TEIREN

보안 취약점 진단 이해

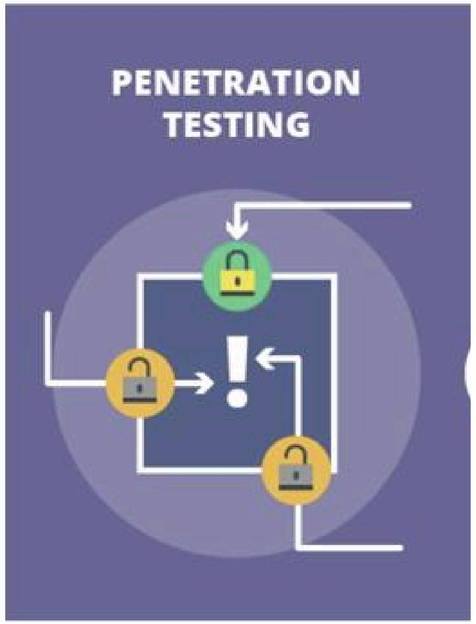
Assessment
VS
Pentest

Assessment VS Pentest

- 국내에서 혼용되고 있으나, 모의해킹(침투테스트)과 취약점 분석평가는 다른것
  - 일반적으로 웹 모의해킹= 웹분야 취약점 분석평가

Wide

Depth



Assesment VS Pentest

취약점 분석 평가(Vulnerability Assessment)

- 체크 리스트 기반으로 웹 사이트를 점검
- 발견된 취약점에 대한 평가(취약 항목 및 위험도 산정)
- 발견된 취약점에 대한 조치 가이드
- 다양한 취약점을 식별하고 평가

모의해킹(침투테스트, Penetration Testing)

- Exploitation & POST Exploitation
- 시나리오 기반으로 실제 해킹 가능성 점검

Assesment VS Pentest

취약점 분석 평가

- 컴플라이언스관점
- 체크리스트점검
- 최대한많은취약점(Vulnerability)을 식별
- 추가공격X

모의해킹

- 해커의 관점에서 모의로 해킹
- 최대한 크리티컬한 취약점을 식별
- 시나리오 기반
- 추가 공격 시도
- 취약점이 위협(Threat)에 의해 위험(Risk) 으로 이어질 수 있는지 점검

Assesment VS Pentest

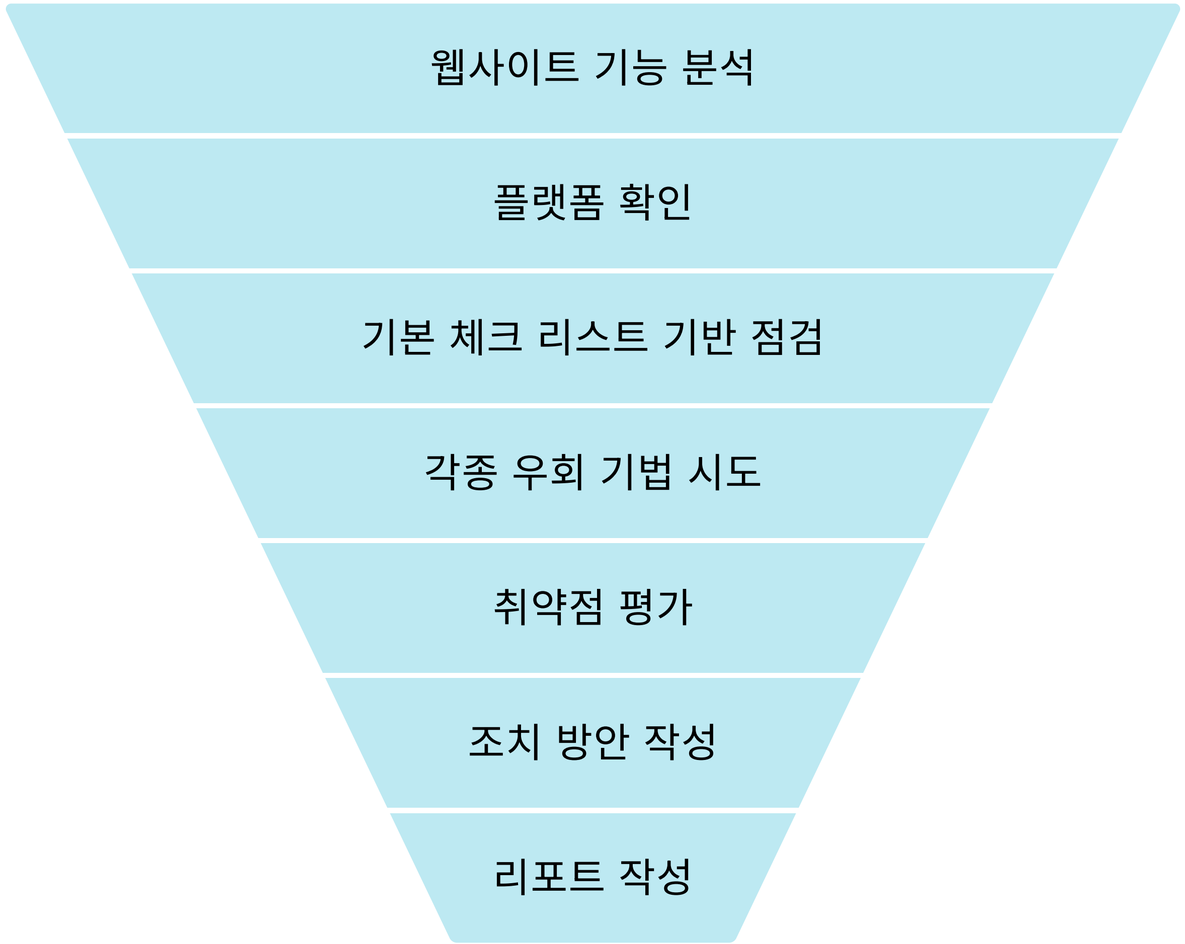
취약점 분석 평가

- 크로스 사이트 스크립팅 2건 (위험도 3)
- SQL 인젝션 1건 (위험도 5)
- 정보 노출 3건(위험도 2)

