|  |
| --- |
| **Confidential** |

**웹 모의해킹**

**진단 보고서**

Coremall.com

**해킹최강 CERT 팀**

**2015. 08. 22**

개 정 이 력

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 버전 | 작성일 | 변경내용 | 작성자 | 비고 |
| 1.0 | 2015.08 |  | 키시아 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

목차

[**1 개요 8**](#_Toc461106445)

[**1.1 목적 8**](#_Toc461106447)

[**1.2 진단 방법 8**](#_Toc461106448)

[**1.3 진단 일정 8**](#_Toc461106449)

[**1.4 진단 담당자 8**](#_Toc461106450)

[**1.5 진단대상 8**](#_Toc461106451)

[**1.6 진단항목 9**](#_Toc461106452)

[**2 총평 10**](#_Toc461106460)

[**2.1 총평 요약 10**](#_Toc461106463)

[**3 상세 진단 결과 11**](#_Toc461106464)

[**3.1 SQL 인젝션 11**](#_Toc461106468)

[**3.1.1 취약점 정의 11**](#_Toc461106469)

[**3.1.2 상세분석 11**](#_Toc461106470)

[**3.1.3 보안대책 12**](#_Toc461106471)

[**3.2 정보누출 13**](#_Toc461106472)

[**3.2.1 취약점 정의 13**](#_Toc461106473)

[**3.2.2 상세분석 13**](#_Toc461106474)

[**3.2.3 보안대책 13**](#_Toc461106475)

[**3.3 악성 컨텐츠 14**](#_Toc461106476)

[**3.3.1 취약점 정의 14**](#_Toc461106477)

[**3.3.2 상세분석 14**](#_Toc461106478)

[**3.3.3 보안대책 15**](#_Toc461106479)

[**3.4 XSS (크로스 사이트 스크립팅) 16**](#_Toc461106480)

[**3.4.1 취약점 정의 16**](#_Toc461106481)

[**3.4.2 상세분석 16**](#_Toc461106482)

[**3.4.3 보안대책 17**](#_Toc461106483)

[**3.5 약한 문자열 강도 18**](#_Toc461106484)

[**3.5.1 취약점 정의 18**](#_Toc461106485)

[**3.5.2 상세분석 18**](#_Toc461106486)

[**3.5.3 보안대책 18**](#_Toc461106487)

[**3.6 불충분한 인증 및 인가 19**](#_Toc461106488)

[**3.6.1 취약점 정의 19**](#_Toc461106489)

[**3.6.2 상세분석 19**](#_Toc461106490)

[**3.6.3 보안대책 21**](#_Toc461106491)

[**3.7 자동화 공격 22**](#_Toc461106492)

[**3.7.1 취약점 정의 22**](#_Toc461106493)

[**3.7.2 상세분석 22**](#_Toc461106494)

[**3.7.3 보안대책 22**](#_Toc461106495)

[**3.8 파일 업로드 23**](#_Toc461106496)

[**3.8.1 취약점 정의 23**](#_Toc461106497)

[**3.8.2 상세분석 23**](#_Toc461106498)

[**3.8.3 보안대책 23**](#_Toc461106499)

[**3.9 불충분한 세션 관리 24**](#_Toc461106500)

[**3.9.1 취약점 정의 24**](#_Toc461106501)

[**3.9.2 상세분석 24**](#_Toc461106502)

[**3.9.3 보안대책 25**](#_Toc461106503)

[**3.10 CSRF (크로스 사이트 요청 변조) 26**](#_Toc461106504)

[**3.10.1 취약점 정의 26**](#_Toc461106505)

[**3.10.2 상세분석 26**](#_Toc461106506)

[**3.10.3 보안대책 27**](#_Toc461106507)

[**3.11 데이터 평문 전송 28**](#_Toc461106508)

[**3.11.1 취약점 정의 28**](#_Toc461106509)

[**3.11.2 상세분석 28**](#_Toc461106510)

[**3.11.3 보안대책 29**](#_Toc461106511)

