


쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립

팀 명 : 모 의 해 킹 3 6 기

이 름 : 구 본 혁

2022-08-18


	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

문서 정보 / 수정 내역

File Name	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립
원안작성자	구본혁
수정작업자	구본혁


수정 날짜	대표 수정자	Revision	추가/수정 항목	내 용
2022.08.16	구본혁	0.0	초안 작성	보고서 초안작성
2022.08.17	구본혁	0.1	회원가입 우회 추가	회원가입 우회 공격 실행 및 내용작성
2022.08.18	구본혁	0.2	관리자 페이지 접근, 타인의 게시물 및 주문정보 수정 내용 추가	회원가입 외 다른 취약점 진단 및 보고서 작성
2022.08.19	구본혁	0.3		최종 확인 및 검토
2022.09.14	구본혁	0.4		대응방법 수정

표 1-1 문서 정보 / 수정 내역

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

목 차

1	개요	8
1.1	프로젝트 주제	8
1.2	프로젝트 추진 배경 및 목표	8
1.3	프로젝트 요약	8
2	시나리오 개요	9
3	GMSHOP대상 취약점 진단	11
3.1	회원가입 계정 인증 우회	11
3.1.1	분석 과정.....	11
3.1.2	대응 방안.....	13
3.2	타인 주문정보 조회	14
3.2.1	분석 과정.....	14
3.2.2	대응 방안.....	16
3.3	타인 게시물 수정 및 삭제.....	18
3.3.1	분석 과정.....	18
3.3.2	대응 방안.....	25
3.4	적립금 조작	26
3.4.1	분석 과정.....	26
3.4.2	대응 방안.....	28
3.5	결제금액 조작	29
3.5.1	분석 과정.....	29
3.5.2	대응 방안.....	31
3.6	관리자 페이지 접근	32
3.6.1	분석 과정.....	32
3.6.2	대응 방안.....	36

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

4	참고 문헌.....	37
4.1	단행본	37
4.2	참조 홈페이지	37


	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

표 목차

표 1-1 문서 정보 / 수정 내역	2
표 1-1 프로젝트 주제	8
표 1-2 프로젝트 추진 배경 및 목표	8
표 1-3 프로젝트 요약	8
표 2-1 가상머신 준비	9
표 2-2 진단 대상	9
표 2-3 취약점 진단 계정	10
표 3-1 공격자와 피해자 주문상세 페이지 URL	14
표 4-1 단행본	37
표 4-2 참조 홈페이지	37


	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

그림 목차

그림 2-1 OWASP-2021	9
그림 3-1 부적절한 아이디 생성 시도 시 경고	11
그림 3-2 응답값 자바스크립트 중 아이디 검증 부분	12
그림 3-3 아이디검증하는 자바스크립트 함수 일부	12
그림 3-4 아이디로 admin 입력	13
그림 3-5 admin아이디 가입신청	13
그림 3-6 admin계정 생성성공	13
그림 3-7 victim1의 주문내역	14
그림 3-8 주문상세로 넘어갈 때 서버응답 캡처	15
그림 3-9 아이디 변조	15
그림 3-10 victim1의 주문상세내역 페이지	16
그림 3-11 victim1이 작성한 1:1문의 게시글	18
그림 3-12 공격자1:1문의게시글	19
그림 3-13 서버로부터의 응답	19
그림 3-14 idx143을 변경 후	20
그림 3-15 victim1의 1:1게시물	21
그림 3-16 수정된 희생자의 게시글	22
그림 3-17 희생자의 비밀게시글 접근	22
그림 3-18 공격자의 수정 요청 시도 캡처	23
그림 3-19 공격자가 작성한 1:1문의 게시판 응답 위조	23
그림 3-20 희생자가 작성한 자유게시글 수정	24
그림 3-21 희생자가 작성한 비밀글 수정	25
그림 3-22 적립금 5000원 사용	26
그림 3-23 주문서 작성 후 결제 요청 캡처	27
그림 3-24 적립금을 음수로 조작	27
그림 3-25 조작된 적립금이 적용됨	27
그림 3-26 장바구니에 물건을 담은 후 결제 진행	29
그림 3-27 결제 단계로 가는 요청 캡처	29
그림 3-28 변조된 구매 금액 정보	30
그림 3-29 결제성공	30
그림 3-30 관리자 로그인 페이지 발견	32
그림 3-31 관리자 페이지 로그인 시도 캡처	32
그림 3-32 인트루더로 로그인 요청 전송	33



	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

그림 3-33 공격 형태 설정	33
그림 3-34 임의 사전파일 생성.....	34
그림 3-35 페이로드 설정	34
그림 3-36 사전파일 대입 시작.....	35
그림 3-37 admin/admin으로 로그인 성공.....	35

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

1 개요

1.1 프로젝트 주제

1. 굿모닝 쇼핑몰 웹사이트 취약점 조사

표 1-1 프로젝트 주제

1.2 프로젝트 추진 배경 및 목표


1. 쇼핑몰 인증 미흡 취약점 진단 및 대응 방안 수립

표 1-2 프로젝트 추진 배경 및 목표

1.3 프로젝트 요약

1. 쇼핑몰 인증 미흡 취약점 진단 및 대응 방안 수립

표 1-3 프로젝트 요약

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

2 시나리오 개요

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

그림 2-1 OWASP-2021

그림 2-1 출처: <https://owasp.org/Top10>


그림 2-1은 OWASP2021 Top10이다. 취약한 인증에 관한 부분은 실무에서도 많이 발견되는 취약점이다. 매년 top10안에 드는 것을 보아 여전히 심각한 문제이지만, 2017년에는 2위에서 2021년 7위로 내려온 사실을 보아 표준화된 프레임워크의 활용이 도움이 되었다고 판단할 수 있다. 웹 사이트 취약점 점검 시나리오에는 회원가입 인증 우회, 관리자 페이지 접근, 타 사용자의 게시물 불법 수정 및 삭제, 타 사용자의 정보 조회, 거래 조작 등이 있다. 이번 과제는 시나리오 구상->취약점 점검->결과 확인->보고서 작성 순으로 진행할 것이다. 과제를 수행하기 앞서, 준비물은 다음과 같다.

