



**OOOO**

**취약점진단 결과보고서**

2023. 00. 00.

**Confidentiality Agreements**

본 보고서는 시스템 정보와 관련한 비공개 사항이 포함되어 있으므로, 열람권한은 우선적으로 정보보안 책임자로 제한되며, 이외의 열람자격은 정보보안 책임자가 허락한 최소한의 인원으로 제한하여 주시기 바랍니다.

본 보고서는 양사간의 사전 협의 없이 어떠한 목적으로도 외부로 유출되거나 무단 복제, 무단 사용될 수 없으며, 기밀성을 유지한다는 전제하에 사용이 엄격하게 제한됩니다.

본 보고서는 SK쉴더스에서 작성 하였으며, 정보보호 서약에 대한 사항을 준수 합니다.

목 차

[1. 개요 10](#_Toc139010452)

[1.1. 진단 목적 10](#_Toc139010453)

[1.2. 진단 대상 10](#_Toc139010454)

[1.3. 진단 일정 10](#_Toc139010455)

[1.4. 진단 인력 10](#_Toc139010456)

[2. 진단 항목 및 도구 11](#_Toc139010457)

[2.1. 취약점진단 진단 도구 11](#_Toc139010458)

[2.2. 진단 항목 11](#_Toc139010459)

[3. 취약점진단 결과요약 13](#_Toc139010460)

[3.1. 총평 13](#_Toc139010464)

[3.2. 대상 별 취약점 요약 14](#_Toc139010465)

[4. 취약점진단 상세결과 15](#_Toc139010466)

[4.1. 메인 서비스 ( http://www.OOO.com ) 15](#_Toc139010467)

[(1) XSS / CSRF 공격 (중요) 15](#_Toc139010468)

[(2) SQL Injection 공격 가능성 (중요) 21](#_Toc139010469)

[(3) 악성코드 파일 업로드 (중요) 22](#_Toc139010470)

[(4) Directory traversal 공격 (중요) 23](#_Toc139010471)

[(5) 접근제어 우회 공격 (일반) 24](#_Toc139010472)

그림 목차

[[그림] 1. 블로그 내 포스트 확인 11](#_Toc139010473)

[[그림] 2. 포스트 댓글 작성 12](#_Toc139010474)

[[그림] 2. 댓글 작성 시 악의적 구문 삽입 후 저장 시도 13](#_Toc139010475)

[[그림] 2. 댓글 저장 시 응답 패킷 확인 13](#_Toc139010476)

[[그림] 2. 저장된 댓글 확인 ① 13](#_Toc139010477)

[[그림] 2. 저장된 댓글 확인 ② 14](#_Toc139010478)

[[그림] 2. 저장된 댓글 확인 ③ 14](#_Toc139010479)

[[그림] 2. 응답 값 내 악의적 구문 필터링 없이 등록 확인 15](#_Toc139010480)

[[그림] 2. 스크립트 실행 확인 15](#_Toc139010481)

[[그림] 3. 테스트 파일 확인 ① 17](#_Toc139010482)

[[그림] 4. 테스트 파일 확인 ② 17](#_Toc139010483)

[[그림] 11. 테스트 파일 확인 ① 18](#_Toc139010484)

[[그림] 12. 테스트 파일 확인 ② 18](#_Toc139010485)

[[그림] 13. 테스트 파일 확인 ① 19](#_Toc139010486)

[[그림] 14. 테스트 파일 확인 ② 19](#_Toc139010487)

[[그림] 31. 테스트 파일 확인 ① 20](#_Toc139010488)

[[그림] 32. 테스트 파일 확인 ② 20](#_Toc139010489)

표 목차

[[표] 1. 진단대상 6](#_Toc139010490)

[[표] 2. 진단 일정 6](#_Toc139010491)

[[표] 3. 진단 인력 6](#_Toc139010492)

[[표] 4. 진단 도구 7](#_Toc139010493)

[[표] 5. 주요 진단 항목 8](#_Toc139010494)

[[표] 6. 대상 별 취약점 요약 10](#_Toc139010495)

개요

* 1. 진단 목적

본 취약점 진단은 **“OOO”**에서 운영중인 애플리케이션 서비스에 대하여 취약점 체크리스트를 기반으로 주요정보의 전자적 침해 행위에 대한 취약점을 분석ᆞ평가하고, 존재하는 위협 요소에 대해 정확한 분석을 통해 보안대책을 수립 및 취약점을 제거하여 보안 위협을 최소화함으로써 사고 예방 및 안전한 운영에 기여하고자 합니다.

