

---

실천 웹 서버 해킹과 대응 8조

## 웹 취약점 점검 보고서

---

2022-06-24



팀장 류 규 원

팀원 조 영 준

양 온 유

손 정 훈

김 성 준

## 목차

1. 수행개요 .....	3
1.1 정의 및 목적 .....	3
1.4 수행 단계 .....	3
1.5 수행 대상 .....	3
1.6 수행 장소 .....	3
2.4 점검 도구 .....	3
2. 점검 항목 .....	4
3. 수행 결과 요약 .....	5
4. 상세 수행 결과 .....	6
4.1 버퍼 오버플로우 .....	6
4.2 포맷스트링 .....	7
4.3 LDAP 인젝션 .....	8
4.4 운영체제 명령 실행 .....	9
4.5 SQL 인젝션 .....	10
4.6 SSI 인젝션 .....	11
4.7 Xpath 인젝션 .....	12
4.8 디렉터리 인덱싱 .....	13
4.9 정보 누출 .....	14
4.10 악성 콘텐츠 .....	15
4.11 크로스사이트 스크립팅 .....	16
4.12 불충분한 인증 .....	17
4.13 취약한 비밀번호 복구 .....	18
4.14 세션 예측 .....	19
4.15 불충분한 세션 만료 .....	20
4.16 자동화 공격 .....	21
4.17 파일 업로드 .....	23
4.18 파일 다운로드 .....	24
4.19 관리자 페이지 노출 .....	25
4.20 데이터 평문 전송 .....	26
4.21 약한 문자열 강도 .....	27
4.22 불충분한 인가 .....	28
4.23 쿠키 변조 .....	29
5. 최종진단 .....	30

## 1. 수행개요

### 1.1. 정의 및 목적

본 진단을 통해 웹해킹 7팀이 구현한 "스터디카페" 웹 서비스에 대한 보안 취약점을 도출하여 이를 사전에 제거함으로써 내·외부의 악의적인 공격으로부터 서비스 및 정보를 보호하기 위한 것이며, 모의해킹 점검을 통해 실제적인 운영환경에서 발생할 수 있는 위협을 도출하고 이에 대한 대응방안을 마련함으로써 정보시스템의 기밀성, 무결성, 가용성의 향상을 목적으로 함.

### 1.2. 수행단계

단계	내용
현황 분석	시스템 현황 파악 및 분석
모의 해킹	목표 시스템을 분석하여 도출된 취약점을 토대로 시스템 내부에 침투 하거나, 주요자원 획득/변조/유출 등이 가능한지 테스트
결과 분석	모의해킹 결과에 대한 취약점 분석 및 평가
보안 대책 수립	발견된 취약점에 대한 보안 강화 방안 수립 및 결과 보고서 작성

### 1.3. 수행대상

No	서비스	도메인	비고
1	스터디카페 홈페이지	https://10.100.40.43:12345	

### 1.4. 수행장소

보안취약점 점검장소 : 건양대학교 의공학관305호

### 1.5. 점검도구

보다 정확하고 신속한 점검을 수행하기 위해서 다음과 같은 도구들 중에서 필요한 도구들을 선별, 컨설턴트의 수작업과 함께 병행하여 점검합니다.

도구	설명
Burp suite	웹 프록시 도구
WireShark	패킷 분석 도구

## 2. 점검 항목

점검영역	CODE	점검항목	위험도
※ 웹 애플리케이션	BO	버퍼 오버플로우	H
	FS	포맷 스트링	H
	LI	LDAP 인젝션	H
	OC	운영체제 명령실행	H
	SI	SQL 인젝션	H
	SS	SSI 인젝션	H
	XI	XPath 인젝션	H
	DI	디렉토리 인덱싱	H
	IL	정보누출	H
	CS	악성콘텐츠	H
	XS	크로스사이트스크립팅	H
	BF	약한문자열강도	H
	IA	불충분한 인증	H
	PR	취약한 패스워드복구	H
	SE	세션 예측	H
	IN	불충분한 인가	H
	SC	불충분한 세션만료	H
	AU	자동화 공격	H
	FU	파일업로드	H
	FD	파일다운로드	H
	AE	관리자페이지 노출	H
	SN	데이터 평문전송	H
	CC	쿠키변조	H

※ 본 진단항목은 “주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세가이드”를 참고하였음.



### 3. 수행결과 요약

점검영역	CODE	점검항목	위험도	진단결과
웹 애플리케이션	BO	버퍼 오버플로우	H	양호
	FS	포맷 스트링	H	양호
	LI	LDAP 인젝션	H	양호
	OC	운영체제 명령실행	H	양호
	SI	SQL 인젝션	H	취약
	SS	SSI 인젝션	H	양호
	XI	XPath 인젝션	H	N/A
	DI	디렉토리 인덱싱	H	양호
	IL	정보누출	H	취약
	CS	악성콘텐츠	H	양호
	XS	크로스사이트스크립팅	H	취약
	BF	약한문자열강도	H	취약
	IA	불충분한 인증	H	취약
	PR	취약한 패스워드복구	H	양호
	SE	세션 예측	H	양호
	IN	불충분한 인가	H	취약
	SC	불충분한 세션만료	H	취약
	AU	자동화 공격	H	취약
	FU	파일업로드	H	취약
	FD	파일다운로드	H	양호
	AE	관리자페이지 노출	H	취약
	SN	데이터 평문전송	H	양호
	CC	쿠키변조	H	양호

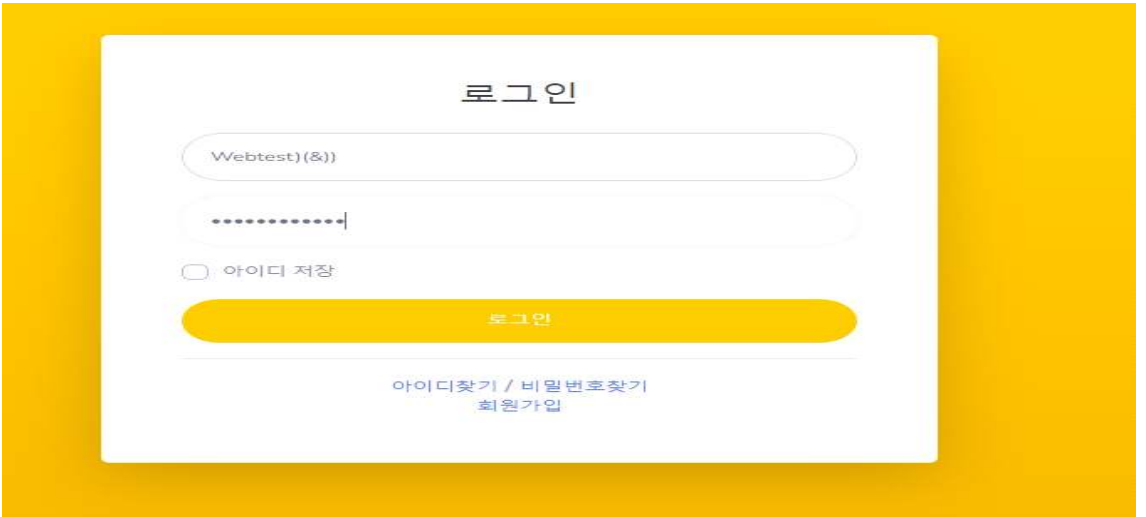
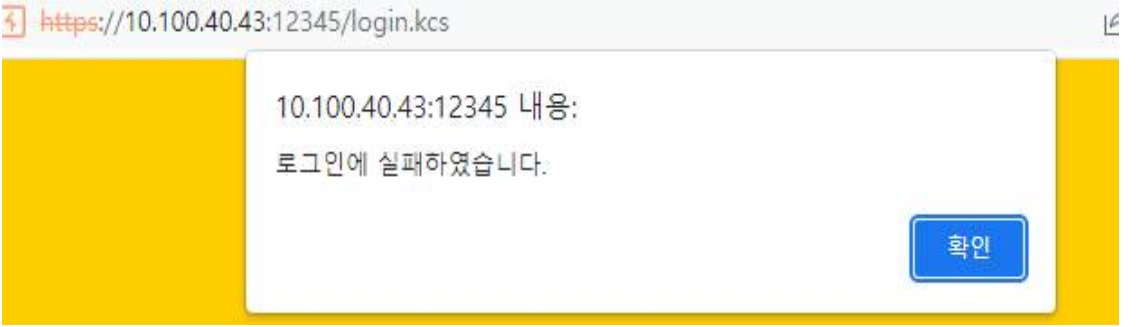
#### 4.1 버퍼오버플로우

[그림 4.1.1] 404페이지확인

## 4.2 포맷스트링

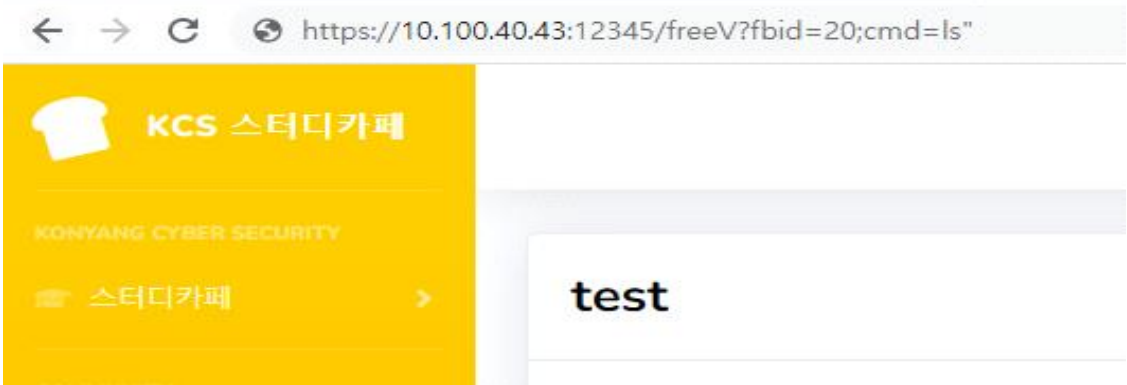

Code	FS	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	웹페이지 내 포맷스트링 취약점 존재 여부 점검				
설 명	printf 등의 함수에서 문자열 입력 포맷을 잘못된 형태로 입력하는 경우 나타나는 취약점으로 루트 권한이 가능한 취약점				
판단기준	<p>양호: 포맷 스트링 버그를 발생시키는 문자열 입력 시 검증 로직이 존재하여 오류가 발생하지 않는 경우</p> <p>취약: 포맷 스트링 버그를 발생시키는 문자열 입력 시 검증 로직이 미흡하여 오류가 발생하는 경우</p>				
취약내용	<p>URL 파라미터 값에 "%n", "%s"와 같은 문자열 함수 입력시 404 페이지 이동으로 양호.</p> <p>1. URL 파라미터 값에 아래와 같은 패턴을 입력시 에러페이지나 오류가 발생하는지 확인.</p> <p>패턴1: %n%n%n%n%n%n%n%n%n%n%n%n%n</p> <p>패턴2: %s%s%s%s%s%s%s%s%s%s%s</p>				
점검결과	 <p>[그림 4.2.1] 404페이지확인</p>  <p>[그림 4.2.2] 404페이지확인</p>				
권고사항	<p>웹 서버 응용프로그램(Apache, Tomcat, IIS 등) 을 최신버전으로 패치하고 임의의 문자열 입력에 대한 검증 로직 구현</p>				

