

웹 취약점 진단 결과보고서

2022.08

케이쉴드 주니어 8기

G-5조

정관우(팀장)

박태범

임혜원

목 차

| | | |
|-----|-------------------------|----|
| 1 | 개요 | 3 |
| 1.1 | 점검 목적 | 3 |
| 1.2 | 점검 일정 | 3 |
| 1.3 | 점검 인원 | 3 |
| 1.4 | 점검 대상 | 3 |
| 1.5 | 점검 툴 | 4 |
| 1.6 | 진단 항목 | 4 |
| 2 | 총평 | 5 |
| 2.1 | 전체적인 진단 결과 | 5 |
| 2.2 | 취약점 요약 | 5 |
| 3 | 상세 결과 | 7 |
| 3.1 | SQL Injection | 7 |
| 3.2 | XSS | 8 |
| 3.3 | 데이터 평문 전송 | 9 |
| 3.4 | 정보 누출 | 11 |
| 3.5 | 관리자 페이지 노출 | 13 |
| 3.6 | CSRF | 15 |
| 3.7 | 불충분한 세션만료 | 18 |
| 3.8 | 불충분한 인증 | 20 |
| 3.9 | 파일 업로드 | 22 |
| 4 | 조치 방법 | 25 |
| 4.1 | SQL Injection | 25 |
| 4.2 | 크로스 사이트 스크립팅(XSS) | 25 |
| 4.3 | 데이터 평문 전송 | 25 |
| 4.4 | 정보 누출 | 26 |
| 4.5 | 관리자 페이지 노출 | 26 |
| 4.6 | CSRF | 26 |
| 4.7 | 불충분한 세션만료 | 26 |
| 4.8 | 불충분한 인증 | 26 |
| 4.9 | 파일 업로드 | 27 |

1 개요

1.1 점검 목적

본 취약점 진단은 굿모닝 Shop과 오예스몰 서비스와 관련된 모든 정보 자산에 대해 취약점을 도출/분석하여 대책을 수립하기 위하여 진행되었다. 발견된 취약점에 대해서는 사전적인 예방을 통한 효과를 발생시키는데 목적이 있다.

1.2 점검 일정

| | |
|-------|-------------------------------|
| 정보수집 | 2022년 08월 01일 ~ 2022년 08월 04일 |
| 진단 | 2022년 08월 05일 ~ 2022년 08월 17일 |
| 보고서작성 | 2022년 08월 18일 ~ 2022년 08월 20일 |

1.3 점검 인원

| 점검자 | IP |
|-----|-----------------|
| 정관우 | 192.168.200.73 |
| 박태범 | 192.168.200.147 |
| 임혜원 | 192.168.190.152 |

1.4 점검 대상

| 점검 대상 | 굿모닝 Shop | 오예스몰 |
|-------|------------------|------------------|
| URL | www.localhost:82 | www.localhost:83 |
| IP | 192.168.106.128 | |

1.5 점검 툴

| | |
|-------------------|----------------------------------|
| Burp suite | 웹 어플리케이션 테스트와 취약점 점검에 주로 사용한다 |
| Wireshark | 네트워크 상에 오가는 패킷을 캡처해서 확인 할 때 사용한다 |
| Nmap | 호스트나 네트워크를 스캐닝 할 때 사용한다 |
| Dirbuster | 웹 서버 디렉터리, 파일을 스캔하는 프로그램이다 |

1.6 진단 항목

| 점검항목 | 항목중요도 | 항목코드 |
|----------------|-------|------|
| 버퍼 오버플로우 | 상 | BO |
| 포맷 스트링 | 상 | FS |
| LDAP 인젝션 | 상 | LI |
| 운영체제 명령 실행 | 상 | OC |
| SQL 인젝션 | 상 | SI |
| SSI 인젝션 | 상 | SS |
| XPath 인젝션 | 상 | XI |
| 디렉터리 인덱싱 | 상 | DI |
| 정보 누출 | 상 | IL |
| 악성 콘텐츠 | 상 | CS |
| 크로스사이트 스크립팅 | 상 | XS |
| 약한 문자열 강도 | 상 | BF |
| 불충분한 인증 | 상 | IA |
| 취약한 패스워드 복구 | 상 | PR |
| 크로스사이트 리퀘스트 변조 | 상 | CF |
| 세션 예측 | 상 | SE |
| 불충분한 인가 | 상 | IN |
| 불충분한 세션 만료 | 상 | SC |
| 세션 고정 | 상 | SF |
| 자동화 공격 | 상 | AU |
| 프로세스 검증 누락 | 상 | PV |
| 파일 업로드 | 상 | FU |
| 파일 다운로드 | 상 | FD |
| 관리자 페이지 노출 | 상 | AE |
| 경로 추적 | 상 | PT |
| 위치 공개 | 상 | PL |
| 데이터 평문 전송 | 상 | SN |
| 쿠키 변조 | 상 | CC |

2 총평

2.1 전체적인 진단 결과

전체 9개의 취약점이 발견되었으며, 주요 취약점은 아래와 같다.

SQL Injection 의 경우 굿모닝 Shop 로그인 페이지에서 SQL 쿼리 입력이 가능하여 데이터베이스를 비정상적으로 조작하는 것이 가능했다.

크로스 사이트 스크립팅의 경우 굿모닝 Shop 검색창에서 스크립트 입력이 가능하여 스크립트 입력이 가능하여 공격자가 악의적인 스크립트를 작성하는 것이 가능했다.

데이터 평문 전송의 경우 굿모닝 Shop 로그인 요청 시 데이터가 평문으로 전송되어 공격자가 패킷을 가로챘을 경우 ID와 비밀번호 유출이 가능했다.

정보 누출의 경우 오예스몰 계정 관리 페이지에서 사용자의 중요 정보인 주민등록번호가 평문으로 노출되고 있었고 마스킹 되어있던 비밀번호가 웹 페이지 소스에 평문으로 노출되고 있었다.

관리자 페이지 노출의 경우 굿모닝 Shop은 추측하기 쉬운 관리자 페이지 경로를 통해 관리자 페이지가 노출되었고 오예스몰은 추측하기 쉬운 관리자 페이지 경로 사용과 더불어 메인 페이지의 Red Zone을 통해 관리자 페이지가 노출되었다.

CSRF의 경우 굿모닝 Shop 자유게시판 글쓰기에서 스크립트 입력이 가능하여 공격자가 악의적인 스크립트를 작성하는 것이 가능했다.

불충분한 세션만료의 경우 굿모닝 Shop의 메인화면에서 로그인을 한 후 일정시간이 지나도 세션이 만료되지 않는 것을 확인하였다.

불충분한 인증의 경우 오예스몰 회원정보관리 페이지에서 추가 인증 없이 중요정보(비밀번호)가 바뀌는 것을 확인하였다.

파일 업로드의 경우 굿모닝 Shop의 자료실에서 Burp suite 툴을 통해 업로드 하지 못하는 asp 파일을 업로드하여 웹 쉘을 실행시키는 것이 가능했다.

