보다도 주위 교통정황을 잘 알고 있으며 단지 내 상가시설 주자가 교통의 흐름이 원활하기 위해 [] 부대차 [] 차량 또한 교통정황의 흐름에 방해가 되지 않기에 13시에 주차 하였으나, 13:32분에 주 정차 위반으로 과태료 부과를 받게 되었습니다. 그러나 []에서 [] 전역 11시~14시까지 교통정황의 흐름에 방해가 되지 않는 한 단속 대상에서 제외한다고 발표한 바 이의를 제기합니다. 당시 교통정황 확인을 하 여 삼엄해 주시길 바랍니다.

3

Google Search Console

http://www.example.com/의 소유권 확인 자세히 알아보기

권장 방법 대체 방법

권장 방법: HTML 파일 업로드

사이트에 HTML 파일 업로드

1. 이 HTML 확인 파일을 다운로드합니다. [google03beeeefb1a62eb.html]

2. http://www.example.com/에 인증 파일을 업로드합니다.

3. 브라우저에서 http://www.example.com/google03beeeefb1a62eb.html 을(를) 방문하여 업로드에 성공했는지 확인합니다.

4. 아래에서 '확인'을 클릭하세요.

확인된 상태를 유지하려면 확인이 완료된 후에도 HTML 파일을 삭제하지 마시기 바랍니다.

확인 다음에

4

Google Search Console

[사이트 추가 완료]

사이트 추가

사이트 관리

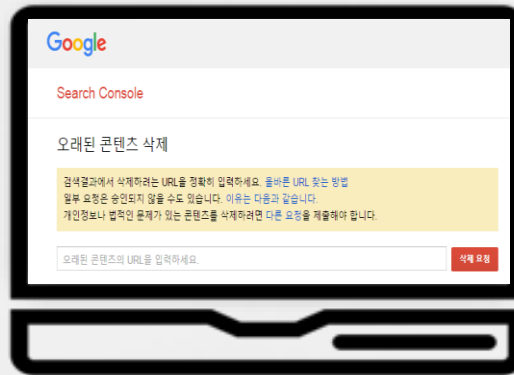
kisatest bl ee

새 메시지나 최근에 발생한 중요한 문제가 없습니다.

검색엔진에 저장된 페이지 삭제 (2)

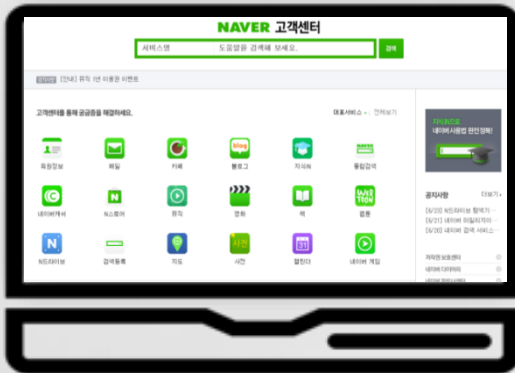


검색엔진 별 캐시페이지 삭제 요청 주소



네~
삭제하겠습니다.

<https://www.google.com/webmasters/tools/removals>



<https://help.naver.com/support/home.nhn>



고객센터(CS)



<https://cs.daum.net/redbell/top.html>

Ⅲ. 개인정보 노출 예방





첨부파일 업로드 前, 개인정보 **확인**하라 !



관리자 페이지 외부 노출은 **치명적**임을 인식하라 !!



홈페이지의 개인정보 노출여부를 **주기적**으로 점검하라 !!!



홈페이지 **비공개** 게시판을 운영하라 !!!!



개인정보 **노출** 주의 **안내문**을 게시하라 !!!!!



개인정보 노출예방 **기술** 지원을 **이용**하라 !!!!!!





첨부파일 업로드 前, 개인정보 확인하라 !!

