

주요 프로젝트 소개

1. UNIX 서버 취약점 진단

기 간	➢ 2018.4.16 ~ 2018.5.31
사용 기술	➢ VMware, CentOS
목 표	➢ '주요정보통신기반 취약점 분석평가 기준'을 토대로 UNIX 서버 취약점 진단

- 분석 결과 보고서

2.2.2. 서버 영역별 보안수준

UNIX 서버의 영역별 보안수준은 계정관리(85%), 서비스관리(93%)로 “양호”, “우수”로 평가되었으며 파일 및 디렉토리 관리(65%), 패치 및 로그 관리(74%) 영역은 영역별 평균 점수보다 낮은 점수로 분석·평가됨

영역	평균 보안수준 (%)
계정 관리	85%
파일 및 디렉터리 관리	65%
서비스 관리	93%
패치 및 로그 관리	74%
평균	82%

[그림 2-2] 서버 영역별 평균 보안수준(Unix)

- 상세점검표

[계정 및 패스워드 관리]

3. 불필요 계정 존재 여부(Default 계정)

정보시스템 현황	점검결과	비고
	/etc/passwd 파일을 확인해본 결과 lp, uucp, gopher, games 등 불필요한 계정이 존재하여 취약함	취약

[계정 및 패스워드 관리]

9. 패스워드의 최대 사용기간 설정

정보시스템 현황	점검결과	비고
	cat /etc/login.defs파일에 PASS_MIN_DAYS가 99999이므로 취약함	취약

2. Simple Recipe Web Site 취약점 진단

기 간	➢ 2018.05.17 ~ 2018.06.10
사용 기술	➢ Cooxie Toolbar, Burp Proxy, Dirbuster, WireShark
목 표	➢ OWASP Top 10에 기반한 Web Site 취약점 진단 ➢ 발견한 취약점에 대한 보안조치

- 진단 요약

3. 수행결과 요약

3.1 초기 진단

모의해킹을 수행한 결과, 점검대상 URL에서 4개의 취약점이 발견되었습니다. 이러한 취약점으로 인해 일반사용자나 관리자의 세션정보를 가로채거나 악성코드에 감염 될 수 있습니다.

발견된 취약점을 요약하면 아래의 표와 같습니다.

점검대상	취약점		위험도	발생 위험
	OWASP Top 10	웹 보안 가이드라인		
Simple Recipe(심플레시피)	크로스사이트스 크립팅(XSS)	크로스사이트스 크립팅	H	일반사용자나 관리자의 세션정보를 가로채거나 악성코드에 감염 될 수 있습니다.
	민감한 데이터 노출	데이터평문전송	H	사용자의 중요 입력 필드가 암호화되지 않아, 사용자 로그인 정보 탈취가 가능합니다.
		정보누출	H	웹 사이트 데이터가 노출되는 것으로 개발과정의 코멘트나 오류 메시지 등에서 중요한 정보가 노출되어 공격자에게 2차공격을 하기 위한 중요한 정보를 제공할 수 있습니다.
	취약한 인증	불충분한 세션만료	H	만료되지 않는 세션 활용이 가능합니다

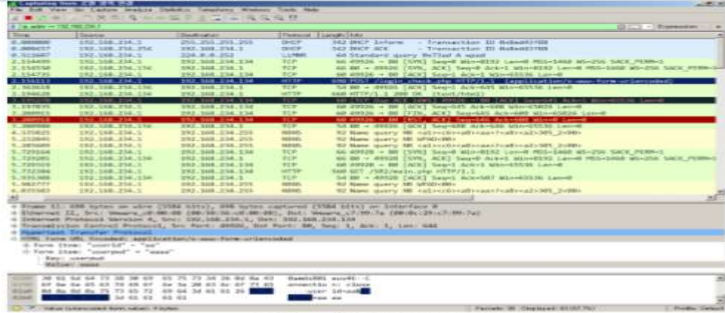
[표 3-1] 초기진단 요약

- 상세점검표

4.1.2. 민감한 데이터 노출 - 데이터 평문 전송

Code	A3	위험도	H
점검영역	웹 애플리케이션		
점검항목	OWASP Top 10	민감한 데이터 노출	
	웹 보안 가이드라인	데이터 평문 전송	

설 명	웹 사이트 데이터가 노출되는 것으로 개발 과정의 코멘트나 오류 메시지 등에서 중요한 정보가 노출되어 공격자에게 2차 공격을 하기 위한 중요한 정보를 제공할 수 있으며, 서버 설정에 의한 웹 서버 버전 정보가 노출될 경우 공격자에 의한 Exploit 공격 등에 노출될 수 있습니다.
취약경로	http:// 192.168.29.218/login.php

