

# 웹 모의해킹 진단 보고서

Coremall.com

연람희

2021. 07. 02

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

## 개 정 이 력

| 버전  | 작성일        | 변경내용 | 작성자 | 비고 |
|-----|------------|------|-----|----|
| 1.0 | 2021.07.02 |      | 연람희 |    |
|     |            |      |     |    |
|     |            |      |     |    |
|     |            |      |     |    |
|     |            |      |     |    |
|     |            |      |     |    |

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

## 목차

|                       |    |
|-----------------------|----|
| 1 개요 .....            | 6  |
| 1.1 목적 .....          | 6  |
| 1.2 진단 방법 .....       | 6  |
| 1.3 진단 일정 및 계획 .....  | 6  |
| 1.4 진단 담당자 .....      | 6  |
| 1.5 진단대상 .....        | 6  |
| 1.6 진단항목 .....        | 7  |
| 2 총평 .....            | 9  |
| 2.1 총평 요약 .....       | 9  |
| 3 상세 진단 결과 .....      | 11 |
| 3.1 SQL 인젝션 .....     | 11 |
| 3.1.1 취약점 정의 .....    | 11 |
| 3.1.2 상세분석 .....      | 11 |
| 3.1.3 보안대책 .....      | 12 |
| 3.2 정보누출 .....        | 13 |
| 3.2.1 취약점 정의 .....    | 13 |
| 3.2.2 보안대책 .....      | 13 |
| 3.3 크로스사이트 스크립팅 ..... | 14 |
| 3.3.1 취약점 정의 .....    | 14 |
| 3.3.2 보안대책 .....      | 15 |
| 3.4 약한 문자열 강도 .....   | 16 |
| 3.4.1 취약점 정의 .....    | 16 |
| 3.4.2 보안대책 .....      | 17 |
| 3.5 불충분한 인증 .....     | 18 |
| 3.5.1 취약점 정의 .....    | 18 |

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

|        |                   |    |
|--------|-------------------|----|
| 3.5.2  | 보안대책 .....        | 18 |
| 3.6    | 취약한 패스워드 복구 ..... | 19 |
| 3.6.1  | 취약점 정의 .....      | 19 |
| 3.6.2  | 보안대책 .....        | 20 |
| 3.7    | 세션만료 .....        | 21 |
| 3.7.1  | 취약점 정의 .....      | 21 |
| 3.7.2  | 보안대책 .....        | 22 |
| 3.8    | 세션고정 .....        | 23 |
| 3.8.1  | 취약점 정의 .....      | 23 |
| 3.8.2  | 보안대책 .....        | 23 |
| 3.9    | 자동화 공격 .....      | 24 |
| 3.9.1  | 취약점 정의 .....      | 24 |
| 3.9.2  | 보안대책 .....        | 25 |
| 3.10   | 관리자 페이지 노출 .....  | 26 |
| 3.10.1 | 취약점 정의 .....      | 26 |
| 3.10.2 | 보안대책 .....        | 26 |
| 3.11   | 데이터 평문 전송 .....   | 27 |
| 3.11.1 | 취약점 정의 .....      | 27 |
| 3.11.2 | 보안대책 .....        | 27 |

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

## 표 목차

|                                       |    |
|---------------------------------------|----|
| <표1- 1> 진단일정 .....                    | 6  |
| <표1- 2> 수행인원 .....                    | 6  |
| <표1- 3> WEB 진단대상 .....                | 6  |
| <표1- 4> 웹 어플리케이션 소스 보안 진단 체크리스트 ..... | 8  |
| <표2- 5> 취약점 진단 결과 .....               | 10 |

## 그림 목차

|  |    |
|--|----|
| [그림 3- 1] SQL 인젝션 공격 시도(로그인) .....               | 11 |
| [그림 3- 2] SQL 인젝션 공격 시도 .....                    | 11 |
| [그림 3- 3] 잘못된 정보를 입력했을 때 에러메시지/포트 정보 누출 모습 ..... | 13 |
| [그림 3- 4] HTML을 사용하여 게시글 등록 .....                | 14 |
| [그림 3- 5] alert 확인 .....                         | 15 |
| [그림 3- 5] test 아이디 로그인 시도 .....                  | 16 |
| [그림 3- 6] test 아이디 로그인 됨을 확인 .....               | 17 |
| [그림 3- 7] 개인정보 페이지 접근 시 바로 정보 확인 가능 .....        | 18 |
| [그림 3- 8] 개인정보 입력 후 패스워드 복구 시도 .....             | 19 |
| [그림 3- 9] 임시 패스워드가 웹페이지 상 노출 .....               | 20 |
| [그림 3- 10] 세션 만료 확인 시작 .....                     | 21 |
| [그림 3- 11] 12분 경과 후 세션 만료되지 않음 .....             | 22 |
| [그림 3- 12] 세션ID 값이 동일하게 남아있는 것을 확인 .....         | 23 |
| [그림 3- 13] 툴을 이용한 도배 공격 중 .....                  | 24 |
| [그림 3- 14] 다수의 패킷이 전송되어 도배글이 작성됨 .....           | 25 |
| [그림 3- 15] 관리자 로그인 페이지가 노출됨을 확인 .....            | 26 |
| [그림 3- 16] 평문으로 아이디와 비밀번호가 보여지는 것을 확인 .....      | 27 |