가상머신
VMware Workstation Pro16

표 2-1 가상머신 준비

진단대상
http://192.168.254.128/gmshop/


표 2-2 진단 대상

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

	계정	브라우저
공격자	attack1	Chrome
희생자	victim1	Chrome, Micro Edge

표 2-3 취약점 진단 계정

이번에 가상서버에 구축된 온라인 쇼핑몰 사이트 '굿모닝 샵' 대한 취약점 점검을 진행하며 모의 해킹 보안 실무자로서 갖춰야 할 역량을 끌어올릴 것이다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

3 gmsshop대상 취약점 진단

3.1 회원가입 계정 인증 우회

3.1.1 분석 과정

점검대상	http://192.168.254.128/gmsshop/member_join.php?bDeal=0&agreement=checkbox
------	---

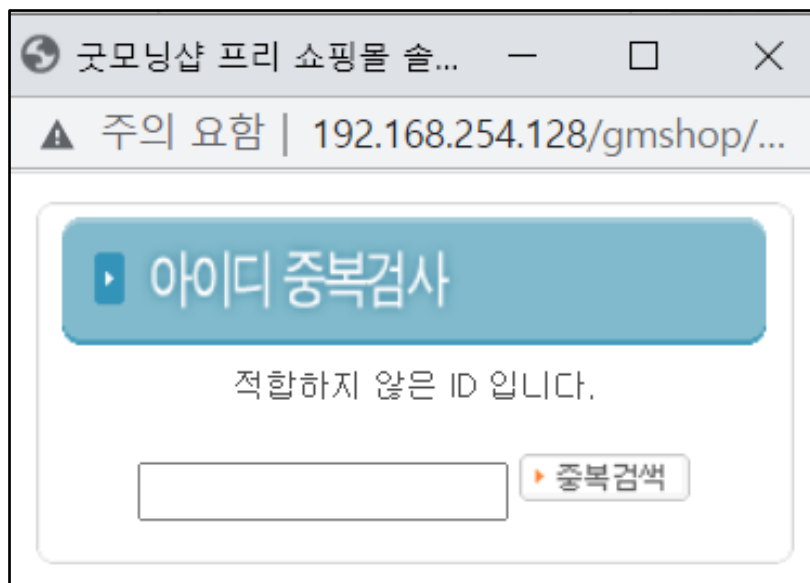



그림 3-1 부적절한 아이디 생성 시도 시 경고

웹사이트 취약점을 점검할 때 제일 먼저 봐야 할 부분은 회원가입 부분이다. 회원가입 부분은 한번 가입할 때만 나타나고 다시 돌아오는 것은 계정을 다시 생성하는 것이 아닌 이상 불가능하기 때문에 처음부터 꼼꼼히 살펴봐야 한다. 만약 html태그가 들어가거나 관리자 관련 아이디 생성을 시도하거나, 또는 기존에 존재하는 사용자에게 내용을 덮어서 회원가입을 시도하는 등의 시도를 ID검증에서 차단해야 한다. 굿모닝 샵에서 회원가입 시 부적절한 아이디를 넣고 검사를 하면 그림 3-1의 '적합하지 않은 ID입니다' 같은 경고 메시지가 출력된다.

회원가입 시 동의 후 자신의 정보를 입력하는 폼으로 넘어가기 전 서버로부터의 응답을 버퍼 스위트로 캡처한다. 그 중 아이디를 검증하는 함수부분은 아래 그림 3-2와 같다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

```

112 function joinSendit()
113 {
114     var form=document.joinForm;
115     if(form.userid.value=="")
116     {
117         alert("아이디를 입력해 주십시오.");
118         form.userid.focus();
119     }
120     else if(checkSpace(form.userid.value) != "")
121     {
122         alert("아이디에 공백을 포함할수 없습니다.");
123         form.userid.focus();
124         form.userid.select();
125     }
126     else if(form.id_check.value == "")
127     {
128         alert("아이디 중복검색을 해주십시오.");
129         form.userid.focus();
130     }
131     else if(form.userid.value!=form.id_check.value)
132     {
133         alert("중복검색된 아이디를 수정하였습니다. 다시 중복검색을 해주십시오.");
134         form.userid.focus();
135     }
136     else if(form.pwd1.value == "")
137     {
138         alert("비밀번호를 입력해 주십시오.");
139         form.pwd1.focus();
140     }

```

그림 3-2 응답값 자바스크립트 중 아이디 검증 부분

Function joinSendit()함수에서 사용자가 입력한 아이디, 비밀번호, 주소 등을 검증하고 부적절한 입력이나 공백이 있는지 확인하고 제출하는 기능을 한다는 것을 알 수 있다. 우리는 관리자 ID와 같거나 유사한 'admin'이라는 아이디로 계정을 생성할 것이다. 만약 'admin'이라는 아이디로 생성을 시도하면 그림 3-1같은 경고가 출력된다.


```

else if(form.id_check.value == "")
{
    alert("아이디 중복검색을 해주십시오.");
    form.userid.focus();
}
else if(form.userid.value!=form.id_check.value)
{
    alert("중복검색된 아이디를 수정하였습니다. 다시 중복검색을 해주십시오.");
    form.userid.focus();
}

```

그림 3-3 아이디검증하는 자바스크립트 함수 일부

우리는 캡처한 서버의 응답 자바 스크립트에서 그림 3-3부분을 제거할 것이다. 이 부분을 제거 후 인터셉트 기능을 끈다. 그리고 그림 3-4처럼 'admin'아이디로 회원가입을 진행한다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

기본정보 ★ 필수항목

> 회원 아이디 ★ 중복검색

> 비밀번호 ★

> 비밀번호 확인 ★

> 이름 ★

그림 3-4 아이디로 admin 입력

```

1 GET /chrome-variatiions/seed?osname=win&channel=stable&milestone=104 HTTP/2
2 Host: clientservices.googleapis.com
3 If-None-Match: SMChYyMDIyMDgxNi0yMTExMzkumTY3MDAwEggIABADGGggABo0CggxNjYwNzEwORIAGAE=
4 A-Im: x-bm,gzip
5 Sec-Fetch-Site: none
6 Sec-Fetch-Mode: no-cors
7 Sec-Fetch-Dest: empty
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
9 Accept-Encoding: gzip, deflate

```

그림 3-5 admin아이디 가입신청

그림 3-5는 회원가입 후 서버로부터의 응답을 캡처한 것이다. 오류 메시지가 출력되지 않는다.

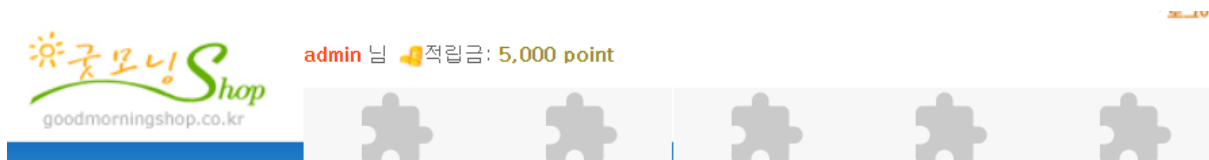



그림 3-6 admin계정 생성성공

아이디 검증 스크립트를 삭제하고 'admin' 아이디로 계정을 생성하는 것을 성공하였다.

