공공기관 홈페이지 개인정보 노출방지 가이드라인(2009년 개정판)

2009. 2.

행정안전부

본 “공공기관 홈페이지 개인정보 노출방지 가이드라인(2009년 개정판)”은 2008년 2월에 행정자치부에서 기배포한 “공공기관 웹사이트 개인정보 노출방지 가이드라인(개정판)”에 아래의 사항이 추가되었습니다.

◈ 인증우회 자가진단 방법(26페이지)

◈ 개인정보 노출 방지대책(39~42페이지)

본 가이드라인이 각 기관의 웹사이트 개인정보 노출 방지에 좋은 길잡이가 되길 바랍니다.

목 차

Ⅰ 개요

1. 개인정보 노출이란 무엇인가요?

홈페이지를 통한 **개인정보 노출이란,**
일반 인터넷 이용자가 해킹 등 특별한 방법을 이용하지 않고 정상적으로 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 방치되어 있는 것을 말합니다.

2. 개인정보 노출이 왜 문제가 되나요?

홈페이지에 개인정보가 노출되는 경우,
악의적인 목적을 가진 사람이 노출된 개인정보를 이용하여 스팸 발송 등으로 프라이버시를 침해할 수 있을 뿐 아니라, **명의도용 등을 통해 경제적인 손실을 가져올 수 있습니다.** 더구나 정상적인 인터넷 이용만으로 개인정보를 쉽게 취득할 수 있어 개인정보 침해사고의 발생 가능성이 매우 높습니다.

3. 침해사고 위험이 높은 개인정보는 어떤 것인가요?

유출 시 침해사고 위험이 높은 개인정보로는
주민등록번호, 신용카드번호, 은행계좌번호, 법인등록번호, 핸드폰번호, 이메일주소 등이 있습니다. 특히 **주민등록번호는 개인을 식별할 수 있는 절대적인 개인정보로써 개인의 경제적인 피해를 줄 수 있는 가장 중요한 개인정보**입니다.

4. 개인정보 노출을 방지하기 위해서는 어디를 관리해야 하나요?

홈페이지의 어느 위치에서든지 개인정보는 노출되어 이용자들에게 쉽게 전달될 수 있습니다.

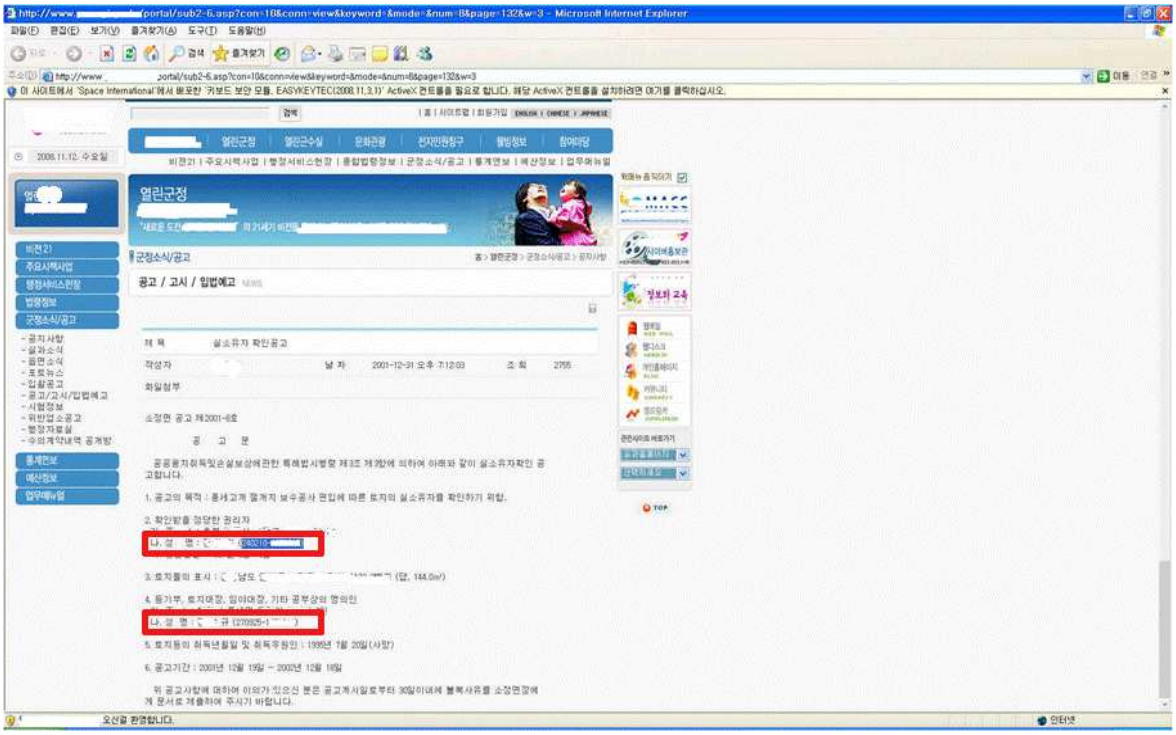
즉, 일반 웹페이지에서부터 게시판, 첨부파일, 각 페이지가 공개하고 있는 소스코드 등은 일반 이용자들의 간편한 클릭으로 개인정보를 노출할 수 있으므로 이를 방지하기 위한 지속적인 관리가 필요합니다.

뿐만 아니라, 홈페이지의 모든 콘텐츠들은 언제든지 구글과 같은 외부 검색엔진에 의해 수집되어 정보가 저장될 수 있으므로 **관리자는 외부 검색엔진으로 관리하는 홈페이지의 개인정보가 유출되지 않도록 지속적으로 확인하고 관리하여야 합니다.**

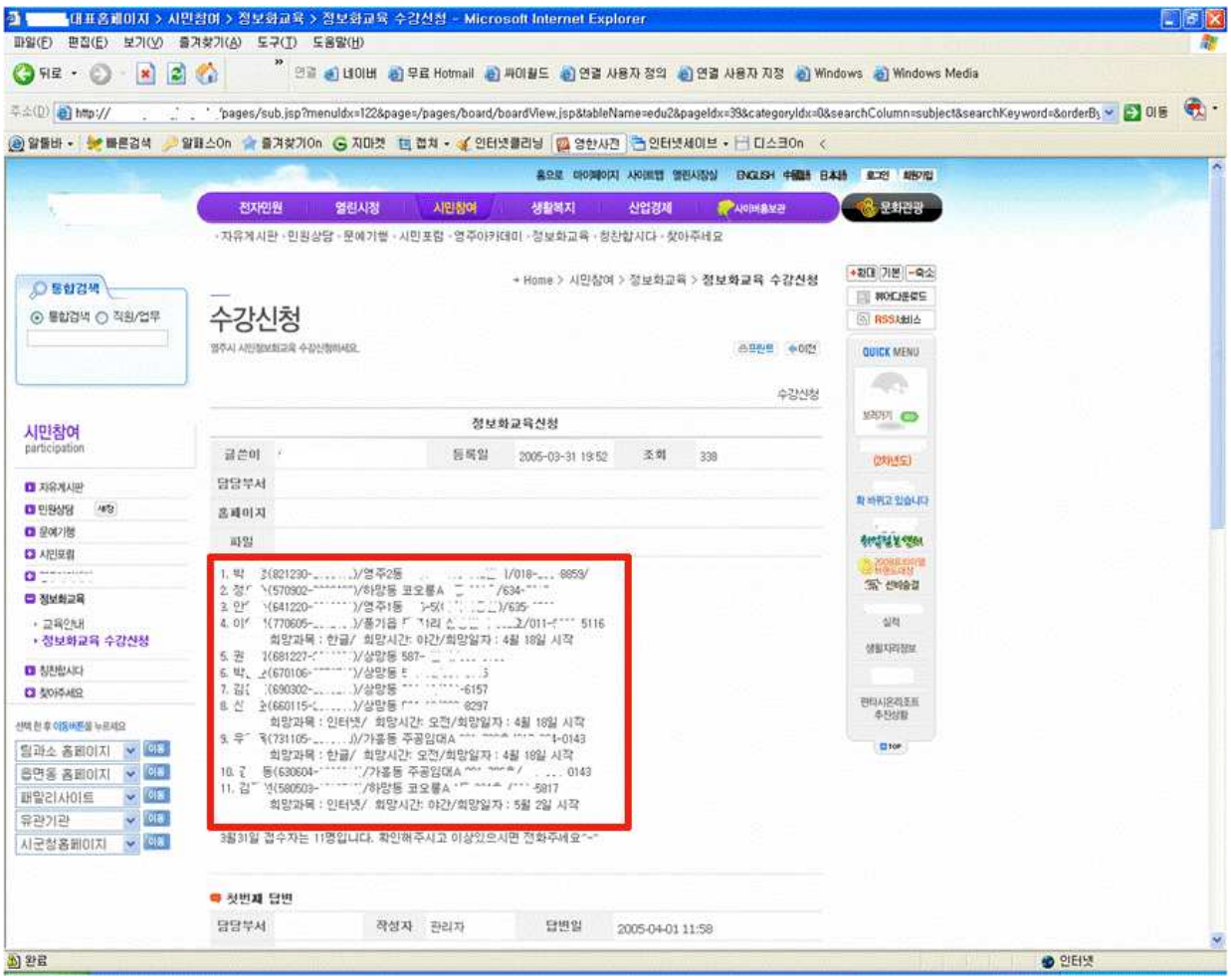
Ⅱ 개인정보 노출유형 및 조치방법

홈페이지에서 개인정보 노출은 웹페이지, 첨부파일, 소스코드, 외부 검색엔진(구글 등) 등 4가지 형태로 발생합니다. 또한 각 형태별로는 다양한 유형의 개인정보 노출이 발생할 수 있습니다. 따라서 개인정보 노출관리자는 관리하는 홈페이지에서 발생할 수 있는 모든 유형의 개인정보 노출에 대해서 점검하여야 합니다. 개인정보 노출 유형과 각각의 조치사항을 설명하면 다음과 같습니다.

1. 웹페이지 노출 유형

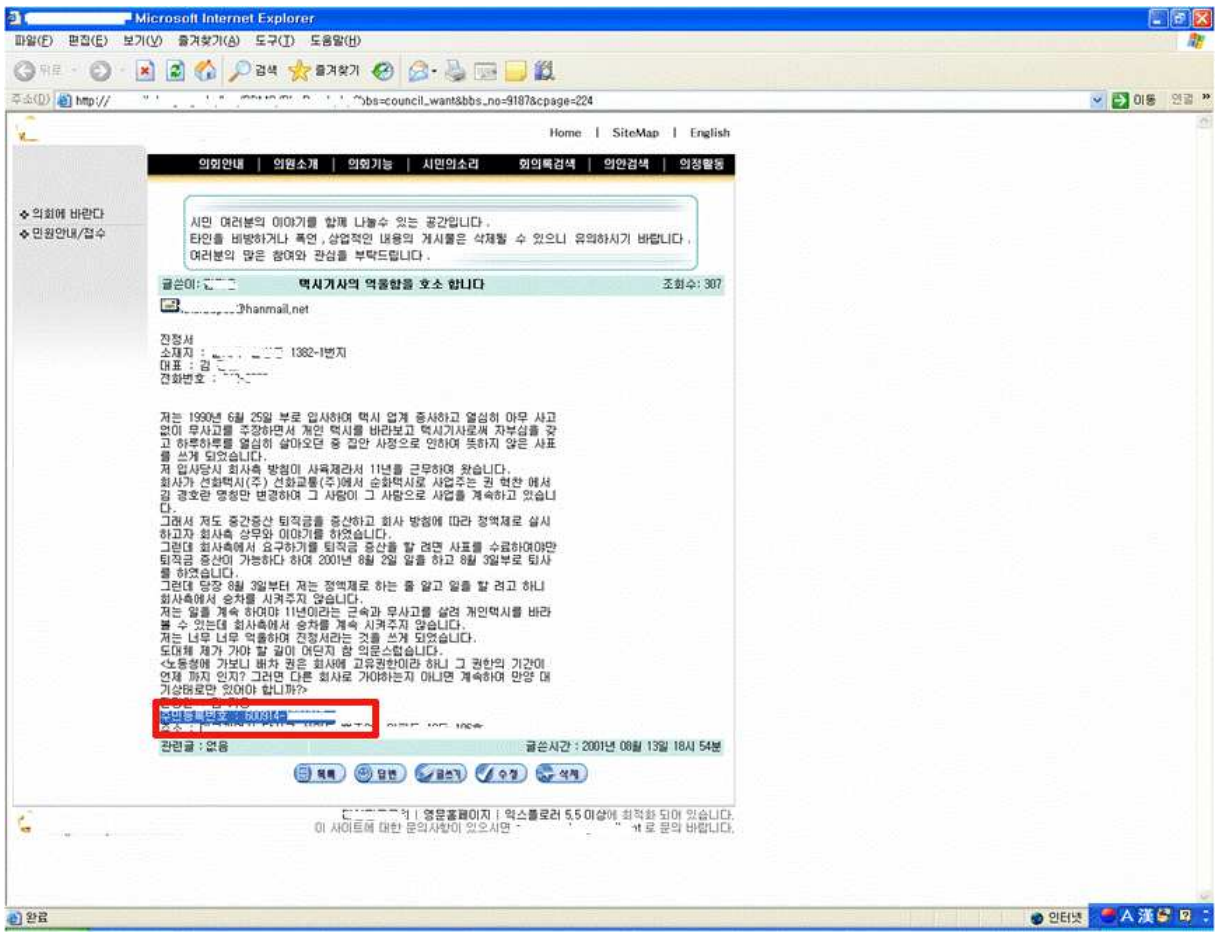
공지사항에 개인정보가 포함된 경우	
	
유형설명	해당 게시물 담당자의 부주의에 의해 개인정보가 포함된 콘텐츠를 그대로 공지한 경우입니다.
조치사항	이러한 유형의 노출이 발견되면, 관리자는 해당 페이지를 즉시 삭제하거나 해당 개인정보 일부를 * 처리 하는 등의 조치를 취해야 합니다.

