

IR(Inform Relief) System

- 시스템 취약점 점검 -



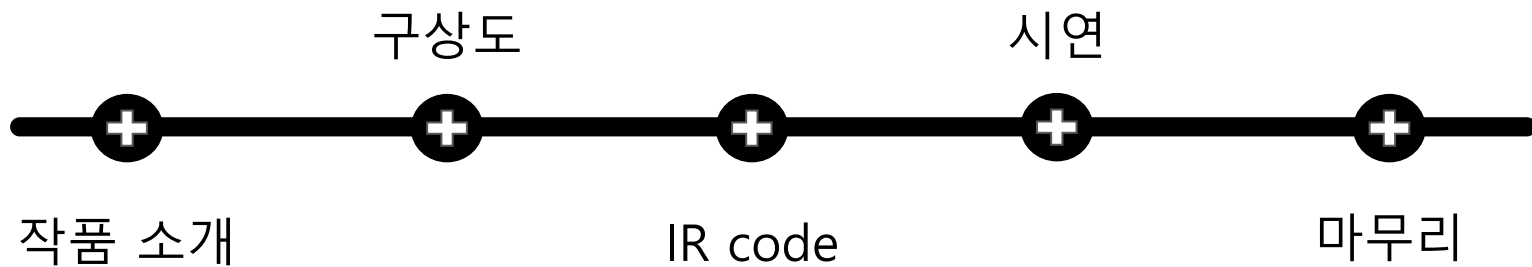
팀명: Checker

팀장: 조서연

팀원 : 김미란, 김성한, 김예리, 이윤지

지도 교수 : 양환석 교수님

목차



작품 소개

- 웹 페이지에서 SSH접속을 통해 시스템 취약점 점검 자동화 서비스를 제공
- 리눅스 운영체제를 대상으로 점검
- 취약점을 점검하고 나면 결과 파일은 DB를 통해 웹서버로 관리
- 이용자는 웹 서비스를 통해 시스템 취약점 점검의 결과를 열람 및 다운로드가 가능함

