

웹 취약점 진단 보고서

K-Shield JR G-5조

정관우
박태범
임혜원

CONTENTS

01

개요

- 목표
- 기대효과
- 프로젝트 내역

02

취약점 진단

- 정보 수집방법
- 취약점 진단
- 보고서 작성 내역
- 가이드 작성

03

향후 과제

- Sql injection 자동화
- 진단 우회 방법
연구

01

개요

01

※ 목표

- ☞ 웹 서비스 내에 존재하는 취약점을 찾고, 해당 취약점을 보완하는 것

※ 기대효과

- ☞ 잠재적인 웹 위협을 사전에 미리 탐지하고 차단할 수 있다

※ 각자 맡은 역할

- ☞ 정관우 – csrf, 불충분한 세션만료, 파일 업로드
- ☞ 박태범 – xss, sql Injection, 데이터 평문 전송
- ☞ 임혜원 – 관리자 페이지 노출, 정보누출, 불충분한 인증

02

취약점 진단

02

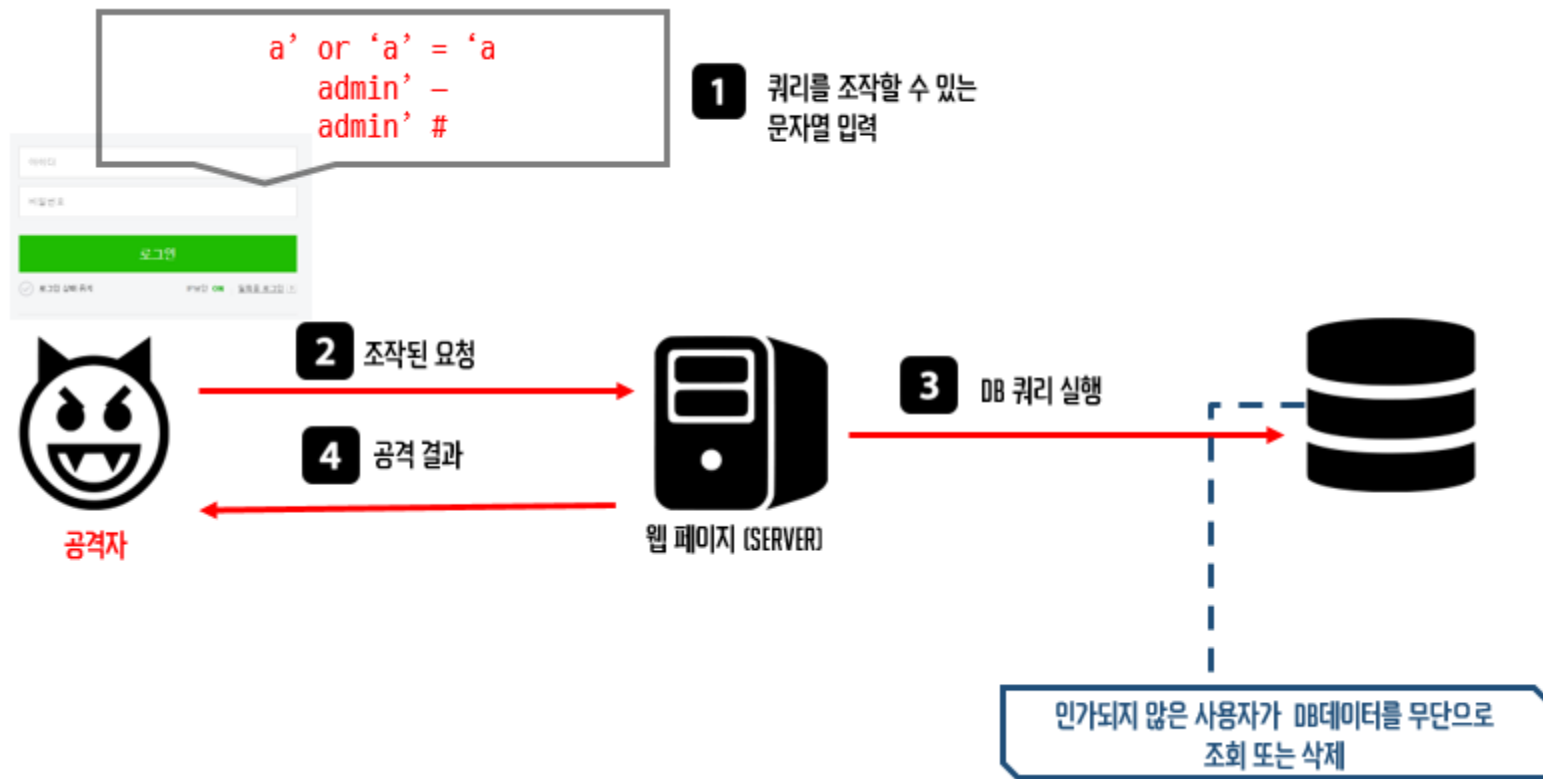


Wireshark

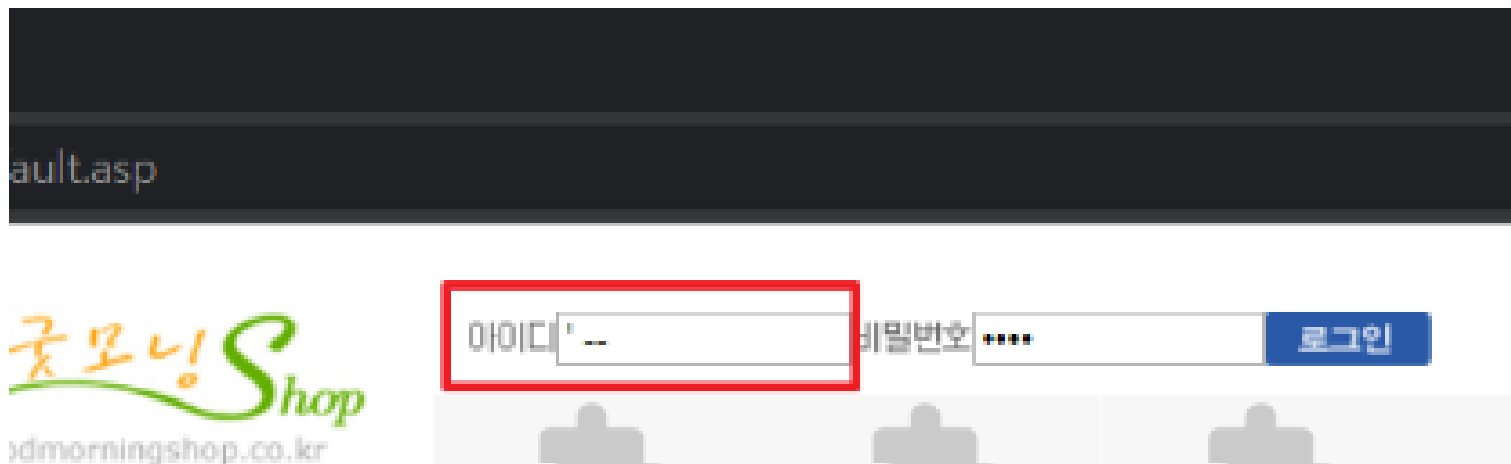


Burp Suite

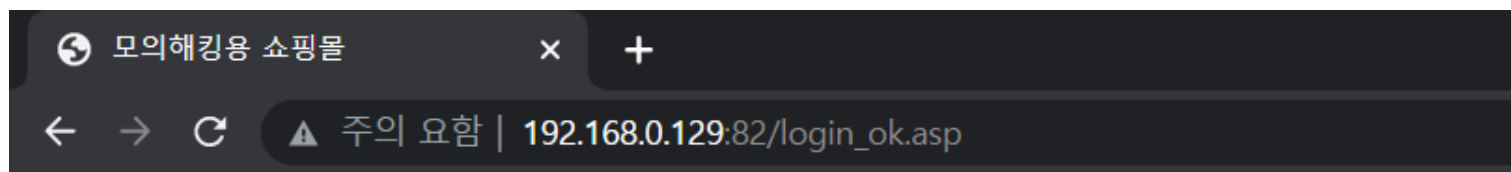
02



02



쿼리 에러를 유발시키는 '(작은 따옴표) 입력



[DB쿼리실패] SELECT * FROM GM_FREE_MEMBER WHERE (userid=' --') and (pwdcompare('1234', pwd)=1)