### 4.3 LDAP인젝션

Code	LI	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	웹페이지 내 LDAP 인젝션 취약점 점검				
설 명	쿼리를 주입함으로써 개인정보 등의 내용이 유출될 수 있는 문제를 이용하는 취약점으로, LDAP는 조직이나 개체, 그리고 인터넷이나 기업 내의 인트라넷 등 네트워크 상에 있는 파일이나 장치들과 같은 자원 등의 위치를 찾을 수 있게 해주는 소프트웨어 프로토콜로, 일부 웹사이트에서 사용자 입력 부분을 LDAP 쿼리로 수행하고, 입력값 필터링을 제대로 처리하지 못할 경우 LDAP 구문을 변경하여 개인정보 등의 내용을 취득할 수 있는 취약점				
판단기준	양호: 임의의 LDAP 쿼리 입력에 대한 검증이 이루어져 변조된 쿼리가 실행되지 않는 경우 취약: 임의의 LDAP 쿼리 입력에 대한 검증이 이루어지지 않아 변조된 쿼리가 실행되는 경우				
취약내용	로그인페이지에 LDAP구문 입력시 오류페이지나 에러페이지가 표시 되지 않아 양호.				
점검결과	<p>1. 사용자 입력값에 LDAP 쿼리 삽입후 실행되는지 확인 사용구문: Webtest&gt;(&amp;))</p>  <p>[그림 4.3.1] 로그인페이지 LDAP구문입력</p> <p>2. LDAP 쿼리 구문이 작동되지 않고 로그인 페이지로 이동</p>  <p>[그림 4.3.2] 로그인 페이지로 이동</p>				
권고사항	지정된 문자열만 입력 허용하고, 임의의 LDAP 쿼리 입력에 대한 검증 로직 구현				



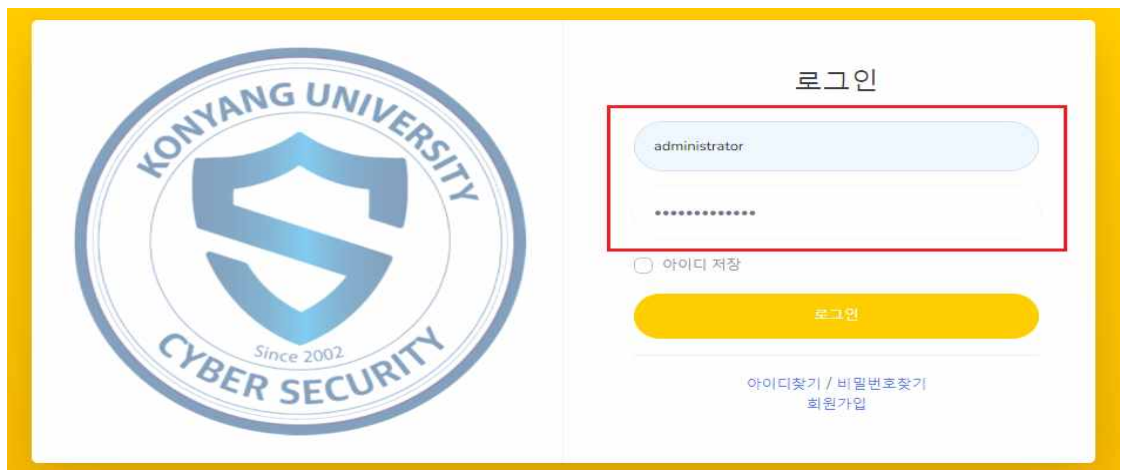
#### 4.4 운영체제명령실행

Code	OC	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	웹사이트 내 운영체제 명령 실행 취약점 존재 여부 점검				
설 명	system(), exec() 와 같은 시스템 명령어를 실행시킬 수 있는 함수를 이용하여 사용자 입력 값에 대한 필터링이 제대로 이루어지지 않을 경우 공격자가 운영체제 시스템 명령어를 호출하여 백도어 설치나 관리자 권한을 탈취 할 수 있는 취약점				
판단기준	양호: 임의의 명령어 입력에 대한 검증이 이루어지는 경우 취약: 임의의 명령어 입력에 대해 명령이 실행되는 경우				
취약내용	URL 파라미터 값에 시스템 명령함수 전달시 명령어가 실행되지 않아 양호함.				
점검결과	<p>1. URL 파라미터 값에 시스템 명령함수 전달.</p> <p>사용구문: ;cmd=ls"</p>  <p>[그림 4.4.1]시스템명령어 전달</p> <p>2. 시스템 명령 함수 실행되지 않고 404페이지로 이동.</p>  <p>[그림 4.4.2] 404페이지 이동</p>				
권고사항	애플리케이션은 운영체제로부터 명령어를 직접적으로 호출하지 않도록 구현하는게 좋지만, 부득이하게 사용해야 할 경우 소스 코드나 웹 방화벽에서 특수문자, 특수 구문에 대한 검증할 수 있도록 조치해야함				

#### 4.5 SQL인젝션

Code	SI	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	웹페이지 내 SQL 인젝션 취약점 존재 여부 점검				
설 명	로그인 폼이나 입력 할 수 있는 폼에 악의적인 쿼리를 삽입하여, 데이터베이스를 조회, 변경, 제거 등이 가능한 취약점				
판단기준	양호: 임의의 SQL Query 입력에 대한 검증이 이루어지는 경우 취약: 임의의 SQL Query 입력에 대한 검증이 이루어지지 않는 경우				
취약내용	로그인 창에 참이 되는 SQL 쿼리 전달시 로그인이 성공적으로 되어 취약함.				

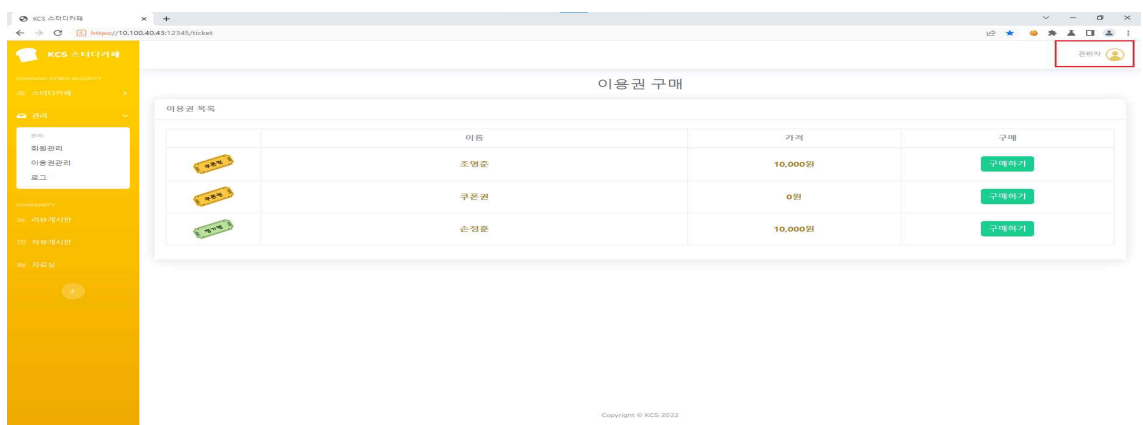
- 로그인 창에 참이 되는 SQL 쿼리 전달시 로그인 되는지 확인.  
사용구문- ID: administrator PW: " or '1'='1'



점검결과

[그림 4.5.1] 참이 되는 쿼리값 전달

- 성공적으로 로그인이 된 것을 확인.





[그림 4.5.2] 성공적으로 로그인

권고사항

소스코드에 SQL 쿼리를 입력 값으로 받는 함수나 코드를 사용할 경우, 임의의 SQL 쿼리 입력에 대한 검증 로직을 구현하여 서버에 검증되지 않는 SQL 쿼리 요청 시 에러 페이지가 아닌 정상 페이지가 반환되도록 필터링 처리하고 웹 방화벽에 SQL 인젝션 관련 룰셋을 적용하여 SQL 인젝션 공격을 차단함

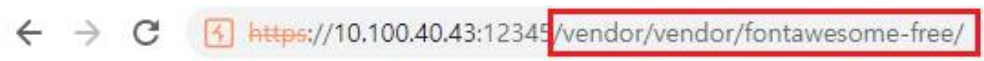

#### 4.6 SSI인젝션

Code	SS	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	웹페이지 내 SSI 인젝션 공격 가능성 점검				
설 명	HTML 페이지의 전체 코드를 수정하지 않고 공통 모듈 파일로 관리하며 동적인 내용을 추가하기 위해 만들어진 기능으로 주로 방문자 수 세거나 홈페이지 로고 수정 등 간단한 기능 추가할 때 사용한다. 또한 '.shtml' 확장자 파일을 사용한다. 만약 SSI 인젝션 취약점이 있는 경우 페이지에 악의적인 코드를 주입하는 공격이 가능한 취약점				
판단기준	양호: 사용자 입력 값에 대한 검증이 이루어지는 경우 취약: 사용자 입력 값에 대한 검증이 이루어지지 않는 경우				
취약내용	인수값이 들어가는 부분에 SSI 구문 삽입후 디렉터리 파일이 표시되지 않아 양호함.				
점검결과	<p>1. 인수값에 해당 구문 삽입후 반환되는 페이지에 디렉터리 파일이 표시되는지 확인.</p> <p>사용구문: &lt;!--exec cmd="ls" --&gt;</p>  <p>[그림 4.6.1] SSI 구문 삽입</p> <p>2. 404페이지 이동.</p>  <p>[그림 4.6.2] 404페이지 이동</p>				
권고사항	사용자 입력 값에 대한 로직 추가 구현				


