A3 – IPS Testing Documentation

Ben Soer

A00843110

Table of Contents

Unit Tests

All unit tests can be examined closer by looking at the appropriate unit test class located in the tests folder. For example to find unit tests for the ArgParcer class, look in the ArgParcerTest.php file. Each test will be labeled with a comment matching the test numbers listed below.

Results will be listed below with screenshots of the results form execution by PHPUnit

Summary

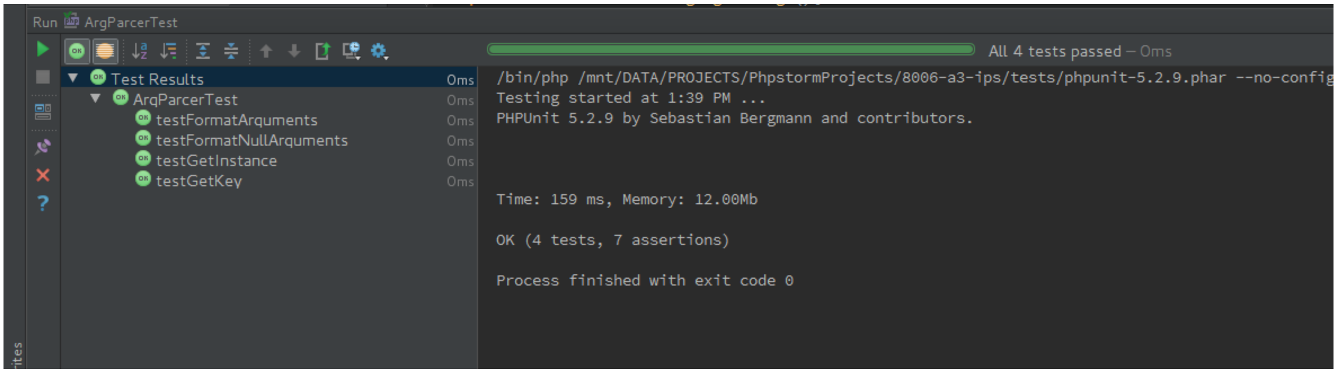
Test #	Class	Test Procedure	Parameters	Expected Outcome	Actual Outcome
AP_UT1	ArgParcer	Can format arguments	`Array("programname", "-a", "value1", "-b", "value2");`	Associative array is returned not empty and has keys “-a” and “-b”	Associative array is returned not empty and has keys “-a” and “-b”
AP_UT2	ArgParcer	Can format an empty array of arguments	`Array()`	Returned value should be an empty array	Returned value is an empty array
AP_UT3	ArgParcer	Can create an instance	N/A	An instance of ArgParcer is returned	An instance of ArgParcer is returned
AP_UT4	ArgParcer	Can get a key from the instance from the given formatted array	`Array("programname", "-a", "value1", "-b", "value2");`	Getting a value with key “-a” will return “value1” and a key of “-b” will return “value2”	Getting a value with key “-a” returns “value1” and a key of “-b” returns “value2”
RM_UT1	RecordManager	Can create an instance	N/A	Instance will create an instance of “RecordManager”	Instantiation creates an instance of “RecordManager”
RM_UT2	RecordManager	Can add a record	Generic record	Record Manager will not be empty and the record manager's array will have our record in it	Record Manager is not be empty and the record manager's array has our record in it
RM_UT3	RecordManager	Can delete a	Generic record	Deleting a	Deleting a

		record		record will have the RecordManagers array empty	record has the RecordManagers array empty
RM_UT4	RecordManager	Can update a record	Generic record	Updating a record will update a record in the record manager with our changes	Updating a record will update a record in the record manager with our changes
RM_UT5	RecordManager	Can get record if exists	Fetching a generic record that does exist	Returned value will be an instance of “Record”	Returned value is an instance of “Record”
RM_UT6	RecordManager	Can get record if exists	Fetching a generic record that does not exist	Returned value will be null	Returned value is null
RM_UT7	RecordManager	Record with attempts under threshold or with identicle timespread can be detected	Determine if a record is offending with identical dates for offence times	Return value will be true as this is an offence	Return value is true
RM_UT8	RecordManager	Record with attempts not under threshold will not be detected as a regular offence	Determine if a record is offending with 2 identical and 1 far future offence time	Return value will be false as this is not an offence	Return value is false
R_UT1	Record	Instantiate record	N/A	Will create instance of “Record”	Created an instance of “Record”
R_UT2	Record	Check Default Attributes	N/A	Default Attributes will be as expected when hardcoded in Record.php file	Default Attributes are as expected
R_UT3	Record	Check Changing Default Attributes		Changes will work	Changes work
SC_UT1	ServiceChecker			Can identify valid SSH	Can identify valid SSH

				record	record
SC_UT2	ServiceChecker			Can identify invalid SSH record	Can identify invalid SSH record
S_UT1	Settings	Check default attributes	N/A	Default attributes are equal to those hardcoded in the Settings.php file	Default attributes are equal to those hardcoded in the Settings.php file
S_UT2	Settings	Check instantiate creates instance of “Settings”	N/A	Creates an instance of “Settings”	Creates an instance of “Settings”
S_UT3	Settings	Check changing settings works	N/A	Altered settings are still their values when changed	Altered settings are still their values when changed

