웹으로 공부하는 취약점 마스터

팀 명	답은 정해져있다
지 도 교 수	이병천 교수님
팀 장	한현동
팀 원	박유찬,손진빈
	이정훈,한완섭

2023. 11.

중부대학교 정보보호학과

목 차

1. 서론

1.1 연구 배경

현대 사회는 4차 산업 혁명의 도래와 함께 기업의 중요한 정보는 디지털 방식으로 저장 및 관리되고 있다. 따라서 기업의 정보 자산은 이전보다 훨씬 다양하고 복잡한 형태에 직면하게 되었고 이러한 자산을 외부로부터 보호하기 위해 기업들은 다양한 정보 보안 인재를 강구하고 있다. 취약점에 대해 공부하고자 하는 학생들이 전문 지식과 기술을 쉽고 유연하게 습득할 수 있는 교육 사이트가 필요하다고 판단하여 취약점을 공부할 수 있는 웹 사이트를 제작하게 되었다.

1.2 연구 목적 및 주제 선정

대부분의 기업은 그들만의 유・무형의 자산을 가지고 있고, 이러한 자산들은 해킹 및 바이러스의 위험에 노출되어 있다. 정보통신 기반 보호법 제9조(취약점의 분석・평가)에 의해 과학기술정보통신부와 KISA에서 고안한 '주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드'(이하 주통기)의 내용을 토대로 대부분의 기업은 정기적으로 취약점 점검을 받아야 한다. 따라서 이번 프로젝트로 만든 학습 사이트 통해 해당 가이드의 내용을 토대로 취약점을 진로로 하는 비전공자나 전공 입문자들이 쉽게 OS 취약점 진단 공부를 할 수 있도록 제작하였다.

2. 관련 연구

2.1 Widows server 2012 R2

"Windows Server 2012 R2"는 마이크로소프트가 개발한 서버로, Windows Server 시리즈의 일부이다.기업 및 조직이 데이터를 관리하고, 네트워크 관리하고, 웹 서비스 제공 등 다양한 서버 기능을 제공할 수 있도록 설계되었다.

2.2 CentOs 7

CentOS 7은 CentOS 프로젝트에서 개발 중인 오픈 소스 배포 중 하나로, Red Hat Enterprise Linux(RHEL)의 소스 코드를 기반으로 다음과 같은 무료 및 오픈 소스 운영체제 이다. CentOS 7은 RHEL 7과 거의 동일한 기능을 제공하며, 엔터프라이즈 환경에서 안정적이고 신뢰성 있는 서버 운영을 위한 선택적인 운영 체제로 많이 사용된다.

2.3 Batch script

Windows Batch Script는 Windows 운영 체제에서 사용되는 명령어 및 명령어 스크립팅 언어이다.배치 스크립트는 일련의 명령어를 포함하며, 이를 한 번에 실행하거나 자동화된 작업을 수행하는 데 사용된다.

2.4 Shell script

(Linux Shell)은 리눅스 및 다른 유닉스 기반 운영 체제에서 사용되는 명령 줄 인터페이스 (CLI)이다. shell은 사용자가 컴퓨터와 상호 작용하고 명령을 실행하는 환경을 제공한다.

2.5. html

웹 페이지를 만들기 위한 표준 마크업 언어이다. HTML은 웹 페이지의 구조와 내용을 정의하고 웹 브라우저에서 페이지를 렌더링하는 데 사용된다.

2.6 javascript

JavaScript는 웹 개발에 필수적인 동적 프로그래밍 언어로, 클라이언트 사이드와 서버 사이드 모두에서 사용이 가능하다. 객체 지향 프로그래밍과 함수형 프로그래밍을 지원하며, 다양한 프레임워크와 라이브러리 덕분에 광범위한 개발 영역에서 활용되고 있다

2.7 node.js

Node.js는 서버 사이드에서 동작하는 JavaScript 런타임으로, 비동기 이벤트 드리븐 아키텍처를 사용하여 효율적인 I/O 처리를 한다.단일 스레드를 사용하면서도 높은 동시성을 제공하며, NPM을 통한 패키지 관리, 다양한 활용 영역, 풍부한 프레임워크 생태계 등으로 유용하다

2.8 express.js

Express.js는 JavaScript 런타임 환경인 Node.js에서 동작하는 웹 서버 및 웹 애플리케이션 개발을 위한 미니멀리스트 웹 프레임워크이다.Express.js는 간단한 구조와 직관적인 API를 가지고 있어, 웹 애플리케이션을 빠르게 개발하고 프로토타입을 만들기에 이상적이다.

2.9 react

Facebook에서 개발한 사용자 인터페이스(UI) 라이브러리로, 웹 및 모바일 애플리케이션의 사용자 인터페이스를 구축하기 위한 자바스크립트 라이브러리이다

React는 컴포넌트 기반 아키텍처를 기반으로 하며, 재사용 가능한 UI 요소를 만들고 이를 조합하여 복잡한 사용자 인터페이스를 구축하는 데 용이하다.

2.10 redux

Redux는 JavaScript 애플리케이션의 상태를 관리하기 위한 오픈 소스 JavaScript 라이브러리로, 주로 React 또는 Angular와 같은 사용자 인터페이스 라이브러리/프레임워크와 함께 사용된다. Redux는 애플리케이션의 상태 관리를 예측 가능하게 만들기 위해 설계되었으며, 애플리케이션의 상태를 중앙 집중화된 저장소(Store)에서 관리한다

2.11 mongodb

MongoDB는 NoSQL 데이터베이스 중 하나로, 스키마리스로 데이터를 BSON 형식으로 저장하는 문서 지향적 데이터베이스이다. 확장성 있게 대용량 데이터를 처리할 수 있으며, 다양한 데이터 조작 및 집계 쿼리를 지원한다. 다양한 데이터 포맷과 동적 스키마로 인해 다양한 애플리케이션에서 유연하게 사용된다.

2.12 css

CSS (Cascading Style Sheets)는 웹 페이지의 스타일을 꾸미는 데 사용되는 스타일시트 언어이다. HTML, XHTML 또는 XML(이 중 SVG와 XUL 포함) 문서의 레이아웃과 디스플레이를 정의하기 위해 주로 사용된다.

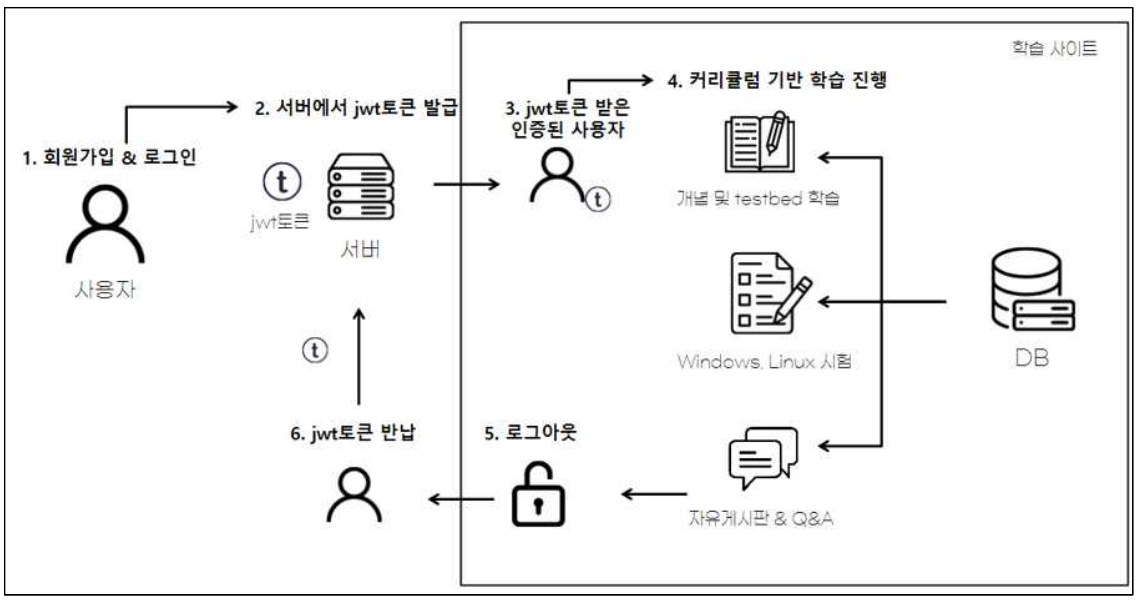
2.13 jsonwebtoken

JSON Web Token (JWT)은 웹 표준 (RFC 7519)으로, 두 엔터티(일반적으로, 사용자와 서버) 사이에서 정보를 안전하게 전송하기 위한 작은 JSON 객체이다. JWT는 사용자 인증 및 정보 교환에 많이 사용되며, 자체적으로 정보의 신뢰성을 검증할 수 있다.

3. 본론

3.1 시스템구성

사용자가 사이트에 가입할 때 정보를 보호하기 위해 JWT토큰을 발행하여 데이터의 누출을 방지한다. 인증된 사용자는 웹사이트에 가입 후 운영체제 및 실습 자료들에 대한 지식을 얻어가며 운영진이 제공하는 문제를 풀어가며 스스로 학습한 내용을 돌아보도록 유도한다.

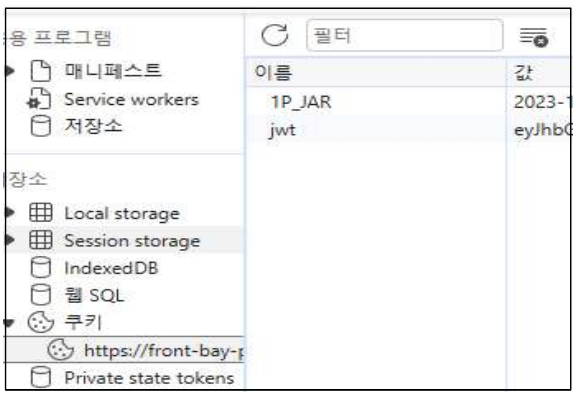


[그림. 3.1-1] 시스템 구상도

3.2 프로그램 구성

3.2.1 회원가입 및 로그인

[그림. 3.2.1-1] 로그인 페이지



[그림. 3.2.1-2] 로그인 후 토큰 부여

사이트에서 데이터 노출을 방지하기 위해 jwt토큰을 이용하며 사용자는 이 토큰을 발급받기 위해 회원가입 및 로그인을 진행한다.

```
function Login() {
  const [cookies] = useCookies([]);
  const navigate = useNavigate();
  useEffect(() => {
    if (cookies.jwt) {
      navigate("/");
    }
  }, [cookies, navigate]);

  const [values, setValues] = useStat
  "", password: "" });
  const generateError = (error) =>
```

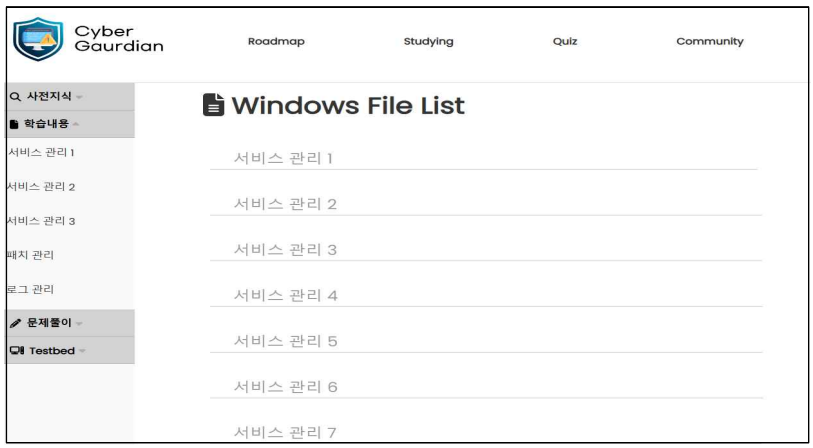
[그림. 3.2.1-3] 토큰을 부여받지 못했을 시 로그인 화면으로 이동

3.2.2 사용자 UI

[그림. 3.2.2-1] Roadmap 페이지로 가이드라인 제시

처음 사용자가 사이트를 입장한 후에 상단 메뉴바에서 'Roadmap'을 통해 사용자가 어떤 순서로 이용해야 하는지에 대한 가이드를 해준다.