#### 4.7 Xpath 인젝션

Code	FS	위험도	H	진단결과	N/A
점검영역	웹 애플리케이션				
점검항목	웹페이지 내 조작된 XPath 쿼리 공격 가능성 점검				
설 명	데이터 베이스와 연동된 웹 애플리케이션에서 XPath 및 XQuery 질의문에 대한 필터링이 제대로 이루어지지 않을 경우 공격자가 입력이 가능한 폼(웹 브라우저 주소 입력창 또는 로그인 폼등)에 조작된 질의문을 삽입하여 인증 우회를 통해 XML 문서로부터 인가되지 않은 데이터를 열람할 수 있는 취약점				
판단기준	양호: 쿼리 입력 값에 대해 검증이 이루어지는 경우				
	취약: 쿼리 입력 값에 대해 검증이 이루어지지 않는 경우				
취약내용	XML 파일이 존재하지 않아 N/A.				
점검결과	N/A				
권고사항	XPath 쿼리에 사용자가 값을 입력할 수 있는 경우, 엄격한 입력 값 검증을 통해 필요 문자만을 받아들이게 함 ( ) = ' [ ] : , * / 등 XPath 쿼리를 파괴하는 특수문자는 입력하지 못하게 하여야 하며, 특정 특수문자만을 필터링하는 것이 아닌 허용된 문자 이외의 모든 입력을 허용하지 않아야 함				

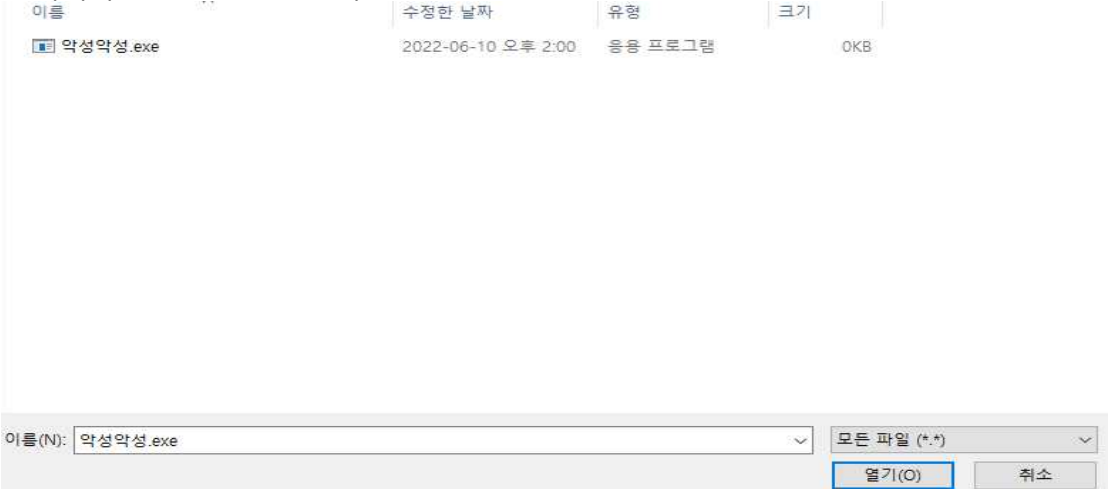
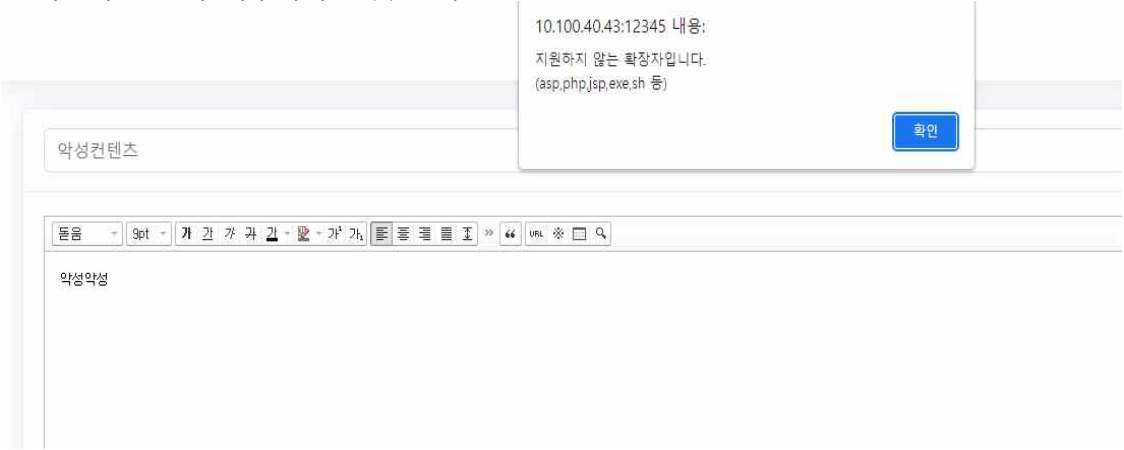
#### 4.8 디렉터리 인덱싱

Code	DI	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	웹서버 내 디렉터리 인덱싱 취약점 존재 여부 점검				
설 명	웹 어플리케이션을 사용하고 있는 서버의 미흡한 설정으로 인해 인덱싱 기능이 활성화가 되어있을 경우, 공격자가 강제 브라우징을 통해 서버내의 모든 디렉터리 및 파일에 대해 인덱싱이 가능하여 웹 어플리케이션 및 서버의 주요 정보가 노출될 수 있는 취약점				
판단기준	양호: 디렉터리 파일 리스트가 노출되지 않는 경우 취약: 디렉터리 파일 리스트가 노출되는 경우				
취약내용	URL 경로 중 상위 디렉터리 이동시 파일 목록이 표시되지 않아 양호함.				
점검결과	<p>1. URL 경로 중 확인하고자 하는 디렉터리 상위폴더로 이동해 인덱싱 여부를 확인.</p>  <p>[그림 4.8.1] 상위 폴더이동</p> <p>2. 디렉터리 파일이 표시되지 않는 것을 확인.</p>  <p>[그림 4.8.2] 디렉터리 목록표시 되지않음</p>				
권고사항	웹 서버 설정을 변경하여 디렉터리 파일 리스트가 노출 되지 않도록 설정				

#### 4.9 정보누출

Code	FS	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	웹 서비스 시 불필요한 정보가 노출되는지 여부 점검				
설 명	웹 애플리케이션의 민감한 정보가 개발자의 부주의로 인해 노출되는 것으로 중요 정보(관리자 계정 및 테스트 계정 등)를 주석구문에 포함시켜 의도하지 않게 정보가 노출되는 취약점				
판단기준	양호: 웹 서비스 에러 페이지가 별도로 지정되어 있는 경우 취약: 웹 서비스 에러 페이지가 별도로 지정되지 않아 에러 발생 시 중요 정보가 노출되는 경우				
취약내용	에러페이지 발생시 Apache 버전정보 노출로 취약.				
점검결과	<p>1. 400 에러페이지 발생으로 Apache 버전정보가 나타나는 것을 확인.</p>  <p>[그림 4.9.1] Apache버전 정보노출</p>				
권고사항	웹 서버 응용프로그램(Apache, Tomcat, IIS 등) 을 최신버전으로 패치하고 임의의 문자열 입력에 대한 검증 로직 구현				

#### 4.10 악성콘텐츠

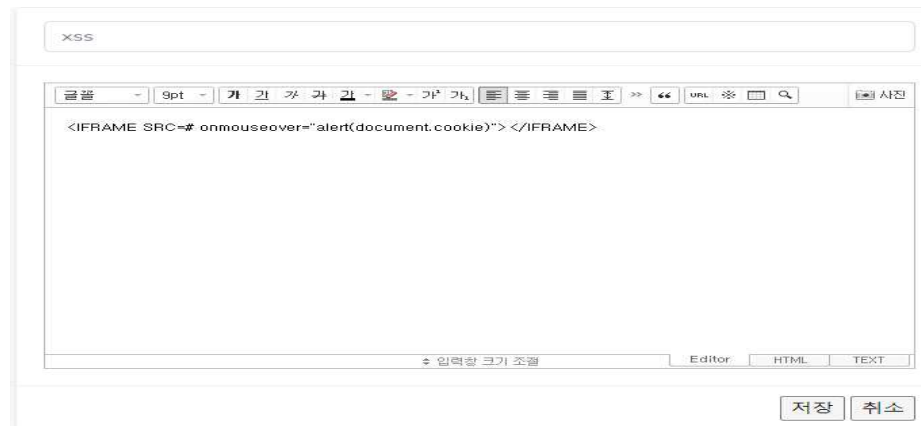
Code	CS	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	게시판 등에 악성 콘텐츠 삽입 및 실행 여부 점검				
설 명	웹 어플리케이션에서 사용자 입력 값에 대한 필터링이 제대로 이루어지지 않을 경우 공격자가 악성코드를 삽입할 수 있으며, 악성콘텐츠가 삽입된 페이지에 접속한 사용자는 악성코드 유포 사이트가 자동으로 호출되어 악성코드에 감염될 수 있는 취약점				
판단기준	양호: 악의적 콘텐츠가 실행되지 않는 경우 취약: 악의적인 콘텐츠가 입력되며, 실행되는 경우				
취약내용	"exe"파일 업로드시 파일 확장자 검증이 이루어져 양호.				
점검결과	<p>1. 악의적인 프로그램 "exe"파일 업로드.</p>  <p>[그림 4.10.1] "exe"파일 업로드</p> <p>2. 확장자 검증이 이루어지는 것을 확인.</p>  <p>[그림 4.10.2] 확장자 검증</p>				
권고사항	게시판의 글 등록 및 파일 업로드 기능에 Flash 파일이나 avi동영상 파일, exe 실행파일 등 악성코드가 포함될 수 있는 콘텐츠를 삽입 또는 업로드 하지 못하게 필터링 적용				

#### 4.11 크로스사이트스크립팅

Code	XS	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	웹 사이트 내 크로스사이트 스크립팅 취약점 존재 여부 점검				
설 명	게시판, 웹 메일 등에 삽입된 악의적인 스크립트에 의해 사용자의 쿠키 및 기타 개인 정보를 특정 사이트로 전송시키는 공격				
판단기준	양호: 사용자 입력 인수 값에 대한 검증 및 필터링이 이루어지는 경우 취약: 사용자 입력 값에 대한 검증 및 필터링이 이루어지지 않으며, HTML 코드가 입력, 실행되는 경우				
취약내용	크로스 사이트 스크립트 구문 IFRAME을 사용하여 쿠키값 노출을 시도한 결과 쿠키값이 노출이 되므로 취약함				

1. 자유게시판 글쓰기 시 다음과 같은 크로스사이트 스크립트 구문 작성 후 저장.