3.1.2 대응 방안

클라이언트 암호화	브라우저에서 전달될 때 매개변수를 암호화한다..
서버 사이드 인증	클라이언트 측에서 버프 스위트 같은 도구를 통해 인증을 쉽게 우회할 수 있기 때문에 서버 측에서 서버 사이드 스크립트를 활용하여 사용자가 임의로 스크립트 변경을 하지 못하게 차단해야 한다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

3.2 타인 주문정보 조회

3.2.1 분석 과정

점검대상	http://192.168.254.128/gmshop/mypage_order.php http://192.168.254.128/gmshop/mypage_order_detail.php
------	--

다른 사람이 주문한 목록을 무단으로 열람할 수 있는 것은 기밀성을 해칠 수 있는 부분이다. 별도의 인증 없이 다른 사람의 주문내역을 조회할 수 있는지 점검할 것이다.

192.168.254.128/gmshop/mypage_order_detail.php?data=idx%3D11%26pagecnt%3D0%26letter_no%3D1%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D0




그림 3-7 victim1의 주문내역

현재 'victim1'은 풍경사진 10개를 주문하였고 그림 3-7은 'victim1'의 주문내역이다. 이제 공격자로 접속해서 물건을 주문한다. 공격자도 똑같이 물건을 아무거나 주문하고 물품을 조회하는 상세 페이지로 가본다. 물품 상세 페이지 열람 시 다음과 같은 URL을 볼 수 있다.

공격자 8	http://192.168.254.128/gmshop/mypage_order_detail.php?data=idx%3D10%26pagecnt%3D0%26letter_no%3D8%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D0
피해자 1	http://192.168.254.128/gmshop/mypage_order_detail.php?data=idx%3D11%26pagecnt%3D0%26letter_no%3D1%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D0

표 3-1 공격자와 피해자 주문상세 페이지 URL

공격자와 피해자의 URL을 자세히 보면 data=idx%3D부분이 다르다. 만약 응답 부분에서 이 부분을 변조한다면 다른 사용자의 주문상세내역을 볼 수 있을 것이다.


	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	



그림 3-8 주문상세로 넘어갈 때 서버응답 캡처

그림 3-8은 공격자 계정에서 주문내역에서 물건에 대한 주문 상세내역 페이지로 넘어갈 때 서버의 응답을 캡처한 것이다.

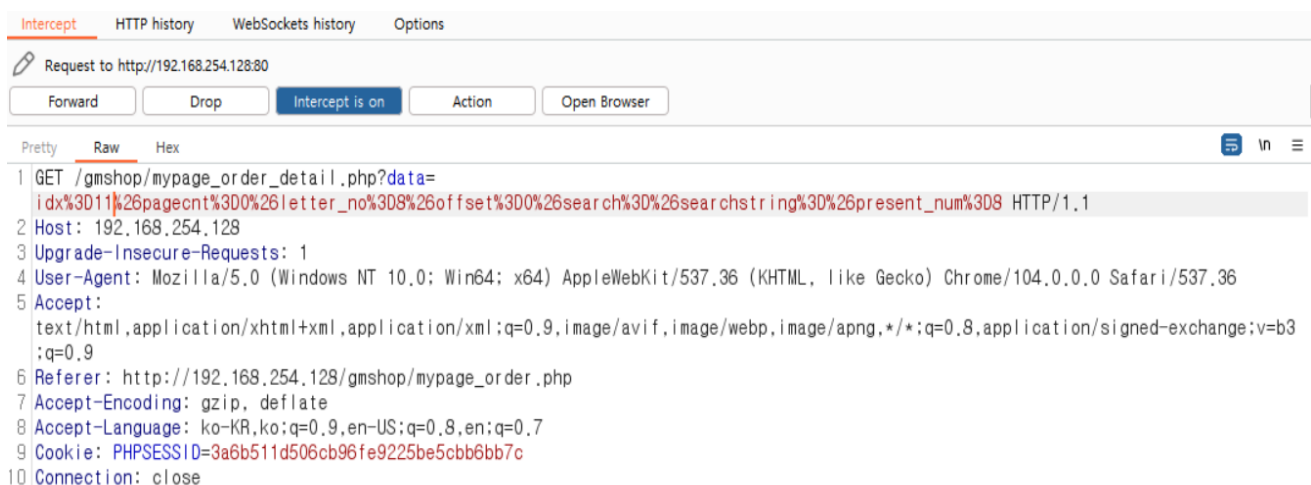



그림 3-9 아이디 변조

그림 3-9처럼 'idx'부분을 변조한다. idx부분을 변조하고 인터셉트를 꺼주면 된다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

커뮤니티

문영자에게 질문사항이 있으시거나 회원간의 정보공유 공간

» 질문과답변(Q&A)
 » 사진컨텐츠
 » 자료실
 » 자유게시판
 » 자유게시판
 » 자유게시판
 » 자유게시판
 » 자유게시판
 » 자유게시판
 » 자유게시판
 » 이미지갤러리

주문내역조회

회원님의 주문날짜 및 배송상태, 주문상품정보를 확인하실 수 있습니다.

상품명	옵션	적립금	구입가	수량	합계	주문상태
 아름다운 풍경 사진		100 원	1,000 원	10	10,000 원	주문접수

주문 정보

주문코드

QUP920591

주문일자

2022-08-18 05:08:09

배송사/송장번호

결제 정보

총상품 금액

10,000 원

사용 적립금

0 원

배 송 비

3,000 원

총 결제 금액

13,000 원

결제 방법

무통장 [한국은행 210-7894-4613 (홍길동)]

주문자 정보

수령자 정보

성명

victim1

이메일

vic@a.com

전화번호

031-1234-5678

휴대폰번호

010-1234-5678

주소

[442-701] 경기 수원시 팔달구 인계동 수원시청

성명

victim1

이메일

vic@a.com

전화번호

031-1234-5678

휴대폰번호

010-1234-5678

주소


[442-701] 경기 수원시 팔달구 인계동 수원시청

그림 3-10 victim1의 주문상세내역 페이지


그림 3-10처럼 'attack1'에서 'victim1'의 주문상세내역 페이지를 열람할 수 있다.

3.2.2 대응 방안

클라이언트 암호화	브라우저에서 전달될 때 매개변수를 암호화한다.
서버 사이드 인증	클라이언트 측에서 버프 스위트 같은 도구를 통해 인증을 쉽게 우회할 수 있기 때문에 서버 측에서 서버 사이드 스크립트를 활용하여 사용자가 임의로 스크립트 변경을 하지 못하게 차단해야 한다.
HTTP메소드 POST방식 사용	GET방식은 URL방식으로 파라미터가 전달되어 정보를 쉽게 열람, 조작할 수 있다. body에 요

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

	청내용을 담아 전달하는 POST방식을 사용하는 것이 더 안전하다.
--	--------------------------------------

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	


3.3 타인 게시물 수정 및 삭제

3.3.1 분석 과정

점검대상	http://192.168.254.128/gmshop/board_view.php http://192.168.254.128/gmshop/ask_view.php http://192.168.254.128/gmshop/ask_edit.php
------	---

다른 사용자가 작성한 자유게시판 게시글과 1:1관리자 문의 게시글을 수정할 수 있는지 점검한다.

