Exam

to start:

1. connect to vpn with openvpn
2. set the dns setting /etc/resolve.config
3. delete all dns servers and add the dns server from the ELS -> because sometime the target machine goes off, which lead for testing sites on the internet

2 RCE -> SSRF + Template Injection
possible RCE -> SQLi
picture bypass uploading
WAF bypass
reverse shell
time/blind based SQLi händisch

report

overview about the vulnerability
URL vulnerablility
Screenshots
POC
remediation