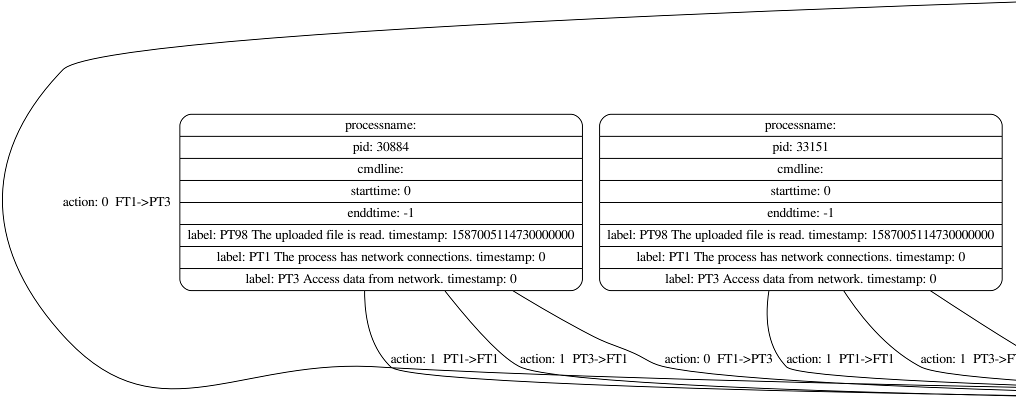
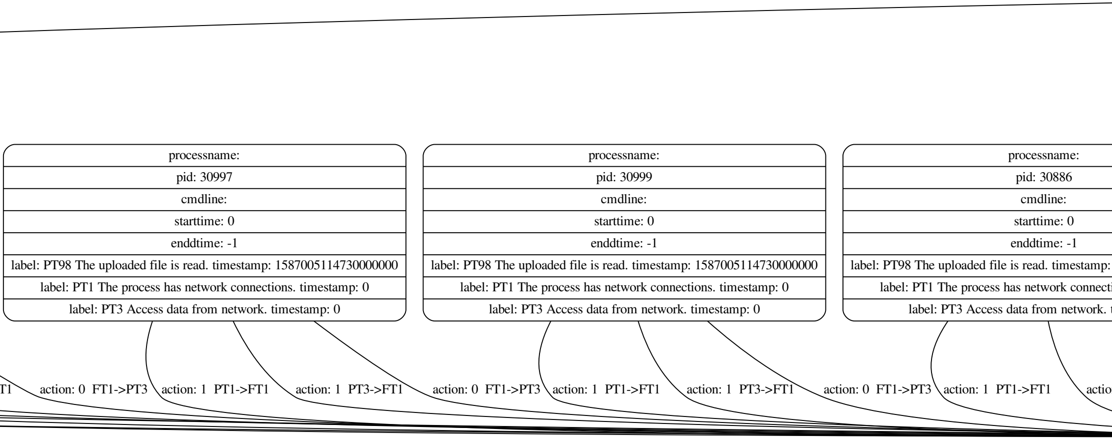
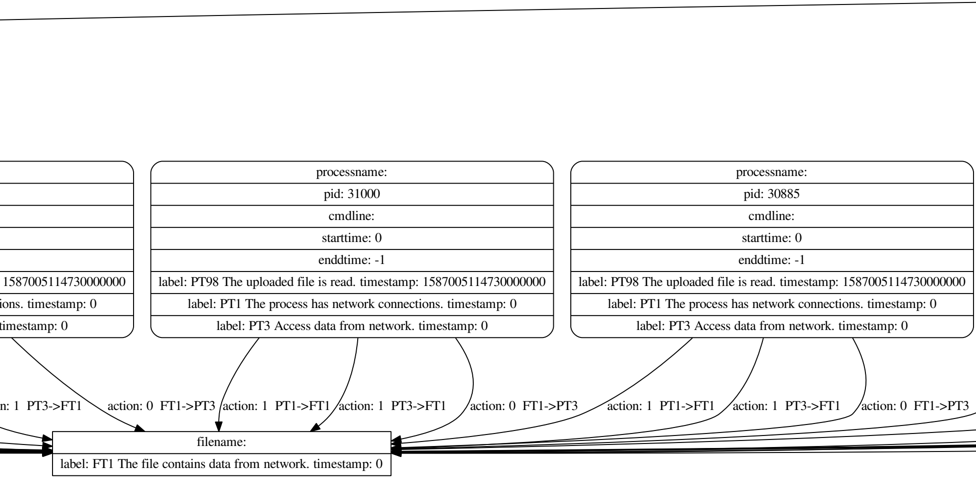