모의해킹

1. 고객정보 탈취 후 외부망 무단 반출
2. 와이파이망을 통한 무선 침투 후 내부망 악성코드유포
3. CVE취약점을 이용한 서버 접근 권한 획득 및 거점 확보
4. 프린터 취약점을 이용한 관리자 권한 획득 및 개인정보 획득

웹 취약점 분석 평가 절차



웹 취약점 분석 평가 절차

웹 사이트 기능 분석

- 사이트 가입 및 고객으로 서비스 이용
- 전자금융, HTTPS 등 확인
- 개인 정보 보관 여부 확인
- 사이트에 전반적으로 익숙해지는 시간
- 보안 솔루션 작동 여부 확인

플랫폼 확인

- 웹사이트 언어(Java/Rails/Django…)
- 프론트엔드 프레임워크 사용 유무
- 템플릿 사용 유무
- 웹 서버 플랫폼 확인(Win or Nix)

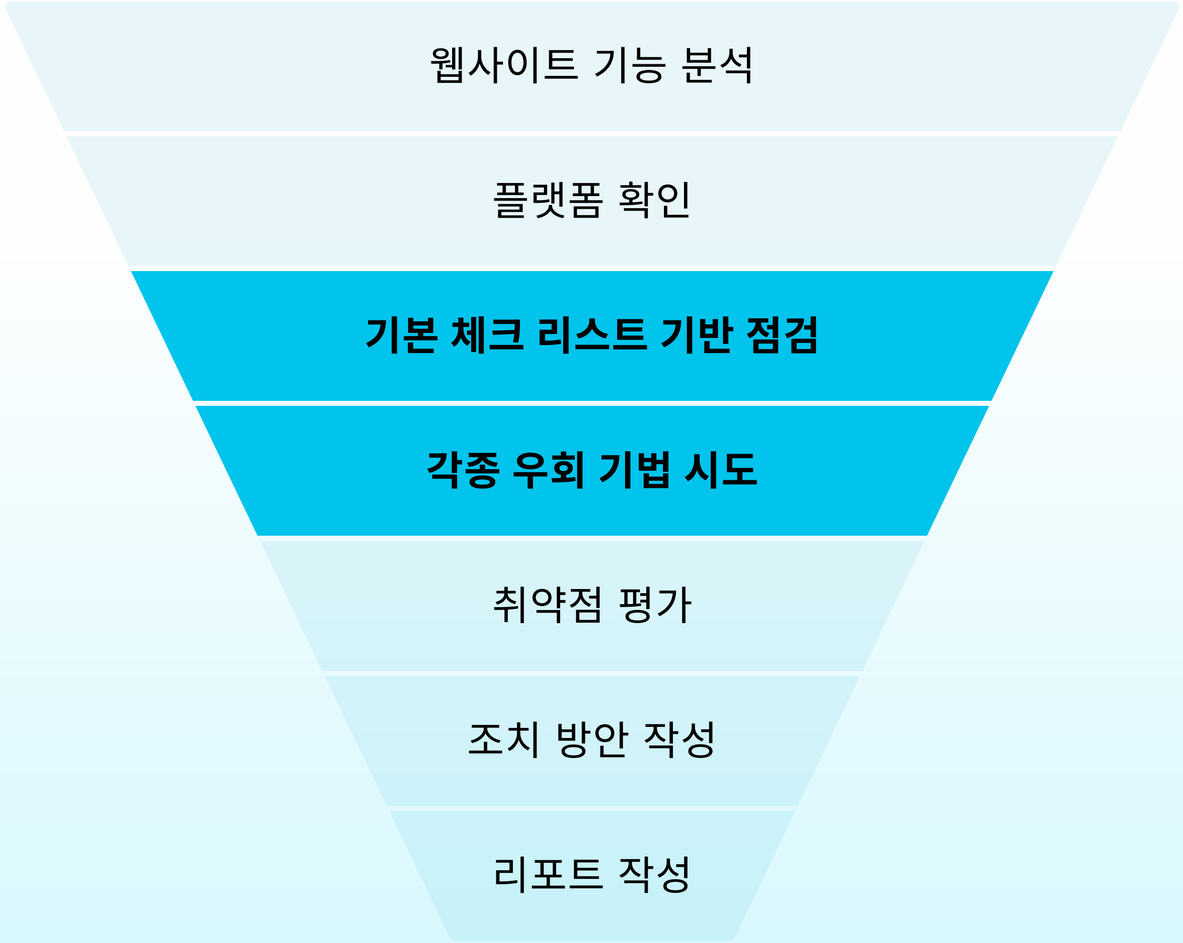
웹 취약점 분석 평가 절차

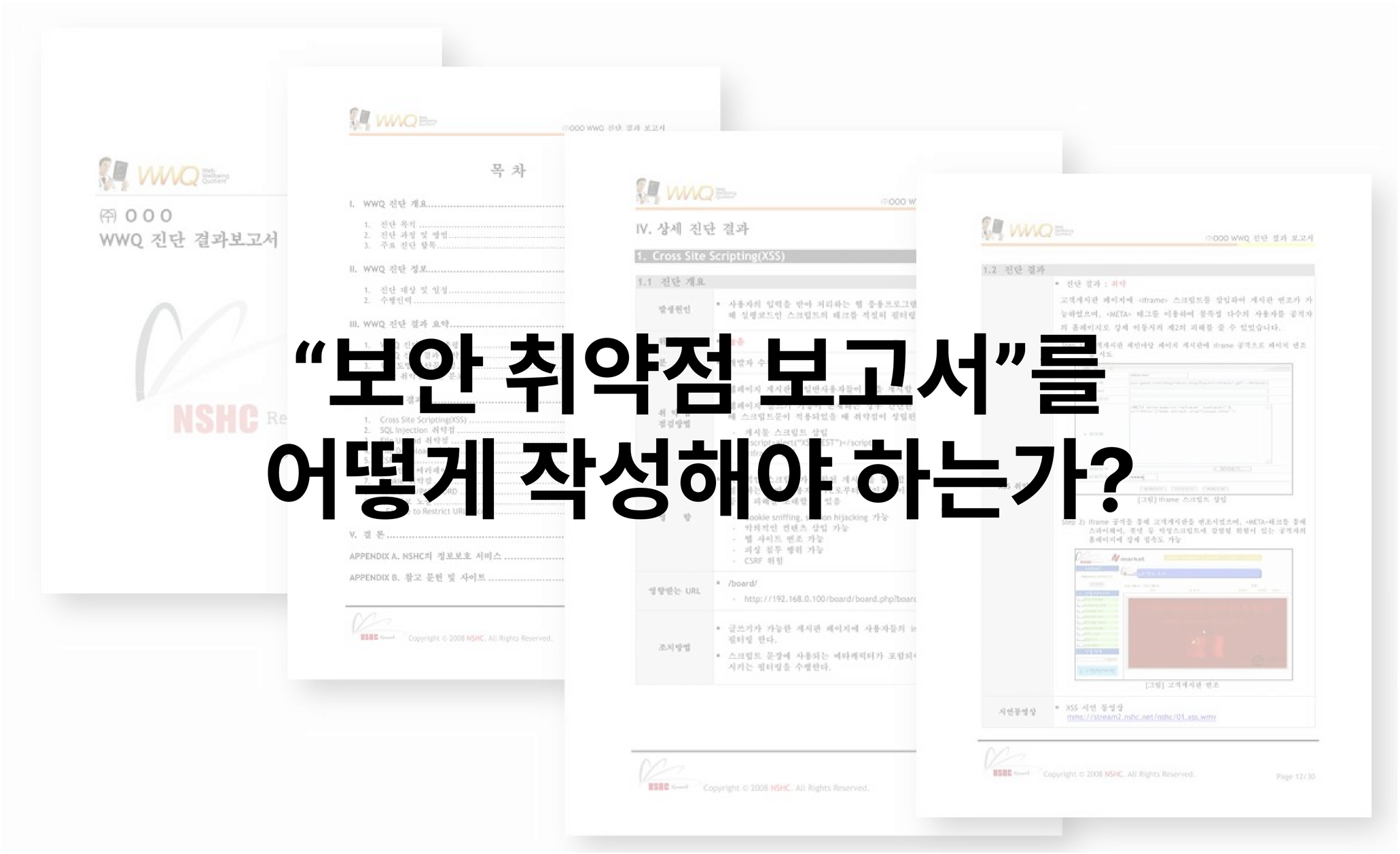
기본체크리스트기반점검

- XSS, CSRF
- SQL Injection
- 정보노출
- 인증및인가
- TLS 항목

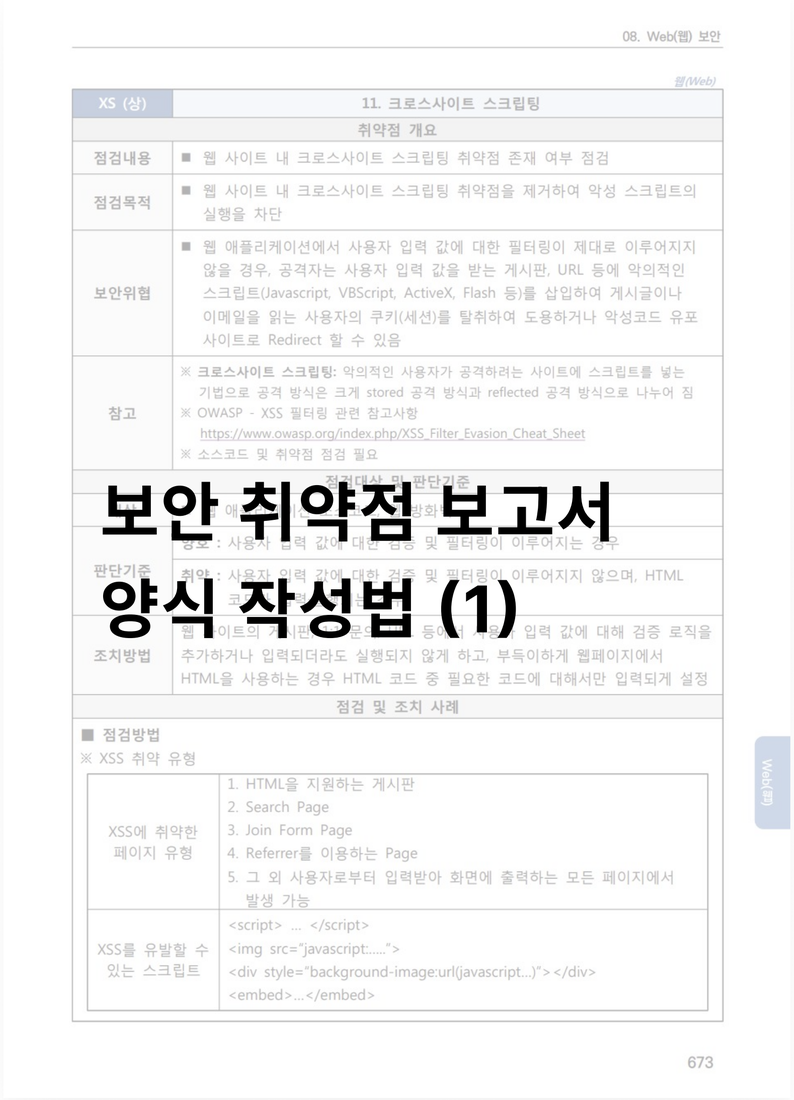
각종우회기법시도

- param=1 and (select
- ''|| xmltype('<'||regexp_replace(utl_raw.cast_to_varchar2(utl_encode.base64_encode(utl_raw.cast_to_raw((select+global_name+from+global_name))))||'%3ax>',chr(10)||'|'||chr(13)||'|%3d',''))||''+from+dual)-