쿼리 에러 발생

02

SQL Injection 취약점 가이드

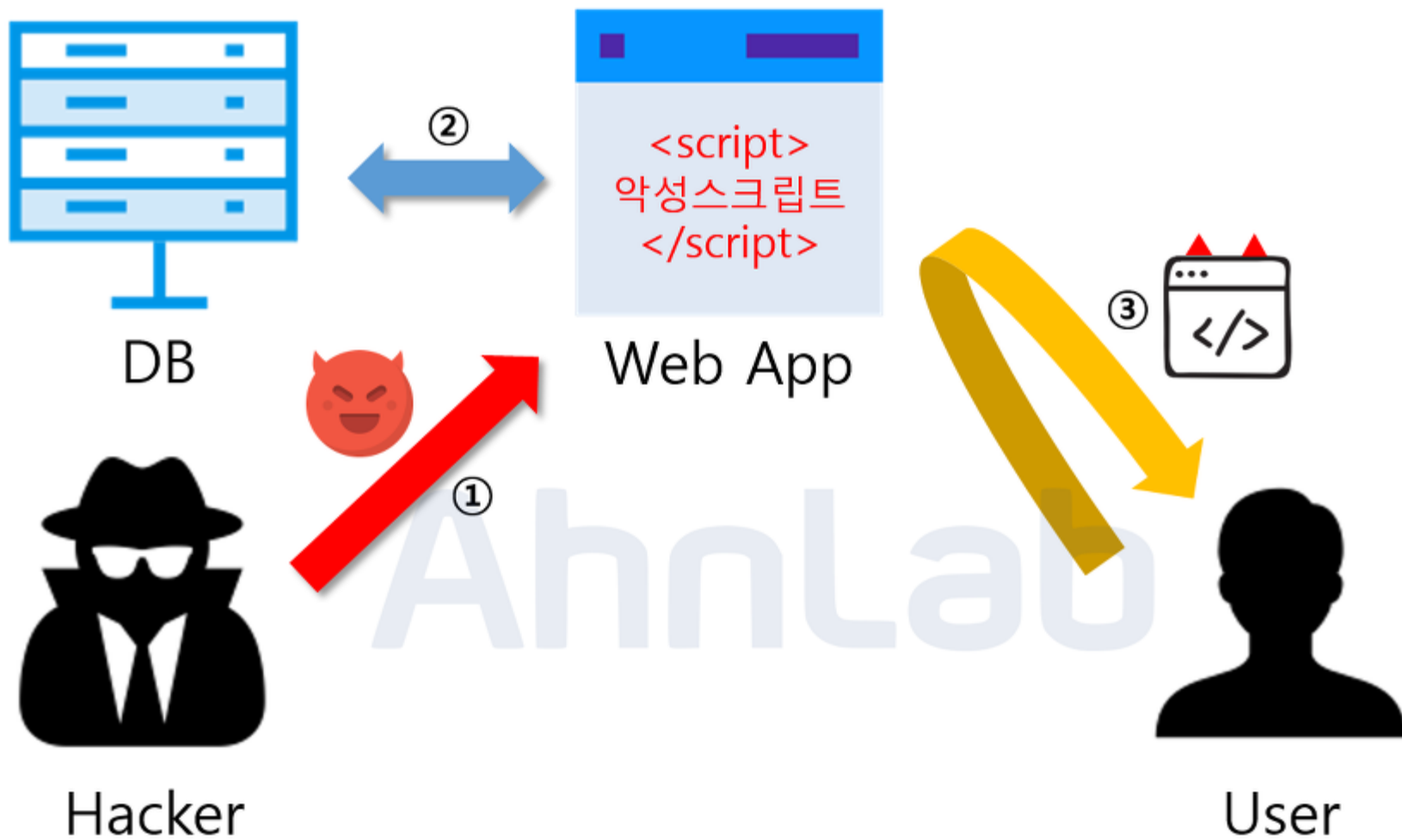
※ 취약점 발생 원인

- ☞ 사용자의 입력 값에 대한 필터링 부재

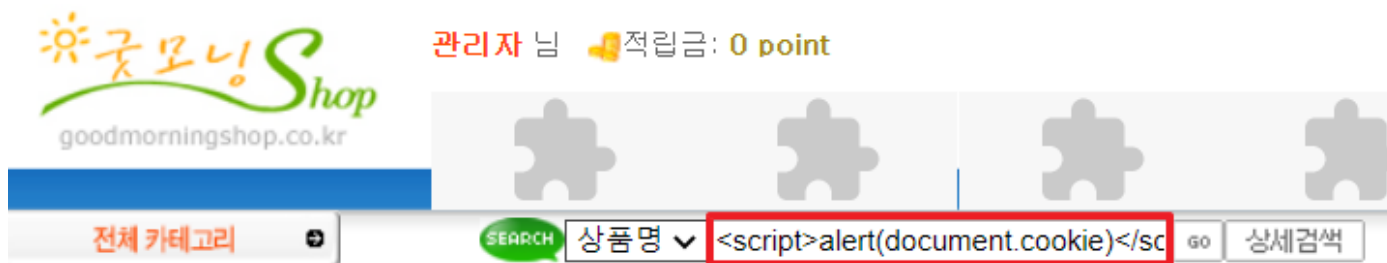
※ 조치 방법

- ☞ SQL 함수, 공백, 싱글 쿼터 등의 사용자 입력 값 필터링
- ☞ SQL 쿼리 검증 로직 추가

02



02



현재 브라우저의 쿠키 출력

02

크로스 사이트 스크립팅(XSS) 취약점 가이드

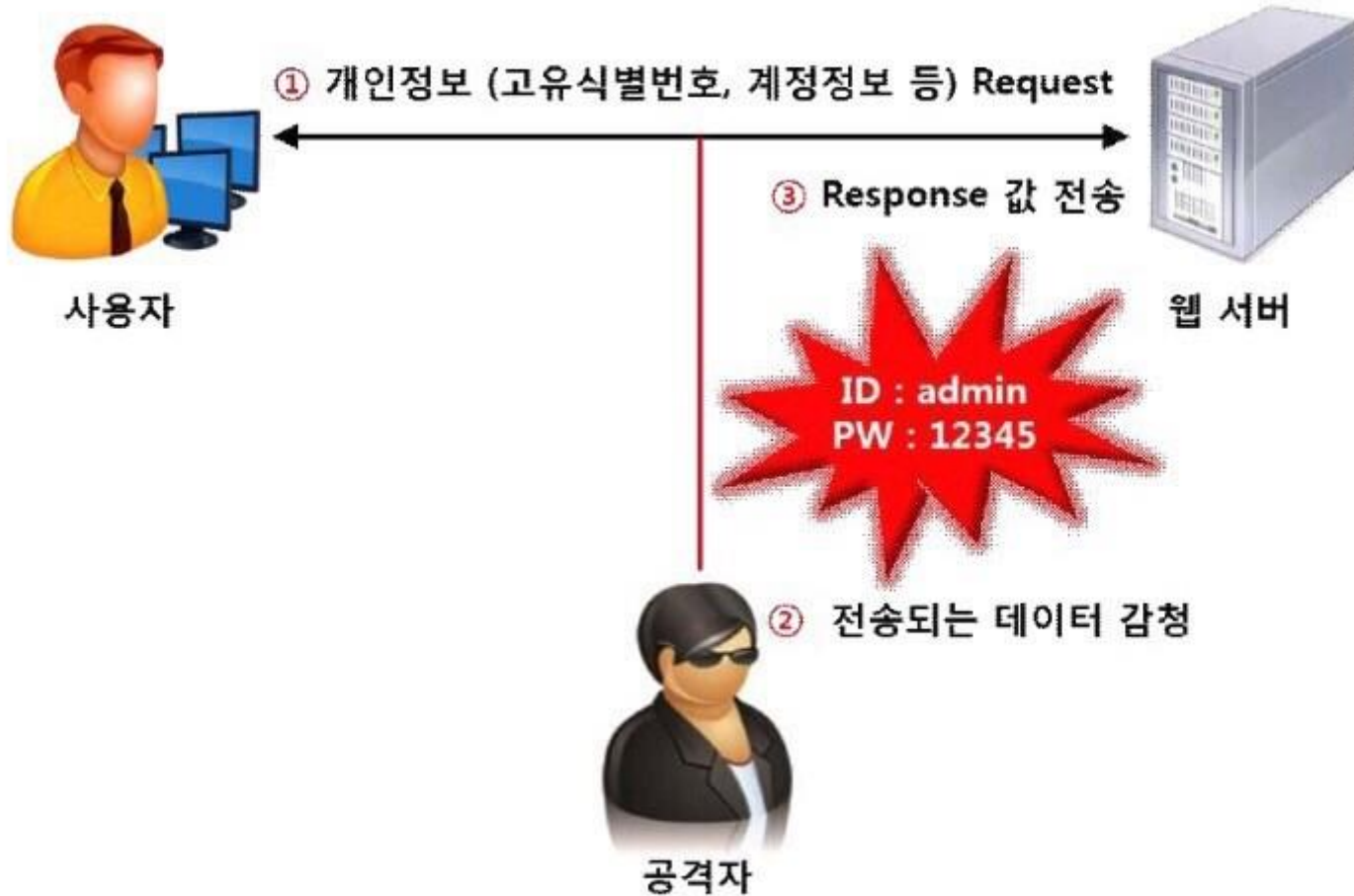
※ 취약점 발생 원인

- ☞ 사용자의 입력 값에 대한 필터링 부재

※ 조치 방법

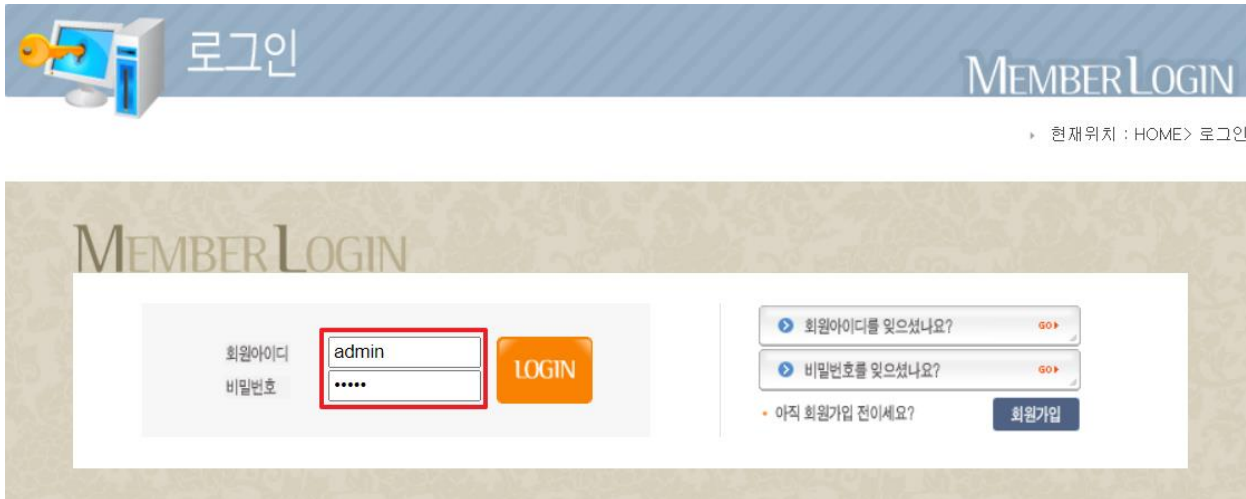
- ☞ 사용자 입력 값 필터링
- ☞ 문자열, 특수 기호 등을 치환하여 저장
- ☞ HTML 태그 화이트리스트 적용

02



[데이터 평문전송 동작 과정]

02



로그인

MEMBER LOGIN

현재위치 : HOME > 로그인

MEMBER LOGIN

회원아이디
비밀번호

admin

LOGIN

회원아이디를 잊으셨나요?

비밀번호를 잊으셨나요?

아직 회원가입 전이세요?

회원가입

02

*VMware Network Adapter VMnet8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
5	4.400169	192.168.0.1	192.168.0.129	HTTP	801	POST /login_ok.asp HTTP/1.1
6	4.492685	192.168.0.129	192.168.0.1	HTTP	502	HTTP/1.1 302 Object moved (1
7	4.496139	192.168.0.1	192.168.0.129	HTTP	621	GET /default.asp HTTP/1.1
8	4.631889	192.168.0.129	192.168.0.1	TCP	54	82 → 1452 [ACK] Seq=449 Ack=:
9	5.124269	192.168.0.129	192.168.0.1	TCP	1514	82 → 1452 [ACK] Seq=449 Ack=:
10	5.124397	192.168.0.129	192.168.0.1	TCP	1514	82 → 1452 [ACK] Seq=1909 Ack=:
11	5.124439	192.168.0.1	192.168.0.129	TCP	54	1452 → 82 [ACK] Seq=1315 Ack=:
12	5.124504	192.168.0.129	192.168.0.1	TCP	1514	82 → 1452 [ACK] Seq=3369 Ack=:
13	5.179279	192.168.0.1	192.168.0.129	TCP	54	1452 → 82 [ACK] Seq=1315 Ack=:
14	5.179553	192.168.0.129	192.168.0.1	TCP	1514	82 → 1452 [ACK] Seq=4829 Ack=:

> Frame 5: 801 bytes on wire (6408 bits), 801 bytes captured (6408 bits) on interface \Device\NPF_{66E67672}

> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_73:52:2f (00:0c:29:73:52:2f)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.129

> Transmission Control Protocol, Src Port: 1452, Dst Port: 82, Seq: 1, Ack: 1, Len: 747

> Hypertext Transfer Protocol

✓ HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "referer" = "http://192.168.0.129:82/default.asp"
- > Form item: "userid" = "admin"
- > Form item: "pwd" = "admin"

0000 00 0c 29 73 52 2f 00 50 56 c0 00 08 08 00 45 00 ...sR/.P V.....E.

0010 03 13 52 cb 40 00 80 06 23 47 c0 a8 00 01 c0 a8 ...R.@... #G.....

굿모닝 Shop 로그인 요청 패킷

02

데이터 평문 전송 취약점 가이드

※ 취약점 발생 원인

- ☞ 암호화 되지 않은 텍스트 기반으로 이루어지는 데이터 통신

※ 조치 방법

- ☞ 중요 정보들을 암호화(AES, RSA 등) 하여 전송
- ☞ HTTPS와 같은 암호화 통신 적용

02



※ 웹사이트에 **중요 정보**(개인정보, 계정정보, 금융정보 등) 이 노출

에러 발생 시 과도한 정보 노출

☞ 노출된 정보를 악용하여 **2차 공격**이 가능

02

OyesMall

one click easy shopping

[logout](#) | [my account](#) | [shopping cart](#) | [Q&A](#)

Red Zone

[men](#) | [women](#) | [kids&baby](#) | [home&office](#) | [electronics](#) | [books&media](#) | [leisure&sports](#) | [hobby](#) | [luxury](#)

Quick Search

Go

Advanced Search ▶

OyesMall Guide

- 주문안내
- 배송안내
- 요금안내
- 반품 및 보험안내
- OyesMall Map

About OyesMall

SALE

Now on sale !

Music

Board

Guest Note

Notice

My Account

home > my account > Apply for leaving OyesMall

회원정보관리

회원님의 정보는 아래와 같습니다.

(*)에 한해 잘못 기재하신 내용이나, 변경사항이 있을 때 언제든지 수정이 가능합니다.

회원님의 정보관리를 통해 Wizwid서비스를 더욱 편리하게 이용하세요.