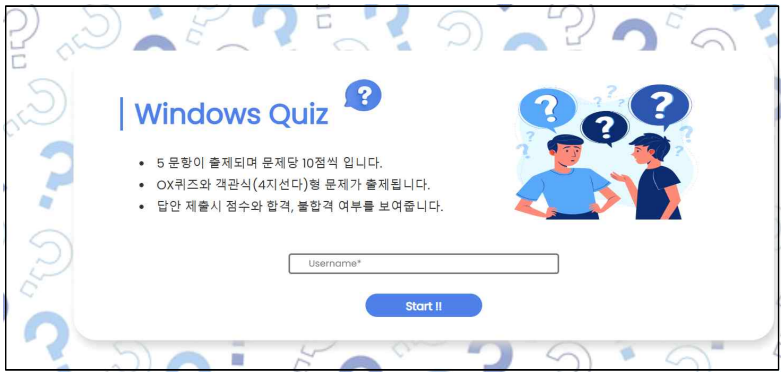
다음 학습 페이지에서는 취약점 팀에서 기획, 작성한 커리큘럼 순서대로 제공하며 윈도우, 리눅스 각각 70가지가 넘는 학습 자료가 준비되어 있다.



[그림. 3.2.2-2] Windows 학습 페이지

[그림. 3.2.2-3] Linux의 학습 자료

학습 자료의 내용들을 공부한 후 문제 풀이 페이지에서 학습이 어느 정도 되었는지 테스트가 가능하다.



[그림. 3.2.2-4] Windows문제 메인화면

[그림. 3.2.2-5] 문제가 제시되는 모습

[그림. 3.2.2-6] 점수를 체크하는 Result페이지

마지막으로 사용자는 주어진 환경을 해결해 나가는 실습 자료를 다운로드하여 직접 문제가 생긴 운영체제 환경을 체험해 볼 수 있으며 자신의 문제 풀이나 경험을 게시판을 통해서 공유 가능하다.

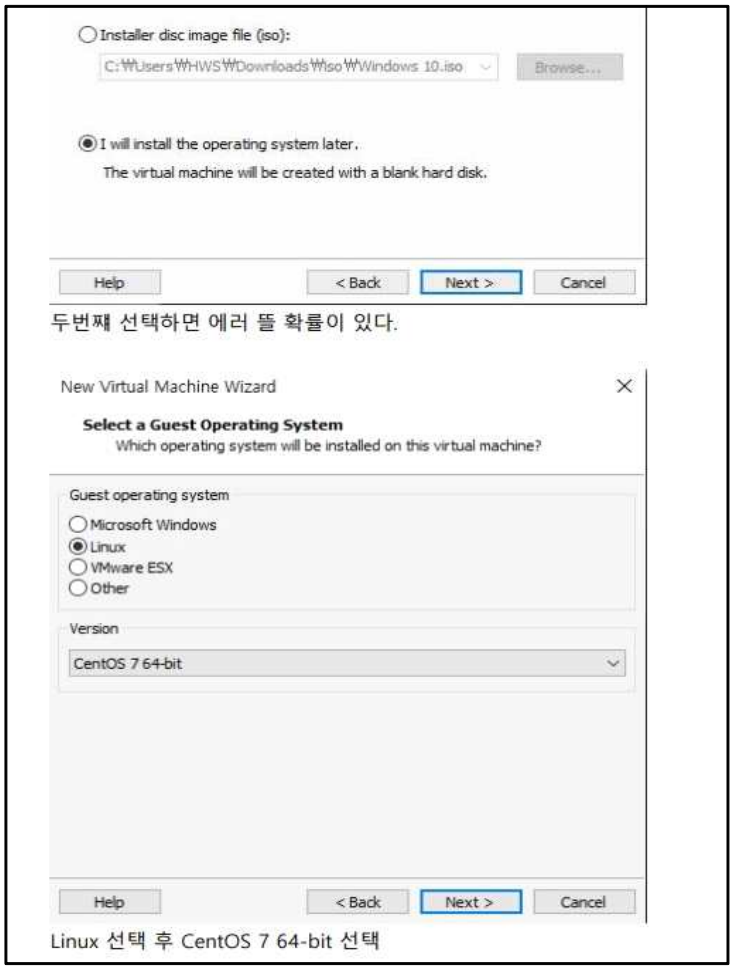
[그림. 3.2.2-7] Testbed 실습자료를 다운로드할 수 있는 자료실

[그림. 3.2.2-8] 소통이 가능한 자유게시판

3.2.3. 관리자 UI

[그림. 3.2.3-1] 관리자 권한이 있는 계정으로 접속 후 보이는 문제추가 페이지

관리자는 문제 혹은 학습 자료를 상시로 추가, 수정, 삭제가 가능하다.



[그림. 3.2.3-2] 실습환경 구축 과정

[그림. 3.2.3-2]와 같이 리눅스서버와 윈도우 서버를 직접 구축하여 실습할 수 있도록 실습환경 구축 가이드를 제공하였다.

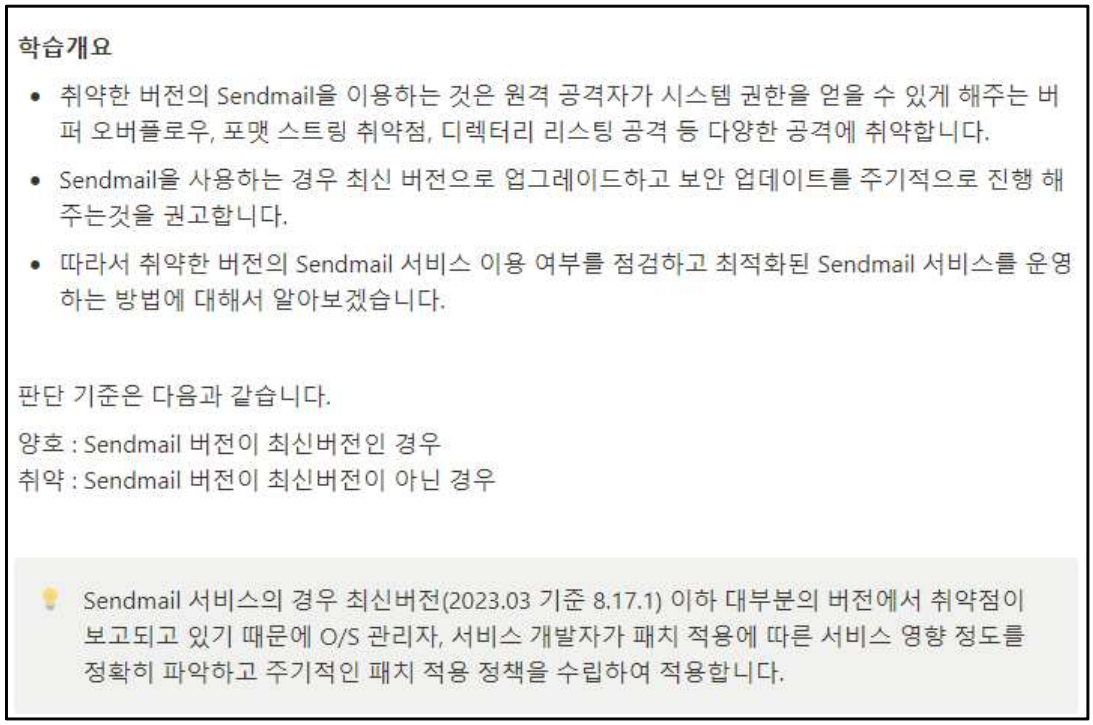
3.3 서비스 구성

3.3.1 진단 및 조치 상세 가이드

kisa의 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드(이하 주통기)에서는 자세한 설명이나 사진 자료가 부족하여 입문자들에게 진입 장벽이 높다.

U-30 (상)	3. 서비스 관리 > 3.12 Sendmail 버전 점검
취약점 개요	
점검내용	■ 취약한 버전의 Sendmail 서비스 이용 여부 점검
점검목적	■ Sendmail 서비스 사용 목적 검토 및 취약점이 없는 버전의 사용 유무 점검으로 최적화된 Sendmail 서비스의 운영
보안위협	■ 취약점이 발견된 Sendmail 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 요출 가능성이 있음
참고	※ Sendmail 서비스의 경우 최신버전(2016.01 기준 8.15.2) 이하 대부분의 버전에서 취약점이 보고되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하고 주기적인 패치 적용 정책을 수립하여 적용함
점검대상 및 판단기준	
대상	■ SOLARIS, LINUX, AIX, HP-UX 등
판단기준	**양호** : Sendmail 버전이 최신버전인 경우
	취약 : Sendmail 버전이 최신버전이 아닌 경우
조치방법	Sendmail 서비스를 사용하지 않을 경우 서비스 중지, 재부팅 후 다시 시작하지 않도록 시작 스크립트 변경, 사용할 경우 패치 관리 정책을 수립하여 주기적으로 패치 적용

[그림. 3.3.1-1] kisa의 주요정보통신기반시설 기술적 취약점 가이드 U-30


학습개요

- 취약한 버전의 Sendmail을 이용하는 것은 원격 공격자가 시스템 권한을 얻을 수 있게 해주는 버퍼 오버플로우, 포맷 스트링 취약점, 디렉터리 리스팅 공격 등 다양한 공격에 취약합니다.
- Sendmail을 사용하는 경우 최신 버전으로 업그레이드하고 보안 업데이트를 주기적으로 진행 해주는것을 권고합니다.
- 따라서 취약한 버전의 Sendmail 서비스 이용 여부를 점검하고 최적화된 Sendmail 서비스를 운영하는 방법에 대해서 알아보겠습니다.

판단 기준은 다음과 같습니다.

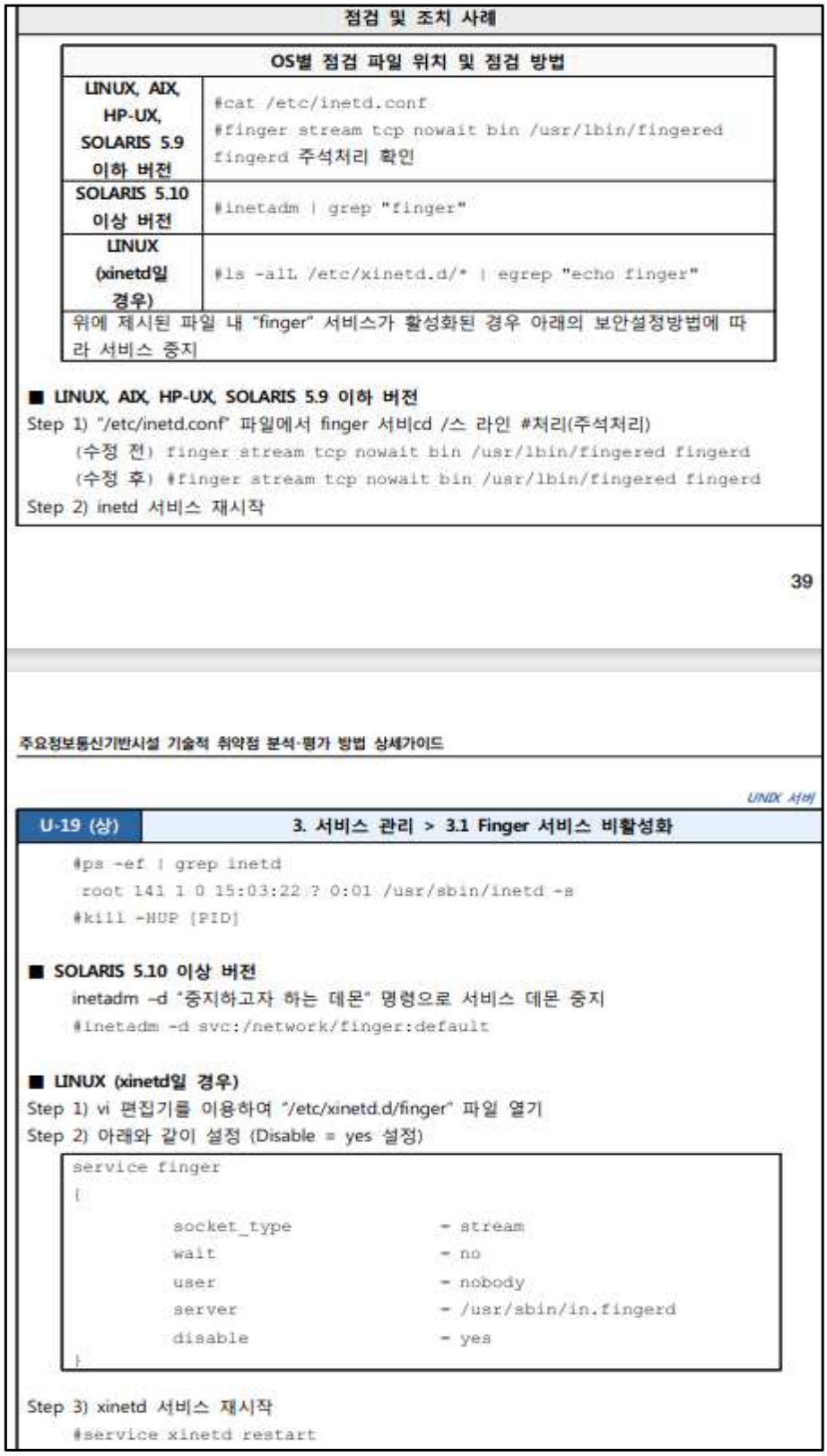
양호 : Sendmail 버전이 최신버전인 경우
취약 : Sendmail 버전이 최신버전이 아닌 경우

Sendmail 서비스의 경우 최신버전(2023.03 기준 8.17.1) 이하 대부분의 버전에서 취약점이 보고되고 있기 때문에 O/S 관리자, 서비스 개발자가 패치 적용에 따른 서비스 영향 정도를 정확히 파악하고 주기적인 패치 적용 정책을 수립하여 적용합니다.