민원인이 게재한 글에 개인정보가 포함된 경우



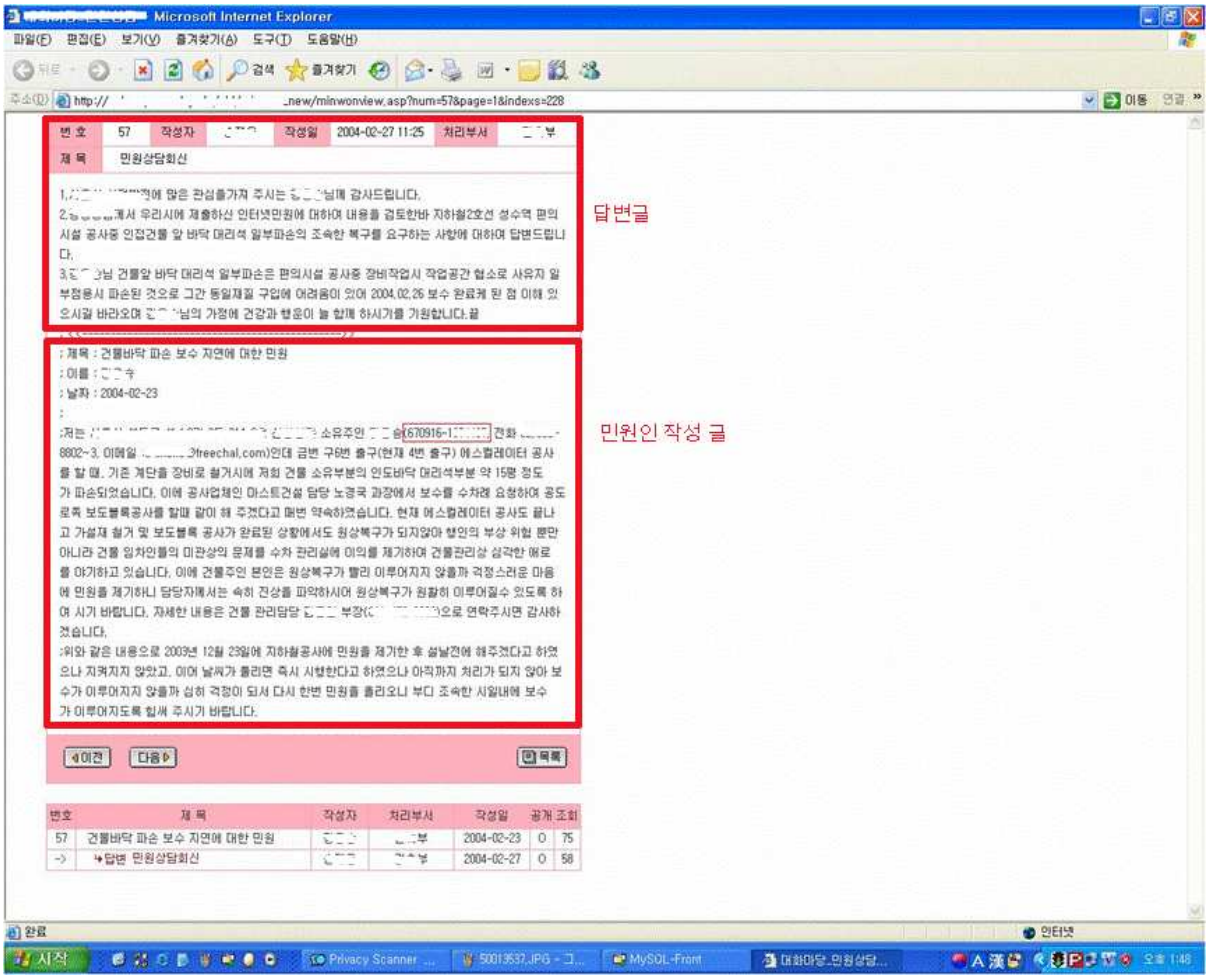
유형설명	해당 민원인의 부주의 또는 신속한 민원처리를 위해 의도적으로 개인정보가 포함된 콘텐츠를 그대로 게재한 경우입니다.
조치사항	이러한 유형의 노출이 발견되면, 관리자는 민원인의 동의를 거쳐 해당 페이지를 즉시 삭제하거나 해당 개인정보 일부를 * 처리 하는 등의 조치를 취해야 합니다.

휴면사이트에 개인정보가 노출되어 있는 경우



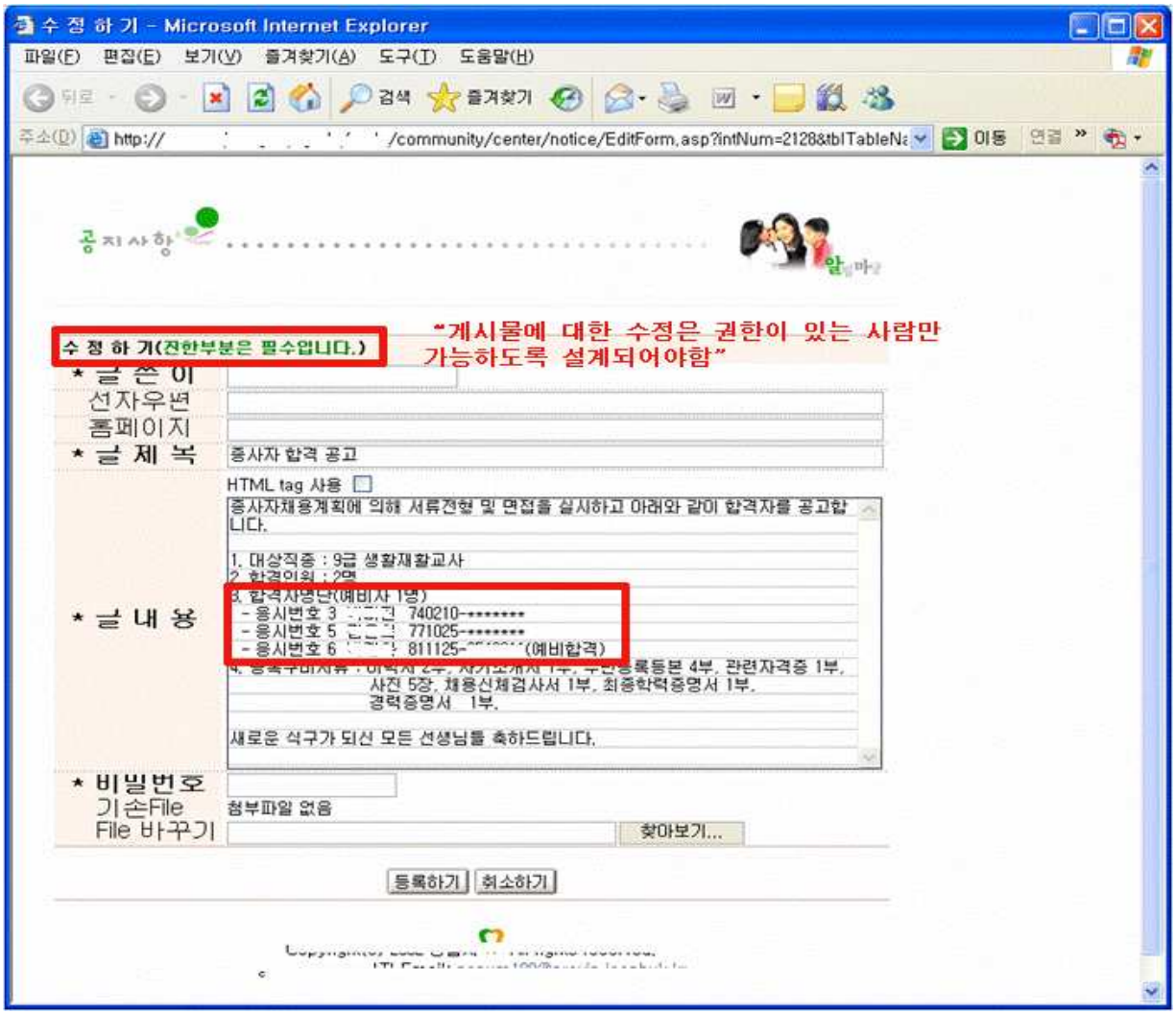
유형설명	현재 운영 중인 홈페이지는 아니지만, 예전에 운영 중인 정보가 웹 서버에 남아서 해당 웹페이지 주소를 알면 해당 게시물을 확인하여 개인정보를 얻을 수 있는 경우입니다. 이 유형은 관리자가 인지하지 못하는 범위에서 발생하는 개인정보 노출이므로 노출이 장기간 방치될 수 있는 위험이 있습니다. 특히 구글과 같은 외부 검색엔진들은 이전에 수집했던 웹페이지 주소정보를 저장하고 있으므로 이 주소정보를 이용하여 지속적으로 개인정보 노출사고를 발생시킬 수 있습니다.
조치사항	이러한 유형의 노출이 발견되면, 관리자는 관리하는 웹서버 내에 잔존하는 휴면 홈페이지를 모두 삭제하거나 휴면 홈페이지의 개인정보 노출여부를 일제히 점검하여 삭제처리하는 등의 관리를 하여야 합니다.

답글에 개인정보가 포함된 경우



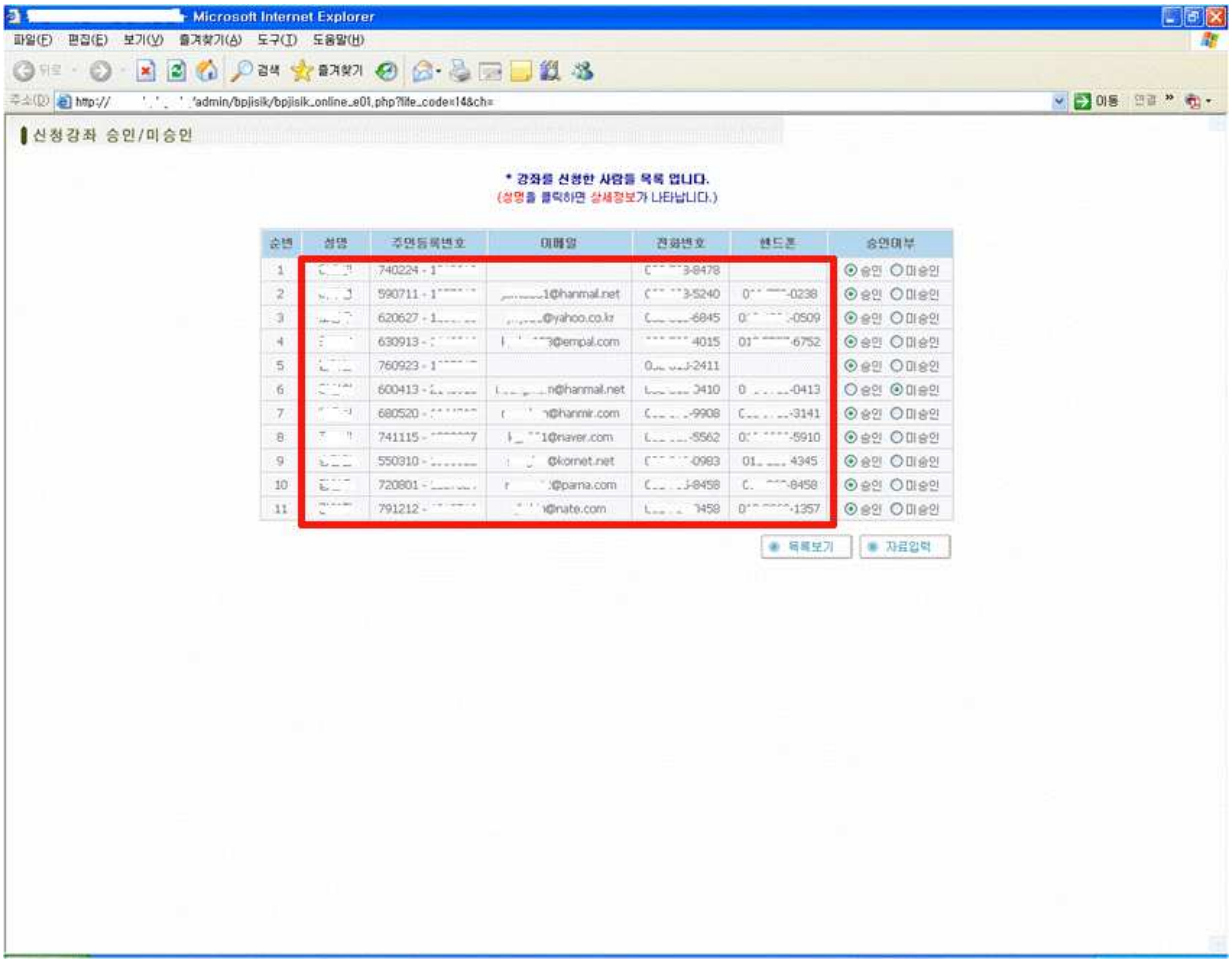
유형설명	해당 민원인의 부주의 또는 신속한 민원처리를 위해 의도적으로 개인정보가 포함된 콘텐츠에 담당자가 답변을 하는 과정에서 초기작성 민원사항에 포함된 개인정보가 그대로 노출된 경우입니다.
조치사항	이러한 유형의 노출이 발견되면, 관리자는 담당자가 해당 페이지에 포함된 개인정보를 즉시 삭제하여 다시 올리도록 해야 합니다.

