This is a retired machine from Hackthebox with various questions.

We start with our usual nmap scan and find two ports open. We see port 22 for SSH and port 80 running Apache . Let's add the domain name to our /etc/hosts file.

Trying /robots.txt revealed a hidden dir /ghost which led to an auth page but we don’t have credentials.

ffuf -w /usr/share/wordlists/amass/bitquark\_subdomains\_top100K.txt -H "Host:FUZZ.linkvortex.htb" -u http://linkvortex.htb -ic -fs 230 gave us “dev” subdomain and nuclei found an interesting jwk-json-leak (but I don’t know what to do with it)

A computer screen with many white text

AI-generated content may be incorrect.

We’ve used -ic to ignore case sensitive and -fs 230 to filter the output so that we don’t get floded with not found errors.

Running gobuster dir -u http://dev.linkvortex.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt provided us with an /.git where maybe we can find something interesting or we can dump it.

A screenshot of a computer program

AI-generated content may be incorrect.

I’ve eventually dumped it and found through “-git status” a committed change to the authentication.test.js so I restored it and found the password for [admin@linkvortex.htb](mailto:admin@linkvortex.htb) with :

grep -r 'pass' ../../../../../ghost/core/test/regression/api/admin/authentication.test.js

A screenshot of a computer program

AI-generated content may be incorrect.

Now that we are inside the system I found the version 5.58.0 that is vulnerable for Arbitrary file read (cve-2023-40028) so I used the POC to gain access inside and another username called bob with pass fibber-talented-worth.

Once ssh-ed inside with bob’s credentials we found the user flag.