

Vulnerability Discovery_9

Target

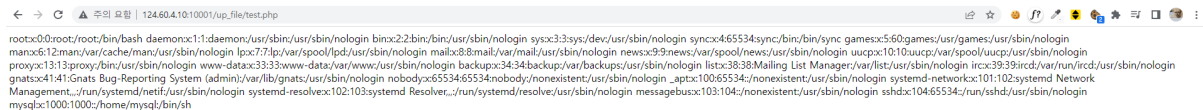
: http://124.60.4.10:10001/up_file/

Payload

: 서버에 /etc/passwd 명령어 실행

Impact

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



```
root@0:root:/root/bin/bash daemon:1:1:daemon/usr/sbin/usr/sbin/nologin bin:2:2:bin/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/lib/mailman/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/ssh/usr/sbin/nologin mysql:1000:1000:/home/mysql/bin/sh
```