1:1 문의게시판



회원과 운영자만이 볼수 있는 비공개 게시판입니다.

글등록하기

이름

victim1

이메일

vic@a.com

제 목

victim1이 작성한 1:1 문의

파일첨부

파일 선택

선택된 파일 없음

내용입력 형식

☐ TEXT
☒ HTML
☐ 웹에디터

희생자가 작성한 문의입니다. 희생 |당할 예정입니다

저장

취소


목록

그림 3-11 victim1이 작성한 1:1문의 게시글

그림 3-11은 'victim1'이 1:1문의 게시판에 작성한 원문이다. 공격자도 똑같이 1:1문의 게시판에 글을 등록한다. 공격자가 게시한 1:1문의 URL을 보면 다음과 같다.

http://192.168.254.128/gmshop/ask_view.php?data=idx%3D145%26pagecnt%3D0%26letter_no%3D1%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D1&boardIndex=

그림 3-12페이지에서 수정을 누르고 버퍼 스위트로 서버로부터의 응답을 잡으면 그림 3-13같다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

1:1 문의게시판


회원과 운영자만이 볼수 있는 비공개 게시판입니다.

제목	공격자가 게시한 1:1문의		
날짜	2022-08-17 09:08:46	조회수	8
글쓴이	attack1	이메일	attack@a.com

공격자가 게시한 1:1 문의 헤헤헤헤헤헤헤헤헤

목록 수정 삭제

그림 3-12 공격자:1:1문의게시글


```

Pretty Raw Hex
1 GET /gmshop/ask_edit.php?data=idx=145 HTTP/1.1
2 Host: 192.168.254.128
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://192.168.254.128/gmshop/ask_view.php?data=idx=145
7 Accept-Encoding: gzip, deflate
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: PHPSESSID=b903c099bd913be1e107aa87850754ce
10 Connection: close

```

그림 3-13 서버로부터의 응답

GET방식으로 서버로부터 게시글을 수정할 수 있는 페이지를 받아온다. 이때 빨간색으로 표시된 URL의 idx부분에 주목하면, 저 부분을 수정할 시 내가 아닌 다른 사람의 수정 페이지로 이동할 수 있다는 것을 알 수 있다. URL의 idx를 143으로 수정하면 아래와 같다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	


▲ 주의 요함 | 192.168.254.128/gmshop/ask_view.php?data=idx=143



그림 3-14 idx143을 변경 후

응답 url의 idx값을 143으로 변경하였을 때 테스트 작성자가 쓴 게시물로 이동하였다.

이번에는 idx값을 144로 변경한다. idx를 변경하면 그림 3-15와 같이 'victim1'의 게시물로 이동할 수 있다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

1:1 문의게시판

회원과 운영자만이 볼수 있는 비공개 게시판입니다.




글수정하기

이름	<input type="text" value="victim1"/>
이메일	<input type="text" value="vic@a.com"/>
제 목	<input type="text" value="victim1이 작성한 1:1 문의"/>
파일첨부	<input type="button" value="파일 선택"/> 선택된 파일 없음
내용입력 형식	<input type="radio"/> TEXT <input checked="" type="radio"/> HTML <input type="radio"/> 웹에디터

희생자가 작성한 문의입니다. 희생 당할 예정입니다
(당신의 게시물... |공격자가 수정합니다)


그림 3-15 victim1의 1:1게시물


'victim1'이 작성한 게시글로 성공적으로 넘어왔다. 여기에서 희생자의 게시글을 수정할 수 있다. 글을 수정하고 저장하면 그림 3-16처럼 게시글이 수정되었다. 이런 방식으로 게시글 수정 말고도 삭제도 가능하다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

1:1 문의게시판

회원과 운영자만이 볼 수 있는 비공개 게시판입니다.





제목	victim10이 작성한 1:1 문의		
날짜	2022-08-17 09:06:53	조회수	0
글쓴이	victim1	이메일	vic@a.com

희생자가 작성한 문의입니다. 희생 당할 예정입니다 (당신의 게시물 ... 공격자가 수정합니다)

목록 수정 삭제

그림 3-16 수정된 희생자의 게시글


이번에는 자유게시판에 작성된 다른 사용자의 글을 수정할 수 있는지 접근할 것이다. 희생자는 자유게시판에 누구나 열람할 수 있는 글 하나, 그리고 관리자만 볼 수 있는 비밀글 하나를 작성한다. 공격자가 비밀글에 접근한다면 다음과 같은 메시지가 출력된다.

192.168.254.128 내용:
비밀번호가 올바르지 않습니다.

확인

그림 3-17 희생자의 비밀게시글 접근

공격자도 자유게시판에 글을 작성하고 수정을 누를 때 서버로 전송되는 요청을 인터셉트하여 idx 값을 조작한다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