[그림. 3.3.1-2] 학습사이트 적용 전 학습내용

[그림. 3.3.1-1]의 주통기 내용을 살펴보면 [그림. 3.3.1-2]에 비해 취약점에 대해 상세하게 기술되어 있지않다. 예를 들어 주통기에서는 버퍼 오버 플로우에 의한 공격만이 기술되어있는데 [그림. 3.3.1-2]의 경우 버퍼 오버플로우 외에도 포맷 스트링이나 디렉토리 리스팅 공격 등 버퍼 오버 플로우 뿐만 아니라 다양한 공격이 있음을 기술하였다.

또한 sendmail 버전이 2016년 기준으로 표시되어 있어 2023년 기준으로 모두 업데이트하였다.



점검 및 조치 사례

OS별 점검 파일 위치 및 점검 방법	
LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전	#cat /etc/inetd.conf #finger stream tcp nowait bin /usr/lbin/fingered fingerd 주석처리 확인
SOLARIS 5.10 이상 버전	#inetadm | grep "finger"
LINUX (xinetd일 경우)	#ls -alL /etc/xinetd.d/* | egrep "echo finger"
위에 제시된 파일 내 "finger" 서비스가 활성화된 경우 아래의 보안설정방법에 따라 서비스 중지	

■ LINUX, AIX, HP-UX, SOLARIS 5.9 이하 버전

Step 1) "/etc/inetd.conf" 파일에서 finger 서비cd /스 라인 #처리(주석처리)

(수정 전) finger stream tcp nowait bin /usr/lbin/fingered fingerd

(수정 후) #finger stream tcp nowait bin /usr/lbin/fingered fingerd

Step 2) inetd 서비스 재시작

39

주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드

UNIX 서버

U-19 (상) 3. 서비스 관리 > 3.1 Finger 서비스 비활성화

```
#ps -ef | grep inetd
 root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s
#kill -HUP [PID]
```

■ SOLARIS 5.10 이상 버전

inetadm –d "중지하고자 하는 데몬" 명령으로 서비스 데몬 중지

```
#inetadm -d svc:/network/finger:default
```

■ LINUX (xinetd일 경우)

Step 1) vi 편집기를 이용하여 "/etc/xinetd.d/finger" 파일 열기

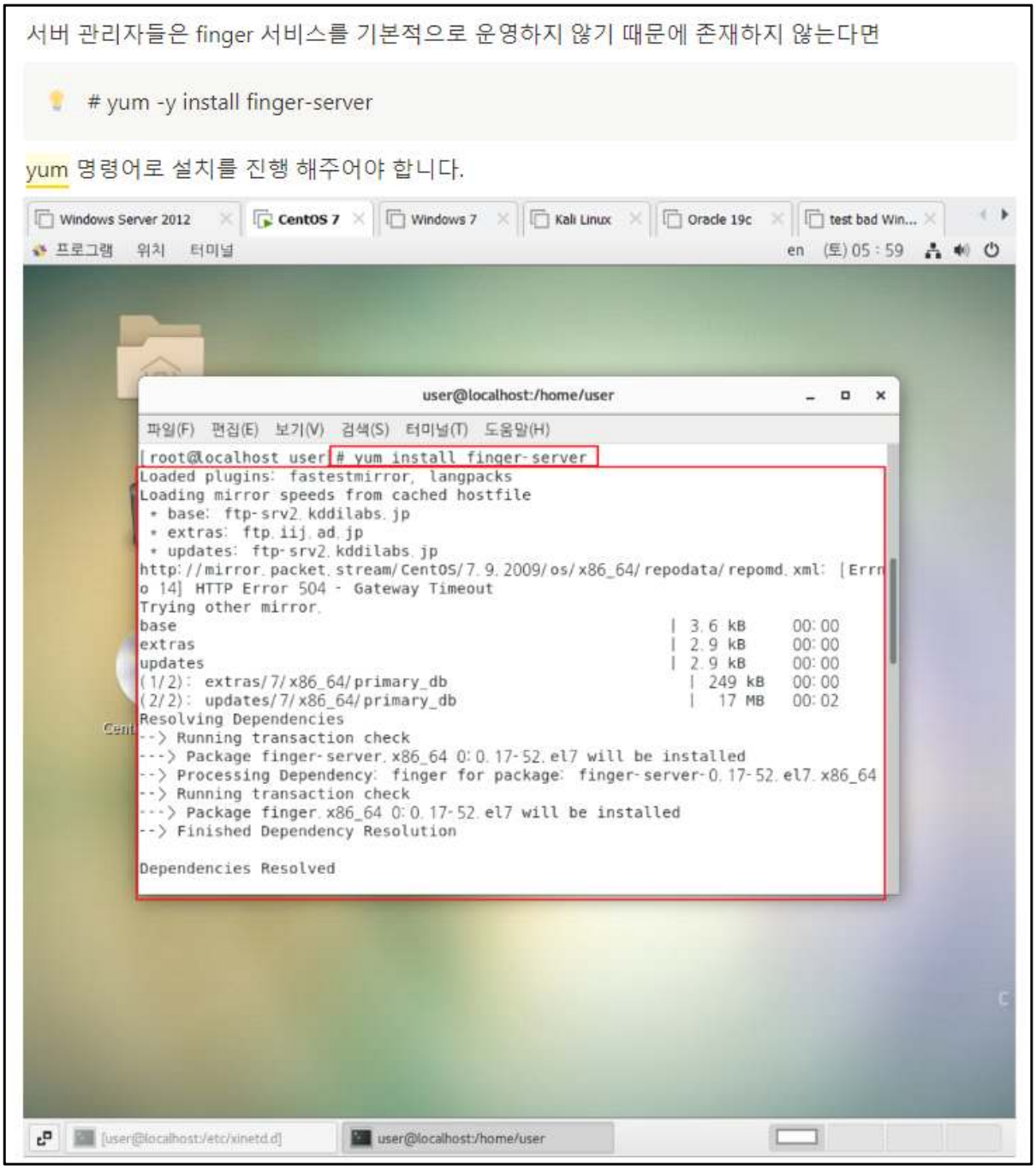
Step 2) 아래와 같이 설정 (Disable = yes 설정)

```
service finger
{
        socket_type             = stream
        wait                    = no
        user                    = nobody
        server                  = /usr/sbin/in.fingerd
        disable                 = yes
}
```

Step 3) xinetd 서비스 재시작

```
#service xinetd restart
```

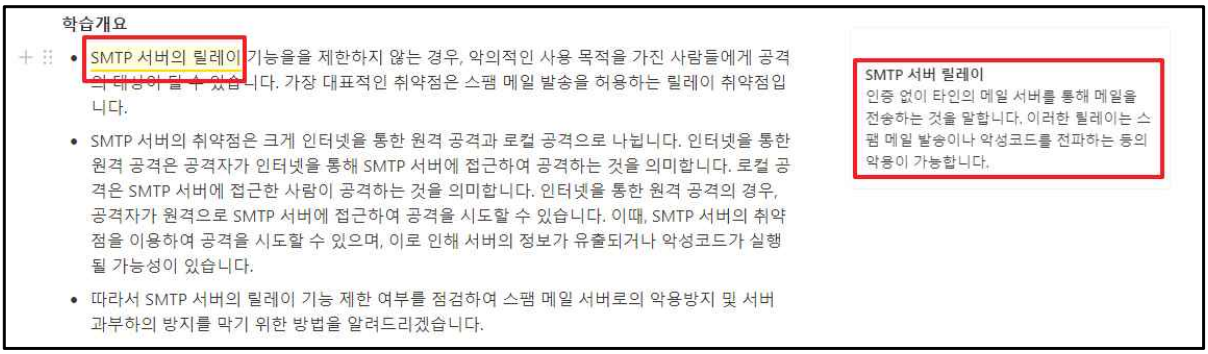
[그림. 3.3.1-3] kisa의 주요정보통신기반시설 기술적 취약점 가이드 U-19



[그림. 3.3.1-4] Finger 서비스 관련 Shell 스크립트 예시

"Finger 서비스 비활성화 항목 같은 경우 finger 서비스와 Xinetd 서비스를 모두 설치해야 하는데 주통에는 이런 설명이 되어있지 않아 처음 진단을 했을 때 헤맬 수 있기 때문에 설치 방법과 설명들을 추가하였다.

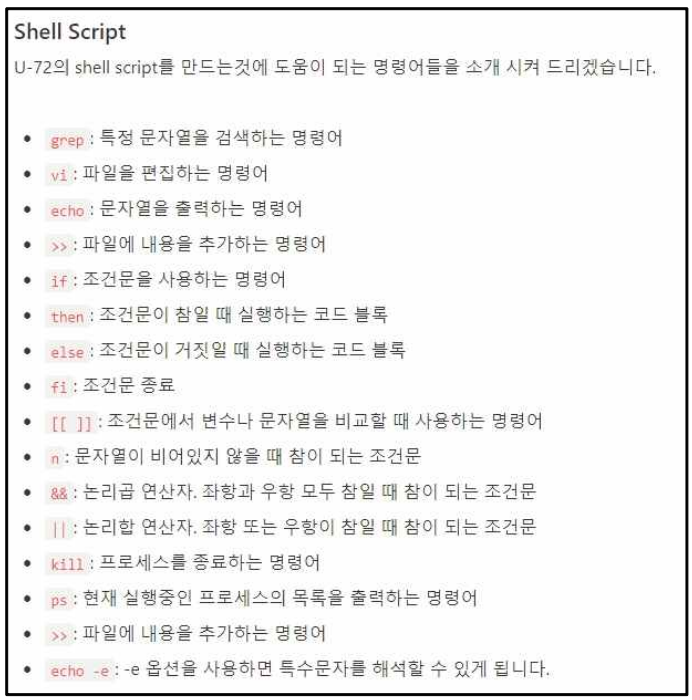
3.3.2 보안용어 설명기능



[그림. 3.3.2-1] 학습사이트 적용 전 단어 설명

보안 입문자들을 대상으로 제공하는 교육용 사이트에 맞게 보안 관련 용어에 대한 설명을 상세하게 제공하고, 쉽게 볼 수 있도록 제작하였다.

3.3.3 Script 명령어



[그림. 3.3.3-1] U-72 항목 Shell script 명령어

각 점검 항목별로 스크립트 제작에 도움이 되는 명령어를 제공하여 입문자들이 자동화 스크립트를 제작하는 것에 도움이 되도록 제작하였다.

