
실천 웹 서버 해킹과 대응 8조

웹 취약점 점검 및
방어 보고서

2022-06-24



팀장	류 규 원
팀원	조 영 준
	양 온 유
	손 정 훈
	김 성 준

목차

1. 수행개요	2
1.1 정의 및 목적	2
1.2 수행단계	2
1.3 수행대상	2
1.4 기대효과	2
2. 점검 항목	3
2.1 취약점 요약	3
2.2 점검 결과	4
3. 취약점 진단 점검 결과	5
3.1 악성콘텐츠	5
3.2 약한문자열강도	6
3.3 불충분한 인증	7
3.4 취약한 패스워드 복구	8
3.5 불충분한 인가	9
3.6 불충분한 세션만료	10
3.7 파일업로드	11
3.8 관리자페이지 노출	12
3.9 데이터평문전송	13

1. 수행 개요

1.1 정의 및 목적

본 진단은 웹해킹 8팀이 구현한 "Upbite" 웹 서비스에 대한 보안 취약점을 도출하여 이를 사전에 제거함으로써 내·외부의 악의적인 공격으로부터 서비스 및 정보를 보호하기 위한 것이며 웹해킹 7조가 웹 취약점을 점검하고 분석을 통해 작성된 공격보고서를 토대로 발생한 취약점을 분석하고 방어하며, 그에 따른 대응책 수립 후 보고서를 작성함.

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	Upbite 홈페이지	https://10.100.40.105:5000	

1.4 기대효과

- 대응책을 확보하여 홈페이지 안정성 증가
- 취약점 발견 과정 중 대처능력 향상
- 장기적인 정보보호 계획 수립 및 이행체계 구축

2. 웹 취약점 진단 점검 결과

2.1 취약점 요약

점검영역	CODE	점검항목	위험도	점검결과
※ 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	양호
	SS	SSI 인젝션	H	양호
	XI	XPath 인젝션	H	양호
	DI	디렉토리 인덱싱	H	양호
	IL	정보누출	H	양호
	CS	악성콘텐츠	H	취약
	XS	크로스사이트스크립팅	H	양호
	BF	약한문자열강도	H	취약
	IA	불충분한 인증	H	취약
	PR	취약한 패스워드복구	H	취약
	SE	세션 예측	H	양호
	IN	불충분한 인가	H	취약
	SC	불충분한 세션만료	H	취약
	AU	자동화 공격	H	양호
	FU	파일업로드	H	취약
	FD	파일다운로드	H	양호
	AE	관리자페이지 노출	H	취약
	SN	데이터 평문전송	H	취약
	CC	쿠키변조	H	양호

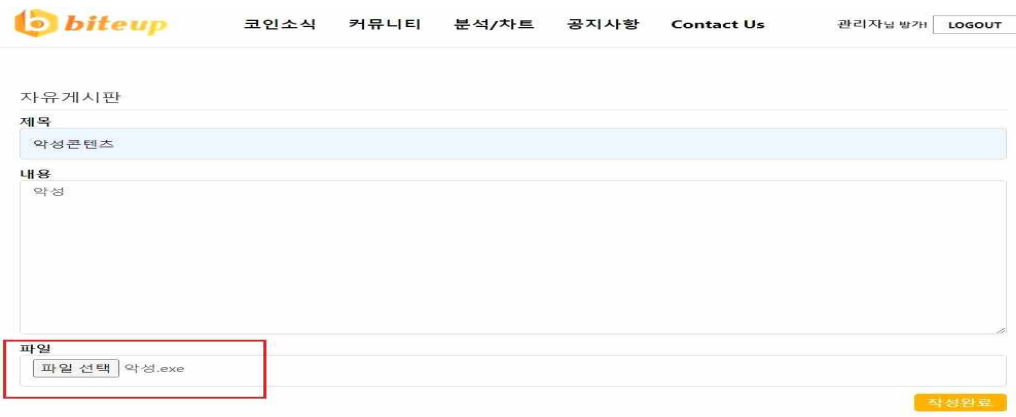
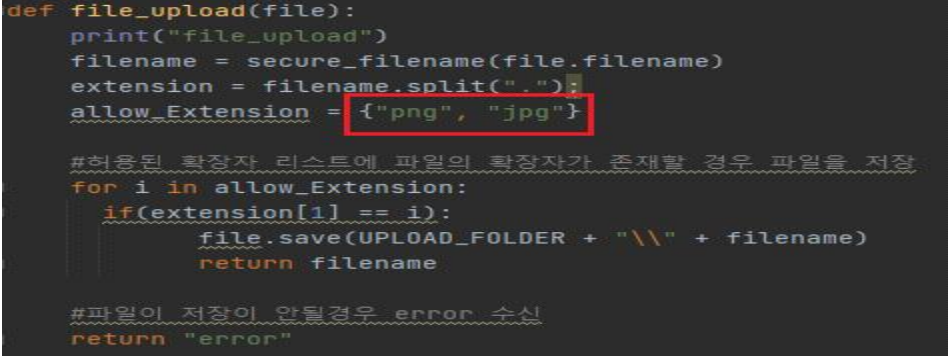
※ 본 진단항목은 “주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세가이드”를 참고하였음.

