

赛题名称：misc03

解题步骤（WriteUp）

将流量包放在 wireshark 里面，发现只有几个 ip

ip.src != 10.22.0.2&&ip.src != 39.144.218.183&&ip.src != 39.144.219.183&&ip.src != 39.168.5.60&&ip.src != 123.147.249.83
--

一个个试

是 39.168.5.60

后续分析流量包，找到了 upload.php 还有 uploads/hacker.php

69644	218.520429	39.168.5.60	10.22.0.2	HTTP	531 GET / HTTP/1.1
69686	218.635936	39.168.5.60	10.22.0.2	HTTP	531 GET / HTTP/1.1
1016...	398.394804	39.168.5.60	10.22.0.2	HTTP	776 POST /uploads/hacker.php HTTP/1.1 (application/x-www-form-urlencoded)
1016...	398.595396	39.168.5.60	10.22.0.2	HTTP	788 POST /uploads/hacker.php HTTP/1.1 (application/x-www-form-urlencoded)
1016...	356.755083	39.168.5.60	10.22.0.2	HTTP	1019 POST /upload.php HTTP/1.1 (image/jpeg)
1016...	398.394754	39.168.5.60	10.22.0.2	TCP	1414 34123 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=1360 [TCP PDU reassembled in 101633]