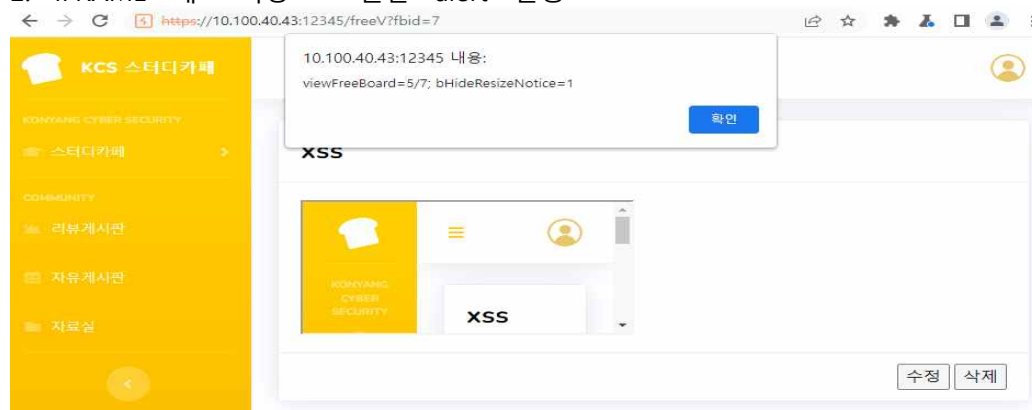
사용구문: <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>



[그림 4.11.1] XSS구문입력

#### 점검결과

2. "IFRAME" 태그 허용으로 인한 "alert" 실행



[그림 4.11.2] 쿠키값 노출

#### 권고사항

웹 사이트의 게시판, 자료실, URL 등에서 사용자로부터 입력받은 인수 값에 대해 검증 로직을 추가하거나 인수 값이 입력되더라도 실행되지 않게 하고, 부득이하게 게시판에서 HTML을 사용하는 경우 HTML 코드중 필요한 코드에 대해서만 입력 가능하도록 설정

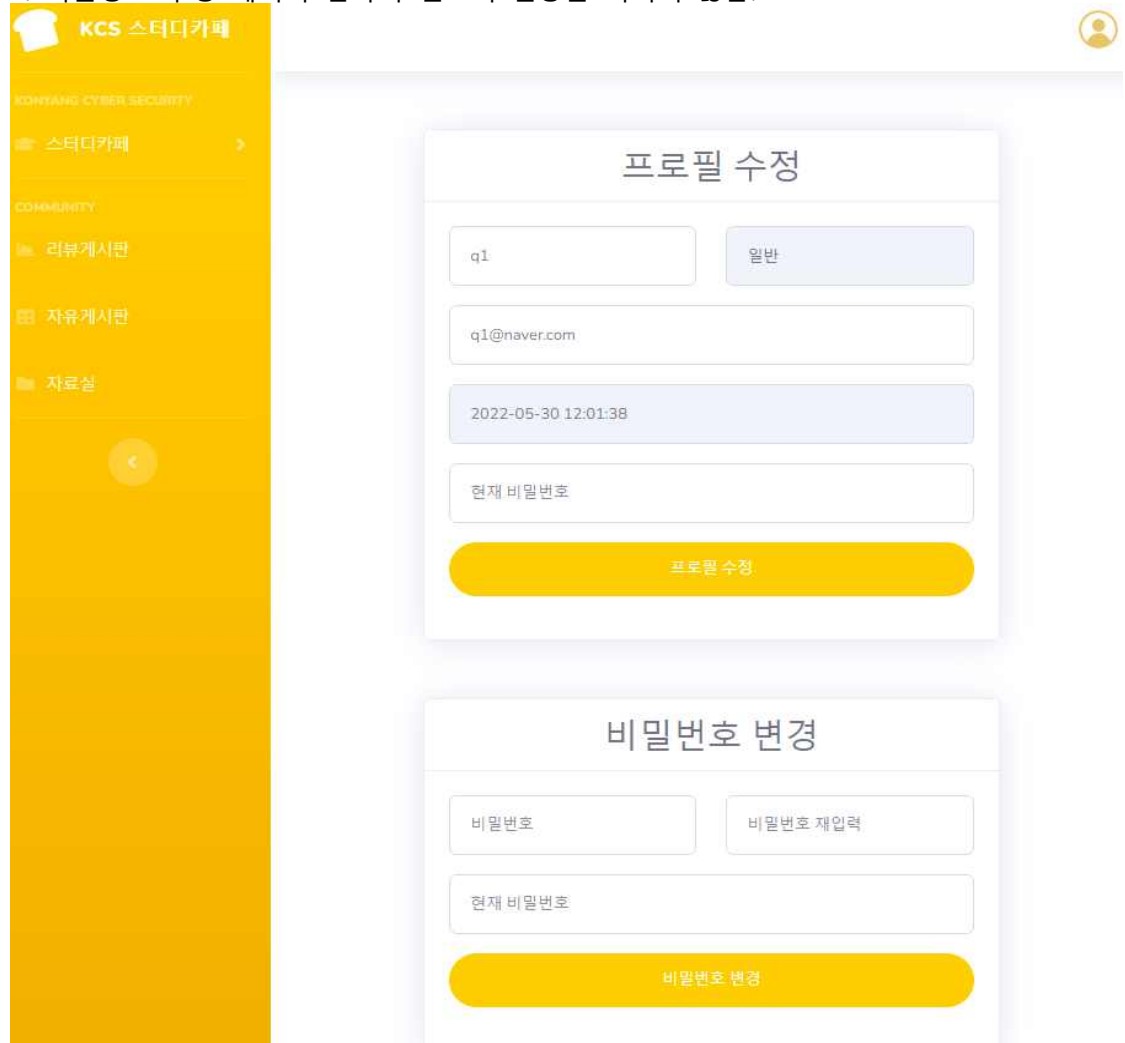


#### 4.12 불충분한인증

Code	IA	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	중요 페이지 접근 시 추가 인증 요구 여부 점검				
설 명	웹 어플리케이션에서 개인정보 수정 페이지나 통합 로그인(SSO)과 같은 곳에서 사용자 인증이 미흡(아이디로 인증)할 경우 공격자가 파라미터로 전달되는 값을 수정하여 사용자 도용 및 개인정보 노출 문제가 발생할 수 있는 취약점				
판단기준	양호: 중요 정보 페이지 접근 시 추가 인증을 하는 경우 취약: 중요 정보 페이지 접근에 대한 추가 인증을 하지 않는 경우				
취약내용	회원정보 수정 페이지 접속시 본인인증이 걸치지 않아 취약함.				

점검결과

1. 회원정보 수정 페이지 접속시 별도의 인증을 거치지 않음.




[그림 4.12.1] 별도인증 미확인

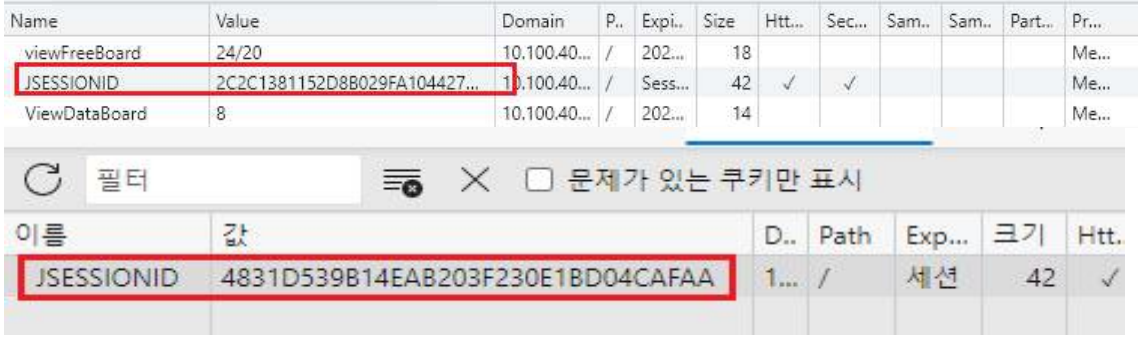
권고사항

중요 정보(회원정보 변경) 페이지와 같은 중요 정보를 표시하는 페이지에서는 본인 인증을 재확인하는 로직을 구현하고, 인증 후 사용자가 이용 가능 페이지에 접근할 때마다 승인을 얻은 사용자인지 페이지마다 검증하여야 함

