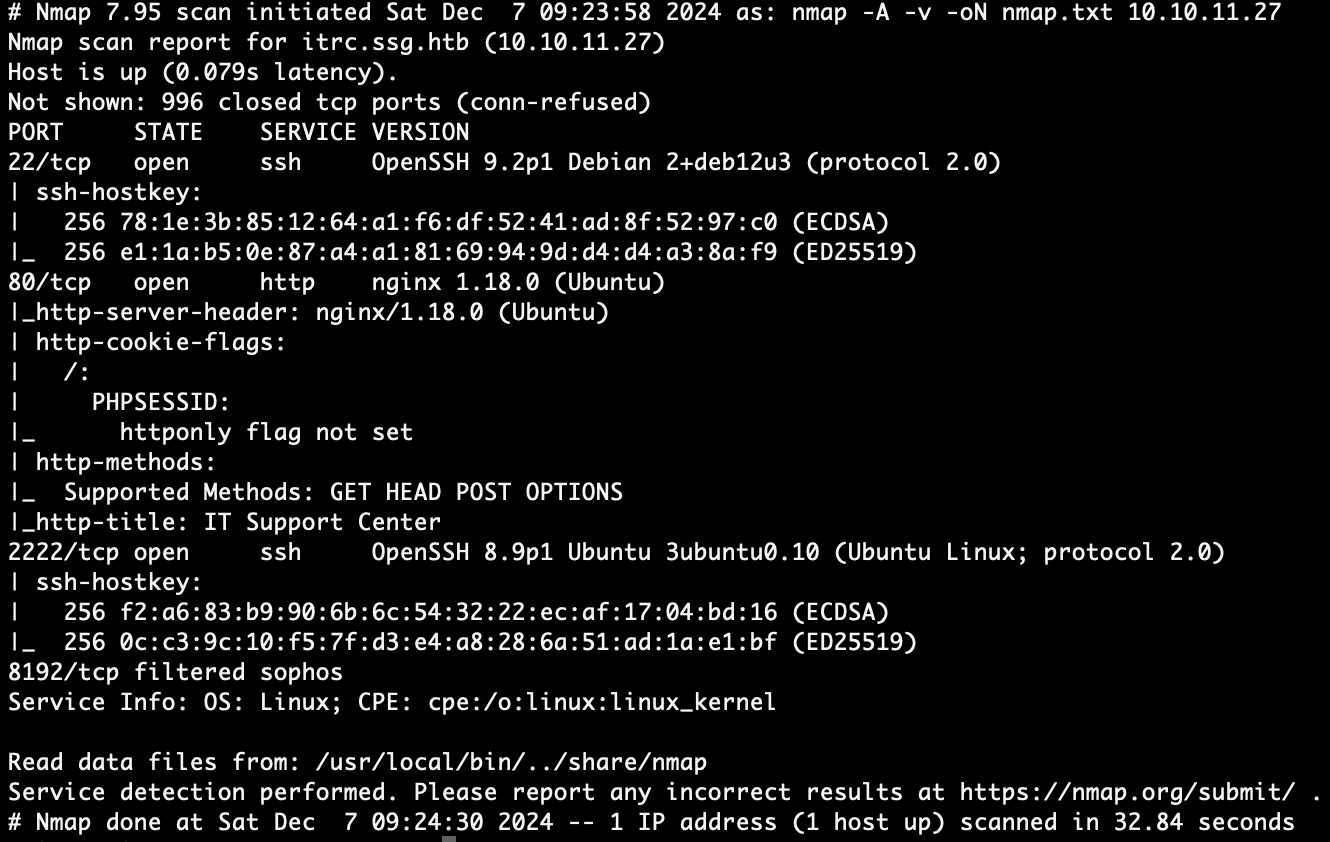
**Resource**

Nmap results:



We see one suspicious port 2222 for extra SSH login besides port 22 (It turns out these extra SSH ports micmic an Active Directory architecture for the Linux system).

Web App:

At first let’s add the ip address of the box and it’s domain to /etc/hosts. This action essentially maps an IP address (10.10.11.27 to a hostname (itrc.ssg.htb).

Command to add the ip address in /etc/hosts:

**echo -e '10.10.11.27\t\titrc.ssg.htb' | sudo tee -a /etc/hosts**

****

****

The domain is http://itrc.ssg.htb/, or SSG (Strategic Solutions Group) IT Resource Center, which is a one-stop shop for resolving website issues, managing SSH access, removing viruses, and addressing different security concerns.  
At this point in time, we do not have any information regarding the web application; so, for the time being, we will just navigate the page by clicking on various links and entering the expected inputs into any input fields that are there. For the time being, all we want to do is get a better understanding of what different items do.

We can register and log in to the dashboard.