- page.action?page=1&order_by_column=YEAR DESC, (select case when instr(user,&order_by_align=chr(65))=0 then 1 else 1/0 end from dual)





“보안 취약점 보고서”를 어떻게 작성해야 하는가?



08. Web(웹) 보안

웹(Web)

XS (상)	11. 크로스사이트 스크립팅
취약점 개요	
점검내용	■ 웹 사이트 내 크로스사이트 스크립팅 취약점 존재 여부 점검
점검목적	■ 웹 사이트 내 크로스사이트 스크립팅 취약점을 제거하여 악성 스크립트의 실행을 차단
보안위협	■ 웹 애플리케이션에서 사용자 입력 값에 대한 필터링이 제대로 이루어지지 않을 경우, 공격자는 사용자 입력 값을 받는 게시판, URL 등에 악의적인 스크립트(Javascript, VBScript, ActiveX, Flash 등)를 삽입하여 게시글이나 이메일을 읽는 사용자의 쿠키(세션)를 탈취하여 도용하거나 악성코드 유포 사이트로 Redirect 할 수 있음
참고	※ **크로스사이트 스크립팅:** 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법으로 공격 방식은 크게 stored 공격 방식과 reflected 공격 방식으로 나누어 짐 ※ OWASP - XSS 필터링 관련 참고사항 https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