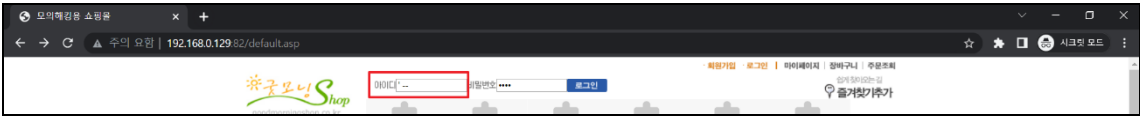
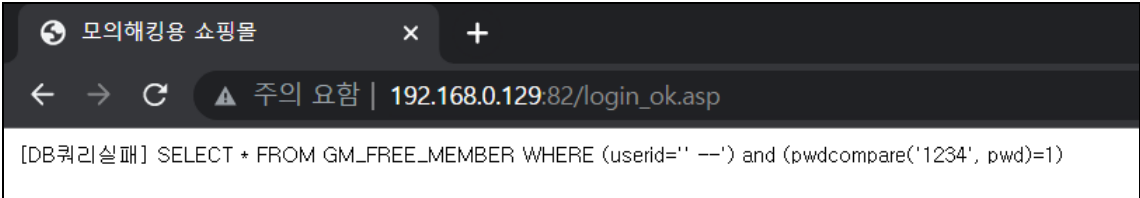
2.2 취약점 요약

| 점검항목 | 항목중요도 | 항목코드 | 발견 |
|------------|-------|------|----|
| 버퍼 오버플로우 | 상 | BO | |
| 포맷 스트링 | 상 | FS | |
| LDAP 인젝션 | 상 | LI | |
| 운영체제 명령 실행 | 상 | OC | |
| SQL 인젝션 | 상 | SI | O |
| SSI 인젝션 | 상 | SS | |
| XPath 인젝션 | 상 | XI | |
| 디렉터리 인덱싱 | 상 | DI | |
| 정보 누출 | 상 | IL | O |
| 악성 콘텐츠 | 상 | CS | |

| | | | |
|-------------------|---|----|---|
| 크로스사이트 스크립팅 | 상 | XS | O |
| 약한 문자열 강도 | 상 | BF | |
| 불충분한 인증 | 상 | IA | O |
| 취약한 패스워드 복구 | 상 | PR | |
| 크로스사이트 리퀘스트 변조 | 상 | CF | |
| 세션 예측 | 상 | SE | |
| 불충분한 인가 | 상 | IN | |
| 불충분한 세션 만료 | 상 | SC | O |
| 세션 고정 | 상 | SF | |
| 자동화 공격 | 상 | AU | |
| 프로세스 검증 누락 | 상 | PV | |
| 파일 업로드 | 상 | FU | O |
| 파일 다운로드 | 상 | FD | |
| 관리자 페이지 노출 | 상 | AE | O |
| 경로 추적 | 상 | PT | |
| 위치 공개 | 상 | PL | |
| 데이터 평문 전송 | 상 | SN | O |
| 쿠키 변조 | 상 | CC | |

3 상세 결과

3.1 SQL Injection

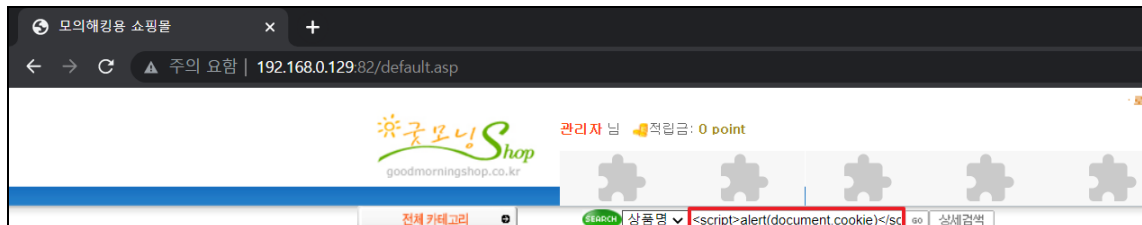
| | |
|---|--|
| 취약점 명 | SQL Injection |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 굿모닝 Shop 로그인 요청 시 작은 따옴표(')나 SQL 쿼리에 대한 필터링이 되어있지 않아 공격자의 의도대로 쿼리문을 실행하거나 발생하는 에러를 통해 데이터베이스에 대한 정보를 파악할 수 있다. |
| 발견 URL, 메뉴명 | ※ http://192.168.0.117:82/login_ok.asp (아이디, 비밀번호 입력 메뉴) |
| 취약점 재현 | |
| <p>1. 로그인 페이지에서 아이디에 작은 따옴표(')와 주석 표시를 의미하는 --를 입력한 뒤 로그인을 시도하였다.</p>  <p>[그림 1-1] 굿모닝 Shop SQL 인젝션 시도</p> <p>2. DB쿼리 오류를 확인할 수 있다.</p>  <p>[그림 1-2] 굿모닝 Shop SQL 인젝션 결과</p> | |

3.2 XSS

| | |
|-------------|---|
| 취약점 명 | XSS(Cross Site Scripting) |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 굿모닝 Shop의 검색창을 통해 스크립트 구문 실행이 가능하여 사용자의 개인정보 및 쿠키정보 탈취, 악성코드 감염, 웹 페이지 변조와 같은 공격이 가능하다. |
| 발견 URL, 메뉴명 | ※ http://192.168.0.117:82/search_result.asp?search=name&searchstring= (검색) ※ http:// 192.168.0.117:82/board_write.asp?boardIndex=5 (글쓰기) |

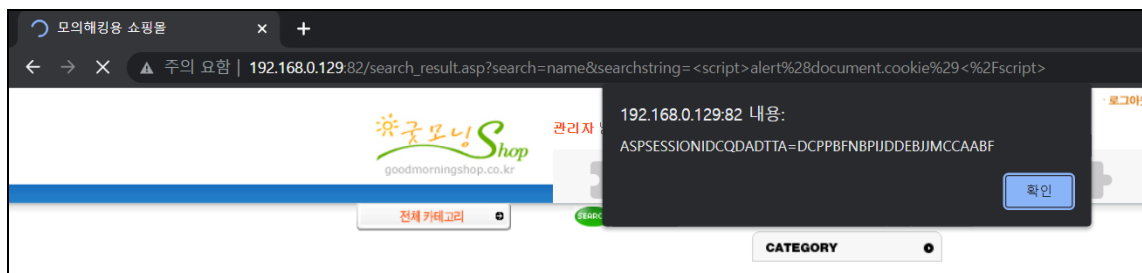
취약점 재현

1. 상품 검색 창에 쿠키를 출력하는 `<script>alert(document.cookie)</script>` 스크립트 구문을 작성한 뒤 검색을 시도하였다.