3.3.4 Shell & Batch script 예시 제공

```
echo -e "[U-03] 계정 잠금 임계값 설정"

CF=/etc/pam.d/system-auth
DENY=$(grep "deny=" $CF | awk '{print $4}' | awk -F= '{if($2<6)print($0)}')

cat $CF >> U1~73/log/[U-03]log.txt

if [[ -n $DENY ]]; then
 echo -e "[U-03] 계정 잠금 임계값이 5이하의 값으로 설정되어 있음 - [양호]" >> U1~73/goo
d/[U-03]good.txt
else
 echo -e "[U-03] 계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되지 않음
- [취약]" >> U1~73/bad/[U-03]bad.txt
 echo -e "[U-03] 계정 잠금 임계값을 5 이하로 설정\n deny 값을 5 이하의 값으로 설정" >>
U1~73/action/[U-03]action.txt
fi
```

[그림. 3.3.4-1] U-03 shell script 예시

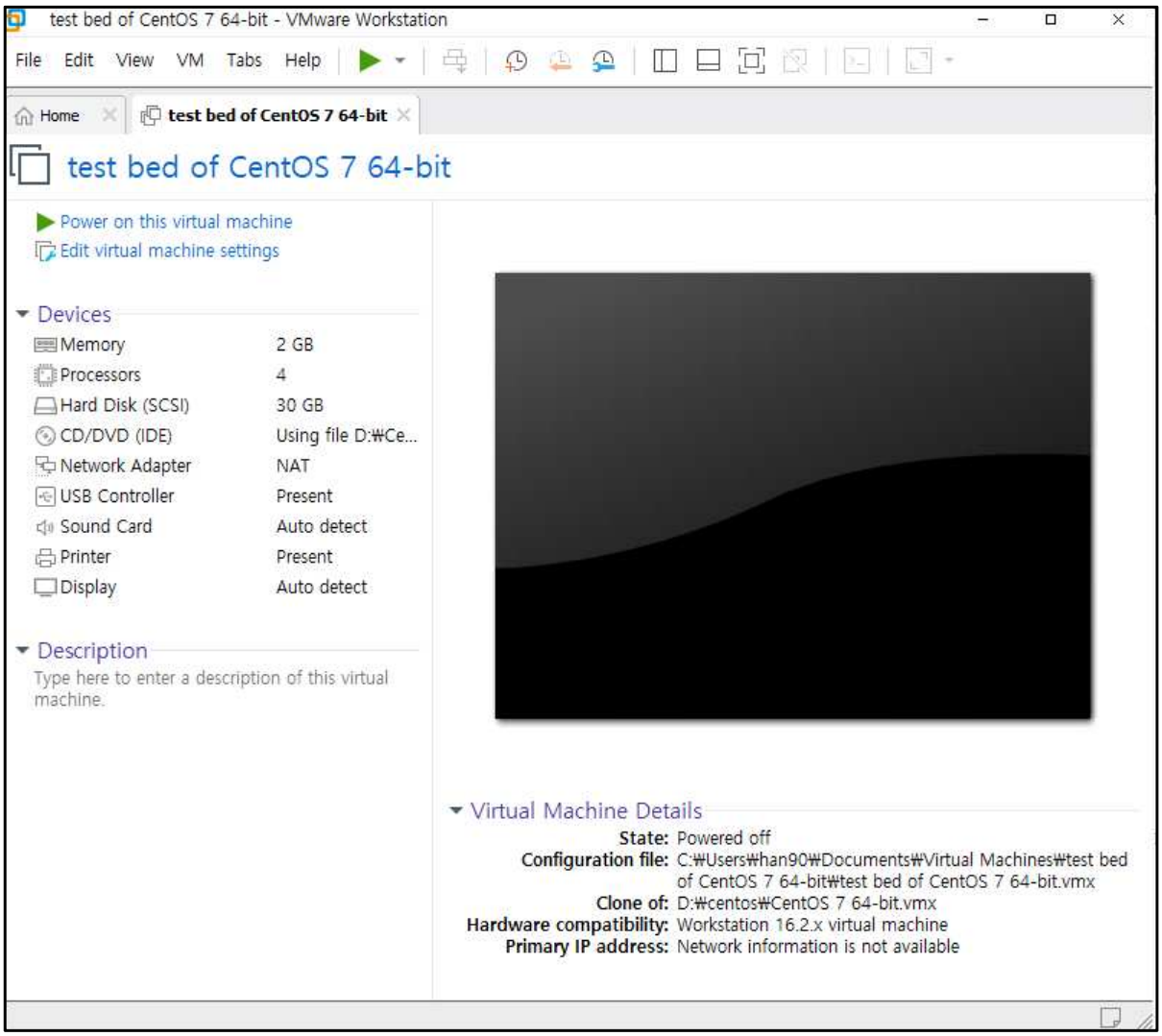
3.3.5 Shell & Batch script 설명 제공

- `echo -e "[U-03] 계정 잠금 임계값 설정"` : "[U-03] 계정 잠금 임계값 설정"이라는 문자열을 출력합니다.
- `CF=/etc/pam.d/system-auth` : 변수 `CF` 에 `/etc/pam.d/system-auth` 경로를 할당합니다.
- `DENY=$(grep "deny=" $CF | awk '{print $4}' | awk -F= '{if($2<6)print($0)}')` : `grep` 명령어를 사용하여 `CF` 파일에서 "deny=" 문자열을 찾아, 그 다음 문자열을 출력합니다. `awk` 명령어를 사용하여 출력 문자열의 네 번째 필드(콜론으로 구분된 필드)를 출력합니다. 그 다음 `awk` 명령어를 사용하여 출력 문자열을 "=" 기호로 구분하여 두 번째 필드의 값을 가져온 후, 5보다 작은 경우 출력 문자열 전체를 출력합니다. `DENY` 변수에 이 값을 할당합니다.
- `cat $CF >> U1~73/log/[U-03]log.txt` : `CF` 파일의 내용을 `U1~73/log/[U-03]log.txt` 파일 끝에 추가합니다.
- `if [[ -n $DENY ]]; then` : `DENY` 변수가 비어 있지 않은 경우, 아래의 코드 블록을 실행합니다.
- `echo -e "[U-03] 계정 잠금 임계값이 5이하의 값으로 설정되어 있음 - [양호]" >> U1~73/good/[U-03]good.txt` : "[U-03] 계정 잠금 임계값이 5이하의 값으로 설정되어 있음 - [양호]"라는 문자열을 `U1~73/good/[U-03]good.txt` 파일 끝에 추가합니다.
- `else` : `DENY` 변수가 비어 있는 경우, 아래의 코드 블록을 실행합니다.
- `echo -e "[U-03] 계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되지 않음 - [취약]" >> U1~73/bad/[U-03]bad.txt` : "[U-03] 계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되지 않음 - [취약]"이라는 문자열을 `U1~73/bad/[U-03]bad.txt` 파일 끝에 추가합니다.

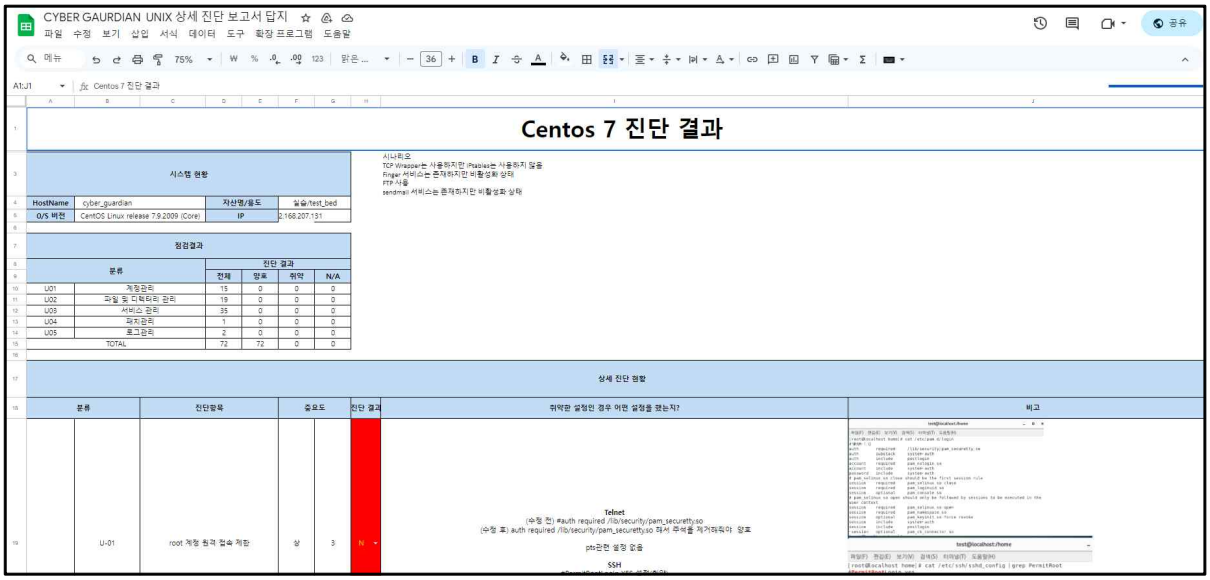
[그림. 3.3.5-1] Shell & Batch script 상세 설명

윈도우의 batch, 리눅스의 shell 스크립트와 이에 대한 설명도 기술되어 있어 학습한 내용을 기반으로 학습자가 취약점을 진단하는 스크립트를 작성하는 데 도움을 줄 수 있다.

3.3.6 Testbed 제공 및 실습 답안지 제공



[그림. 3.3.6-1] CentOs testbed 사진

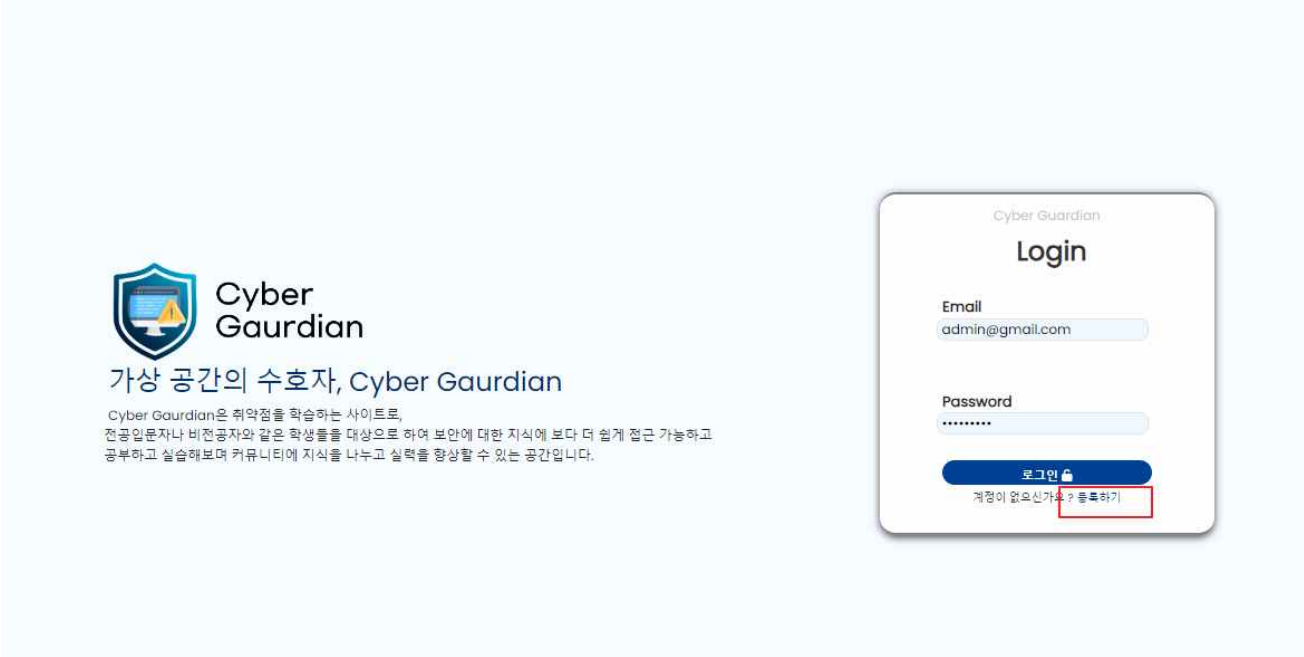


[그림. 3.3.6-2] 실습 파일 답안

작성한 스크립트를 가지고 학습 사이트에서 제공하는 testbed 파일을 통해 제공된 환경에서 실습해보며 답안과 비교해보고 이후에도 취약점 관련된 질문이나 정보를 주고받을 수 있는 게시판까지 운영하여 학습에 더욱 도움이 될 것이다.