Results

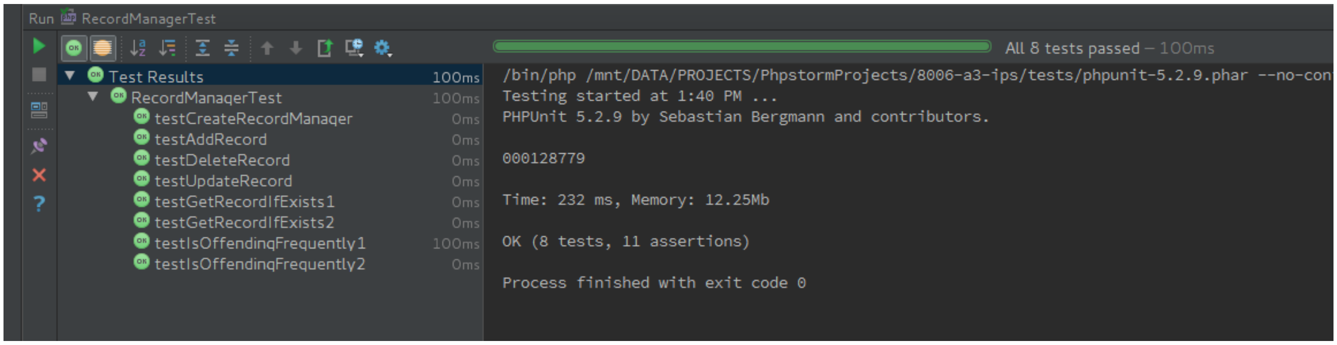
ArgParcer Unit Tests



```
Test Results                  0ms
  ArqParcerTest               0ms
    testFormatArquments       0ms
    testFormatNullArquments   0ms
    testGetInstance           0ms
    testGetKey                0ms
```

```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/tests/phpunit-5.2.9.phar --no-config
Testing started at 1:39 PM ...
PHPUnit 5.2.9 by Sebastian Bergmann and contributors.



Time: 159 ms, Memory: 12.00Mb

OK (4 tests, 7 assertions)

Process finished with exit code 0
```

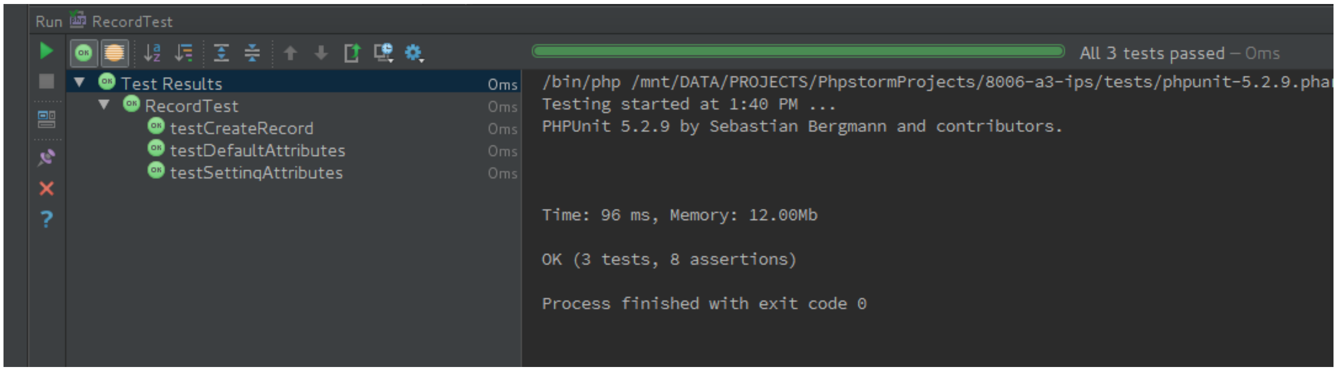
RecordManager Unit Tests



```
Test Results                      100ms
  RecordManaqerTest               100ms
    testCreateRecordManaqer         0ms
    testAddRecord                   0ms
    testDeleteRecord                0ms
    testUpdateRecord                0ms
    testGetRecordIfExists1          0ms
    testGetRecordIfExists2          0ms
    testIsOffendinqFrequently1    100ms
    testIsOffendinqFrequently2      0ms
```

```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/tests/phpunit-5.2.9.phar --no-con
Testing started at 1:40 PM ...
PHPUnit 5.2.9 by Sebastian Bergmann and contributors.

000128779

Time: 232 ms, Memory: 12.25Mb

OK (8 tests, 11 assertions)

Process finished with exit code 0
```

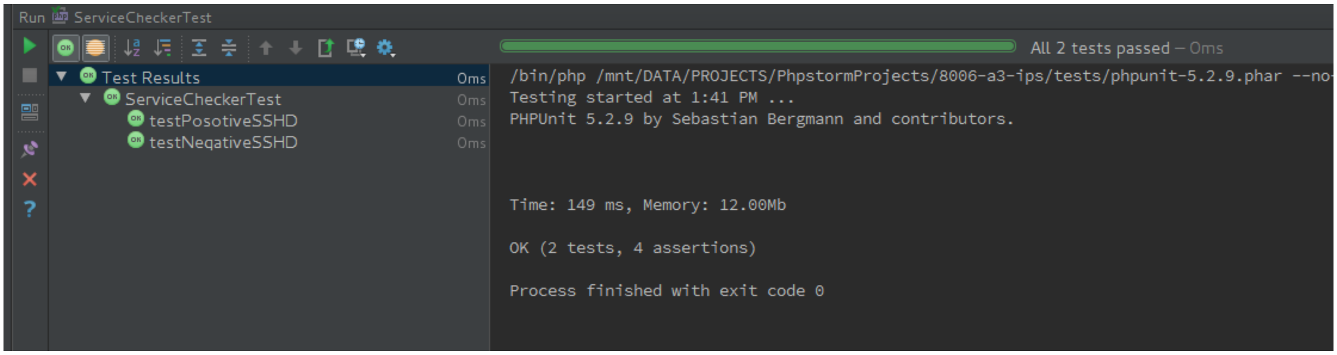
Record Unit Tests



```
▼ Test Results                    0ms
  ▼ RecordTest                    0ms
      testCreateRecord            0ms
      testDefaultAttributes       0ms
      testSettingAttributes       0ms
```

```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/tests/phpunit-5.2.9.phar
Testing started at 1:40 PM ...
PHPUnit 5.2.9 by Sebastian Bergmann and contributors.



Time: 96 ms, Memory: 12.00Mb

OK (3 tests, 8 assertions)

Process finished with exit code 0
```