- ☞ 업무상 **불필요한 내용은 삭제**.. 필요한 최소한의 정보만 게시
- ☞ 부득이 개인정보 게시할 경우에는 **마스킹(****)** 처리
- ☞ 엑셀 등 숨겨진 기능을 통해 개인정보가 숨겨져 있는지 확인
- ☞ 개인정보 검색 제품이 설치된 사용자 PC는 **개인정보 포함** 여부 점검 후, 게시

파일	홈	삽입	페이지 레이아웃	수식	데이터	검토	보기
자격증 합격자 관리대장							
필요한 항목(1)	필요한 항목(2)	필요한 항목(3)	필요한 항목(4)				
연도	수험번호	성명	주민등록번호	연락처	주소	자격증명	합격여부
2015	20107894002	홍*동	850101-2	010-4841	서울시	정보처리기사	합격
2015	20107894011	박*곤	900607-1	010-6325	서울시	정보처리기사	불합격
2015	20097894041	유*하	911152-1	010-9135	인천시	정보처리기사	합격
2015	20117894029	고*동	880206-2	010-3157	경기도	정보처리기사	합격
2014	20107894020	백*생	851122-1	010-2265	강원도	정보처리기사	불합격
2014	20127894009	김*자	901021-1	010-1212	경상남도	정보처리기사	합격
2014	20087894100	유*섬	830111-1	010-9696	전라남도	정보처리기사	불합격
2014	20057894071	호*이	881010-2	010-6391	서울시	정보처리기사	합격
2015	20107894002	홍*동	850101-2	010-4841	서울시	정보처리기사	합격
2015	20107894011	박*곤	900607-1	010-6325	서울시	정보처리기사	불합격

새 파일 작성

파일	홈	삽입	페이지 레이아웃	수식	데이터	검토	보기
자격증 응시자 명부							
필요한 내용만 게시 마스킹 처리							
수험번호	성명	자격증명	합격여부				
20107894002	홍*동	정보처리기사	합격				
20107894011	박*곤	정보처리기사	불합격				
20097894041	유*하	정보처리기사	합격				
20117894029	고*동	정보처리기사	합격				
20107894020	백*생	정보처리기사	불합격				
20127894009	김*자	정보처리기사	합격				
20087894100	유*섬	정보처리기사	불합격				
20057894071	호*이	정보처리기사	합격				
20107894002	홍*동	정보처리기사	합격				
20107894011	박*곤	정보처리기사	불합격				



관리자 페이지 외부 노출은 **치명적**임을 인식하라!!

- ➡ **접근제한** (특정 IP, 전용선 또는 가상사설망(VPN) 이용하여 접근 권한 관리)
비인가자일 경우 접속시 마다 로그인페이지로 리다이렉트 조치
- ➡ 홈페이지 각 페이지 마다 “세션” 확인 구문 입력
- ➡ 관리자 페이지를 추측하기 어려운 명칭으로 수정 (개발업체에 **반드시** 확인)
※ **사용금지** : 도메인/admin, admin.도메인 등





홈페이지의 개인정보 노출여부를 주기적으로 **점검**하라 !!

☞ 웹사이트 **변경(통합, 개선 등)시 점검**

- 웹 취약점 진단 및 시큐어 코딩 준수여부 점검
- 회원 식별자를 개인정보로 사용하고 있는지 점검
- 암호화 대상인 개인정보의 암호화 여부를 점검
- 변경된 웹사이트는 외부에 공개하기 전, 반드시 **개인정보** 포함 여부 점검

☞ 주기적으로 외부 검색엔진에 개인정보가 수집되는지 점검

- 검색엔진 고급검색 기능을 이용하여 **개인정보를 주기적으로 점검**
※ 검색단어(예) : 번호, 주민, 전화, 여권 등으로 검색
- 디렉터리 **리스팅** 여부 점검



홈페이지 비공개 게시판을 운영하라 !!!!

- ☞ 일반 공개 게시판과 **1:1상담** 게시판을 분리하여 운영
 - 공개 게시판은 담당자가 관리하고 누구나 읽을 수 있도록 공개하여 운영
 - 1:1 상담 게시판은 **작성자**와 **담당자**만 읽을 수 있도록 **비공개** 운영
- ☞ 개인정보가 포함된 경우, 즉시 삭제할 수 없을 때는 “**비공개**”로 전환

1255	기타	🔒 문의드립니다.	김**	2016/01/02	3	답변완료
1254	기타	🔒 상담요청	이**	2016/01/02	3	답변완료
1253	기타	🔒 기타 문의	박**	2016/01/02	2	답변완료
1252	문의	🔒 문의요	김**	2016/01/02	8	답변완료
1251	기타	🔒 문의드립니다.	홍**	2016/01/02	3	답변완료
1250	기타	🔒 상담요청합니다.	김**	2016/01/02	8	답변완료





개인정보 노출 주의 안내문을 게시하라 !!!!!