작품 소개

- 2017 '주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세가이드'를 기반으로 함



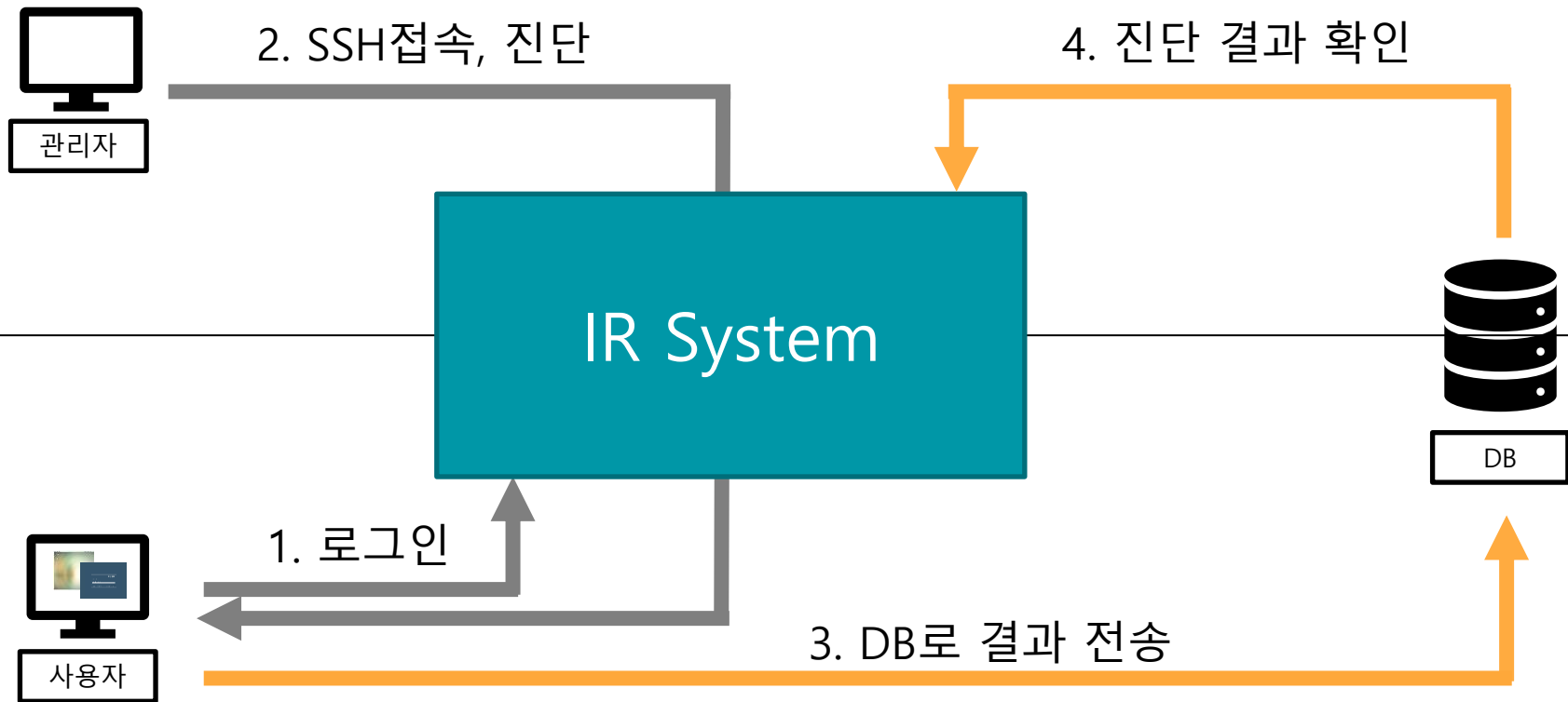
II. 보안가이드라인 - UNIX 서버 9

UNIX 서버 취약점 분석·평가 항목			
분류	점검항목	항목 중요도	항목코드
1. 계정관리	root 계정 원격 접속 제한	상	U-01
	패스워드 복잡성 설정	상	U-02
	계정 잠금 임계값 설정	상	U-03
	패스워드 파일 보호	상	U-04
	root 이외의 UID가 '0'금지	중	U-44
	root 계정 su 제한	하	U-45
	패스워드 최소 길이 설정	중	U-46
	패스워드 최대 사용기간 설정	중	U-47
	패스워드 최소 사용기간 설정	중	U-48
	불필요한 계정 제거	하	U-49
	관리자 그룹에 최소한의 계정 포함	하	U-50
	계정이 존재하지 않는 GID 금지	하	U-51
	동일한 UID 금지	중	U-52
	사용자 shell 점검	하	U-53
Session Timeout 설정	하	U-54	
2. 파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정	상	U-05
	파일 및 디렉터리 소유자 설정	상	U-06
	/etc/passwd 파일 소유자 및 권한 설정	상	U-07
	/etc/shadow 파일 소유자 및 권한 설정	상	U-08
	/etc/hosts 파일 소유자 및 권한 설정	상	U-09
	/etc/oinetd.conf 파일 소유자 및 권한 설정	상	U-10
	/etc/slog.conf 파일 소유자 및 권한 설정	상	U-11
	/etc/services 파일 소유자 및 권한 설정	상	U-12
	SUID, SGID, Sticky bit 설정 파일 점검	상	U-13
	사용자 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	U-14
	world writable 파일 점검	상	U-15
	/dev에 존재하지 않는 device 파일 점검	상	U-16
	\$HOME/.rhosts, hosts.equiv 사용 금지	상	U-17
	접속 IP 및 포트 제한	상	U-18
hosts.lpd 파일 소유자 및 권한 설정	하	U-55	
NIS 서비스 비활성화	중	U-56	
UMASK 설정 관리	중	U-57	
홈디렉토리 소유자 및 권한 설정	중	U-58	
홈디렉토리로 지정한 디렉토리의 존재 관리	중	U-59	
숨겨진 파일 및 디렉터리 검색 및 제거	하	U-60	

II. 보안가이드라인 - UNIX 서버 11

UNIX 서버	
U-01 (상)	1. 계정관리 > 1.1 root 계정 원격 접속 제한
취약점 개요	
점검내용	<ul style="list-style-type: none"> 시스템 정책에 root 계정의 원격 터미널 접속 차단 설정이 적용 되어 있는지 점검
점검목적	<ul style="list-style-type: none"> root 계정 원격 접속 차단 설정 여부를 점검하여 외부 비인가자의 root 계정 접근 시도를 원천적으로 차단하는지 확인하기 위함
보안위험	<ul style="list-style-type: none"> 각종 공격(무작위 대일 공격, 사전 대일 공격 등)을 통해 root 원격 접속 차단이 적용되지 않은 시스템의 root 계정 정보를 비인가자가 획득할 경우 시스템 계정 정보 유출, 파일 및 디렉터리 변조 등의 행위 침해사고가 발생할 수 있음
참고	<ul style="list-style-type: none"> root 계정: 여러 사용자가 사용하는 컴퓨터에서 전체적으로 관리할 수 있는 총괄 권한을 가진 유일한 특별 계정. 유닉스 시스템의 루트(root)는 시스템 관리자인 슈퍼 관리자(Super User)로서 윈도우의 관리자(Administrator)에 해당하며, 사용자 계정을 생성하거나 소프트웨어를 설치하고, 종량 및 설정을 변경하거나 시스템의 유격을 잠시 및 제거할 수 있음 무작위 대일 공격(Brute Force Attack): 특정한 암호를 찾기 위해 가능한 모든 값을 대입하는 공격 방법 사전 대일 공격(Dictionary Attack): 사전에 있는 단어를 입력하여 암호를 알아내거나 암호를 해독하는 데 사용되는 컴퓨터 공격 방법
점검대상 및 판단기준	
대상	SOLARIS, LINUX, AIX, HP-UX 등
판단기준	<p>양호 : 원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우</p> <p>취약 : 원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우</p>
조치방법	원격 접속 시 root 계정으로 바로 접속 할 수 없도록 설정파일 수정
점검 및 조치사례	
OS별 점검 파일 위치 및 점검 방법	
SOLARIS	#cat /etc/default/login CONSOLE=/dev/console
LINUX	#cat /etc/pam.d/login auth required /lib/security/pam_security.so #cat /etc/security/pts/0 - pts/x 관련 설정이 존재하지 않음
AIX	#cat /etc/security/user rlogin = false
HP-UX	#cat /etc/security/console
위에 제시된 내용으로 설정되어 있을 경우 root 원격 접속이 차단됨 / 내용 설정에 대해서는 아래의 보안설정방법을 참고함	

구상도



IR Code (Linux)

```
root@localhost:/m
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
echo ""
echo "[분류]"
echo "서비스 관리"
echo ""
echo "[항목코드]"
echo "U-35"
echo ""
echo "[점검항목]"
echo "웹 서비스 디렉토리 리스팅 제거"
echo ""
echo "[중요도]"
echo "상"
echo ""
echo "[점검현황]"
#####기능#####
IFS_backup="$IFS"
IFS=$'\n'
INDEXES_CHECK='sed -n '/O
or_log/${FILE_NAME} | gre
for line in ${INDEXES_CHE
do
if [ $? -eq 0 ]; then
    if [[ ${L
```

U-35 항목 코드

```
root@localhost:/my_w
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
echo "서비스 관리"
echo ""
echo "[항목코드]"
echo "U-39"
echo ""
echo "[점검항목]"
echo "Apache 링크 사용금지"
echo ""
echo "[중요도]"
echo "상"
echo ""
echo "[점검현황]"
#####기능#####
mkdir ${MAIN_PATH}/error_log > /dev/null 2>&1
string='grep -i "options" /etc/httpd/conf/httpd.conf 2>${MAIN_PATH}/error_log/${
FILE_NAME} | grep -v "#"
```