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

## 1 개요

### 1.1 목적

- 운영 중인 코어몰 사이트의 보안진단을 통해 고객사의 개인정보 유출 및 보안 사고 방지 등 보안 강화에 그 목적

### 1.2 진단 방법

- 고객과 협의 하에 운영 중인 사이트에 최적화된 진단항목을 이용하여 웹 페이지를 진단 수행
- 진단 항목을 기반으로 웹 페이지 진단 수행

### 1.3 진단 일정 및 계획

- 취약성 진단 수행 세부 일정 아래 참조

| 구분        | 내용                  | 일정                      |
|-----------|---------------------|-------------------------|
| 대상선정      | 대상 협의 / 환경 분석       | 2021.06.25              |
| 점검항목      | 주요 점검 항목 정리 및 계획 수립 | 2021.06.25              |
| 기술적 점검    | 취약점 점검 수행           | 2021.06.25 - 2021.07.01 |
| 결과분석 / 보고 | 취약점 결과보고서 및 보안대책 작성 | 2021.07.01              |
|           | 보안진단결과보고서 제출 및 발표   | 2021.07.02              |

<표1- 1> 진단일정

### 1.4 진단 담당자

- 취약성 진단을 수행하는 인력

| 수행인원 | 수행업무       | 연락처 |
|------|------------|-----|
| 연람희  | 계획, 점검, 보고 |     |
|      |            |     |
|      |            |     |
|      |            |     |

<표1- 2> 수행인원

### 1.5 진단대상

| 구분 | IP             | WEB                    | 비고         |
|----|----------------|------------------------|------------|
| 1  | 124.53.136.207 | http://124.53.136.207/ | Web Server |

<표1- 3> WEB 진단대상

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

## 1.6 진단항목

- 진단항목 취약점 항목의 경우 'OWASP TOP 10'과 '주요 정보 통신 기반시설 취약점 분석·평가 기준' 항목을 바탕으로 작성됨.
- 총 28개 항목으로 세분화되었으며, 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   |

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

| 번호 | 코드 | 항목         | 위험도 |
|----|----|------------|-----|
| 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



|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

## 2 총평

### 2.1 총평 요약

- 코어몰 사이트 진단 결과 11 개의 취약점 발견
- SQL 인젝션, 정보노출, 악성 콘텐츠, 약한 문자열 강도 자동화 공격, 데이터 평문 전송, 불충분한 세션 관리 파라미터 변조, 관리자 페이지 노출 등 취약점이 발견됨.
- SSL 데이터 암호화 및 시큐어 코딩 등과 같은 보안 대책을 권고.

| 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   | 양호   |
| 7  | XI | XPath 인젝션            | 상   | 양호   |
| 8  | DI | 디렉터리 인덱싱             | 상   | 양호   |
| 9  | IL | 정보 누출                | 상   | 취약   |
| 10 | CS | 악성 콘텐츠               | 상   | 양호   |
| 11 | XS | 크로스사이트 스크립팅          | 상   | 취약   |
| 12 | BF | 약한 문자열 강도            | 상   | 취약   |
| 13 | IA | 불충분한 인증              | 상   | 취약   |
| 14 | PR | 취약한 비밀번호 복구          | 상   | 취약   |
| 15 | CF | 크로스사이트 리퀘스트 변조(CSRF) | 상   | 양호   |
| 16 | SE | 세션 예측                | 상   | 양호   |
| 17 | IN | 불충분한 인가              | 상   | 양호   |
| 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   | 양호   |

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

| 번호 | 코드 | 항목         | 위험도 | 진단결과 |
|----|----|------------|-----|------|
| 22 | FU | 파일 업로드     | 상   | 양호   |
| 23 | FD | 파일 다운로드    | 상   | 양호   |
| 24 | AE | 관리자 페이지 노출 | 상   | 취약   |
| 25 | PT | 경로 추적      | 상   | 양호   |
| 26 | PL | 위치 공개      | 상   | 양호   |
| 27 | SN | 데이터 평문 전송  | 상   | 취약   |
| 28 | CC | 쿠키 변조      | 상   | 양호   |

<표2- 5> 취약점 진단 결과

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3 상세 진단 결과

#### 3.1 SQL 인젝션

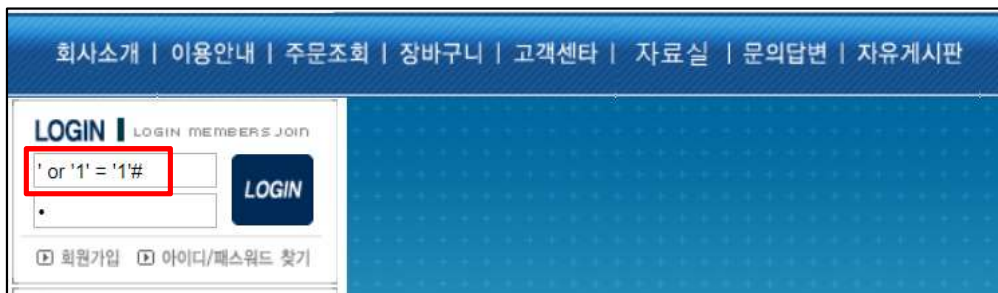
##### 3.1.1 취약점 정의

SQL 인젝션(SQL 삽입, SQL 주입으로도 불린다)은 코드 인젝션의 한 기법으로 클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격할 수 있는 공격방식을 말함.