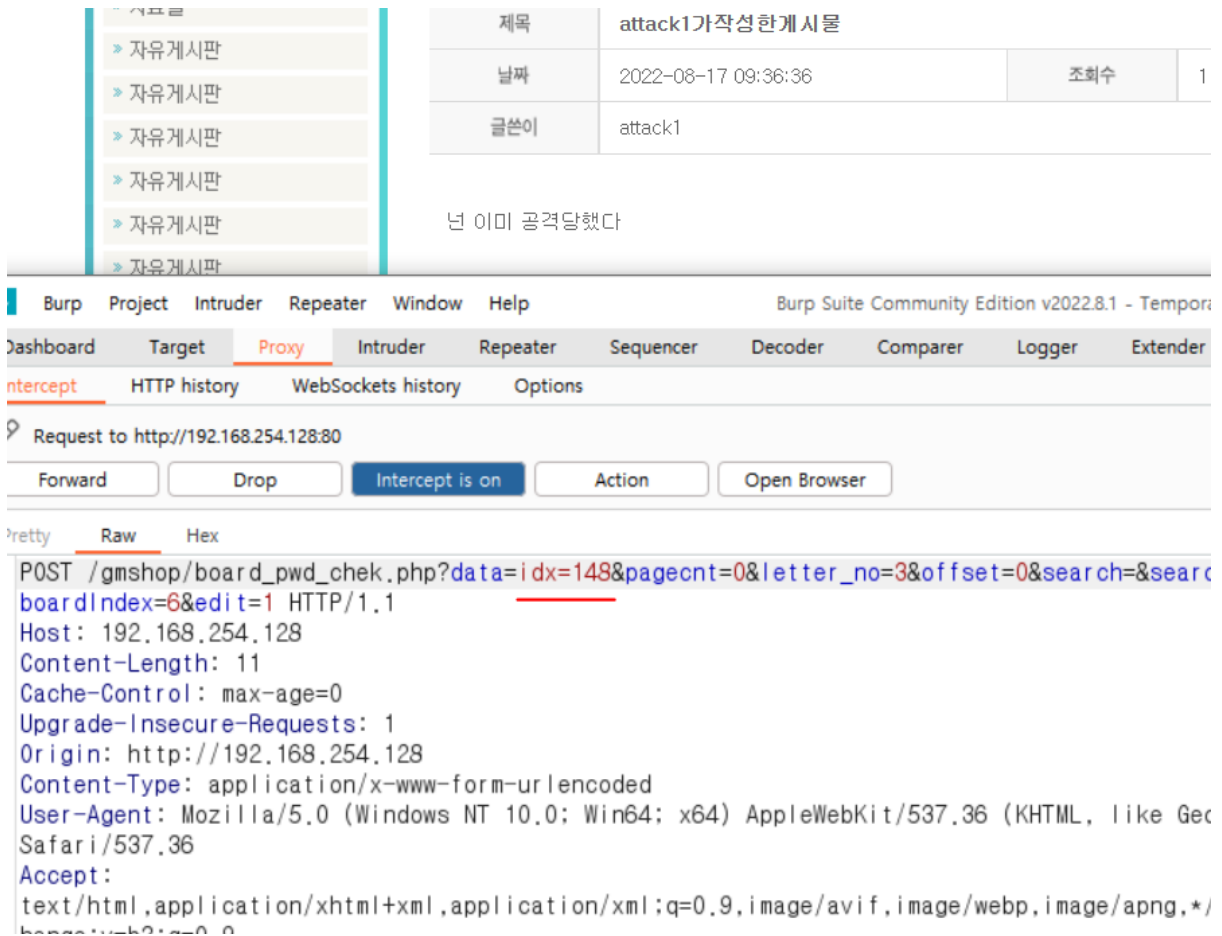


그림 3-18 공격자의 수정 요청 시도 캡처

그림 3-18처럼 idx를 변경해서 요청하면 그림 3-17와 같은 메시지가 출력된다. 이는 서버 측에서 비밀번호를 확인한다는 의미이다. 클라이언트에서 idx를 위조하는 것으로는 접근이 불가능한 것이다. 비밀번호가 필요 없던 1:1문의 게시판에서 우회해서 들어가는 방법이 있다.

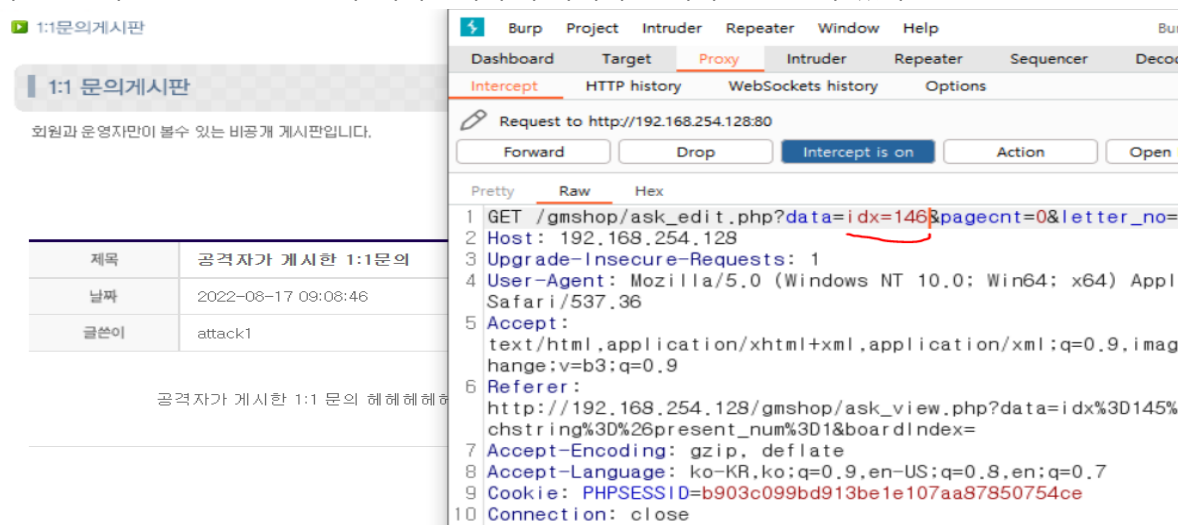


그림 3-19 공격자가 작성한 1:1문의 게시판 응답 위조


	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

그림 3-19같이 idx부분을 145에서 146으로 변경한다. 그러면 타인이 작성한 자유게시글에 접근할 수 있다.


victim1 님 적립금: 5,000 point 함께찾아오는길
즐거찾기

SEARCH 상품명 go 상세검색

카뮤니티 COMMUNITY 현재위치 : HOME > 게시판

자유게시판

회원분들이 자유롭게 글을 올리실 수 있는 게시판입니다.



게시판6


제목	victim1이 작성한 자유게시글 1 (공격자왔다감)		
날짜	2022-08-17 09:31:20	조회수	5
글쓴이	victim1		

짜늘하다.... 게시글에 공격이 날아와 꽃힐거같다.. (침투에 성공하였다!!!!)

이름	내용	날짜	삭제
이름 <input type="text"/> 비밀번호 <input type="password"/>	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: right; margin-top: 5px;">COMMENT 등록</div>		
비밀번호 <input type="password"/>			

그림 3-20 희생자가 작성한 자유게시글 수정

만약 idx를 147로 수정한다면 그림 3-21처럼 비밀글에 접근이 가능하다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

자유게시판

회원분들이 자유롭게 글을 올리실 수 있는 게시판입니다.



게시판6

제목	victim1이작성한자유게시글2 (공격자 왔다감)		
날짜	2022-08-17 09:33:32	조회수	1
글쓴이	victim1		

Stay this Way 무린 뜨겁고 눈부셔 자유롭게 춤춰 저 달이 오늘 따라 예뻐서 Stay this Way 깊고 짙은 Blue~~~날 바라보며 Stay this way (공격자 작성) 그림 같은 우리 such a party moonlight 그림자 groove it 춤을 추지 파도 소리에 몸을 맡겨 hey 매일이 난 sunday 월요일은 사라져

이름	내용	날짜	삭제
이름 <input type="text"/> 비밀번호 <input type="password"/>	<div> <div></div> <div>COMMENT 등록</div> </div>		

비밀번호

목록

수정


답글

삭제

그림 3-21 희생자가 작성한 비밀글 수정

3.3.2 대응 방안

클라이언트 암호화	브라우저에서 전달될 때 매개변수를 암호화한다.
서버 사이드 인증	클라이언트 측에서 버퍼 스위트 같은 도구를 통해 인증을 쉽게 우회할 수 있기 때문에 서버 측에서 서버 사이드 스크립트를 활용하여 사용자가 임의로 스크립트 변경을 하지 못하게 차단해야 한다.
HTTP메소드 POST방식 사용	GET방식은 URL방식으로 파라미터가 전달되어 정보를 쉽게 열람, 조작할 수 있다. body에 요청내용을 담아 전달하는 POST방식을 사용하는 것이 더 안전하다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

3.4 적립금 조작

3.4.1 분석 과정

점검대상	http://192.168.254.128/gmshop/order_sheet.php http://192.168.254.128/gmshop/order_table.php
------	--

상품을 주문하고 결제하는 과정에서 요청을 변조하여 적립금 조작이 가능한지 점검한다. 적립금 부정적립과 실제 결제에 영향을 주는지 확인한다. 굿모닝샵에 회원가입하면 5000포인트를 받고 물건 주문 시 적립금을 사용할 수 있다.

