**프로젝트 수행중**

**보고서 작성 Tip**

*목 차*

[1. 수행 3](#_Toc492396735)

[1.1. 스크린샷 저장은 최대한 자세히 3](#_Toc492396736)

[1.2. 보고서는 그날그날 3](#_Toc492396737)

[2. 템플릿 4](#_Toc492396738)

[2.1. 만든 이, 마지막으로 저장한 사람, 스타일명 4](#_Toc492396739)

[2.2. 잘된 템플릿 그냥 쓴다? 6](#_Toc492396740)

[2.3. 새 문서 줄 간격 6](#_Toc492396741)

[2.4. 다음장 넘기기 : Ctrl+Enter? 6](#_Toc492396742)

[3. 그림 7](#_Toc492396743)

[3.1. 캡쳐 찍는법 크게/글자크기는 본문이랑 7](#_Toc492396744)

[3.2. 스크린샷 오피스에서 자르기 8](#_Toc492396745)

[4. 글자 9](#_Toc492396746)

[4.1. 오탈자?->office, 네이버 9](#_Toc492396747)

[4.2. 색깔/볼드/이탤릭/언더바 9](#_Toc492396748)

[5. 검토 10](#_Toc492396749)

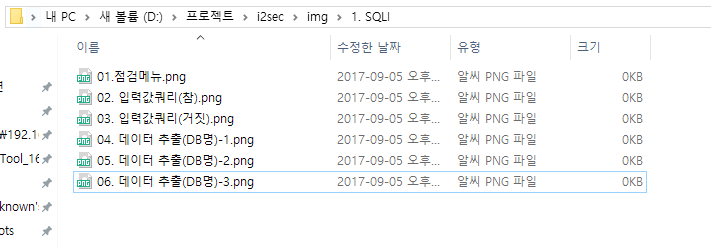
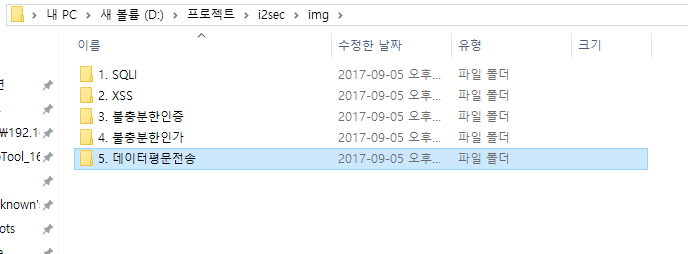
[5.1. 프린트해서 볼 것 10](#_Toc492396750)

[5.2. 상위자 검토는 꼭! 10](#_Toc492396751)

# 수행

## **스크린샷** 저장은 최대한 자세히

스크린샷은 나만 보는 게 아닙니다. 차후에 증적 자료로 PM이나 고객에게 전달할 수도 있고, 다음번에 진단할 이행점검자에게 전달할 수도 있습니다. 혹은 보고서를 다시 수정할 미래에 나에게 전달할 수도 있습니다. 스크린샷을 저장할 때는 폴더별로 조금 더 신경 써서 저장합니다.



## 보고서는 그날그날

1. 보고서 작성을 미루면 그 사이 페이지가 변경되는 경우가 꽤 자주 일어나므로 그날 작업한 것은 그날 작성하는 습관을 길러야 합니다.

* 개발계에서 테스트하는 경우 더욱더 그렇고,
* 일부 금융권에서는 담당자가 관제가 얼마나 잘 잡는지 보려고 알리지 않아, 관제에서 패턴을 막는경우도 있습니다.
* 혹은 홈페이지 담당자가 게시글이나 공격 증적을 보고 그날 막아버리는 경우도 있습니다.

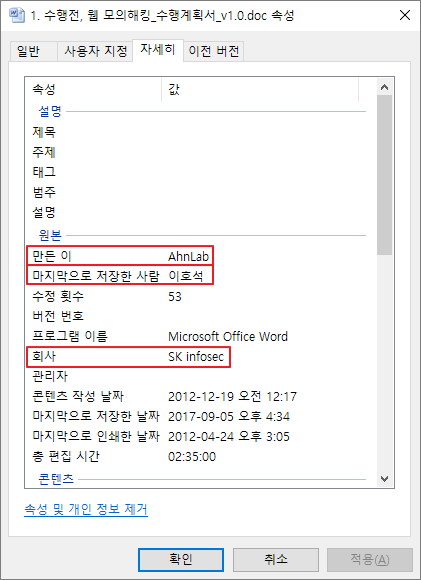
1. 데이터 평문 전송의 경우 이미지가 아닌 패킷 파일(pcap등)을 별도로 저장해 둡니다.
2. 포트스캔 결과는 nmap이나 xml로 따로 저장해 둡니다.

