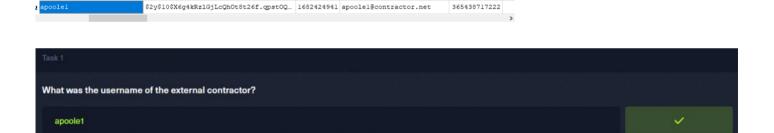


What was the username of the external contractor?

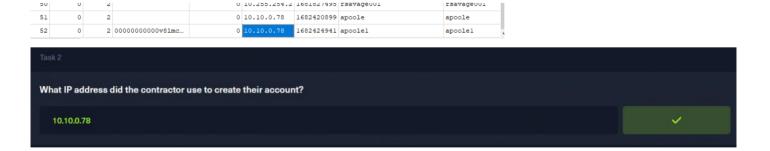
\$2v\$10\$7dv/



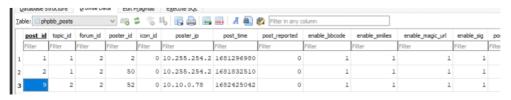
312440918521

1682423286 apoole@contractor.net

What IP address did the contractor use to create their account?



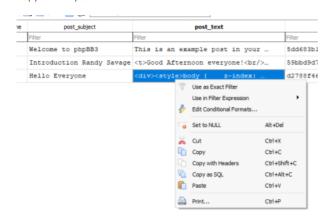
What is the post_id of the malicious post that the contractor made?

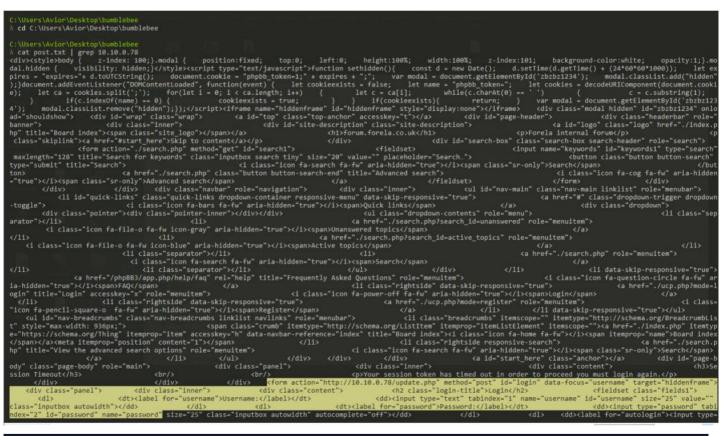


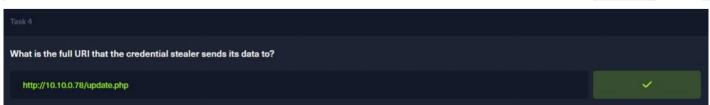


What is the full URI that the credential stealer sends its data to?

Copy the full post:



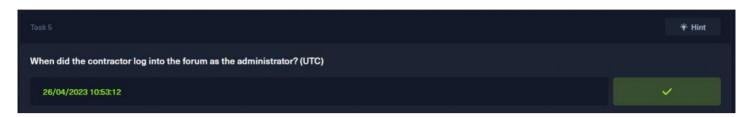




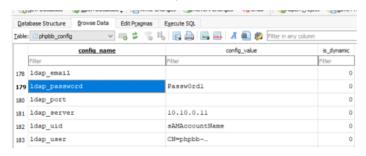
When did the contractor log into the forum as the administrator? (UTC)

```
(OSET 3-KTON - OSETACH CONTROLL - CALL - CA
ba2267dfc066187582&mode=main&action=enable&ext_name=rokx%2Fdborldap&hash=f8bbcf4e" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chro
le/112.0.0.0 Safari/537.36"
0.255.254.2 - [25/Apr/2023:112:46:10 +0100] "GET /adm/style/admin.js?assets_version=4 HTTP/1.1" 200 2568 "http://10.10.0.27/adm/index.php?i=acp_extensions&sid=041ca559047513b
2267dfc066187582&mode=main&action=list" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
0.10.10.27.36 - [26/Apr/2023:1153:12.40100] "GET /adm/style/admin.css?assets_version=4 HTTP/1.1" 200 1030" "http://10.10.0.27/adm/index.php?i=acp_help_phpbb&mode=help_phpbb&side
eca30c1b75dc3eed1720423aa1ff9577" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
0.10.0.78 - [26/Apr/2023:11:53:13 +0100] "GET /adm/style/admin.js?assets_version=4 HTTP/1.1" 200 2568 "http://10.10.0.27/adm/index.php?i=acp_help_phpbb&mode=help_phpbb&sid=
a30c1b75dc3eed17204232311:53:13 +0100] "GET /adm/images/phpbb_logo.png HTTP/1.1" 200 2568 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
0.10.0.78 - [26/Apr/2023:11:53:13 +0100] "GET /adm/images/innerbox_bg.gif HTTP/1.1" 200 2565 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
0.10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
                                                                                                       X04, rv:109.0) deck0/20100101 Firefox/112.0
[26/Apr/2023:11:53:13 +0100] "GET /adm/images/arrow_right.gif HTTP/1.1" 200 331 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows N
(64; rv:109.0) Geck0/20100101 Firefox/112.0"
```

26/Apr/2023:11:53:12 convert to UTC

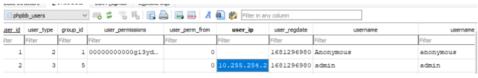


In the forum there are plaintext credentials for the LDAP connection, what is the password?





What is the user agent of the Administrator user?



ers\Avior\Desktop\bumblebee
access.log | grep admin
5.254.2 - - [25/Apr/2023:12:46:08 +0100] "GET /adm/style/admin.css?assets_version=4 HTTP/1.1" 200 10308 "http://10.10.0.27/adm/index.php?i=acp_extensions&sid=041ca559047
67dfc066187582&mode=main&action=enable&ext_name=rokx%2Fdborldap&hash=f8bbcf4e" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebkit/537.36 (KHTML, like Gecko) Ch 3ba2267dfc06618758Z&mode=main&action=enable&ext_name=rokxe2roboficospanain
me/112.0.0.0 Safari/537.36"

10.255.254.2 - [25/Apr/2023:12:46:10 +0100] "GET /adm/style/admin.js?assets_version=4 HTTP/1.1" 200 2568 "http://10.10.0.27/adm/index.php?i=acp_extensions&sid=041ca55904751
a2267dfc06618758Z&mode=main&action=list" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
10.10.0.78 - [26/Apr/2023:11:53:12 +0100] "GET /adm/style/admin.css?assets_version=4 HTTP/1.1" 200 10307 "http://10.10.0.27/adm/index.php?i=acp_help_phpb&mode=help_phpb&s:
=eca30c1b75dc3eed1720423aa1ff9577" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"



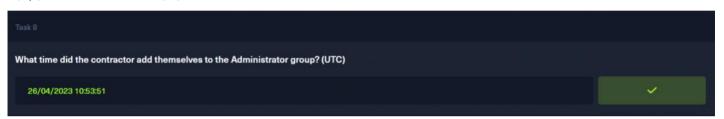
What time did the contractor add themselves to the Administrator group? (UTC)