2.2 진단결과

점검영역	CODE	점검항목	위험도	진단결과
웹 애플리케이션	CS	악성콘텐츠	H	취약
	BF	약한문자열강도	H	취약
	IA	불충분한 인증	H	취약
	RP	취약한 패스워드 복구	H	취약
	IN	불충분한 인가	H	취약
	SC	불충분한 세션만료	H	취약
	FU	파일업로드	H	취약
	AE	관리자페이지 노출	H	취약
	SN	데이터평문전송	H	취약

3. 취약점 진단 점검 결과

3.1 악성콘텐츠

Code	CS	위험도	H	진단결과	취약
설 명	웹 어플리케이션에서 사용자 입력 값에 대한 필터링이 제대로 이루어지지 않을 경우 공격자가 악성콘텐츠를 삽입할 수 있으며, 악성콘텐츠가 삽입된 페이지에 접속한 사용자는 악성코드 유포 사이트가 자동으로 호출되어 악성코드에 감염될 수 있는 취약점				
취약내용	 <p>악의적인 프로그램 "exe"파일 업로드 가능함.</p>				
대응방안	 <p>파일 업로드 기능에 Flash 파일이나 avi동영상 파일, exe 실행파일 등 악성코드가 포함될 수 있는 콘텐츠를 삽입 또는 업로드 하지 못하게 필터링.</p>				