[**3.12 파라미터 변조 30**](#_Toc461106512)

[**3.12.1 취약점 정의 30**](#_Toc461106513)

[**3.12.2 상세분석 30**](#_Toc461106514)

[**3.12.3 보안대책 31**](#_Toc461106515)

[**3.13 위치 공개 32**](#_Toc461106516)

[**3.13.1 취약점 정의 32**](#_Toc461106517)

[**3.13.2 상세분석 32**](#_Toc461106518)

[**3.13.3 보안대책 32**](#_Toc461106519)

**표 목차**

[**<표1- 1> 진단일정 8**](#_Toc461106828)

[**<표1- 2> 수행인원 8**](#_Toc461106829)

[**<표1- 3> WEB 진단대상 8**](#_Toc461106830)

[**<표1- 4> 웹 어플리케이션 소스 보안 진단 체크리스트 9**](#_Toc461106831)

[**<표2- 5> 취약점 진단 결과 10**](#_Toc461106832)

**그림 목차**

[**[그림 3- 1] SQL 인젝션 공격으로 DB 정보 획득 11**](#_Toc461106833)

[**[그림 3- 2] 잘못된 정보를 입력했을 때 DB 정보가 누출 된 모습 13**](#_Toc461106834)

[**[그림 3- 3] 악성 컨텐츠 작성 14**](#_Toc461106835)

[**[그림 3- 4] 작성된 악성 컨텐츠를 통해 이동된 페이지 이동 예 15**](#_Toc461106836)

[**[그림 3- 5] 제목에 스크립트를 삽입하는 모습 16**](#_Toc461106837)

[**[그림 3- 6] 스크립트가 실행된 모습 16**](#_Toc461106838)

[**[그림 3- 7] 단순한 패스워드로 회원가입 가능 18**](#_Toc461106839)

[**[그림 3- 8] idx 번호를 알아내는 모습 19**](#_Toc461106840)

[**[그림 3- 9] 다른 사용자의 글을 수정하는 페이지로 접근한 모습 20**](#_Toc461106841)

[**[그림 3- 10] 다른 사용자의 글을 삭제하는 페이지로 접근하는 모습 20**](#_Toc461106842)

[**[그림 3- 11] 다른 사용자의 글이 삭제 된 모습 21**](#_Toc461106843)

[**[그림 3- 12] 로그인 인증 실패 22**](#_Toc461106844)

[**[그림 3- 12] 악성프로그램 첨부 가능 23**](#_Toc461106845)

[**[그림 3- 13] 관리자의 쿠키로 변경하는 모습 24**](#_Toc461106846)

[**[그림 3- 14] 관리자로 로그인 된 모습 25**](#_Toc461106847)

[**[그림 3- 15] 사용자에 의해 작성된 글 26**](#_Toc461106848)

[**[그림 3- 16] 스크립트를 삽입 26**](#_Toc461106849)

[**[그림 3- 17] 게시 글 조회 시 스크립트에 의해 게시 글 삭제 27**](#_Toc461106850)

[**[그림 3- 18] 회원 가입 시 입력 정보가 평문으로 전송되는 모습 28**](#_Toc461106851)

[**[그림 3- 19] 회원 가입 시 패스워드가 평문으로 전송되는 모습 28**](#_Toc461106852)

[**[그림 3- 20] idx 값을 변경하여 다른 글을 삭제하는 페이지로 접근하는 모습 30**](#_Toc461106853)

[**[그림 3- 21] 다른 글이 삭제 된 모습 31**](#_Toc461106854)

[**[그림 3- 22] 실제 웹 페이지가 저장되는 경로의 노출 32**](#_Toc461106855)

1 개요

1. 1. **목적**

* 운영 중인 ??? 사이트의 보안진단을 통해 고객사의 개인정보 유출 및 보안 사고 방지 등 보안 강화에 그 목적
  1. **진단 방법**
* 고객과 협의 하에 운영 중인 사이트에 최적화된 진단항목을 이용하여 웹 페이지를 진단 수행
* 진단 항목을 기반으로 웹 페이지 진단 수행
  1. **진단 일정**
* 취약성 진단 수행 세부 일정은 다음과 같습니다.