* 1. 진단 대상

|  |  |  |
| --- | --- | --- |
| No | URL | 서비스명 |
| 1 | http://www.OOO.com |  |
| 2 | http://www.OOO.com |  |
| 3 | http://www.OOO.com |  |

[표] 1. 진단대상

* 1. 진단 일정

|  |  |
| --- | --- |
| 업무 수행 내역 | 일정 |
| 사전준비 및 대상 관련 자료 수령 | 2020.00.00 이전 |
| 취약점 점검 | 2020.00.00~ 2020.00.00 |
| 결과 분석 및 결과 보고서 작성 | 2020.00.00 |
| 보고서 최종 수정 및 완료 | 2020.00.00 |

[표] 2. 진단 일정

* 1. 진단 인력

|  |  |  |  |
| --- | --- | --- | --- |
| 이름 | 수행업무 | 연락처 | E-Mail |
| OOO 선임 | 취약점진단 | 010-0000-0000 | OOOOOOO@sk.com |

[표] 3. 진단 인력

진단 항목 및 도구

* 1. 취약점진단 진단 도구

취약점진단의 특성상 툴을 이용한 진단은 정확도가 떨어지며 상황 별 판단이 필요하므로 대부분 취약점진단 전문인력이 수동으로 진단합니다.

취약점진단을 수행하기 위해 사용되는 도구들을 정리하면 다음과 같습니다.

|  |  |
| --- | --- |
| 구분 | 진단 항목 설명 |
| Paros / Burp proxy | Proxy 기능을 이용한 웹 세션 조작 도구 |
| nmap | 다양한 port scan 기능과 OS Identification을 제공함.  http://www.insecure.org/nmap/ |
| Wireshark | 네트워크 패킷 점검 도구  http://www.wireshark.com/ |
| 기타 | 진단자가 작성한 Exploit Code 및 Script, 기타 점검 도구 |

[표] 4. 진단 도구

* 1. 진단 항목

진단에 사용될 항목은 OWASP[[1]](#footnote-1), NIST[[2]](#footnote-2), 행정안전부 등에서 권고하는 내용을 기반으로 본 프로젝트와 연관성이 있는 보안상의 문제점을 주축으로 총 8개 분류 28개 항목의 체크리스트로 수립한 항목입니다.