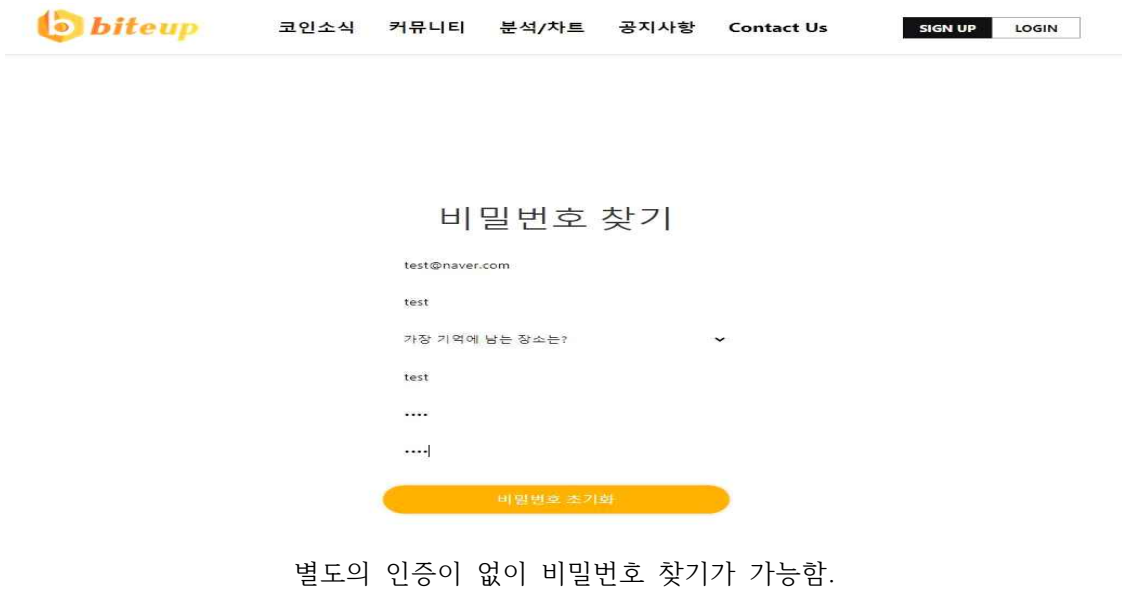
3.2 약한문자열강도

Code	BF	위험도	H	진단결과	취약
설 명	웹 어플리케이션에서 회원가입 시 안전한 비밀번호 규칙이 적용되지 않아 취약한 비밀번호로 회원가입이 가능할 경우 공격자가 추측을 통한 대입 및 주변 정보를 수집하여 작성한 사전(dictionary) 파일을 통한 대입을 시도하여 사용자의 패스워드를 추출할 수 있는 취약점				
취약내용	<pre> 10.100.40.43 - - [08/Jun/2022 15:45:56] "GET /static/bootstrap.min.css HTTP/1.1" 304 - 10.100.40.43 - - [08/Jun/2022 15:45:56] "GET /static/bootstrap.min.js HTTP/1.1" 304 - 10.100.40.43 - - [08/Jun/2022 15:45:56] "GET /static/style.css HTTP/1.1" 304 - 10.100.40.43 - - [08/Jun/2022 15:45:56] "GET /static/jquery-3.6.0.min.js HTTP/1.1" 404 - 10.100.40.43 - - [08/Jun/2022 15:45:56] "GET /static/topbutton.png HTTP/1.1" 304 - 로그인 : biteup@biteup.com 10.100.40.43 - - [08/Jun/2022 15:46:00] "POST /login_re HTTP/1.1" 302 - 10.100.40.43 - - [08/Jun/2022 15:46:00] "GET / HTTP/1.1" 200 - 10.100.40.43 - - [08/Jun/2022 15:46:00] "GET /static/jquery-3.6.0.min.js HTTP/1.1" 404 - 10.100.40.43 - - [08/Jun/2022 15:46:00] "GET /static/style.css HTTP/1.1" 304 - 10.100.40.43 - - [08/Jun/2022 15:46:00] "GET /static/bootstrap.min.css HTTP/1.1" 304 - 10.100.40.43 - - [08/Jun/2022 15:46:00] "GET /static/bootstrap.min.js HTTP/1.1" 304 - 10.100.40.43 - - [08/Jun/2022 15:46:00] "GET /static/topbutton.png HTTP/1.1" 304 - 10.100.40.43 - - [08/Jun/2022 15:46:00] "GET /static/logo.png HTTP/1.1" 304 - </pre> <p>공격자 IP 10.100.40.43에서 관리자 계정으로 로그인한 정황이 포착됨.</p>  <p>홈페이지 하단 “메일주소”가 관리자계정으로 되어있어 공격자가 추측을 통한 대입 및 주변 정보를 수집을 통해 계정탈취 이루어짐.</p>				
대응방안	<p>-유추가능한 계정 및 패스워드 사용 하지 않도록 조치.</p> <p>-취약한 계정 및 패스워드를 삭제하고, 사용자가 취약한 계정이나 패스워드를 등록하지 못하게 패스워드 규정이 반영이 된 체크로직을 구현하여야 한다.</p>				

3.3 불충분한 인증

Code	IA	위험도	H	진단결과	취약
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				
취약내용	 <p>공격자 IP "10.100.40.41"가 관리자 계정을 임의로 비밀번호를 변경한 정황을 포착함.</p>				
대응방안	 <p>사용자가 이용 가능 페이지에 접근할 때마다 승인을 얻은 사용자인지 페이지마다 검증하는 모듈을 구현하여야 한다.</p>				