판단기준	**양호 :** 사용자 입력 값에 대한 검증 및 필터링이 이루어지는 경우 **취약 :** 사용자 입력 값에 대한 검증 및 필터링이 이루어지지 않으며, HTML 코드
조치방법	웹 사이트의 게시판, 문의하기 등에서 사용자 입력 값에 대해 검증 로직을 추가하거나 입력되더라도 실행되지 않게 하고, 부득이하게 웹페이지에서 HTML을 사용하는 경우 HTML 코드 중 필요한 코드에 대해서만 입력되게 설정
점검 및 조치 사례	

■ 점검방법

※ XSS 취약 유형

XSS에 취약한 페이지 유형	1. HTML을 지원하는 게시판 2. Search Page 3. Join Form Page 4. Referrer를 이용하는 Page 5. 그 외 사용자로부터 입력받아 화면에 출력하는 모든 페이지에서 발생 가능
XSS를 유발할 수 있는 스크립트	<script> ... </script> <img src="javascript:....."> <embed>...</embed>

673

보안 취약점 보고서 양식 작성법 (1)

제목

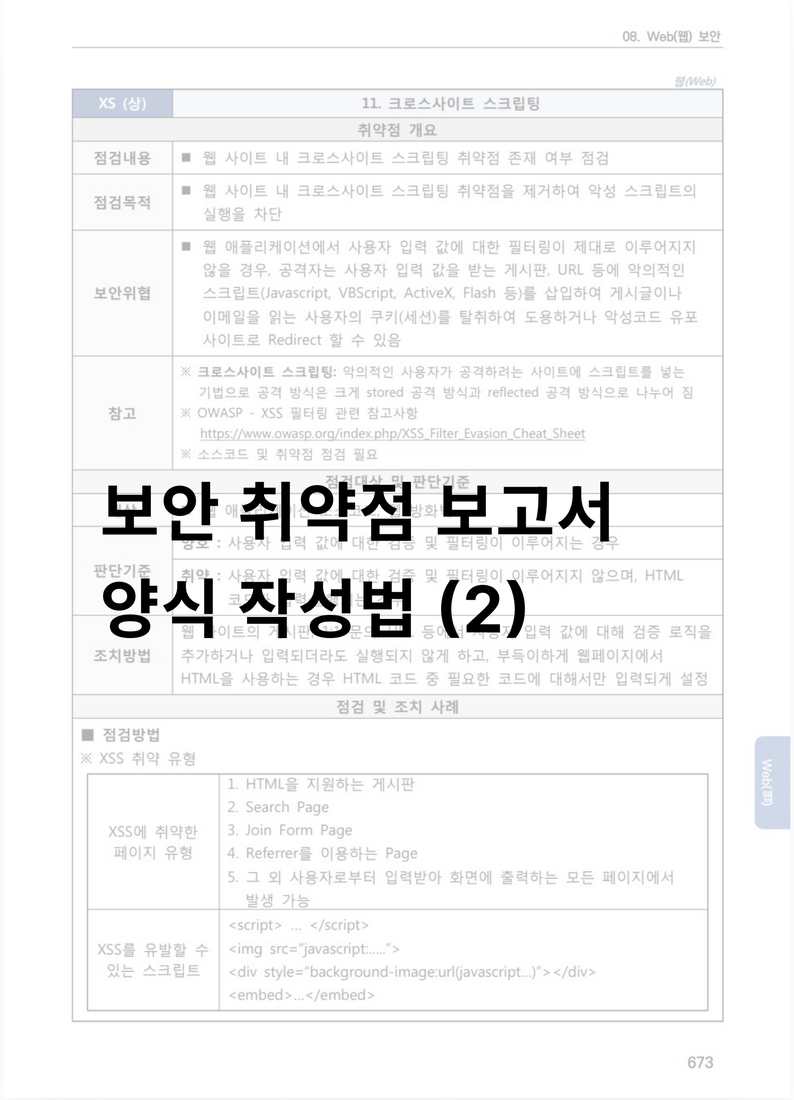
- 좋은 제목은 버그의 유형, 발견된 곳 그리고 영향력을 포함해야 함.
- 좋은예) “이력서 업로드 양식에서 파일 업로드 취약점 발생 및 원격 임의코드 실행 가능”
- 나쁜예) “앱에서 RFI Injection 발견”

