Sandworm

Enumeration

```
└─$ nmap -sC -sV -oN nmap/init.nmap 10.10.11.218
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 05:28 EDT
Nmap scan report for 10.10.11.218
Host is up (0.098s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp  open  http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to https://ssa.htb/
443/tcp open  ssl/http nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Secret Spy Agency | Secret Security Service
| ssl-cert: Subject: commonName=SSA/organizationName=Secret Spy Agency/stateOrProvinceName=Classified/countryName=SA
| Not valid before: 2023-05-04T18:03:25
|_Not valid after:  2050-09-19T18:03:25
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.89 seconds
```

port 80 redirects to port 443, so we can only access via https

viewing the ssl certificate, we get an email: atlas@ssa.htb 😀

Gobuster seems to be finding stuff. Including a /login and /guide directory

PGP

The webserver gives a demo of PGP encryption.
We are able to encrypt and sign using their public key, and decrypt using their private key on the backend.
There is also a contact page which accepts PGP encrypted messages

The webapp has a feature which allows you to verify a signature by giving it a signed message as well as your public key
This feature is vulnerable to SSTI on the Full Name field.

We find out the box is using Jinja2, and we can find payloads for that with some research.

Command injection works, but a lot of reverse shell payloads fail, probably due to some bad characters or

security measures in place

After trying A LOT of payloads, the following works:
let var = base64 encoded version of standard reverse shell
then payload is:
    echo var | base64 -d | bash

this gives us a shell as atlas

atlas

With now have a shell as atlas.

The directory /var/www/html/SSA/SSA/submissions has some pgp encrypted files which can probably be decrypted using atlas' private key found in ~/.gnupg/private-keys-v1.d

LATERAL MOVEMENT:

Looking around, we find plaintext creds in:
~/.config/httpie/sessions/localhost_5000/admin.json

silentobserver:quietLiketheWind22

using these creds, we can ssh in!

privesc