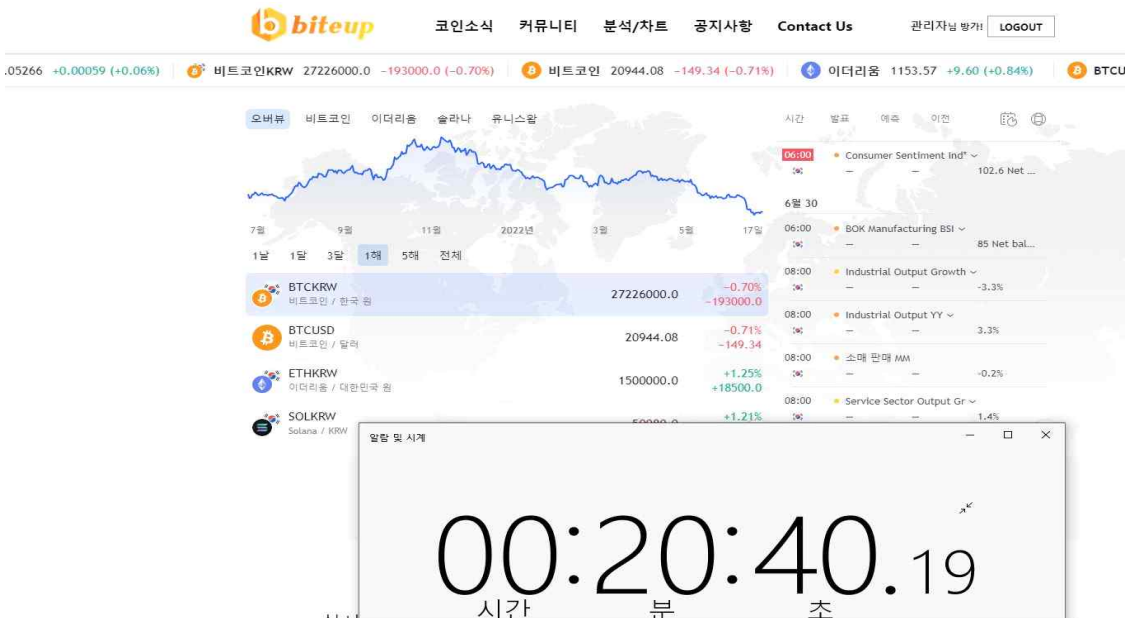
3.4 취약한 패스워드 복구

Code	RP	위험도	H	진단결과	취약
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				
취약내용	 <p>별도의 인증이 없이 비밀번호 찾기가 가능함.</p>				
대응방안	<p>-사용자 개인 정보(연락처, 주소, 메일 주소 등)로 패스워드를 생성하지 말아야 하며, 난수를 이용한 불규칙적이고 최소 길이(6자 이상 권고) 이상의 패턴이 없는 패스워드를 발급하여야 함</p> <p>-사용자 패스워드를 발급해주거나 확인해줄 때 웹 사이트 화면에 바로 출력해주는 것이 아니라 인증된 사용자 메일이나 SMS로 전송해주어야 함</p>				

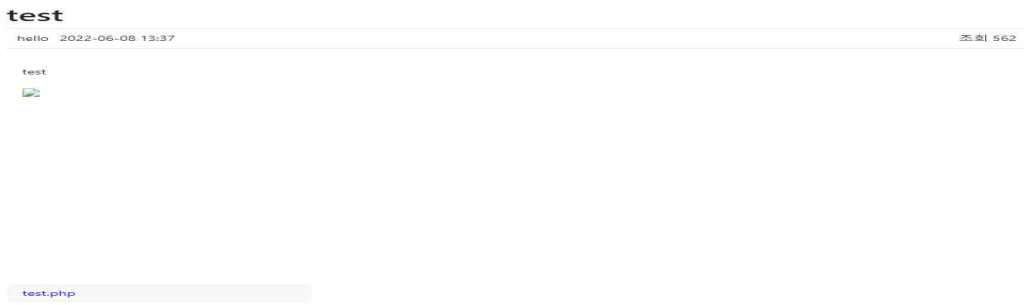
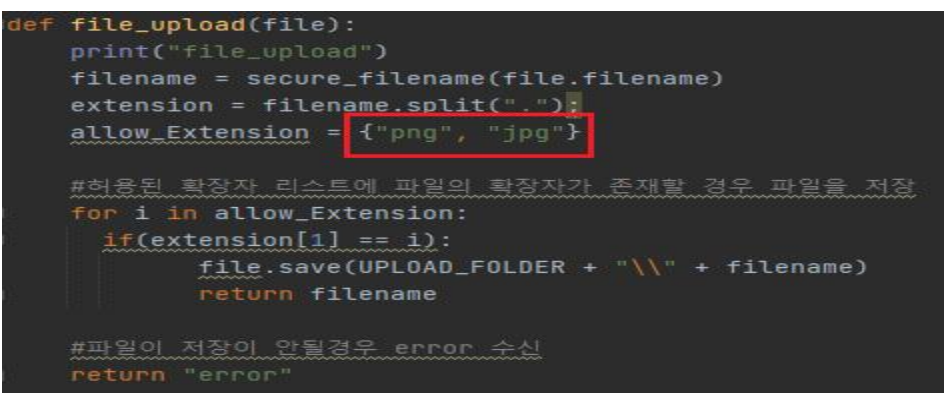
3.5 불충분한 인가

