NeverLAN CTF

Trivia :

Milk Please !

Value : 250 pts

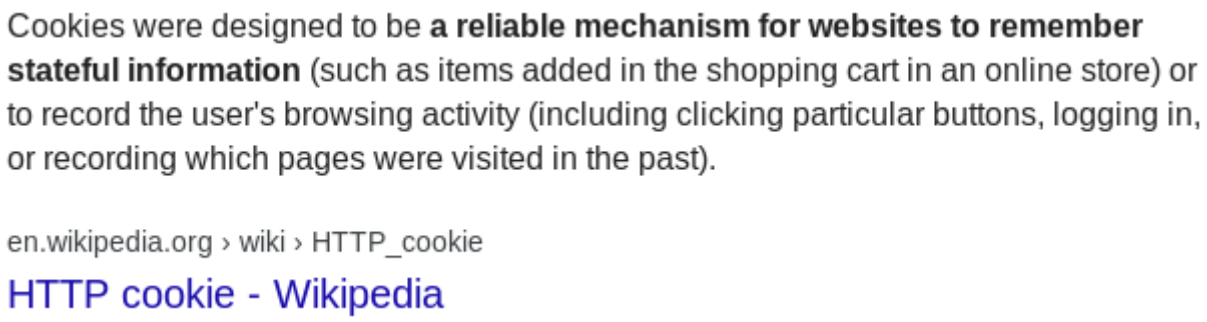
Difficulty : Easy

Trivia Question : a reliable mechanism for websites to rembmer stateful infromation. Yummy !

Your flag won’t be in the normal flag{flagGoesHere} syntax. Instead, you’re looking for the answer to the definition given.

Solution :

Searching on google and we found our answer was «cookie».



Flag : cookie

Professional guessing

Value : 10 pts

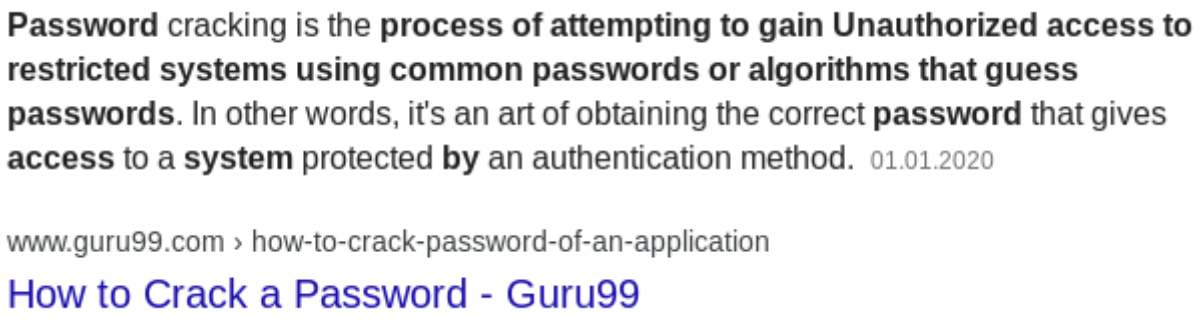
Difficulty : Easy

Trivia Question : The process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords.

Your flag won’t be in the normal flag{flagGoesHere} syntax. Instead, you’re looking for the answer to the definition given.

Solution :

Searching on google and we found our answer was «password cracking».