취약내용	
------	--

[그림 1] 데이터 평문 전송

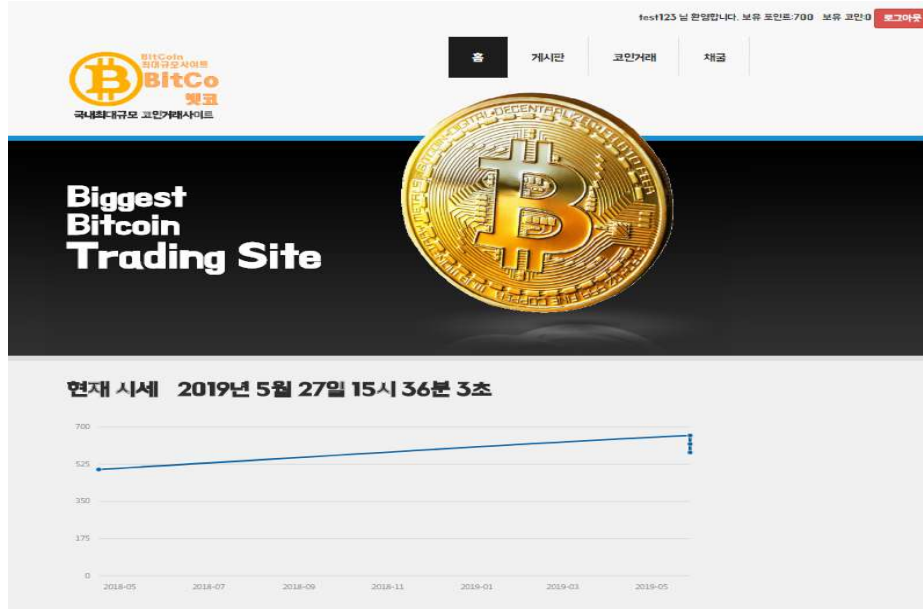
아이디 값 aa와 비밀번호 aaaa가 그대로 노출된 것을 확인 할 수 있다.

권고사항	<ul style="list-style-type: none">■ 웹 서버 내에서의 조치<ul style="list-style-type: none">■ 웹 서버는 전자서명인증서, SSL(Secure Socket Layer)을 이용하여 사용자 식별 및 DATA 전송 시 암호화 통신으로 데이터 전송의 안전성을 확보■ 조치 완료 후 인증과정 등의 주요 정보 노출 여부를 재점검■ 홈페이지 개발 보안 조치<ul style="list-style-type: none">■ 홈페이지는 중요정보와 관련된 민감한 데이터(개인정보, 비밀번호 등) 전송 시 통신채널(또는 전송데이터) 암호화적용
------	---

3. 가상화폐 거래소 BITCO Web Site 개발

기 간	➢ 2018.5.17~2018.6.10
사용 기술	➢ Windows 2008 R2, IIS, MySQL, phpMyAdmin, PHP, JavaScript, Bootstrap, CSS
목 표	➢ PHP기반 Web Site 개발 ➢ 예상 공격경로 차단
기 능	➢ 가상화폐 BITCO 매매 ➢ 실시간 시세 그래프 ➢ BITCO 채굴을 통한 통화량 조절

- 홈 화면



- 코인거래 및 채굴 화면

BITCO

구매 판매

코인의 현재 가격은 660포인트입니다.

1개 ▼

구매

BITCO

MINING

비트코인

일일량

게임 시작

채굴

- 공격경로 예상 및 대응

공격경로 및 대응방안

SQL Injection

- Prepared Statement 사용

```
$password =hash( algo: "sha256",$_POST['pass']);  
$stmt=mysqli_stmt_init($db);  
$sql->prepare("SELECT * FROM member WHERE mail=?");  
$mail = $_POST['mail'];  
$stmt->bind_param( types: 's' , &var1: $mail);  
$stmt->execute();  
$stmt->bind_result( &var1: $mail, &...: $name,$pass);  
$hash_pw = $pass;
```