|  |  |  |
| --- | --- | --- |
| **구분** | **내용** | **일정** |
| 대상선정 | 대상 협의 / 환경 분석 | 2015.08.15 |
| 기술적 점검 | 취약점 점검 수행 | 2015.08.15-2015.08.20 |
| 결과분석 / 보고 | 취약점 결과보고서 및 보안대책 작성 | 2015.08.21 |
| 보안진단결과보고서 제출 | 2015.08.22 |

<표1- 1> 진단일정

* 1. **진단 담당자**
* 취약성 진단을 수행하는 인력은 다음과 같습니다.

|  |  |  |
| --- | --- | --- |
| **수행인원** | **수행업무** | **연락처** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

<표1- 2> 수행인원

* 1. **진단대상**

|  |  |  |  |
| --- | --- | --- | --- |
| **구분** | **IP** | **WEB** | **비고** |
| 1 | 221.159.202.3 | ???.com | Web Server |

<표1- 3> WEB 진단대상

* 1. **진단항목**

진단항목 취약점 항목의 경우 'OWASP TOP 10‘과 ’주요 정보 통신 기반시설 취약점 분석·평가 기준‘ 항목을 바탕으로 작성.

총 28개 항목으로 세분화 되었으며, 실제 사이트에 접근하여 보안취약점 존재여부를 확인하는 방법으로 진단을 수행.



| **번호** | **코드** | **항목** | **위험도** |
| --- | --- | --- | --- |
| 1 | BO | 버퍼 오버플로우 | 상 |
| 2 | FS | 포맷스트링 | 상 |
| 3 | LI | LDAP 인젝션 | 상 |
| 4 | OC | 운영체제 명령 실행 | 상 |
| 5 | SI | SQL 인젝션 | 상 |
| 6 | SS | SSI 인젝션 | 상 |
| 7 | XI | XPath 인젝션 | 상 |
| 8 | DI | 디렉터리 인덱싱 | 상 |
| 9 | IL | 정보 누출 | 상 |
| 10 | CS | 악성 콘텐츠 | 상 |
| 11 | XS | 크로스사이트 스크립팅 | 상 |
| 12 | BF | 약한 문자열 강도 | 상 |
| 13 | IA | 불충분한 인증 | 상 |
| 14 | PR | 취약한 패스워드 복구 | 상 |
| 15 | CF | 크로스사이트 리퀘스트 변조(CSRF) | 상 |
| 16 | SE | 세션 예측 | 상 |
| 17 | IN | 불충분한 인가 | 상 |
| 18 | SC | 불충분한 세션 만료 | 상 |
| 19 | SF | 세션 고정 | 상 |
| 20 | AU | 자동화 공격 | 상 |
| 21 | PV | 프로세스 검증 누락 | 상 |
| 22 | FU | 파일 업로드 | 상 |
| 23 | FD | 파일 다운로드 | 상 |
| 24 | AE | 관리자 페이지 노출 | 상 |
| 25 | PT | 경로 추적 | 상 |
| 26 | PL | 위치 공개 | 상 |
| 27 | SN | 데이터 평문 전송 | 상 |
| 28 | CC | 쿠키 변조 | 상 |

<표1- 4> 웹 어플리케이션 소스 보안 진단 체크리스트

2 총평

2. 1. **총평 요약**

???사이트 진단 결과 13개의 취약점이 발견 되었으며, 불충분한 인증 및 인가

취약점, 파일 업로드 등은 빠른 조치를 취할 것을 권고 합니다.

또한, SQL 인젝션, 서버 정보노출, 악성 콘텐츠, XSS, 약한 문자열 강도

자동화 공격, 데이터 평문 전송, 쿠키 변조, 불출분한 세션 관리 파라미터 변조

관리자 페이지 노출 등 취약점이 발견 되었습니다.