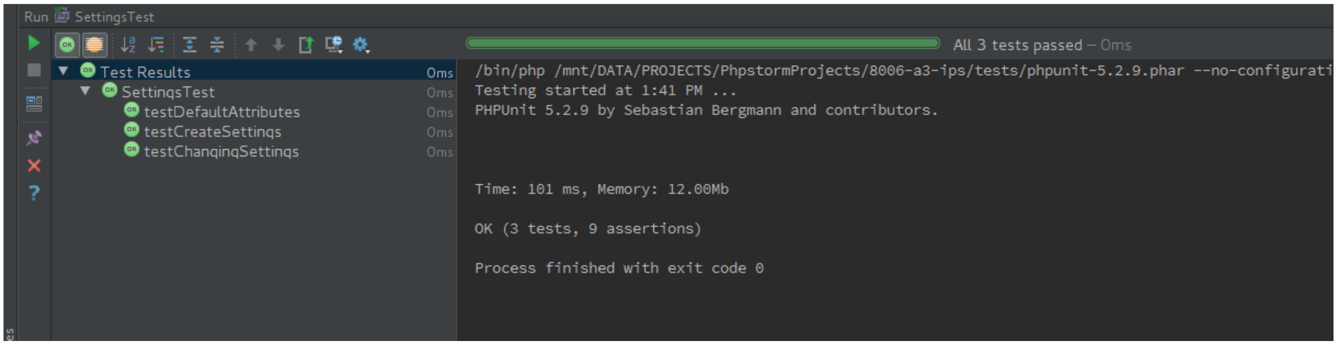
ServiceChecker Unit Tests



```
▼ Test Results                    0ms
  ▼ ServiceCheckerTest            0ms
      testPosotiveSSHD            0ms
      testNegativeSSHD            0ms
```

```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/tests/phpunit-5.2.9.phar --no-
Testing started at 1:41 PM ...
PHPUnit 5.2.9 by Sebastian Bergmann and contributors.



Time: 149 ms, Memory: 12.00Mb

OK (2 tests, 4 assertions)

Process finished with exit code 0
```

Settings Unit Tests



```
▼ Test Results                    0ms
  ▼ SettingsTest                  0ms
      testDefaultAttributes       0ms
      testCreateSettings          0ms
      testChangingSettings        0ms
```

```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/tests/phpunit-5.2.9.phar --no-configurati
Testing started at 1:41 PM ...
PHPUnit 5.2.9 by Sebastian Bergmann and contributors.



Time: 101 ms, Memory: 12.00Mb

OK (3 tests, 9 assertions)

Process finished with exit code 0
```

General Tests

Summary

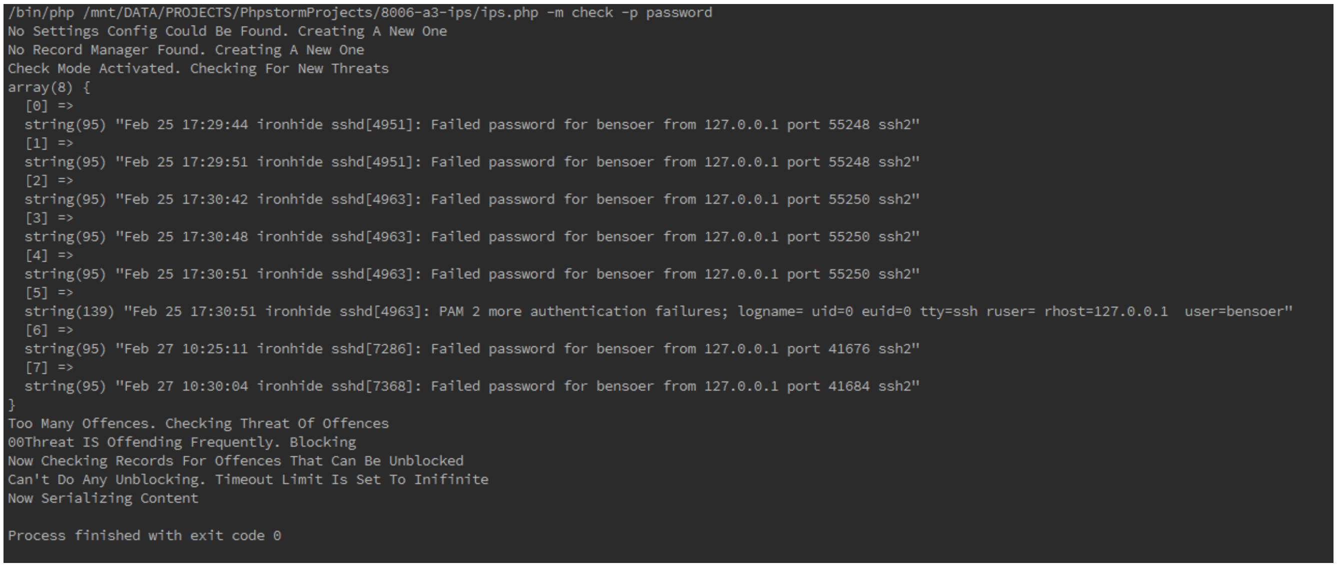
Test #	Class	Test Procedure	Parameters	Expected Outcome	Actual Outcome
SSH_T1		Fail SSH login 3 times	Block has no release time. Read from /var/log/secure	Ips blocks after reading it out of logs	Ips blocks after reading it out of logs
SSH_T2		Fail SSH Login	Read from	Ips blocks after	Ips blocks after