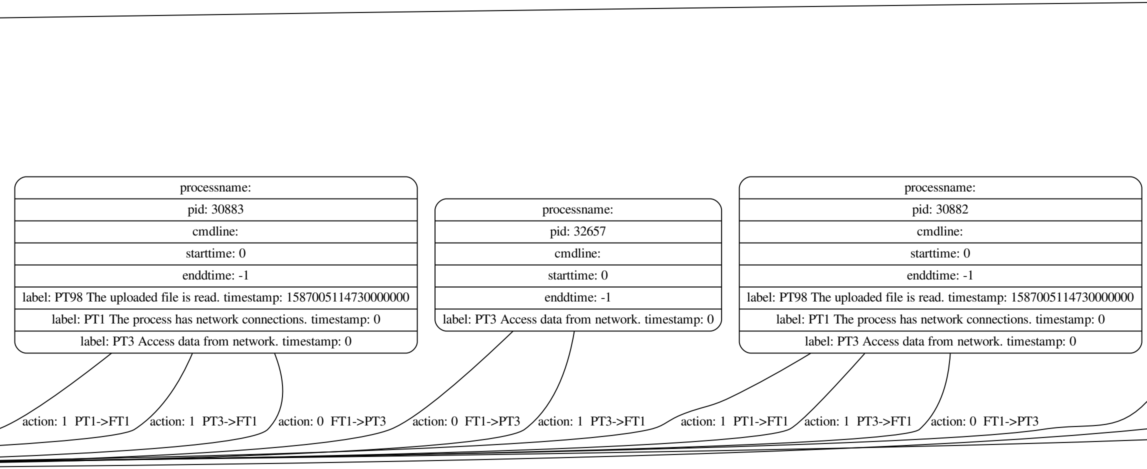
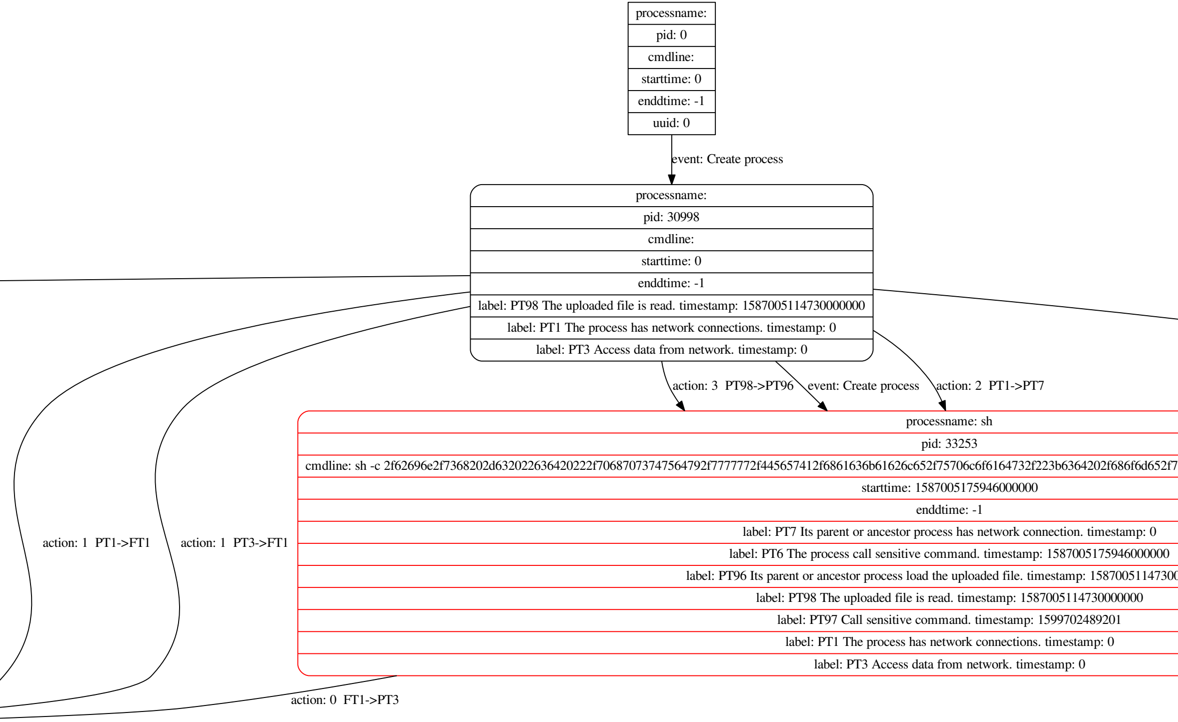