# 템플릿

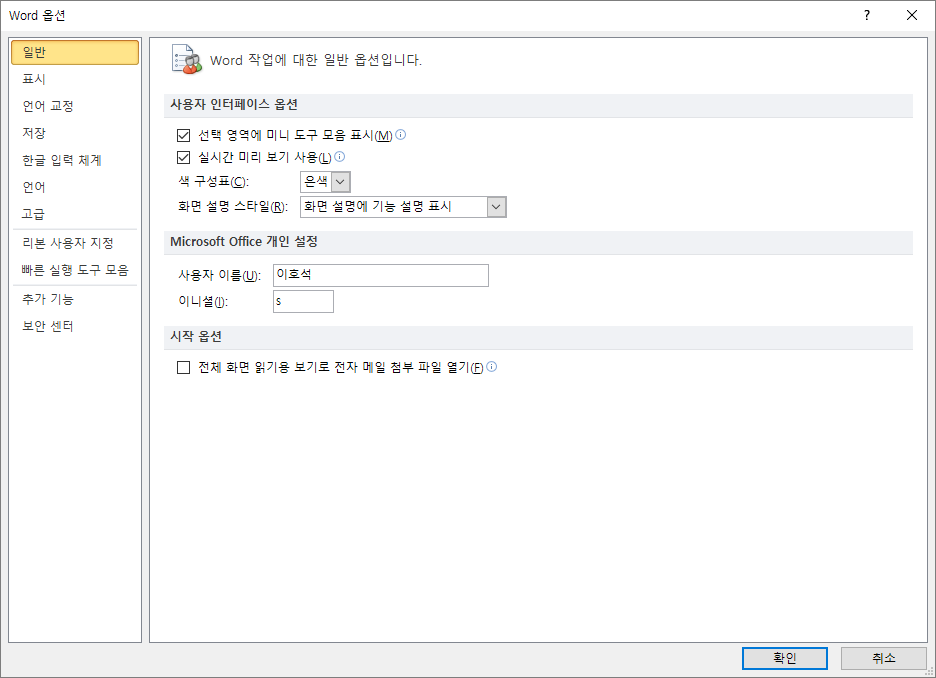
## 만든 이, 마지막으로 저장한 사람, 스타일명

위 3가지 사항이 타 컨설팅업체나 고객사명등으로 되어 있는경우가 있습니다. 이는 다른 업체의 문서를 배꼈다고 대놓고 광고하는 것이므로 꼭 주의하도록 해야합니다.

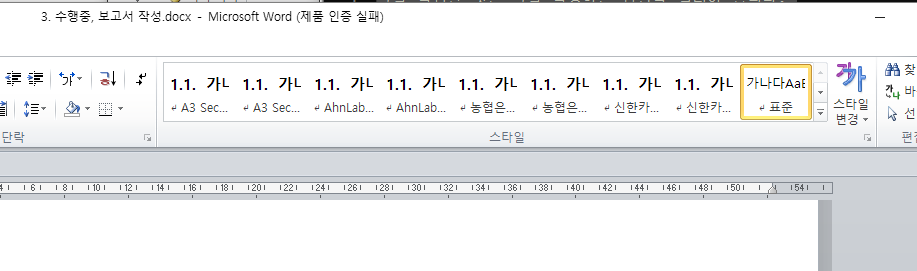
* 파일 우클릭 > 속성에서 확인시 “만든 이, 회사”가 타 컨설팅 업체로 되어 있는 경우 : 속성에서 만든이 수정이 가능합니다.



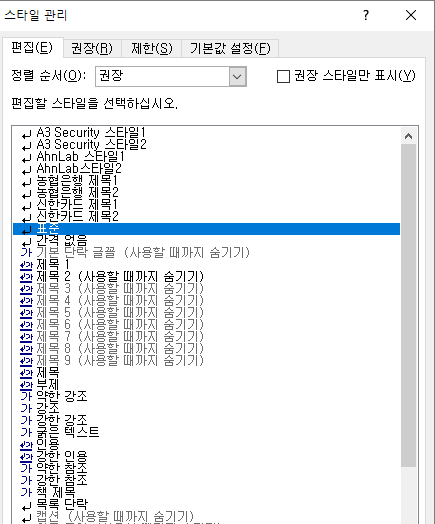
* 파일 우클릭 > 속성에서 확인시 “마지막으로 저장한 사람”이 타인에 이름으로 저장되어 있는 경우 : 워드 옵션에서 이름 변경 후 저장시 갱신됨



* 빠른 스타일에 타 컨설팅 업체명이나 다른데서 수행한 고객사명이 명시되어 있는 경우 : 삭제 후 본인이 다시 만들어서 사용합니다.



* 빠른 스타일에는 보이지 않지만 스타일 관리에 타 컨설팅 업체명이나 다른데서 수행한 고객사명이 명시되어 있는 경우 : 삭제 후 본인이 다시 만들어서 사용합니다.

