Binary Exploitation

### 1. basic-file-exploit

### 

### Following the hint given

### 

### Flag: picoCTF{M4K3\_5UR3\_70\_CH3CK\_Y0UR\_1NPU75\_1B9F5942}

### 2. CVE-XXXX-XXXX

### 

### Search for the CVE of the first recorded RCE vulnerability in 2021

### 

### Flag: picoCTF{CVE-2021-34527}

### 3. buffer overflow 0

### 

### Solution: On inspecting the source code we can see that the gets() command is used for taking string input. This command is susceptible to buffer overflow attacks as it doesn’t know the size of the sting being entered.

### 

### It is also seen that the size allocated for the string is 16 characters.

### 

### So if we enter a string longer than 16 characters it will cause a buffer overflow.

### 

### Flag: picoCTF{ov3rfl0ws\_ar3nt\_that\_bad\_a065d5d9}

### 4. clutter-overflow

### 

### Solution: On inspecting the code, we see the use of gets(). This is susceptible to buffer overflow attacks.

### 

### We know the size of clutter, hence the buffer overflows when we enter more than 265 characters.

### 

### We have the flag using this information and the fact that the machines use little-endian format, entering the code accordingly

### 

### Flag: picoCTF{c0ntr0ll3d\_clutt3r\_1n\_my\_buff3r}

### 5. RPS

### 

### Solution: On analysing the code we see the use of strstr function.

### 

### So if we use rockpaperscissors, we win every time. After winning 5 times we get the flag.

### 

### Flag: picoCTF{50M3\_3X7R3M3\_1UCK\_58F0F41B}

### 6. Stonks

### 

Solution: There is no format specifier for the print function which can be exploited by inputting any format specifier.

### 

### Inputting %x several times, we get an API token as a list of hexadecimal values

### 

### Using online tools, we find the flag but it is in little endian.Using cyberchef to swap endians and converting hex to ASCII, we have the flag.

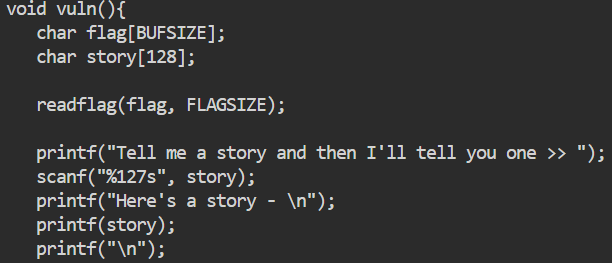
### 

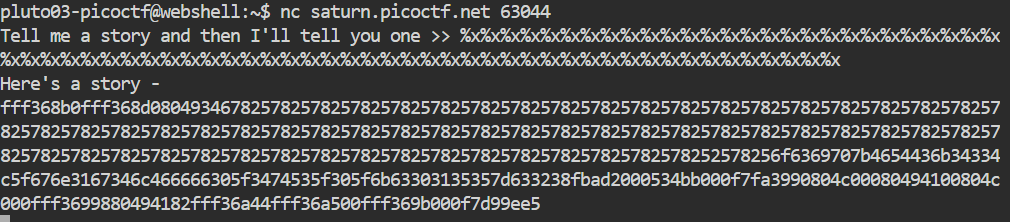
### picoCTF{I\_l05t\_4ll\_my\_m0n3y\_c7cb6cae}

### 7. flag leak

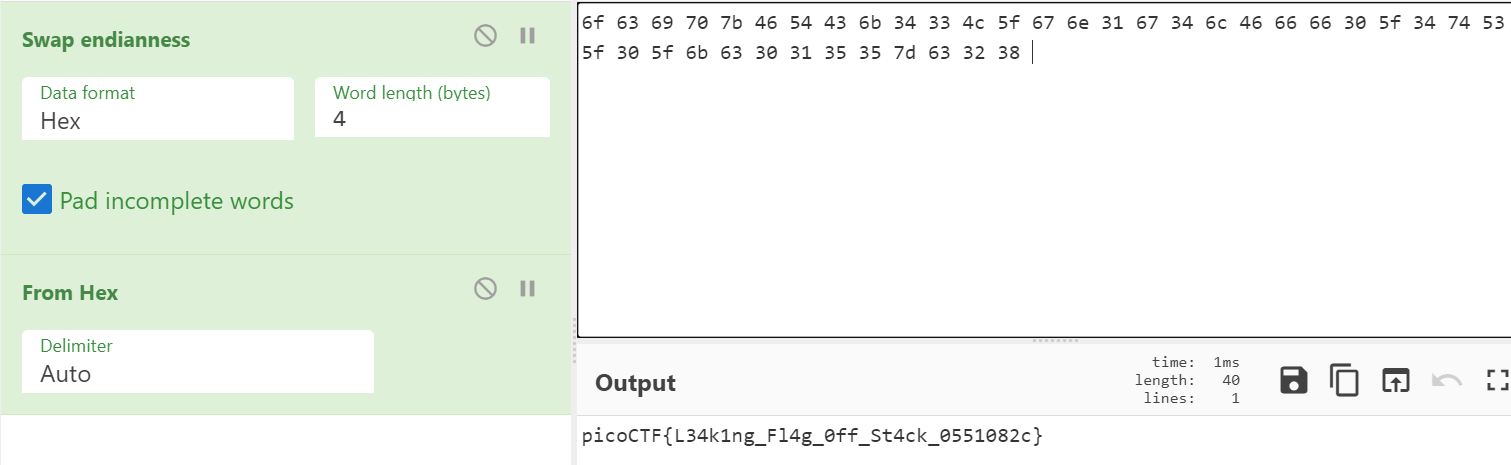
### 

### Solution: There is no format specifier for the print function which can be exploited by inputting any format specifier.





Convert it from hex to ASCII and change the endianness



Flag: picoCTF{L34k1ng\_Fl4g\_0ff\_St4ck\_0551082c}