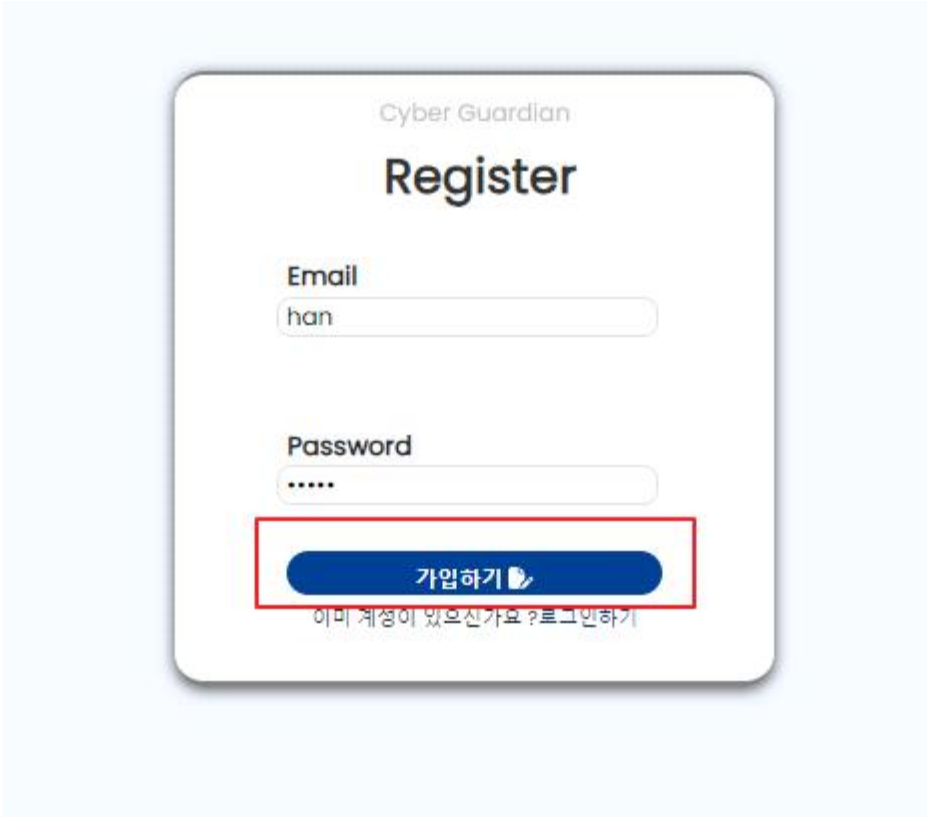
4. 활용

4.1 실제 활용 예시



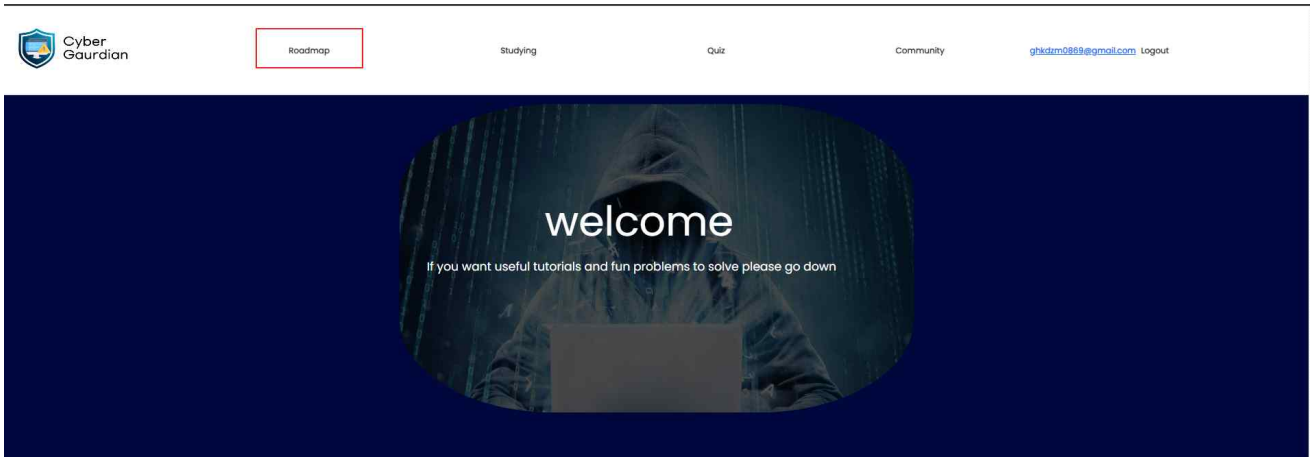
[그림. 4.1-1] 첫 로그인 시 보여지는 Login & Register 페이지

먼저 사이트를 사용하기 위해 회원등록을 한다.



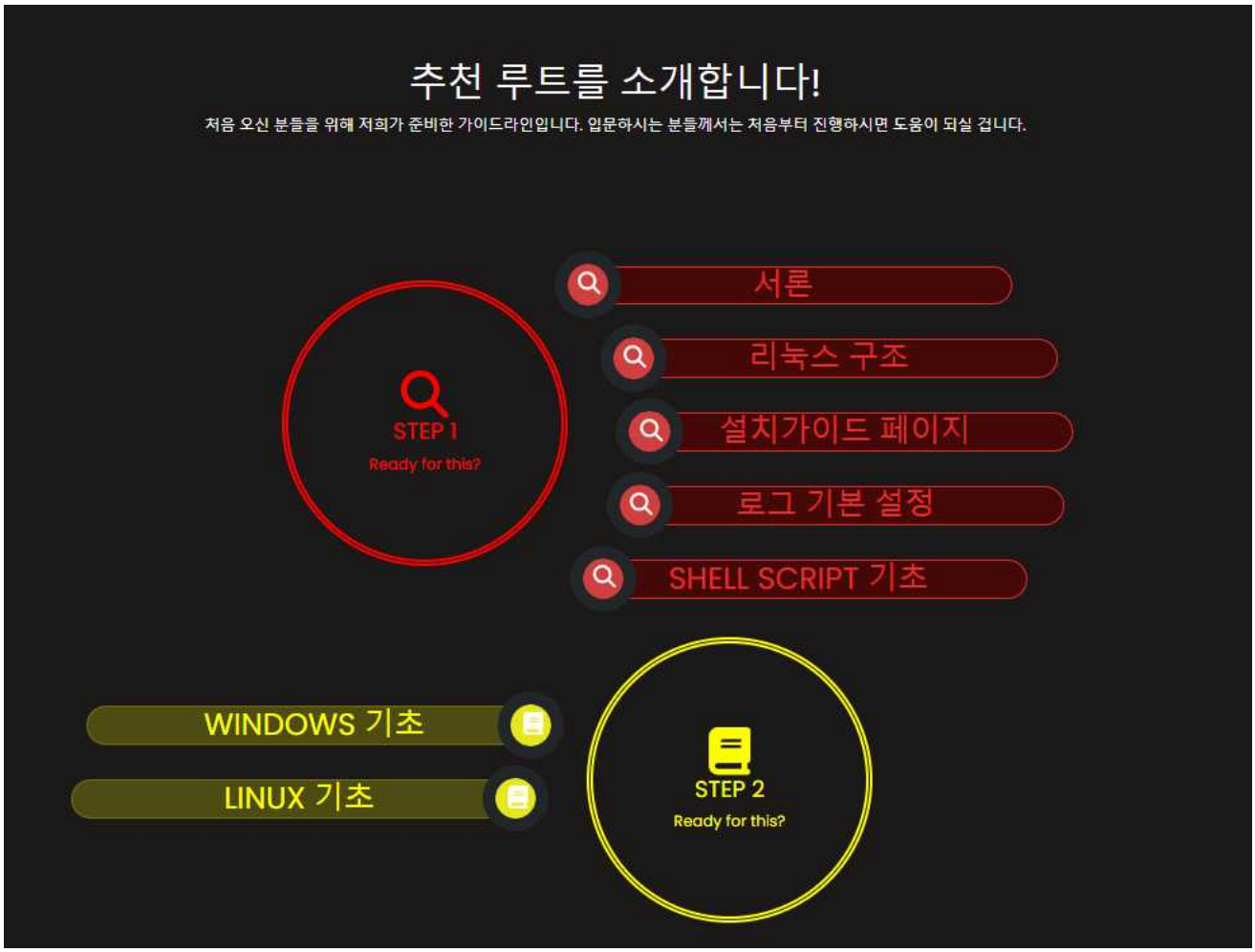
[그림. 4.1-2] 회원가입 예시

아이디와 패스워드 입력 후 가입을 진행한다.



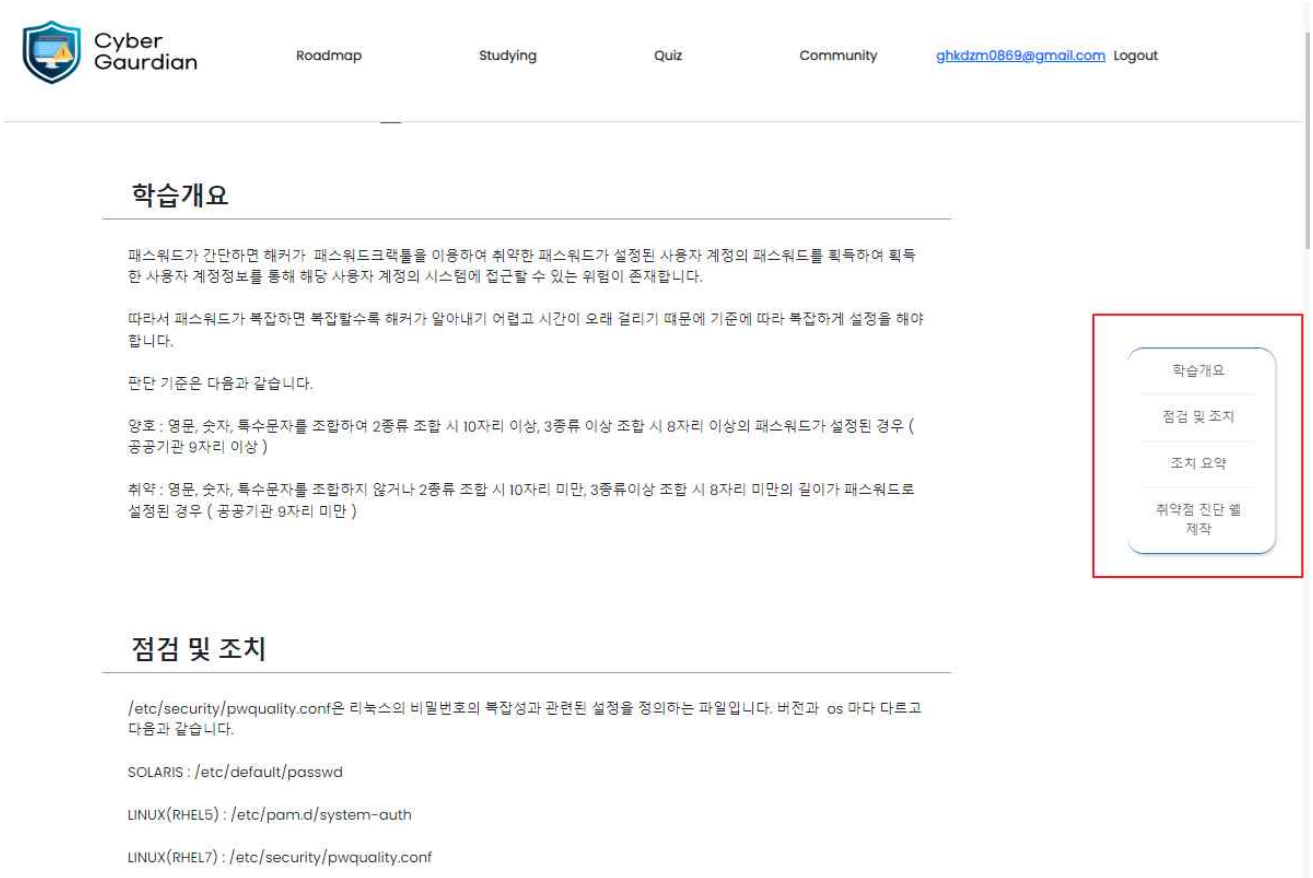
[그림. 4.1-3] roadmap 페이지 접속 방법 안내

사이트 좌측 상단의 로드맵을 클릭



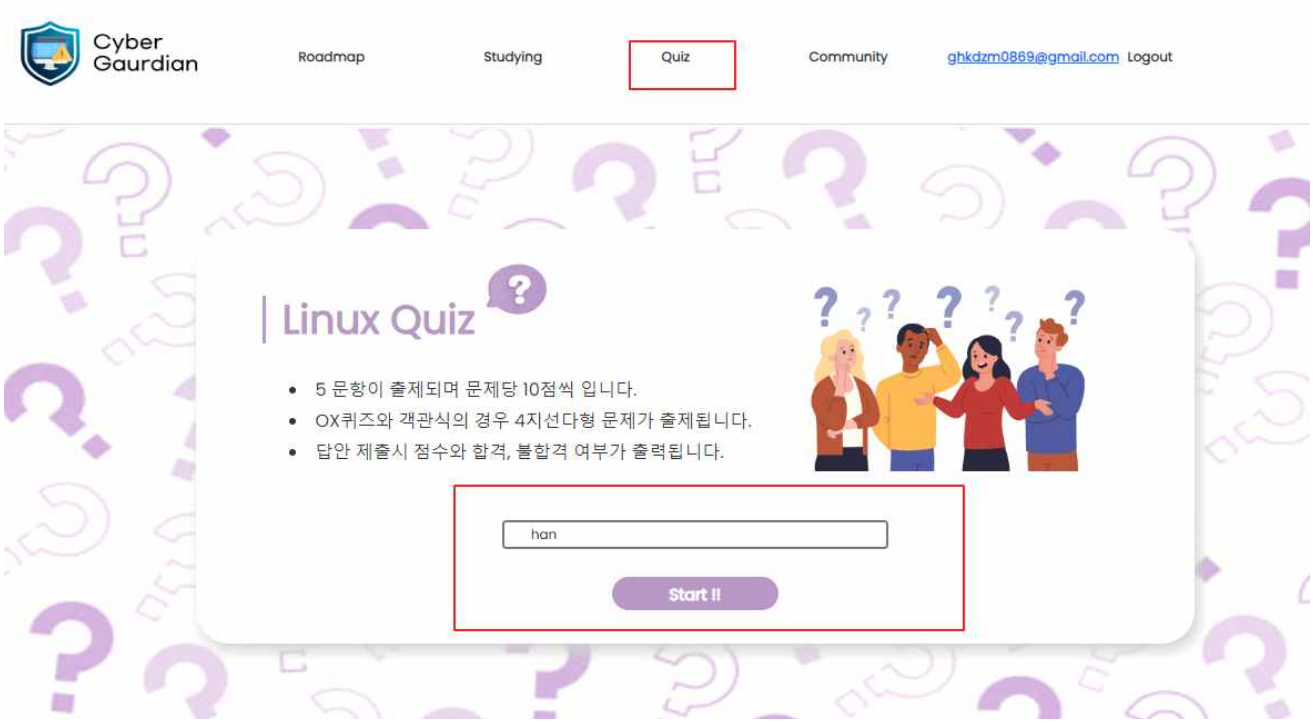
[그림 4.1-4] Roadmap 페이지

위에서부터 로드맵대로 차근차근 교육을 진행할 수 있다.