입력/수정 화면에 개인정보가 포함된 경우



유형설명	게시물을 수정/편집하는 화면을 접근권한이 없는 이용자가 열람할 수 있도록 홈페이지를 설계하여 발생한 개인정보 노출 유형입니다. 원래 홈페이지에서 게시물을 수정/편집하는 화면은 해당 게시자나 홈페이지 관리자 등 접근권한을 가진 이용자만이 접근할 수 있도록 보안기능을 고려하여 설계하여야 합니다. 그러나 각 페이지별로 접근권한 및 인증 등의 절차가 제대로 구현되지 않으면 이와 같이 노출이 발생할 수 있습니다.
조치사항	이러한 유형의 노출이 발견되면, 웹페이지에 대한 보안기능이 어떻게 설계 되었는지를 파악하여 각 웹페이지별로 접근권한에 따른 인증절차를 준수하도록 수정하여야 합니다.

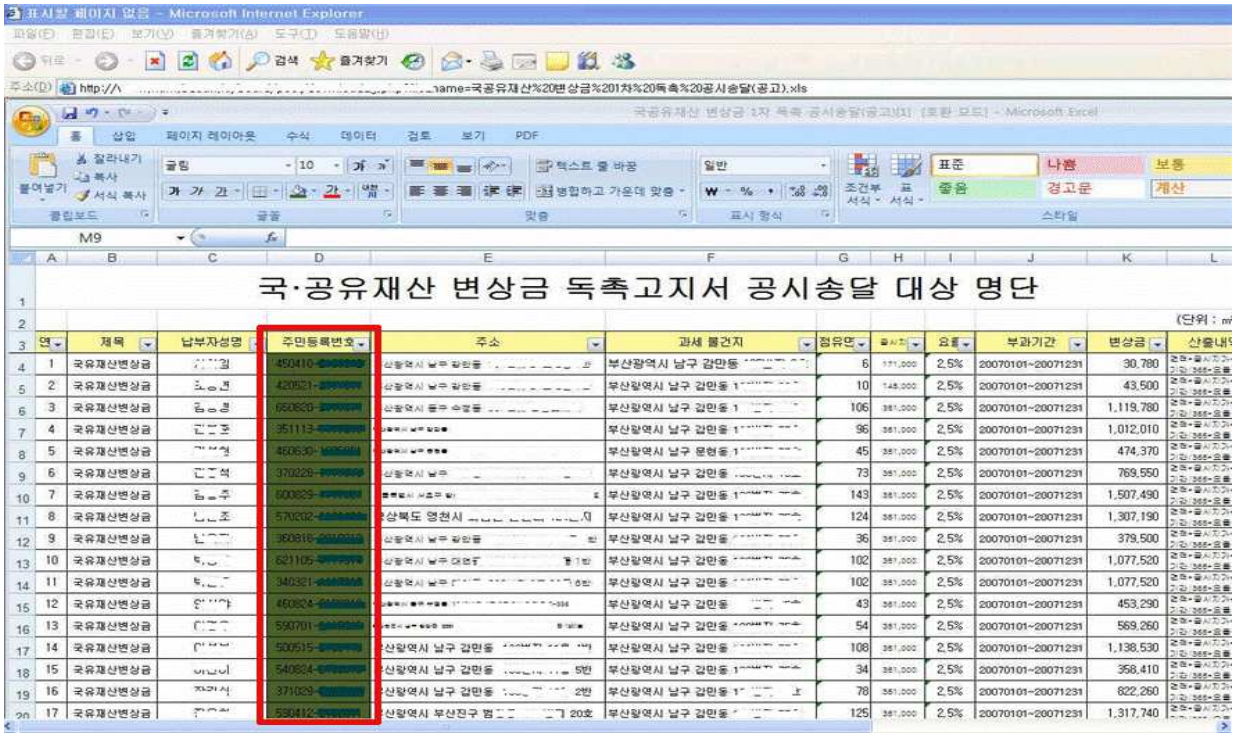
접근제한 페이지에 개인정보가 포함된 경우



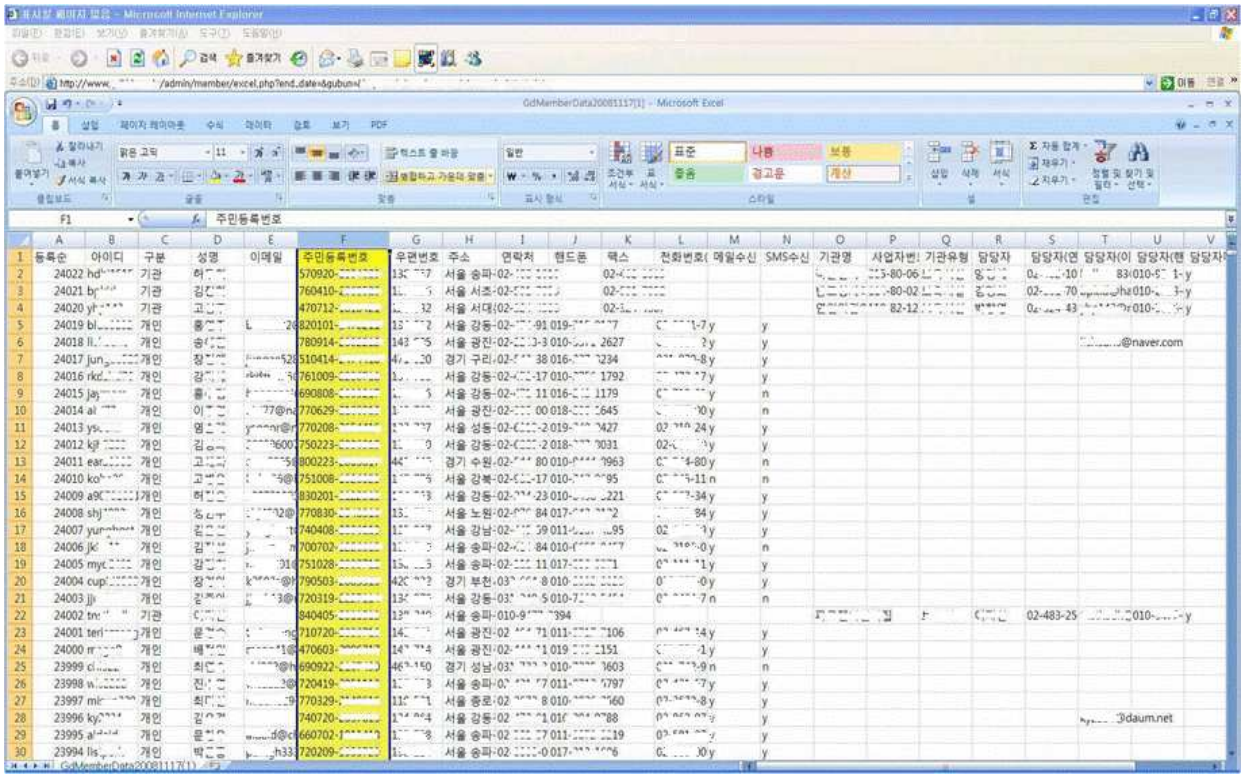
유형설명	접근권한을 가진 이용자만 접근할 수 있는 웹페이지를 접근권한이 없는 이용자가 접속할 수 있도록 홈페이지를 설계하여 발생한 개인정보 노출 유형입니다. 원래 접근제한 웹페이지는 접근권한을 가진 이용자만이 접근할 수 있도록 설계하여야 합니다. 그러나 이러한 접근권한 및 인증 등의 절차가 제대로 구현되지 않으면 이와 같이 노출이 발생할 수 있습니다.
조치사항	이러한 유형의 노출이 발견되면, 홈페이지의 접근권한 관련 보안기능이 어떻게 설계 되었는지를 파악하여 각 웹페이지별로 접근권한에 따른 정확한 인증절차를 준수하도록 수정하여야 합니다.

2. 첨부파일 노출 유형

홈페이지의 게시판에는 엑셀, 혼글, 파워포인트, PDF, ZIP 등의 첨부파일이 존재할 수 있으며, 이 파일들에서 개인정보가 노출될 수 있으므로 이에 대한 점검 및 조치가 필요합니다. 첨부파일에서 발생하는 개인정보 노출 유형과 조치 사항은 다음과 같습니다.

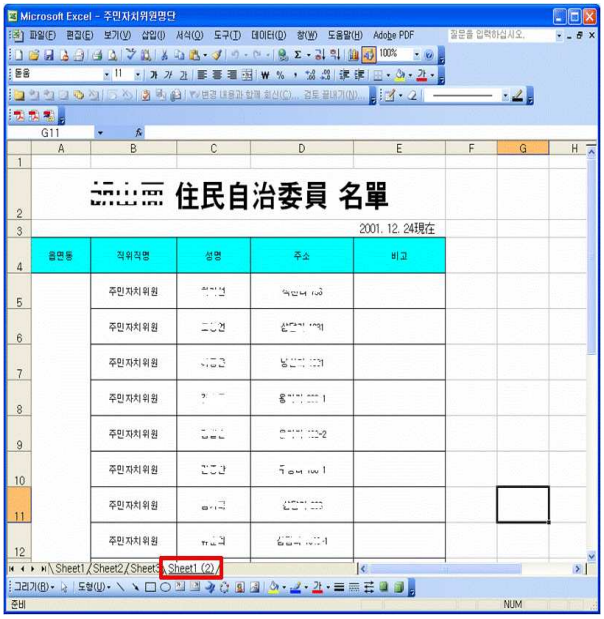
<table>
<tr><th colspan="2">일반적인 경우</th></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td>유형설명</td><td>공공기관 홈페이지의 게시판에는 엑셀, 혼글, 파워포인트, PDF, ZIP 등의 첨부파일이 있으며, 게시판에 있는 첨부파일에 개인정보가 포함되어 발생한 개인정보 노출 유형입니다.
특히 가장 일반적인 경우는 첨부파일을 열었을 때, 개인정보를 쉽게 확인할 수 있는 경우입니다.</td></tr>
<tr><td>조치사항</td><td>이러한 유형의 노출이 발견되면,
해당 게시자에게 통보하여 게시판에서 해당 게시물을 삭제한 후, 개인정보를 제거한 파일을 다시 업로드 하도록 조치하여야 합니다.</td></tr>
</table>

관리자페이지의 첨부파일이 노출된 경우



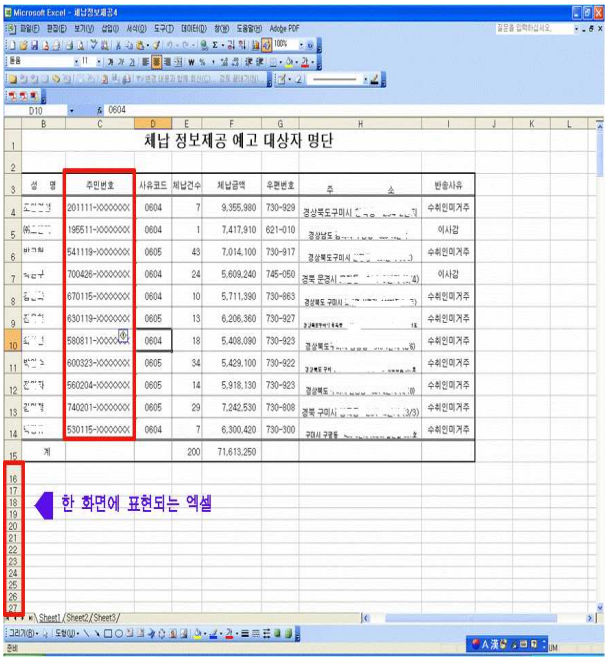
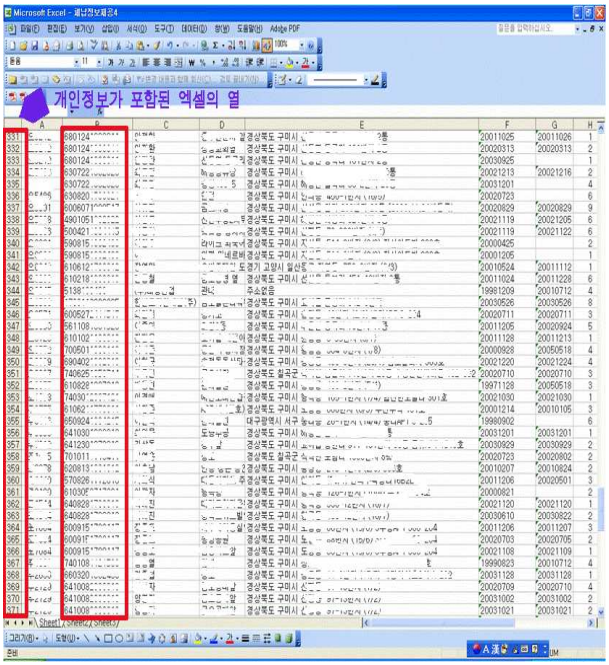
유형설명	접근권한을 가진 이용자만 접근할 수 있는 웹페이지를 접근권한이 없는 이용자가 접속할 수 있도록 홈페이지를 설계하여 발생한 개인정보 노출 유형입니다. 원래 접근제한 웹페이지는 접근권한을 가진 이용자만이 접근할 수 있도록 보안기능을 고려하여 설계하여야 합니다. 그러나 이러한 접근권한 및 인증 등의 절차가 제대로 구현되지 않으면 이와 같이 노출이 발생할 수 있습니다.
조치사항	이러한 유형의 노출이 발견되면, 홈페이지의 접근권한 관련 보안기능이 어떻게 설계 되었는지를 파악하여 각 웹페이지별로 접근권한에 따른 정확한 인증절차를 준수하도록 수정하여야 합니다.