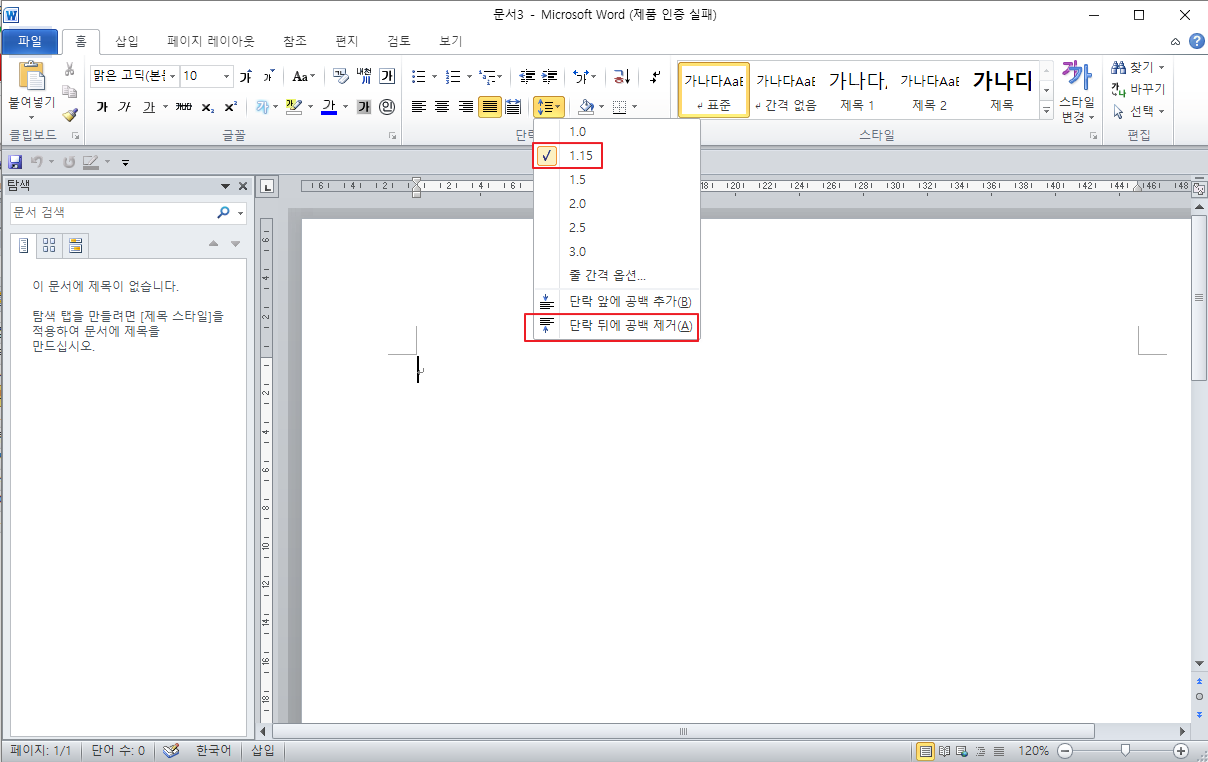


## 잘된 템플릿 그냥 쓴다?

잘된 템플릿을 그냥 쓰기만 하면 절대 소프트스킬이 늘지 않습니다. 처음에는 시간이 걸리더라도 새문서를 열고 템플릿과 똑같이 만드는 연습을 해야합니다.

## 새 문서 줄 간격

새 문서를 만들면 줄 간격이 굉장히 넓게 설정되어 있습니다. 줄 간격은 1.15에서 1.0으로, 단락 앞뒤 공백은 제거해줍니다.

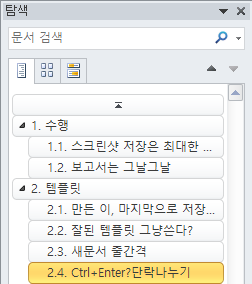
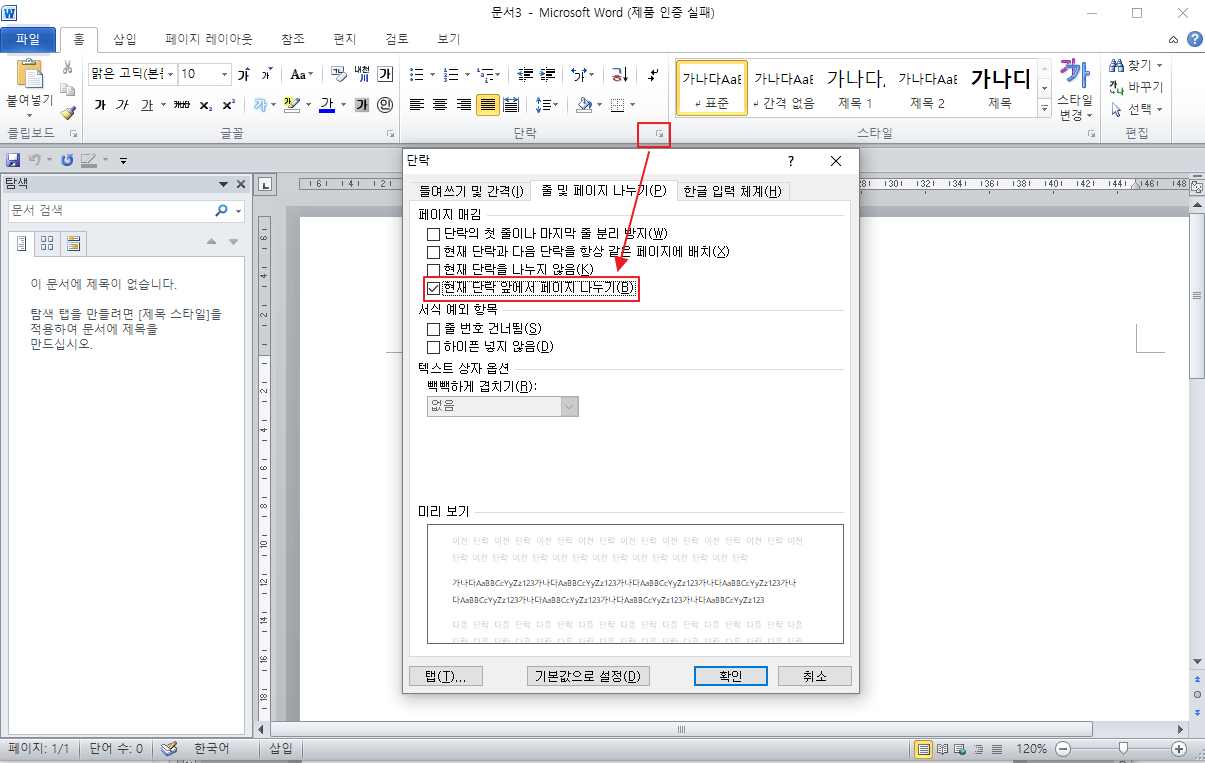