##### 3.1.2 상세분석

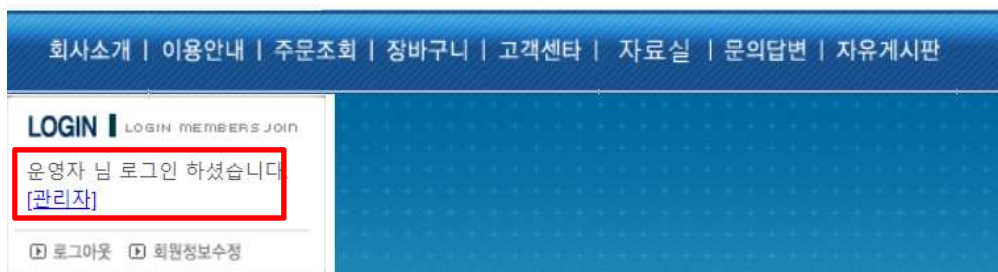
|        |   |
|--------|---|
| 취약한 경로 | ' or '1' = '1'#<br>ID'#(예: test'#)                            |
| 설명     | SQL 인젝션 공격에 취약한 파라미터가 존재하며, 이 취약점을 통해 DB의 중요한 정보를 공격자가 탈취 가능함 |

##### [Step #1] 로그인창에 SQL 인젝션 구문 [' or '1'='1'#] 삽입



[그림 3- 1] SQL 인젝션 공격 시도(로그인)

##### [Step #2] 운영자 계정으로 로그인 확인



[그림 3- 2] SQL 인젝션 공격 시도

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.1.3 보안대책

- 웹 서버 이전에 웹 방화벽 설치
- 사용자 입력 값 중 DB 쿼리에 사용될 수 있는 ', ", -와 같은 문자의 필터링을 권고
- 시큐어 코딩 작성. SQL 인젝션에 취약하지 않는 프로그래밍 코딩 수행.
- 허용된 문자만 입력 받는 White list 방식으로 필터링

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

## 3.2 정보누출

### 3.2.1 취약점 정의

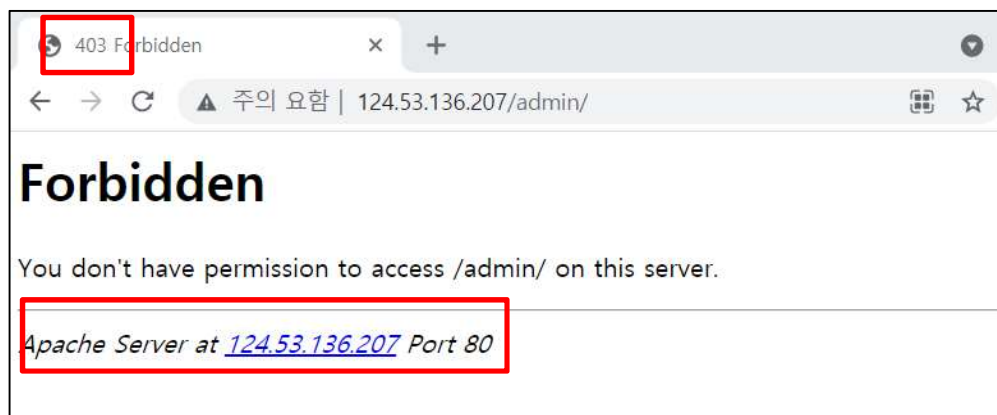
웹 사이트에 중요정보(개인정보, 계정정보, 금융정보 등)가 노출되거나 에러발생 시 과도한 정보(애플리케이션 정보, DB 정보, 웹 서버 구성 정보, 개발 과정의 코멘트 등)가 노출될 경우 공격자들의 2차 공격을 위한 정보로 활용될 수 있음.

에러 페이지로 인한 노출은 웹 서버의 버전과 어떤 시스템을 사용 중인지, 그리고 물리적인 디렉토리 경로까지 노출될 수 있음.

#### 상세분석

|        |   |
|--------|---|
| 취약한 경로 | http://124.53.136.207/admin/<br>http://124.53.136.207/board_data/ |
| 설명     | 페이지 에러 메시지 중 에러 타입, 포트번호 확인 가능                                    |

#### [Step #1] 디렉토리 접근 시도



[그림 3- 3] 잘못된 정보를 입력했을 때 에러메시지/포트 정보 누출 모습

### 3.2.2 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 필수.
- 웹 서버 보안 설정 : 공통된 에러 메시지를 표시하도록 설정

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.3 크로스사이트 스크립팅

#### 3.3.1 취약점 정의

웹에서 사용자 입력 값에 대한 필터링이 이루어지지 않을 경우 공격자는 게시판을 사용하여 악의적인 스크립트를 삽입하여 악성코드를 유포 사이트로 Redirect 할 수 있음

#### 상세분석

|        |  |
|--------|--|
| 취약한 경로 |  |
| 설명     | 코드를 사용하여 경고창이 나오도록 공격                    |