사용자 ID	test
* 비밀번호 (비밀번호는 4~12자이내의 영문자나 숫자이어야 합니다.)
* 비밀번호 힌트	좋아하는 색깔은? ▼ 비밀번호 분실시 사용될 질문내용입니다.
* 답변	빨강 비밀번호 분실시 질문에 대한 답변입니다.
* 이름	테스터 실명을 입력하십시오.
주민등록번호	123123 - 1231234
생년월일	1912 년 01 월 23 일 <input checked="" type="radio"/> 양력 <input type="radio"/> 음력
* 결혼여부	<input checked="" type="radio"/> 미혼 <input type="radio"/> 기혼
* 주 소	[130-080] 서울 동대문구 이문동 우리집
* 전화번호	02 - 123 - 1234 <input checked="" type="radio"/> 직장 <input type="radio"/> 자택
휴대폰	- -
* 직 업	학생 ▼

회원 계정 관리 페이지에서 주민등록번호가 평문으로 노출

02

```

        <TD style="PADDING-LEFT: 6px" bgColor=#feffeb colSpan=3
            height=60 ><FONT class=C55>회원님의 정보는 아래와 같습니다. <BR><FONT
            class=C66>*</FONT></FONT>에 한해 잘못 기재하신 내용이나, 변경사항이 있을 때 언제든지 수정이 가능합니다.
            <BR>회원님의 정보관리를 통해 Wizwid서비스를 더욱 편리하게 이용하세요. </FONT></TD>
        </TR>

        <TR>
            <TD style="PADDING-LEFT: 6px" bgColor=#f3f2f2 >&nbsp;&nbsp;&nbsp;<FONT class=C55>사용자 ID</FONT></TD>
            <TD style="PADDING-LEFT: 4px" bgColor=white colSpan=2 height=25><INPUT maxLength=8 size=10 name=user_id value="test" type=text CLASS=txtfld read
        </tr>

        <tr >
            <TD style="PADDING-LEFT: 6px" bgColor=#f3f2f2><FONT class=C66>*</FONT>&nbsp;&nbsp;<FONT class=C55>비밀번호</FONT></TD>
            <TD style="PADDING-LEFT: 4px" bgColor=white colSpan=2>
                <INPUT maxLength=8 size=10 name=passwd value="admin123" type=password CLASS=txtfld><BR><FONT class=c3><FONT color=#47b3b7>(비밀번호는 4~12자 이내)
            </Tr>

        <TR height=25>
            <TD style="PADDING-LEFT: 6px" bgColor=#f3f2f2><FONT
                class=C66>*</FONT>&nbsp;&nbsp;<FONT class=C55>비밀번호 힌트</FONT></TD>
            <TD style="PADDING-LEFT: 4px" bgColor=white colSpan=2>
                <SELECT style="FONT-SIZE: 12px; WIDTH: 202px" name=passwd_q>
                    <OPTION >어머니의 성함은?</OPTION>
                    <OPTION >아버지의 성함은?</OPTION>
                    <OPTION >자신의 별명은?</OPTION>
                    <OPTION >기억에 남는 추억의 장소는?</OPTION>
                    <OPTION >가장 여행하고 싶은 나라는?</OPTION>
                    <OPTION >자신의 보물 제1호는?</OPTION>
                    <OPTION >가장 감명깊게 본 영화는?</OPTION>

```

회원 계정 관리 페이지에서는 마스킹 되어있던 **비밀번호**가 웹페이지 소스에 평문으로 노출

02

정보 누출 취약점 가이드

※ 취약점 발생 원인

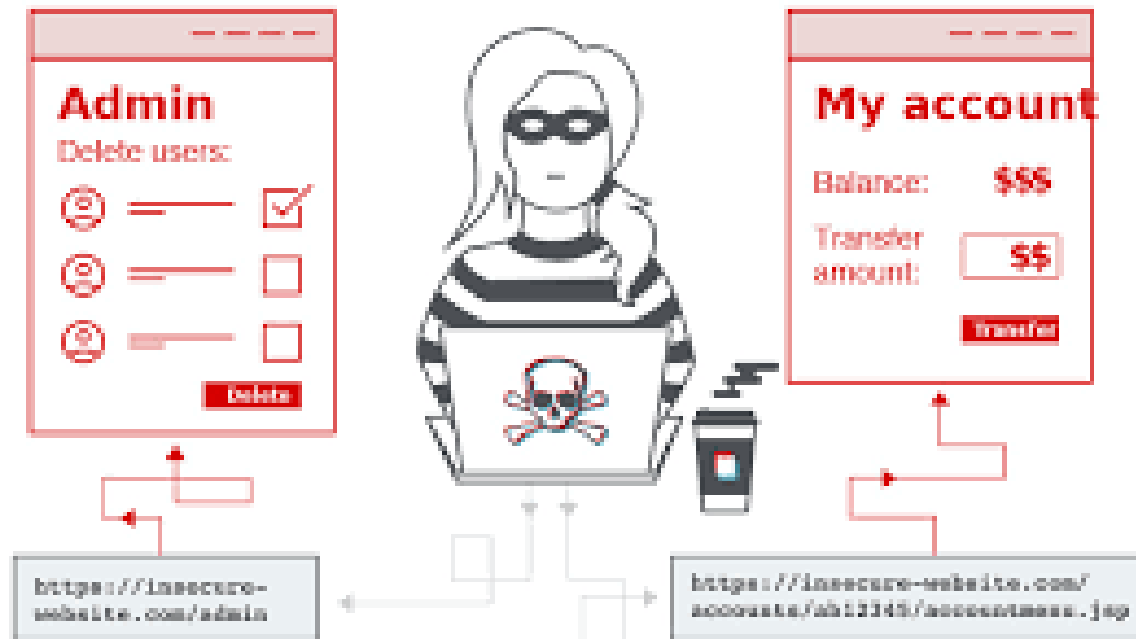
☞ 홈페이지 설계 구축 단계에서 개인정보 노출이나 보안 취약점을 고려하지 않아서 발생