공격경로 및 대응방안

SQL Injection

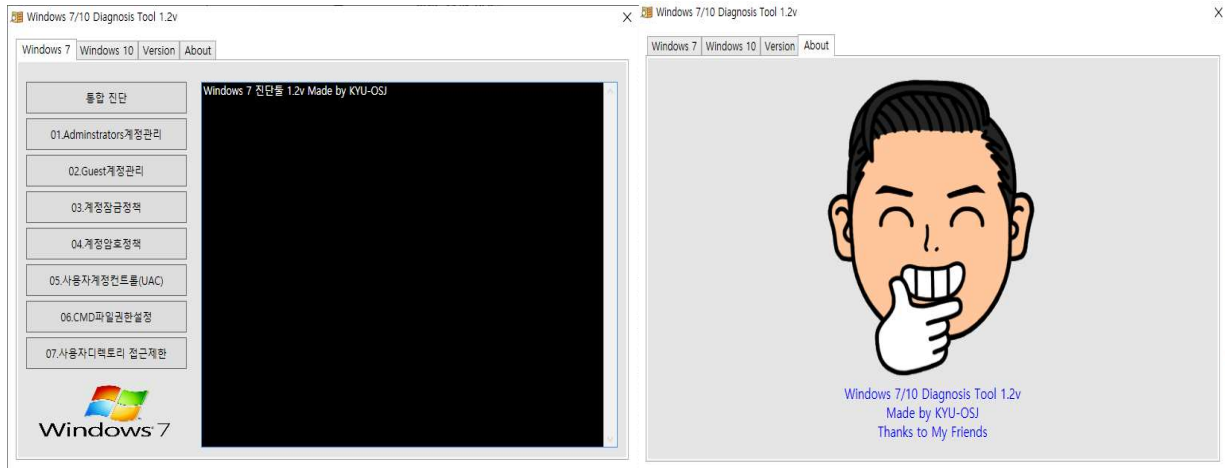
- Prepared Statement 사용

```
$password =hash( algo: "sha256",$_POST['pass']);  
$stmt=mysqli_stmt_init($db);  
$sql->prepare("SELECT * FROM member WHERE mail=?");  
$mail = $_POST['mail'];  
$stmt->bind_param( types: 's' , &var1: $mail);  
$stmt->execute();  
$stmt->bind_result( &var1: $mail, &...: $name,$pass);  
$hash_pw = $pass;
```

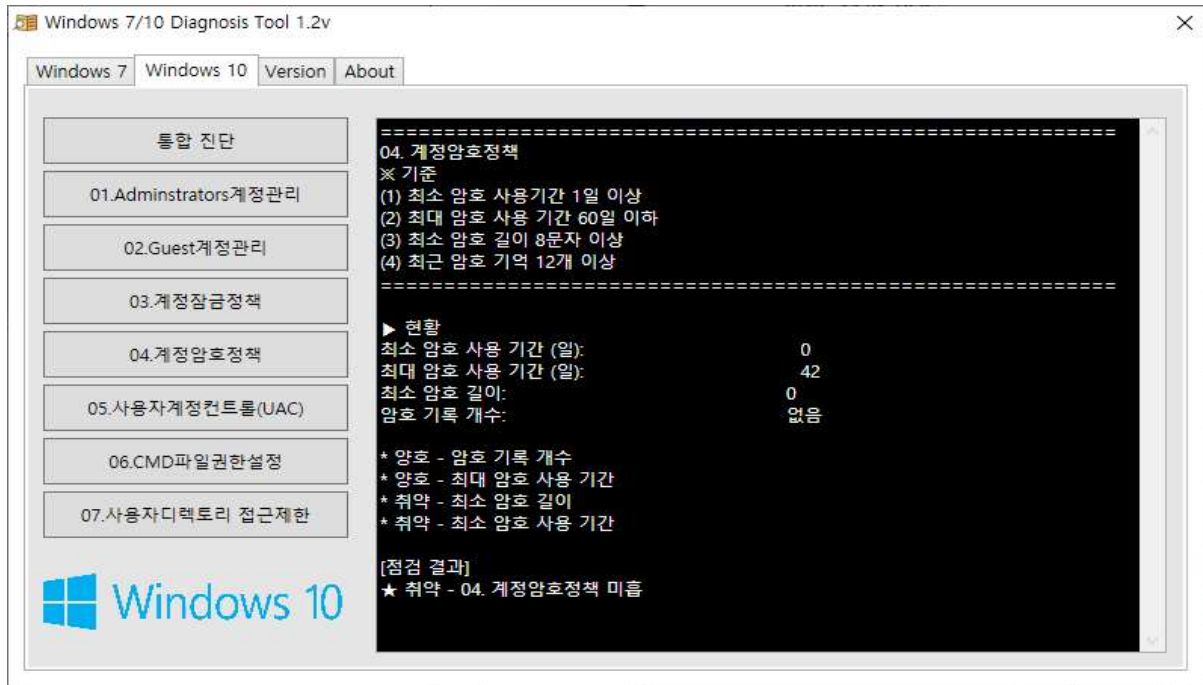
4. Windows 7/10 취약점 진단 Script 제작

기 간	➤ 2018.8.28 ~ 2018.12.23
사용 기술	➤ Windows Batch, C++
목 표	➤ 주요정보통신기반시설 기술적 취약점 분석·평가 가이드를 기반으로 Windows 취약점 진단
기 능	➤ 하나의 프로그램으로 Windows 7, 10 취약점 점검 ➤ 개별 및 통합 진단 후 세부사항 바로보기