번호	상품명	옵션	상품가	적립금	수량	합계 (원)
1	 아름다운 풍경사진		1,000	10	1	1,000
[배송비 : 3,000 원 , 적립금 10원] 결제금액 : 4,000원						

적립금 정보

적립금	5,000 원
사용가능 적립금	5,000 원
적립금 사용	사용할 적립금 입력 : <input type="text" value="5000"/> <input type="button" value="적립금사용함"/>


※ 결제금액이 0 원 이상이며 적립금이 5,000원 이상일때 무제한 사용 가능합니다.

구매금액정보

상품금액	1000 원
배 송 료	3000 원
결 제금액	4000 원

그림 3-22 적립금 5000원 사용

아무 물건을 담고 주문한다. 이때 5000원을 입력하고 '적립금사용함' 버튼을 누른다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

```

Pretty Raw Hex
1 POST /gmshop/card_update.php HTTP/1.1
2 Host: 192.168.254.128
3 Content-Length: 113
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.254.128
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.254.128/gmshop/order_table.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: PHPSESSID=2df02f8736a766261b6053b70ca931ca
14 Connection: close
15
16 useP=5000&tradeCode=KEB365591&payM=8000&transM=3000&totalM=10000&transMethod=t&pay_ready=paysendit&payMethod=card

```

그림 3-23 주문서 작성 후 결제 요청 캡처

그림 3-23은 결제 요청 시 서버로 가는 요청을 버프 스위트로 잡았다. 붉은색으로 표시된 부분 'useP'부분이 적립금임을 파악할 수 있다.

```

Pretty Raw Hex
1 POST /gmshop/card_update.php HTTP/1.1
2 Host: 192.168.254.128
3 Content-Length: 113
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.254.128
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.254.128/gmshop/order_table.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: PHPSESSID=2df02f8736a766261b6053b70ca931ca
14 Connection: close
15
16 useP=-50000&tradeCode=KEB365591&payM=8000&transM=3000&totalM=10000&transMethod=t&pay_ready=paysendit&payMethod=card

```

그림 3-24 적립금을 음수로 조작

그림 3-24처럼 5000에서 -50000 음수로 적립금을 조작하고 서버로 전송한다.

attack1 님 🧡적립금: 55,000 point

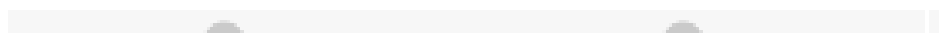




그림 3-25 조작된 적립금이 적용됨

그림 3-25처럼 적립금을 조작하여 적립하는 것이 가능하다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

3.4.2 대응 방안

클라이언트 암호화	브라우저에서 전달될 때 매개변수를 암호화한다.
서버 사이드 인증	클라이언트 측에서 버프 스위트 같은 도구를 통해 인증을 쉽게 우회할 수 있기 때문에 서버 측에서 서버 사이드 스크립트를 활용하여 사용자가 임의로 스크립트 변경을 하지 못하게 차단해야 한다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

▶ 구매금액정보

상품금액	500000 원
배 송 료	0 원
결제금액	500 원

그림 3-28 변조된 구매 금액 정보

변조한대로 결제단계에서 금액이 500원으로 바뀌었다.

SEARCH

상품명 ▼

GO

상세검색

▶ 주문정보

현재위치 : HOME > >

1. 장바구니 담기

2. 주문서 작성하기

3. 결제하기

4. 주문완료



상품주문완료

"저희 쇼핑몰을 이용해주셔서 감사합니다."

회원님은 로그인 후 마이페이지 주문정보에서 주문상태를 확인하실 수 있습니다.

주문 코드 : IPW399831

결제 금액 : 500 원

결제 종류 : 무통장 [한국은행 210-7894-4613 (홍길동)]

상단의 주문조회에서 주문내역 확인 가능합니다.

물품이 배송되면 주문조회에서 해당 주문에 대한 배송완료 처리를 해주셔야 합니다.

▶ 주문내역보기

▶ 메인으로


그림 3-29 결제성공

그림 3-29같이 500,000원에서 500원으로 결제하는데 성공하였다. 결제 금액 요청을 조작할 수 있다는 취약점이 존재한다.

Page 30 of 37


결과보고서

Copyright © 2015 By www.boanproject.com All Rights Reserved.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

3.5.2 대응 방안

클라이언트 암호화	브라우저에서 전달될 때 매개변수를 암호화한다.
서버 사이드 인증	클라이언트 측에서 버프 스위트 같은 도구를 통해 인증을 쉽게 우회할 수 있기 때문에 서버 측에서 서버 사이드 스크립트를 활용하여 사용자가 임의로 스크립트 변경을 하지 못하게 차단해야 한다.
HTTP메소드 POST방식 사용	GET방식은 URL방식으로 파라미터가 전달되어 정보를 쉽게 열람, 조작할 수 있다. body에 요청내용을 담아 전달하는 POST방식을 사용하는 것이 더 안전하다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

3.6 관리자 페이지 접근

3.6.1 분석 과정

점검대상	http://192.168.254.128/gmshop/admin.php
------	---

굿모닝샵의 관리자 페이지를 유추하고 접근할 수 있는지 검사한다. 만약 관리자 페이지를 발견했을 때 아이디와 패스워드를 추측하고 로그인이 되는지 확인한다.




그림 3-30 관리자 로그인 페이지 발견

http://192.168.254.128/gmshop/admin.php로 이동했을 때 그림 3-30같이 관리자 페이지 로그인창이 보인다. 우선 관리자 페이지 로그인 창이 노출되는 것만으로도 큰 문제이다.



그림 3-31 관리자 페이지 로그인 시도 캡처

그림 3-31은 관리자 페이지 로그인 시도 시 사용자의 요청을 버퍼 스위트로 캡처한 것이다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

서버로 가는 요청을 인트루더로 보낸다. 관리자 페이지 로그인을 사전 파일 공격으로 로그인 시도를 할 것이다.