		3 times, wait 3 minutes. Run again	/var/log/secure	reading it out of logs and then unblocks after 3 minutes	reading it out of logs and then unblocks after 3 minutes
SSH_T3		3 times, wait 3minutes. Run again	/var/log/messages	Ips blocks after reading it out of logs	Ips blocks after reading it out of logs
SSH_T4		3 times, wait 3minutes. Run again	/var/log/messages	Ips blocks after reading it out of logs and then unblocks after 3 minutes	Ips blocks after reading it out of logs and then unblocks after 3 minutes
G_T1		Fail a login	Block has no release time. Read from /var/log/messages	Block should never be released	Block is never released
TELNET_T1		Fail Telnet Login 3 times	Block has no release time. Read from /var/log/messages	Block should never be released	Block is never released
TELNET_T2		Fail Telnet Login 3 times, wait 3 minutes		Ips blocks after reading it out of logs and then unblocks after 3 minutes	Ips blocks after reading it out of logs and then unblocks after 3 minutes
G_T2		Change Settings	-tl 3 -al 3 -ld /var/log/messages	Ips time limit is set to 3 min, attempt limit is set to 3 and log dir is set to the messages file	Ips time limit is set to 3 min, attempt limit is set to 3 and log dir is set to the messages file

Results

SSH_T1

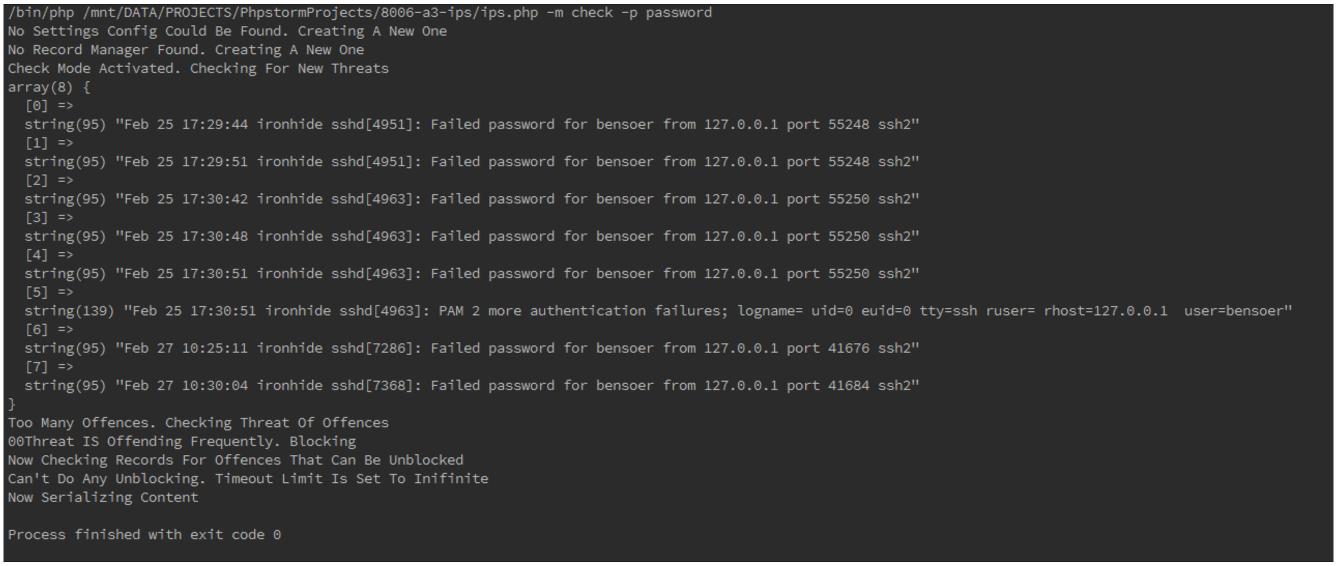
Blocking Found



```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/ips.php -m check -p password
No Settings Config Could Be Found. Creating A New One
No Record Manager Found. Creating A New One
Check Mode Activated. Checking For New Threats
array(8) {
  [0] =>
  string(95) "Feb 25 17:29:44 ironhide sshd[4951]: Failed password for bensoer from 127.0.0.1 port 55248 ssh2"
  [1] =>
  string(95) "Feb 25 17:29:51 ironhide sshd[4951]: Failed password for bensoer from 127.0.0.1 port 55248 ssh2"
  [2] =>
  string(95) "Feb 25 17:30:42 ironhide sshd[4963]: Failed password for bensoer from 127.0.0.1 port 55250 ssh2"
  [3] =>
  string(95) "Feb 25 17:30:48 ironhide sshd[4963]: Failed password for bensoer from 127.0.0.1 port 55250 ssh2"
  [4] =>
  string(95) "Feb 25 17:30:51 ironhide sshd[4963]: Failed password for bensoer from 127.0.0.1 port 55250 ssh2"
  [5] =>
  string(139) "Feb 25 17:30:51 ironhide sshd[4963]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1  user=bensoer"
  [6] =>
  string(95) "Feb 27 10:25:11 ironhide sshd[7286]: Failed password for bensoer from 127.0.0.1 port 41676 ssh2"
  [7] =>
  string(95) "Feb 27 10:30:04 ironhide sshd[7368]: Failed password for bensoer from 127.0.0.1 port 41684 ssh2"
}
Too Many Offences. Checking Threat Of Offences
00Threat IS Offending Frequently. Blocking
Now Checking Records For Offences That Can Be Unblocked
Can't Do Any Unblocking. Timeout Limit Is Set To Inifinite
Now Serializing Content

Process finished with exit code 0
```