☞ 개인정보 노출예방에 대한 안내를 받을 수 있도록 안내글이나 팝업창 제공

※ 개인정보 게시에 대한 주의안내

게시글 작성시 개인정보가 노출될 수 있으니, 글게시 전에 불필요한 개인정보가 있는지 반드시 확인하세요

행정 처분 공개

행정처분번호			
업종명		안허가번호	
업소명		대표자명	
소재지	<input type="checkbox"/> 도로명 : <input type="checkbox"/> 지번명 : 서울특별시		
행정처분	<input type="checkbox"/> 처분사항 : 등록취소 <input type="checkbox"/> 처분확정일자 : <input type="checkbox"/> 처분기간 : ~ <input type="checkbox"/> 안내사항 :		
위반내용(1)차	<input type="checkbox"/> 위반일자 : <input type="checkbox"/> 위반사항 : <input type="checkbox"/> 법적근거 : <input type="checkbox"/> 위반사유 : <input type="checkbox"/> 위반장소 :		
처리부서	<input type="text"/> 과	담당자	
전화번호	<input type="text"/>	이메일	

예시

목록



개인정보 노출 기술지원 Help Desk를 이용하라 !!!!!

Help Desk 정보



02-405-4844

✓ 유선 및 메일을 통한 상담 지원



privacycheck@onlinecheck.kr

✓ AM 9:00 ~ PM 18:00 (평일)

지 원 분 야

기술 지원

- ✓ 노출 원인분석 및 조치방안 지원(관련 문서 제공 등)
 - 홈페이지 설계오류 확인 및 조치 방법
 - 올바른 관리자 페이지 구성방법 등
- ✓ 웹 취약점 점검
- ✓ 웹 보안도구(악성코드 탐지, 웹 방화벽 설치) 배포
- ✓ 정보보호 컨설팅 및 교육 · 세미나 실시

법률 상담

- ✓ 개인정보보호법 관련 법률 상담
- ✓ 개인정보보호법 준수사항 컨설팅

기타 지원

- ✓ 개인정보 노출방지 가이드라인 배포
- ✓ 지역 정보보호지원센터 등 유관기관 안내
 - 인천, 경기, 청주, 대구, 광주, 부산



No	자 료 명	출 처	다운로드 위치
1	홈페이지 개인정보 노출방지 안내서 (2016.06)	행정자치부 KISA	개인정보 종합포털 > 자료마당
2	홈페이지 개발 보안 안내서 (2010.01)	방송통신위원회 KISA	KISA > 자료실 > 기술안내서가이드
3	전자정부 SW개발·운영자를 위한 소프트웨어 개발보안 가이드 (2017.01)	행정자치부 KISA	KISA > 자료실 > 기술안내서가이드
4	개인정보보호 법령 및 지침·고시 해설 (2016.12)	행정자치부	개인정보 종합포털 > 자료마당
5	전자정부 개발·운영자를 위한 JAVA 시큐어코딩 가이드 (2012.09)	행정자치부	KISA > 자료실 > 기술안내서가이드
6	전자정부 개발·운영자를 위한 C 시큐어코딩 가이드 (2012.09)	행정자치부	KISA > 자료실 > 기술안내서가이드
7	개인정보의 안전성 확보조치 기준 해설서 (2017.01)	행정자치부 KISA	개인정보 종합포털 > 자료마당
8	개인정보의 암호화 조치 안내서 (2017.01)	행정자치부 KISA	개인정보 종합포털 > 자료마당

Q & A

Internet On, Security In!

Thank you

- 개인정보보호 종합포털 : www.privacy.go.kr
- e프라이버시 클린서비스 : www.eprivacy.go.kr
- 개인정보침해신고센터 : (국번없이) 118
(홈페이지) privacy.kisa.or.kr