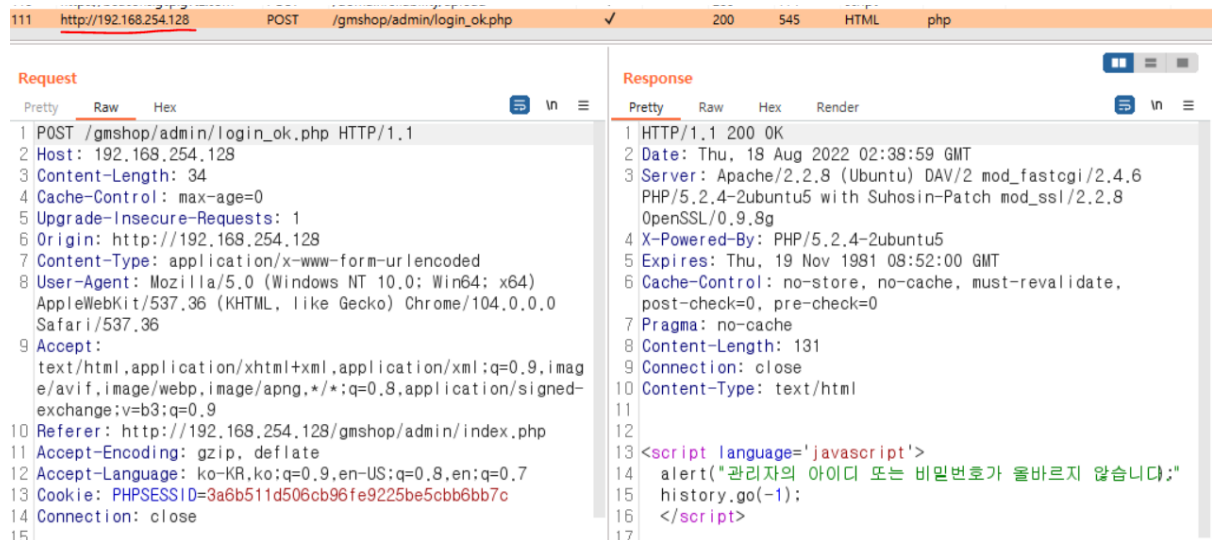


그림 3-32 인트루더로 로그인 요청 전송



그림 3-33 공격 형태 설정


공격 형태는 4가지가 있다. Sniper, Battering ram, Pitchfork 그리고 Cluster bomb가 있다.

Sniper는 하나의 페이로드set만 설정하여 공격하고 여러 개의 페이로드 포지션이 설정되어 있으면 한 번에 하나 포지션에 페이로드set을 차례로 삽입하고 해당 set이 다 삽입되면 다음 포지션에 페이로드set을 대입한다.

Battering ram은 페이로드를 반복하여 사용하며 페이로드가 정의된 모든 위치에 동일한 페이로드를 대입하는 방법이다.

Pitchfork는 설정한 페이로드 포지션의 개수만큼 페이로드 집합을 설정한다.

Cluster bomb은 pitchfork와 방식이 유사하지만 첫 번째 페이로드set을 반복 삽입하며 동시에 두번째 페이로드set을 차례대로 반복 삽입한다는 점이 pitchfork와 다르다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

Cluster Bomb을 공격 타입으로 지정한다.