U-39 항목 코드

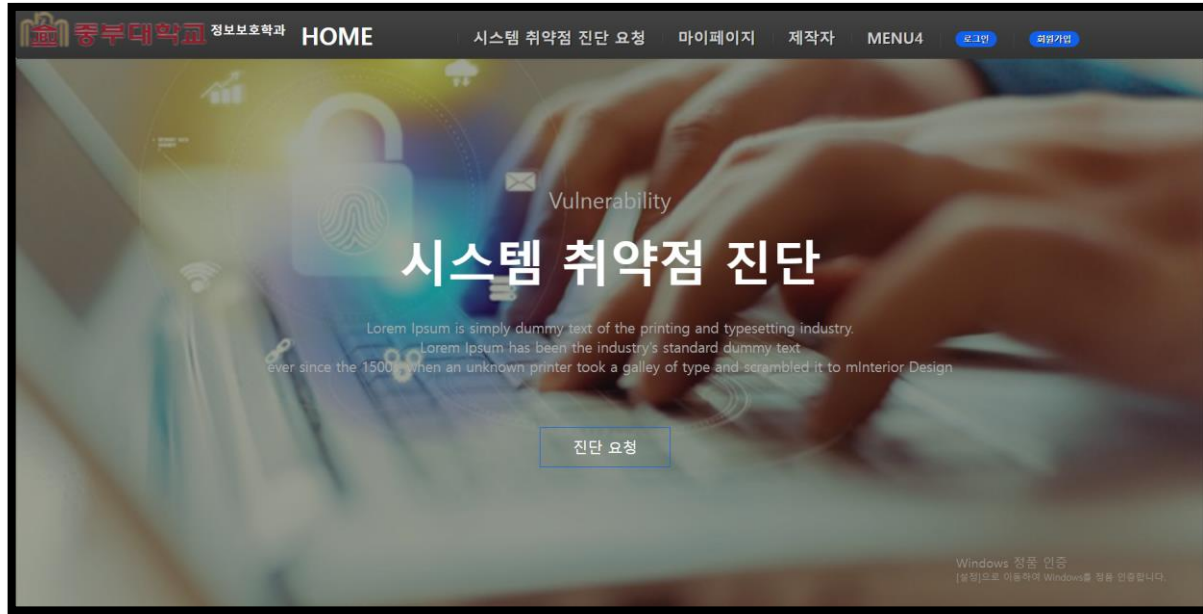
```
root@localhost:/
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
[항목코드]
U-35
[점검항목]
웹 서비스 디렉토리 리스팅 제거
[중요도]
상
[점검현황]
Options에 Indexes가 지정되어 있음
Options에 Indexes가 지정되어 있지 않음
[진단결과]
부분만족
[조치사항]
모든 Options에서 Indexes설정을 제거
```

U-35 항목 결과

```
root@localhost
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
[항목코드]
U-37
echo "1"
[점검항목]
echo "모
웹서비스 상위 디렉토리 접근금지
제한" >>action
[중요도]
상
[점검현황]
AllowOverride 옵션이 None으로 지정되어 있음
[진단결과]
불만족
[조치사항]
모든 AllowOverride 옵션에서 None제거
[분류]
서비스 관리
```

U-39 항목 결과

IR System - User



[그림 U-1] 웹 페이지

IR System - User

The registration form is titled '회원가입' (Sign Up) and is set against a dark background with a city street scene. It contains the following fields and elements:

- 이름** (Name): Input field containing '김성현'.
- 아이디** (ID): Input field containing 'abc1234'.
- 비밀번호** (Password): Input field with masked characters '*****'.
- 비밀번호 확인** (Confirm Password): Input field with masked characters '*****'.
- 전화번호** (Phone Number): Input field containing '010-1234-5678'.
- 회원가입** (Sign Up): A prominent blue button at the bottom.

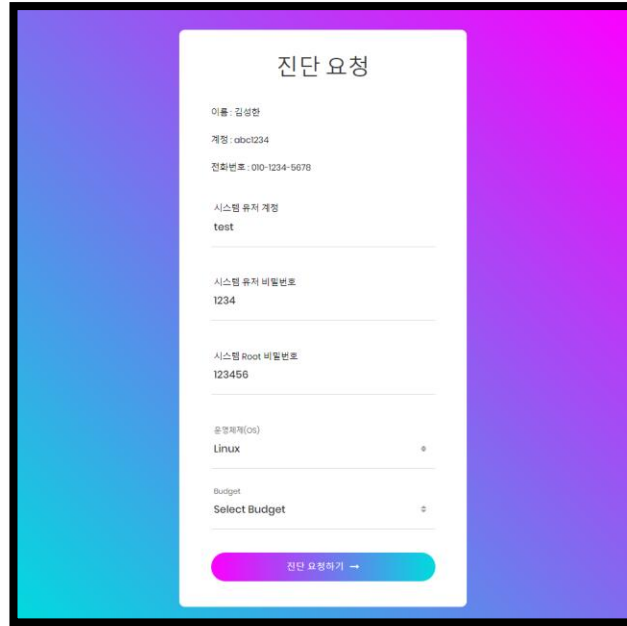
[그림 U-2] 회원가입

The login form is titled '로그인' (Login) and is set against a dark background with a city street scene. It contains the following fields and elements:

- 아이디** (ID): Input field containing 'abc1234'.
- 비밀번호** (Password): Input field with masked characters '*****'.
- 로그인** (Login): A prominent blue button.
- 회원가입** (Sign Up): A blue button located below the login button.