#### [Step #1] 코드 입력

옵션

☒ HTML사용
 ☐ 비밀번호사용

제목

XSS 테스트

내용



첨부\_1

파일 선택

선택된 파일 없음

[그림 3- 4] HTML을 사용하여 게시물 등록

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

#### [Step #2] 공격 완료



[그림 3- 5] alert 확인

#### 3.3.2 보안대책

- 웹 사이트에서 실행될 수 있는 스크립트 언어(HTML, Javascript 등) 태그 사용을 제한하고 사용자 입력 값에 대한 필터링 작업이 필요

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.4 약한 문자열 강도

#### 3.4.1 취약점 정의

웹페이지 내 로그인 폼 등에 약한 강도의 문자열 사용. 유추 가능한 문자열을 사용하여 타 이용자의 아이디로 로그인을 함

해당 취약점 존재 시 유추가 용이한 계정 및 패스워드의 사용으로 인한 사용자 권한 탈취 위험이 존재하며, 해당 위험을 방지하기 위해 값의 적절성 및 복잡성을 검증하는 로직을 구현하여야 함

#### 상세분석

|        |                                |
|--------|--------------------------------|
| 취약한 경로 | ID: test, PW: 1234             |
| 설명     | test 라는 아이디와 취약한 패스워드를 사용해 로그인 |

#### [Step #1] 유추 가능한 로그인 아이디/비밀번호 입력



[그림 3- 6] test 아이디 로그인 시도



|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

**[Step #2] 로그인 내용 확인**



[그림 3- 7] test 아이디 로그인 됨을 확인

**3.4.2 보안대책**

- 계정 및 비밀번호의 체크 로직을 구현하여 쉽게 유추하지 못하도록 함
  - 1) 영문 대소문자, 숫자, 특수문자 조합의 비밀번호로 설정하도록 함
  - 2) 연속적인 숫자, 생일, 전화번호 등의 아이디와 비밀번호는 사용하지 않도록 권고
  - 3) 비밀번호 유효기간을 설정하여 주기적으로 변경할 것을 권고
  - 4) 최근 사용되었던 비밀번호 재사용 금지
- 기존에 생성되어있던 계정들을 재점검하여 비밀번호를 변경할 수 있도록 함

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.5 불충분한 인증

#### 3.5.1 취약점 정의

중요정보 페이지에 대한 인증 절차가 불충분할 경우 권한이 없는 사용자가 중요 정보 페이지에 접근할 수 있음

#### 상세분석

|        |                       |
|--------|-----------------------|
| 취약한 경로 | 개인정보수정                |
| 설명     | 개인정보 페이지 접근 시 재인증 불충분 |

#### [Step #1] 회원정보 수정 페이지로 접근

HOME > 회원수정

회원 수정폼 ( 표시는 필수 항목입니다. 반드시 기입하여 주십시오)

|         |  |          |  |
|---------|--|----------|--|
| 아이디     | test   |          |  |
| 기존 패스워드 |  |          |  |
| 새 패스워드  |  | 새 패스워드확인 |  |
| 성명(실명)  | test   |          |  |
| 주민등록번호  | 870302 - *****   |          |  |
| 성별      | 남성 <input checked="" type="radio"/> 여성 <input type="radio"/> | 생년월일     |  |
| 연락처     | 010-1234-4568  | 휴대전화     |  |
| 우편번호    | 158 - 752  | 우편번호찾기   |  |
| 자택주소    | 서울시  |          |  |

[그림 3- 8] 개인정보 페이지 접근 시 바로 정보 확인 가능

#### 3.5.2 보안대책

- 중요정보를 표시하는 페이지에 접근할 시 본인 인증을 재확인하는 룰을 설정해야하며, 사용자가 인증 후 이요 가능한 페이지에 접근할 때마다 승인된 사용자인지 검증하여야함