| **분류** | **취약점 번호** | **세부 진단 항목** | **준수기준** |
| --- | --- | --- | --- |
| 입/출력 값  검증 부재 | **1-1** | **XSS / CSRF 공격 가능성** | **중요** |
| **1-2** | **삽입 (Injection) 공격 가능성** | **중요** |
| **1-3** | **파라미터 값 및 히든(hidden) 필드 조작 가능성** | **중요** |
| **1-4** | **SSRF / File Inclusion 공격 가능성** | **중요** |
| 1-5 | 검증되지 않은 리다이렉트와 포워드 | 일반 |
| **1-6** | **입력 값 크기 및 무결성 검증오류** | **중요** |
| 취약한  파일처리 | **2-1** | **악성코드파일 업로드** | **중요** |
| **2-2** | **중요 정보 파일 다운로드 가능성** | **중요** |
| 취약한 접근  통제 관리 | 3-1 | 패스워드 정책 유무 및 반영 여부 | 일반 |
| 3-2 | 인증 실패 횟수 제한 | 일반 |
| 3-3 | 계정 정보 파악 가능성 | 일반 |
| 3-4 | 관리자 페이지 분리 여부 | 일반 |
| 3-5 | 검색엔진 정보 노출 가능성 | 일반 |
| 3-6 | 백업 파일 및 테스트 파일 존재 여부 | 일반 |
| 취약한 인증 및  세션 관리 | 4-1 | 쿠키(Cookie) 및 웹 스토리지(Web Storage) 조작 가능성 | 일반 |
| 4-2 | 인증(세션 및 토큰) 값 안전성 설정 여부 | 일반 |
| 4-3 | 접근제어 우회 가능성 확인 | 일반 |
| 4-4 | 비인증 상태로 중요 page접근 가능성 | 일반 |
| 4-5 | 일반계정 권한 상승 가능성 | 일반 |
| 중요 정보 저장/전송 처리 미흡 | 5-1 | 소스코드 내 주요정보 노출 여부 | 일반 |
| **5-2** | **요청 및 응답 값 내 주요정보 포함여부 확인** | **중요** |
| 부적절한  오류 처리 | 6-1 | 오류페이지를 통한 정보 노출 여부 | 일반 |
| 6-2 | 일괄적인 오류 처리 페이지 존재 여부 | 일반 |
| 취약한  컴포넌트  구성요소 | 7-1 | Client Request Method | 일반 |
| 7-2 | 파일 목록화 가능성 | 일반 |
| 7-3 | 서버 헤더정보 노출 | 일반 |
| 7-4 | 취약한 보안설정 | 일반 |
| 기타 취약점 | 8-1 | 취약점 진단 항목에 정의되지 않은 취약점 | - |

[표] 5. 주요 진단 항목

취약점진단 결과요약

3. 1. 총평

**“OOO”**의 총 0개의 도메인을 대상으로 웹 취약점진단을 진행한 결과 외부에 오픈된 3개 사이트에서 **“XSS / CSRF 공격 가능성”** 취약점이 발견되었고, 상품 구매 시 결제 금액 변조 등의 **중요** 취약점과 그 외 다수의 일반 취약점이 발견되었습니다.

자세한 사항은 아래 취약점진단 상세결과를 확인하시고 본 결과보고서와 함께 제공해드리는 보안 가이드라인을 참고하시어 적절한 보안 대책을 수립 후 조치하시길 권고 드립니다.

**※ 본 진단은 상용 서버에서 수행하였으며, 서비스 영향도 이슈로 인해 메뉴(기능) 전수 진단이 아닌 샘플링 동적 진단으로 진행하여 최소한의 취약 포인트만 확인하므로 다수의 취약점 누락 발생 가능성이 존재합니다. 또한, 발견된 취약점의 모든 취약 포인트를 식별하지 않으므로 유사 취약 포인트에 대해 Application 담당자 직접 확인 후 조치가 필요합니다.**

**※ 2개 도메인(000, 대표홈페이지)을 제외한 0개 대상에서 1개의 계정만 제공되어 일반 계정을 통한 권한 상승 등의 일부 항목은 진단에서 제외 하였습니다.**

* 1. 대상 별 취약점 요약

| 대상(도메인) | 위험도 | 취약점 명칭 | 개수 |
| --- | --- | --- | --- |
| **OOO**  **(www.OOO.com)** | **중요** | **요청 및 응답 값 내 주요정보 포함여부 확인** | **0** |
| 일반 | 백업 파일 및 테스트 파일 존재 여부 | 0 |
| **OOO**  **(www.OOO.co.kr)** | **중요** | **XSS / CSRF 공격 가능성** | **0** |
| 일반 | 검증되지 않은 리다이렉트와 포워드 | 0 |
| 일반 | 접근제어 우회 가능성 확인 | 0 |
| 일반 | 오류페이지를 통한 정보노출 여부 | 0 |
| 일반 | 취약점 진단 항목에 정의되지 않은 취약점 | 0 |