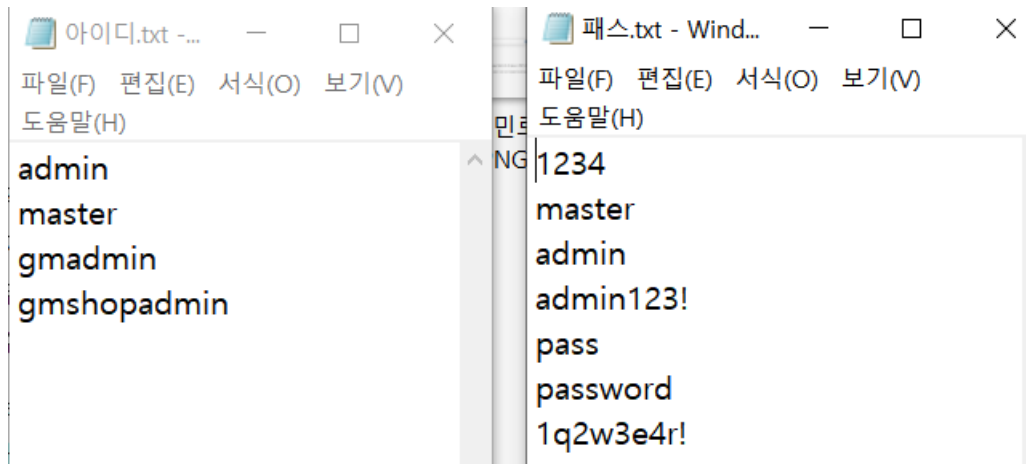


그림 3-34 임의 사전파일 생성

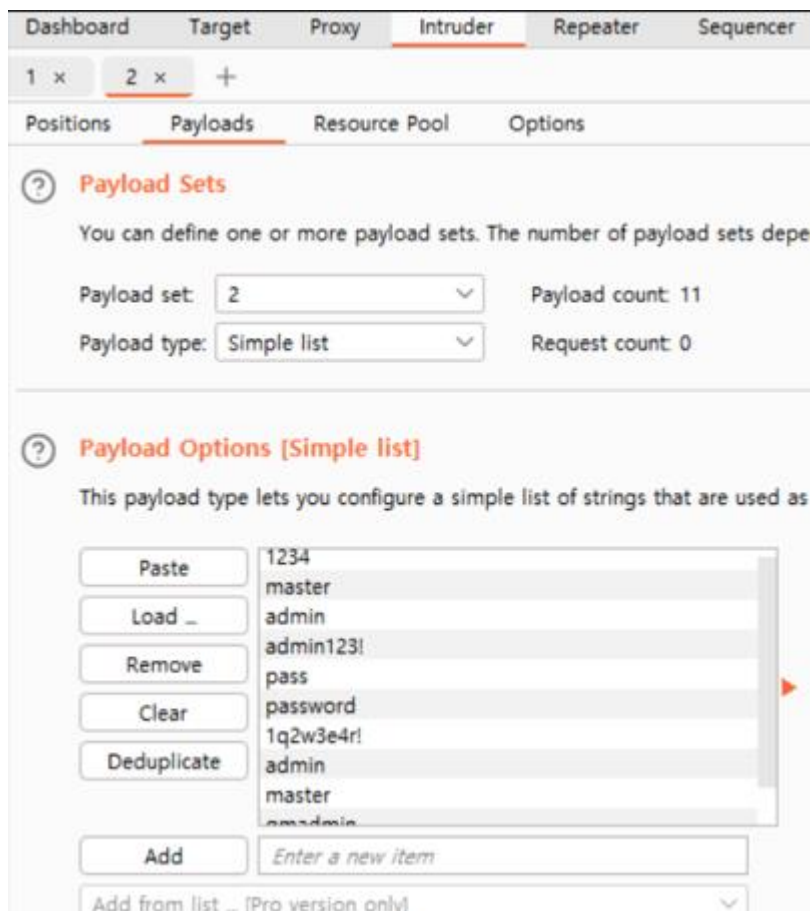


그림 3-35 페이로드 설정


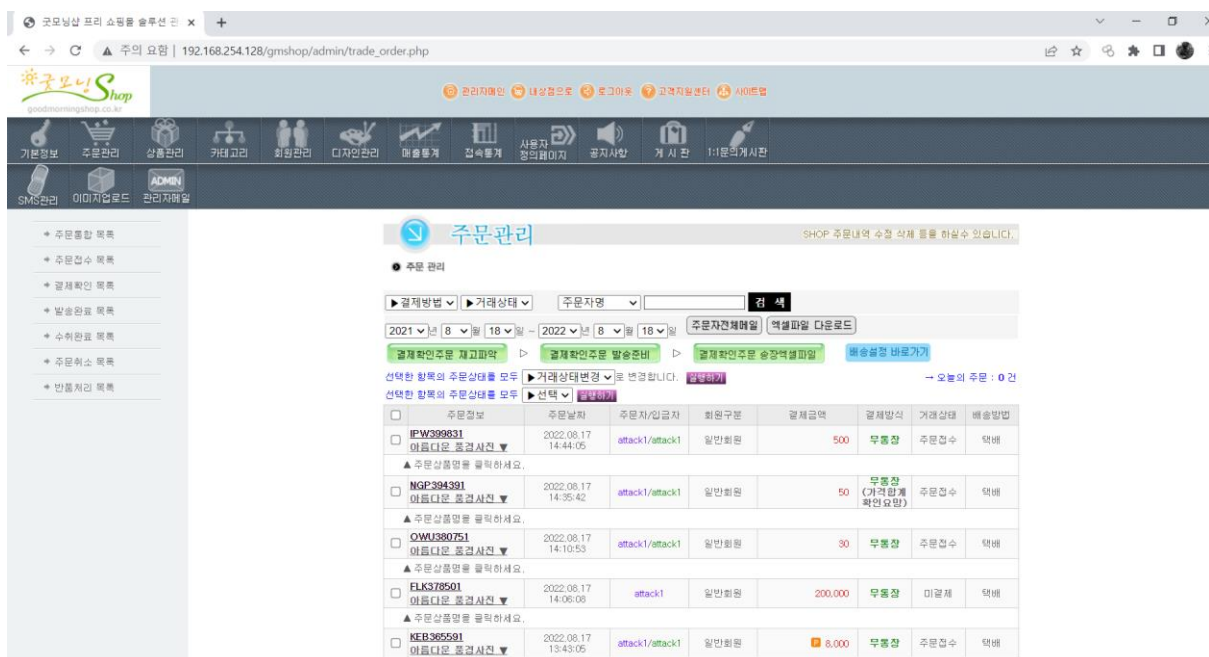
	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

그림 3-35처럼 페이로드 집합을 id/pw 대입을 위해 2로 설정하고 그림 3-34에서 생성한 임의 사전파일을 불러온다.

18	admin	master	200	<input type="checkbox"/>	<input type="checkbox"/>	545
19	admin123!	master	200	<input type="checkbox"/>	<input type="checkbox"/>	545
20	pass	master	200	<input type="checkbox"/>	<input type="checkbox"/>	545
21	password	master	200	<input type="checkbox"/>	<input type="checkbox"/>	545
22	1q2w3e4r!	master	200	<input type="checkbox"/>	<input type="checkbox"/>	545
23	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	473
24	master	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	589
25	gmadmin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	545
26	gmshopadmin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	545
27	1234	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	545
28	master	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	545
29	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	473
30	admin123!	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	589

그림 3-36 사전파일 대입 시작

사전파일 대입공격을 시작하면 오른쪽에 응답값의 길이가 출력된다. 그림 3-36에서 길이가 473, 589로 다른 두 조합을 찾았다. 다른 조합과 비교하였을 때 응답값이 다를 경우 맞는 id/pw조합일 확률이 높다.




The screenshot shows the '주문관리' (Order Management) interface. It includes a sidebar with navigation links like '주문합계', '주문접수', '결제확인', etc. The main content area shows a table of orders. Key entries include:

- Order ID: IPW399831, Date: 2022.08.17 14:44:05, Amount: 500, Status: 무통장 (가계부계좌입금), Method: 주문접수, Delivery: 택배
- Order ID: NGP394391, Date: 2022.08.17 14:35:42, Amount: 50, Status: 무통장 (가계부계좌입금), Method: 주문접수, Delivery: 택배
- Order ID: OWU380751, Date: 2022.08.17 14:10:53, Amount: 30, Status: 무통장 (가계부계좌입금), Method: 주문접수, Delivery: 택배
- Order ID: ELK378501, Date: 2022.08.17 14:06:08, Amount: 200,000, Status: 무통장 (가계부계좌입금), Method: 미결제, Delivery: 택배
- Order ID: KEB365591, Date: 2022.08.17 13:43:05, Amount: 8,000, Status: 무통장 (가계부계좌입금), Method: 주문접수, Delivery: 택배


그림 3-37 admin/admin으로 로그인 성공

아이디와 패스워드를 'admin' / 'admin'으로 로그인한 결과 관리자 페이지 로그인에 성공하였다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

3.6.2 대응 방안

권한 확인 루틴 구현	서버가 제공하는 모든 기능에는 각 기능을 요청하는 사용자가 해당 기능을 실행할 수 있는 적절한 권한을 가졌는지 확인하는 루틴이 필요하다. 관리자 기능이나 RBAC기능이 구현되어 있다면 철저한 검증이 필요하다.
쉬운 디렉터리 명 사용 지양	/admin/처럼 쉽게 추측할 수 있는 디렉터리 사용을 지양해야 한다. 관리자 인터페이스를 별도의 포트번호에서 제공해야 한다. 관리자 메뉴는 HTTPS를 이용하여 외부에 전송되는 데이터가 노출되지 않도록 해야 한다.
지정 사용자만 접근	웹 애플리케이션 외부적으로 특정 IP범위를 지정하여, 지정된 사용자만 관리자 메뉴에 접근할 수 있도록 접근통제를 구축한다.

	쇼핑몰 대상 인증 미흡 취약점 진단 및 대응 방안 수립			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.4	2022.09.14	

4 참고 문헌

4.1 단행본

도서명	저자	출판사
화이트 해커를 위한 웹 해킹의 기술	최봉환	BJ퍼블릭

표 4-1 단행본

4.2 참조 홈페이지

참조 홈페이지
https://owasp.org/Top10 https://securitycode.tistory.com/21 https://www.digicert.com/kr/what-is-ssl-tls-and-https

표 4-2 참조 홈페이지