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.6 취약한 패스워드 복구

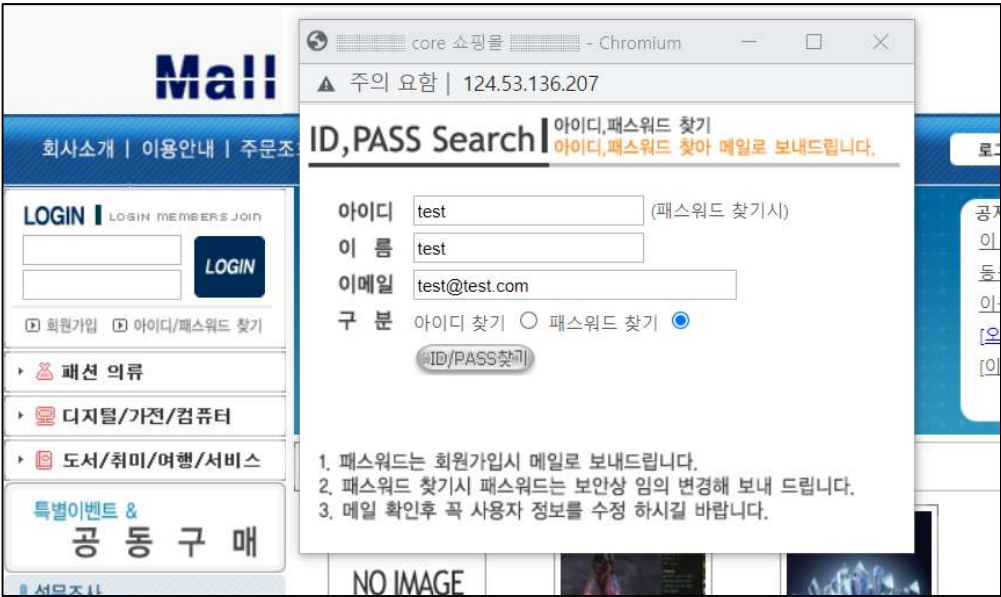
#### 3.6.1 취약점 정의

취약한 패스워드 복구 로직으로 인하여 공격자가 다른 사용자의 패스워드를 획득, 변경할 수 있음

#### 상세분석

|        |                              |
|--------|------------------------------|
| 취약한 경로 | 패스워드 변경                      |
| 설명     | 패스워드 변경 시 임시 패스워드가 웹페이지 상 노출 |

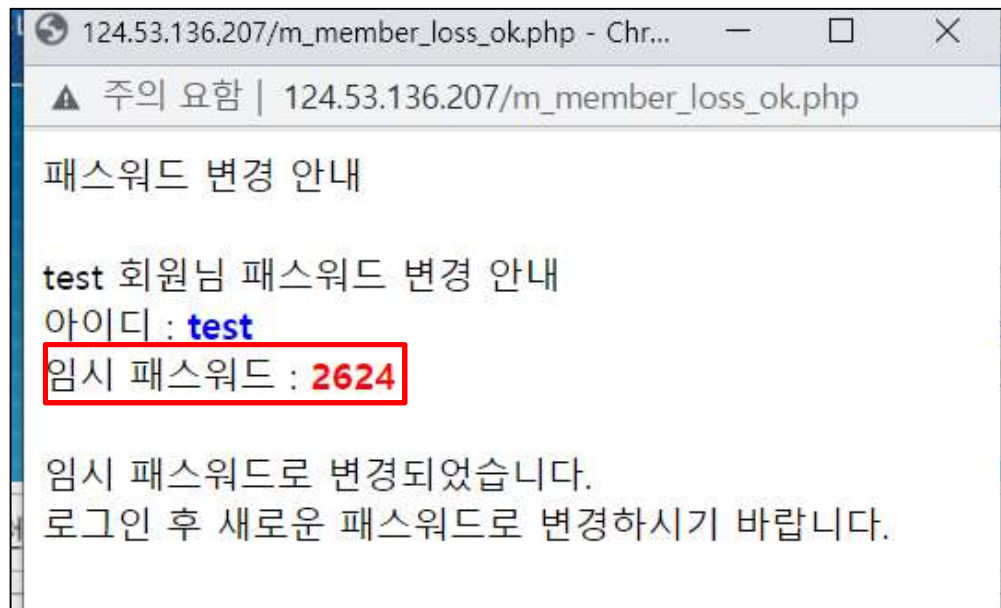
#### [Step #1] 패스워드 복구



[그림 3- 9] 개인정보 입력 후 패스워드 복구 시도

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

**[Step #2] 패스워드 복구 내용 확인**



[그림 3- 10] 임시 패스워드가 웹페이지 상 노출

### 3.6.2 보안대책

- 사용자 패스워드 발급 혹은 확인 시 웹 사이트 화면에 바로 출력해주는 것이 아니라 인증된 사용자 메일이나 SMS 로 전송
- 패스워드 재발급 검증 실패에 대한 횟수를 계산하여 일정 횟수 이상 실패한 경우 다른 방식으로 패스워드 찾기 기능을 제공해야함.

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.7 세션만료

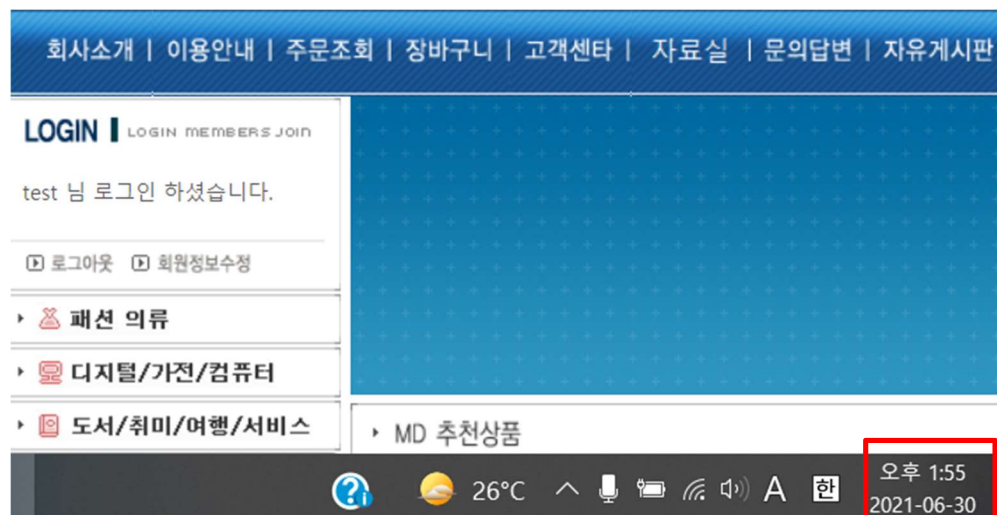
#### 3.7.1 취약점 정의

세션 만료 기간을 정하지 않거나 만료기한을 너무 길게 설정한 경우 악의적인 사용자가 만료되지 않은 세션을 활용하여 불법 접근을 할 수 있음

#### 상세분석

|        |                          |
|--------|--------------------------|
| 취약한 경로 | 로그인 세션 만료                |
| 설명     | 10 분 후 로그인 세션이 만료 되는지 확인 |