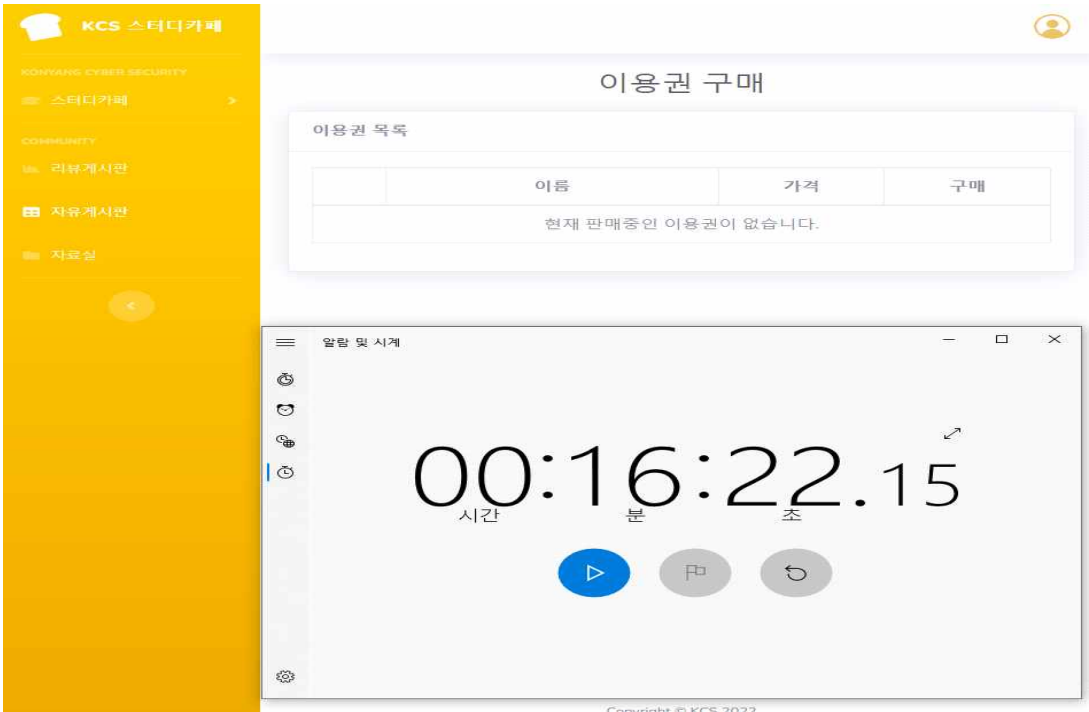
#### 4.13 취약한패스워드복구

Code	PR	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	웹 사이트 내 패스워드 복구 절차의 적절성 점검				
설 명	웹 어플리케이션에 존재하는 비밀번호 찾기 기능 또는 관리자에 의한 임시 비밀번호 발급 시 사용자 인증이 미흡하거나 비밀번호를 화면에 즉시 출력할 경우 공격자가 불법적으로 다른 사용자의 비밀번호를 획득, 변경, 복구할 수 있는 취약점				
판단기준	양호: 패스워드 재설정 시 난수를 이용하여 재설정하고 인증된 사용자 메일이나 SMS 로 재설정된 패스워드 전송 시				
	취약: 패스워드 재설정 시 일정 패턴으로 재설정되고 웹 사이트 화면에 바로 출력시				
취약내용	패스워드 찾기시 이메일로 임시 비밀번호가 전송되어 양호함.				
점검결과	<p>1. 패스워드 찾기시 이메일로 임시 비밀번호가 전송되는 것을 확인.</p>  <p>[그림 4.13.1] 이메일로 임시비밀번호 발송</p>				
권고사항	패스워드 복구 로직을 변경하고 인증된 사용자 메일이나 SMS에서만 재설정된 패스워드를 확인 가능하도록 조치				

#### 4.14 세션예측

Code	SE	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	단순한 방법(연속된 숫자 할당 등)으로 생성되는 세션 ID를 예측하여 세션 탈취 여부 점검				
설 명	단순히 숫자가 증가하는 방법 등의 취약한 특정 세션의 ID를 예측하여 세션을 가로챌 수 있는 취약점				
판단기준	양호: 추측 불가능한 세션 ID가 발급되는 경우 취약: 세션 ID가 일정한 패턴으로 발급되는 경우				
취약내용	각기 다른 시간 및 브라우저로 접속시 예측 할 수 없는 세션이 발급이 되어 양호함.				
점검결과	<p>1. 각기 다른 시간 및 브라우저로 접속시 예측 할 수 없는 세션을 가짐.</p>  <p>[그림 4.14.1] 세션예측 불가</p>				
권고사항	추측 불가능한 세션 ID가 발급되도록 로직 구현				

#### 4.15 불충분한세션만료

Code	SC	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	세션의 만료 기간 설정 여부 점검				
설 명	세션의 만료 기간을 정하지 않거나, 만료기한을 너무 길게 설정된 경우 악의적인 사용자가 만료되지 않은 세션을 활용하여 불법적인 접근이 가능할 수 있음				
판단기준	양호: 세션 종료 시간이 설정되어 있는 경우 취약: 세션 종료시간이 설정되어 있지 않아 세션 재사용이 가능한 경우				
취약내용	로그인시 세션이 만료시간 15분이 지나도 로그아웃이 되지 않아 취약함				
점검결과	<p>1. 로그인후 권장 세션시간 15분이 지나도 로그아웃이 되지 않음.</p>  <p>[그림 4.15.1]권장 세션 시간초과</p>				
권고사항	세션 종료 시간 또는 자동 로그아웃 기능 구현(세션 종료 시간은 사이트의 특성에 따라 달라질 수 있으므로 사이트의 특성에 맞게 적정 시간 설정)				

#### 4.16 자동화공격

Code	AU	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	자동화된 공격으로 인한 다수 수의 프로세스 실행 여부 점검				
설명	어플리케이션 운영 시 특정 프로세스에 대한 접근시도 횟수 제한을 설정하지 않을 경우 공격자가 자동화 툴 및 봇을 활용하여 일분에 수백 번의 접근을 시도 할 수 있으며 특정 프로세스를 반복 수행함으로써 자동으로 수많은 프로세스(DoS, 무차별 대입 기법 등)가 진행 되어 시스템 성능에 영향을 미칠 수 있는 취약점				
판단기준	양호: 웹 애플리케이션의 데이터 등록 등의 기능 사용 시 대량 사용에 대한 통제가 이루어지는 경우 취약: 웹 애플리케이션의 데이터 등록 등 기능 사용 시 통제가 이루어지지 않는 경우				
취약내용	프록시 툴 Burpsuite 기능 "Repeater"를 사용해 자동화공격이 가능하므로 취약함.				

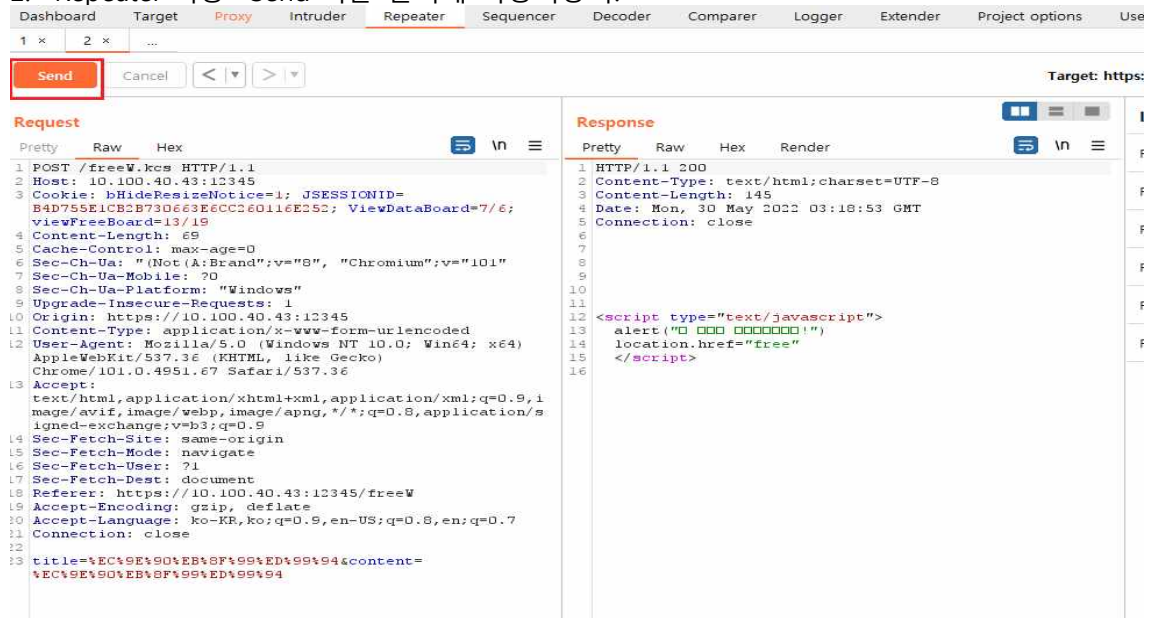
1. 게시판 글쓰기 기능에서 패킷을 잡아 "Action" -> "Repeater"로 이동.



[그림 4.16.1] 패킷잡은후 "Repeater" 이동

2. "Repeater"기능 "Send"버튼 클릭해 자동화공격.

점검결과



[그림 4.16.2]자동화공격게시

3. 여러개의 글이 올라온 것을 확인.

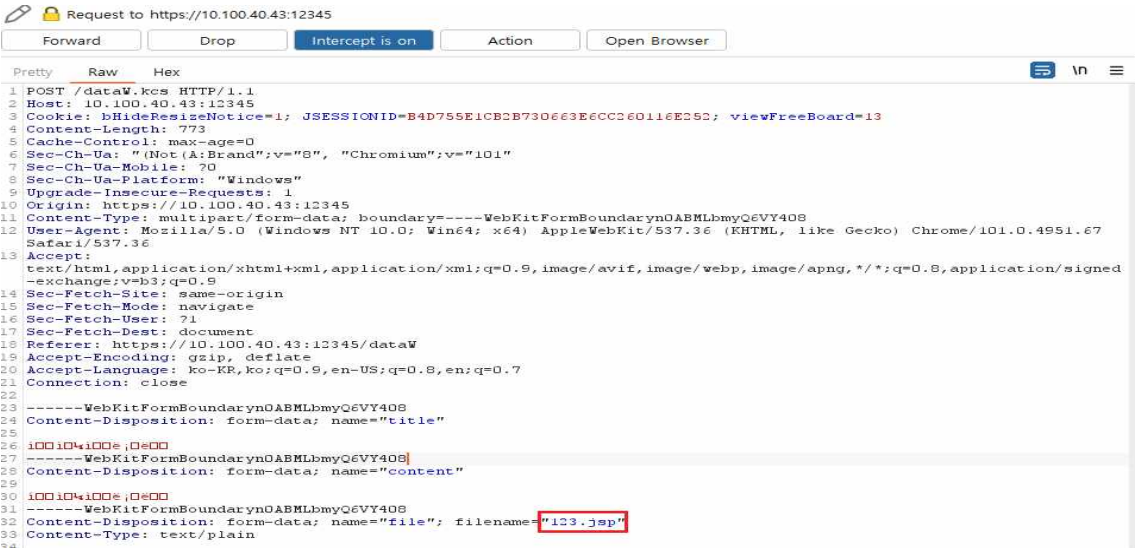
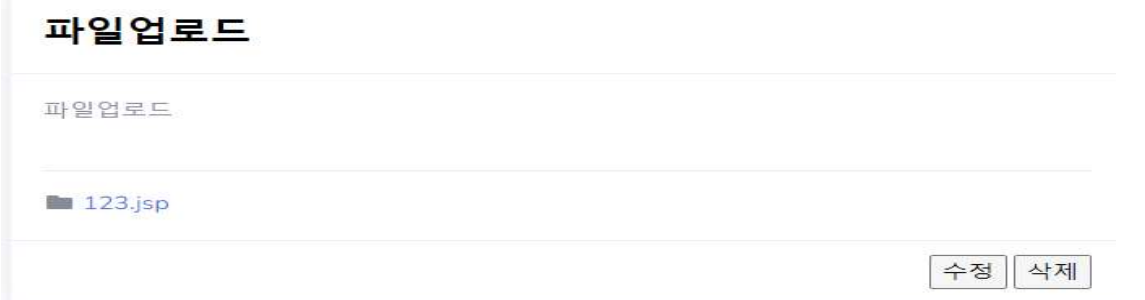
No	제목	작성자	작성일	조회 수
24	자동화	admin	2022-05-30	0
23	자동화	admin	2022-05-30	0
22	자동화	admin	2022-05-30	0
21	자동화	admin	2022-05-30	0
20	test	조영준	2022-05-30	1