[그림 2-1] 굿모닝 Shop 스크립트 실행 시도

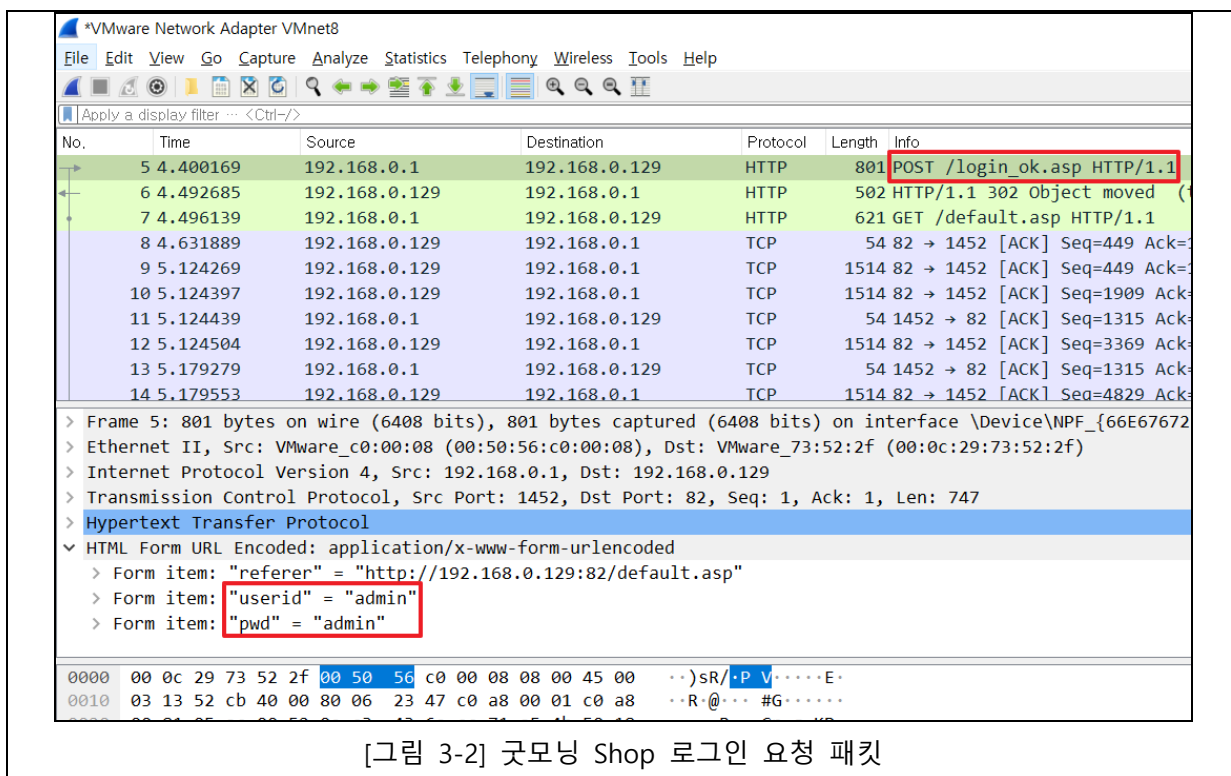
2. 스크립트가 실행되어 현재 브라우저의 쿠키가 출력되고 있다.



[그림 2-2] 굿모닝 Shop 스크립트 실행 결과

3.3 데이터 평문 전송

| | |
|--|---|
| 취약점 명 | 데이터 평문 전송 |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 굿모닝 Shop의 로그인 페이지는 암호화 되지 않은 평문으로 데이터 통신이 이루어지고 있기 때문에 공격자가 도청을 통해 계정 정보와 같은 민감한 데이터를 쉽게 획득 할 수 있다. |
| 발견 URL, 메뉴명 | ※ http://192.168.0.117:82/login.asp (ID, PW 입력창) |
| 취약점 재현 | |
| <p>1. 와이어샤크를 실행한 뒤 로그인 페이지에서 아이디와 암호를 입력 후 로그인을 시도하였다.</p>  <p>[그림 3-1] 굿모닝 Shop 로그인</p> <p>2. 와이어샤크에서 다음과 같은 HTTP 요청이 이루어진 것을 확인할 수 있다. 자세히 살펴보면 userid와 pwd를 암호화 없이 평문으로 전송하고 있는 것을 볼 수 있다.</p> | |



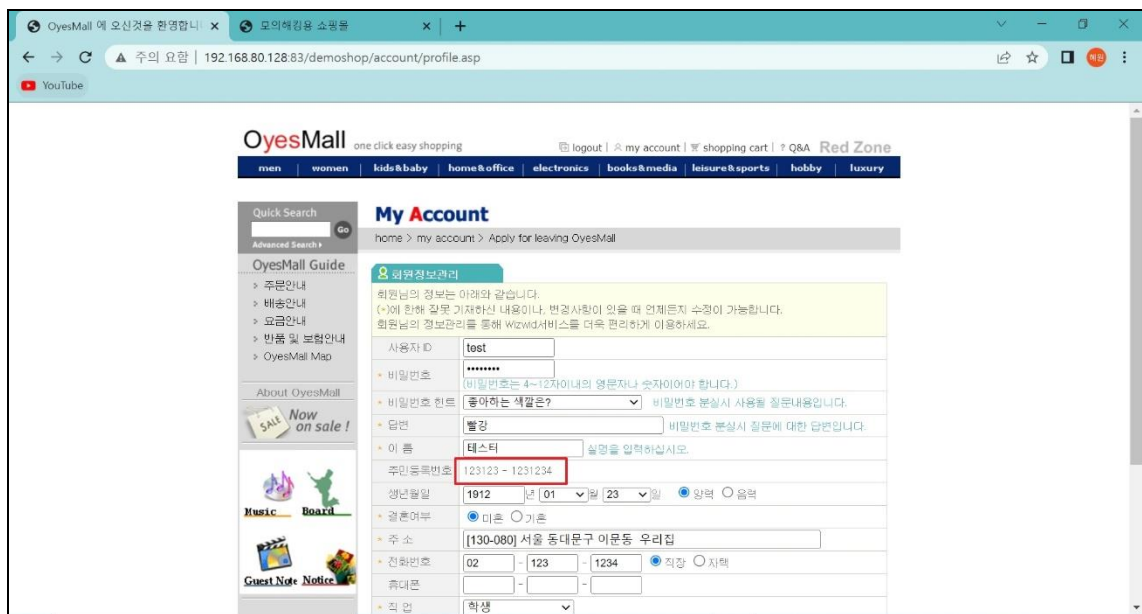
[그림 3-2] 굿모닝 Shop 로그인 요청 패킷

3.4 정보 누출

| | |
|-------------|--|
| 취약점 명 | 정보 누출 |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 오예스몰의 계정관리 페이지에서 중요정보인 주민등록번호를 평문으로 노출되고 있으며, 마스킹 된 비밀번호 또한 웹페이지 소스를 통해 평문으로 노출되어 공격자의 2차 공격에 취약하다. |
| 발견 URL, 메뉴명 | ※ http://192.168.0.117:82/order_table.asp (결제 페이지) ※ http://192.168.0.117:82/mypage_member.asp (회원정보수정 페이지) ※ http://192.168.0.117:82/login_ok.asp (로그인 페이지) |