C:\Users\Avior\Desktop\bumblebee

\(\) cat access.log \| grep group

10.10.8.78 - \[26/Apr/2023:11:53:34 +0100 \] "GET \| adm\index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=acp_groups&icat=12&mode=manage HTTP/1.1" 200 3418 \| "http://10.10.0.27/adm index.php?i=acp_users&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&action=list&g=5 \| HTTP/1.1" 200 3418 \| "http://10.10.0.27/adm index.php?i=acp_users&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&action=list&g=5 \| HTTP/1.1" 200 3941 \| "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&action=list&g=5 \| HTTP/1.1" 200 3941 \| "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&g=5 \| HTTP/1.1" 200 2623 \| "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&g=5 \| HTTP/1.1" 200 2623 \| "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&action=list&g=5 \| HTTP/1.1" 200 3966 \| "http://10.10.0.78 - \[26/Apr/2023:11:53:54 +0100 \] "GET \| adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&g=5 \| "Mozilla/5.0 \| (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefc \| 112.0.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&action=list&g=5 \| HTTP/1.1" 200 3966 \| "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&g=5 \| "Mozilla/5.0 \| (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefc \| 112.0.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&g=5 \| "Mozilla/5.0 \| (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefc \| 112.0.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&g=5 \| "Mozilla/5.0 \| (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefc \| 112.0.0.27/adm/index.php?i=acp_groups&sid=eca30c1b7

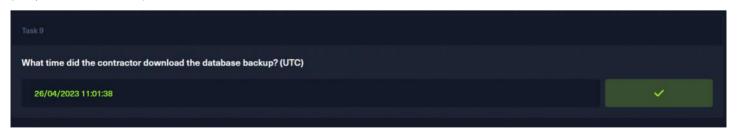
26/Apr/2023:11:53:51 +0100 -> 26/04/2023 10:53:51 UTC



What time did the contractor download the database backup? (UTC)

C:\Users\Avion\Desktop\bumblebee
 \tau access.log | grep backup
 10.10.78 - [26/Apr/2023:11:54:17 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=acp_database&mode=backup HTTP/1.1" 200 3768 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=25" "Mozilla/s.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/2010011 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:11:54:22 +0100] "DOST /adm/index.php?l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&mode=backup&action=download HTTP/1.1" 200 2463 "http://10.10.0.78 - [26/Apr/2023:11:54:22 +0100] "DOST /adm/index.php?l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&mode=backup&action=download HTTP/1.1" 200 2463 "http://10.10.0.78 - [26/Apr/2023:11:54:24 +0100] "GET /adm/index.php?l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&mode=backup&action=download HTTP/1.1" 200 3771 "http://lo.10.0.78 - [26/Apr/2023:11:54:30 +0100] "DOST /adm/index.php?l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&mode=backup&action=download HTTP/1.1" 200 2474 "http://lo.10.0.78 - [26/Apr/2023:11:54:30 +0100] "GET /adm/index.php?l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&mode=backup&action=download HTTP/1.1" 200 2474 "http://lo.10.0.78 - [26/Apr/2023:11:55:28 +0100] "GET /adm/index.php?l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&mode=backup&action=download HTTP/1.1" 200 3770 "http://lo.10.0.27/adm/index.php?l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&l=acp_database&sid=eca30c1b75dc3eed1720423aa1ff9577&l=acp_database&mode=backup HTTP/1.1" 200 3770 "http://lo.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&l=acp_database&mode=backup HTTP/1.1" 200 3770 "http://lo.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&l=acp_database&mode=backup HTTP/1.1" 200 3770 "http://lo.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&l=acp_database&mode=backup HTTP/1.1" 200 3770 "http://lo.10.0.27/adm/index.p

[26/Apr/2023:12:01:38 +0100] -> 26/04/2023 11:01:38 UTC



What was the size in bytes of the database backup as stated by access.log?

php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=25" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"

10.10.0.78 - [26/Apr/2023:12:01:38 +0100] "GET /store/backup_1682506471_dcsr71p7fyijoyq8.sql.gz HTTP/1.1" 200 34707 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"

10.10.0.78 - [26/Apr/2023:12:01:52 +0100] "GET /ucp.php?mode=logout&sid=eca30c1b75dc3eed1720423aa1ff9577 HTTP/1.1" 302 949 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=acp_database&mode=backup" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"

10.10.0.78 - [26/Apr/2023:12:01:53 +0100] "GET /index.php?sid=ba3cc5e2de08bafa4044f552813e2cbe HTTP/1.1" 200 3796 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423

aa1ff9577&i=acp_database&mode=backup" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"