취약점 유형

- 명확하게 제시
- 예를 들어, 발견된 버그가 XSS 인 경우에
- DOM base XSS인지 Reflected XSS인지 정확히 제시

타겟 범위

- 타겟팅 된 URL, 기능 등이 가장 중요함



08. Web(웹) 보안

웹(Web)

XS (상)	11. 크로스사이트 스크립팅
취약점 개요	
점검내용	■ 웹 사이트 내 크로스사이트 스크립팅 취약점 존재 여부 점검
점검목적	■ 웹 사이트 내 크로스사이트 스크립팅 취약점을 제거하여 악성 스크립트의 실행을 차단
보안위협	■ 웹 애플리케이션에서 사용자 입력 값에 대한 필터링이 제대로 이루어지지 않을 경우, 공격자는 사용자 입력 값을 받는 게시판, URL 등에 악의적인 스크립트(Javascript, VBScript, ActiveX, Flash 등)를 삽입하여 게시글이나 이메일을 읽는 사용자의 쿠키(세션)를 탈취하여 도용하거나 악성코드 유포 사이트로 Redirect 할 수 있음
참고	※ **크로스사이트 스크립팅:** 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법으로 공격 방식은 크게 stored 공격 방식과 reflected 공격 방식으로 나누어 짐 ※ OWASP - XSS 필터링 관련 참고사항 https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
판단기준	**양호 :** 사용자 입력 값에 대한 검증 및 필터링이 이루어지는 경우 **취약 :** 사용자 입력 값에 대한 검증 및 필터링이 이루어지지 않으며, HTML 코드
조치방법	웹 사이트의 게시판, 문의하기 등에서 사용자 입력 값에 대해 검증 로직을 추가하거나 입력되더라도 실행되지 않게 하고, 부득이하게 웹페이지에서 HTML을 사용하는 경우 HTML 코드 중 필요한 코드에 대해서만 입력되게 설정
점검 및 조치 사례	

■ 점검방법

※ XSS 취약 유형

XSS에 취약한 페이지 유형	1. HTML을 지원하는 게시판 2. Search Page 3. Join Form Page 4. Referrer를 이용하는 Page 5. 그 외 사용자로부터 입력받아 화면에 출력하는 모든 페이지에서 발생 가능
XSS를 유발할 수 있는 스크립트	<script> ... </script> <img src="javascript:....."> <embed>...</embed>

673

Web(웹)

보안 취약점 보고서 양식 작성법 (2)

취약점 점검 방법

- 세부 점검 내용은 매우 세부적이어야 함.
- 최대한 많은 정보를 제공해야 하며, 화면 캡처도 중요함

영향

- 발견한 취약점에 대한 영향력과 위험도에 대한 설명
- 간결하게 작성하는 게 좋으며, 담당 업무 담당자가 이해할 수 있도록 설명
- 해당 영향력의 범위를 산정해, 필요한 예산 및 조치 방안을 결정