※ 조치 방법

☞ 웹 사이트에 노출되는 중요정보는 마스킹 적용

☞ 발생 가능한 에러에 대해 최소한의 정보 또는 사전에 준비된 메시지만
출력

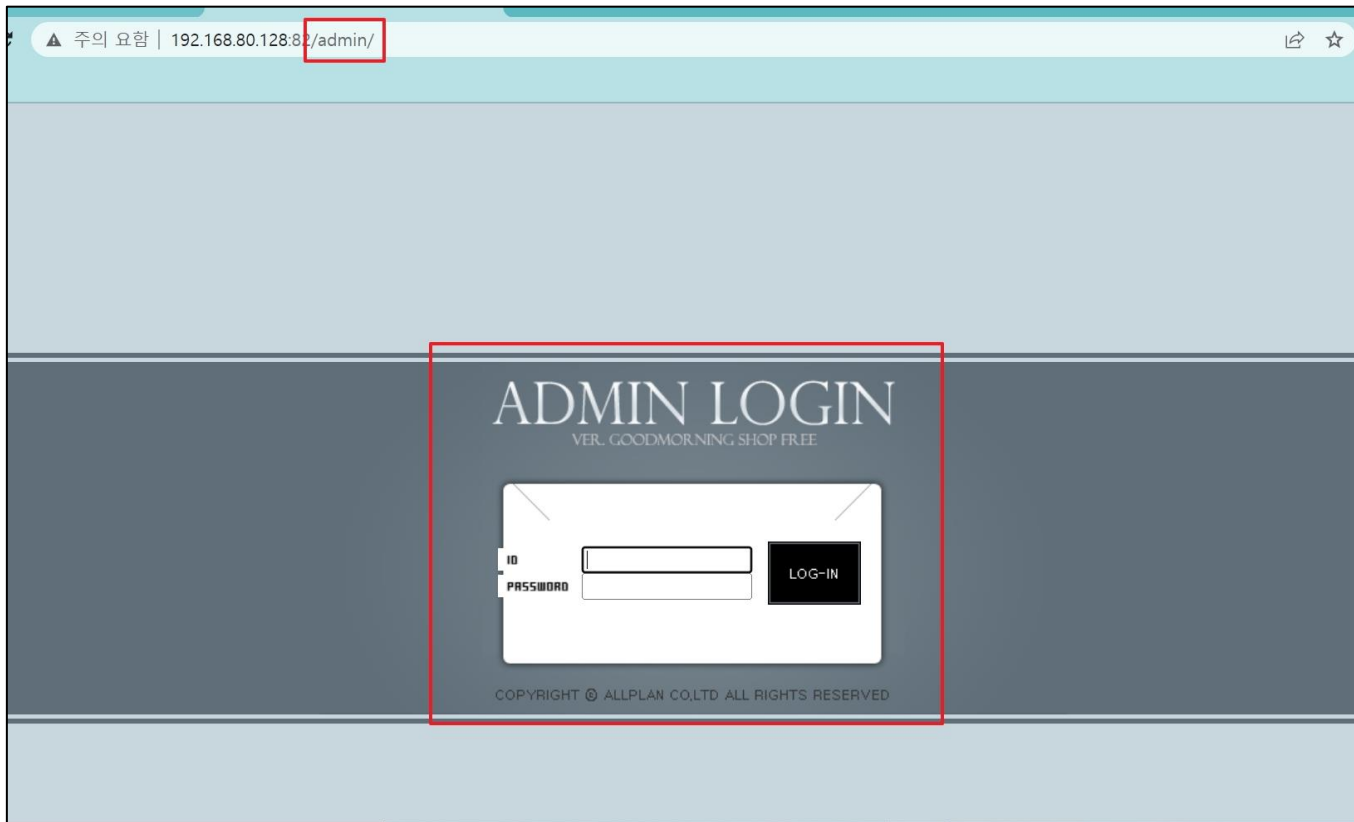
02



※ 관리자 페이지가 유추하기 쉬운 이름(/admin)