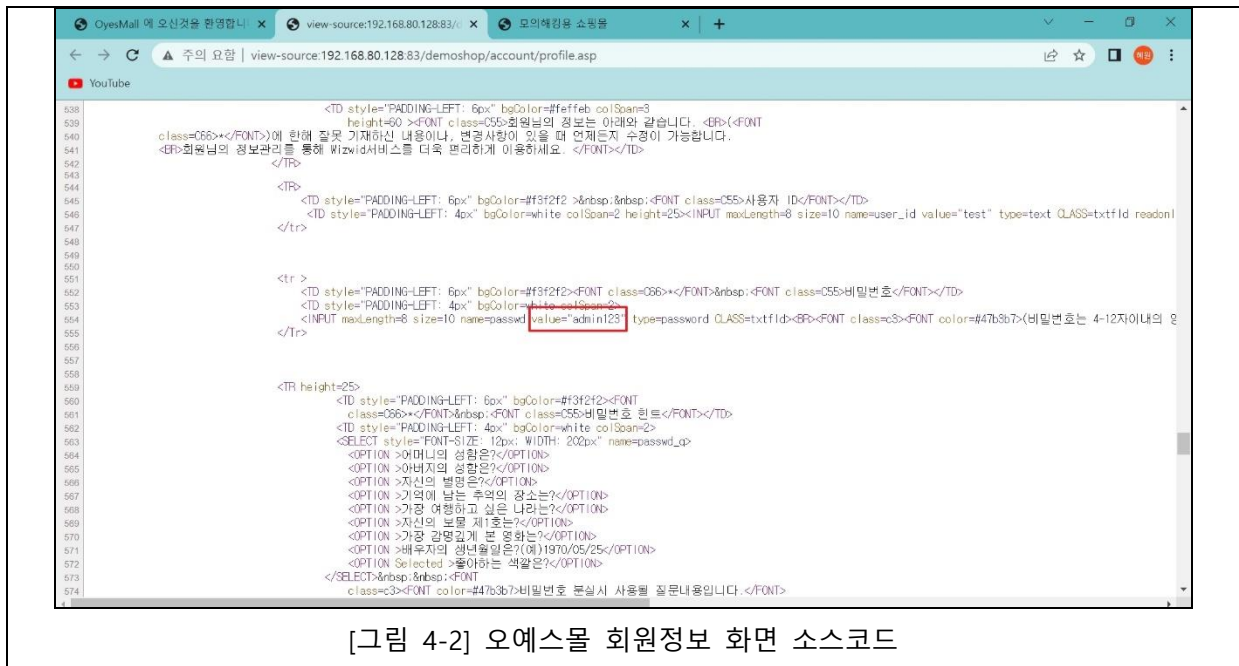
취약점 재현

1. 웹 사이트에 중요정보(주민등록번호)가 평문으로 노출되고 있다.



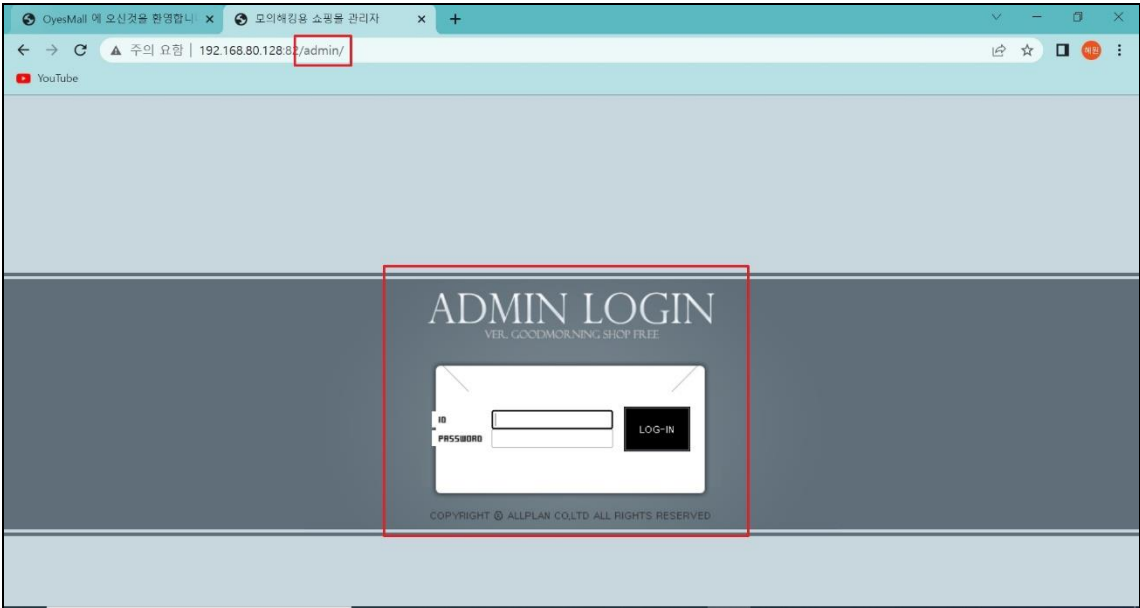
[그림 4-1] 오예스몰 회원정보 화면

2. 웹페이지에 마스킹 된 중요정보(비밀번호)가 웹페이지 소스에 평문으로 노출되고 있다.



[그림 4-2] 오예스몰 회원정보 화면 소스코드

3.5 관리자 페이지 노출

| | |
|---|---|
| 취약점 명 | 관리자 페이지 노출 |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 굿모닝 Shop과 오예스몰 모두 추측하기 쉬운 관리자 페이지 경로(/admin)를 사용하고 있어 관리자 페이지로의 접근이 가능했다. 오예스몰은 메인 페이지를 통해서도 쉽게 관리자 페이지로 접근이 가능하다. 공격자는 관리자 페이지를 이용하여 웹 사이트 변조 등을 할 수 있다. |
| 발견 URL, 메뉴명 | ※ http://192.168.0.117:82/admin/ (관리자 페이지) |
| 취약점 재현 | |
| <p>1. 추측하기 쉬운 관리자 페이지 경로 (/admin) 으로 접근을 시도 했을 때 관리자 페이지 접근이 가능했다.</p>  <p>[그림 6-1] 굿모닝 Shop 관리자 페이지</p> | |
| <p>2. 오예스몰 메인 페이지의 Red Zone 버튼을 통해 관리자 페이지에 쉽게 접근할 수 있으며 추측하기 쉬운 관리자 페이지 경로 (/admin) 를 사용하고 있다.</p> | |