엑셀파일의 다른 Sheet에 개인정보가 포함된 경우

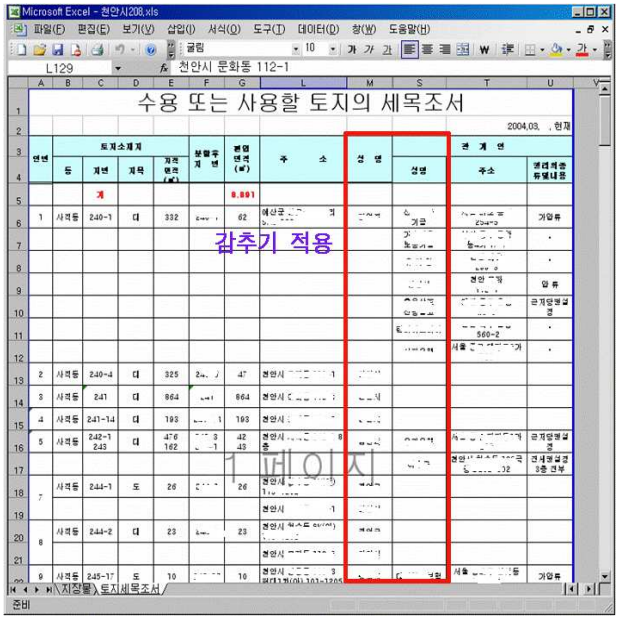
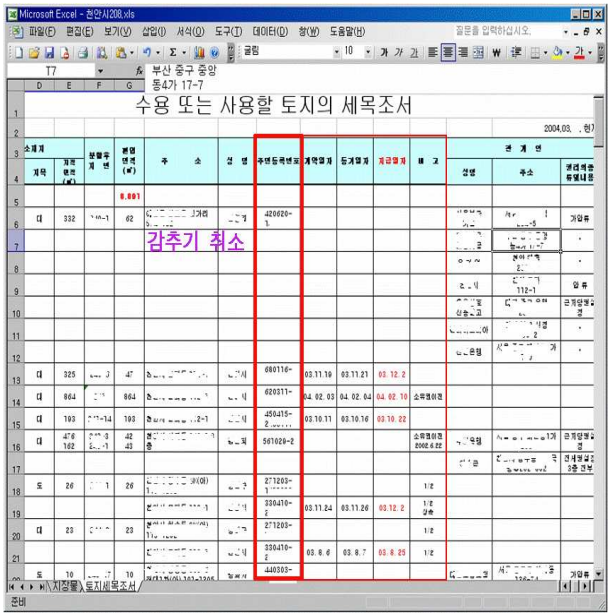
<<노출이 발견되는 않는 sheet>>	<<노출이 발견되는 다른 sheet>>
	

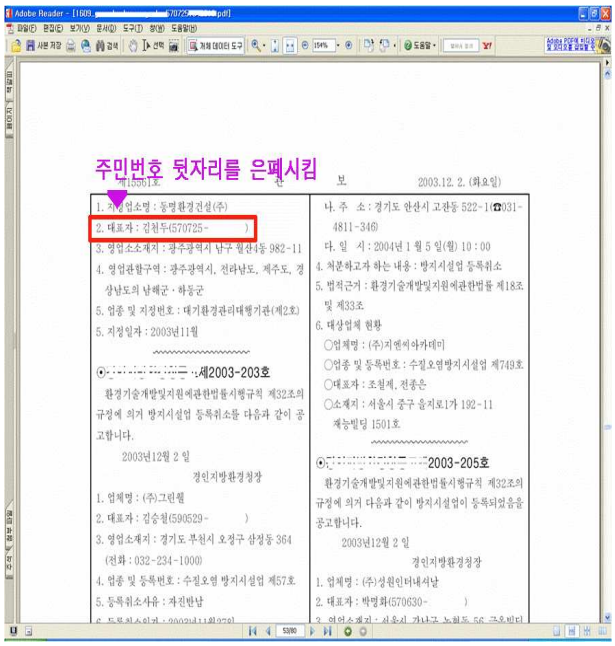
유형설명	엑셀파일에서만 나타나는 유형으로 첨부파일을 열었을 때에는 보이지 않지만, 엑셀파일 내의 다른 Sheet에 개인정보가 포함되어 발생하는 노출 유형입니다.
조치사항	이러한 유형의 노출이 발견되면, 해당 게시자에게 세부사항을 통보하여 게시판에서 해당 게시물을 삭제한 후, 개인정보를 제거한 파일을 다시 업로드 하도록 조치하여야 합니다.

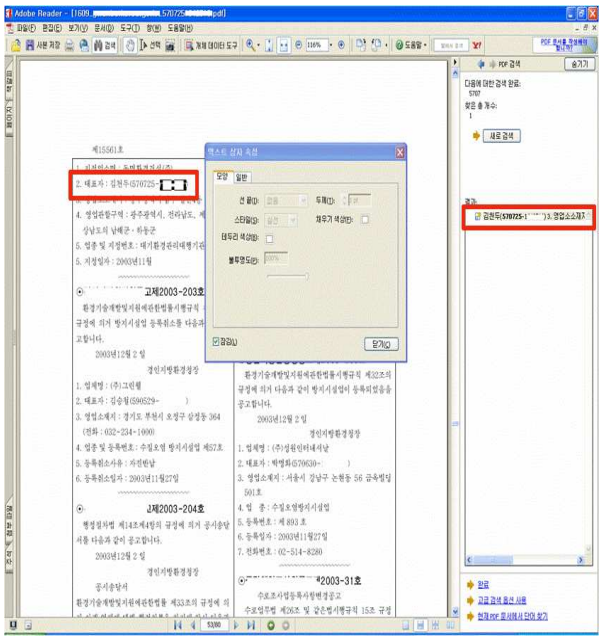
잘 보이지 않는 곳에 개인정보가 포함된 경우

<<노출이 보이지 않음>>	<<최하단에서 노출이 발견됨>>
	

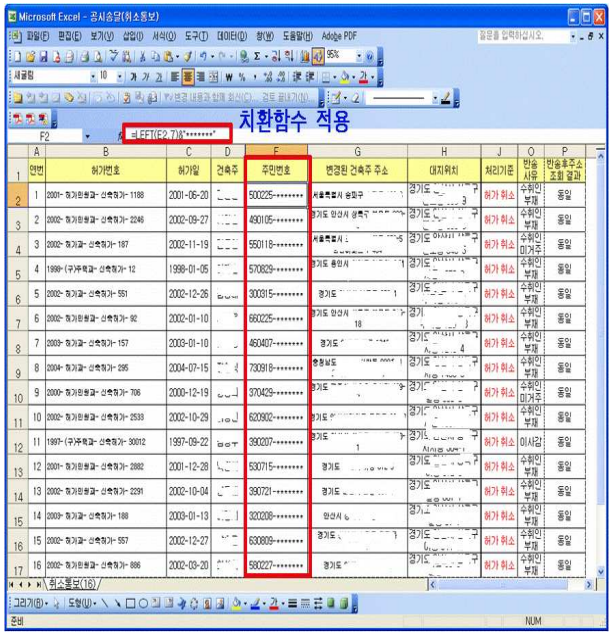
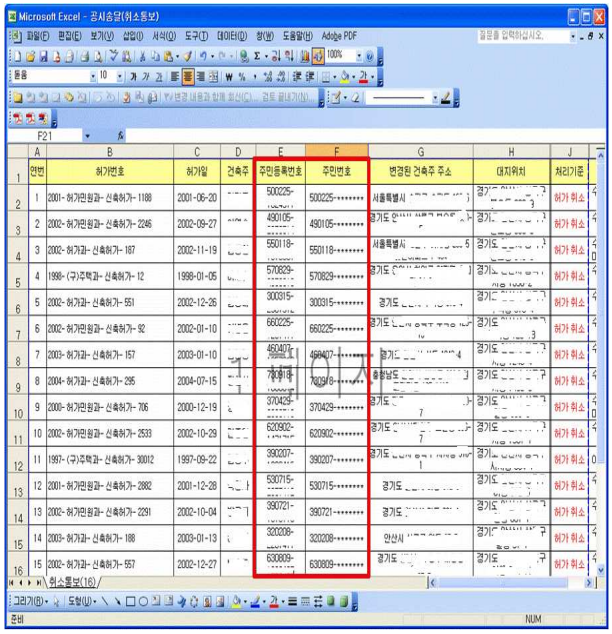
유형설명	엑셀파일에서 주로 나타나는 유형으로 파일을 열었을 때 바로 보이는 부분에서는 개인정보가 발견되지 않지만, 셀 최하단 또는 최우측으로 이동하였을 때, 개인정보가 발견되는 경우입니다.
조치사항	이러한 유형의 노출이 발견되면, 해당 게시자에게 세부사항을 통보하여 게시판에서 해당 게시물을 삭제한 후, 개인정보를 제거한 파일을 다시 업로드하도록 조치하여야 합니다.

<table>
<tr><th colspan="2">개인정보를 숨김처리를 하였지만 노출되는 경우</th></tr>
<tr><td><<개인정보를 숨김처리를 한 경우>></td><td><<개인정보 숨김을 취소한 경우>></td></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>유형설명</td><td colspan="2">엑셀파일에서 주로 나타나는 유형으로 파일을 열었을 때 개인정보가 포함된 셀이 숨김처리가 되어 개인정보가 발견되지는 않지만, 숨김을 취소하면 개인정보가 발견되는 경우입니다.
또한 숨김처리를 하면서 암호화를 하더라도 문서변환도구를 이용하면 쉽게 해당 내용을 볼 수 있으므로 유의하여야 합니다.</td></tr>
<tr><td>조치사항</td><td colspan="2">이러한 유형의 노출이 발견되면,
해당 게시자에게 세부사항을 통보하여 게시판에서 해당 게시물을 삭제한 후, 개인정보를 제거한 파일을 다시 업로드하도록 조치하여야 합니다.</td></tr>
</table>

<table>
<tr><th colspan="2">개인정보를 은폐하였지만 노출되는 경우</th></tr>
<tr><td><<개인정보를 은폐한 화면>></td><td><<개인정보가 검색된 화면>></td></tr>
<tr><td colspan="2"> 

 </td></tr>
<tr><td>유형설명</td><td>모든 첨부파일에서 나타날 수 있는 유형으로 파일에 있는 개인정보 중 일부를 은폐하기 위해서 해당 개인정보 위에 이미지 등을 덮어씌워 보이지 않지만, 파일 검색 기능을 이용하였을 때 개인정보가 발견되는 경우입니다.
예를 들어, 주민등록번호가 파일에 있는 경우, 13자리 숫자 중 7자리에 대해 은폐처리를 하더라도 이 발견되는 7자리 숫자로 검색을 하면 13자리 주민등록번호를 모두 확인할 수 있습니다.</td></tr>
<tr><td>조치사항</td><td>이러한 유형의 노출이 발견되면,
해당 게시자에게 세부사항을 통보하여 게시판에서 해당 게시물을 삭제한 후, 개인정보를 제거한 파일을 다시 업로드 하도록 조치하여야 합니다.</td></tr>
</table>

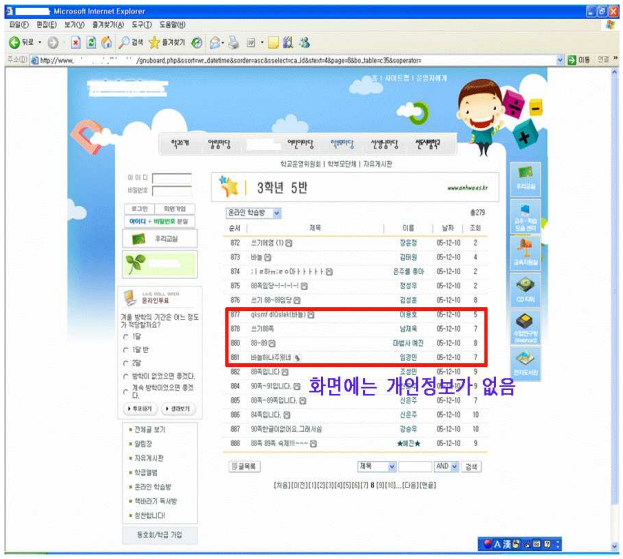
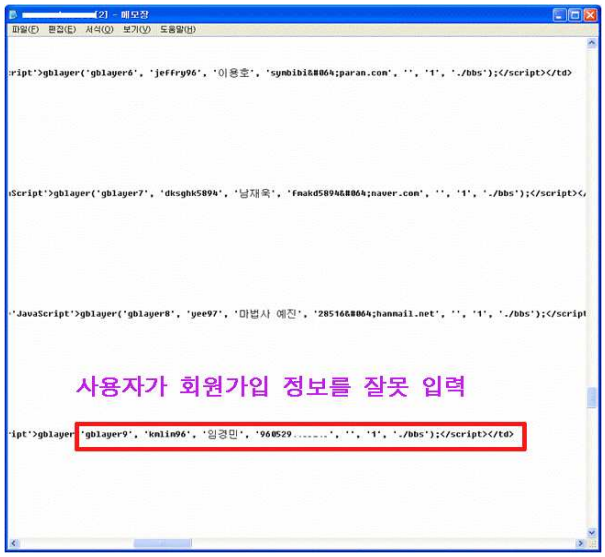
치환함수 등을 이용하였지만 노출되는 경우