[그림. 4.1-5] 학습자료 페이지 세부

학습자료에 접속한 페이지이다. 우측의 목차를 누르면 스크롤을 위아래로 내릴 필요 없이 해당 내용으로 스크롤이 자동 이동한다.



[그림. 4.1-6] Linux Quiz 메인 페이지

학습자가 학습을 완료한 후 자신의 학습 성취도를 확인하기 위해 문제를 풀 수 있다. 이름을 입력하고 start 버튼을 누르면 문제를 풀 수 있다.

[그림. 4.1-7] Windows Quiz 문제풀이 페이지

문제는 다음과 같이 4지 선다형의 객관식 문제로 답안을 체크하여 문제를 풀 수 있고, Next버튼을 눌러 다음 문제로 넘어갈 수 있다.

[그림. 4.1-8] Result 페이지

문제를 다 풀게 되면 다른 이용자의 점수도 확인할 수 있으며 어느 정도 이상의 문제를 맞혀야만 passed를 받아 자신의 학습 성취를 체감할 수 있다.

Test Bed의 설정 및 기본 정보

기본 설정

학생들과 교류하는 학습 서비스를 제공하는 서버

기본적으로 IIS로 사이트 상에서 학생들에게 필요한 자료를 제공, 및 과제를 받음

이런 자료의 교환은 FTP로 이루어지고 있음

관리를 위해 DNS 서버를 운영 중 - client 불필요 - 이외에도 client이름을 가진 서비스 불필요

SNMP 서비스는 운영중이라면 필요, 아니라면 불필요 하다 정의

메일을 통해 건의를 받고 있기에 SMTP서버 운영 중 - 관련 항목 점검 필요

inetpub 내의 important 폴더는 유출 및 변조되면 안되기에 관리자만 접근가능해야함

inetpub 내의 업무 폴더에 업무 관련 자료가 있음

2022/10/10을 기준으로 함 - 로그 보고서 같은 항목이 2022/10/10까지 없으면 취약으로 판단

계정 종류

administrator (JBadmin) - 관리자 계정 - PW : admin

Professer - 교수 계정 - pro

student - 학생 계정 - stu

notuse - 비사용 계정으로 존재 시 취약으로 판단

test - test

guest

IP 별 허용 및 거부

서버 IP - 192.168.31.131

허용 IP - 192.168.31.96~128 (교수들의 IP) - 192.168.31.96 서브넷 : 255.255.255.224
192.168.31.224~255 (학생들의 IP) - 192.168.31.224 서브넷 : 255.255.255.224

- 허용 IP를 제외한 IP는 모르는 사용자로 위험하다 판단 - 허용되면 안됨

거부 IP - 192.168.31.144 - 과거 공격이 들어온 적 있는 공격자 IP

100.200.144.0~255 - 공격자로 추측되는 위험 IP

[그림. 4.1-9] Testbed실습 학습자료

또한 testbed 실습을 통해 실제 실무와 같이 취약한 os를 직접 진단해 보며 보안 전문가로서 한걸음 나아갈 수 있다.

[그림. 4.1.-10] Testbed 자료실 페이지

testbed 파일은 'Testbed' 페이지에서 다음 링크를 클릭하여 다운로드할 수 있다.

5. 결론

5.1 결론

취약점 진단에 처음 입문하는 비전공자와 학생들이 효율적으로 공부할 수 있게 사이트를 구성하였고, 학습자는 취약점 학습 내용을 보고 이해하는 데에 그치지 않고 다양한 문제를 통해 문제해결 능력을 높이고 시스템에서 잠재적인 보안 위험을 파악하며 필요한 예방 조치를 취할 수 있을 것이다. 또한 윈도우의 batch, 리눅스의 shell 스크립트 작성에 대한 내용도 기술되어 있어 학습한 취약점에 관한 내용을 기반으로 취약점을 자동 진단하는 스크립트를 작성할 수 있다. 작성한 스크립트를 가지고 학습 사이트에서 제공하는 testbed 파일을 통해 제공된 환경에서 실습해보며 답안과 비교해 볼 수 있다. 이후에도 취약점 관련된 질문이나 정보를 주고받을 수 있는 게시판도 운영하였다.

5.2 기대 효과

기존 '주요 정보 통신 기반 시설 기술적 취약점 평가 가이드'는 취약점에 대한 조치만이 적혀있고 자세한 내용이 기술되어 있지 않아 초심자가 보았을 때 이해도가 낮을 것으로 보인다. 따라서 '웹으로 공부하는 취약점 마스터'는 취약점을 처음 접하는 사람들의 눈높이에 맞게 커리큘럼을 제작하여 취약점에 대한 진입장벽을 낮출 수 있을 것으로 예상한다. 취약점 관련된 질문이나 정보를 주고받을 수 있는 게시판도 운영하여 학습자들이 다른 학습자들과 원활한 소통을 통해 지식을 공유하는 선순환을 할 수 있을 것으로 예상한다.

6. 별첨

6.1 소스코드

6.1.1. 웹 소스코드(github)

https://github.com/withsjb/front (손진빈,박유찬)

https://github.com/withsjb/back (손진빈)

6.1.2. 배치 스크립트코드

https://jewel-peanut-1ef.notion.site/Windows-Server-9b330061e8a74570bb33c39c7bec2510?pvs=4(한현동, 이정훈 한완섭)

6.1.3. 쉘 스크립트 코드

https://jewel-peanut-1ef.notion.site/CentOS-7-Shell-Script-ffeaa78b50244328bc0d102a22e91af9?pvs=4 (한현동, 이정훈 한완섭)

6.2 웹사이트 링크

https://cybergaurdian.vercel.app

6.3 팀원소개

손진빈 91812505 web front & back 담당

박유찬 91812373 web front 담당

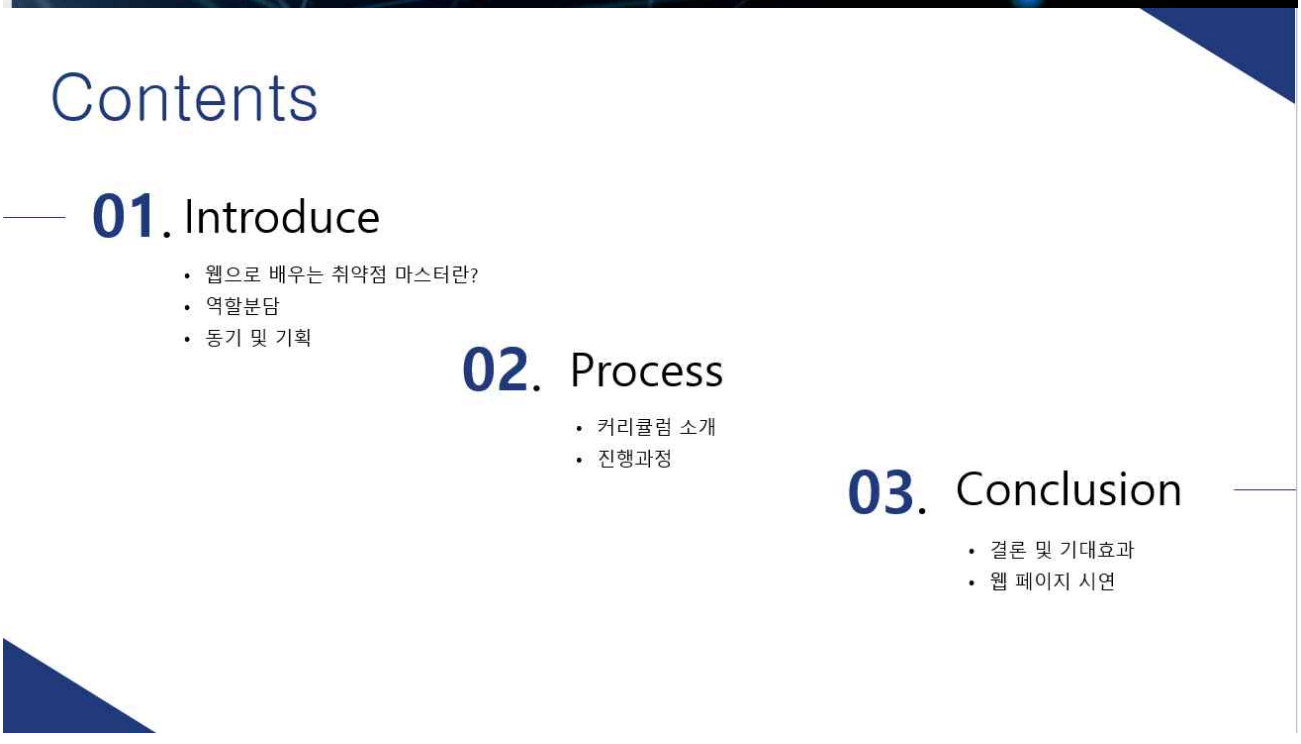
한현동 91813262 취약점 커리큘럼 담당

이정훈 91812945 취약점 커리큘럼 담당

한완섭 91914420 취약점 커리큘럼 담당

6.4. 발표 자료

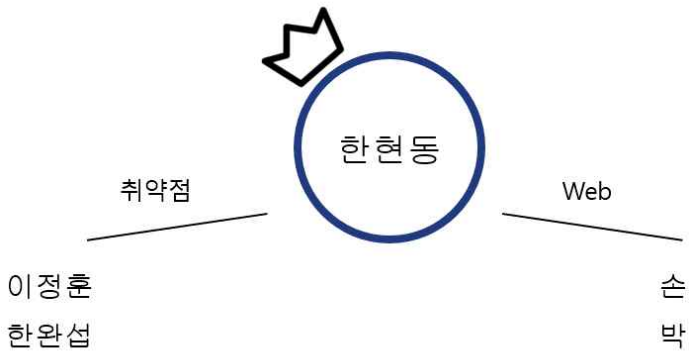

웹으로 배우는
취약점 마스터
Cyber Guardian
Team.답은 정해져있다
한현동
이정훈
한완섭
박유찬
손진빈


Contents
01. Introduce
• 웹으로 배우는 취약점 마스터란?
• 역할분담
• 동기 및 기획
02. Process
• 커리큘럼 소개
• 진행과정
03. Conclusion
• 결론 및 기대효과
• 웹 페이지 시연

01. 웹으로 배우는 취약점 마스터란?

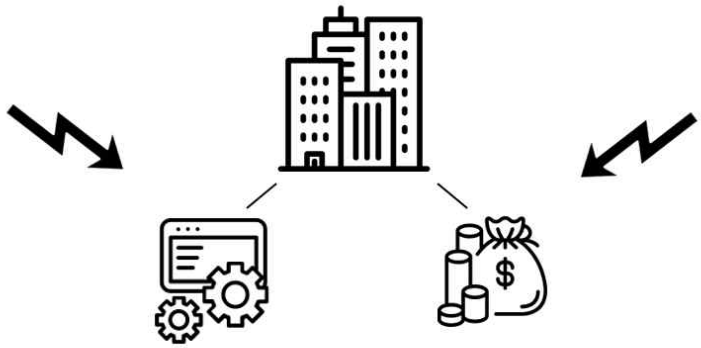
'주요통신기반시설 기술적 취약점 분석 평가 방법 상세가이드'를 기반으로 학습하여
실무에서 원활한 취약점 진단을 할 수 있는 능력을 함양시키는 학습사이트입니다.