## 다음장 넘기기 : Ctrl+Enter?

다음장으로 넘길 때 Ctrl+Enter를 입력하고 제목 입력시, Office 2007 탐색창에서 제목이 사라집니다.

Ctrl+Enter대신 “단락 > 줄 및 페이지 나누기 > 현재 단락 앞에서 페이지 나누기” 기능을 이용해서 다음장으로 넘겨줘야 합니다.

(※. 위의 경우 Office 2007에 버그인데 폐쇠된 OA망의 경우 패치를 하지 않고 사용하는 경우가 있어 Office 2010을 사용하는 컨설턴트는 잘 보이지만, Office 2007을 사용하는 담당자는 탐색창이 이상하게 되어 있는 경우가 있습니다.)

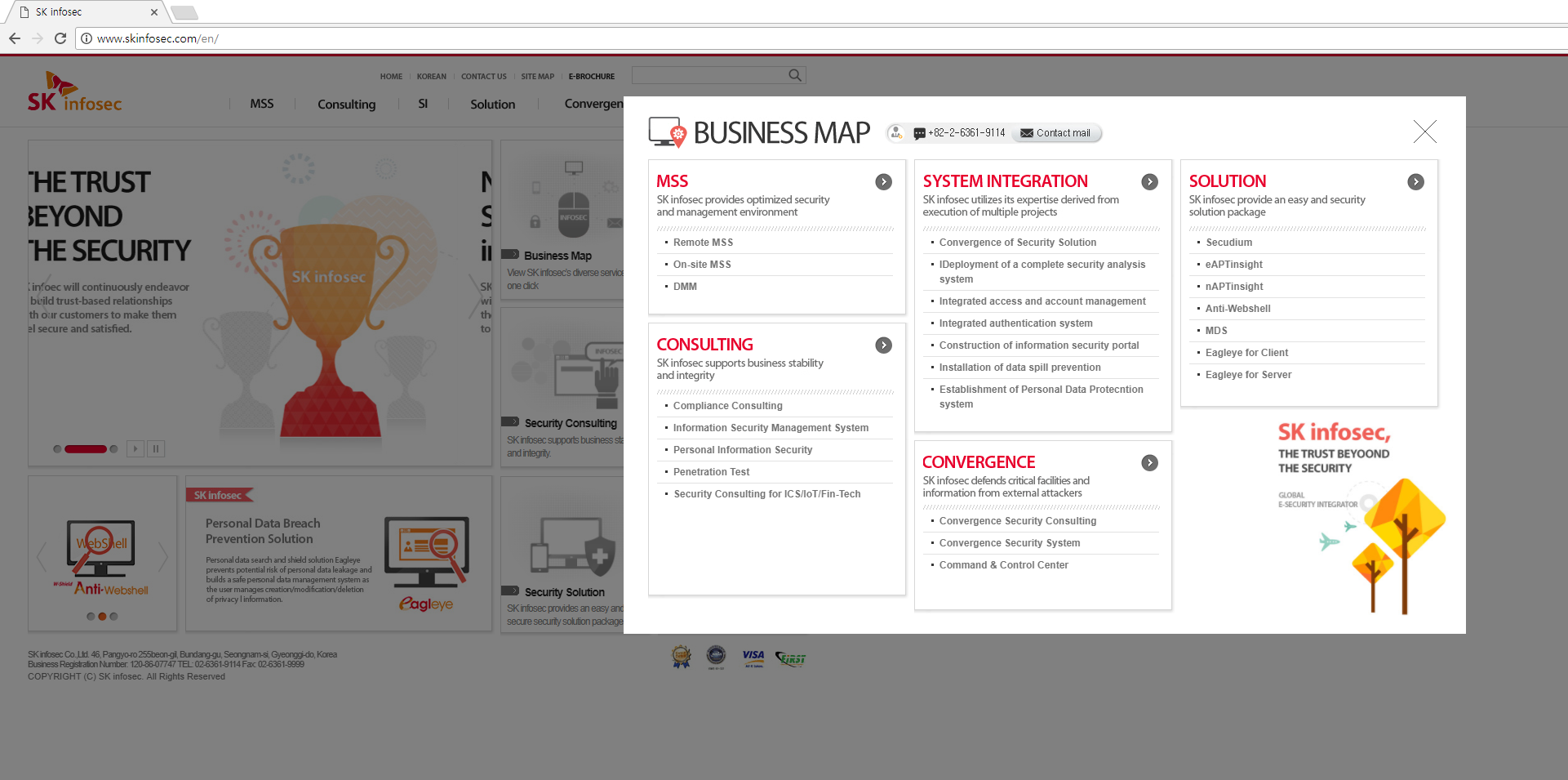
# 그림

## 캡쳐 찍는법 크게/글자크기는 본문이랑

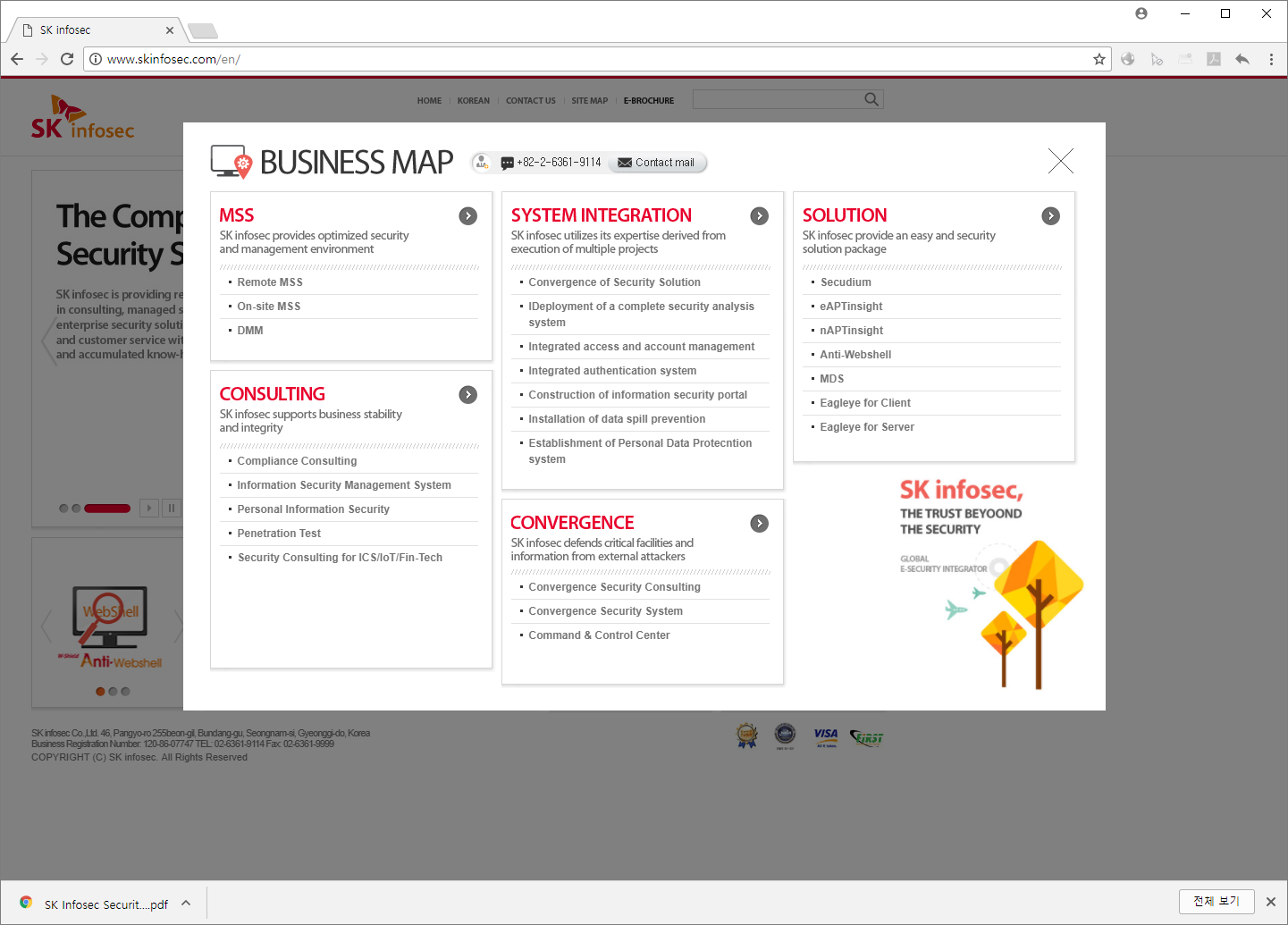
워드에서 편집하려고 이미지를 무조건 크게 찍는 것은 바람직하지 않습니다.

그림 이미지에서 보이는 글자와 워드글자크기가 비슷한 것이 잘 작성된 보고서입니다.

* 팝업 앞/뒤 화면이 둘 다 출력되어야 하는 스크린샷의 경우(ex. XSS : 메뉴에 전반적인 화면과 alert창이 보여져야하는 형태) 전체화면으로 찍으면 팝업창 위치 때문에 전체화면을 다 넣어야합니다. 이럴 경우 글자크기가 너무 작아져 스크린샷을 다시 찍어야합니다.