조치 방법

- 조치 방법에 대한 제안 내용을 포함
- 예) 보안 솔루션 도입, 시큐어코딩 개선, 마스킹 처리 등

취약점 점검 방법의 나쁜 예

www.naver.com 메인페이지에서 XXS 취약점 발생

취약점 점검 방법의 좋은 예

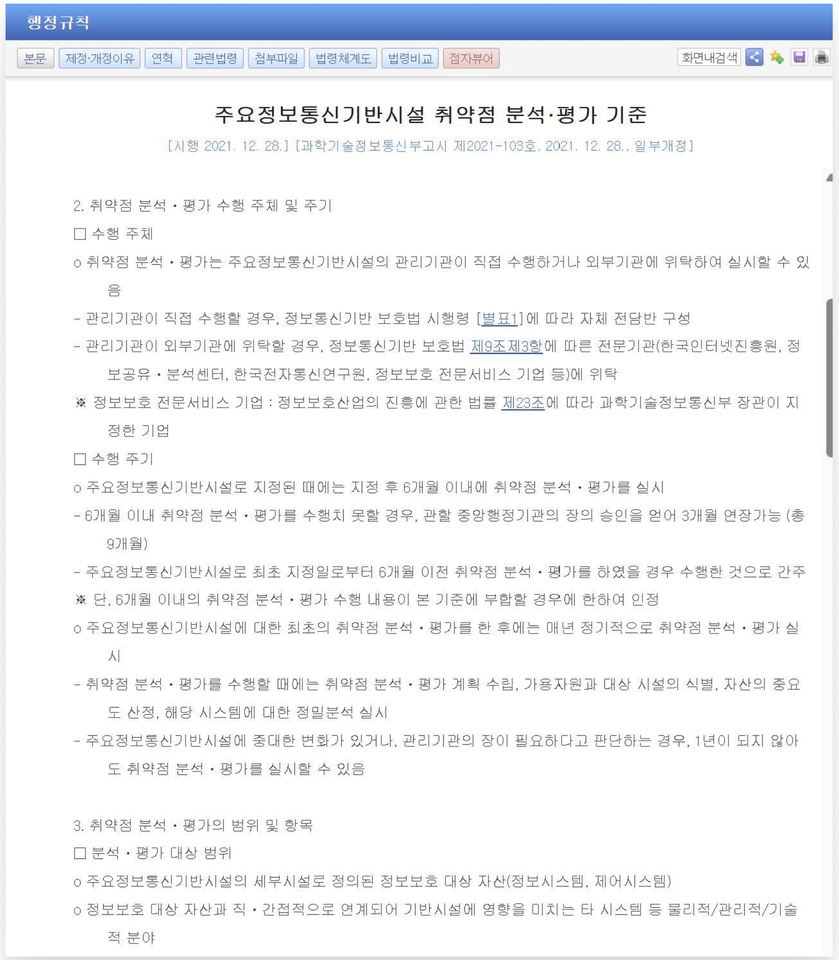
- ‘www.thatsite.com’에 접속. “upload image” 버튼을 클릭.
- 첨부된 스크린샷 1(screenshot1.png)에서 버튼의 위치를 확인할 수 있음.
- “choose file” 버튼을 오른쪽 클릭,
- 그리고“inspect element”를 선택한다.
- “choose file” 버튼을 클릭하고 shell.php 파일을 선택.
- 쉘을업로드. 쉘은[URL]에서접속이가능하다.
- 이 쉘은 원격에서 서버를 조종 가능.
- 예를 들어, 현재의 디렉토리에 속하는 파일들의 목록을 볼 수 있음.
- 더 자세한 정보는 첨부된 파일(details.txt)과 자세한 화면이 포함된 스크린샷 6(screenshot6.png)에서 확인할 수 있다.

```
1  POST /login?destination=node HTTP/1.1
2  HOST: [Site]
3  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
4  Accept-Encoding: gzip, deflate
5  Accept-Language: en-US,en;q=0.5
6  Referer: https://[site]/login?destination=node
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 99
9
10 name[0;update%20user_roles%20set%20rid%3D3%20where%20uid%3D[numeric user id];#%20%20]=test&name[0]=
```

주요정보통신기반시설 취약점 분석 평가

주요정보통신기반시설 취약점 분석·평가란?

국가가 지정한 핵심 정보통신 인프라(금융·통신·에너지 등)에 대해
해킹·악성코드·설계·구성상의 약점을 찾아내고(분석),
그 위험도를 평가해 개선권고를 내리는 법적·기술적 절차



행정규칙

본문 | 제정·개정이유 | 연혁 | 관련법령 | 첨부파일 | 법령체계도 | 법령비교 | 점자뷰어 | 화면내검색

주요정보통신기반시설 취약점 분석·평가 기준

[시행 2021. 12. 28.] [과학기술정보통신부고시 제2021-103호, 2021. 12. 28., 일부개정]

2. 취약점 분석·평가 수행 주체 및 주기

□ 수행 주체

○ 취약점 분석·평가는 주요정보통신기반시설의 관리기관이 직접 수행하거나 외부기관에 위탁하여 실시할 수 있음

- 관리기관이 직접 수행할 경우, 정보통신기반 보호법 시행령 [별표1]에 따라 자체 전담반 구성
- 관리기관이 외부기관에 위탁할 경우, 정보통신기반 보호법 제9조제3항에 따른 전문기관(한국인터넷진흥원, 정보공유·분석센터, 한국전자통신연구원, 정보보호 전문서비스 기업 등)에 위탁

※ 정보보호 전문서비스 기업 : 정보보호산업의 진흥에 관한 법률 제23조에 따라 과학기술정보통신부 장관이 지정한 기업

□ 수행 주기

○ 주요정보통신기반시설로 지정된 때에는 지정 후 6개월 이내에 취약점 분석·평가를 실시

- 6개월 이내 취약점 분석·평가를 수행치 못할 경우, 관할 중앙행정기관의 장의 승인을 얻어 3개월 연장가능 (총 9개월)
- 주요정보통신기반시설로 최초 지정일로부터 6개월 이전 취약점 분석·평가를 하였을 경우 수행한 것으로 간주

※ 단, 6개월 이내의 취약점 분석·평가 수행 내용이 본 기준에 부합할 경우에 한하여 인정

○ 주요정보통신기반시설에 대한 최초의 취약점 분석·평가를 한 후에는 매년 정기적으로 취약점 분석·평가 실시

- 취약점 분석·평가를 수행할 때에는 취약점 분석·평가 계획 수립, 가용자원과 대상 시설의 식별, 자산의 중요도 산정, 해당 시스템에 대한 정밀분석 실시
- 주요정보통신기반시설에 중대한 변화가 있거나, 관리기관의 장이 필요하다고 판단하는 경우, 1년이 되지 않아도 취약점 분석·평가를 실시할 수 있음

3. 취약점 분석·평가의 범위 및 항목

□ 분석·평가 대상 범위

○ 주요정보통신기반시설의 세부시설로 정의된 정보보호 대상 자산(정보시스템, 제어시스템)