[그림 U-3] 로그인

IR System - User



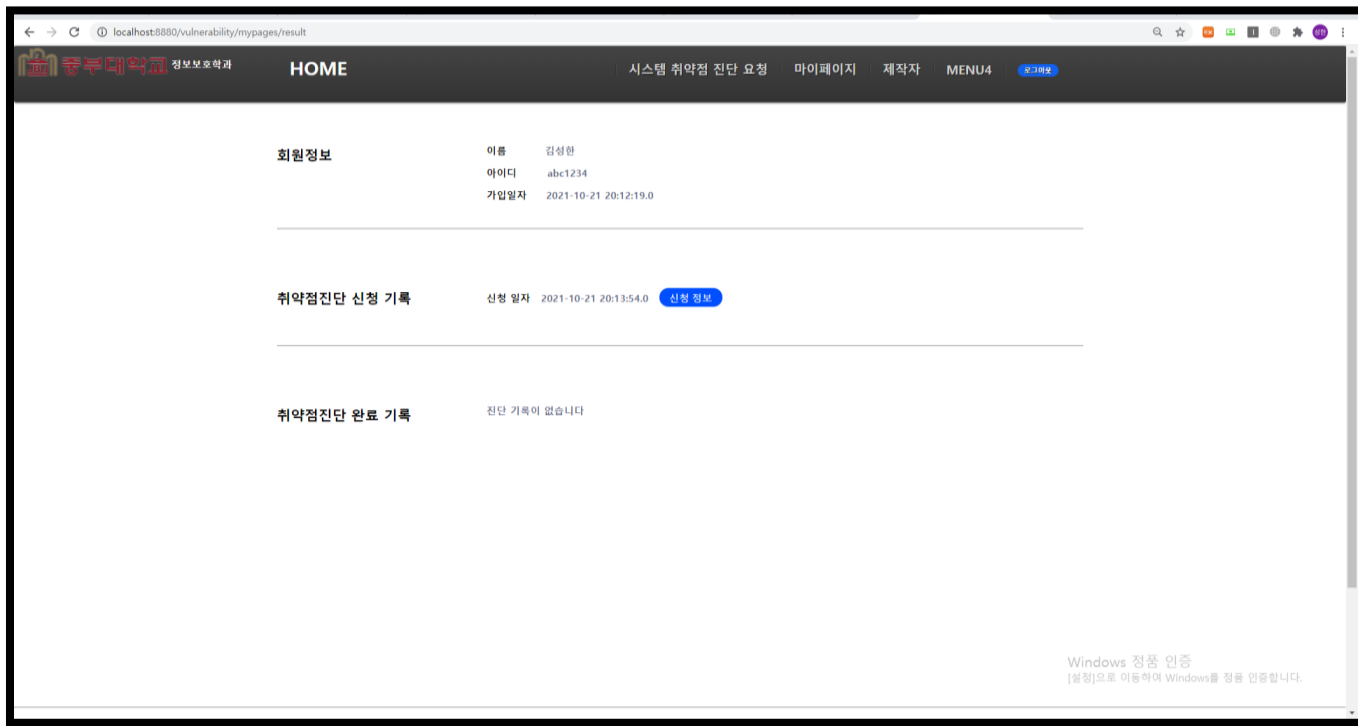
The image shows a web form titled "진단 요청" (Request for Diagnosis) set against a colorful gradient background. The form contains the following fields and values:

- 이름: 김성환
- 계정: abc1234
- 전화번호: 010-1234-5678
- 시스템 유저 계정: test
- 시스템 유저 비밀번호: 1234
- 시스템 Root 비밀번호: 123456
- 운영체제(OS): Linux
- Budget: Select Budget

At the bottom of the form is a button labeled "진단 요청하기 →" (Request for Diagnosis →).