[그림 4.16.3] 자동화공격확인

**권고사항**

데이터 등록 및 메일 발송 기능에서 사용자 등록이 일회성이 될 수 있도록, 캡차(이미지를 이용하여 확인 값을 표시하고 사용자가 값을 등록하여 인증함) 등 일회성 확인 로직을 구현하여야함

#### 4.17 파일업로드

Code	FU	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	웹 사이트의 게시판, 자료실 등에 조작된 Server Side Script 파일 업로드 및 실행가능 여부 점검				
설 명	파일 업로드 기능이 존재하는 웹 어플리케이션에서 확장자 필터링이 제대로 이루어지지 않았을 경우 공격자가 악성 스크립트 파일(웹쉘)을 업로드 하여 웹을 통해 해당 시스템을 제어할 수 있어 명령어 실행 및 디렉터리 열람이 가능하고 웹 페이지 또한 변조가 가능한 취약점				
판단기준	양호: 업로드 되는 파일에 대한 확장자 검증이 이루어지는 경우 취약: 업로드 되는 파일에 대한 확장자 검증이 이루어지지 않는 경우				
취약내용	프록시 툴 "Burpsuite" 이용하여 패킷 캡처후 파일확장자 변경시 업로드 가능으로 취약함.				
점검결과	<p>1. 패킷을 잡아 파일 확장자 변경하여 업로드.</p>  <p>[그림 4.17.1] 확장자명 변경후 업로드</p> <p>2. 파일업로드가 정상적으로 된 것을 확인.</p>  <p>[그림 4.17.1] 정상적 업로드 완료</p>				
권고사항	업로드 되는 파일에 대한 확장자 검증 및 실행 권한 제거				

#### 4.18 불충분한세션만료

Code	FD	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	다운로드 파일 저장이 허용된 디렉터리 외 다른 디렉터리의 접근이 가능한지 여부 점검				
설 명	파일 다운로드 기능이 존재하는 웹 어플리케이션에서 파일 다운로드 시 파일의 경로 및 파일명을 파라미터로 받아 처리하는 경우 파일에 대한 접근 권한이 설정되어 있지 않다면 공격자가 파라미터를 조작하여 환경설정 파일, 웹 소스코드 파일, 데이터베이스 연동 파일 등을 다운 받을 수 있는 취약점				
판단기준	양호: 다운로드 파일이 저장된 디렉터리 이외에 접근이 불가능한 경우 취약: 다운로드 파일이 저장된 디렉터리 이외에 접근이 가능한 경우				
취약내용	URL 파라미터 값에 "/etc/passwd"파일 다운로드시 404 페이지 이동으로 양호.				

1. URL 파라미터 값에 상대경로(/)로 "/etc/passwd"파일 다운로드 가능한지 확인.



[그림 4.18.1] "/etc/passwd" 파일다운

#### 점검결과

2. 파일 다운로드 되지 않고 404페이지로 이동.



#### 10.100.40.43 페이지를 찾을 수 없음

다음 웹 주소(<https://10.100.40.43:12345/dataV.down?dbid=8>)에 대해 발견된 웹페이지가 없습니다.

HTTP ERROR 404

새로고침

[그림 4.18.2] 404페이지

권고사항 다운로드 시 정해진 경로 이외의 디렉터리와 파일에 접근할 수 없도록 구현



#### 4.19 관리자페이지노출

Code	AE	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	유추하기 쉬운 URL로 관리자 페이지 메뉴 접근의 가능 여부 점검				
설 명	웹 어플리케이션의 전반적인 기능 설정 및 회원 관리를 할 수 있는 관리자페이지가 추측 가능한 형태로 구성되어 있을 경우 공격자가 관리자페이지에 쉽게 접근을 할 수 있으며 무차별 대입 공격을 통하여 관리자 권한을 획득할 수 있는 취약점				
판단기준	양호: 포맷 스트링 버그를 발생시키는 문자열 입력 시 검증 로직이 존재하여 오류가 발생하지 않는 경우				
	취약: 포맷 스트링 버그를 발생시키는 문자열 입력 시 검증 로직이 미흡하여 오류가 발생하는 경우				
취약내용	관리자 페이지 접속 가능해 취약함.				
점검결과	<p>1. 관리자 페이지 "admin.member" 확인.</p> 				
	[그림 4.19.1] 관리자페이지접속				
권고사항	<p>유추하기 어려운 이름(포트 번호 변경 포함)으로 관리자 페이지를 변경하여 쉽게 추측하여 관리자 페이지에 접근할 수 없도록 하고 근본적인 해결을 위해 지정된 IP 만관리자 페이지에 접근 가능하도록 제한하여야 함</p> <p>단, 부득이하게 관리자 페이지를 외부에 노출을 하여야 할 경우 관리자 페이지 로그인시 2차 인증(otp, vpn, 인증서 등)을 해야만 로그인 가능하도록 적용하는 것이 좋음</p>				

4.20 데이터평문전송

Code	SN	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	서버와 클라이언트 간 통신 시 데이터의 암호화 여부 점검				
설 명	로그인 또는 실명인증 시 민감한 데이터(개인 식별번호, 계정정보 등)가 평문으로 통신 채널을 통해 송수신 될 경우 공격자가 감청(스니핑)을 통해 다른 사용자의 민감한 데이터를 획득 할 수 있는 취약점.				
판단기준	양호: 중요정보 전송구간에 암호화 통신이 적용된 경우 취약: 중요정보 전송구간에 암호화 통신이 이루어지지 않는 경우				
취약내용	HTTPS(SSL/TLS)적용으로 로그인 패킷 확인 불가로 양호함.				

1. 로그인시 "Wireshark"이용해 패킷 확인.

No.	Time	Source	Destination	Protocol	Length	Info
390	10.935641	10.100.40.43	10.100.40.67	TLSv1.3	94	Application Data
391	10.93584	10.100.40.43	10.100.40.67	TCP	54	56160 → 12345 [ACK] Seq=1636 Ack=805 Win=130560 Len=0
392	10.940700	10.100.40.43	10.100.40.67	TLSv1.3	94	Application Data
393	10.940792	10.100.40.43	10.100.40.67	TLSv1.3	94	Application Data
394	10.941178	10.100.40.43	10.100.40.67	TCP	60	12345 → 56160 [ACK] Seq=805 Ack=1717 Win=64160 Len=0
395	10.975001	10.100.40.67	10.100.40.43	TCP	60	56160 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
396	10.975062	10.100.40.43	10.100.40.67	TCP	66	12345 → 56160 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
397	10.976177	10.100.40.67	10.100.40.43	TCP	54	56160 → 12345 [ACK] Seq=1 Ack=1 Win=131328 Len=0
398	10.978199	10.100.40.67	10.100.40.43	[TLSv1.3]	623	Client Hello
399	10.981026	AEONtec_60:Be:F4	Broadcast	ARP	60	Who has 220.123.79.220? Tell 220.123.79.5
400	10.987038	10.100.40.43	10.100.40.67	TLSv1.3	188	Server Hello
401	11.018888	192.168.21.109	192.168.21.255	UDP	186	52993 → 51007 Len=144
402	11.033763	AEONtec_60:Be:F4	Broadcast	ARP	60	Who has 220.123.79.219? Tell 220.123.79.5
403	11.041468	10.100.40.67	10.100.40.43	TCP	54	56160 → 12345 [ACK] Seq=570 Ack=135 Win=131072 Len=0

> Frame 398: 623 bytes on wire (4984 bits), 623 bytes captured (4984 bits) on interface \Device\NPF{3054E9E0-B942-4C0F-9060-4F838725E8FA}, id 0  
> Ethernet II, Src: Dell\_Sa2b2ed (70:b5:e8:6a:2b:ed), Dst: Dell\_6c:34:41 (70:b5:e8:6c:34:41)  
> Internet Protocol Version 4, Src: 10.100.40.67, Dst: 10.100.40.43  
> Transmission Control Protocol, Src Port: 56160, Dst Port: 12345, Seq: 1, Ack: 1, Len: 569  
> Transport Layer Security