○ 정보보호 대상 자산과 직·간접적으로 연계되어 기반시설에 영향을 미치는 타 시스템 등 물리적/관리적/기술적 분야

수행 주체

- 관리기관이 직접 수행하거나 외부기관에 위탁하여 실시
- 한국인터넷진흥원, 정보공유 · 분석센터, 한국전자통신연구원, 정보보호 전문서비스 기업 등

수행 주기

- 주요정보통신기반시설로 지정된 때에는 지정 후 6개월 이내에 취약점 분석 · 평가를 실시
- 관할 중앙행정기관의 장의 승인을 얻어 3개월 연장가능 (총 9개월)
- 분석 · 평가를 한 후에는 매년 정기적으로 취약점 분석 · 평가 실시

분석 · 평가 항목

- 관리적, 물리적, 기술적으로 구분
- 기본항목은 3단계(상 · 중 · 하)로 중요도를 분리
- 기본 항목의 중요도 "상"인 점검항목은 매년 1회 필수적으로 점검
- 기본 항목의 중요도 "중", "하" 인 항목은 기관의 사정에 따라 선택 점검

일반적인 수행 절차

계획

범위(시스템·서브시스템), 허가,
일정, 방법론 확정

정보수집

자산목록, 서비스·포트·버전 정보 수집

취약점 탐지

자동화 스캐너(패치·포트·취약점 DB 대조)로 1차 탐지

취약성 확인

자동화에서 잡히지 않는 로직 취약점·
설계 취약 수동검증

영향도 평가

영향·가능성·우선순위 산정

보고

발견항목·재현방법(또는 증거)·
권고조치·시정기한 포함

조치·재검증

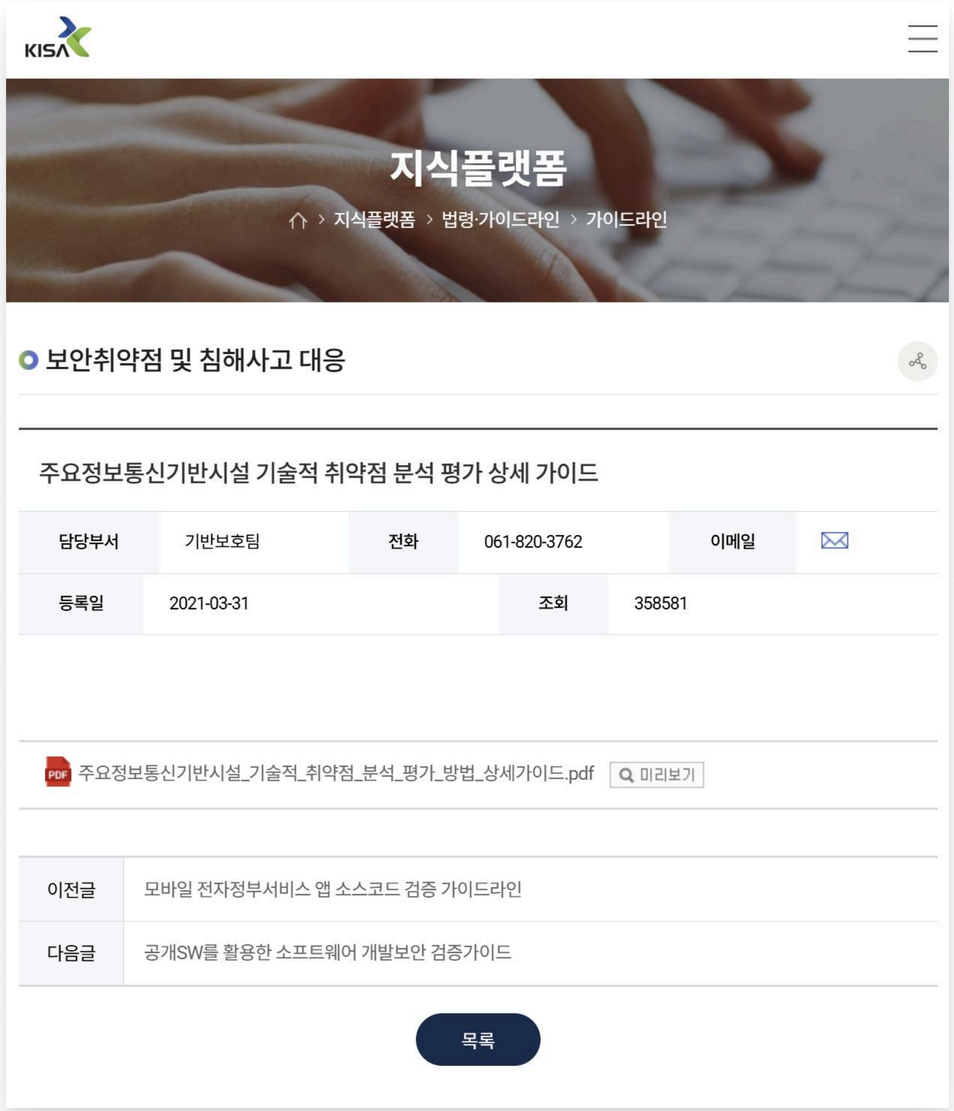
수정 후 재평가로 완결

점검 항목 예시

- 웹 애플리케이션 취약점: SQLi, XSS, 파일업로드 취약 등
- 네트워크·프로토콜: 미설정 포트, 취약한 서비스, 프래그먼트·DoS 취약 등
- 시스템·OS 설정: 불필요 서비스, 권한설정 오류, 패치 누락
- 인증·접근통제: 약한 암호정책, 세션관리, 인증우회 가능성
- 클라우드·가상화 특유 항목: IAM 설정, 이미지 취약, 멀티테넌시 위험 등

