**U-44 (중)**

## 1. 점검 내용

- 사용자 계정 정보가 저장된 파일에 계정에 root 계정(UID=0)과 동일한 UID를 가진 계정이 존재하는지 점검

*UID (User Identification) : 여러명의 사용자가 동시에 사용하는 시스템에서 사용자가 자신을 대표하기 위해 쓰는 이름

---

## 2. 점검 목적

- root 계정과 동일한 UID가 존재하는지 점검하여 root 권한이 일반 사용자 계정이나 비인가자의 접근 위협에 안전하게 보호되고 있는지 확인하기 위한 목적

---

## 3. 취약 판단 기준

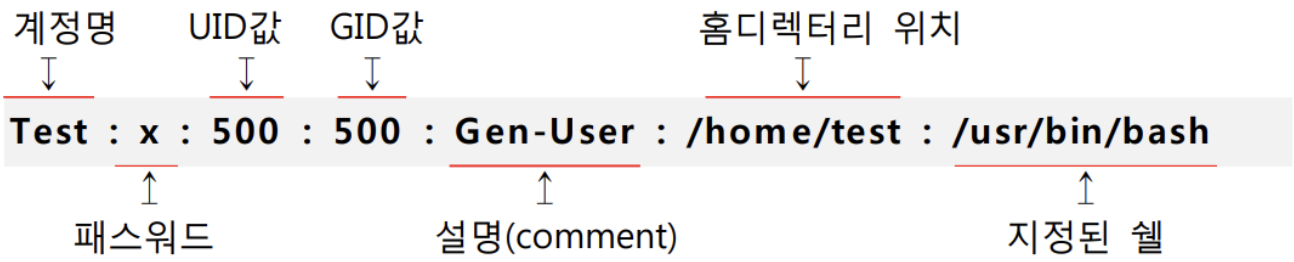
- root 계정과 동일한 UID를 갖는 계정이 존재하는 경우 취약하다고 판단

---

## 4. 점검 방법

### 4.1. /etc/passwd 파일 확인

- /etc/passwd 파일 구조




- 패스워드
  - 사용자 비밀번호가 저장되는 필드였으나 보안 상의 이유로 /etc/shadow 파일로 암호화 되어 옮겨지고 x로 표시된다
- UID (User Identification)
  - 사용자의 ID 번호
- GID (Group Identification)
  - 사용자가 속한 그룹의 ID 번호

/etc/passwd 파일 확인

```
cat /etc/passwd
awk -F: '$3 == 0 {print $1}' /etc/passwd # UID 가 0인 부분만 출력하는 명령어
```

---

## 5. 보안 조치 방법

- UID 가 0인 계정이 존재할 시 변경할 UID를 확인 후 다른 UID로 변경하거나 불필요할 경우 삭제한다
- 계정이 사용 중이면 명령어 조치가 불가 하므로 /etc/passwd 파일을 변경한다

```
sudo usermod -u 500 사용자아이디
```

- 500 이상의 UID로 수정한다