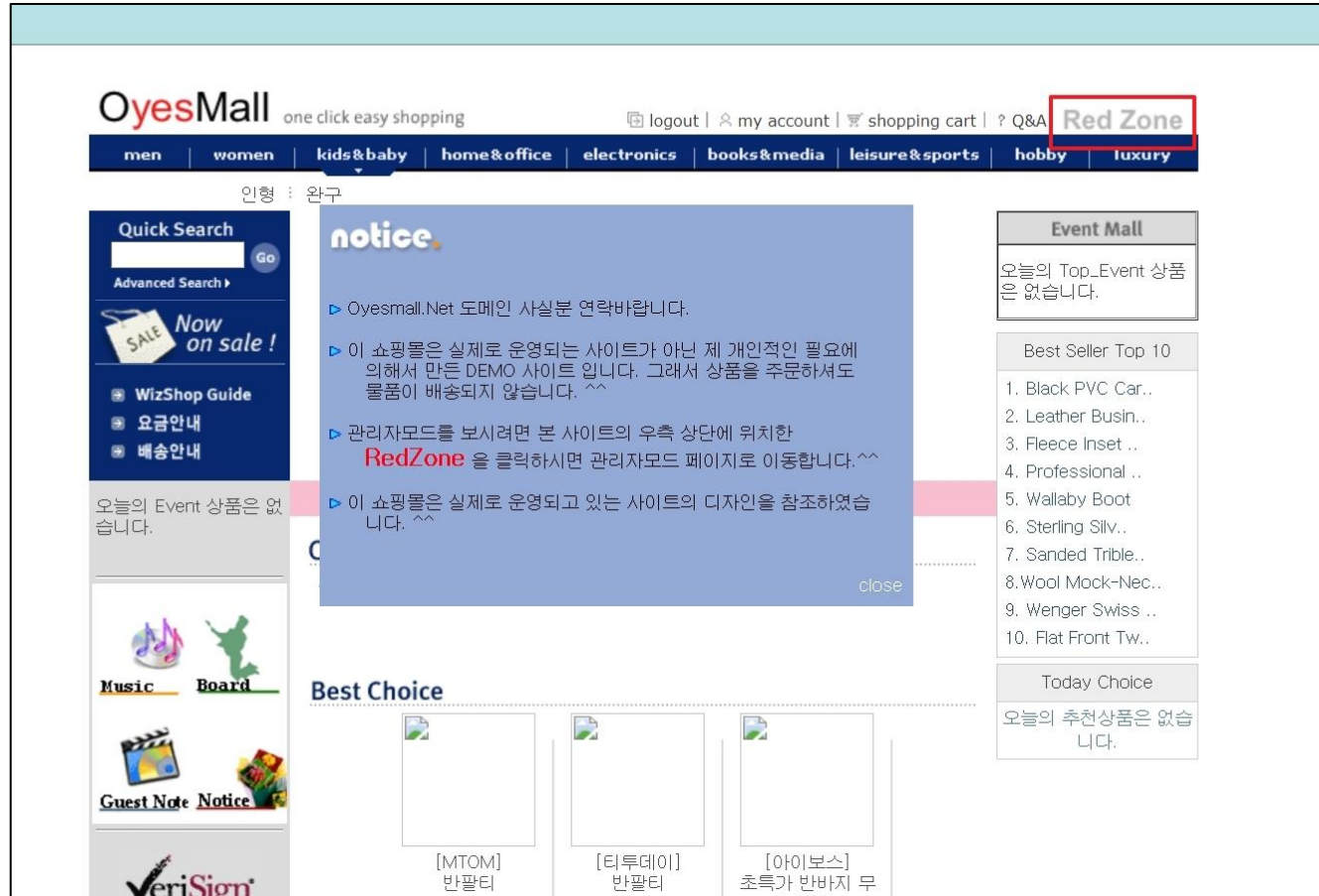
👉 웹 사이트의 **변조**, 웹 서버의 **권한 노출** 가능

02



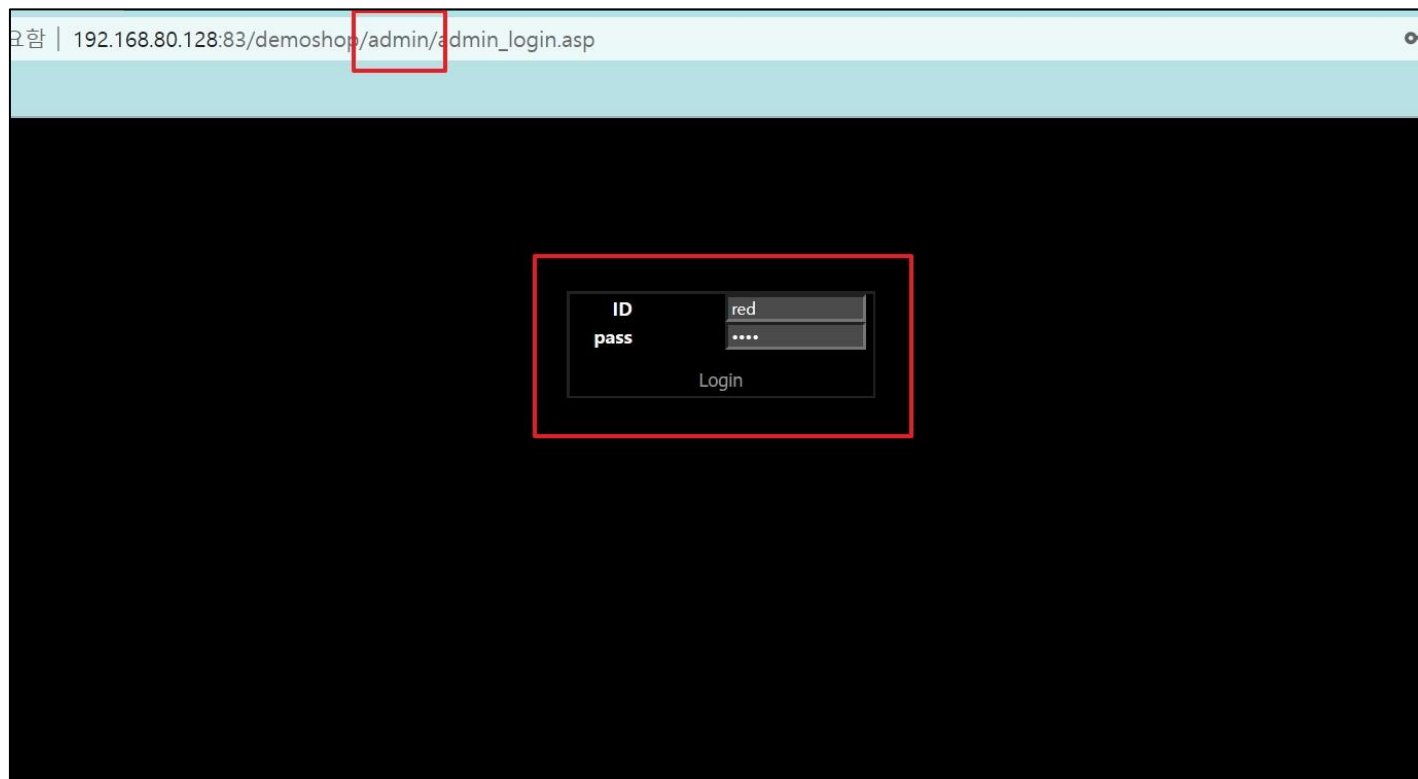
/admin 으로 접근을 시도했을 때 관리자 페이지 접근 가능

02



메인 페이지의 Red Zone 버튼을 통해 관리자 페이지 접근 가능

02



/admin으로 접근을 시도했을 때도 관리자 페이지 접근 가능

02

관리자 페이지 노출 취약점 가이드

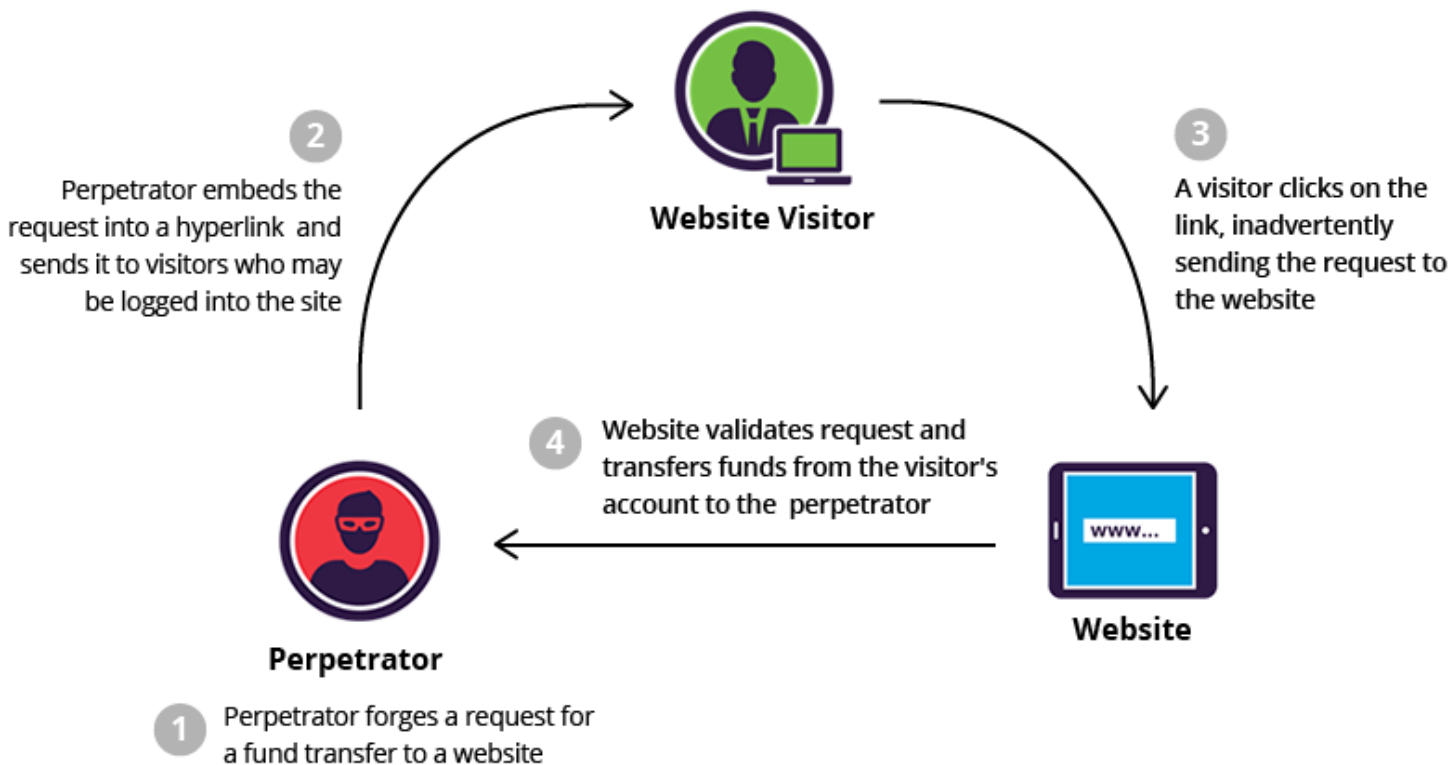
※ 취약점 발생 원인

- ☞ 관리자 페이지의 URL을 유추하기 쉬운 이름 사용

※ 조치 방법

- ☞ 유추하기 어려운 이름으로 변경
- ☞ 지정된 IP만 접근 할 수 있도록 제한
- ☞ 부득이한 경우 관리자 페이지 로그인 시 2차 인증 적용


02




※ 공격자가 사용자의 의지와 상관없이 강제로 행하도록 유도

☞ 악성 스크립트 실행 또는 게시물 임의 작성 등의 피해 발생 우려

02

 게시판6

 글수정하기

이름

| 관리자

이메일

| s@d.com

제 목

| ★필독★ 공지사항

비밀번호

| . <수정,삭제시 필요> ☐ 게시글 잠금 (본인과 관리자만 열람가능)

내용입력 형식

| ☐ TEXT ☒ HTML ☐ 웹에디터

```
<form name="bbsForm" method="post" action="board_write_ok.asp"
enctype="multipart/form-data">
<input class="box_s" type="hidden" name="boardIndex" value="5">
<input class="box_s" type="hidden" name="name" value="dummy">
<input class="box_s" type="hidden" name="pwd" value="1">
<input class="box_s" type="hidden" name="title" value="babo">
<input class="box_s" type="hidden" name="content" value="hahaha">
<input class="box_s" type="hidden" name="TextContent" value="hahaha111">
<input class="box_s" type="hidden" name="bHtml" value="1">
<input type="submit" value="버튼을 클릭해주세요">
</form>
```

저장

취소

목록

관리자를 사칭하여 공격자가 악성 스크립트 작성

02

게시판6

제목	★필독★ 공지사항		
날짜	2022-08-15 오후 11:41:55	조회수	5
글쓴이	관리자		

버튼을 클릭해주세요

이름

이름

비밀번호

삭제

MENT

등록

삭제

← 이전글

s

→ 다음글

babo

192.168.0.117:82 내용:

등록완료 하였습니다.