- 프로그램 실행 화면



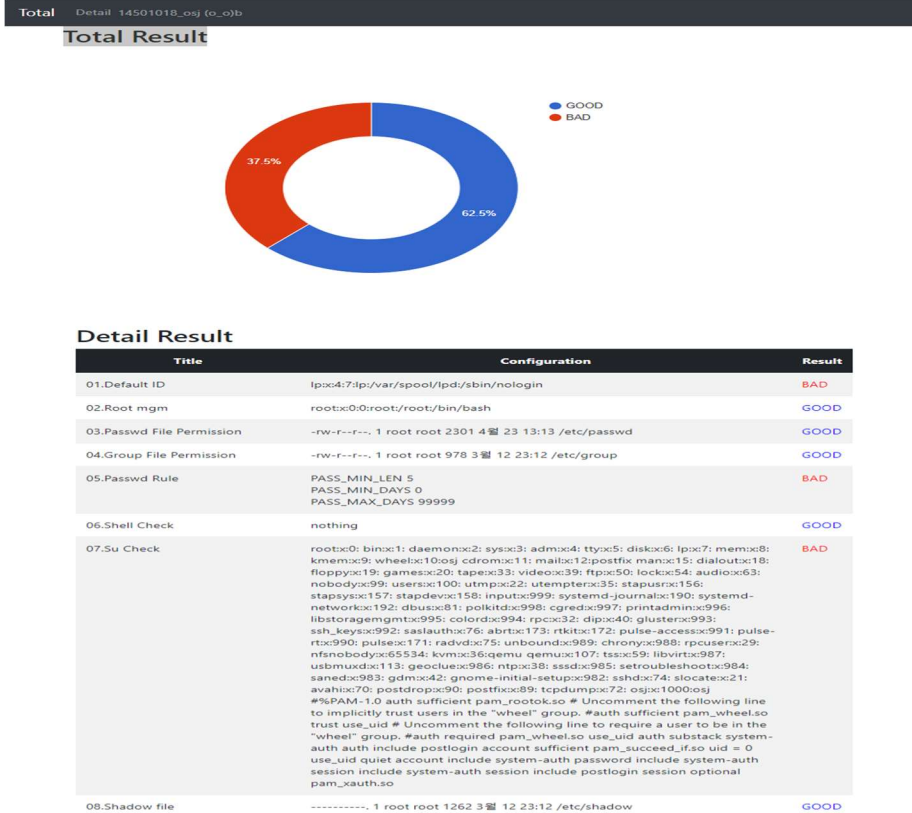
- 스크립트 실행 후 화면



5. Linux 취약점 진단 Shell Script 제작

기 간	➤ 2019.5.22 ~ 2019.6.21
사용 기술	➤ CentOS, Shell Script
목 표	➤ Shell Script 제작을 통해 취약점 자동 진단 ➤ 발견된 취약점에 대한 보안조치

- 결과화면



- 스크립트

```
#sysinfo_system
osif=`head -n 1 /etc/centos-release`
hostif=`uname -n`
kernelif=`uname -r`

#sysinfo_network
ifconfig -a >> $infofile
info=`cat ./infofile`

#01. Default ID
config1=`cat /etc/passwd |grep "lp:|uucp:|nuucp:"`

if [ `cat /etc/passwd |grep "lp:|uucp:|nuucp:" |wc -l` -eq 0 ]; then
    result1="GOOD"
    good=$((good+1))
else
    result1="BAD"
    bad=$((bad+1))
fi

#02.Root mgm Start
config2=`awk -F: ' $3==0 ' /etc/passwd`

if [ `awk -F: ' $3==0 ' /etc/passwd |wc -l` -eq 1 ]; then
    result2="GOOD"
    good=$((good+1))
else
    result2="BAD"
    bad=$((bad+1))
fi

#03.Passwd File Permission Check Start
config3=`ls -al /etc/passwd`

if [ `ls -al /etc/passwd |awk '{print $1}' |grep ".rw-r--r--" |wc -l` -eq 1 ]; then
    result3="GOOD"
    good=$((good+1))
else
    result3="BAD"
    bad=$((bad+1))
fi
```