[그림 4.20.1] 로그인 패킷

2. SSL 적용으로 패킷 내용 확인 불가.

Wireshark - Follow TCP Stream (tcp.stream eq 1) - 이더넷	<pre>.....+..... .....3.k.i.....f.....c2.6.....XT..gE f.....A.....Y.j.....ZC@.....m..V.....3..4.W.d..... .....4.....9.....[.....&amp;.....b.....d.....\$.....q6.....6..1.....+10C.....s.....QH.....m..v.d..I..T.f..j%\\..1.....PXm.....L.....I..b.....X..[.7..... .....g.....AB.....U.....+.....3.E.....A.3.d7.....A.)&lt;b?.....j.....G.....C.Dg58.....q.T.....G.RP.....q.....Q.....0.....mm.....(.....m.....Ay0; P/0)8Z. 8.mv.....(.....V.....3.Z.&amp;.....Ys.....o..... .....r.XL.....(.....?.....&gt;)H .....U9.....(.....0.....xt)q.....a.....3.....;.....?.....1.....kz1Uuk.S.....7..2.....So#2n.....Tf.....Q.....SaY.....F..... 6.....f.....G.....K\\d.....9.....8.....B.....\\[B0md..\$R.....^1..Pa.Y&lt;.....}.....c.....^.....\$.....Q.....E.YR.I.0.....umd.....Gb.....o.....gB.....{.....9. [.....Y.....p.....U.....g.....Fg.p.m.m.....%.....^VH.....(.....D.....{.....B.....r.....v.....4. .....U...../.....\$0tv.X.....twD.....&gt;.....3.....o\$B.....H.KK2n#&amp;.....e.....-.....).....78.@W.....t.....aJ.....Y.ad.M.OM.D.....E.....U.oPo.....0.....N&gt;.....].....S5V.??zf.e..... \${&lt;...W*. .o\\q.....r.....f.....D.....m.....[.....\$.....\$.....K.....W.K.....X.....0.....B.....d.....f.....y.....o\$M.....;.....V.....r1.....[.....6.....c.....c.....\$\$. .....K.&amp;..... .....%.....C.....[E.F.....@&gt;.....7c;.....d.....%.....X^.....t.....\$.....m.....u.....z.....X.....l.....u.....#.....w.....z^.....h.....[.....].....&gt;.....y.....^.....v.....&lt;.....^.....Ia3.5.d...../ &gt;g*cm.....a.....m(s^.....5.....S.....^D.....o.....Y.....H.....(.....^8.OD.....Y.....IY.....^.....S.....o.....u...../.....q.....3.B&amp;.....N.....%.....C.....(.....P.....[.....d2.Xt. 0BF6t.....K.V.....@.....:.....k.....0i.....1A.....D^0[.....]VAU.JF.....t.....Ue.....T.....a.....e..... .....4n.....cOS.....2.....L.....(.....P.....R.....m.....t.....ctj.....).....8F.....&gt;.....&gt;.....14.....2a.....Qq4X.....[.....+...../.....q..... .....0.....X.....e.....g..... .....1um8;5.0.....6.....0.....i.....PP.DS .....t.....t.....6K.....(.....).....2.....&lt;[U.....u.....).....mp%.....i.....1.....zi.P\$Cy.....eU.....g.....BT.p.2o.60..... .....2.....z.....v.....ye.....v.....(.....d.....j.....(.....d.....[.....j.....KJ.....'.....2.....xJ.....I s&gt;c&gt;Z.A.....a.....l.....c.....V.....n.sx.i.k.....?.....o.....l.....[4K .....&amp;b.....&lt;.....[.....H.....@k.0Y.....[.....G.....Hg.2.....[.....m .....].....Q.4.....[.....X.....d.....&amp;.....\$.....h.....%.....c.....^.....0.....b.....m.....r.....n.....u.....C.....1.....l.....(.....^.....)bF.....p.....p.....P.....y.....l.....S.....0.....r.....l.....0%.....[.....{.....-.....2.D.....C. .....&amp;.....M.....%.....s.....t.....1%.....].....z.....b.....f.....;.....R.....@.....G.....s.....X.....c.....&lt;.....X.....s.....{.....s.....M.....K.....a.....B.....&lt;.....I.....[.....j.....j.....).....5.....n.....&lt;.....oS.....(.....I.....K.....%.....3n.....j.....838A.T..... {.....h.....#3.A.k.....j.....[.....q..... .....P.....f.....E.....E.....Q.....3.6.o.....A.....[.....].....8u.....k.....m7.A.....[.....].....g.....p.....^.....@.....1 Z.....c...../.....W.....if3.....[.....P.....@.....s.....MP.....q.....H.....X.....[.....s.....}.....+wX.B.....[.....[.....8.....X.....1.....9.....].....K.....&lt;.....?.....By.....S.....r.....l.....z.....g.....X^B.....p.....S.....[.....Hg.....?.....?.....]..... .....\\.....%.....[.....[.....1L.B.....[.....].....Y.....2.....q.....h.....6.....&gt;.....D.....(.....snEF.20%0.....Q...../.....y.....C.....m.....Q.....r....._.....2.....z.....R^.....GNDs.....X.....I.....3..... kF...../.....).....z.....Rdo.....t4.....[..... .....?.....0.....^.....^.....XQ.....(.....).....-.....8.....(.....u.....@.....X.....).....%.....h.....Y.....m.....zm.E...../.....l.....l.....I.....I.....?..... .....A.....ho.....[.....&amp;.....+.....U.....n^b.....f.....P.....[.....\\.....H.....[.....].....@.....x.....i.....(.....H.....[.....].....).....-.....*.....0.....6#j.....7e.....(+.....&lt;.....I.....v.....z.....5.....8j.....793.....#..... .....q.....e.....l.....x.....c..... .....AZ.....j.....^3 19.....&gt;.....gtE.)G.HN.....;Q^T.....&lt;.....y.....P8.....[.....(mp.....D.....[.....q.....[.....Cag.....y.....c.....+.....@?.....^.....0.....tQ.....c.....(.....("kv&lt;R.&amp;W.....^.....F.....c.....hA&amp;.....c.....B. [.....].....081.H.....[.....].....&gt;.....D/B.D81&lt;.....&lt;.....&gt;.....}.....t..... .....3.....u.....v.....P#H.....&amp;...../.....(.....).....q.....t.....&amp;.....q&amp;.....[.....g.....6.....+.....+.....+.....+.....S1.....\\.....^....._.....oV.....K.....a.....[.....&gt;.....Q.....\\.....[.....].....\$.....%.....).....\\.....=.....i.....c.....u.....x.....[.....F..... (.....w.....l.....k.....%.....{.....I.....Y.....r.....[.....].....W.....Y.....[.....].....S.....T.....[.....].....M.....\$.....[.....].....v.....u.....D.....[.....].....Zo.....+.....@.....[.....].....d.....[.....].....b..... (.....r.....&gt;.....c.....[.....].....[.....r....._.....P....._.....3.....^.....o.....&gt;.....b.....c.....o.....r.....Dm.....I..... .....*.....#.....j.....I.....c.....n.....w.....g.....[.....].....5..... a.....(.....[.....Ue.....%.....C.....m.....&gt;.....z.....Z.....c.....B9.....[.....].....5.....^.....).....x.....R.....3ee.....N.....j.....62q.....m.....V...../..... 0.....j.....[.....].....s.....N.....m.....#.....f.....^.....89.....[.....].....^.....h.....k.....w.....[.....].....F.....mQo.....Y.....gwJ.....cib.....V.....FD.....A.....N.....&amp;M.3I.....N.....kr.....[.....TNSV." z.....r.....I.....0.....0.....%.....M.....[.....].....q.....[.....].....g.....&amp;.....3.....I.....[.....].....^.....D.....Q.....[.....].....(.....A.....R.....^.....W.....[.....].....Oa.E)FTA.&lt;j5 #.....D.....[.....].....H.....+.....[.....].....KA.....t.....*.....i.....c.....T.....33B.3F.....[.....].....s2.....[.....].....&gt;.....R.....I.....u.....Om.....[.....].....&gt;.....I.....m.....Pd..... .....3.....[.....].....3.....[.....].....5U4#..... .....l.....j.....(.....C.....Y.....t.....*.....q9.....M.....7.....Z.....Y.....r.....3.....[.....].....f.....c.....9.Y5J.....1.3v.....^.....4D?.....G.....e.....h.....t.....I.....(.....3z.9.....LYe.9.....\\.....V.....[.....].....T.....\\.....Ik.....[.....].....B..... .....^.....*.....1.....aZ.....[.....].....?.....a.....[.....].....A.....oP.....[.....].....V.....m..... R.....[.....].....x.....0.....[.....].....%.....&amp;.....[.....].....l.....[.....].....Y.....[.....].....p.....[.....].....QD.3.....[.....].....p.....UBZ.....*.....kG=4v.d.z.s.y.?.....^.....8.....n.....y.....g.....Qm.....u.....+.....Q.....R3.....[.....].....l.....g.....ut.....&gt;.....p.....7.....(.....[.....].....k.....^...../.....7.m..... 2PS.....*.....K.....f.....W.....t.....o.....s.....[.....].....D...../.....^.....c.....r.....m.....n.....#.....[.....].....W.....[.....].....j.....s.....n.....y.....X.....[.....].....6.....k.....[.....].....w.....H.....F.....l.....E.....^.....G.....[.....].....R.....m.....w.....V.....[.....].....W.....?...../ +mcD.....^.....T.....z.....Z.....Yy.....[.....].....).....?ovX&lt;.....^.....d.....daAYt.K.....[.....].....).....9D.....E.....[.....].....t.....v.....z.....S..... *.....e.....#.....?.....9Ob.....[.....].....Z.....[.....].....c.....vz.....[.....].....).....U.....T.....96.....[.....].....).....QxWc.....[.....].....8n.....W.....2.....[.....].....%.....8.....t.....\\.....s.....o.....r..... mN.....[.....].....6.....[.....].....X.....1.....l.....[.....].....^.....[.....].....w.....K.....\\.....^.....6N1.....[.....].....c.....^.....[.....].....l.....[.....].....F.....[.....].....^.....x.....g.....s5.V.....[.....].....B.....[.....].....5.....[.....].....C.....[.....].....q.....c.....[.....]..... .....[.....].....Bul.....[.....].....nk.....UT[.....].....[.....].....[.....].....\\.....E.....?.....?.....u.....Z.....[.....].....v.....[.....].....R.....^.....?.....#.....[.....].....c.....@.....[.....].....Z.....V.....[.....].....*.....[.....].....+.....q.....2</pre>
-------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[그림 4.20.2] 정보확인 불가

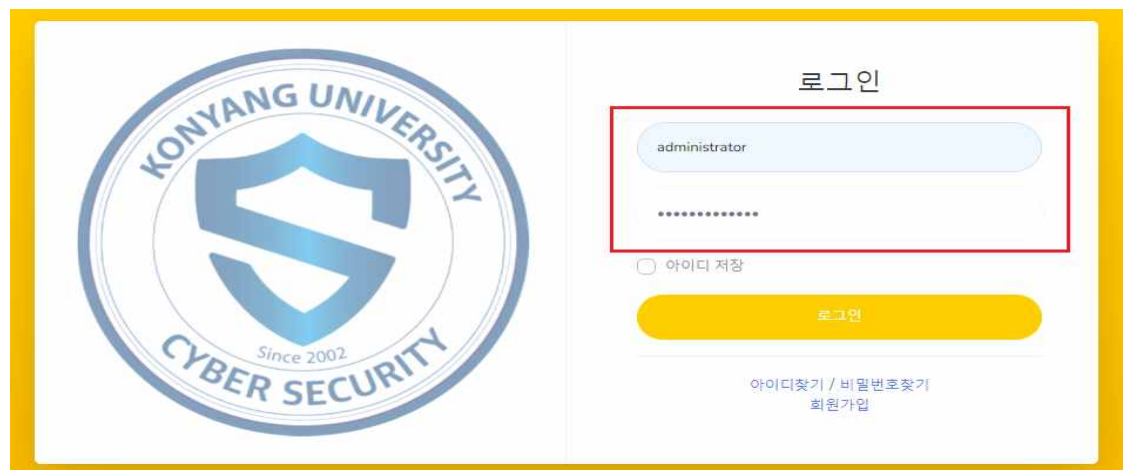
권고사항	사이트의 중요정보 전송구간(로그인, 회원가입, 회원정보관리, 게시판 등) 암호화 통신(https, 애플리케이션방식) 적용
------	---------------------------------------------------------------------

#### 4.21 약한문자열강도

Code	BF	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	웹페이지 내 로그인 폼 등에 약한 강도의 문자열 사용 여부 점검				
설 명	웹 어플리케이션에서 회원가입 시 안전한 패스워드 규칙이 적용되지 않아 취약한 패스워드로 회원가입이 가능할 경우 공격자가 추측을 통한 대입 및 주변 정보를 수집하여 작성한 사전(dictionary) 파일을 통한 대입을 시도하여 사용자의 패스워드를 추출할 수 있는 취약점				
판단기준	양호: 관리자 계정(비밀번호 포함)이 유추하기 어려운 계정으로 설정되어 있는 경우 취약: 관리자 계정(비밀번호 포함)이 유추하기 쉬운 계정으로 설정되어 있는 경우				
취약내용	유추 가능한 관리자 계정으로 추측하여 로그인시 로그인이 가능하므로 취약함.				

