U-44

- 분류 : 계정 점검
- 위험도 : 중

---

1. 점검 내용

- 사용자 계정 정보가 저장된 파일에 root(UID=0) 계정과 동일한 UID(User Identification)를 가진 계정이 존재하는지 점검

---

2. 점검 목적

- root 계정과 동일한 UID가 존재하는지 점검하여 root권한이 일반 사용자 계 정이나 비인가자의 접근 위협에 안전하게 보호되고 있는지 확인하기 위한 목적

---

3. 보안 위협

- root 계정과 동일 UID가 설정되어 있는 일반사용자 계정도 root 권한을 부 여받아 관리자가 실행 할 수 있는 모든 작업이 가능하다ㅌ
- root와 동일한 UID를 사용하므로 사용자 감사 추적 시 어려움이 발생함

---

4. 참고

- UID(User Identification) : 여러 명의 사용자가 동시에 사용하는 시스템에서 사용자가 자 신을 대표하기 위해 쓰는 이름

---

5. 취약 판단 기준

- root 계정과 동일한 UID를 갖는 계정이 존재하는 경우 취약하다고 판단

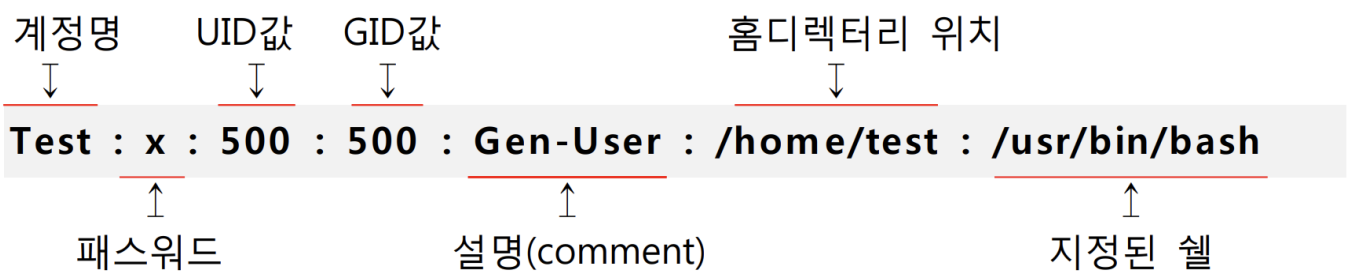
---

6. 점검 방법

6.1. /etc/passwd 파일 점검

```
cat /etc/passwd

# UID가 0인 계정출력
awk -F: '($3 == 0) {print $1}' /etc/passwd
```



- UID (User Identification)
  - 사용자의 ID 번호
- GID (Group Identification)
  - 사용자가 속한 그룹의 ID 번호

---

7. 조치 방법

7.1. 다른 UID로 변경하거나 불필요한 계정일 경우 삭제

```
sudo usermod -u 500 사용자아이디
```

- 500 이상의 UID로 수정
  - 시스템 계정과 일반 사용자 계정의 분리를 위해