01. 역할 분담



이번 프로젝트는 팀장 한현동을 축으로 이정훈, 한완섭은 취약점 팀으로 취약점 커리큘럼 및 문제 작성,다음은 웹팀으로 손진빈은 Frontend와 Backend 개발을,
저는 UI/UX, CSS개발과 발표를 맡아 진행되었습니다.

01. 동기 및 기획

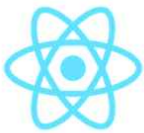


기업은 그들만의 유・무형의 자산을 가지고 있고,
이 자산들은 해킹 및 바이러스의 위험에 노출되어 있습니다.
따라서 대부분의 기업은 '주통기 가이드' 내용을 토대로 정기적인 취약점 점검을 받아야 합니다.

01. 동기 및 기획

이러한 취약점들에 대해 공부하여 바이러스로 부터 지킬 수 있는 능력을 함양하고자
취약점에 관심이 있는 전공 입문자 또는 비 전공자들을 대상으로 하는
학습사이트를 제작하기로 하였습니다.

01. 기획 [개발환경]



개발 환경으로는 MERN으로 불리는 'MongoDB, Express, React, node js'과
배포한정으로는 frontend는 vercel, backend는 cloud type를
이용하여 프로젝트 개발을 진행하였습니다.

02. 커리큘럼 소개

Curriculum

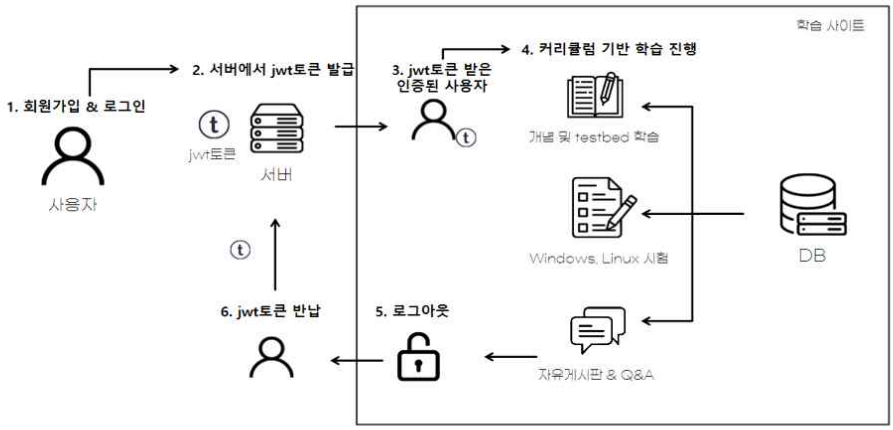
- 기초개념
- OS (Windows, Linux)
  양호 및 취약 기준안내
  진단방법
  조치 방법 등
- 배치 파일 스크립트(.bat)
- testbed 실습

Web page

- 이론 및 가이드
- 문제풀이 Quiz
- 취약점 단어장
- 자유게시판, Q&A
- 자료실

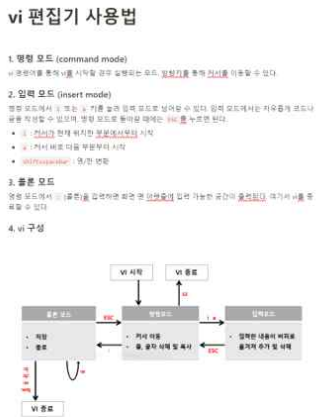
이번 프로젝트의 세부적인 기획 내용입니다.
저희가 직접 작성한 커리큘럼과 그 내용들을 학습할 수 있게 웹 페이지를 구성하였습니다.

02. 커리큘럼 소개 [구상도]



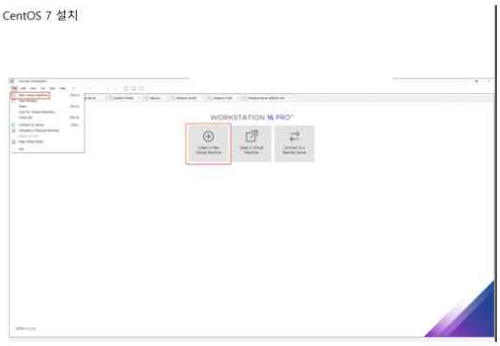
이용자는 로그인 > 사이트 안내 > 학습 > testbed를 통한 실습 > 시험 > 게시판 이용하여
학습자는 취약점에 대한 이해를 높일 수 있고, 시스템에서 잠재적인 보안 위험을 파악하며
필요한 예방 조치를 취할 수 있는 효과를 기대하고 있습니다.

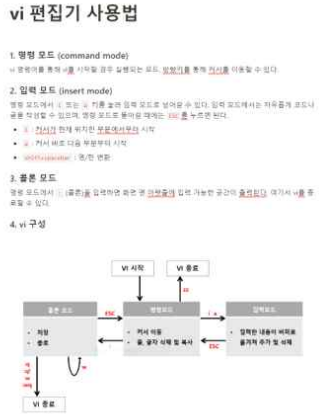
02. 진행과정 [기초개념 정리1]



기초개념 내용들 입니다.
좌측 내용은 testbed 실습환경 제작에 대한 이미지이고,
우측 내용은 Linux의 vi 편집기 사용법에 대한 설명입니다.

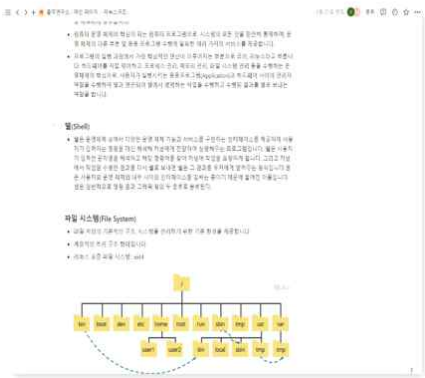
02. 진행과정 [기초개념 정리1]





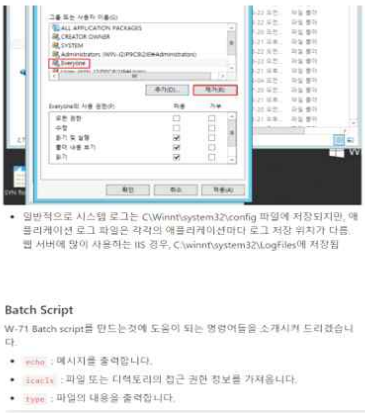
기초개념 내용들 입니다.
좌측 내용은 testbed 실습환경 제작에 대한 이미지이고,
우측 내용은 Linux의 vi 편집기 사용법에 대한 설명입니다.

02. 진행과정 [기초개념 정리2]



Notion에 정리된 기초개념 내용들 입니다.
좌측 내용은 Linux의 구조(Shell과 File System)에 대한 설명이고,
우측 내용은 Linux의 Shell scripts에 대한 설명입니다.

02. 진행과정 [학습내용 정리]

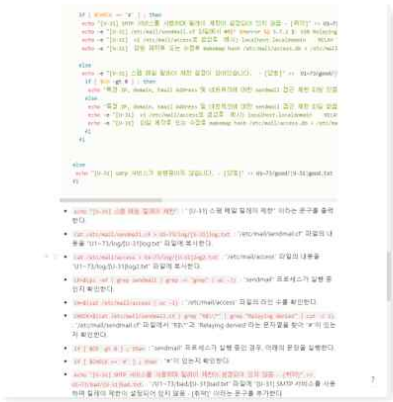


- 일반적으로 시스템 로그는 C:\Winnt\system32\config 파일에 저장되지만, 애플리케이션 로그 파일은 각각의 애플리케이션마다 로그 저장 위치가 다름. 웹 서버에 많이 사용하는 IIS 경우, C:\winnt\system32\LogFiles에 저장됨

Batch Script

W-71 Batch script를 만드는것에 도움이 되는 명령어들을 소개시켜 드리겠습니다.

- `echo` : 메시지를 출력합니다.
- `icacls` : 파일 또는 디렉토리의 접근 권한 정보를 가져옵니다.
- `type` : 파일의 내용을 출력합니다.

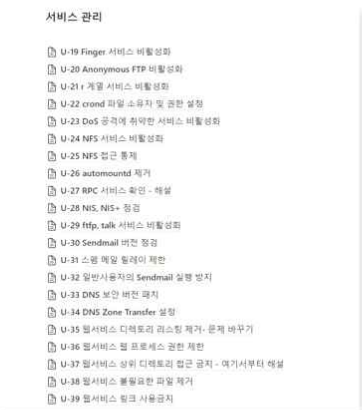


Notion에 정리된 OS 학습내용들 입니다.

좌측 내용은 Windows의 Batch file scripts에 대한 설명이고,

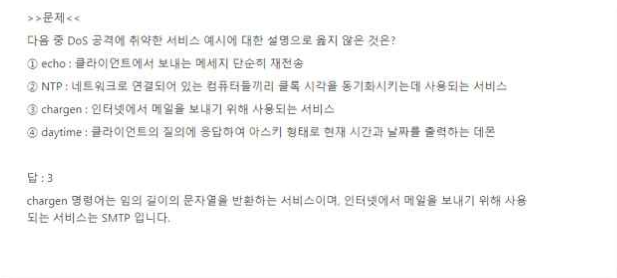
우측 사진은 직접 작성한 리눅스 취약점 진단 스크립트 및 해설입니다.

02. 진행과정 [학습내용 list]



서비스 관리

- U-19 Finger 서비스 비활성화
- U-20 Anonymous FTP 비활성화
- U-21 r 계열 서비스 비활성화
- U-22 crond 파일 소유자 및 권한 설정
- U-23 DoS 공격에 취약한 서비스 비활성화
- U-24 NFS 서비스 비활성화
- U-25 NFS 접근 통제
- U-26 automountd 제거
- U-27 RPC 서비스 확인 - 해설
- U-28 NIS, NIS+ 점검
- U-29 ftfp, talk 서비스 비활성화
- U-30 Sendmail 버전 점검
- U-31 스팸 메일 릴레이 제한
- U-32 일반사용자의 Sendmail 실행 방지
- U-33 DNS 보안 버전 패치
- U-34 DNS Zone Transfer 설정
- U-35 웹서비스 디렉토리 리스팅 제거- 문제 바꾸기
- U-36 웹서비스 웹 프로세스 권한 제한
- U-37 웹서비스 상위 디렉토리 접근 금지 - 여기서부터 해설
- U-38 웹서비스 불필요한 파일 제거
- U-39 웹서비스 링크 사용금지



>>문제<<

다음 중 DoS 공격에 취약한 서비스 예시에 대한 설명으로 옳지 않은 것은?

① echo : 클라이언트에서 보내는 메세지 단순히 재전송

② NTP : 네트워크로 연결되어 있는 컴퓨터들끼리 클록 시각을 동기화시키는데 사용되는 서비스

③ chargen : 인터넷에서 메일을 보내기 위해 사용되는 서비스

④ daytime : 클라이언트의 질의에 응답하여 아스키 형태로 현재 시간과 날짜를 출력하는 데몬

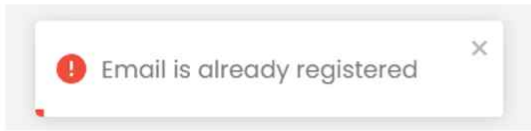
답 : 3

chargen 명령어는 임의 길이의 문자열을 반환하는 서비스이며, 인터넷에서 메일을 보내기 위해 사용되는 서비스는 SMTP 입니다.

이러한 내용들은 '주통기 가이드'의 내용을 토대로 항목별로 정리 되어있습니다.

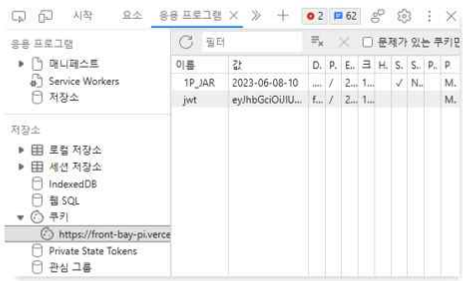
추가적으로 우측 사진과 같이 각 항목별 내용 설명 이후 문제도 포함되어 있습니다.