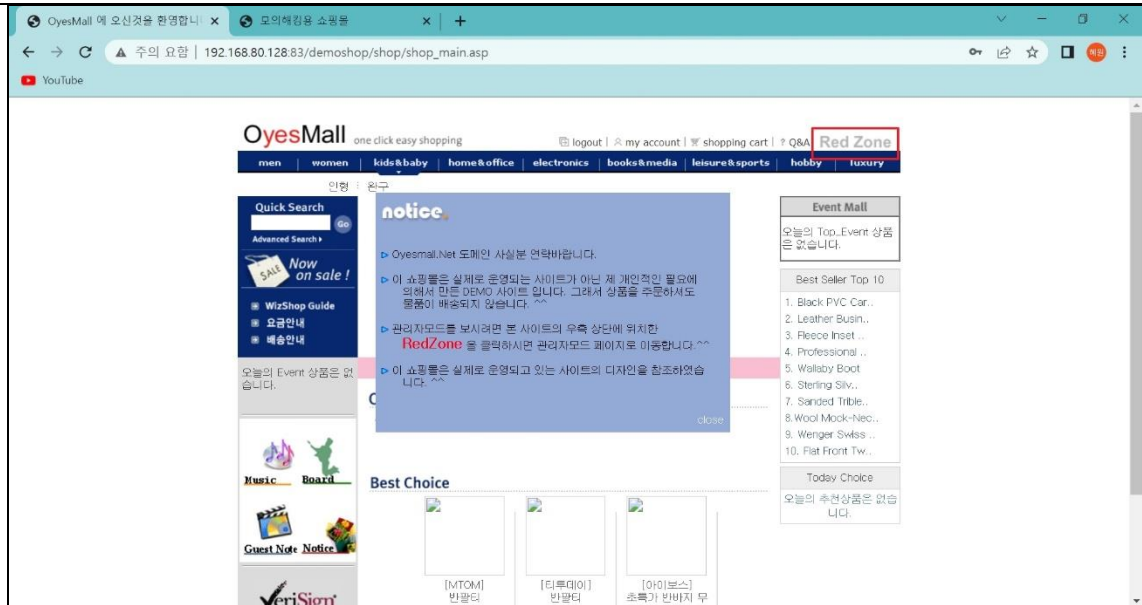
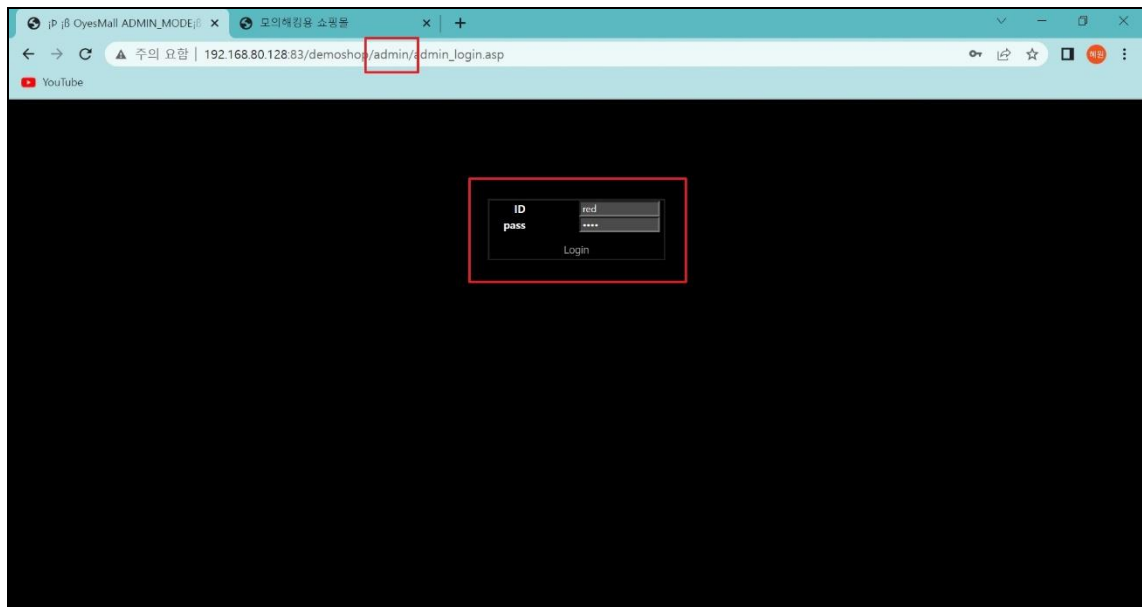


그림 [6-2] 오에스몰 메인화면



3.6 CSRF

| | |
|-------------|--|
| 취약점 명 | CSRF(Cross Site Request Forgery) |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 굿모닝Shop 웹 페이지에서는 글쓰기게시판에 html 스크립트를 작성할 수 있게 하여 공격자가 스크립트를 작성할 수 있게 되었다. 사용자가 공격자가 작성한 글을 열람했을 때 악성스크립트가 실행되어 공격자의 의도대로 게시글이 사용자의 의지와 상관없이 작성될 수 있다. |
| 발견 URL, 메뉴명 | ※ http://192.168.0.117:82/board_list.asp?boardIndex=5 (자유게시판) |

취약점 재현

1. 자유게시판 글쓰기 페이지에서 글을 작성해 보았다. 관리자가 작성한 것처럼 작성자와 제목을 작성했고, 버튼을 눌렀을 때 글이 강제로 작성되게 하는 스크립트를 작성했다.

게시판6

글수정하기

이름 | 관리자

이메일 | s@d.com

제 목 | ★필독★ 공지사항

비밀번호 | . <수정,삭제시 필요> ☐ 게시를 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

[그림 7-1] 굿모닝 Shop 게시판 스크립트 작성

2. 작성한 글에 들어가면 아래와 같이 버튼이 활성화 되어 있다.

게시판6

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

버튼을 클릭해주세요

| | | | |
|----|----|----|----|
| 이름 | 내용 | 날짜 | 삭제 |
|----|----|----|----|

이름

비밀번호

COMMENT

등록

비밀번호

목록

수정

답글

삭제

← 이전글

s

→ 다음글

babo

[그림 7-2] 스크립트가 적용된 게시글

- 임의의 사용자가 해당 게시물을 들어가서 버튼을 클릭하게 되면 글 작성이 완료되었을 때 나타나는 메시지가 출력된다.

192.168.0.117:82 내용:

등록완료 하였습니다.

확인

[그림 7-3] 게시글 버튼 클릭 응답 메시지

- 게시판 목록을 확인해보면 위에서 공격자가 작성한 내용대로 게시글이 생성된 것을 확인할 수 있다.

자유게시판

회원분들이 자유롭게 글을 올리실 수 있는 게시판입니다.