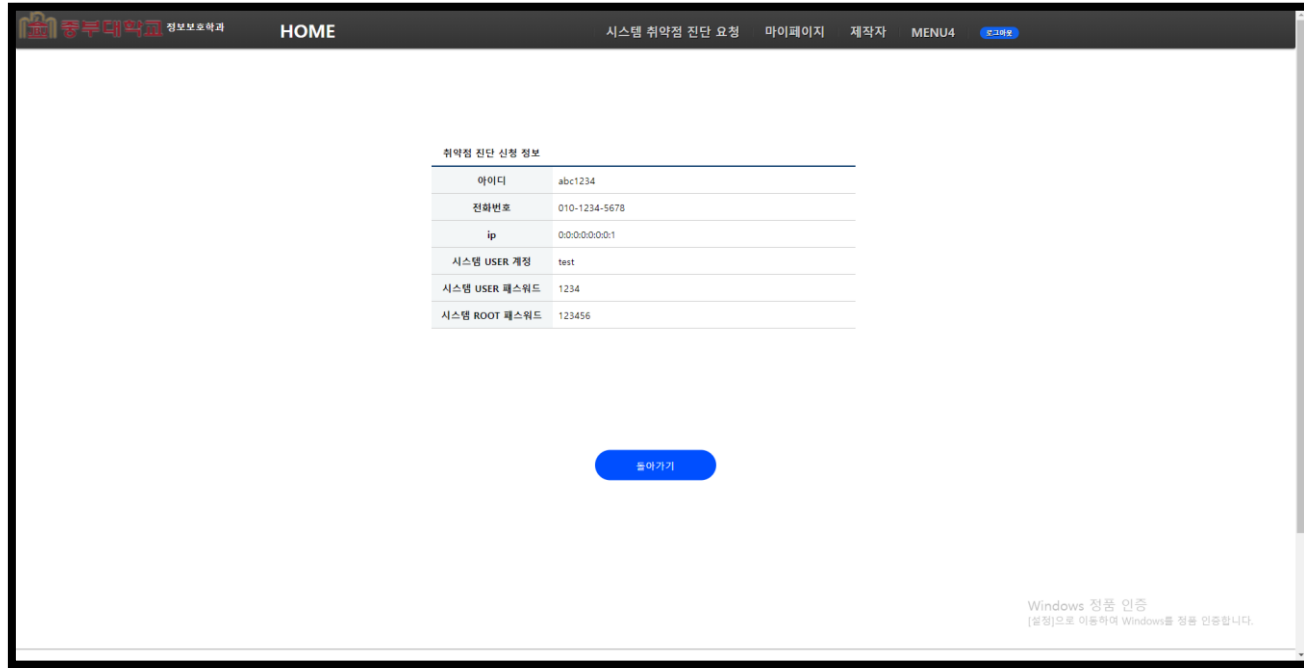
[그림 U-4]점검 시스템 진단 요청

IR System - User



[그림 U-5] 사용자의 마이페이지

IR System - User



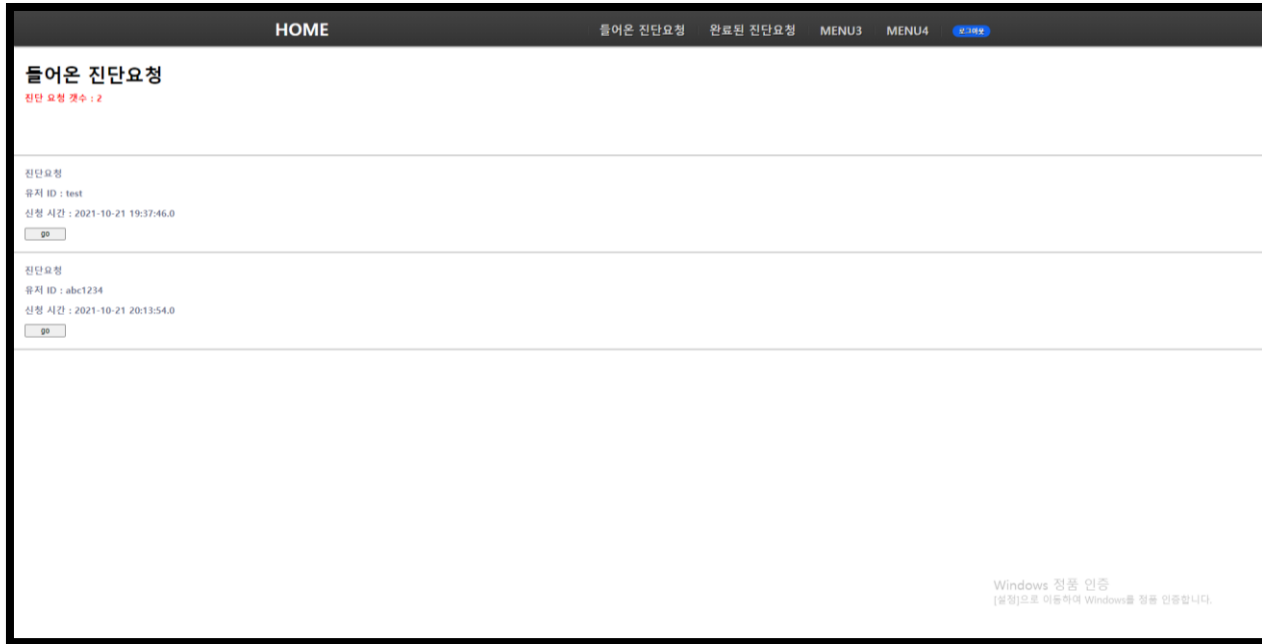
The screenshot displays a web application interface for an IR System. At the top, there is a navigation bar with the following elements: a logo for '충북대학교' (Chungbuk National University) and '정보보호학과' (Department of Information Security), the word 'HOME', and several menu items: '시스템 취약점 진단 요청', '마이페이지', '제작자', 'MENU4', and a blue button labeled '로그아웃'. The main content area features a table titled '취약점 진단 신청 정보' (Vulnerability Assessment Application Information). The table contains the following data:

취약점 진단 신청 정보	
아이디	abc1234
전화번호	010-1234-5678
ip	0:0:0:0:0:1
시스템 USER 계정	test
시스템 USER 패스워드	1234
시스템 ROOT 패스워드	123456

Below the table, there is a blue button labeled '돌아가기' (Go Back). In the bottom right corner of the page, there is a Windows logo and the text 'Windows 정품 인증 [불법]으로 이루어져 Windows를 정품 인증합니다.' (Windows Genuine Activation [Illegal] is performed to certify Windows as genuine).

[그림 U-6] 사용자의 신청 정보 확인

IR System - Admin



The screenshot displays the admin interface of the IR System. At the top, there is a navigation bar with the word "HOME" on the left and several menu items: "들어온 진단요청" (Incoming Diagnosis Request), "완료된 진단요청" (Completed Diagnosis Request), "MENU3", "MENU4", and a blue button with a left-pointing arrow and the text "←3/31→".

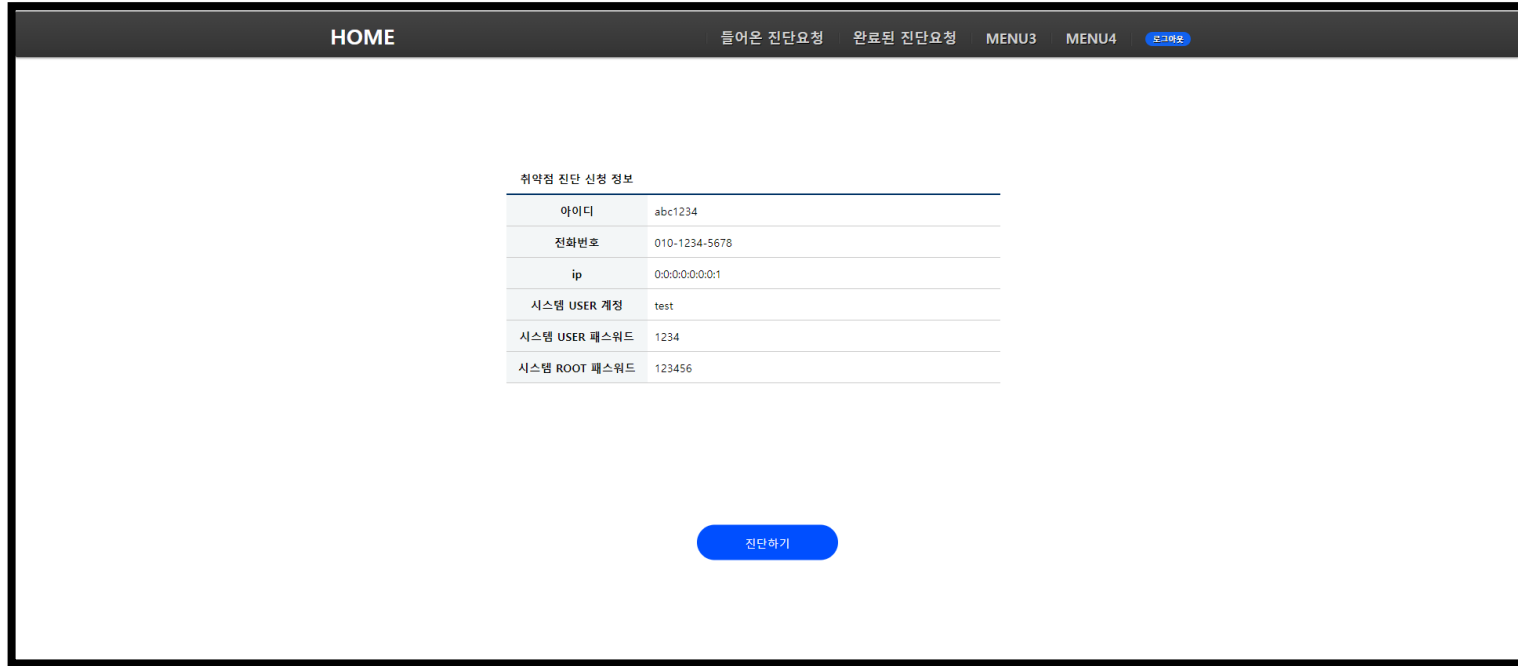
The main content area is titled "들어온 진단요청" (Incoming Diagnosis Request) in bold black text. Below the title, it shows "진단 요청 갯수 : 2" (Diagnosis Request Count : 2) in red text. The interface lists two requests, each with a "진단요청" (Diagnosis Request) header, a "유저 ID" (User ID), and a "신청 시간" (Application Time). Each entry includes a small "GO" button.