확인

공격자가 작성한 글을 다른 이용자가 열람

02

게시판6

제목	babo		
날짜	2022-08-16 오후 8:02:14	조회수	0
글쓴이	dummy		

hahaha111

이름	내용	날짜	삭제
----	----	----	----

이름

비밀번호

COMMENT
등록

비밀번호

목록

수정

답글

삭제

← 이전글

babo

악성 스크립트가 실행되어 게시글이 강제로 작성됨

02

CSRF 취약점 가이드

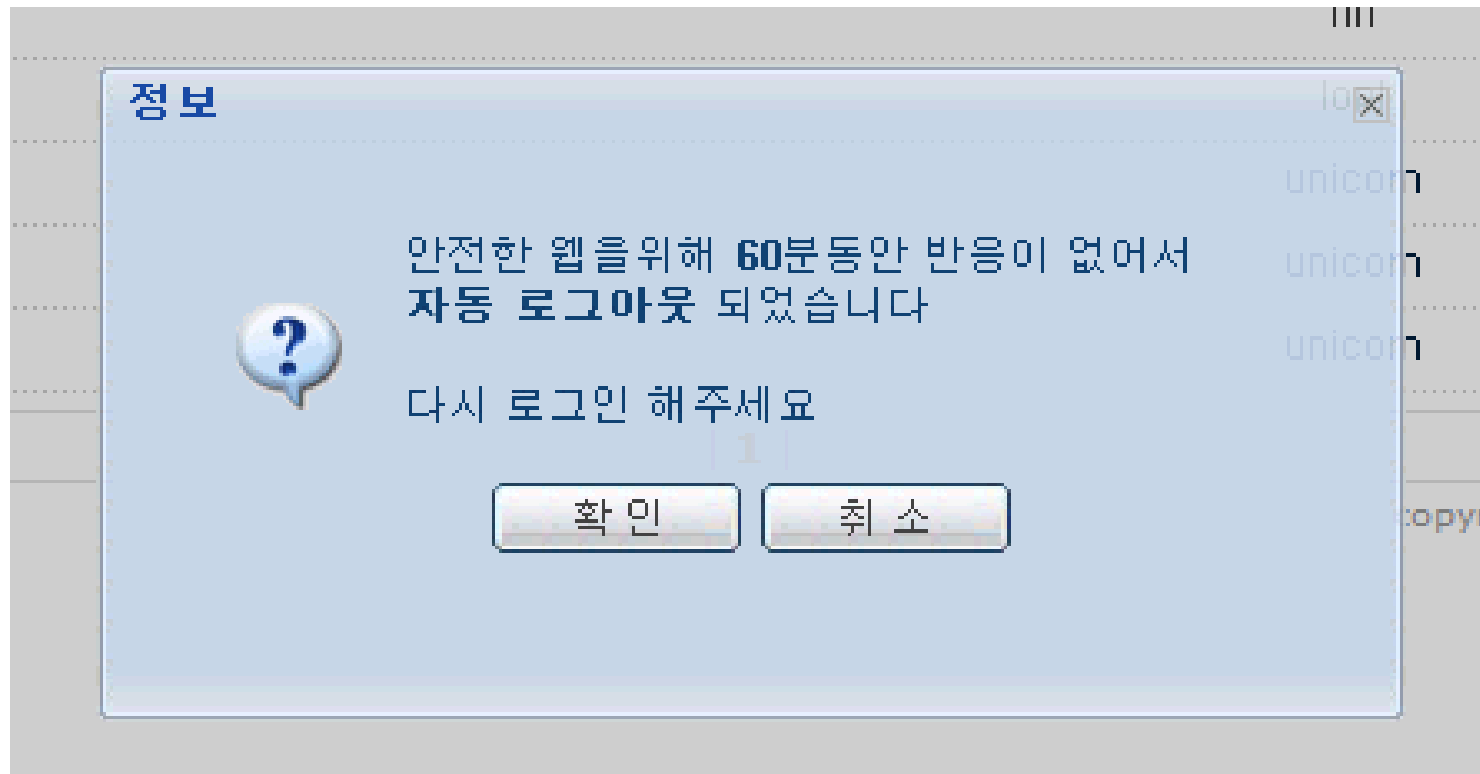
※ 취약점 발생 원인

- ☞ 특정 웹페이지에서 스크립트 작성을 허용했기 때문

※ 조치 방법

- ☞ CSRF 토큰사용
- ☞ 게시물 작성 시 필터링

02



※ 세션 만료 기간을 정하지 않거나 만료기한을 길게 설정한 경우

☞ 계정의 세션이 남아있는 경우, 공격자의 **세션 탈취** 가능성 ↑

The screenshot shows the Good Morning Shop website interface. At the top, there's a navigation bar with links like '로그아웃', '마이페이지', '장바구니', and '주문조회'. Below this, a banner for 'eTV Chance' is visible. The main content area features a large image of a house with the text '생활의 멋과 여유' and '다들 못에서 찾지 마세요 쇼핑 기회전에 다왔습니다'. Below the banner, there are several product categories and a 'LANCÔME PARIS' advertisement. On the right side, there's a calendar widget showing the date '오후 8:09:29' and '2022년 8월 16일 화요일'.

오후 8:09:29
2022년 8월 16일 화요일

2022년 8월

일	월	화	수	목	금	토
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

오늘

어디에 있어야 하는지를 보려면 일정을 설정하세요.

시작

일정 목록 설정 숨기기

웹 페이지에 접속 및 로그인 후 로그인 시간 기록

The screenshot displays the Good Morning Shop website interface. At the top, the header includes the site logo, user information (관리자님, 적립금: 0 point), and navigation links (로그아웃, 마이페이지, 장바구니, 주문조회). A session timeout warning is visible: "참가찾아오는길 즐겨찾기추가" and "로그아웃".

The main content area features a large banner for "생활의 멋과 여유" (The style and leisure of life) with a red star-themed illustration. Below the banner, there are several product categories and promotions:

- Category List:** 컴퓨터 주변기기, 가전 | 핸드폰, 가구 | 인테리어, 패션잡화 | 명품, 화장품 | 미용, 스포츠 | 레저.
- Product Promotions:**
 - 삼성 사이클로믹스 청소기 VC-BD916 (7000MP)
 - 사프 전자사전 7000MP
 - 삼성 레인지 RE-C23AN
 - 특! 별! 기! 획! 전! (Samsung SP-SPLS THEMAP series)
 - 올리브Stripe 레이어드 T (니븐스타일의 필수 아이템)
 - CLASSIC CANVAS (고무 밑창과 코튼 캔버스 스타일의 스니커즈)
 - VIVENNE WESTWOOD (브리지 부분이 밀어 있어 완벽한 캐즈 아이들 연출함)
- LANCÔME PARIS** banner.
- Community Section:** 커뮤니티, 운명처럼 알게 될문서장이 있으시거나 회원간의 정보공유 공간.

On the right side, a calendar overlay shows the date "오후 9:29:44" and "2022년 8월 16일 화요일". The calendar grid highlights the 16th. Below the calendar, there is a "시작" (Start) button and a link to "일정 목록 설정 숨기기".

일정 시간 후 로그인 세션 유지 확인

02

불충분한 세션만료 취약점 가이드

※ 취약점 발생 원인

- ☞ 로그인 세션을 제한 시간 없이 계속 유지하였음

※ 조치 방법

- ☞ 세션 종료 시간 설정
- ☞ 자동 로그아웃 기능 구현
- ☞ 타임아웃 구현

02



※ 중요정보 페이지에 대한 인증 절차가 불충분

☞ 권한 없는 사용자가 접근하여 정보 **유출** 또는 **변조** 가능

> 매종안내
 > 요금안내
 > 반품 및 보험안내
 > OyesMall Map

About OyesMall

SALE Now on sale !

Music Board

Guest Note Notice

(*)에 한해 잘못 기재하신 내용이나, 변경사항이 있을 때 언제든지 수정이 가능합니다.
 회원님의 정보관리를 통해 Wizwid서비스를 더욱 편리하게 이용하세요.

사용자 ID	test
* 비밀번호	***** (비밀번호는 4~12자 이내의 영문자나 숫자이어야 합니다.)
* 비밀번호 힌트	좋아하는 색깔은? ▼ 비밀번호 분실시 사용될 질문내용입니다.
* 답변	빨강 ▼ 비밀번호 분실시 질문에 대한 답변입니다.
* 이름	테스틱 실명을 입력하십시오.
주민등록번호	123123 - 1231234
생년월일	1912 년 01 월 23 일 <input checked="" type="radio"/> 양력 <input type="radio"/> 음력
* 결혼여부	<input checked="" type="radio"/> 미혼 <input type="radio"/> 기혼
* 주 소	[130-080] 서울 동대문구 이문동 우리집
* 전화번호	02 - 123 - 1234 <input checked="" type="radio"/> 직장 <input type="radio"/> 자택
휴대폰	- -
* 직 업	학생 ▼
* E-Mail	onesider@naver.com (예)redmaster@oyesmall.net...

정보변경

192.168.80.128:83 내용:
회원님의 정보가 수정되었습니다. ^^

about oyesmall | oyesmall guide | 개인정보 보호정책 | contact

(주)OyesMall 대표이사 RED MASTER
 사업자 등록번호 : red-1004 Tel: 011-9068-0010
 Copyright© 2002 OyesMall Korea Co. Ltd. All rights reserved.

