

# 1 Nginx Range filter shaping overflow vulnerability

- 2
- 3 when using nginx std module , an attacker can obtain the header information of the cache files in the response by sending a header request containing the malicious construct range filed
- 4
- 5 cache file header may contain the ip address |

with weppolyzer  
you can find  
if web using  
nginx

or  
> curl -I url

7 or other sensitive of the backend server  
resulting in information leakage

8  
9  
10  
11 nginx server uses proxy cache . the  
attacker can use the vulnerability to  
get the real ip or other sensitive  
information

## \* How to hunt?

1. detection with a script (xyz.py)
2. exploit (fgfg.py)