시큐어 코딩 등과 같은 보안 대책을 권고 합니다.

| **번호** | **코드** | **항목** | **위험도** | **진단결과** |
| --- | --- | --- | --- | --- |
| 1 | BO | 버퍼 오버플로우 | 상 | **양호** |
| 2 | FS | 포맷스트링 | 상 | **양호** |
| 3 | LI | LDAP 인젝션 | 상 | **양호** |
| 4 | OC | 운영체제 명령 실행 | 상 | **양호** |
| 5 | SI | SQL 인젝션 | 상 | **취약** |
| 6 | SS | SSI 인젝션 | 상 | **취약** |
| 7 | XI | XPath 인젝션 | 상 | **취약** |
| 8 | DI | 디렉터리 인덱싱 | 상 | **취약** |
| 9 | IL | 정보 누출 | 상 | **취약** |
| 10 | CS | 악성 콘텐츠 | 상 | **취약** |
| 11 | XS | 크로스사이트 스크립팅 | 상 | **취약** |
| 12 | BF | 약한 문자열 강도 | 상 | **취약** |
| 13 | IA | 불충분한 인증 | 상 | **취약** |
| 14 | PR | 취약한 패스워드 복구 | 상 | **취약** |
| 15 | CF | 크로스사이트 리퀘스트 변조(CSRF) | 상 | **취약** |
| 16 | SE | 세션 예측 | 상 | **취약** |
| 17 | IN | 불충분한 인가 | 상 | **취약** |
| 18 | SC | 불충분한 세션 만료 | 상 | **취약** |
| 19 | SF | 세션 고정 | 상 | **취약** |
| 20 | AU | 자동화 공격 | 상 | **취약** |
| 21 | PV | 프로세스 검증 누락 | 상 | **취약** |
| 22 | FU | 파일 업로드 | 상 | **취약** |
| 23 | FD | 파일 다운로드 | 상 | **취약** |
| 24 | AE | 관리자 페이지 노출 | 상 | **취약** |
| 25 | PT | 경로 추적 | 상 | **취약** |
| 26 | PL | 위치 공개 | 상 | **취약** |
| 27 | SN | 데이터 평문 전송 | 상 | **취약** |
| 28 | CC | 쿠키 변조 | 상 | **취약** |