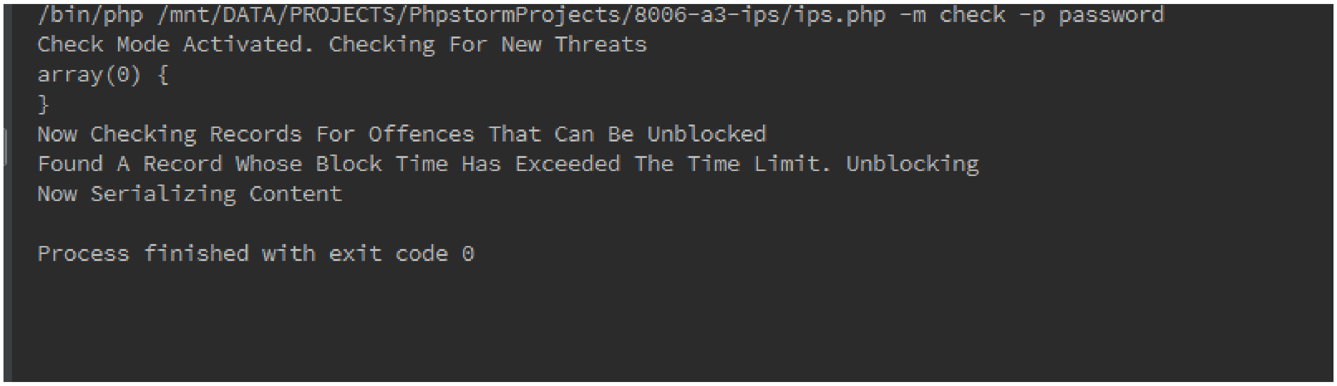
SSH_T2

Blocking Found



```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/ips.php -m check -p password
No Settings Config Could Be Found. Creating A New One
No Record Manager Found. Creating A New One
Check Mode Activated. Checking For New Threats
array(8) {
  [0] =>
  string(95) "Feb 25 17:29:44 ironhide sshd[4951]: Failed password for bensoer from 127.0.0.1 port 55248 ssh2"
  [1] =>
  string(95) "Feb 25 17:29:51 ironhide sshd[4951]: Failed password for bensoer from 127.0.0.1 port 55248 ssh2"
  [2] =>
  string(95) "Feb 25 17:30:42 ironhide sshd[4963]: Failed password for bensoer from 127.0.0.1 port 55250 ssh2"
  [3] =>
  string(95) "Feb 25 17:30:48 ironhide sshd[4963]: Failed password for bensoer from 127.0.0.1 port 55250 ssh2"
  [4] =>
  string(95) "Feb 25 17:30:51 ironhide sshd[4963]: Failed password for bensoer from 127.0.0.1 port 55250 ssh2"
  [5] =>
  string(139) "Feb 25 17:30:51 ironhide sshd[4963]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1  user=bensoer"
  [6] =>
  string(95) "Feb 27 10:25:11 ironhide sshd[7286]: Failed password for bensoer from 127.0.0.1 port 41676 ssh2"
  [7] =>
  string(95) "Feb 27 10:30:04 ironhide sshd[7368]: Failed password for bensoer from 127.0.0.1 port 41684 ssh2"
}
Too Many Offences. Checking Threat Of Offences
00Threat IS Offending Frequently. Blocking
Now Checking Records For Offences That Can Be Unblocked
Can't Do Any Unblocking. Timeout Limit Is Set To Inifinite
Now Serializing Content

Process finished with exit code 0
```

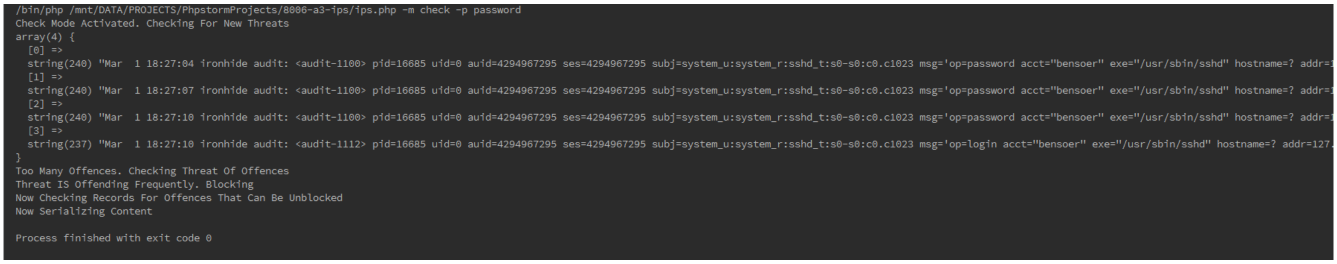
Blocking Released



```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/ips.php -m check -p password
Check Mode Activated. Checking For New Threats
array(0) {
}
Now Checking Records For Offences That Can Be Unblocked
Found A Record Whose Block Time Has Exceeded The Time Limit. Unblocking
Now Serializing Content

Process finished with exit code 0
```