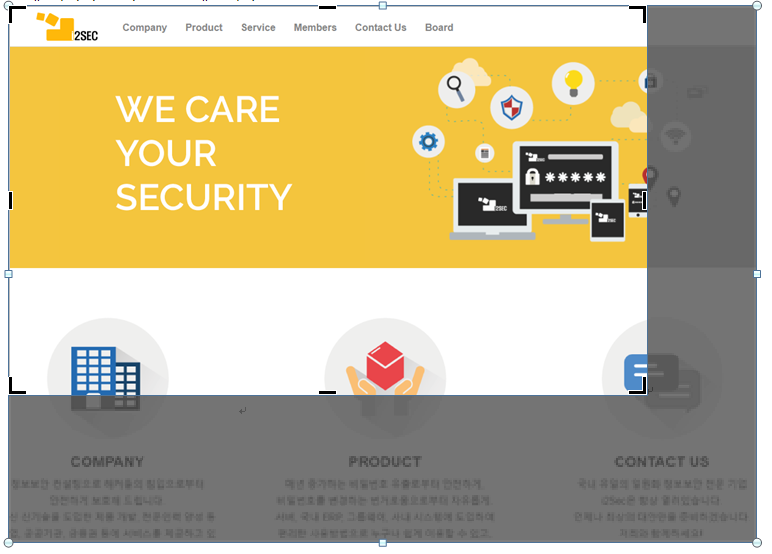
따라서 본문에 들어갈 폰트크기를 생각해서 이미지를 찍어야합니다.



## 스크린샷 오피스에서 자르기

스크린샷을 잘라서 넣으면 최종 검토자가 편집하기 어렵습니다. 스크린샷을 워드 본문에 넣은 후 자르기 옵션을 통해 이미지 크기를 조정해줍니다.

(이렇게 자르기 기능을 통해 이미지 크기를 조절해야 워드에 불필요한 여백을 조정할 수 있습니다.