processname:
pid: 30884
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0
processname:
pid: 33151
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0
action: 0 FT1->PT3
action: 1 PT1->FT1
action: 1 PT3->FT1
action: 0 FT1->PT3
action: 1 PT1->FT1
action: 1 PT3->F


processname:
pid: 30997
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0
processname:
pid: 30999
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0
processname:
pid: 30886
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp:
label: PT1 The process has network connecti
label: PT3 Access data from network. t
T1
action: 0 FT1->PT3
action: 1 PT1->FT1
action: 1 PT3->FT1
action: 0 FT1->PT3
action: 1 PT1->FT1
action: 1 PT3->FT1
action: 0 FT1->PT3
action: 1 PT1->FT1
actio



1587005114730000000
ions. timestamp: 0
timestamp: 0
processname:
pid: 31000
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0
processname:
pid: 30885
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0
n: 1 PT3->FT1
action: 0 FT1->PT3
action: 1 PT1->FT1
action: 1 PT3->FT1
action: 0 FT1->PT3
action: 1 PT1->FT1
action: 1 PT3->FT1
action: 0 FT1->PT3
filename:
label: FT1 The file contains data from network. timestamp: 0


processname:
pid: 30883
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0
processname:
pid: 32657
cmdline:
starttime: 0
enddtime: -1
label: PT3 Access data from network. timestamp: 0
processname:
pid: 30882
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0
action: 1 PT1->FT1
action: 1 PT3->FT1
action: 0 FT1->PT3
action: 0 FT1->PT3
action: 1 PT3->FT1
action: 1 PT1->FT1
action: 1 PT3->FT1
action: 0 FT1->PT3

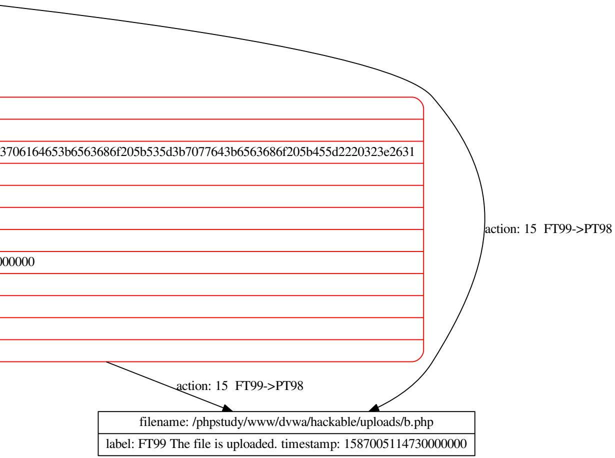


event: Create process
action: 3 PT98->PT96
event: Create process
action: 2 PT1->PT7
action: 1 PT1->FT1
action: 1 PT3->FT1
action: 0 FT1->PT3

processname:
pid: 0
cmdline:
starttime: 0
enddtime: -1
uuid: 0

processname:
pid: 30998
cmdline:
starttime: 0
enddtime: -1
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0

processname: sh
pid: 33253
cmdline: sh -c 2f62696e2f7368202d632022636420222f70687073747564792f7777772f445657412f6861636b61626c652f75706c6f6164732f223b6364202f686f6d652f7
starttime: 1587005175946000000
enddtime: -1
label: PT7 Its parent or ancestor process has network connection. timestamp: 0
label: PT6 The process call sensitive command. timestamp: 1587005175946000000
label: PT96 Its parent or ancestor process load the uploaded file. timestamp: 158700511473000
label: PT98 The uploaded file is read. timestamp: 1587005114730000000
label: PT97 Call sensitive command. timestamp: 1599702489201
label: PT1 The process has network connections. timestamp: 0
label: PT3 Access data from network. timestamp: 0


3706164653b6563686f205b535d3b7077643b6563686f205b455d2220323e2631
000000
action: 15 FT99->PT98
action: 15 FT99->PT98
filename: /phpstudy/www/dvwa/hackable/uploads/b.php
label: FT99 The file is uploaded. timestamp: 1587005114730000000