<표2- 5> 취약점 진단 결과

3 상세 진단 결과

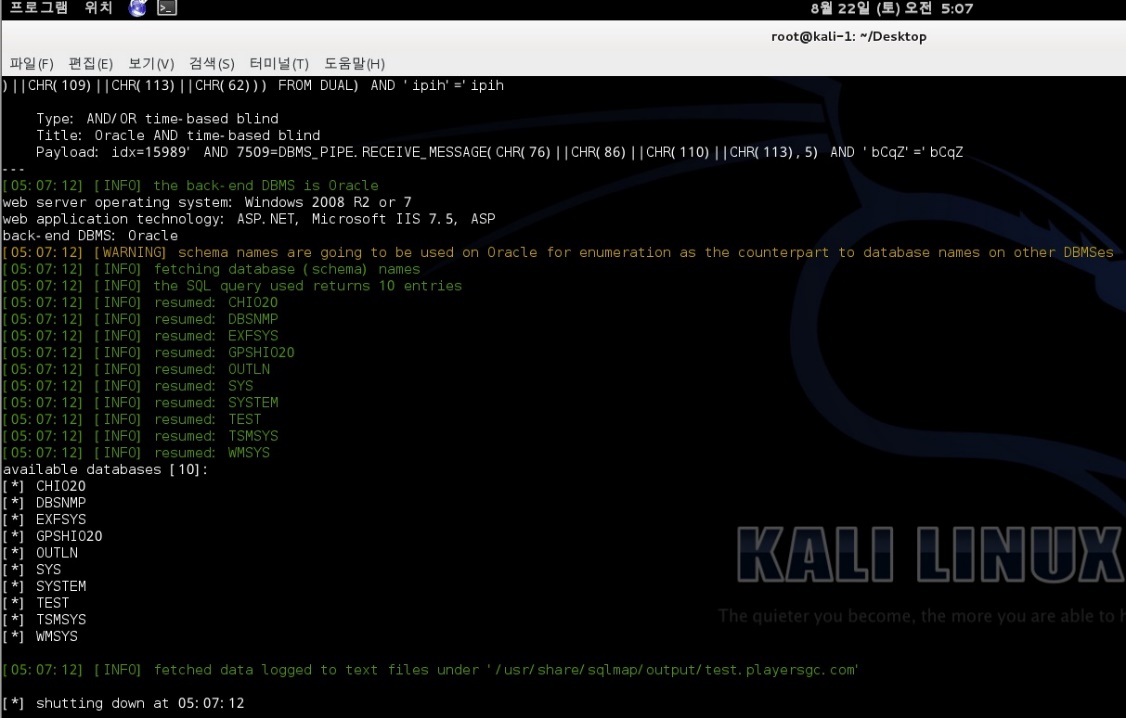
3. 1. **SQL 인젝션**
      1. **취약점 정의**

SQL 인젝션은 응용프로그램 보안 상의 허점을 의도적으로 이용해, 개발자가 생각지 못한 SQL문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작하는 공격 방법입니다.

* + 1. **상세분석**

|  |  |
| --- | --- |
| 취약한 경로 | /04/01\_view.asp?idx=  /04/02\_view.asp?idx=  /04/03\_view.asp?idx=  /04/04\_view.asp?idx=  /04/05\_view.asp?idx= |
| 설명 | SQL 인젝션 공격에 취약한 파라미터가 존재하며, 이 취약점을 통해 DB의 중요한 정보를 공격자가 탈취 가능함 |

**[Step #1]**



[그림 3- 1] SQL 인젝션 공격으로 DB 정보 획득

* + 1. **보안대책**

- 사용자 입력 값 중 DB 쿼리에 사용될 수 있는 ‘, “, -와 같은 문자의 필터링을 권고합니다.

또한 아래코드 형태의 BlackList 필터링 기법이 아닌 허용된 문자만 입력 받는 WhiteList방식으로 필터링 될 것을 권고합니다.

**[ BlackList = Array("--", ";", "/\*", "\*/", "@@", "@",\_**

**"char", "nchar", "varchar", "nvarchar",\_**

**"alter", "begin", "cast", "create", "cursor",\_**

**"declare", "delete", "drop", "end", "exec",\_**

**"execute", "fetch", "insert", "kill", "open",\_**

**"select", "sys", "sysobjects", "syscolumns",\_**

**"table", "update","'", "and", "cast", "substring",\_**

**"<script>", "</script>","document.cookie") ]**

* 1. **정보누출**
     1. **취약점 정의**

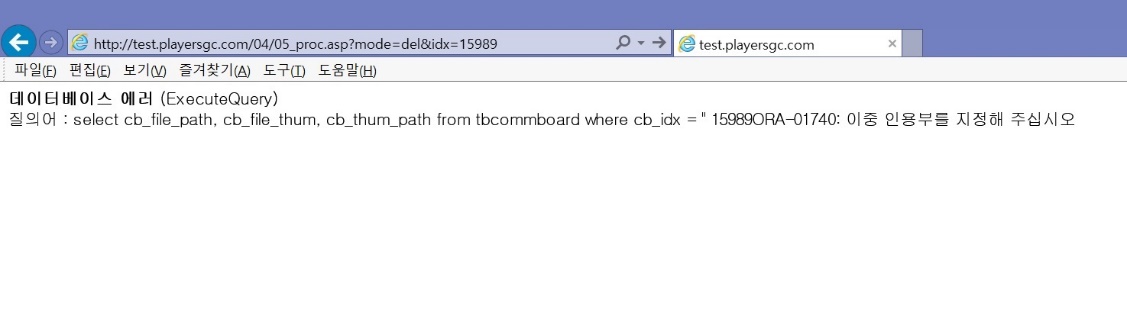
웹 어플리케이션의 민감한 정보가 개발자의 부주의로 인해 노출되는 것으로 중요 정보(관리자 계정 및 테스트 계정 등)를 주석구문에 포함시켜 의도하지 않게 정보가 노출되는 취약점 입니다.