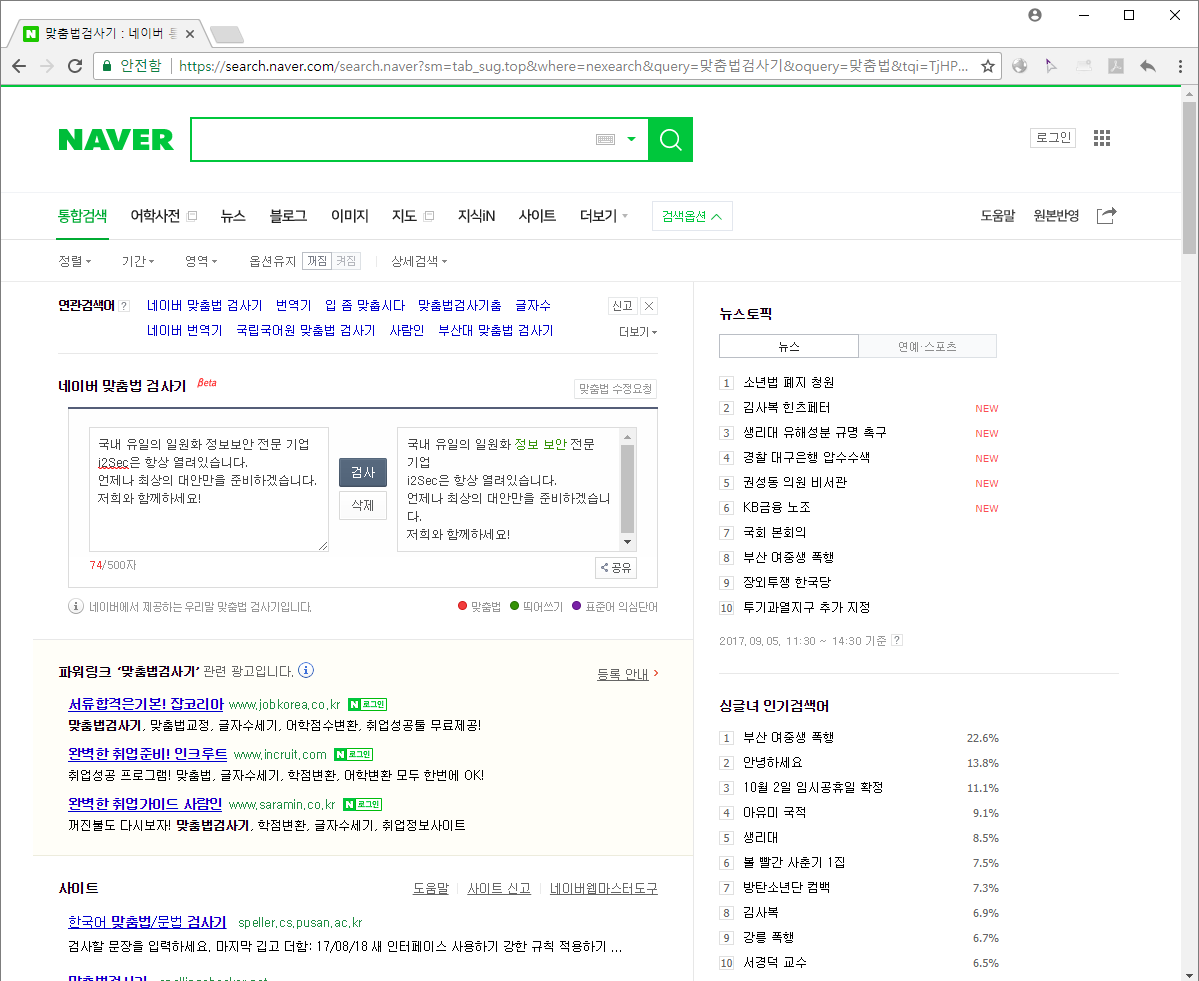


# 글자

## 오탈자?->office, 네이버

오탈자는 워드에서 보이는 빨간 줄이 70%정도 걸러줍니다. 하지만 빨간줄이 오탐인 경우도 있고, 30%의 미탐의 경우를 찾으려면 좀 더 정확한 도움이 필요합니다.

* 네이버 맞춤법 검사기 추천



## 색깔/볼드/이탤릭/언더바

* 색깔은 뉴스에 나올정도의 크리티컬한 취약점이 아닌 경우 모두 검정색을 쓰는게 좋습니다. 붉은 계열을 쓰면 그 글자가 너무 강조되어서 다른 본문이 묻힙니다.
* 강조가 필요한 문구는 볼드정도가 적당하고,
* 이탤릭은 목차등의 개요의 제목 구성 외에는 거의 사용하지 않습니다.
* 언더바의 경우 구분이 잘 되지 않을 때 많이 사용합니다.

# 검토

## 프린트해서 볼 것

보고서는 모두 작성 후 꼭 프린트 해보는 것을 강력하게 추천합니다. 모니터로 볼 때 오탈자, 문맥상 수정사항이 하나도 없어보이는데, 출력하면 꼭 나타납니다. 프린트비 아끼지 말고, 고객의 신뢰를 얻으세요.

## 상위자 검토는 꼭!

수행경험이 2년이하일 경우 차상위자에게 꼭 검토를 받으시기 바랍니다. PM이 프로젝트의 책임자이긴 하지만, 보고서에 들어가는 이름은 본인이라는 것을 상기하시기 바랍니다. **남는건 보고서 산출물 1개뿐입니다.**

# 보안가이드

## 보안가이드는 동일하니, 복사/붙여넣기?

파라미터 변조와 같이 매 상황이 다른 경우는 보안가이드가 매번 다르겠지만, XSS취약점과 같이 보안가이드가 비슷한 경우는 복사/붙여넣기 하는게 맞지 않냐는 생각이 들 수 있습니다.

XSS취약점이 발견된 경우, 미리 작성된 필터링 로직을 포함 할 수는 있습니다. 하지만, 이 필터링 로직을 왜 넣어야하는지 현재 홈페이지에 현상을 분석한 컨설턴트/진단자의 시각이 들어간 상세한 내용이 꼭 들어가야합니다.

* 현재 서버측 상황 : 예를 들어 XSS의 보안대책은 근본적인 해결책, White List Filter, Black List Filter 방식 이렇게 3개로 구분할 수 있는데, 현재 상태는 어떤것에 해당하고,
* 상세 현황 : 이 상황 중 (ex, Black List Filter라고 가정) 대부분의 패턴이 막혀있는데, img태그에 EventHandler API가 몇 개 누락되었습니다.
* img 태그에 EventHandler를 추가하여 XSS를 막는 방법이 있지만 근본적인 해결책은 다음과 같습니다.

와 같은 XSS에 대한 보안지식이 없는 초급 개발자도 조치할 수 있도록 쉽게, 그리고 자세히 써야합니다.

상세내용(Step별로 취약점의 현황을 작성한 것)을 2페이지 작성하였다면, 보안가이드는 1페이지 이상 작성할 수 있도록 구성해야 합니다.

# 보고서 잘 포장 하는법

각각의 보고서를 보고 피드백을 드리는 것이 가장 효과적이지만, 전반적으로 취약점은 잘 찾는데, 보안담당자나 PM이 보기에 별로 중요한 취약점이 아니라는 생각이 든다는 보고서라고 가정하고, 전반적인 내용에 대해 얘기해보겠습니다.

## 위험도 기준 수립

SQLI이 위험하다는 것은 누구나 알고 있습니다. 하지만 파라미터 변조, XSS가 위험하다고 어떻게 설득할 수 있나요? 진단자에 감으로 이건 위험한 것 같다라는 뉘앙스에 얘기는 아무리 길고 잘 써도 와닿지가 않습니다. 왜 그럴까요? 논리적이지 않기 때문입니다. 어떤 근거나 기준에 의해서 이 취약점은 “상”입니다. 와 같은 기준이 있어야 납득이 가능하고 신뢰할 수 있다는 말입니다.