질문과답변

사진컨텐츠

자료실

이미지갤러리

Guest Board

게시판6

전체 [7]개

| 번호 | 제목 | 글쓴이 | 날짜 | 조회수 |
|----|----------------------------|-------|------------|-----|
| 7 | babo NEW | dummy | 2022-08-16 | 0 |
| 6 | babo NEW | dummy | 2022-08-16 | 0 |
| 5 | 1 NEW | d | 2022-08-16 | 0 |
| 4 | babo NEW | dummy | 2022-08-15 | 1 |
| 3 | babo NEW | dummy | 2022-08-15 | 1 |
| 2 | ★필독★ 공지사항 NEW | 관리자 | 2022-08-15 | 6 |
| 1 | s NEW | as | 2022-08-15 | 1 |

PREV

1

NEXT

작성자

글쓰기

[그림 7-4] 스크립트가 실행되어 새로운 게시글이 추가된 게시판

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

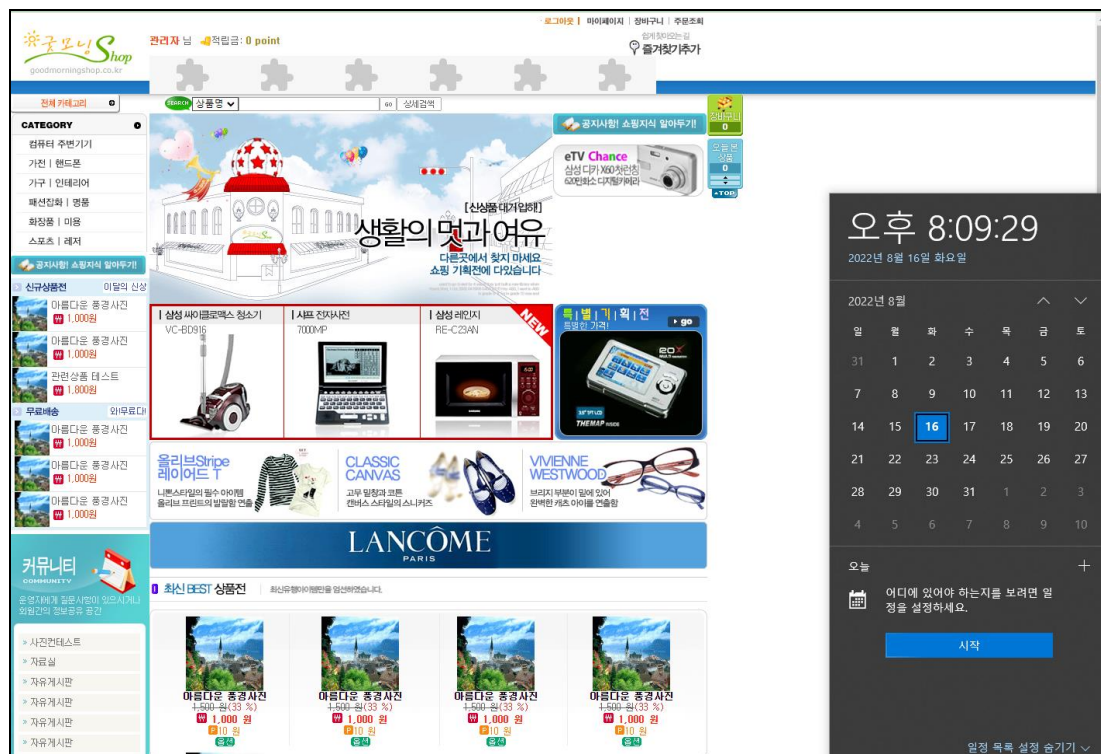
[그림 7-5] 스크립트가 실행되어 새롭게 추가된 게시글

3.7 불충분한 세션만료

| | |
|-------------|---|
| 취약점 명 | 불충분한 세션만료 |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 굿모닝Shop 웹 페이지에서는 세션 만료 되는 시간을 별도로 지정해 놓지 않았기 때문에 로그인 세션이 계속 남아있게 되어 로그아웃이 되지 않기 때문에 개인정보가 유출될 수 있다. |
| 발견 URL, 메뉴명 | ※ http://192.168.0.117:82/default.asp (메인 페이지) |

취약점 재현

1. 홈페이지에 접속 한 뒤 로그인을 하고 로그인 한 시간을 기록해두었다.



[그림 8-1] 굿모닝 Shop 로그인 후 시간 기록

2. 일정 시간이 경과했는데도 로그아웃 되지 않고 로그인이 유지된 것을 볼 수 있다.

The screenshot shows the Good Morning Shop website interface. At the top, there's a navigation bar with the site logo, user information (관리자님, 적립금: 0 point), and links for login/logout. Below the navigation bar, there's a main banner area with a large image of a building and text promoting a sale. To the left of the banner is a category menu. Below the banner are several product tiles for various items like a vacuum cleaner, a laptop, a microwave, and a digital scale. On the right side of the page, there's a dark overlay containing a digital clock showing '오후 9:29:44' and a calendar for August 2022, with the 16th highlighted. Below the calendar, there's a section for '오늘' (Today) with a button labeled '시작' (Start).

[그림 8-2] 일정 시간 지난후에도 세션 유지

3.8 불충분한 인증

| | |
|-------------|--|
| 취약점 명 | 불충분한 인증 |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 굿모닝 Shop의 계정 정보 변경 페이지에서 회원 정보 변경 시 재인증을 수행하지 않아 권한이 없는 사용자가 정보를 유출하거나 변조할 수 있다. |
| 발견 URL, 메뉴명 | ※ http:// 192.168.0.117:83/demoshop/account/profile.asp (회원정보관리) |

취약점 재현

1. 회원 정보를 변경할 수 있는 페이지에 접근 시 재인증을 수행하지 않는다.

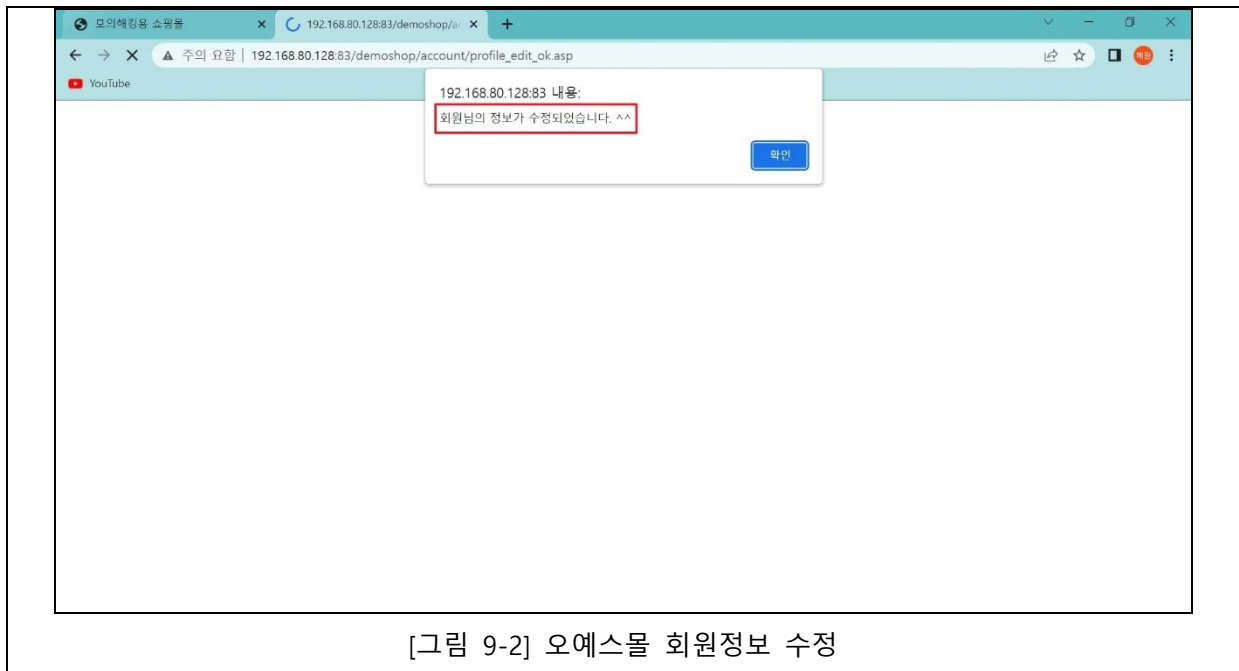
The screenshot shows a web browser window with the URL <http://192.168.0.117:83/demoshop/account/profile.asp>. The page displays a user profile form with the following fields and values:

- 사용자 ID: test
- 비밀번호: (masked)
- 비밀번호 힌트: (empty)
- 비밀번호 확인: (empty)
- 이름: 테스트
- 주민등록번호: 123123 - 1231234
- 생년월일: 1912년 01월 23일
- 관공여부: (radio buttons for Male/Female)
- 주소: [130-080] 서울 동대문구 이문동 우리집
- 전화번호: 02 - 123 - 1234
- 휴대폰: (empty)
- 직업: 학생
- E-Mail: onesider@naver.com

A red box highlights the '정보변경' (Update Info) button at the bottom of the form.

[그림 9-1] 오예스몰 회원정보 페이지

2. 재인증 없이 중요정보(개인정보 및 비밀번호)가 바뀌는 것을 볼 수 있다.



[그림 9-2] 오예스몰 회원정보 수정

3.9 파일 업로드

| | |
|-------------|--|
| 취약점 명 | 파일 업로드 |
| 취약점 등급 | 상 |
| 현황 및 문제점 | 굿모닝Shop 웹 페이지에서는 자료실에 파일을 업로드 할 수 있는데 이때 1차적으로 필터링을 진행하는데 공격자가 파일 확장자를 변경한뒤, 글쓰기 요청 전송을 가로채어 확장자를 다시 ASP 형태로 변경하면 업로드가 정상적으로 가능해진다. 공격자가 사용자의 요청을 필터링 하지 않는다는 점을 이용하여 악성 웹 쉘을 업로드 하여 악성코드 삽입, DB 데이터 삭제 등의 공격을 할 수 있다. |
| 발견 URL, 메뉴명 | ※ http:// 192.168.0.117:82/board_list.asp?boardIndex=4 (자료실) |

취약점 재현

1. 자료실에 스크립트가 들어있는 asp 파일 업로드를 시도했다. 글작성시 보안상의 이유로 asp 형식의 파일의 업로드가 제한되었다.

The screenshot shows a web application interface for file uploads. At the top, there's a header with a logo and the text '자료실' (File Room). Below it, a search bar is labeled '글등록하기' (Post Registration). The main form contains several input fields: '이름' (Name) with 'hacker', '이메일' (Email) with 'c@naer.com', '제 목' (Subject) with 'check this file', and '파일첨부' (File Attachment) with 'itmu.asp'. A red warning message states: '※ ASP, 스크립트 파일은 업로드할수 없습니다.' (ASP, script files cannot be uploaded). There's also a checkbox for '게시물 잠금 (본인과 관리자만 열람가능)' (Lock post (only you and admin can view)). Below the form, there are radio buttons for '내용입력 형식' (Content input format): 'TEXT' (selected), 'HTML', and '웹에디터'. A large text area contains the message: '192.168.0.117:82 내용: ASP, HTML 파일은 보안상 업로드할수 없습니다.' (192.168.0.117:82 content: ASP, HTML files cannot be uploaded for security reasons). A blue '확인' (Confirm) button is at the bottom right of the text area. At the very bottom, there are buttons for '저장' (Save) and '목록' (List).

[그림 10-1] 굿모닝 Shop 게시판 파일 업로드 시도

2. 확장자를 jpg로 변경하고, Burp suite를 통해 요청을 가로채어 파일이름을 강제로 asp 형식으로 수정하여 다시 재요청을 보냈다.

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

[그림 10-2] asp 파일 확장자 변경

```


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=----WebKitFormBoundaryQrfpxDMSFhcxUy
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=0.5,en;q=0.7
13 Cookie: ASPSESSIONIDACSBQACC=80FHEKCEBFEIDNDUJCNH; ASPSESSIONIDCSBPACC=HOMFKADBNHJIKDHEHNGKMF; ASPSESSIONIDCAPB70C=DOLLEKLEKALKHNHIDATJAL
14 Connection: close
15
16 -----WebKitFormBoundaryQrfpxDMSFhcxUy
17 Content-Disposition: form-data; name="boardIndex"
18
19 4
20 -----WebKitFormBoundaryQrfpxDMSFhcxUy
21 Content-Disposition: form-data; name="ref"
22
23
24 -----WebKitFormBoundaryQrfpxDMSFhcxUy
25 Content-Disposition: form-data; name="re_step"
26
27
28 -----WebKitFormBoundaryQrfpxDMSFhcxUy
29 Content-Disposition: form-data; name="re_level"
30
31
32 -----WebKitFormBoundaryQrfpxDMSFhcxUy
33 Content-Disposition: form-data; name="data"
34
35
36 -----WebKitFormBoundaryQrfpxDMSFhcxUy
37 Content-Disposition: form-data; name="name"
38
39 hacker
40 -----WebKitFormBoundaryQrfpxDMSFhcxUy
41 Content-Disposition: form-data; name="email"
42
43
44 c@naxi.com
45 -----WebKitFormBoundaryQrfpxDMSFhcxUy
46 Content-Disposition: form-data; name="title"
47
48 check this file
49 -----WebKitFormBoundaryQrfpxDMSFhcxUy
50 Content-Disposition: form-data; name="up_file"; filename="12345.asp"
51 Content-Type: image/jpeg

```

[그림 10-3] 게시판 파일 업로드

3. 파일이 정상적으로 업로드 된 것을 확인할 수 있다.