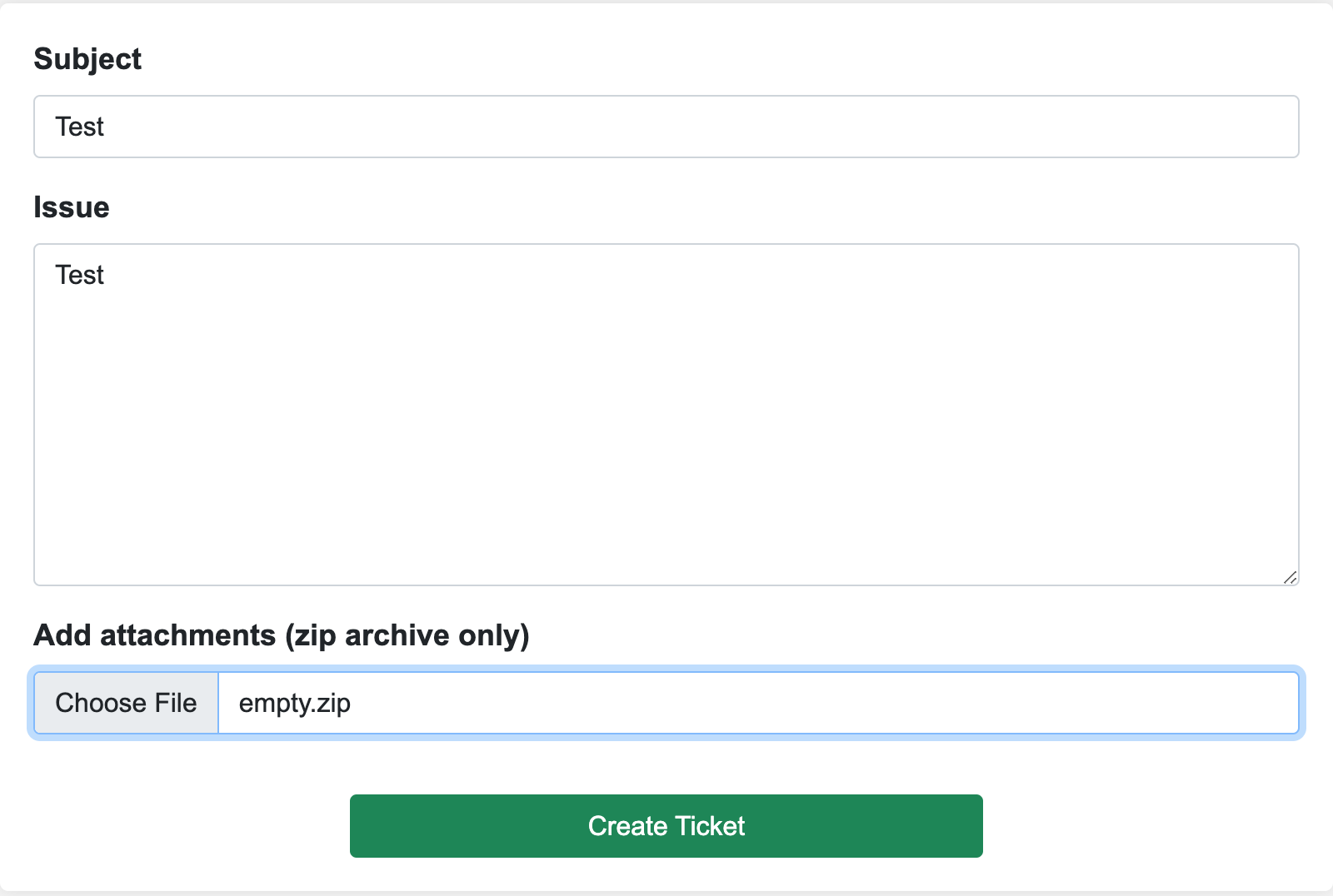
A screen shot of a ticket

Description automatically generated

Creating the tickets without attachment. Let’s create an empty zipfile. The web app only accepts the zipfile.



Which will create a empty zipfile and let’s create a ticket.

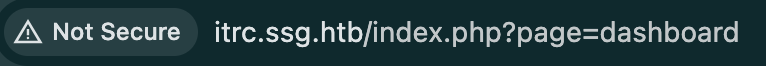


We get an error when we try to submit an empty zipfile.

**Deprecated**: ZipArchive::open(): Using empty file as ZipArchive is deprecated in **/var/www/itrc/savefile.inc.php** on line **38**  
  
**Warning**: hash\_file(/tmp/php4KIerb): Failed to open stream: No such file or directory in **/var/www/itrc/savefile.inc.php** on line **48**  
  
**Warning**: Cannot modify header information - headers already sent by (output started at /var/www/itrc/savefile.inc.php:38) in **/var/www/itrc/api/create\_ticket.php** on line **31**

Older PHP versions discourage the attempt of opening an empty or non-existent file made by the ZipArchive::open() method. Furthermore failing the hash\_file() function is its inability to locate the desired file at /tmp/php4KIerb. This implies that the script's creation, storage, or referencing of files could be risky.

By looking at the url we can find out there could be path traversing using conventional path.



Now fuzzing to find hidden directories with cookies.