<<치환함수를 적용한 화면>>	<<개인정보가 검색된 화면>>
	

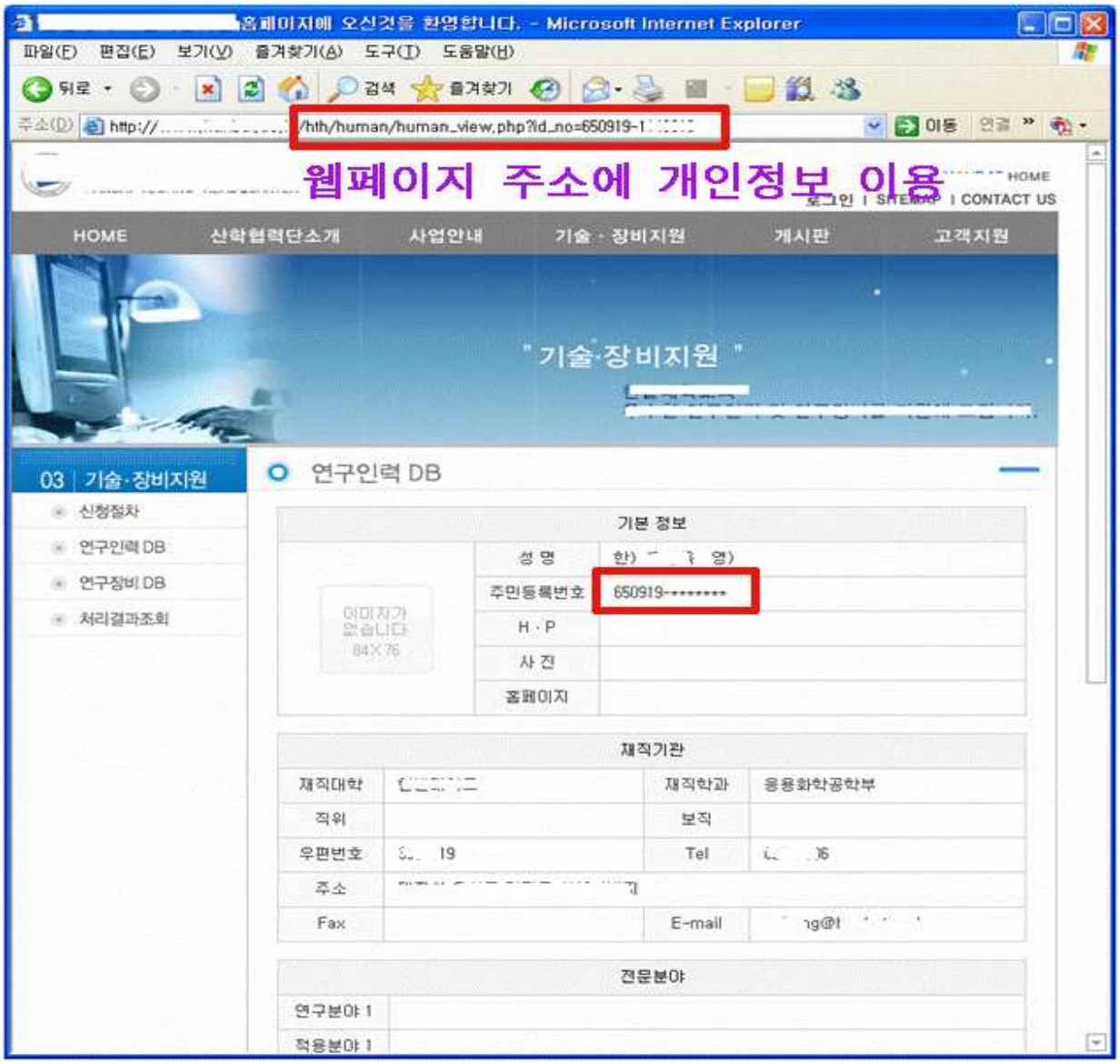
유형설명	엑셀파일에서 주로 나타나는 유형으로 개인정보가 포함된 셀에 LEFT 등의 치환함수를 적용하여 *처리 등으로 개인정보가 은폐된 것처럼 보이게 하지만, 엑셀파일의 검색기능을 이용하면 개인정보가 발견되는 경우입니다. 특히 치환함수를 적용하기 위해서는 어딘가에 해당 개인정보가 숨김처리 되어 있어야 하므로 개인정보가 숨김처리되어 있는 경우와 유사한 경우입니다.
조치사항	이러한 유형의 노출이 발견되면, 해당 게시자에게 세부 사항을 통보하여 게시판에서 해당 게시물을 삭제한 후, 개인정보를 제거한 파일을 다시 업로드 하도록 조치하여야 합니다.

3. 소스코드 노출 유형

모든 웹페이지는 기본적으로 소스코드가 공개되어 있습니다. 해당 웹페이지의 소스코드는 웹페이지 위에 마우스를 놓고 오른쪽 버튼을 클릭하였을 때, 나타나는 팝업 메뉴에서 선택하면 볼 수 있습니다. 이와 같은 소스코드에 의한 노출은 명의 도용을 하려는 이용자가 게시판의 게재자의 정보가 소스코드에 있는지 등을 확인하는 경향이 있다는 점에서 개인정보 노출의 유형으로 볼 수 있습니다. 소스코드에서 발생하는 개인정보 노출 유형과 조치 사항은 다음과 같습니다.

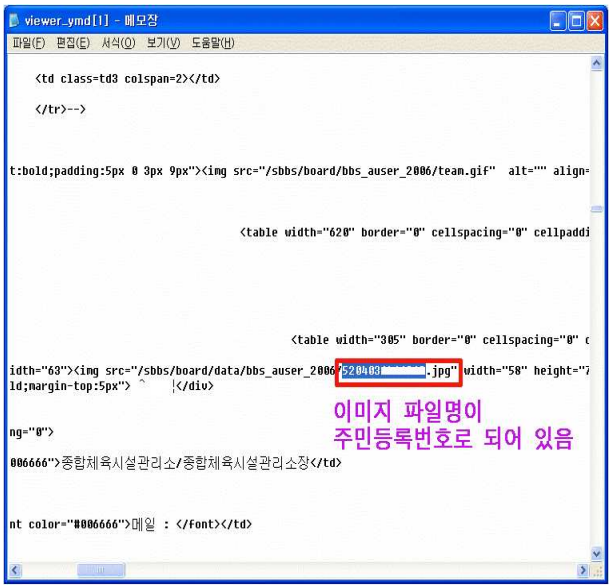
<table>
<tr><th colspan="2">게시판 소스코드에 개인정보가 포함된 경우</th></tr>
<tr><td><<일반적인 웹페이지 화면>></td><td><<개인정보가 포함된 소스코드>></td></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>유형설명</td><td colspan="2">웹페이지의 게시판 소스코드에서 나타나는 유형입니다.
홈페이지 설계 시, 게시물에 대한 구분자로서 게시자의 개인정보를 이용하는 경우, 소스코드에는 이 개인정보가 그대로 나타날 수 있습니다.</td></tr>
<tr><td>조치사항</td><td colspan="2">이러한 유형의 노출이 발견되면,
홈페이지 설계단계에서 검토가 필요합니다. 가장 간단한 조치방법으로는 웹페이지를 구별하기 위해 이용되는 개인정보를 해쉬함수 등 함수를 이용하여 변환하면 됩니다.</td></tr>
</table>

웹페이지 URL에 개인정보가 포함된 경우



유형설명	웹페이지의 URL에서 주로 나타나는 유형으로, 홈페이지 설계 시, 조직 구성원 등의 소개 웹페이지나 개인홈페이지에 주소부여 체계에서 개인정보를 이용하는 경우에 발생할 수 있습니다.
조치사항	이러한 유형의 노출이 발견되면, 홈페이지 설계단계에서 검토가 필요합니다. 이에 대한 조치 사항으로는 해당 웹페이지와 관련된 새로운 주소부여체계를 적용할 수 있으며, 보다 간단한 조치방법으로는 웹페이지 URL에 이용되는 개인정보를 해쉬함수 등 함수를 이용하여 변환하면 됩니다.

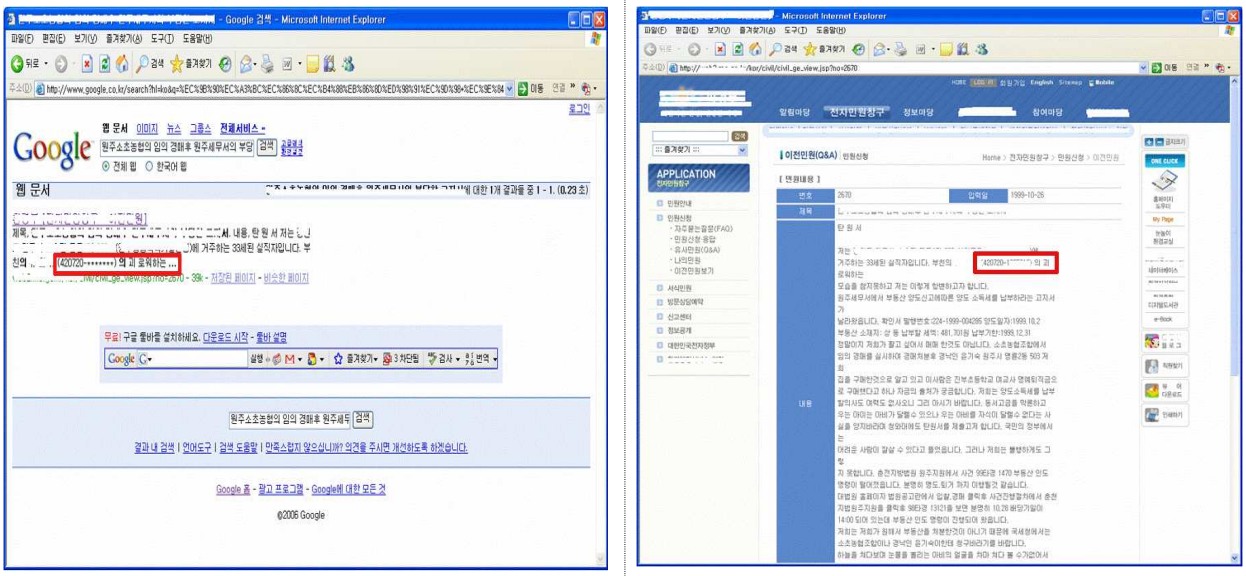
웹페이지 소스코드 파일명에 개인정보가 포함된 경우

<<일반적인 웹페이지 화면>>	<<개인정보가 포함된 소스코드>>
	

유형설명	웹페이지의 파일명에 해당하는 소스코드에서 나타나는 유형입니다. 홈페이지 구축 시, 조직구성원의 이미지 파일명으로 개인정보를 이용하는 경우 소스코드에는 이 개인정보가 그대로 나타날 수 있습니다.
조치사항	이러한 유형의 노출이 발견되면, 해당 파일의 이름을 모두 개인정보와 무관한 파일명으로 변경하면 됩니다.

4. 외부 검색엔진 노출 유형

현재 외부 검색엔진 중 구글 검색엔진은 전 세계적으로 가장 강력한 성능을 가진 검색엔진으로 명의도용 의도를 가진 이용자가 자주 이용하는 창구역할을 하고 있습니다. 따라서 홈페이지를 통한 개인정보 노출 방지를 위해서는 관리 홈페이지에서 노출된 개인정보를 구글 검색엔진이 수집하였는지 지속적으로 파악하고 점검할 필요가 있습니다. 구글 검색엔진을 통한 노출 유형과 조치 사항은 다음과 같습니다.

<table>
<tr><th colspan="2">일반적인 경우</th></tr>
<tr><td><<구글에 개인정보가 검색된 경우>></td><td><<링크된 개인정보 노출화면>></td></tr>
<tr><td colspan="2">  </td></tr>
<tr><td>유형설명</td><td>구글 검색엔진을 통해 방문한 해당 웹페이지에 개인정보가 발견되는 유형입니다.
최근 구글 검색엔진은 주민등록번호 중 뒤의 7자리를 *로 치환하여 검색결과를 일부 제공하기도 하지만, 여전히 주민등록번호 13자리가 모두 검색결과로 제공되는 경우가 발생하고 있습니다.
따라서 이 유형은 검색결과의 * 치환 여부와 관계없이 검색 결과를 클릭하였을 때, 해당 웹페이지에 개인정보가 존재하는 경우를 말합니다.</td></tr>
<tr><td>조치사항</td><td>이러한 유형의 노출이 발견되면,
먼저 해당 웹페이지에 있는 내용 중 개인정보를 즉시 삭제하여야 합니다.
그 후에 검색엔진 배제표준이나 메타 태그를 적용합니다.</td></tr>
</table>

검색엔진 배제표준을 적용하기 위해서는 다음과 같은 내용으로 된 robots.txt 파일을 웹서버의 루트 디렉토리에 저장합니다.

User-Agent: *
Disallow:/

또한 메타태그를 적용하기 위해서는 삭제하려는 웹페이지의 소스코드 파일(HTML 파일)에 <META NAME = GOOGLEBOT" CONTENT= "NOINDEX, NOFOLLOW">를 포함시킵니다.

이제 구글의 자동삭제 시스템에 접속하여 개인정보 노출이 발견된 웹페이지를 캐쉬에서 삭제 처리해달라고 요청하는데, 그 세부절차는 다음과 같습니다. 구글 자동삭제 시스템을 이용하지 않고, 구글 웹사이트 관리자에게 이메일을 통해 삭제를 요청하는 정상적인 프로세스를 통하면 삭제 처리는 요청 후 6주~8주가 소요됩니다.

가) 구글 회원 가입 및 로그인

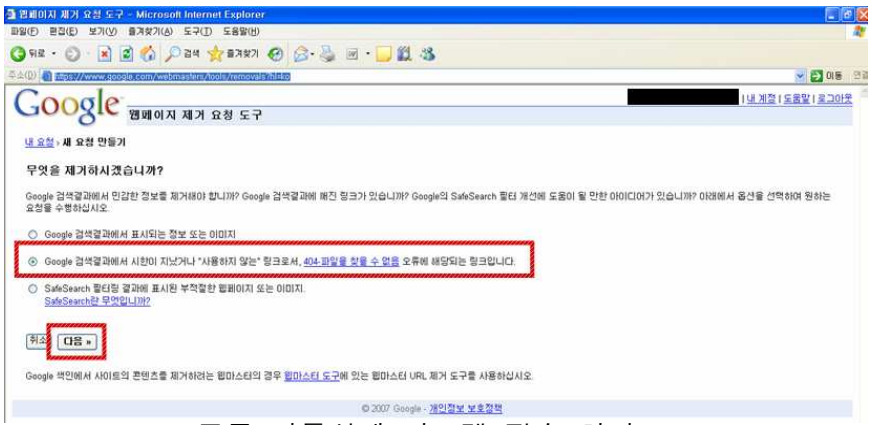
구글 자동삭제 시스템 이용을 위해서 먼저 구글 웹사이트에 가입 한 후 로그인합니다.