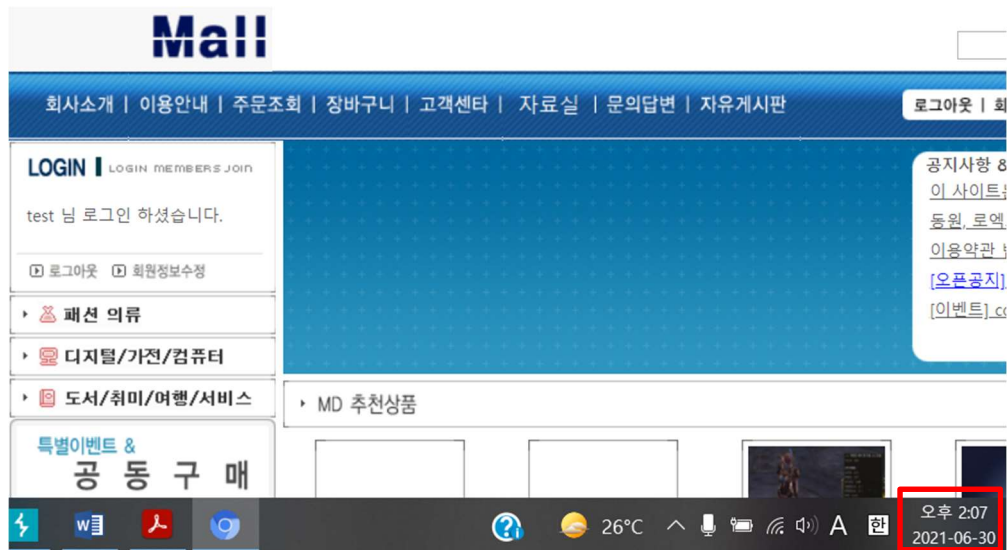
#### [Step #1] 10 분간 세션 만료 여부 확인



[그림 3- 11] 세션 만료 확인 시작

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

**[Step #2] 10 분 후 세션 만료 여부 확인**



[그림 3- 12] 12분 경과 후 세션 만료되지 않음

### 3.7.2 보안대책

- 세션 타임아웃 구현 시 타임아웃 시간은 10 분으로 설정할 것을 권고

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.8 세션고정

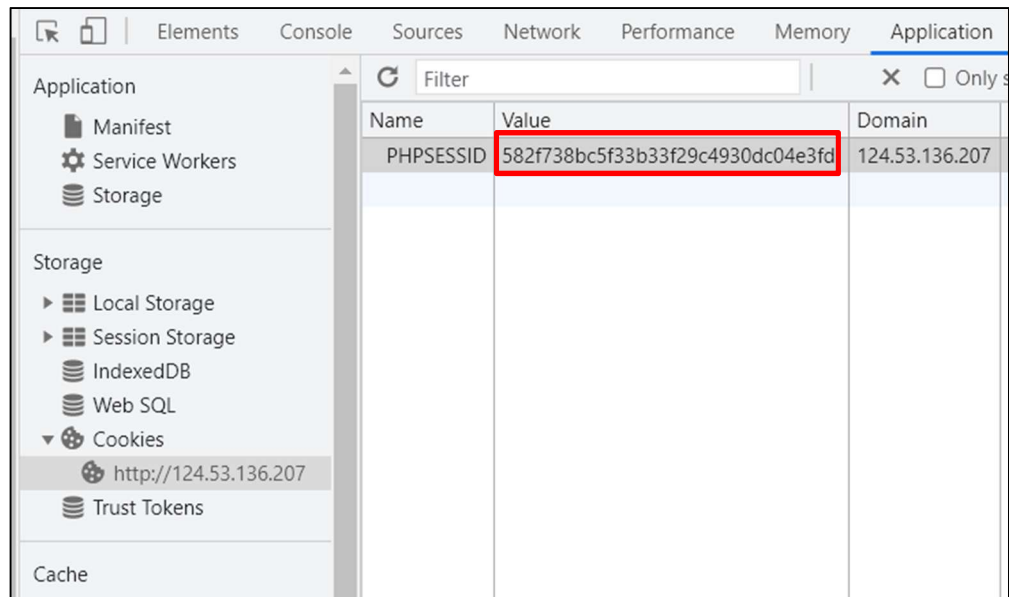
#### 3.8.1 취약점 정의

사용자 로그인 시 항상 일정하게 고정된 세션 ID 가 발생하는 경우 세션 ID 를 도용한 접근 및 권한 우회가 가능

#### 상세분석

|        |                             |
|--------|-----------------------------|
| 취약한 경로 | 로그인 세션 ID 고정                |
| 설명     | 로그아웃후 다시 로그인 시도 시 세션 동일함 확인 |