Flag : password cracking

Professional guessing

Value : 10 pts

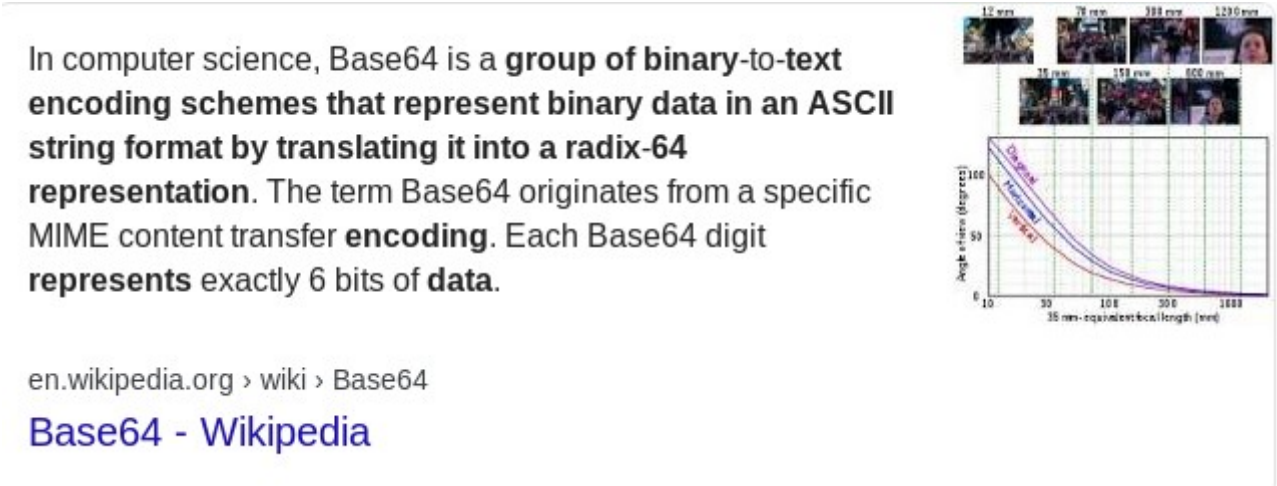
Difficulty : Easy

Trivia Question : A group of binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation.

Your flag won’t be in the normal flag{flagGoesHere} syntax. Instead, you’re looking for the answer to the definition given.

Solution :

Searching on google and we found our answer was «Base64».



Flag : Base64

AAAAAAAAAAAAA ! I hate CVEs

Value : 20 pts

Difficulty : Easy

Trivia Question : This CVE reminds me of some old school exploits. If flag is enabled in sudoers.

Your flag won't be in the normal flag{flagGoesHere} syntax.

Solution :

Searching on google about «CVE linux exploit sudoers» and we found an exploit from exploit-db.

Source : https://www.exploit-db.com/exploits/47995

Reading the exploit details and it said «There is no impact unless pwfeedback has been enables.».

```
# Due to a bug, when the pwfeedback option is enabled in the sudoers file, a user may be
able to trigger a stack-based buffer overflow.
# This bug can be triggered even by users not listed in the sudoers file. There is no
impact unless pwfeedback has been enabled.
```

Flag : pwfeedback

Rick Rolled by the NSA ??

Value : 50 pts

Difficulty : Hard

Trivia Question : This CVE proof of concept Shows NSA.gov playing «Never Gonna Give You Up,» by 1980s heart-throb Rick Astley.

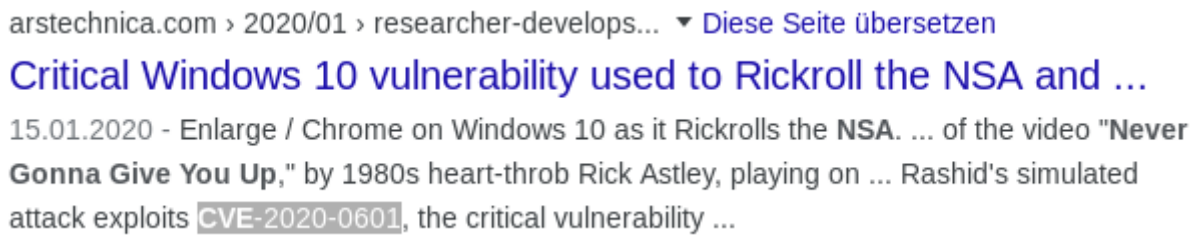
Use the CVE ID for the flag. flag{CVE-?????????}

Your flag won’t be in the normal flag{flagGoesHere} syntax.

Solution :

Searching on google about «CVE NSA never gonna give you up» and we found a blog post about a Critical Windows 10 Vulnerability used to rickroll the NSA with the CVE in description.

Source : https://arstechnica.com/information-technology/2020/01/researcher-develops-working-exploit-for-critical-windows-10-vulnerability/



Flag : flag{CVE-2020-0601}