SSH_T3

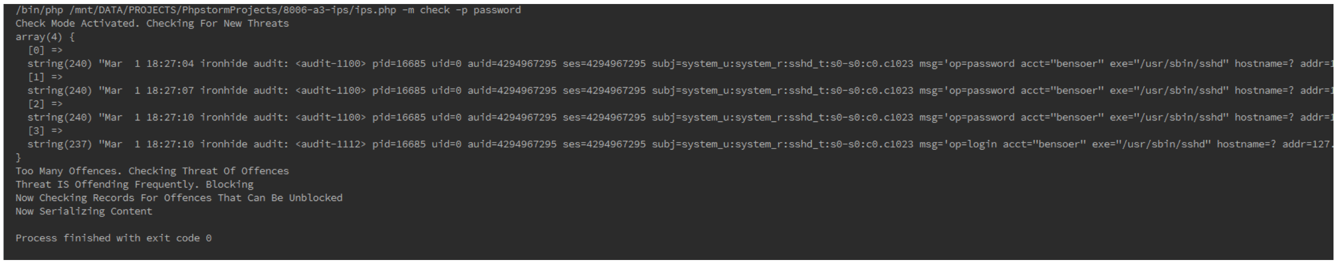
Blocking Found



```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/ips.php -m check -p password
Check Mode Activated. Checking For New Threats
array(4) {
  [0] =>
  string(240) "Mar  1 18:27:04 ironhide audit: <audit-1100> pid=16685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=password acct="bensoer" exe="/usr/sbin/sshd" hostname=? addr=1
  [1] =>
  string(240) "Mar  1 18:27:07 ironhide audit: <audit-1100> pid=16685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=password acct="bensoer" exe="/usr/sbin/sshd" hostname=? addr=1
  [2] =>
  string(240) "Mar  1 18:27:10 ironhide audit: <audit-1100> pid=16685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=password acct="bensoer" exe="/usr/sbin/sshd" hostname=? addr=1
  [3] =>
  string(237) "Mar  1 18:27:10 ironhide audit: <audit-1112> pid=16685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="bensoer" exe="/usr/sbin/sshd" hostname=? addr=127.
}
Too Many Offences. Checking Threat Of Offences
Threat IS Offending Frequently. Blocking
Now Checking Records For Offences That Can Be Unblocked
Now Serializing Content

Process finished with exit code 0
```

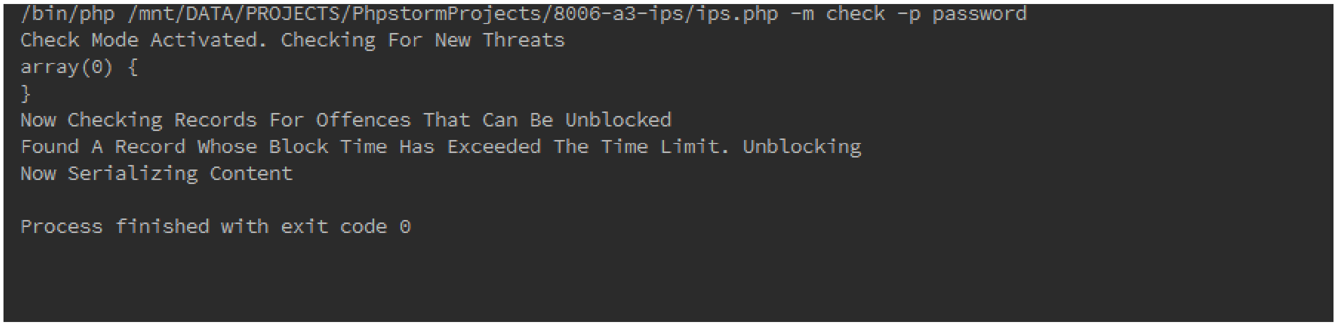
SSH_T4

Blocking Found



```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/ips.php -m check -p password
Check Mode Activated. Checking For New Threats
array(4) {
  [0] =>
  string(240) "Mar  1 18:27:04 ironhide audit: <audit-1100> pid=16685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=password acct="bensoer" exe="/usr/sbin/sshd" hostname=? addr=1
  [1] =>
  string(240) "Mar  1 18:27:07 ironhide audit: <audit-1100> pid=16685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=password acct="bensoer" exe="/usr/sbin/sshd" hostname=? addr=1
  [2] =>
  string(240) "Mar  1 18:27:10 ironhide audit: <audit-1100> pid=16685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=password acct="bensoer" exe="/usr/sbin/sshd" hostname=? addr=1
  [3] =>
  string(237) "Mar  1 18:27:10 ironhide audit: <audit-1112> pid=16685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="bensoer" exe="/usr/sbin/sshd" hostname=? addr=127.
}
Too Many Offences. Checking Threat Of Offences
Threat IS Offending Frequently. Blocking
Now Checking Records For Offences That Can Be Unblocked
Now Serializing Content

Process finished with exit code 0
```

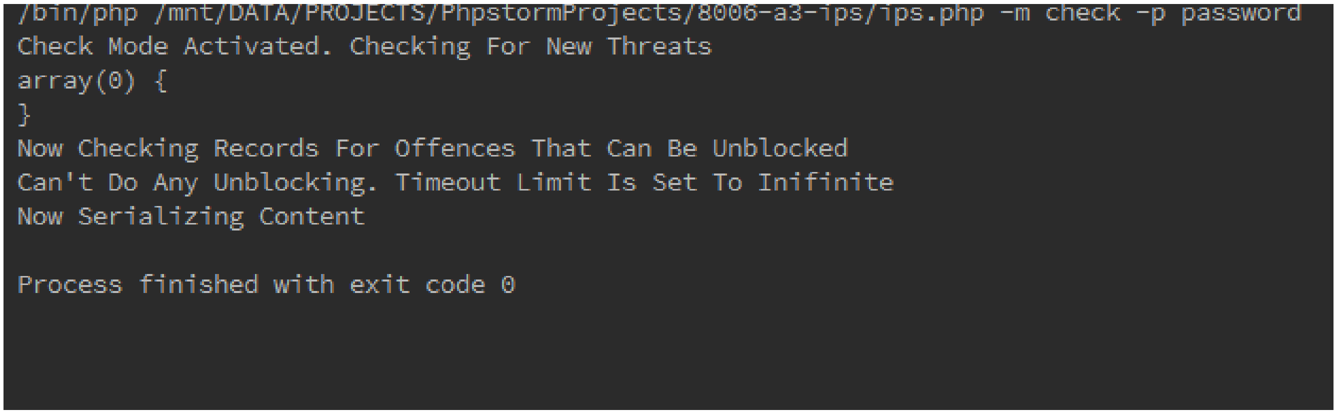
Blocking Released



```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/ips.php -m check -p password
Check Mode Activated. Checking For New Threats
array(0) {
}
Now Checking Records For Offences That Can Be Unblocked
Found A Record Whose Block Time Has Exceeded The Time Limit. Unblocking
Now Serializing Content

Process finished with exit code 0
```