1. 유추 가능한 취약한 관리자 계정 및 패스워드를 추측으로 로그인.

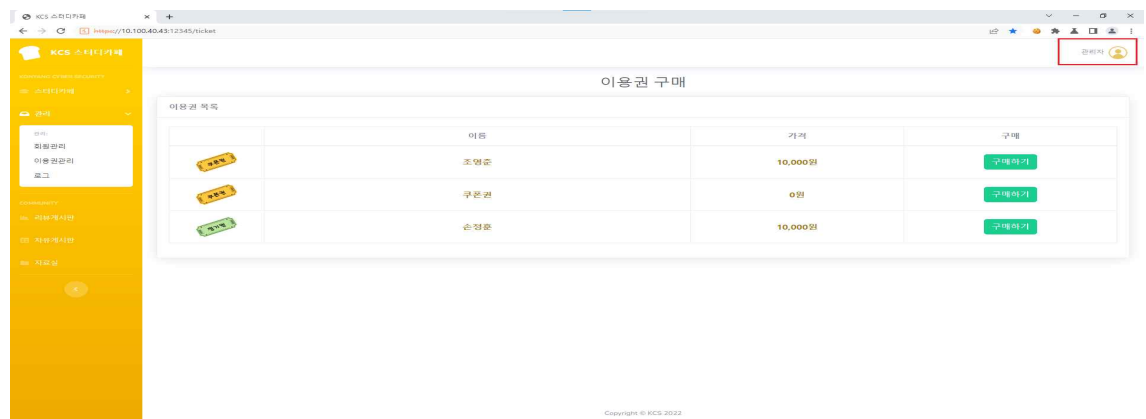
사용구문- ID: administrator PW: " or '1'='1'



점검결과

[그림 4.21.1] 관리자 계정 로그인

2. 성공적으로 로그인이 된 것을 확인.

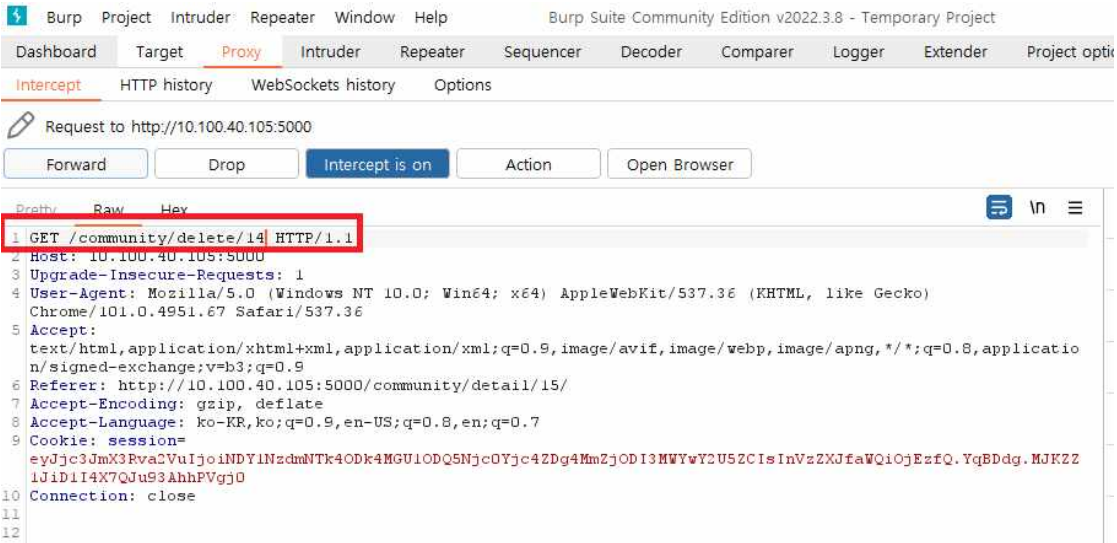


[그림 4.21.2] 성공적으로 로그인

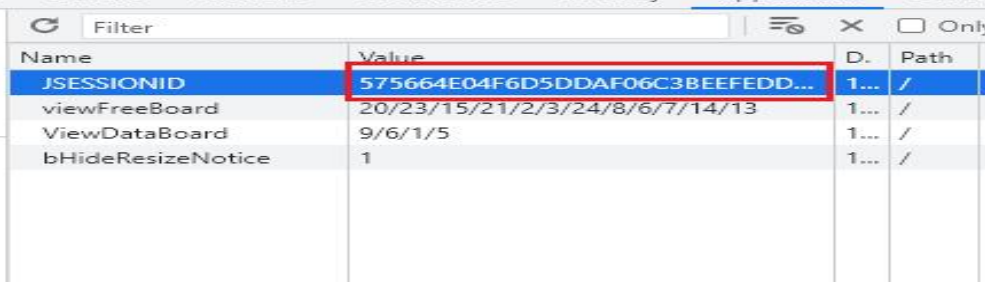
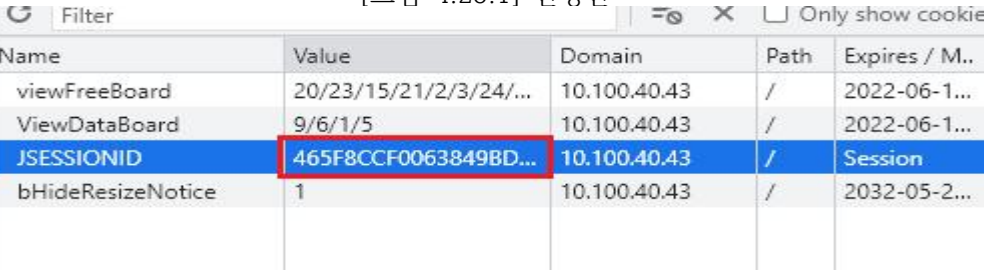
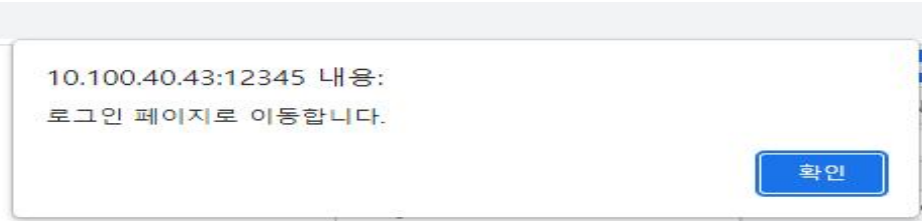
권고사항

취약한 계정 및 패스워드를 삭제하고, 사용자가 취약한 계정이나 패스워드를 등록하지 못하도록 패스워드 규정이 반영 된 체크 로직을 구현하여야 함

## 4.22 불충분한인가

Code	IN	위험도	H	진단결과	취약
점검영역	웹 애플리케이션				
점검항목	민감한 데이터 또는 기능에 접근 및 수정 시 통제 여부 점검				
설 명	접근제어가 필요한 중요 페이지의 통제수단이 미흡한 경우, 비인가자가 URL 파라미터값 변경 등의 방법으로 중요 페이지에 접근하여 민감한 정보 열람 및 변조 가능한 취약점				
판단기준	양호: 접근제어가 필요한 중요 페이지의 통제수단이 적절하여 비인가자의 접근이 불가능한 경우 취약: 접근제어가 필요한 중요 페이지의 통제수단이 미흡하여 비인가자의 접근이 가능한 경우				
취약내용	파라미터 변조를 통해 타 사용자의 게시물 삭제 가능하므로 취약함.				
점검결과	<p>1. 데이터 전송 방식이 "GET" 방식이기 때문에 "Delete"를 입력 후 게시물 번호를 입력하면 타사용자의 게시물 삭제가능.</p>  <p>[그림 4.22.1] 파라미터변조</p>				
권고사항	접근제어가 필요한 모든 페이지에 권한검증 로직 구현				

#### 4.23 쿠키변조

Code	CC	위험도	H	진단결과	양호
점검영역	웹 애플리케이션				
점검항목	쿠키 사용 여부 및 사용하는 경우 안전한 알고리즘으로 암호화 여부 점검				
설 명	클라이언트에 전달되는 쿠키에 사용자 식별 값이 평문으로 노출될 경우 쿠키 변조를 통해 다른 사용자의 유효한 세션을 취득할 수 있으며, 기타 중요정보의 유출 및 변조 가능한 취약점				
판단기준	<p>양호: 쿠키를 사용하지 않고 Server Side Session 을 사용하고 있거나, 쿠키(또는 Session)를 사용하는 경우 안전한 알고리즘(SEED, 3DES,AES)이 적용되어있는 경우</p> <p>취약: 클라이언트에 전달되는 쿠키에 사용자 식별 값이 평문으로 노출될 경우 쿠키 변조를 통해 다른 사용자의 유효한 세션을 취득할 수 있으며, 기타 중요정보의 유출 및 변조 가능함</p>				
취약내용	세션값으로 로그인시 로그인 화면으로 이동하므로 양호함.				
점검결과	<p>1. 사용자 세션정보 변경을 통해 로그인 되는지 확인.</p>  <p>[그림 4.23.1] 변경전</p>  <p>[그림 4.23.] 변경후</p> <p>2. 로그인 페이지로 이동되는 것을 확인.</p>  <p>[그림 4.23.2] 로그인 페이지 이동</p>				
권고사항	웹 서버 응용프로그램(Apache, Tomcat, IIS 등) 을 최신버전으로 패치하고 임의의 문자열 입력에 대한 검증 로직 구현				

## 5. 최종 진단

	취약점	비율
취약	10	43.4%
양호	12	56.5%
N/A	1	0%
계	23	100%

**웹 서버보안 점수는 56점으로 - “미흡” 단계인 것으로 파악됨.**

※점검항목/점검 분야의 취약도가 높아 위협에 노출될 경우 심각한 피해를 초래 할 수 있음.