나) 구글 자동삭제 시스템에 접속

① 로그인 상태에서 다음과 같은 구글 자동삭제 시스템에 방문합니다.

https://www.google.com/webmasters/tools/removals?hl=ko

② 초기 화면에서 “Google 검색결과에서 시한이 지났거나 “사용하지 않는 링크”로서, 404-파일을 찾을 수 없음 오류에 해당되는 링크입니다” 를 선택하고 “다음” 버튼을 선택합니다.

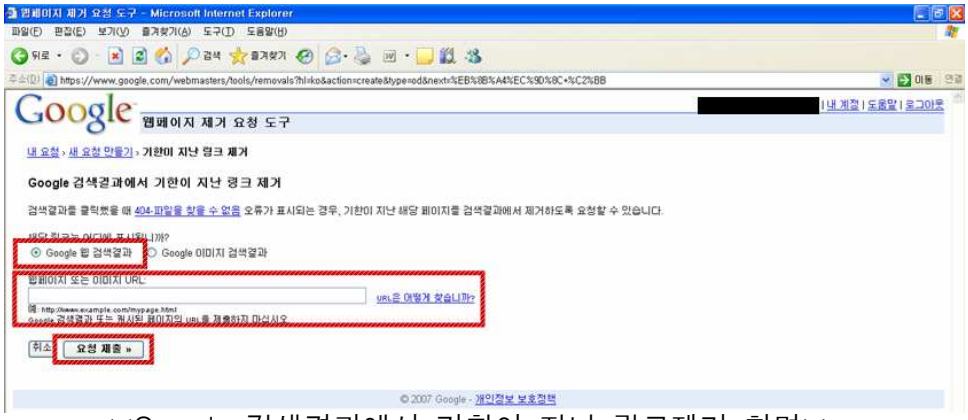


<< 구글 자동삭제 시스템 접속 화면>>

다) Google 검색결과에서 기한이 지난 링크제거

① “Google 웹 검색결과” 를 선택합니다.

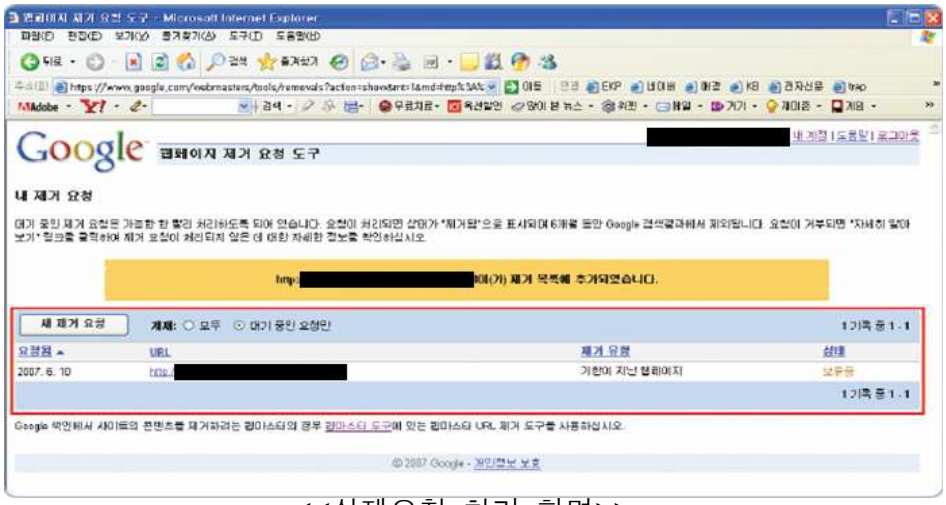
② “웹페이지 또는 이미지 URL”에 기 삭제한 홈페이지 URL 주소를 입력하고 “요청 제출”을 클릭합니다.(이 때, 구글 캐쉬 주소를 입력하면 삭제처리가 되지 않으므로 주의합니다.)



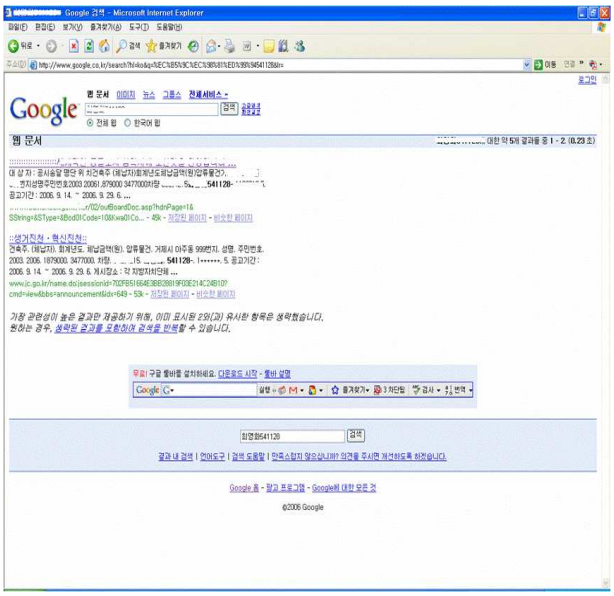
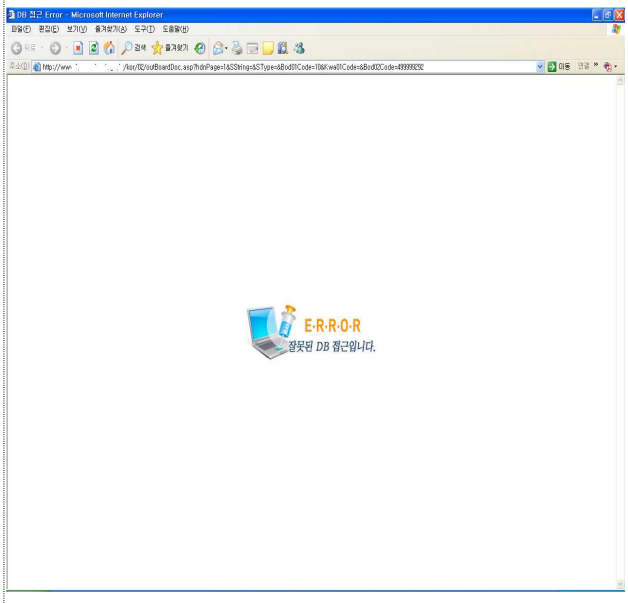
<<Google 검색결과에서 기한이 지난 링크제거 화면>>

라) 삭제 요청 처리 상태 확인

자동 삭제처리 시스템에서 “내 제거 요청”을 클릭하면 현재 삭제 요청 정보 및 처리 상태를 확인할 수 있습니다.



<<삭제요청 처리 화면>>

<table>
<tr><th colspan="3">구글 DB에만 노출이 존재하는 경우</th></tr>
<tr><td colspan="2"><<구글에 개인정보가 검색된 화면>></td><td><<삭제된 해당 웹페이지 화면>></td></tr>
<tr><td colspan="2">  </td><td> 
</td></tr>
<tr><td>유형설명</td><td colspan="2">개인정보가 포함되어 있는 웹페이지는 삭제되었으나, 구글 검색엔진에 저장되어 검색 시 개인정보가 발견되는 유형입니다.</td></tr>
<tr><td>조치사항</td><td colspan="2">이러한 유형의 노출이 발견되면,
먼저 검색엔진 배제표준이나 메타 태그를 적용합니다. 검색엔진 배제표준을 적용하기 위해서는 다음과 같은 내용으로 된 robots.txt 파일을 웹서버의 루트 디렉토리에 저장합니다.

User-Agent: *
Disallow:/

또한 메타태그를 적용하기 위해서는 삭제하려는 웹페이지의 소스코드 파일(HTML 파일)에 <META NAME = GOOGLEBOT" CONTENT= "NOINDEX, NOFOLLOW">를 포함합니다.

이제 구글의 자동삭제 시스템에 접속하여 개인정보 노출이 발견된 웹페이지를 캐쉬에서 삭제 처리해달라고 요청하는데, 그 세부절차는 p19~21의 구글 자동삭제 시스템 이용절차와 같습니다. 구글 자동삭제 시스템을 이용하지 않고, 구글 웹사이트 관리자에게 이메일을 통해 삭제를 요청하는 정상적인 프로세스를 통하면 삭제 처리는 요청 후 6주~8주가 소요됩니다.</td></tr>
</table>

구글 검색엔진의 인증 우회

인증우회 개요	일반적으로 웹 서버는 관리자 페이지와 같이 접근제한이 필요한 일부 영역에 대해서 인증 등의 절차를 통하여 제한적으로 접근을 허용하도록 구성되어 있습니다. **그러나 웹 서버의 접근제한 기능이 불완전하게 구성되는 경우,** 구글과 같은 검색엔진은 인증절차를 거치지 않고 우회하여 인증이 필요한 페이지에 접근하고, 접근하여 획득한 정보를 검색엔진 DB에 저장함으로써 일반 인터넷 이용자에게 해당 정보가 제공됩니다. 특히 웹 서버내의 각 관리자 페이지들은 서로 링크되어 있어서 하나의 관리자 페이지에만 접속하면 모든 관리자페이지에 접근할 수 있으므로 **인증이 필요한 영역 전체에 완전한 인증절차를 요구하도록 홈페이지를 구현하여야 합니다.**

<table>
<tr>
<td>검색엔진의
인증우회
방법</td>
<td>구글과 같은 검색엔진은 해킹과 같은 비정상방법이 아닌 정상적인 웹 서버 접근방법에 의해서 인증을 우회할 수 있습니다. 이 때 구글과 같은 검색엔진이 정상적인 접근에 의해 인증을 우회하는 방법은

가) 관리자 페이지 영역의 URL 자동접근

이 경우는 구글과 같은 검색엔진은 웹 서버에 접근할 때, 일반 이용자들이 웹 브라우저를 이용하는 것과는 달리 Socket을 통해서 웹 서버에 접근하기 때문에 발생합니다.
먼저 구글과 같은 검색엔진은 웹 서버 내의 정보 검색 시 현재 접근한 페이지의 링크 추적, 과거에 접근했던 URL 리스트를 이용한 검색, URL에 포함된 파라미터값 자동 계산 등의 다양한 방법을 이용하여 검색할 수 있습니다.
이러한 검색과정에서 관리자 페이지에 해당하는 특정 URL이 검색되면, 웹 브라우저를 이용하여 URL에 접근하는 경우에는 웹 서버가 접근을 요청한 웹 브라우저의 아이디에 대한 세션 체크 등의 접근 유효성을 검사하지만, 검색엔진의 Socket 통신을 이용하는 경우 이러한 유효성 검사를 생략하므로 해당 웹 페이지에 바로 접근할 수 있습니다.

나) 웹보안 취약점을 통한 접근

이 경우는 웹 서버가 디렉토리 리스팅과 같은 보안 취약점을 갖는 경우에 발생합니다.
즉, 구글과 같은 검색엔진은 URL 정보 획득 과정에서 URL 뒤에 / 만을 붙여서 체크할 수 있는 디렉토리 리스팅 취약점 페이지 정보를 획득하게 되고, 이 취약점에 노출된 디렉토리가 관리자 페이지와 같이 인증을 필요로 하는 페이지인 경우 인증을 거치지 않고 접근할 수 있습니다.</td>
</tr>
<tr>
<td>검색엔진의
인증우회
방지방법</td>
<td>가) 관리자 페이지 영역의 URL 자동접근

검색엔진의 인증우회는 근본적으로 인증이 필요한 페이지 영역 전체에 대해 인증 요구 절차가 완전히 구현되지 않아서 발생합니다.
따라서 관리자는 인증을 필요로 하는 모든 영역에 속한 모든 페이지 접근 시 인증절차를 거치도록 설계하여야 합니다.</td>
</tr>
</table>

예를 들어 JAVA로 구현된 웹페이지의 경우, 각 웹 페이지 상단에 다음과 같은 소스 코드를 삽입합니다.

```
<jsp:include flush="true" page="session_check.jsp" />
```

여기서 session_check.jsp 파일은 인증을 처리하는 파일로 실제 적용 코드에는 이 파일이 있는 전체 URL을 적습니다.

이 때 session_check.jsp 파일의 예는 다음과 같습니다.

```
<%
 // 세션 체크
 SPInfoBean bean = (SPInfoBean) session.getAttribute("user.login");
 if (bean == null) {
%>
  <script>
   alert('로그인 정보가 없습니다.');
   this.location = "index.jsp";
  </script>
<%
 }
%>
```

나) 웹보안 취약점을 통한 접근

웹보안 취약점을 통한 접근에 대한 인증우회를 방지하기 위해서는 웹 서버 내의 모든 디렉토리에 대한 디렉토리 리스팅 취약점을 제거하여야 합니다. 이에 대한 조치방법은 본 가이드라인 p28~29에 설명되어 있습니다.

인증우회 자가진단 방법

관리자 웹페이지의 인증 부재 확인

=> 관리자 페이지 시작점에만 인증 모듈이 설치되어 있는지 여부를 확인합니다.

- 관리자 페이지 시작부분과 웹을 이루고 있는 각 서버 스크립트 모듈마다 인증을 검사하는 모듈이 존재하는지 확인합니다. 즉, 관리자 어플리케이션 각각에 대해서 모두 인증을 수행하는 공통모듈을 통하여 접근권한을 부여 하는지 검증을 실시합니다.
- 좀더 자세한 확인을 위해서는 관리자 페이지 아래에 위치한 URL들을 모두 조사한 후 해당 URL을 권한이 없는 상태에서 하나씩 입력해 봅니다.

개발 오류에 의한 인증 부재 확인

=> 인증우회를 유발하는 코드를 포함하고 있는지 여부를 확인합니다.

- 개발시 필요에 의해 인증기능을 일시 정지하여 놓은 부분이 있는지 확인합니다. (이렇게 짧은 시간의 인증 정지라 하더라도 검색엔진은 관리자 페이지 정보를 수집해 갈 수 있습니다.)
- 개발시 데이터를 입력하는 폼에만 사용자 인증을 충실히 수행하고 관리자 입력 정보를 데이터베이스에 연계처리하는 부분에 인증을 적용하지 않은 부분이 있는지 확인합니다.