[표] 6. 대상 별 취약점 요약

취약점진단 상세결과

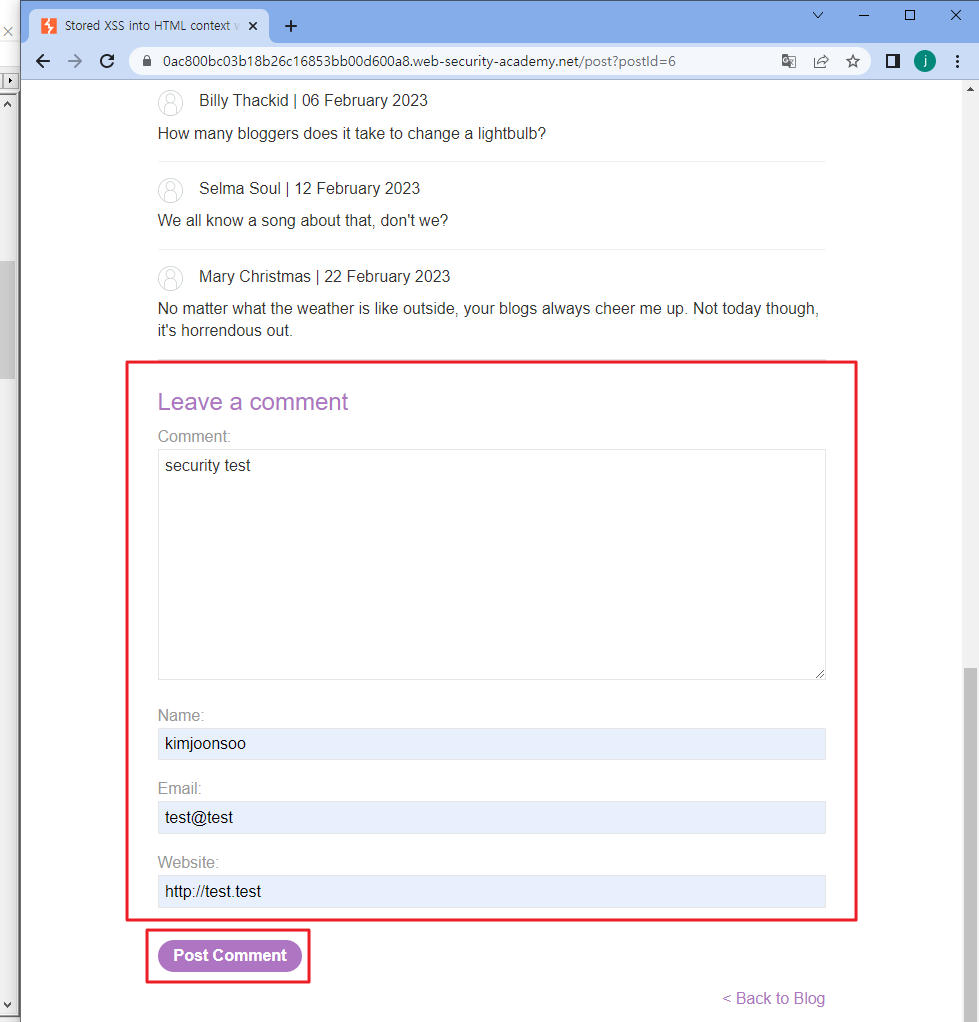
* 1. 메인 서비스 ( http://www.OOO.com )
     1. XSS / CSRF 공격 (중요)
        1. **문제점**