확인

계정 정보 변경(비밀번호) 시 재인증 절차 없이 변경 가능

02

불충분한 인증 취약점 가이드

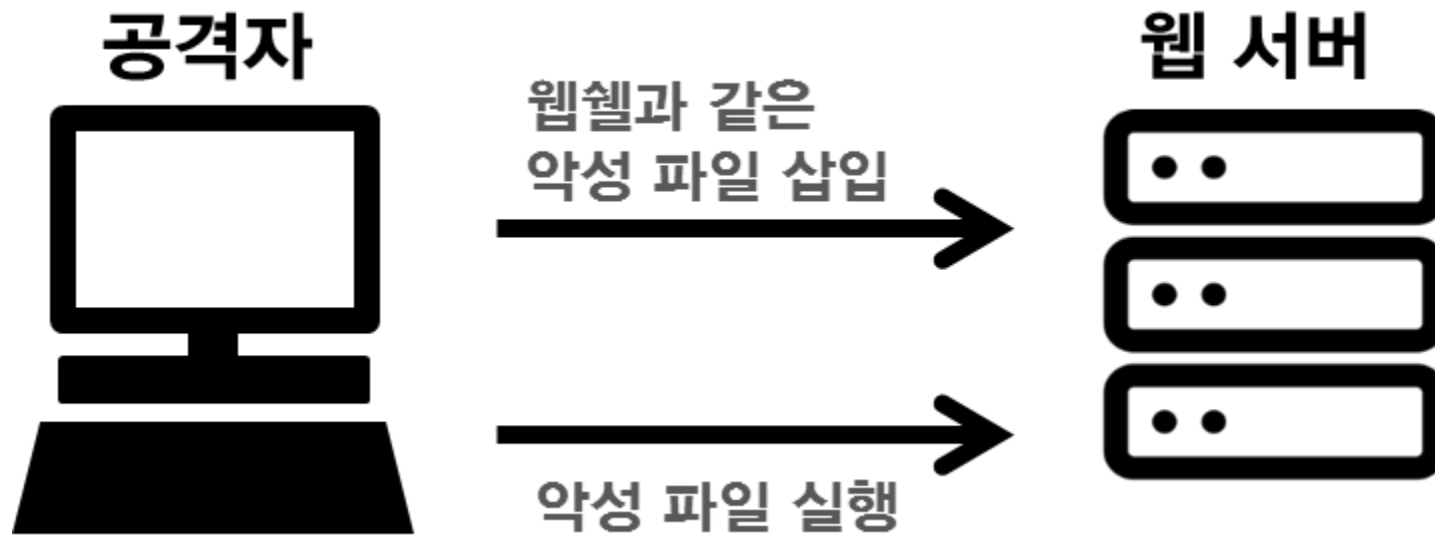
※ 취약점 발생 원인

☞ 중요정보 페이지에 대한 인증 불충분

※ 조치 방법

☞ 중요정보 페이지에 대한 추가 인증 로직 구현

02



※ 파일업로드 기능이 존재하는 웹사이트의 필터링이 미흡한 경우

☞ 공격자가 **악성파일** 업로드 하여 여러가지 문제를 일으킬 수 있음

02

자료실

글등록하기

이름

hacker

이메일

c@naer.com

제 목

check this file

파일첨부

파일 선택

itmu.asp

※ ASP, 스크립트 파일은 업로드할수 없습니다.

비밀번호

*

<수정,삭제시 필요>

☐ 게시물 잠금 (본인과 관리자만 열람가능)

내용입력 형식

☒ TEXT ☐ HTML ☐ 웹에디터

192.168.0.117:82 내용:

ASP, HTML 파일은 보안상 업로드할수 없습니다.



확인

저장

목록

특정 파일 확장자를 필터링 하는 기능이 있어 업로드 제한

02

 itmu.asp	2012-12-12 오후 5:37	ASP 파일	26KB
 itmu.jpg	2012-12-12 오후 5:37	JPG 파일	26KB

```

1 POST /board_write_ok.asp HTTP/1.1
2 Host: 192.168.0.117:82
3 Content-Length: 27228
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.0.117:82
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQrFpxDNSFhrhcXUy
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://192.168.0.117:82/board_write.asp?boardIndex=4
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: ASPSESSIONIDASC5RECC=LFNHHECBKJFCGPKGPMIMJOM; ASPSESSIONIDCSBSQACC=BOFNENCBPBKBDNIDJNCJIMHN; ASPSESSIONIDCSBPRACC=HOMFKADBMENOJIMDNEHHGEMK; ASPSESSIONIDCARBBTQD=DOILKLLBDKALMHEBNIDAIELAJ
14 Connection: close
15
16 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
17 Content-Disposition: form-data; name="boardIndex"
18
19 4
20 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
21 Content-Disposition: form-data; name="ref"
22
23
24 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
25 Content-Disposition: form-data; name="re_step"
26
27
28 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
29 Content-Disposition: form-data; name="re_level"
30
31
32 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
33 Content-Disposition: form-data; name="data"
34
35
36 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
37 Content-Disposition: form-data; name="name"
38
39 hacker
40 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
41 Content-Disposition: form-data; name="email"
42
43 c@naer.com
44 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
45 Content-Disposition: form-data; name="title"
46
47 check this file
48 -----WebKitFormBoundaryQrFpxDNSFhrhcXUy
49 Content-Disposition: form-data; name="up_file"; filename="itmu.asp"
50 Content-Type: image/jpeg

```

업로드 대상 스크립트파일 확장자 변경 및 요청 변조

📁

자료실

제목	check this file		
날짜	2022-08-16 오후 8:32:33	조회수	0
글쓴이	hacker		
첨부	<div>📎 itmu(1).asp</div>		

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

비밀번호

☰ 목록

✓ 수정

↩ 답글

✕ 삭제

← 이전글

1

공격자가 원하는 형식으로 파일이 업로드 됨

02

Commands are : **sql**, **upload**, **reverse**, **browser**

C:\web\web\gmsshop\upload\bbs

[UP]	..
[FILE] 2012-08-14 오후 5:38:12 23797	1.jpg
[FILE] 2022-08-16 오후 9:01:02 339	cmd.php
[FILE] 2022-08-16 오후 8:32:33 25795	itmu(1).asp
[FILE] 2022-08-16 오후 6:29:21 25795	itmu.asp
[FILE] 2022-08-16 오후 9:53:32 1028	monkey.asp
[FILE] 2012-08-14 오전 12:07:34 505	name20061106093357.GIF
[FILE] 2012-08-14 오전 12:07:34 402	name20061106093556.GIF
[FILE] 2012-08-14 오전 12:07:34 484	name20061106093710.GIF
[FILE] 2012-08-14 오전 12:07:34 526	name20061106093814.GIF
[FILE] 2012-08-14 오전 12:07:34 526	name20061106093905.GIF
[FILE] 2012-08-14 오전 12:07:34 526	name20061106094007.GIF
[FILE] 2012-08-14 오전 12:07:34 526	name20061106094058.GIF
[FILE] 2012-08-14 오전 12:07:34 526	name20061106094203.GIF
[FILE] 2012-08-14 오전 12:07:34 526	name20061106094229.GIF
[FILE] 2012-08-14 오전 12:07:34 526	name20061106094309.GIF
[FILE] 2012-08-14 오전 12:07:34 1894	name20061106094438.GIF
[FILE] 2022-08-16 오후 8:44:02 2015	new.asp
[FILE] 2022-08-16 오후 9:56:32 349	plz.php
[FILE] 2022-08-16 오후 9:26:11 1410	sss.asp
[FILE] 2022-08-16 오후 9:38:45 952	test(1).asp
[FILE] 2022-08-16 오후 9:38:45 952	test(2).asp
[FILE] 2022-08-16 오후 8:41:01 952	test.asp
[FILE] 2012-08-14 오전 12:07:34 32356	wmp54g_1.gif

웹 셸 실행화면

02

파일 업로드 취약점 가이드

※ 취약점 발생 원인

- ☞ 자료실 글쓰기 페이지의 확장자 필터링이 미흡하였다

※ 조치 방법

- ☞ 파일 확장자 필터링
- ☞ 실행 권한 제거
- ☞ 물리적인 위치 분리

03

향후 과제

03

※ 추가적인 공격 시도

☞ 다양한 공격 방법을 시도하여 추가적인 취약점 찾기

※ 코드 수정

☞ 시큐어 코딩 학습하여 문제 코드 수정

※ 자동화 코드

☞ 위의 과정을 자동화하는 코드 작성

Q & A

**THANK
YOU**