Ⅲ 개인정보 노출 취약점 점검 및 조치방법

홈페이지를 통한 개인정보 노출이 발생하는 원인은 크게 관리적인 원인과 기술적인 원인으로 나눌 수 있습니다.

구 분	설 명
관리적인 원인	홈페이지 관리자와 이용자의 개인정보에 대한 인식 부족이나 관리 소홀 때문에 발생하는 원인
기술적인 원인	홈페이지 설계 및 구축 단계에서 개인정보 노출이나 보안 취약점을 고려하지 않아서 발생하는 원인

그 중에서 개인정보 노출에 직접적인 원인이 되는 것은 관리적인 원인과 기술적인 원인 중 개인정보 노출을 고려하지 않아서 발생하는 원인들인데, 이 원인들은 앞 2장의 각 유형에 포함되어 있습니다.

한편, 기술적인 원인 중에서 보안 취약점을 고려하지 않고 설계, 구축된 홈페이지는 개인정보 노출의 간접적인 원인을 제공합니다.

예를 들어, 웹 서버의 디렉토리 및 파일 목록을 보여주는 디렉토리 인덱싱과 같은 보안 취약점이 존재하는 경우, 구글 검색엔진은 디렉토리 인덱싱 웹페이지를 검색에 활용하므로 웹 서버 내에 존재하는 개인정보가 그대로 노출될 위험이 있습니다.

이 장에서는 개인정보 노출에 대한 간접적인 원인이 되는 웹서버 보안취약점을 관리자가 자체적으로 점검할 수 있는 방법과 개인정보 노출 시 조치사항을 설명합니다.

특히 여기서는 관리 웹서버의 개인정보 노출과 관련된 보안취약점 뿐만 아니라, 보안취약점이 발생한 웹페이지가 구글 검색DB에 저장되어 있는지 여부를 점검하는 방법도 제공합니다.

1. 디렉토리 리스팅 취약점

개요	인터넷 이용자에게 웹 서버 내 모든 디렉토리 및 파일 목록을 보여주고, 파일의 열람 및 저장도 가능하게 하는 취약점
점검범위	점검 대상이 되는 해당 홈페이지에 디렉토리 리스팅 취약점이 존재하는지 여부와 디렉토리 리스팅 취약점 페이지가 구글엔진에 저장되었지는 여부를 점검합니다.
점검방법	
구글을 통한 점검방법	○ 구글 사이트에 접속합니다. ○ 고급 검색으로 이동합니다. ○ 도메인 설정 란에는 해당 사이트 주소를 입력하고, 검색창에는 다음을 입력하여 디렉토리 목록이 저장된 페이지를 찾습니다. - intitle:index.of "parent directory" - intitle:index.of name size ○ 검색 결과를 바탕으로 해당 사이트의 디렉토리 노출을 확인합니다.
직접 점검방법	○ 해당 웹 사이트의 하위 디렉토리 정보를 사전에 모두 확인합니다. ○ 웹 루트의 모든 하위 디렉토리에 대해서 웹 브라우저에 해당 주소를 입력해서 디렉토리 노출 여부를 점검합니다. 예) http://www.sample.go.kr/ 이란 웹 서버의 웹 루트 밑에 “file”이란 디렉토리가 있다면 웹 브라우저의 URL 주소 입력란에 http://www.sample.go.kr/file/ 이라고 입력한다. 이 때 “file” 디렉토리 하위 내용이 모두 화면에 출력된다면 디렉토리 리스팅 취약점이 존재하는 것이다.(반드시 맨 끝의 ‘/’ 까지 입력) ○ 모든 디렉토리에 대해 디렉토리 리스팅 취약점 존재 여부를 확인합니다.

<table>
<tr><th colspan="3">조치방법</th></tr>
<tr><td colspan="2">구글 캐쉬에 노출된 경우</td><td>○ 개인정보 취약점 페이지가 구글에 노출된 경우에는 먼저 홈페이지에도 개인정보 취약점 노출이 있는지 여부를 확인하여 홈페이지의 개인정보 취약점을 제거 한 후, 구글 검색 사이트에 해당 캐쉬에 대해 삭제를 요청하는 이메일을 발송합니다.
○ 개인정보의 노출 정도가 심각하여 긴급하게 노출을 방지하고자 한다면, 구글의 자동 URL 삭제 시스템을 이용하여, URL이 검색되지 않도록 합니다.

구글 자동 URL 삭제 시스템:
http://services.google.com:8882/urlconsole/controller?cmd=reload&lastcmd=login</td></tr>
<tr><td rowspan="2">직접 점검 시 노출의 경우</td><td>윈도우</td><td>○ [제어판]→[관리도구]의 [인터넷 서비스 관리자](혹은 [인터넷 정보 서비스]) 메뉴에서 [기본 웹 사이트]의 마우스 오른쪽 클릭, ‘속성’ 부분을 보면 ‘기본 웹 사이트 등록 정보’가 나옵니다.
○ ‘기본 웹 사이트 등록 정보’에서 ‘홈 디렉토리’ 부분을 클릭한 후 ‘디렉토리 검색(B)' 부분의 체크를 해지합니다.</td></tr>
<tr><td>리눅스/유닉스</td><td>○ 서버에서 “httpd.conf” 라는 파일을 찾습니다.
○ 파일 내용 중 Options 항목 뒤에 Indexes 라는 단어를 지우고 파일을 저장합니다. 이 때, Options 항목은 디렉토리 별로 설정할 수 있게 되어 있으므로 모든 디렉토리에 대해서 Options 항목을 제거합니다.
○ 설정을 적용하기 위해 웹 서버 데몬을 다시 띄워줍니다.</td></tr>
</table>

2. 파일 다운로드 취약점

개요	게시판 등에 저장된 자료에 대해 위치 지정에 대한 제한을 부여하지 않음으로써 웹 서버 내의 비공개 자료를 다운로드 받을 수 있도록 하는 취약점
점검범위	점검 대상이 되는 홈페이지에 파일 다운로드 기능이 존재하는지 여부를 점검하고, 파일 다운로드 스크립트 이용 여부를 확인한 후, 다운로드 스크립트의 매개변수를 변경하면서 주요 파일 다운로드를 시도합니다.

점검방법

○ 게시판이 존재하는지, 그리고 그 게시판에 파일 다운로드 기능이 있는지 점검합니다. 파일 다운로드 기능이 존재하지 않으면 '파일 다운로드' 취약점은 존재하지 않습니다.

○ 파일 다운로드 기능이 존재하는 경우, 파일 다운로드 시 URL 주소를 확인하여 파일 다운로드 스크립트를 이용하는지 여부를 확인한다. 파일 다운로드 URL 주소 확인은 첨부파일 하이퍼링크 부분에 마우스를 가져가 아래 상태표시줄로부터 링크를 확인하거나 팝업 메뉴의 '바로가기 복사(T)'를 클릭하고 메모장 등에서 '붙여넣기' 함으로써 확인할 수 있습니다. 파일 다운로드 스크립트를 이용하지 않으면 '파일 다운로드' 취약점은 존재하지 않습니다.

<<다운로드 스크립트를 사용하지 않는 경우의 예>>
http://servername.go.kr/test/download/공지사항1.hwp
<<다운로드 스크립트를 사용하는 경우의 예>>
http://servername.go.kr/test/filedown.down?file=공지사항3.hwp&path=download

○ 파일 다운로드 스크립트를 이용하는 경우, 매개변수를 변경하면서 주요 파일 다운로드를 시도합니다. 이 때, 매개변수의 개수 및 경로를 적는 형식이 조금씩 다르므로 링크 주소에 따라 상대적으로 매개변수 변경을 시도해야 합니다.

/etc/passwd 파일 다운로드 시도	ASP 게시판	<정상적인 링크>	http://servername.go.kr/pr/download.asp?filename=test.hwp
		<다운로드 시도>	http://servername.go.kr/pr/download.asp?filename=/etc/passwd http://servername.go.kr/pr/download.asp?filename=../../../etc/passwd 등의 형태로 시도하되, 링크 중 ../의 개수를 1개부터 10개까지 점차 증가시키면서 시도합니다.
	PHP 게시판	<정상적인 링크>	http://servername.go.kr/includes/download.php?sub_path=upfiles&filename=test.hwp
		<다운로드 시도>	http://servername.go.kr/includes/download.php?sub_path=../../../etc&filename=passwd http://servername.go.kr/includes/download.php?sub_path=upfiles&filename=../../../../../../etc/passwd 등의 형태로 시도하되, 위의 두 가지 링크 각각에 대해 ../의 개수를 1개부터 10개까지 점차 증가시키면서 시도합니다.
	JSP 게시판	<정상적인 링크>	http://servername.go.kr/include/down.jsp?upfile=test.hwp&dir=/data
		<다운로드 시도>	http://servername.go.kr/include/down.jsp?upfile=passwd&dir=/etc http://servername.go.kr/include/down.jsp?upfile=passwd&dir=/data/../../../etc 등의 형태로 시도하되, 위의 두 번째 링크에 대해 ../의 개수를 1개부터 10개까지 점차 증가시키면서 시도합니다.
	기타 게시판	<정상적인 링크>	http://servername.go.kr/servlet/Down?path=/DATA/docu/2006/10/10&name=test.hwp
		<다운로드 시도>	http://servername.go.kr/servlet/Down?path=../../../../etc&name=passwd http://servername.go.kr/servlet/Down?path=/DATA/../../../etc&name=passwd 등의 형태로 시도하되, 링크 중 ../의 개수를 1개부터 10개까지 점차 증가시키면서 시도합니다.

<table>
<tr><td rowspan="3">download 파일 다운로드 시도</td><td>ASP 게시판</td><td><정상적인 링크></td><td>http://servername.go.kr/pr/download.asp?filename=test.hwp</td></tr>
<tr><td></td><td><다운로드 시도></td><td>http://servername.go.kr/pr/download.asp?filename=../pr/download.asp
등의 형태로 시도하되, 링크 중 ../의 개수를 1개부터 10개까지 점차 증가시키면서 시도합니다.</td></tr>
<tr><td>PHP 게시판</td><td><정상적인 링크></td><td>http://servername.go.kr/includes/download.php?sub_path=upfiles&filename=test.hwp</td></tr>
<tr><td></td><td><다운로드 시도></td><td>http://servername.go.kr/includes/download.php?sub_path=includes&filename=download.php
http://servername.go.kr/includes/download.php?sub_path=upfiles&filename=../../../../../includes/download.php
등의 형태로 시도하되, 위의 두 번째 경우에 대해서는 ../의 개수를 1개부터 10개까지 점차 증가시키면서 시도합니다.</td></tr>
<tr><td></td><td>JSP 게시판</td><td><정상적인 링크></td><td>http://servername.go.kr/include/down.jsp?upfile=test.hwp&dir=/data</td></tr>
<tr><td></td><td></td><td><다운로드 시도></td><td>http://servername.go.kr/include/down.jsp?upfile=down.jsp&dir=/include
등의 형태로 시도하되, 링크 중 ../의 개수를 1개부터 10개까지 점차 증가시키면서 시도합니다.</td></tr>
</table>

○ 다운로드 시도가 성공하는 경우 직접 웹 브라우저 화면에 내용이 뜨거나 '파일 저장'을 통해 저장이 될 수 있습니다. 이 경우들은 모두 파일 다운로드 취약점을 가지고 있는 경우입니다.

조치방법

첨부파일이 저장되어 있는 특정 디렉토리에 있는 파일만을 다운 받을 수 있도록 하기 위해 첨부파일을 다운받기 위해 사용하는 다운로드 스크립트를 다음과 같은 방법으로 수정해야 합니다.

○ 다운받기 위한 파일 이름에 "..", "/", "₩"와 같은 문자열이 존재하면 모두 필터링합니다. 이 부분은 웹 서버 설정으로 해결할 수 있는 것이 아니므로 스크립트의 내용을 수정해야 합니다.l

○ 스크립트 수정이 된 후에 다시한번 취약점 점검 때와 같이 파일 다운로드가 되는지 여부를 확인하는 시도를 통해 취약점이 여전히 존재하는지를 점검합니다.

3. 파일 업로드 취약점

개요	게시판에서 첨부파일을 업로드 하는 경우, 악성 실행 프로그램을 업로드한 후에 홈페이지 접속 방식으로 웹서버를 원격 제어할 수 있게 하는 취약점
점검범위	점검 대상이 되는 홈페이지에 파일 업로드 기능이 존재하는지 여부를 점검하고, 특정 확장자를 가진 악성파일의 업로드를 시도합니다.

점검방법

○ 게시판이 존재하는지, 그리고 그 게시판에 파일 업로드 기능이 있는지 점검합니다. **파일 업로드 기능이 존재하지 않으면 '파일 업로드' 취약점은 존재하지 않습니다.**

○ 파일 업로드 기능이 존재하는 모든 게시판에 대해서 php, php3, asp, jsp, cgi, inc, pl 등의 확장자를 가진 파일 업로드를 시도합니다. 파일 업로드를 확인하였을 때, 실제 업로드가 되었다면 '파일 업로드' 취약점이 존재합니다.

조치방법

게시판의 첨부파일 업로드를 처리하는 웹 소스코드에서 첨부파일의 확장자를 필터링하도록 처리합니다.

○ 게시판 작성 후 업로드 버튼을 클릭할 때, 첨부파일을 확인하여 php, php3, asp, jsp, cgi, inc, pl 등의 확장자를 갖는 파일의 경우는 경고창을 띄워 업로드를 제한합니다.

○ 웹 소스 수정을 한 후에 다시 한 번 취약점 점검과 같은 시도를 통해 취약점이 여전히 존재하는지 점검합니다.