G_T1

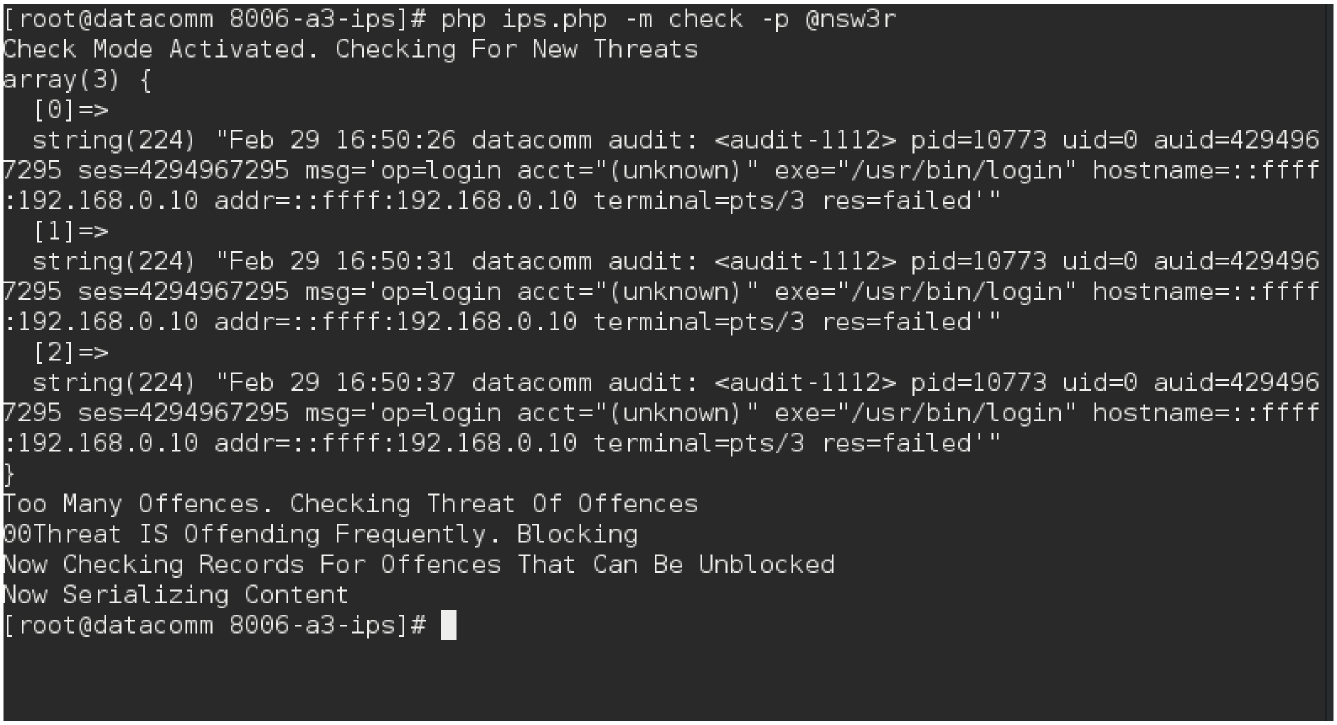
Block with No Release Time



```
/bin/php /mnt/DATA/PROJECTS/PhpstormProjects/8006-a3-ips/ips.php -m check -p password
Check Mode Activated. Checking For New Threats
array(0) {
}
Now Checking Records For Offences That Can Be Unblocked
Can't Do Any Unblocking. Timeout Limit Is Set To Inifinite
Now Serializing Content

Process finished with exit code 0
```

