

Files

master + 🔍

🔍 Go to file t

📄 classic-forensic.md

📄 fibonacci.md

📄 lost-head.md

> 📁 osint

> 📁 reverse-engineering

> 📁 steganography

ctf-writeups / 2020 / affinity-lite / web / sooodefault.md 📄

klassiker Add Affinity Lite

d5b31b2 · 4 years ago 🕒 History

Preview Code Blame 29 lines (21 loc) · 974 Bytes

Raw 📄 ⬇️ ✎ ▾ ☰

soodefault

Task

Can you find the flag?

<http://web2.affinityctf.com/>

Solution

It's the `Apache2 Ubuntu Default Page`. Since this was a low points task I looked at the source code and noticed that the `A` of that string is a HTML entity.

Grepping them after using `curl` and then converting them to chars:

```
$ curl -s web2.affinityctf.com | grep -o '&#[0-9]*' | tr -d '\n';echo
&#65&#70&#70&#67&#84&#70&#123&#104&#116&#109&#108&#101&#110&#116&#105&#116&#121&#125
```

```
$ python
>>> s = "&#65&#70&#70&#67&#84&#70&#123&#104&#116&#109&#108&#101&#110&#116&#105&#116&#121&#125"
>>> s.split("&#")
['', '65', '70', '70', '67', '84', '70', '123', '104', '116', '109', '108', '101', '110', '116', '105', '116', '121', '125']
>>> [chr(int(x)) for x in s.split("&#") if x != ""]
['A', 'F', 'F', 'C', 'T', 'F', '{', 'h', 't', 'm', 'l', 'e', 'n', 't', 'i', 't', 'y', '}']
>>> ''.join([chr(int(x)) for x in s.split("&#") if x != ""])
'AFFCTF{htmlentity}'
```