4. 크로스 사이트 스크립트(XSS) 취약점

개요	게시판에서 글쓰기를 하는 경우, 입력 내용 중 실행코드인 스크립트의 태그에 대한 필터링을 하지 않아서 악의적인 스크립트 등록을 통해 일반 이용자 PC로부터 개인정보인 쿠키 등을 유출할 수 있게 하는 취약점
점검범위	점검 대상이 되는 홈페이지 게시판에 글쓰기 기능이 존재하는지 여부를 점검하고, 간단한 스크립트 문장을 입력하여 게시를 시도합니다.

점검방법

○ 게시판, 의견쓰기, 게시마당, 민원신청, 여론마당 등에 대해 일반 사용자들이 글을 게시할 수 있는 기능이 있는지 점검합니다. **글쓰기 기능이 전혀 없으면 'XSS 취약점' 은 존재하지 않습니다.**

○ 글쓰기 기능이 있는 게시판에 대해 본문에 다음과 같은 스크립트 문장을 입력하고 게시를 시도합니다.

```
<script>alert('XSS 취약점 존재');</script>
```

○ 글을 게시하는 중에 스크립트 태그 사용에 대한 '에러'나 '경고' 메시지가 뜨면서 등록이 안된다면 'XSS 취약점'이 존재하지 않는 것입니다.

○ 윈도우 경고창이 전혀 뜨지 않고 글 본문에 스크립트 문장이 입력한 대로 나오면 XSS 취약점이 존재하지 않는 것입니다.

○ 윈도우 경고창을 통해 'XSS 취약점 존재' 나 "XSS 취약점 존재"와 같은 형태의 팝업창이 뜨면 'XSS 취약점'이 존재하는 것입니다.

조치방법

XSS 취약점은 웹 서버 설정으로는 조치할 수 없습니다. 글쓰기가 가능한 게시판 페이지에서 이용자들의 입력 중 스크립트에 대해 다음과 같이 모두 필터링 합니다.

○ 스크립트 문장에 존재할 수 있는 <, >, (,), #, & 등의 메타 문자를 다른 문자로 변환하거나 글 게재 시점에서 스크립트가 있는 경우에는 게재를 차단합니다.

○ 웹 소스코드 수정이 된 후에 다시 한 번 취약점 점검 때와 같은 시도를 통해 취약점이 존재하지 않는지 확인합니다.

5. SQL Injection

개요	웹브라우저 주소창, 이용자 ID 및 패스워드 입력화면 등에서 데이터베이스 SQL문에 이용되는 문자기호 입력을 필터링하지 않아서 SQL 조작에 의한 입력으로 데이터베이스에 인증절차 없이 접근하여 자료를 무단 유출하거나 변조할 수 있게 하는 취약점
점검범위	웹사이트의 기본적인 사용자 인증창 우회 SQL Injection 취약점 점검 방법을 이용하여 취약점 존재 가능성을 점검합니다.

점검방법

○ 홈페이지 관리자 로그인 페이지로 이동합니다.
○ 관리자 아이디와 패스워드에 아래 문자열을 입력하여 결과를 확인합니다.

① 'or 1=1;- - ② ' ' or 1=1- - ③ "or 1=1 -- ④ or 1=1-- ⑤ 'or 'a'='a ⑥ " or "a"="a	⑦ ')or('a'='a ⑧ sql' or 1=1- - ⑨ sql" or 1=1-- ⑩ + or 1=1- - ⑪ ';- -

○ 인증 실패 메시지가 나타날 경우, 'SQL Injection 취약성'은 존재하지 않습니다.
○ 로그인 될 경우, SQL Injection 취약점이 존재합니다.
○ 홈페이지 오류 메시지가 나타날 경우, SQL Injection 가능성이 있으므로 세부적인 점검이 필요하다는 것을 의미합니다.

조치방법

○ ID, Password 란에 특수문자(따옴표, 공백 등)을 입력하지 못하도록 소스코드를 수정합니다.
○ 웹 소스코드 수정이 된 후에 다시 한 번 취약점 점검 때와 같은 시도를 통해 취약점이 존재하지 않는지 확인합니다.

6. 쿠키 암호화

개요	쿠키 변조에 의해 불법적인 인증을 수행하여 웹서버에 접근하는 취약점
점검범위	쿠키정보를 통해 개인정보 노출 발생 여부를 확인하기 위해 쿠키정보가 암호화되어 저장되었는지를 점검합니다.

점검방법

○ 로그인을 수행합니다.
○ 웹 브라우저 주소 창에 javascript:document.cookie; 를 입력해서 내용이 암호화되었는지 여부를 확인합니다.

조치방법

○ 가장 효과적인 방법은 SSL과 같은 보안 서버 기능을 적용함으로써 로그인 트랜잭션 전체를 암호화하는 방법입니다.
○ 쿠키저장 시 타인이 임의로 쿠키를 읽을 수 없도록 도메인과 경로 지정에 유의해야 하며, 브라우저에 저장되는 쿠키방식보다는 서버 측에 일부 정보를 저장하여 상호 대조할 수 있는 세션 방식으로 대체하고 세션방식의 경우도 사용자의 IP 주소 등을 함께 저장하여 유효성 여부를 확인합니다.

7. 접근통제 취약점

개요	권한이 없는 이용자가 특정 경로를 통해 관리자 페이지나 DB에 접근할 수 있게 하는 취약점
점검범위	접근 통제의 기본이 되는 ID/PW 정보의 노출 및 관리자 홈페이지의 노출 여부를 점검합니다.
점검방법	
구글을 통한 점검방법	○ 구글 사이트에 접속합니다. ○ 고급 검색으로 이동합니다. ○ 도메인 설정에는 해당 홈페이지 주소를 입력하고 검색어 입력 박스에 다음을 입력하여 ID/PW 노출 및 관리자 홈페이지 노출 페이지를 찾습니다. - login | logon - password|passcode|비밀번호|“your password is"|"당신의 비밀번호는” - admin | administrator
직접 점검방법	○ 일반적으로 많이 사용하는 관리자 페이지 명을 입력하여 관리자 페이지가 존재하는지 점검합니다. - http://admin.test.go.kr - http://www.test.go.kr/admin/ - http://www.test.go.kr/manager/ - http://www.test.go.kr/master/ - http://www.test.go.kr/system/ ○ 이용자 인증을 통과하여 페이지에 접속한 후, 인증과정 없이 중간 페이지에 접속하여 접속이 가능한지 점검합니다.

조치방법	
구글 캐쉬에 노출된 경우	○ 개인정보 취약점 페이지가 구글에 노출된 경우에는 먼저 홈페이지에도 개인정보 취약점 노출이 있는지 여부를 확인하여 홈페이지의 개인정보 취약점을 제거 한 후, 구글 검색 사이트에 해당 캐쉬에 대해 삭제를 요청하는 이메일을 발송합니다. ○ 검색엔진 배제표준을 이용하여 개인정보가 포함된 주소를 지정하는 robot.txt 파일을 만들어 서버 루트 디렉토리에 저장하거나 해당 페이지의 HTML 안에 메타태그를 입력합니다. ○ 개인정보의 노출 정도가 심각하여 긴급하게 노출을 방지하고자 한다면, 구글의 자동 URL 삭제 시스템을 이용하여, URL이 검색되지 않도록 합니다. 구글 자동 URL 삭제 시스템: http://services.google.com:8882/urlconsole/controller?cmd=reload&lastcmd=login
직접 점검을 통해 노출된 경우	○ 직관적으로 접근할 수 없도록 관리자 호스트 IP 만 접근 가능하도록 설정합니다. ○ 웹 관리자 메뉴의 접근을 특정 네트워크 대역으로 제한하여, IP 주소까지도 인증 요소로 체크하도록 웹 관리자 사용자 인터페이스를 개발하고, 관리자 인증 후 접속할 수 있는 페이지의 경우 해당 페이지 주소를 직접 입력하여 접속하지 못하도록 관리자 페이지 각각에 대하여 관리자 인증을 위한 세션 관리를 합니다.

Ⅳ 개인정보 노출 방지대책

1. 개인정보 노출방지를 위한 관리방침 제정 및 운영

홈페이지를 통한 개인정보 노출을 방지하기 위해서는 이를 위한 기술적, 관리적인 정책 및 방침을 미리 지정하여 운영하는 것이 무엇보다도 중요합니다. 이 방침에는 다음 사항이 포함되어야 합니다.

1) 관리 대상인 개인정보 항목
2) 관리적용 범위(관리 홈페이지 범위)
3) 노출방지 체계
4) 노출 발견 시 조치 절차
5) 상시/즉시 노출관리를 위한 방법
6) 관리 이력 내용 및 작성 양식
7) 점검 보고서 예시

또한, 지정된 관리방침에 따라 노출방지를 위한 프로세스를 상시 운용하며, 환경적인 변화 등 필요에 따라 현실을 반영하여 방침이 업데이트하도록 하여야 합니다.

2. 3단계 노출방지 관리

개인정보의 노출은 개인정보가 포함된 콘텐츠 업로드를 통해 노출이 발생하는 생성단계, 생성된 콘텐츠가 지속적으로 저장되어 홈페이지를 통해 서비스되는 저장단계, 구글과 같은 외부 검색엔진에 의해 수집되어 제공되는 제공단계 등의 3단계를 통해 발생합니다. 따라서 이 **3가지 단계에 적합한 체계적인 노출방지 관리가 수행되어야 합니다.**

<<3단계 노출방지 관리>>

단 계	설 명
생성단계	□ 먼저, **생성단계를 관리하기 위해서는 "개인정보 점검필터" 를 적용**합니다. □ 개인정보 점검필터는 홈페이지 이용자가 게시물을 게재하는 시점에서 개인정보 포함여부를 점검하는 기능을 수행합니다.
저장단계	□ **저장단계를 관리하기 위해서는 "스캐너" 를 운용**합니다. □ 스캐너는 웹 검색엔진으로 홈페이지 내의 모든 콘텐츠를 검색하여 개인정보를 포함하고 있는 콘텐츠가 존재하는지 여부를 확인하여 이를 관리자에게 알려주는 기능을 수행합니다.
제공단계	□ **제공단계를 관리하기 위해서는 "구글 스캐너" 를 운용**합니다. □ 구글 스캐너는 구글 DB 내에 저장되어 있는 관리 사이트의 콘텐츠 중 개인정보가 포함된 콘텐츠를 점검하여 관리자에게 알려주는 기능을 수행합니다.

● 최근 일부 개인정보 관리자들은 개인정보 노출을 방지하기 위해서 **사전에 차단을 하는 개인정보 점검필터만을 이용하는 것으로 완벽한 방지대책이 수립된 것으로 오해**하는 경우가 많은데, 이는 매우 위험한 생각입니다. **그 이유는…**

각 홈페이지에서 개인정보 점검필터를 운용할 때, 개인정보가 발견된 해당 콘텐츠를 무조건 차단하는 "차단 정책"보다는 개인정보가 발견되면 이를 이용자에게 고지하여 이용자가 게재 여부를 판단하도록 하는 "고지정책" 이 현실적으로 적용되고,

개인정보가 포함된 콘텐츠를 관리자가 처리할 때까지 홈페이지 내에서 해당 웹페이지의 자기복제(URL 생성) 및 구글 등 외부 검색엔진에 저장되는 과정이 반복되기 때문입니다.

3. 휴면 사이트 일제 점검

관리자는 관리하는 웹서버 내에 잔존하는 휴면 사이트가 존재하는지 여부를 전체적으로 확인하여 이에 대한 삭제 조치를 취해야 합니다. **휴면 사이트 점검을 위해서**

> 먼저 관리하는 웹서버들의 물리적인 위치를 파악하여 해당 웹서버에 저장된 콘텐츠 내용들을 점검하는 것 뿐 아니라, 관리 도메인에 대한 원격 스캐닝을 통해 개인정보 포함여부를 점검합니다.

4. 노출관리 체계 구축

홈페이지에서 개인정보 노출이 발생하는 경우, 관리자는 이를 즉시 파악하여 조치를 취할 수 있어야 하는 것이 무엇보다 중요합니다. 이를 위해서는 각 홈페이지 개인정보 노출 관리를 위한 상시적이고 즉각적인 조치를 취할 수 있는 관리가 필요합니다. **상시적인 관리를 위해서는**

> 기관 홈페이지에 대한 개인정보 노출 상시 모니터링이 가능한 체계를 구축하여야 하며, 노출발생 시 관리자가 이를 즉시 파악하기 위해서는 노출 발견 시 이메일이나 SMS로 관리자에게 즉각적으로 원격 통보될 수 있도록 운영해야 합니다.

5. 홈페이지 설계 오류 정비

홈페이지의 구조적인 문제가 발생하면 다량의 개인정보 노출이 발생할 가능성이 있으므로 홈페이지 구조상에 개인정보 노출 위험이 없는지에 대해서 점검하고 정비를 해야 합니다. **홈페이지 보안 구조 정비를 위해서는**

먼저 각 웹페이지의 모든 접근 경로에 대한 접근권한별 인증 기능이 적용되었는지 여부를 확인하고, 인증에 활용되는 개인정보가 공개되지 않도록 하는지 여부를 점검하여야 합니다. 뿐만 아니라, 향후 홈페이지 개인정보 노출 가능성을 방지하기 위해서는 이용자들이 쉽게 접근할 수 있는 널리 알려진 웹 보안취약점 진단방법을 이용하여 홈페이지 설계단계의 오류를 정비하여야 합니다.

6. 홈페이지 이용자 주의사항 안내

홈페이지는 이용자들에 의해 콘텐츠가 생성되는 만큼 이용자들의 마인드가 무엇보다도 중요합니다. 따라서 **각 홈페이지 담당자는** 게시물에 개인정보가 포함되지 않도록 해당 기관의 내부 직원들을 대상으로 정기적인 교육을 실시하고, **민원인 등의 개인정보 노출에 대한 계도를 위해서** 업로드하는 게시판에 주의사항을 고지하여 개인정보 노출에 주의하도록 해야 합니다.