02. 진행과정 [Login & Register]



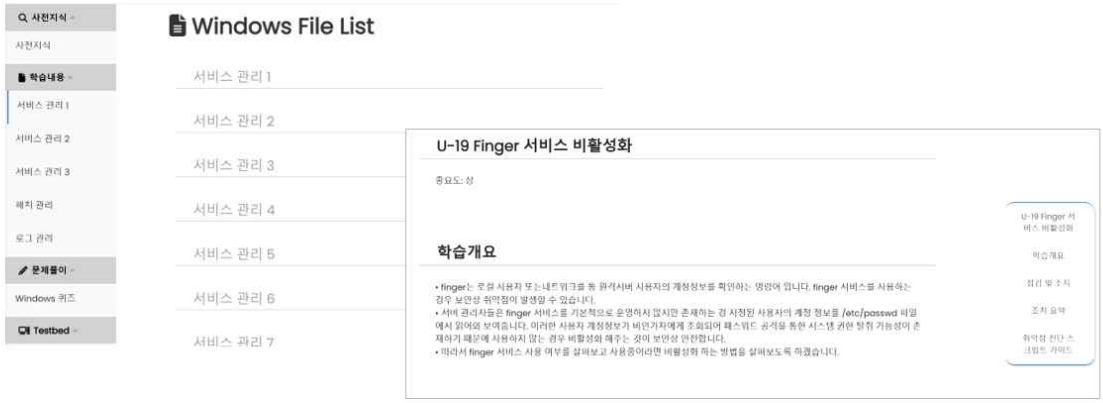
회원가입 페이지에서 Email 형식에 맞게 작성해야 가입이 가능하며
해당 ID 가 이미 있을 때에는 react-toastify 메세지가 우측 하단에 표시됩니다.

02. 진행과정 [로그인 구현]



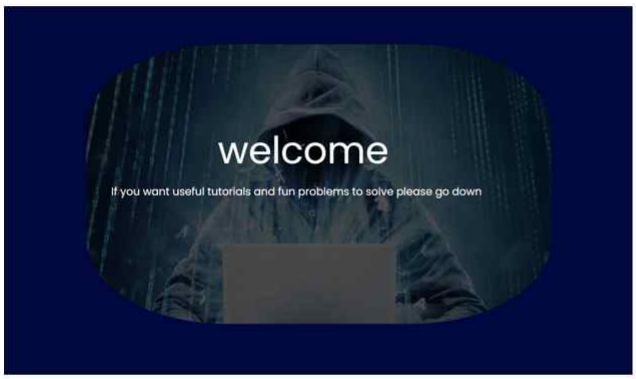
로그인 페이지에서 로그인을 완료하게 되면 사용자는 jwt토큰을 통해 인증을 받아
사이트에 접속하게 되고 Password에 대한 정보는 암호화되어 저장됩니다.

02. 진행과정 [이론 및 가이드]



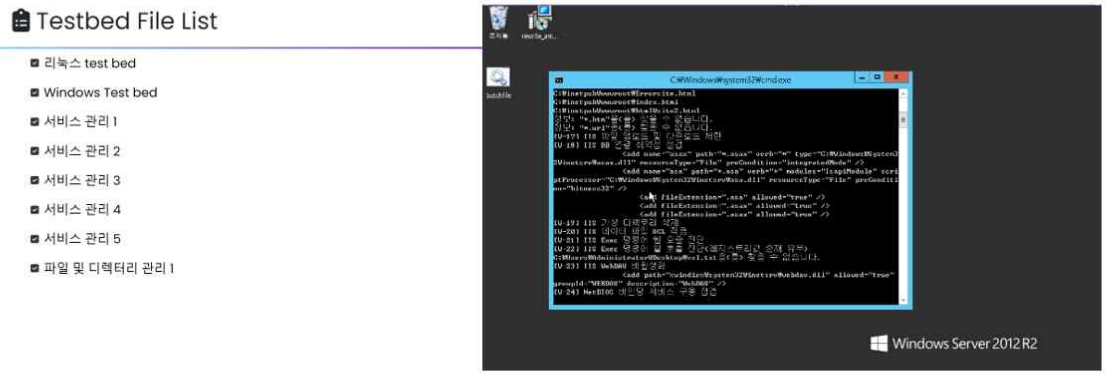
Notion에서 정리한 내용들을 바탕으로 학습할 수 있는 페이지입니다.
사전지식, 각 OS에서 필요한 지식들, 문제풀이, 실습 파일인 testbed도 제공됩니다.

02. 진행과정 [Roadmap]



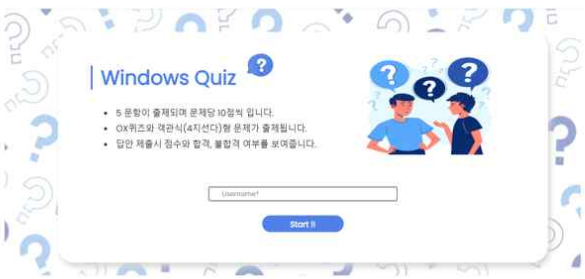
처음 접속했을 때 보여지는 메인 페이지와
로드맵을 통해서 저희 사이트를 이용할 때의 안내를 제공하고 있습니다.

02. 진행과정 [Testbed]



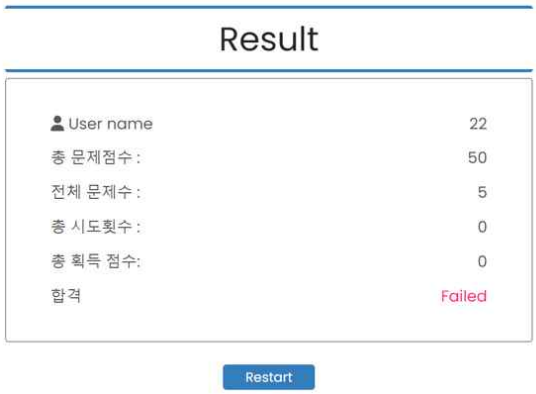
실습을 위한 자료를 다운로드받는 testbed 자료실 입니다.
해당 링크를 클릭하여 testbed를 다운로드 받고
개인 VMware환경에서 실습을 진행 할 수 있습니다.

02. 진행과정 [Quiz page] – Windows Quiz페이지



앞서 커리큘럼에서 제시한 내용들을 학습한 후에
퀴즈를 통하여 학습한 내용을 확인해보는 컨텐츠도 추가하였습니다.

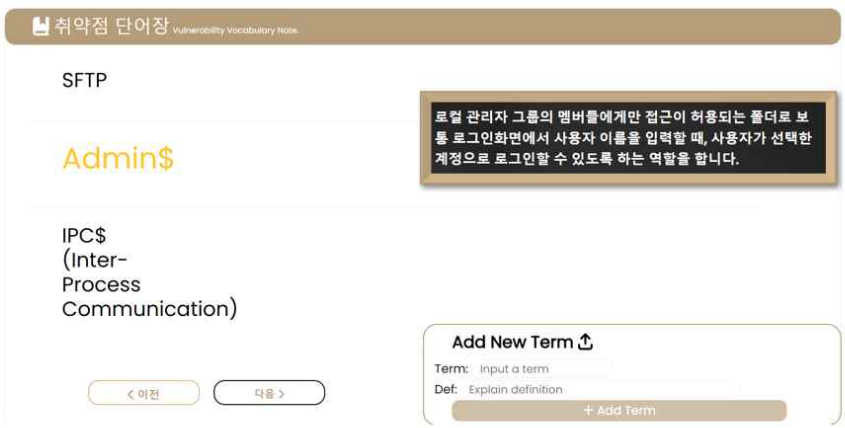
02. 진행과정 [결과]

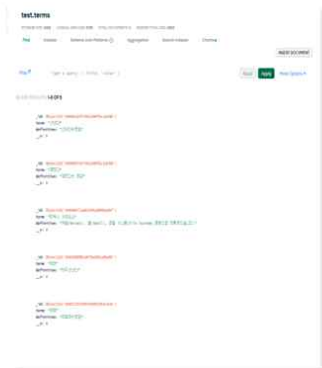


Name	Attemps	Earn Points	Result
kfkf	3	30	Passed
dd	5	20	Failed
dasgasdga	3	20	Passed

문제를 다 푼 뒤에는 총 문제점수, 전체 문제 수, 시도횟수, 취득점수와 합격 여부가 출력되며,
Restart 버튼을 통해 다시 도전하실 수도 있습니다.
하단에는 학습자들간에 점수와 합격여부를 확인하실 수 있습니다.

02. 진행과정 [취약점 단어장]





취약점에 대한 내용을 처음 공부를 시작할 때 접하게 되는 용어들이 생소할 수 있기에
'취약점 단어장'을 통하여 용어와 정의를 제공하여 공부에 도움이 되고자 하였습니다.
학습페이지에서는 마우스 호버기능을 통해 모달창이 출력되어 단어장에 등록된 설명이 나오게 됩니다.

02. 진행과정 [자유게시판]

저희 사이트를 이용중인 학습자들 간의 자유로운 소통을 위한 자유게시판 입니다.
작성자명, 작성일, 글 제목과 내용, 추천과 댓글 기능까지 구현하였습니다.

03. 결론 및 기대효과

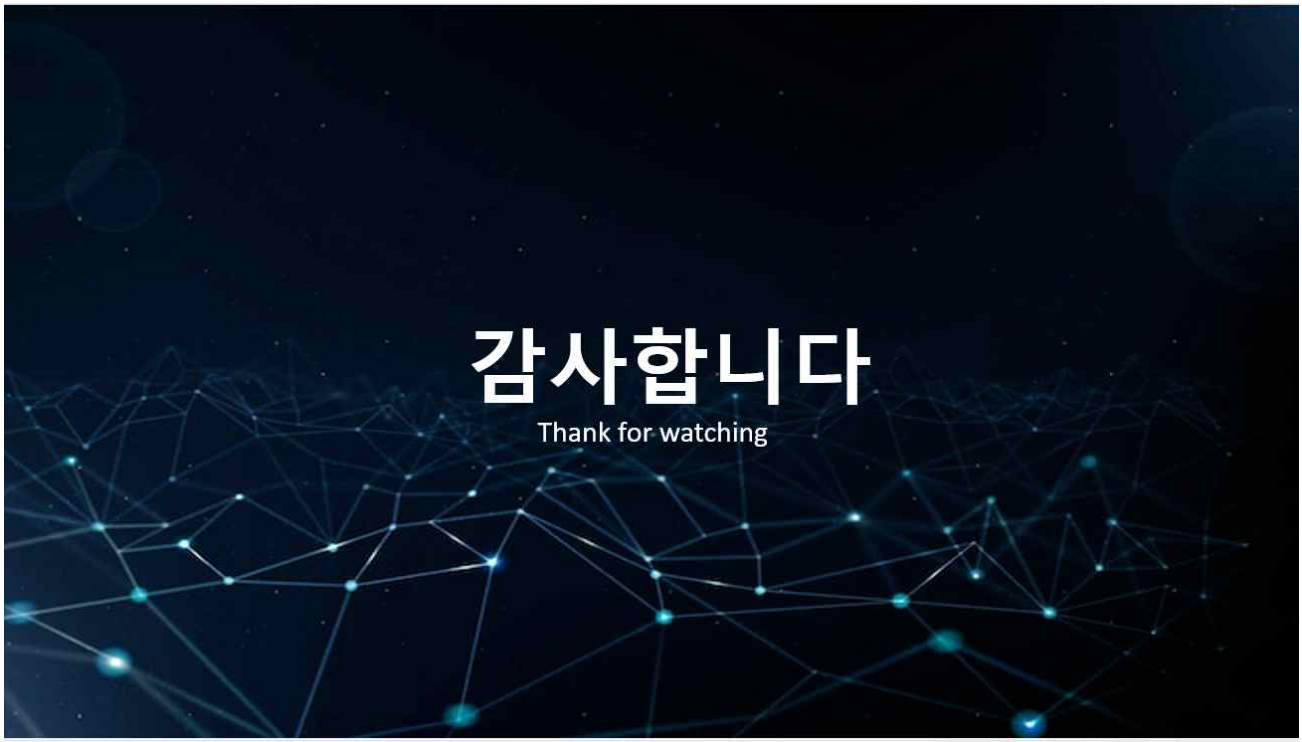
Conclusion

- 기초적인 OS라고 할 수 있는 Windows와 Linux(centOS 7)에 대해서 취약점에 대해 차근차근 배워 볼 수 있는 학습사이트를 제작하였다.

Expectation Effectiveness

- 직접 구성한 취약점 커리큘럼에 맞춰 공부를 진행한다면 실무에서 응용해서 취약점에 대해 보완할 수 있을 것

- 취약점에 대해 관심이 있는 초심자들의 눈높이에 맞춰서 제작하였기에 쉽고 부담없이 접근할 수 있어 많은 이용자들이 늘어날 것으로 예상된다.


감사합니다
Thank for watching