#### [Step #1] 로그아웃, 재 로그인 시도



[그림 3- 13] 세션ID 값이 동일하게 남아있는 것을 확인

#### 3.8.2 보안대책

- 로그인 시 세션 ID 발행 내용을 확인하고 로그아웃 후 다시 로그인 할 때 예측 불가능한 새로운 세션 ID 발급하도록 조치
- 기존 세션 ID 는 파기해야함

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.9 자동화 공격

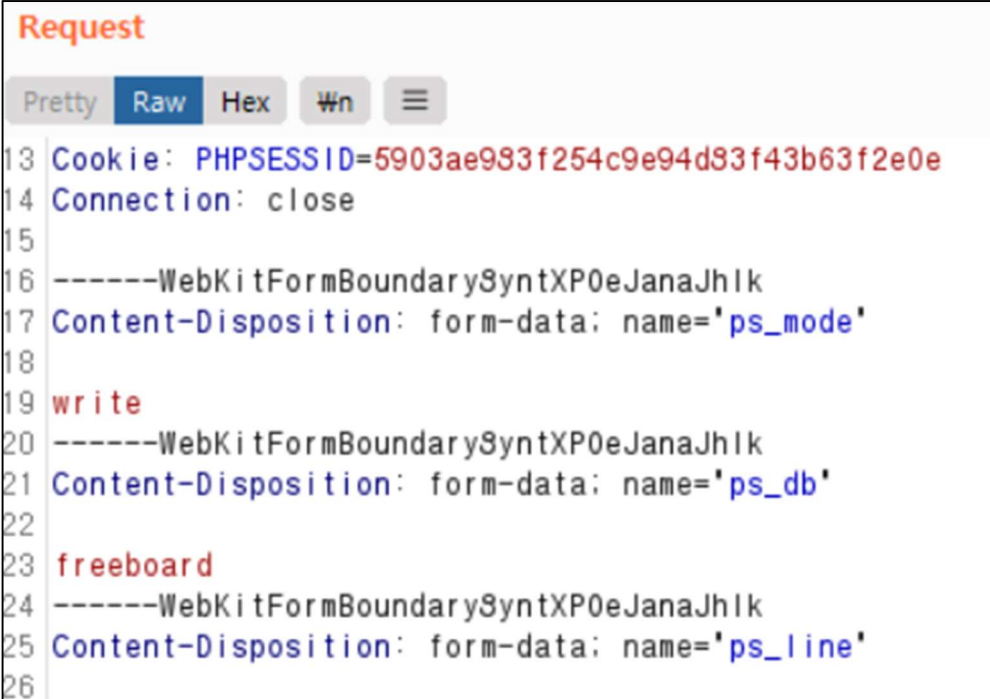
#### 3.9.1 취약점 정의

특정 프로세스에 대한 반복적인 요청으로 인한 무차별 대입 공격으로 게시글 등록 또는 SMS 발송 등의 작업을 반복하여 웹 어플리케이션 자원을 고갈시킬 수 있음

#### 상세분석

|        |                    |
|--------|--------------------|
| 취약한 경로 | 게시판                |
| 설명     | 게시글 도배 공격이 가능한지 확인 |

#### [Step #1] 자동화 툴을 사용하여 도배 공격 시도



```

Request
Pretty Raw Hex Wn
13 Cookie: PHPSESSID=5903ae983f254c9e94d93f43b63f2e0e
14 Connection: close
15
16 -----WebKitFormBoundarySyntXP0eJanaJhIk
17 Content-Disposition: form-data; name='ps_mode'
18
19 write
20 -----WebKitFormBoundarySyntXP0eJanaJhIk
21 Content-Disposition: form-data; name='ps_db'
22
23 freeboard
24 -----WebKitFormBoundarySyntXP0eJanaJhIk
25 Content-Disposition: form-data; name='ps_line'
26
  
```

[그림 3- 14] 툴을 이용한 도배 공격 중



|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

#### [Step #2] 게시글 내용 확인

|     |   |                      |            |
|-----|---|----------------------|------------|
| 100 |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |
| 99  |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |
| 98  |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |
| 97  |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |
| 96  |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |
| 95  |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |
| 94  |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |
| 93  |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |
| 92  |  <a href="#">[일반]도배 테스트 ..</a>  | <a href="#">test</a> | 2021-06-30 |

[그림 3- 15] 다수의 패킷이 전송되어 도배글이 작성됨

#### 3.9.2 보안대책

- 로그인 시도나 게시글 등록 등에 대한 사용자 요청이 일회성이 될 수 있도록 일회성 확인 로직을 도입해야함.
- 캡차(CAPTCHA) 같은 자동화된 사람과 컴퓨터간의 판별 기술 도입이 필요
- 다수의 패킷이 전송될 때 이를 방어할 수 있는 시스템 구축이 필요