또한 디폴트로 설정된 에러 페이지를 그대로 사용할 경우 시스템 내부 문제점을 자세하게 출력해주기 때문에 절대경로, 상태코드, 데이터베이스 종류, 질의 문 등이 노출될 수 있으며 이 밖에도 공격자가 검색엔진을 통하여 각종 개인 정보 및 서버 정보 등 해킹에 필요한 정보를 획득할 수 있습니다.

* + 1. **상세분석**

|  |  |
| --- | --- |
| 취약한 경로 | /04/01\_view.asp?idx=  /04/02\_view.asp?idx=  /04/03\_view.asp?idx=  /04/04\_view.asp?idx=  /04/05\_view.asp?idx= |
| 설명 | DB에러페이지에서 DB 테이블 및 칼럼 정보 노출 |

**[Step #1]**



[그림 3- 2] 잘못된 정보를 입력했을 때 DB 정보가 누출 된 모습

* + 1. **보안대책**

- 웹 어플리케이션 : 모든 웹 페이지에 대해 개발단계에서 디버깅 및 테스트를 목적으로 작성한 주석구문에 서버 주요 정보가 포함되어 있을 경우 공격자가 해당 정보를 다른 취약점과 연계해 사용할 수 있으므로 제거 권고합니다.

- 웹 서버 보안 설정 : 공통의 에러 페이지를 웹 서버에서 보안 설정 합니다.