@ 자료실

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

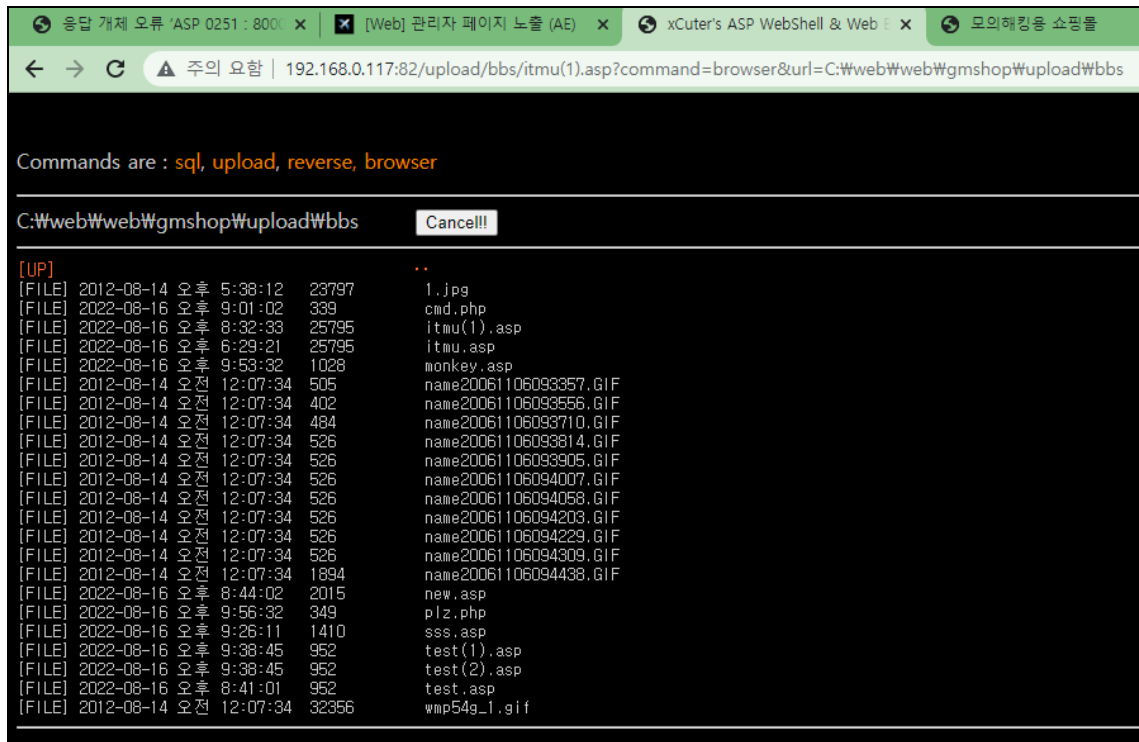
| 이름 | 내용 | 날짜 | 삭제 |
|--|-------------------------------|----|----|
| 이름 <input type="text"/> | 비밀번호 <input type="password"/> | | |
| <input style="width: 100%;" type="text"/> <div style="text-align: right;">COMMENT 등록</div> | | | |

비밀번호

목록
✓ 수정
↳ 답글
✕ 삭제

[그림 10-4] asp 파일이 업로드 된 게시글

4. 업로드된 파일을 누르면 asp 웹 셸이 실행되어 공격자가 원하는 역할을 수행할 수 있게 된다. 아래의 페이지는 파일 업로드 페이지로 악성코드를 서버의 경로 안에 삽입할 수 있게 된다.



[그림 10-5] 웹 셸 실행화면

4 조치 방법

4.1 SQL Injection

SQL Injection 조치방법

① 입력 값 유효성 검증

- 특수문자(' , " , ₩ , ; , % , space , -- , + , < , > , (,) , # , & 등)를 필터링한다
- 입력문자열 길이를 제한한다
- SQL 구문 입력을 제한한다
- 입력 받은 변수와 데이터베이스 필드 값의 데이터 형을 일치시킨다

② DB 구문에 영향을 줄 수 있는 입력값 유효성 검증

- /*, -, ' , ", ?, # , (), ; , @ , = , * , + union , select , drop , update , from , where , join , substr , user_tables....

4.2 크로스 사이트 스크립팅(XSS)

Cross Site Scripting 조치방법

① 입력 값 치환

- XSS 공격은 기본적으로 <script> 태그를 사용하기 때문에 XSS 공격을 차단하기 위해 태그 문자(< , >) 등 위험한 문자 입력 시 문자 참조(HTML entity)로 필터링한다.
- 서버에서 브라우저로 전송 시 문자를 인코딩한다. 문자 "<"를 동일한 의미의 HTML인 "<"로 변경한다. 이렇게 인코딩하면 HTML 문서에서 <script>로 나타나기 때문에 일반 문자로 인식하고 스크립트로 해석되어 실행되지 않는다.

② 입력 값 검증

- 입력 데이터의 길이 제한
- 지정된 문자 또는 형식으로 입력되었는지 확인
- 정해진 규칙을 벗어난 입력 값 무효화

4.3 데이터 평문 전송

데이터 평문 전송 조치방법

① 데이터 암호화

- 다양한 암호 알고리즘을 사용하여 데이터를 암호화해서 보낸다.

② 서버와 클라이언트 통신 시 중요정보가 사용되는 구간에 SSL, HTTPS 등의 안전한 암호화 통신을 적용한다.

4.4 정보 누출

정보 누출 조치방법

- ① Html 소스 안에 기록되는 정보는 사용자가 웹 브라우저 소스보기 기능만 사용해도 간단히 내용을 볼 수 있으므로, 중요 정보를 코멘트 처리하거나 hidden 등의 값으로 기록하지 말아야 한다

4.5 관리자 페이지 노출

관리자 페이지 노출 조치방법

- ① 유추하기 어려운 이름으로 관리자 페이지를 변경하여 비인가자가 관리자 페이지에 접근할 수 없게 하고, 근본적인 해결을 위해 지정된 ip만 관리자 페이지에 접근할 수 있도록 제한해야 한다. 부득이하게 관리자 페이지를 외부에 노출해야 하는 경우 관리자 페이지 로그인 시 2차 인증을 적용시켜야 한다

4.6 CSRF

Cross Site Request Forgery 조치방법

- ① CSRF 토큰사용
 - ➔ 로그인시 session value에 CSRF_TOKEN이라는 값을 저장한다. 그리고 사용자가 웹 페이지 요청 시 CSRF_TOKEN 값을 서버에게 전송하게 하고, 요청을 받을 시 인터셉터에서 CSRF_TOKEN 값을 검증하도록 한다.

4.7 불충분한 세션만료

불충분한 세션만료 조치방법

- ① 세션 종료 시간 설정 또는 자동 로그아웃 기능을 구현한다.
- ② 세션 타임아웃 기능을 구현한다 타임아웃 시간은 10분으로 하는 것을 권고한다.

4.8 불충분한 인증

불충분한 인증 조치방법

- ① 중요정보를 표시하는 페이지에서는 본인 인증을 재확인하는 로직을 구현하고, 사용자가 인증 후 이용 가능한 페이지에 접근할 때마다 승인을 얻은 사용자인지 페이지마다 검증해야한다.

4.9 파일 업로드

파일 업로드 조치방법

① 파일 확장자 필터링

- ➔ Jsp, php, asp 등의 스크립트로 작성될 가능성이 있는 파일 확장자의 경우 whitelist를 통해 허용되는 내용을 제외한 모든 부분을 필터링해서 안전한 확장자가 아닐 시, 업로드에 제한을 두게 한다

② 실행 권한 제거

- ➔ 파일이 저장되는 경로에서 실행 권한을 제거하여, 악성 스크립트가 업로드 되더라도 실행하지 못하게 한다.

③ 물리적인 위치 분리

- ➔ 웹 서버와 파일이 업로드 되는 서버를 물리적으로 분리한다.