진단요청
유저 ID : test 신청 시간 : 2021-10-21 19:37:46.0 <input type="button" value="GO"/>
진단요청
유저 ID : abc1234 신청 시간 : 2021-10-21 20:13:54.0 <input type="button" value="GO"/>

In the bottom right corner of the interface, there is a "Windows 정품 인증" (Windows Genuine Activation) watermark with the text "(실정)으로 이동하여 Windows를 정품 인증합니다." (Move to (Actual) to activate Windows as genuine).

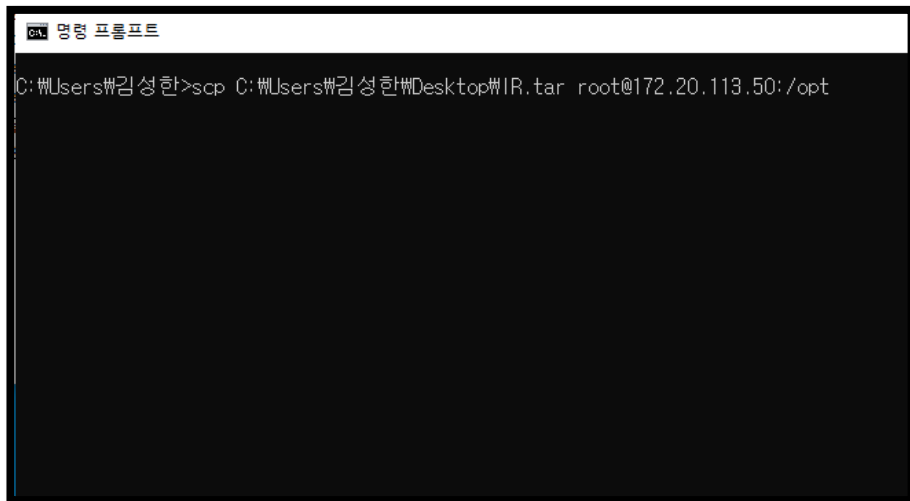
[그림 A-1] 요청 리스트

IR System - Admin



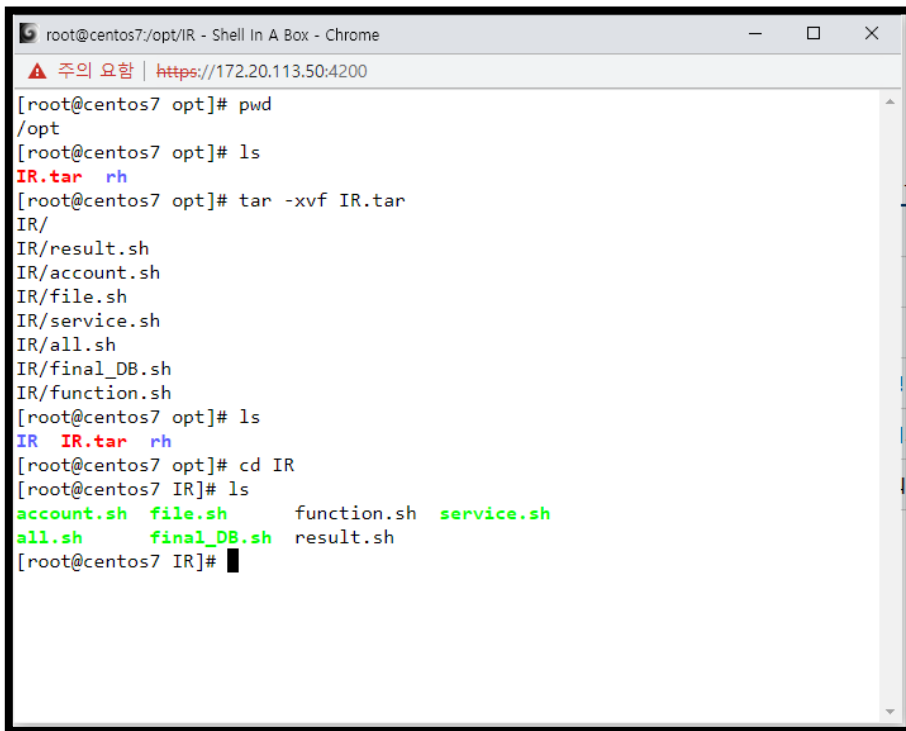
[그림 A-2] 특정 시스템 요청 확인

IR System - Admin



```
명령 프롬프트
C:\Users\김성한>scp C:\Users\김성한\Desktop\IR.tar root@172.20.113.50:/opt
```