1. **[별첨] 진단항목**

* 행전안전부에서 제시한 “주요정보통신기반시설 웹(WEB) 취약점 분석․평가 가이드라인”에 근거하여 통제평가 리스트를 작성하였음

|  |  |  |  |
| --- | --- | --- | --- |
| **코드** | **취약점명** | **설 명** | **등급** |
| BO | 버퍼  오버플로우 | 메모리나 버퍼의 블록 크기보다 더 많은 데이터를 넣음으로써 결함을 발생시키는 취약점 | H |
| FS | 포맷스트링 | 스트링을 처리하는 부분에서 메모리 공간에 접근할 수 있는 문제를 이용하는 취약점 | H |
| LI | LDAP  인젝션 | LDAP(Lightweight Directory Access Protocol) 쿼리를 주입함으로서 개인정보 등의 내용이 유출될 수 있는 문제를 이용하는 취약점 | H |
| OC | 운영체제  명령실행 | 웹 사이트의 인터페이스를 통해 웹 서버를 운영하는 운영체제 명령을 실행하는 취약점 | H |
| SI | SQL인젝션 | SQL문으로 해석될 수 있는 입력을 시도하여 데이터베이스에 접근할 수 있는 취약점 | H |
| SS | SSI인젝션 | SSI(Server-side Include)는 “Last modified"와 같이 서버가 HTML 문서에 입력하는 변수 값으로, 웹 서버 상에 있는 파일을 include 시키고, 명령문이 실행되게 하여 데이터에 접근할 수 있는 취약점 | H |
| XI | XPath  인젝션 | 조작된 XPath(XML Path Language) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리해 올 수 있는 취약점 | H |
| DI | 디렉터리  인덱싱 | 요청 파일이 존재하지 않을 때 자동적으로 디렉터리 리스트를 출력하는 취약점 | H |
| IL | 정보누출 | 웹 사이트 데이터가 노출되는 것으로 개발과정의 코멘트나 오류 메시지 등에서 중요한 정보가 노출되어 공격자에게 2차 공격을 하기 위한 중요한 정보를 제공할 수 있는 취약점 | H |
| CS | 악성콘텐츠 | 웹 어플리케이션에 정상적인 콘텐츠 대신에 악성 콘텐츠를 주입하여 사용자에게 악의적인 영항을 미치는 취약점 | H |
| XS | 크로스  사이트  스크립팅 | 웹 어플리케이션을 사용해서 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점 | H |
| BF | 약한문자열강도 | 사용자의 이름이나 패스워드, 신용카드 정보나 암호화 키 등을 자동으로 대입하여 여러 시행착오 후에 맞는 값이 발견되는 취약점 | H |
| IA | 불충분한 인증 | 민감한 데이터에 접근할 수 있는 곳에 취약한 인증 메커니즘으로 구현된 취약점 | H |
| PR | 취약한  패스워드 복구 | 취약한 패스워드 복구 메커니즘(패스워드 찾기 등)에 대해 공격자가 불법적으로 다른 사용자의 패스워드를 획득, 변경, 복구할 수 있는 취약점 | H |
| CF | 크로스사이트  리퀘스트  변조(CSRF) | CSRF 공격은 로그온 한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 취약한 웹 어플리케이션에 전송하는 취약점 | H |
| SE | 세션 예측 | 단순히 숫자가 증가하는 방법 등의 취약한 특정 세션의 식별자(ID)를 예측하여 세션을 가로챌 수 있는 취약점 | H |
| IN | 불충분한 인가 | 민감한 데이터 또는 기능에 대한 접근권한 제한을 두지 않은 취약점 | H |
| SC | 불충분한 세션만료 | 세션의 만료 기간을 정하지 않거나, 만료 일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하게 되는 취약점 | H |
| SF | 세션고정 | 세션 값을 고정하여 명확한 세션 식별자(ID) 값으로 사용자가 로그인하여 정의된 세션 식별자(ID)가 사용 가능하게 되는 취약점 | H |
| AU | 자동화공격 | 웹 어플리케이션에 정해진 프로세스에 자동화된 공격을 수행함으로써 자동으로 수많은 프로세스가 진행되는 취약점 | H |
| PV | 프로세스  검증누락 | 공격자가 응용의 계획된 플로우 통제를 우회하는 것을 허가하는 취약점 | H |
| FU | 파일업로드 | 파일을 업로드 할 수 있는 기능을 이용하여 시스템 명령어를 실행할 수 있는 웹 프로그램을 업로드 할 수 있는 취약점 | H |
| FD | 파일  다운로드 | 파일 다운로드 스크립트를 이용하여 첨부된 주요 파일을 다운로드 할 수 있는 취약점 | H |
| AE | 관리자  페이지 노출 | 단순한 관리자 페이지 이름(admin, manager 등)이나 설정, 프로그램 설계상의 오류로 인해 관리자 메뉴에 직접 접근할 수 있는 취약점 | H |
| PT | 경로추적 | 공격자에게 외부에서 디렉터리에 접근할 수 있는 것이 허가되는 문제점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하고 실행 할 수 있는 취약점 | H |
| PL | 위치공개 | 예측 가능한 디렉터리나 파일명을 사용하여 해당 위치가 쉽게 노출되어 공격자가 이를 악용하여 대상에 대한 정보와 민감한 정보가 담긴 데이터에 접근이 가능하게 되는 취약점 | H |
| SN | 데이터  평문전송 | 서버와 클라이언트 간의 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 평문으로 전송되는 취약점 | H |
| CC | 쿠키변조 | 적절히 보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등이 가능한 취약점 | H |

**※ 취약도 정의**

|  |  |
| --- | --- |
| * H (High) | 악의적인 사용자가 직접적으로 시스템의 관리자 권한을 획득하여 웹 위변조가 가능하거나, 웹 사용자의 개인정보를 유출할 수 있는 취약점 |
| * M (Medium) | 악의적인 사용자에 의해 시스템에 중요자원 및 웹 최상위 권한을 획득할 수 있고 이로 인해 추가 공격으로 이용될 수 있는 취약점 |
| * L (Low) | 해당 취약점의 노출로 인해 시스템의 정보를 획득하여 추가 공격으로 이용될 수 있는 취약점 |