**[CASE 1] Stored XSS 공격**

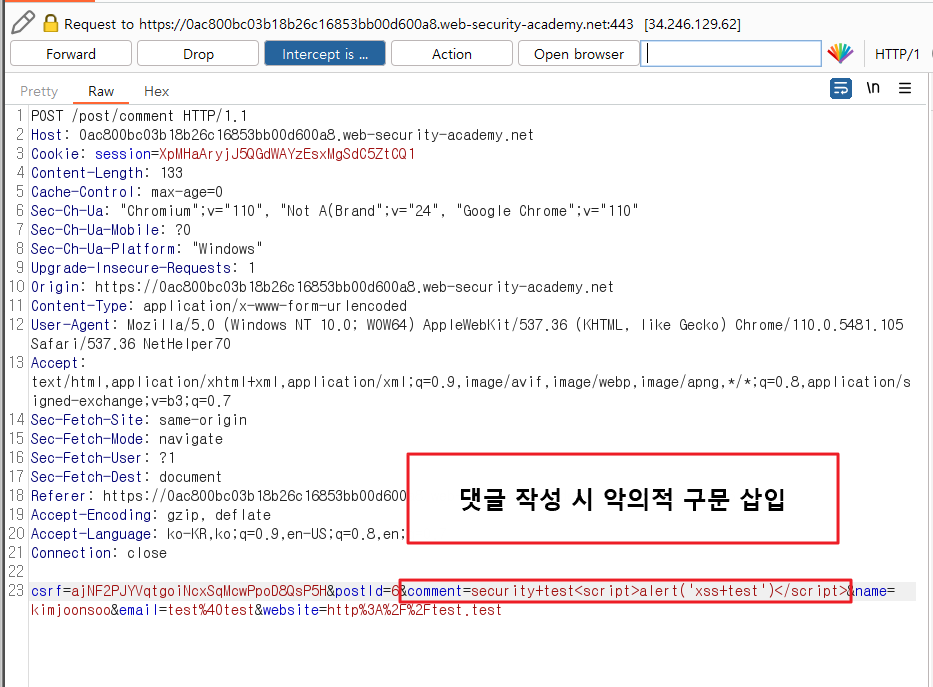
Web Security Academy 서비스 내 일부 페이지에서 입/출력 값에 대한 필터링 검증이 부재하여 댓글 기능 이용/사용 시 악성 스크립트 삽입 및 실행이 가능하며 이로 인해 타사용자의 인증정보 획득 및 악성 코드 유포 가능성이 존재합니다.