Code	IN	위험도	H	진단결과	취약
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				
취약내용	<p>공격자 IP "10.100.40.43"에서 일반계정"123@123.com"으로 관리자 계정"biteup@biteup.com"의 게시글"손정"을 삭제하는 정황이 포착됨.</p> <pre> 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /community/detail/17/ HTTP/1.1" 200 - 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /static/bootstrap.min.css HTTP/1.1" 304 - 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /static/style.css HTTP/1.1" 304 - 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /static/bootstrap.min.js HTTP/1.1" 304 - 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /static/jquery-3.6.0.min.js HTTP/1.1" 40 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /static/topbutton.png HTTP/1.1" 304 - 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /static/bootstrap.min.css.map HTTP/1.1" 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /static/bootstrap.min.js.map HTTP/1.1" 4 10.100.40.43 - - [10/Jun/2022 14:08:46] "GET /static/logo.png HTTP/1.1" 304 - </pre> <p>게시글 삭제됨 test@naver.com -> biteup@biteup.com 제목 : 1 본문 : 1</p> <pre> 10.100.40.43 - - [10/Jun/2022 14:09:19] "GET /community/delete/16 HTTP/1.1" 200 - 10.100.40.43 - - [10/Jun/2022 14:09:20] "GET /community/list HTTP/1.1" 200 - 10.100.40.43 - - [10/Jun/2022 14:09:20] "GET /static/bootstrap.min.css HTTP/1.1" 304 10.100.40.43 - - [10/Jun/2022 14:09:20] "GET /static/style.css HTTP/1.1" 304 - 10.100.40.43 - - [10/Jun/2022 14:09:20] "GET /static/bootstrap.min.js HTTP/1.1" 304 - 10.100.40.43 - - [10/Jun/2022 14:09:20] "GET /static/jquery-3.6.0.min.js HTTP/1.1" 40 10.100.40.43 - - [10/Jun/2022 14:09:20] "GET /static/topbutton.png HTTP/1.1" 304 - 10.100.40.43 - - [10/Jun/2022 14:09:20] "GET /static/bootstrap.min.js.map HTTP/1.1" 4 </pre> <p>게시글을 수정하려고 할 때 로그인한 계정과 게시글을 생성한 계정을 확인하여 일치하는 지 확인한 후 게시글 삭제 권한을 주어야함.</p>				
대응방안	<pre> def delete(community_id): community = Community.query.get_or_404(community_id) if g.user != community.user and g.user.email != "biteup@biteup.com": print("게시글 삭제 권한 없음") print(g.user.email+" -> "+community.user.email) return '<script>alert("삭제 권한이 없습니다.");location.href="/community/detail/' + str(community_id) + '"/</script>' </pre> <p>사용자가 이용 가능 페이지에 접근할 때마다 승인을 얻은 사용자인지 페이지마다 검증하는 모듈을 구현하여야 한다.</p>				


3.6 불충분한 세션만료

Code	SC	위험도	H	진단결과	취약
설 명	세션의 만료 기간을 정하지 않거나, 만료기한을 너무 길게 설정된 경우 악의적인 사용자가 만료되지 않은 세션을 활용하여 불법적인 접근이 가능할 수 있는 취약점				
취약내용	 <p>로그인후 권장 세션시간 15분이 지나도 로그아웃이 되지 않음.</p>				
대응방안	<pre>def create_app(): app = Flask(__name__) app.config.from_object(config) app.config["PERMANENT_SESSION_LIFETIME"] = timedelta(minutes=10) # ORM db.init_app(app) if app.config['SQLALCHEMY_DATABASE_URI'].startswith("sqlite"): migrate.init_app(app, db, render_as_batch=True) else: migrate.init_app(app, db) from . import models</pre> <p>세션 타임아웃 권장시간인 10분으로 권고하고 있다.</p>				