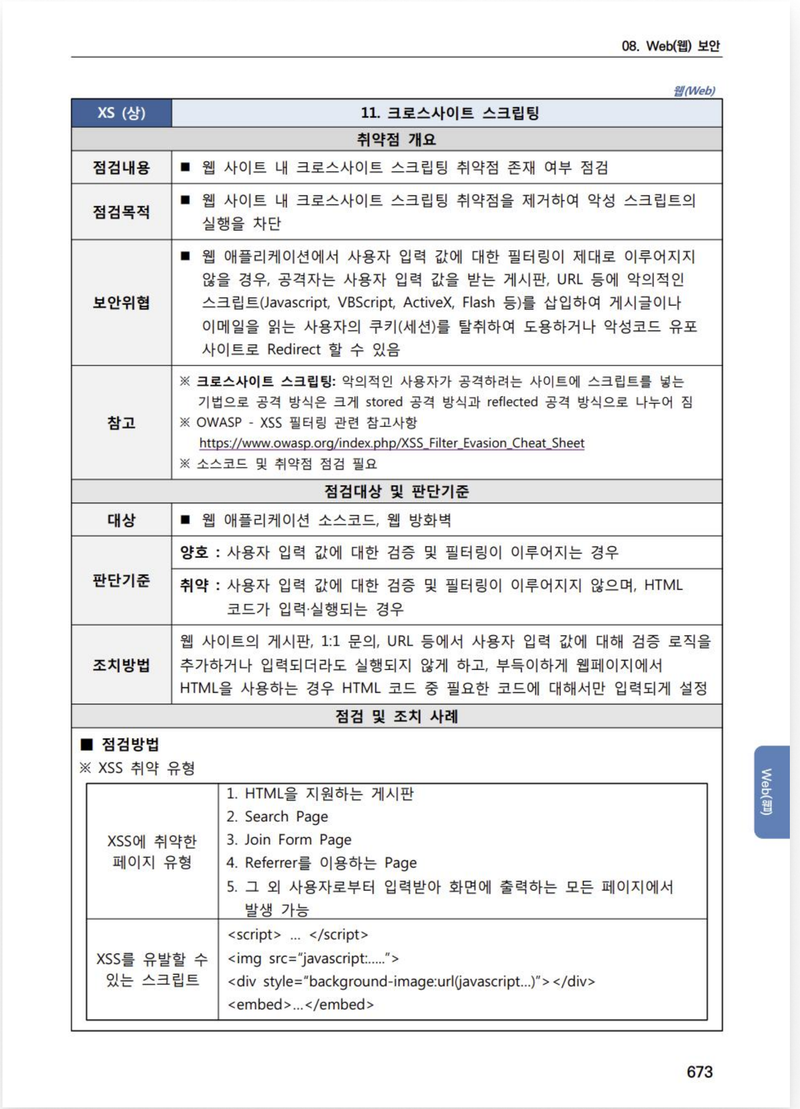
주요정보통신기반시설
“기술적” 취약점 분석·평가 체크리스트 확인

1. 한국인터넷진흥원홈페이지
2. 지식플랫폼 > 법령·가이드라인 > 가이드라인
3. “주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드”



주요정보통신기반시설
“기술적” 취약점 분석·평가 체크리스트 확인

- 총 10개 분야
- 유닉스, 윈도우즈, 보안장비, 네트워크 장비, 제어시스템, PC, 데이터베이스, 웹, 이동통신, 클라우드 분야



08. Web(웹) 보안

웹(Web)

XS (상)	11. 크로스사이트 스크립팅
취약점 개요	
점검내용	■ 웹 사이트 내 크로스사이트 스크립팅 취약점 존재 여부 점검
점검목적	■ 웹 사이트 내 크로스사이트 스크립팅 취약점을 제거하여 악성 스크립트의 실행을 차단
보안위협	■ 웹 애플리케이션에서 사용자 입력 값에 대한 필터링이 제대로 이루어지지 않을 경우, 공격자는 사용자 입력 값을 받는 게시판, URL 등에 악의적인 스크립트(Javascript, VBScript, ActiveX, Flash 등)를 삽입하여 게시글이나 이메일을 읽는 사용자의 쿠키(세션)를 탈취하여 도용하거나 악성코드 유포 사이트로 Redirect 할 수 있음
참고	※ **크로스사이트 스크립팅:** 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법으로 공격 방식은 크게 stored 공격 방식과 reflected 공격 방식으로 나누어 짐 ※ OWASP - XSS 필터링 관련 참고사항 https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet ※ 소스코드 및 취약점 점검 필요
점검대상 및 판단기준	
대상	■ 웹 애플리케이션 소스코드, 웹 방화벽
판단기준	**양호 :** 사용자 입력 값에 대한 검증 및 필터링이 이루어지는 경우
	취약 : 사용자 입력 값에 대한 검증 및 필터링이 이루어지지 않으며, HTML 코드가 입력·실행되는 경우
조치방법	웹 사이트의 게시판, 1:1 문의, URL 등에서 사용자 입력 값에 대해 검증 로직을 추가하거나 입력되더라도 실행되지 않게 하고, 부득이하게 웹페이지에서 HTML을 사용하는 경우 HTML 코드 중 필요한 코드에 대해서만 입력되게 설정
점검 및 조치 사례	

■ **점검방법**

※ XSS 취약 유형

XSS에 취약한 페이지 유형	1. HTML을 지원하는 게시판 2. Search Page 3. Join Form Page 4. Referrer를 이용하는 Page 5. 그 외 사용자로부터 입력받아 화면에 출력하는 모든 페이지에서 발생 가능
XSS를 유발할 수 있는 스크립트	<script> ... </script> <img src="javascript:....."> <embed>...</embed>

673

Web(웹)