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.10 관리자 페이지 노출

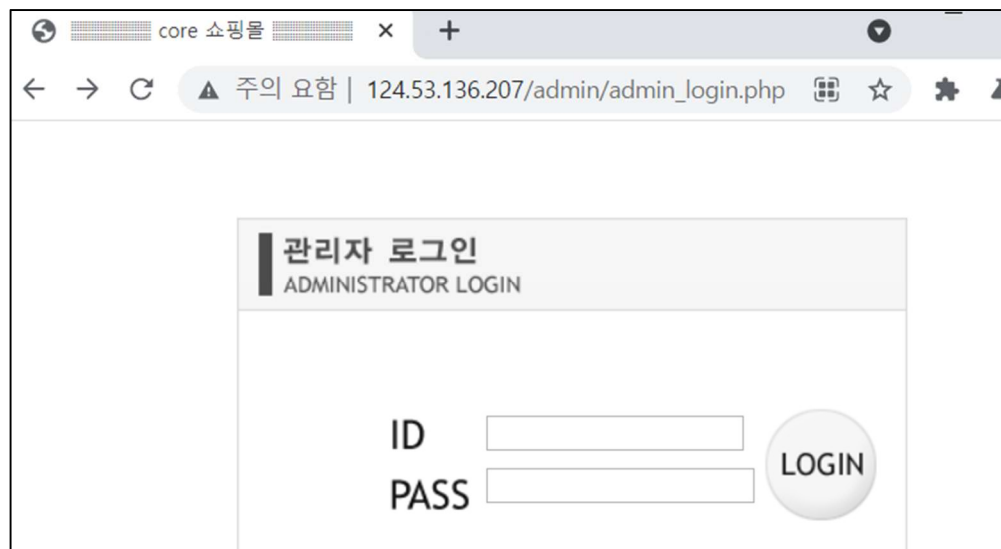
#### 3.10.1 취약점 정의

웹 관리자의 권한이 노출될 경우 웹 사이트의 변조가 가능. 취약성 정도에 따라 웹 서버의 권한까지 노출될 우려가 있음

#### 상세분석

|        |   |
|--------|---|
| 취약한 경로 | http://124.53.136.207/admin/admin_login.php |
| 설명     | 추측 가능한 관리자 페이지 경로 접근 시 페이지 노출               |

#### [Step #1] 추측하기 쉬운 페이지 경로 입력



[그림 3- 16] 관리자 로그인 페이지가 노출됨을 확인

#### 3.10.2 보안대책

- 일반 사용자의 접근이 불필요한 관리자 로그인 페이지 주소를 유추하기 어려운 이름으로 변경 및 관리자 페이지 접근 포트를 변경
- 특정 사용자만 접근할 수 있도록 페이지마다 세션 검증 필요.
- 웹 방화벽을 이용해 특정 IP 만 접근 가능하도록 설정

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

### 3.11 데이터 평문 전송

#### 3.11.1 취약점 정의

웹상의 데이터 통신은 대부분 텍스트로 이루어져 있기 때문에 서버와 클라이언트 간에 암호화를 구현해놓지 않으면 스니핑(sniffing) 도청을 통해 정보 탈취를 할 수 있음

#### 상세분석

|        |   |
|--------|---|
| 취약한 경로 | http  |
| 설명     | 툴(wireshark)을 이용하여 패킷에 담겨있는 데이터(아이디/비밀번호) 확인 가능 |

#### [Step #1] 페이지 로그인 시 전달되는 패킷 분석

|   |                   |
|---|-------------------|
| 62 63 69 64 3d 26 70 73 5f 6c 69 6e 65 3d 26 70 | bcid=&ps_line=&p  |
| 73 5f 63 68 6f 69 3d 26 70 73 5f 64 69 76 69 3d | s_choi=& ps_divi= |
| 26 70 73 5f 73 65 6c 65 3d 26 70 73 5f 71 75 65 | &ps_sele =&ps_que |
| 73 3d 26 70 73 5f 70 61 67 65 3d 26 70 73 5f 63 | s=&ps_pa ge=&ps_c |
| 74 69 64 3d 26 70 73 5f 67 6f 69 64 3d 26 70 73 | tid=&ps_goid=&ps  |
| 5f 70 6e 61 6d 65 3d 26 6c 6f 67 69 6e 5f 69 64 | _pname=& login_id |
| 3d 74 65 73 74 26 78 3d 33 30 26 79 3d 32 30 26 | =test&x= 30&y=20& |
| 6c 6f 67 69 6e 5f 70 61 73 73 3d 37 34 31 30    | login_pa ss=7410  |

[그림 3- 17] 평문으로 아이디와 비밀번호가 보여지는 것을 확인

#### 3.11.2 보안대책

- 웹상에서 전송되는 중요 정보는 반드시 SSL 등의 암호화 통신을 사용하여 도청으로부터의 위험을 제거해야함

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

## I. [별첨] 진단항목

- 과학기술정보통신부에서 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 주입함으로써 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 영향을 미치는 취약점   | H  |

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

|    |                      |   |   |
|----|----------------------|---|---|
| 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 로그인 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 |

|       |           |    |              |
|-------|-----------|----|--------------|
| 멀티캠퍼스 | 웹 모의해킹 진단 | 버전 | v1.0         |
|       |           | 일자 | 2021. 07. 02 |

|    |               |   |   |
|----|---------------|---|---|
| AE | 관리자<br>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<br>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 사용자에게 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