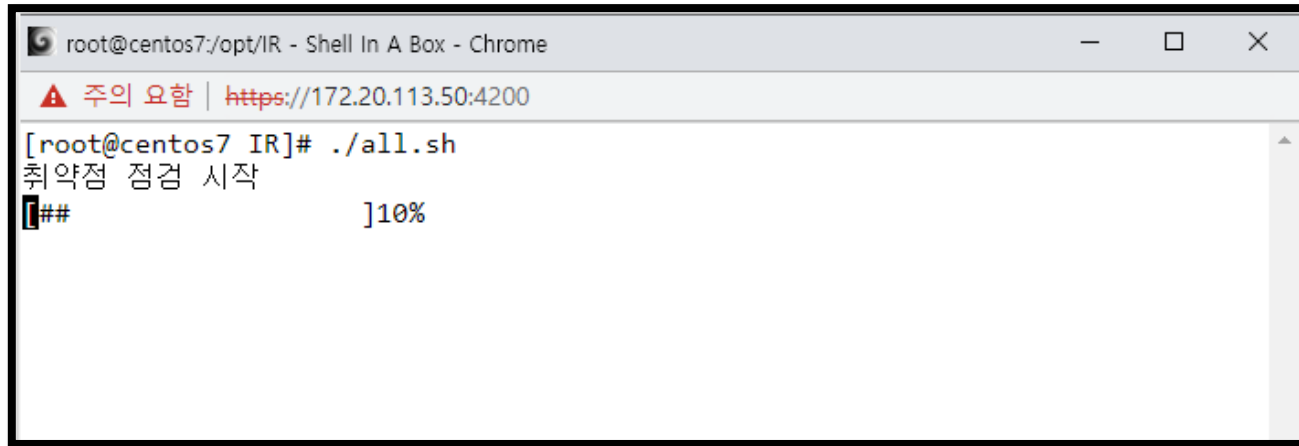
[그림 A-3] IR Code 전송



```
root@centos7:/opt/IR - Shell In A Box - Chrome
주의 요함 | https://172.20.113.50:4200
[root@centos7 opt]# pwd
/opt
[root@centos7 opt]# ls
IR.tar  rh
[root@centos7 opt]# tar -xvf IR.tar
IR/
IR/result.sh
IR/account.sh
IR/file.sh
IR/service.sh
IR/all.sh
IR/final_DB.sh
IR/function.sh
[root@centos7 opt]# ls
IR IR.tar rh
[root@centos7 opt]# cd IR
[root@centos7 IR]# ls
account.sh  file.sh      function.sh  service.sh
all.sh     final_DB.sh result.sh
[root@centos7 IR]#
```

[그림 A-4] 해당 시스템 접속

IR System - Admin

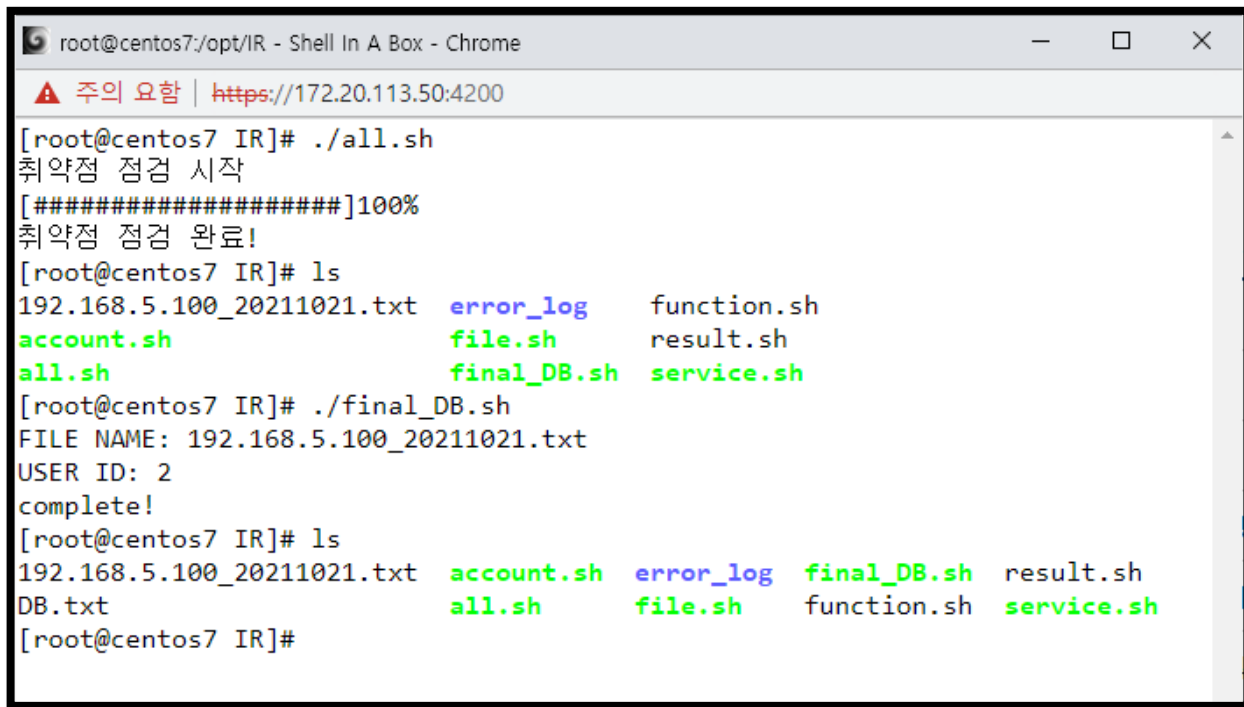


The image shows a terminal window titled "root@centos7:/opt/IR - Shell In A Box - Chrome". The address bar displays a warning icon and the text "주의 요함 | https://172.20.113.50:4200". The terminal content shows the command `[root@centos7 IR]# ./all.sh` being executed. The output consists of two lines: "취약점 점검 시작" followed by a cursor and "###", and then "10%".

```
root@centos7:/opt/IR - Shell In A Box - Chrome
주의 요함 | https://172.20.113.50:4200
[root@centos7 IR]# ./all.sh
취약점 점검 시작
[###                               ]10%
```