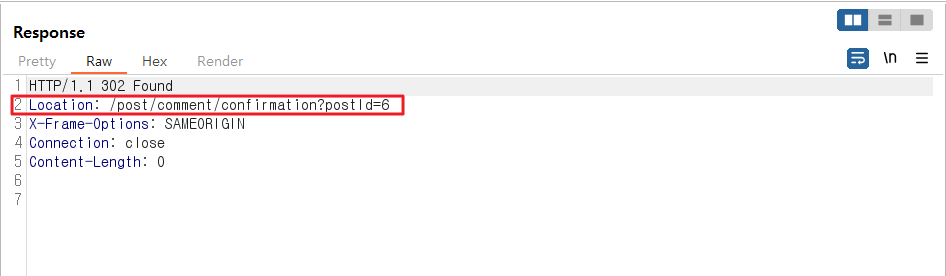
[그림] 1. 블로그 내 포스트 확인



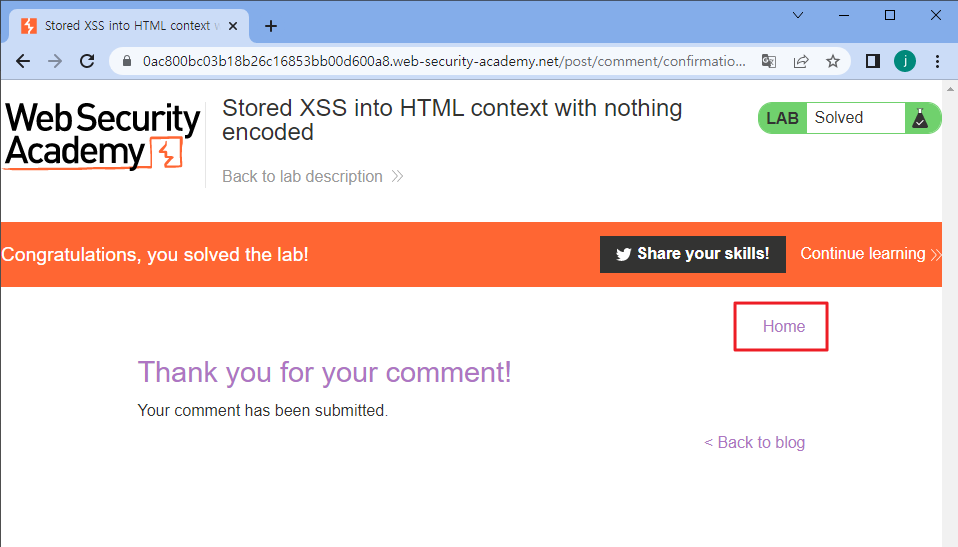
[그림] 2. 포스트 댓글 작성



[그림] . 댓글 작성 시 악의적 구문 삽입 후 저장 시도



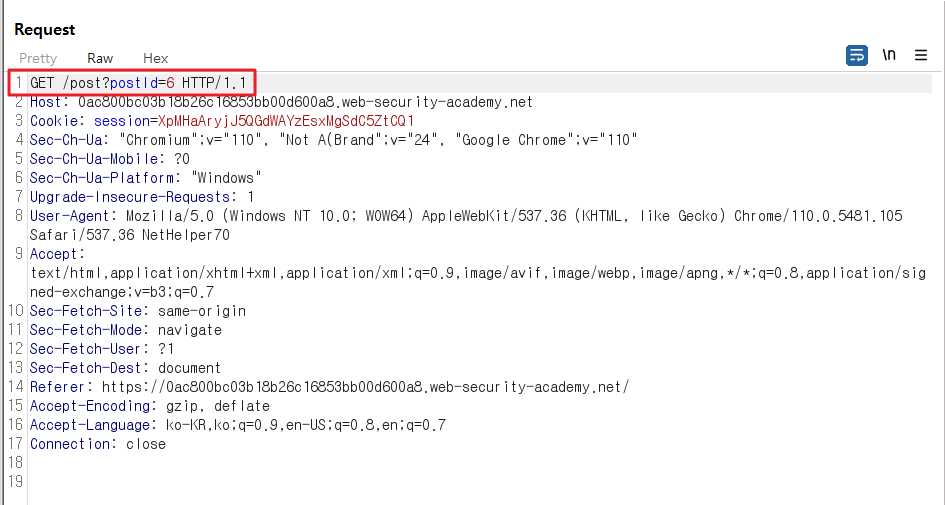
[그림] . 댓글 저장 시 응답 패킷 확인



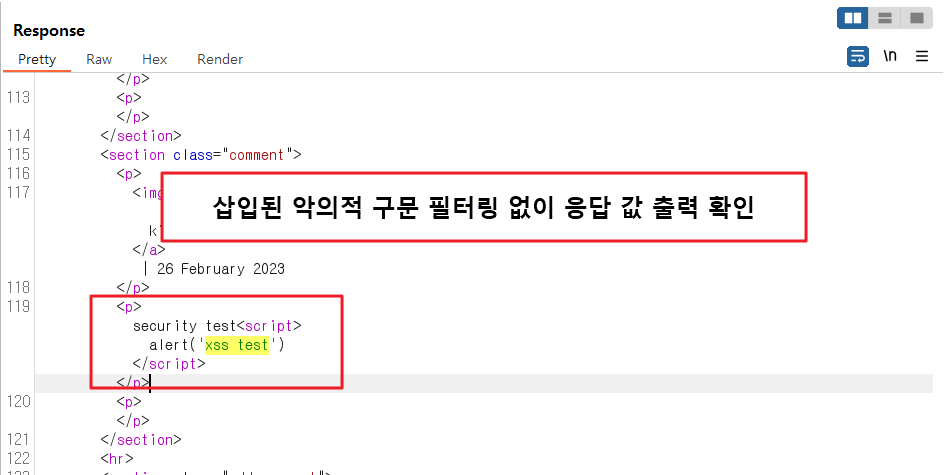
[그림] . 저장된 댓글 확인 ①



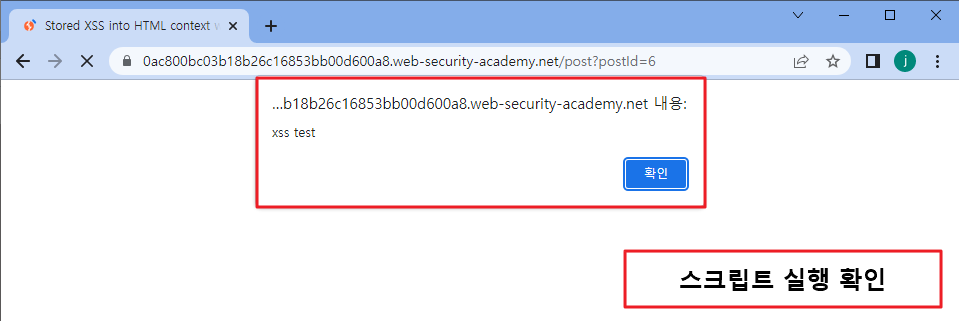
[그림] . 저장된 댓글 확인 ②



[그림] . 저장된 댓글 확인 ③



[그림] . 응답 값 내 악의적 구문 필터링 없이 등록 확인



[그림] . 스크립트 실행 확인

* + - 1. **관련 URL**

| **번호** | **경로** | **URL** |
| --- | --- | --- |
| 1 | View Post > Post Comment | /post/comment?comment |

* + - 1. **해결방안**

모든 입/출력 값에 대한 검증은 스크립트가 아닌 서버 측에서 검증을 수행해야 하며, 입/출력 값 필터링시 아래와 같은 문자들에 대해서 필터링을 설정 해야 합니다.

| **From** | **To** |
| --- | --- |
| < | & l t; |
| > | & g t; |
| ( | & # 4 0; |
| ) | & # 4 1; |
| # | & # 3 5; |
| & | & # 3 8; |
| ‘ | & # 3 9; |
| “ | &quot; |

[표] 3. XSS가 가능한 태그 목록

**※ Keyword 필터링은 대/소문자 구분 없이 적용하여야 하며 일괄 적용 시 오류가 발생할 수 있으니 서비스 및 운영상의 영향도를 확인하시어 적용해야 합니다.**

* + 1. SQL Injection 공격 가능성 (중요)
       1. **문제점**

테스트

[그림] 10. 테스트 파일 확인 ①

[그림] 11. 테스트 파일 확인 ②

* + - 1. **관련 URL**

| **번호** | **경로** | **URL** |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |

* + - 1. **해결방안**

ㅇㅇㅇ

※ 서버 내 존재하는 테스트파일 및 업로드 폴더 내 의심되는 파일(웹쉘 및 개발자가 임의로 생성한 파일)은 삭제 하여 주시기 바랍니다.

* + 1. 악성코드 파일 업로드 (중요)
       1. **문제점**

테스트

[그림] 12. 테스트 파일 확인 ①

[그림] 13. 테스트 파일 확인 ②

* + - 1. **관련 URL**

| **번호** | **경로** | **URL** |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |

* + - 1. **해결방안**

ㅇㅇㅇ

※ 서버 내 존재하는 테스트파일 및 업로드 폴더 내 의심되는 파일(웹쉘 및 개발자가 임의로 생성한 파일)은 삭제 하여 주시기 바랍니다.

* + 1. Directory traversal 공격 (중요)
       1. **문제점**

테스트

[그림] 14. 테스트 파일 확인 ①

[그림] 15. 테스트 파일 확인 ②

* + - 1. **관련 URL**

| **번호** | **경로** | **URL** |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |

* + - 1. **해결방안**

ㅇㅇㅇ

※ 서버 내 존재하는 테스트파일 및 업로드 폴더 내 의심되는 파일(웹쉘 및 개발자가 임의로 생성한 파일)은 삭제 하여 주시기 바랍니다.

* + 1. 접근제어 우회 공격 (일반)
       1. **문제점**

테스트

[그림] 16. 테스트 파일 확인 ①

[그림] 17. 테스트 파일 확인 ②

* + - 1. **관련 URL**

| **번호** | **경로** | **URL** |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |

* + - 1. **해결방안**

ㅇㅇㅇ

※ 서버 내 존재하는 테스트파일 및 업로드 폴더 내 의심되는 파일(웹쉘 및 개발자가 임의로 생성한 파일)은 삭제 하여 주시기 바랍니다.

1. 주) OWASP : The Open Web Application Security Project [↑](#footnote-ref-1)
2. 주) NIST : National Institute of Standards and Technology [↑](#footnote-ref-2)