3.7 파일업로드

Code	FU	위험도	H	진단결과	취약
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				
취약내용	 <p>“php”파일이 업로드 된 것을 확인.</p> <pre> 192.168.148.1 - - [08/Jun/2022 13:36:57] "GET /static/topbutton.png HTTP/1.1" 304 - 192.168.148.1 - - [08/Jun/2022 13:36:57] "GET /static/icon.png HTTP/1.1" 304 - file_upload 게시글 생성 작성자 : hello@naver.com 별명 : hello 제목 : test 내용 : test 업로드 파일 : test.php 192.168.29.140 - - [08/Jun/2022 13:37:12] "POST /community/create HTTP/1.1" 200 - 192.168.29.140 - - [08/Jun/2022 13:37:13] "GET /community/list HTTP/1.1" 200 - 192.168.29.140 - - [08/Jun/2022 13:37:13] "GET /static/bootstrap.min.css HTTP/1.1" 304 - 192.168.29.140 - - [08/Jun/2022 13:37:13] "GET /static/bootstrap.min.js HTTP/1.1" 304 - </pre> <p>공격자 IP 192.168.148.1에서 허용되면 안되는 확장자 PHP업로드 정황이 포착됨.</p>				
대응방안	 <pre> def file_upload(file): print("file_upload") filename = secure_filename(file.filename) extension = filename.split(".")[-1] allow_Extension = ["png", "jpg"] #허용된 확장자 리스트에 파일의 확장자가 존재할 경우 파일을 저장 for i in allow_Extension: if(extension[i] == i): file.save(UPLOAD_FOLDER + "\\" + filename) return filename #파일이 저장에 안될경우 error 수신 return "error" </pre> <p>업로드 된 파일의 확장자를 이미지 관련 확장자로 화이트리스트 정책을 적용한다.</p>				

3.8 관리자페이지 노출

Code	AE	위험도	H	진단결과	취약
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				
취약내용	 <p>관리자페이지가 존재하는 것이 확인됨.</p>				
대응방안	<pre>@bp.route('/', methods=('POST', 'GET')) @login_required def login(): if g.user.email == "biteup@biteup.com": print("관리자 페이지 접근 성공: " + g.user.email) return '<script>alert("관리자 입니다.");location.href="/admin/main"</script>' else: print("관리자 페이지 접근 실패 : " + g.user.email) return render_template('404.html')</pre> <p>관리자 페이지 주소를 직접 입력하여 접근하지 못하도록 관리자 페이지 각각에 대하여 관리자 인증을 통해 접근하도록 설정한다.</p>				

3.9 데이터평문전송

Code	SN	위험도	H	진단결과	취약
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.				

취약내용

The image shows a Wireshark packet capture of an HTTP POST request. The packet list on the left shows packet 94107 selected. The packet details pane on the right shows the 'Hypertext Transfer Protocol' section with the 'HTML Form URL Encoded' data. The body of the request is visible in the packet bytes pane at the bottom, showing a clear-text password '1=bitewup 540bitewup.com&password=admin' highlighted with a red box.

로그인정보(패스워드 등)가 평문으로 전송되는 것이 확인됨.

대응방안

The image shows a Wireshark packet capture of an SSL/TLS connection. The packet list on the left shows packet 57 selected. The packet details pane on the right shows the 'Hypertext Transfer Protocol' section with the 'HTML Form URL Encoded' data. The body of the request is visible in the packet bytes pane at the bottom, showing a clear-text password '1=bitewup 540bitewup.com&password=admin' highlighted with a red box.

서버와 클라이언트 통신 시 중요정보가 사용되는 구간에 SSL 등의 안전한 암호화 통신을 적용하여 중요정보가 노출되어도 알아 볼 수 없도록 한다.