[그림 A-5] 진단 시작

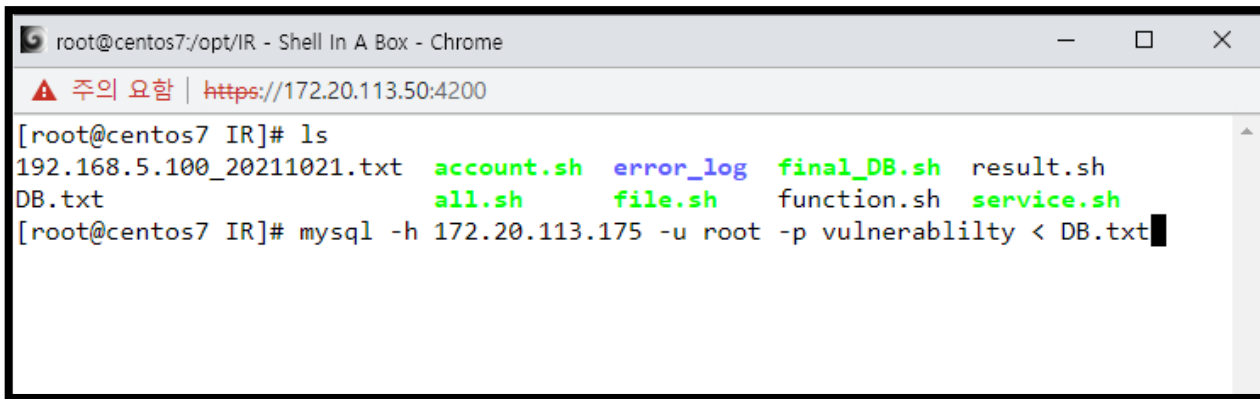
IR System - Admin



```
root@centos7:/opt/IR - Shell In A Box - Chrome
주의 요함 | https://172.20.113.50:4200
[root@centos7 IR]# ./all.sh
취약점 점검 시작
[#####]100%
취약점 점검 완료!
[root@centos7 IR]# ls
192.168.5.100_20211021.txt  error_log  function.sh
account.sh                file.sh    result.sh
all.sh                    final_DB.sh  service.sh
[root@centos7 IR]# ./final_DB.sh
FILE NAME: 192.168.5.100_20211021.txt
USER ID: 2
complete!
[root@centos7 IR]# ls
192.168.5.100_20211021.txt  account.sh  error_log  final_DB.sh  result.sh
DB.txt                      all.sh     file.sh    function.sh  service.sh
[root@centos7 IR]#
```

[그림 A-6] 점검 완료 후 DB 가공

IR System - Admin

A screenshot of a terminal window titled "root@centos7:/opt/IR - Shell In A Box - Chrome". The address bar shows "주의 요함 | https://172.20.113.50:4200". The terminal content shows a shell prompt [root@centos7 IR]# followed by the command 'ls'. The output lists files: 192.168.5.100_20211021.txt, account.sh, error_log, final_DB.sh, result.sh, DB.txt, all.sh, file.sh, function.sh, and service.sh. The next command is 'mysql -h 172.20.113.175 -u root -p vulnerabililty < DB.txt' with a cursor at the end.

```
root@centos7:/opt/IR - Shell In A Box - Chrome
주의 요함 | https://172.20.113.50:4200
[root@centos7 IR]# ls
192.168.5.100_20211021.txt  account.sh  error_log  final_DB.sh  result.sh
DB.txt                    all.sh     file.sh    function.sh  service.sh
[root@centos7 IR]# mysql -h 172.20.113.175 -u root -p vulnerabililty < DB.txt
```

[그림 A-7] DB로 전송

IR System - Admin

HOME 들어온 진단요청 완료된 진단요청 MENU3 MENU4 로그인

회원 정보

이름 : 조서민
계정 : test
연락처 : 01012345678
점검 완료일 : 2021-10-22 04:18:54.0

진단 결과

호스트	진재항목	점검항목	만족	부분 만족	불만족	N/A	보안점수
centos7	72	49	21	5	23	23	29

상세 결과

분류	원래 코드	점검 항목	중요도	점검 현황	진단 결과	조치 사항
계정 관리	U-01	상	root 계정 원격 접속 제한	PermiRootLogin에 주석 설정이 되어 있음 /etc/security/passwd 내 /pts/* 관련 설정이 존재하지 않음	부분만족	PermiRootLogin 설정에서 주석을 제거한 후 No로 설정
	U-02	상	패스워드 복잡성 설정	dcredit 설정에 주석처리 되어 있음 minlen 설정에 주석처리 되어 있음 ocredit 설정에 주석처리 되어 있음 ucredit 설정에 주석처리 되어 있음	불만족	dcredit 값이 -10이 되게 설정해야함 dflok 값이 8이아기 되게 설정해야함 minlen 값이 8이아기 되게 설정해야함 ocredit 값이 -10이아기 되게 설정해야함 ucredit 값이 -10이아기 되게 설정해야함
	U-03	상	계정 원격 로그인 설정	계정 원격값이 설정되어 있지 않음	불만족	이러와 같은 내용으로 변경 auth required /lib64/security/pam_tallock.so deny=5 unlock_time=120 no_magic_root account required /lib64/security/pam_tallico no_magic_root reset
	U-04	상	패스워드 파일 보호	/etc/shadow 파일이 존재하지 않음 /etc/passwd 파일 내 두번째 필드가 x임	부분만족	패스워드 암호화 저장 및 관리 설정 적용 필요
	U-44	중	root 이외의 UID가 0 관리자	root 이외의 UID가 0인 계정 이 존재하지 않음	만족	
U-45	하	root 계정 su 제한	/usr/bin/su 파일의 권한이 4750이 아닌 4755 그룹이 존재함	부분만족	/usr/bin/su 파일의 권한을 4750으로 변경	

Windows 정품 인증
(선택)으로 이용하여 Windows 정품 인증합니다.

[그림 A-8] 점검 결과 확인

Q & A



감사합니다