아래 예시와 같이 위험도를 보고서에 명시하고, (예시이니 그대로 사용하지 마세요. 프로젝트 성격, PM/고객성향에 따라 바뀔수 있습니다.) 취약점마다 위험도를 표기하시기 바랍니다.

|  |  |  |
| --- | --- | --- |
| **위험도** | **내용** | **예시** |
| 상 | ｏ 서버 장악 / 네트워크 침입이 가능한 취약점 ｏ 개인 정보의 대량 유출 가능한 취약점 | ｏ 웹쉘 업로드 / SQL injection ｏ DB 정보 / 서버 계정 노출 ｏ 인가/인증 미비로 인한 타 사용자의 개인정보 대량 열람 가능 |
| ｏ 금전적 피해가 발생 가능한 취약점 | ｏ 상품 결재 시 가격 변조 ｏ 계좌 이체 / 계좌 조회 관련 취약점 ｏ 금융 사이트의 계정 도용 |
| 중 | ｏ 위험도가 높은 정보의 소규모 노출 | ｏ 개인정보가 1건씩 소규모로 유출 가능한 경우 ｏ Stored 방식의 XSS ｏ 파일 다운로드 취약점 |
| ｏ 웹 사이트의 기능을 개발 의도에 부합하지 않게 오용 가능한 취약점 | ｏ 인가 / 인증 미비로 인하여 허가되지 않은 기능의 무단 접근 및 실행 게시판 변조 |
| ｏ "상" 등급 취약점 공격에 이용될 수 있는 취약점 | ｏ 모든 취약점 해당 |
| 하 | ｏ 발생될 조건이 까다롭거나 발생될 확율이 낮은 취약점 | ｏ Reflected 방식의 XSS ｏ 세션 고정 ｏ 중요 정보 평문 전송 |
| ｏ 자체로는 영향도가 없으나 2차 공격에 활용될 가능성이 있는 취약점 | ｏ 에러 처리 미비 ｏ 위치 공개 |
| 권고사항 | ｏ 보안 지침 / 기준에 위배되는 사항 ｏ 관리 영역의 위험도와 매핑이 필요할 경우, 사항에 따라 개별 평가하여 "하"로 평가하거나 취약점에서 제외한다. | ｏ 약한 문자열 강도 ｏ 관리자 페이지 노출 |

## 취약점 요약, 위험도, 위협 명시

취약점에 대한 상세내용 윗부분에 표로 취약점 요약, 위험도, 위협을 각각 1~2줄 내외로 작성해주세요. 실무담당자 1,2명외에는 이 표만 보게 되니 표에 취약점 내용이 함축될 수 있도록 잘 작성해주세요.

위협에는 이 취약점으로 인해 발생할 수 있는 정보, 피해, 연계취약점등을 작성하면 되는데 2~3단계 너무 나아가서 소설을 쓰면 신뢰도가 떨어집니다.

## 강조하고 싶은 취약점의 상세내용 컨텐츠

상세내용에는 단순히 FACT만 쓰는 것이 맞지만, 보고서 중 강조하고 싶은 부분에는 위협에 명시할 내용을 좀 풀어서 써주는것도 괜찮습니다.

ex) XSS의 경우 BeEF와 같은 해킹툴과 연계하여 악성 URL을 사용자가 클릭하면, 사용자 Client의 취약한 소프트웨어 취약점을 이용해 사용자Shell획득이나 페이스북/구글 가짜 로그인 페이지 유도등 다양한 공격이 가능합니다

덧) 에러처리의 경우 .net일 경우 iis short name이나 403, 404반응에 따른 홈페이지 구조 파악등

## 같은 단어 다른 느낌

파라미터 변조보다는 권한 상승이라는 단어가 보고받는 입장에서는 의미전달이나 위험도 파악에 도움이 됩니다. 이처럼 좀 더 자극적이지만 왜곡되지 않은 단어를 잘 선택하여 문장을 윤색해주시기 바랍니다. 단어 하나가 이 취약점 전체에 색깔을 결정 할 수 있습니다.

## 같은 취약점 다른 느낌

예를 들어, 내부망의 메일 서버에서 타사용자 메일 수/발신함을 읽는 것이 가능한 취약점이 나왔다고 가정할 때, 테스트 사용자, 담당자의 수/발신 목록보다는 좀 더 윗직급의 정보로 작성하시기 바랍니다.

내부망의 경우 사내메신저나 그룹웨어등 내부사용자 정보를 얻을수 있는 채널이 많습니다. 이를 이용해 좀 더 윗직급자의 수/발신 목록을 모자이크 처리하여 보고서에 명시하세요. 대표님이나 CISO도 좋습니다.

(대표님이나 CISO로 작성하면 200% 보안담당자가 더 낮은 직급으로 수정해달라고 하겠지만, 취약점의 위험성에 대해서는 100마디 말보다 더 효과적입니다.)

## 총평

총평 위치는 상세 내용보다 위에 있지만, 작성은 가장 마지막에 합니다.

* 큰그림 : 상세내용에 각자 발생할 수 있는 위험이나 위협에 대해 작성하였다면, 총평에는 이 취약점들이 모였을 때 어떤 사고가 일어날 수 있는지에 대한 큰그림에 대한 내용이 들어가야 합니다. 이 내용을 쉽게 이해시키기 위해 실제 그림을 그려도 좋고, 일부 취약점을 예시로 들 수 있습니다.
* 다각도 : 총평에 전반적인 평 외에도, 가장 Critical한 취약점, 장점, 단점, 주요취약점에 대한 summary, 취약점 항목 대비 취약점 나온 비율, 위험도 상,중,하가 몇 개 등 여러 시야에서 본 대상의 분석내용을 담을 수 있어야 합니다.