TELNET_T1

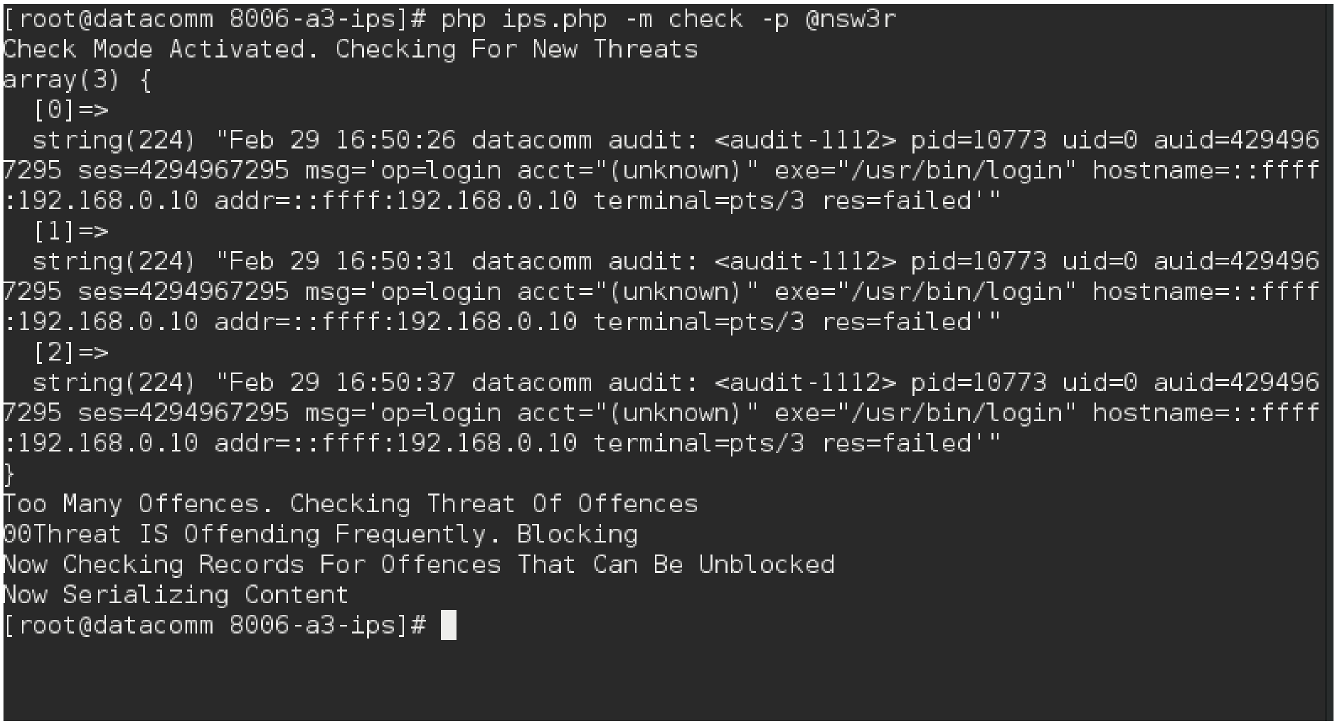
Block Found



```
[root@datacomm 8006-a3-ips]# php ips.php -m check -p @nsw3r
Check Mode Activated. Checking For New Threats
array(3) {
  [0]=>
  string(224) "Feb 29 16:50:26 datacomm audit: <audit-1112> pid=10773 uid=0 auid=429496
7295 ses=4294967295 msg='op=login acct="(unknown)" exe="/usr/bin/login" hostname=::ffff
:192.168.0.10 addr=::ffff:192.168.0.10 terminal=pts/3 res=failed'"
  [1]=>
  string(224) "Feb 29 16:50:31 datacomm audit: <audit-1112> pid=10773 uid=0 auid=429496
7295 ses=4294967295 msg='op=login acct="(unknown)" exe="/usr/bin/login" hostname=::ffff
:192.168.0.10 addr=::ffff:192.168.0.10 terminal=pts/3 res=failed'"
  [2]=>
  string(224) "Feb 29 16:50:37 datacomm audit: <audit-1112> pid=10773 uid=0 auid=429496
7295 ses=4294967295 msg='op=login acct="(unknown)" exe="/usr/bin/login" hostname=::ffff
:192.168.0.10 addr=::ffff:192.168.0.10 terminal=pts/3 res=failed'"
}
Too Many Offences. Checking Threat Of Offences
00Threat IS Offending Frequently. Blocking
Now Checking Records For Offences That Can Be Unblocked
Now Serializing Content
[root@datacomm 8006-a3-ips]# 
```

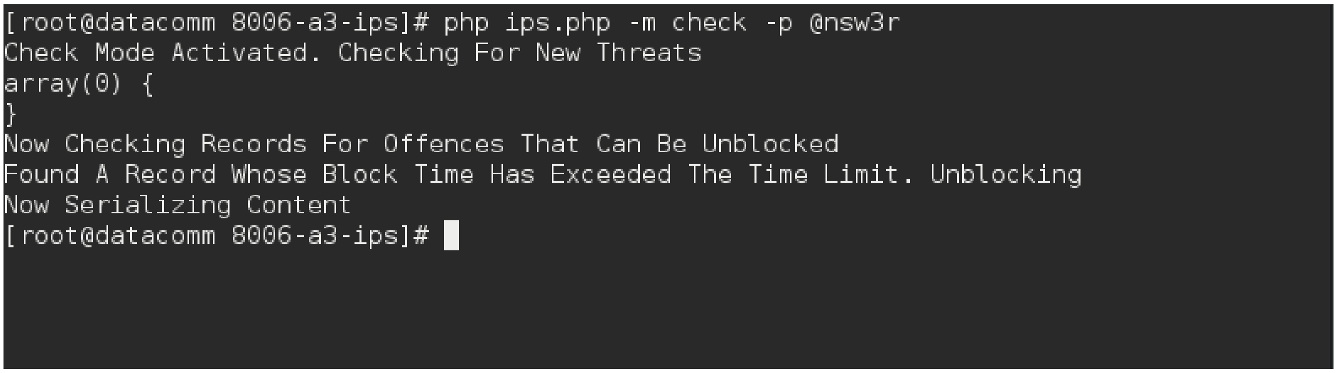
TELNET_T2

Block Found



```
[root@datacomm 8006-a3-ips]# php ips.php -m check -p @nsw3r
Check Mode Activated. Checking For New Threats
array(3) {
  [0]=>
  string(224) "Feb 29 16:50:26 datacomm audit: <audit-1112> pid=10773 uid=0 auid=429496
7295 ses=4294967295 msg='op=login acct="(unknown)" exe="/usr/bin/login" hostname=::ffff
:192.168.0.10 addr=::ffff:192.168.0.10 terminal=pts/3 res=failed'"
  [1]=>
  string(224) "Feb 29 16:50:31 datacomm audit: <audit-1112> pid=10773 uid=0 auid=429496
7295 ses=4294967295 msg='op=login acct="(unknown)" exe="/usr/bin/login" hostname=::ffff
:192.168.0.10 addr=::ffff:192.168.0.10 terminal=pts/3 res=failed'"
  [2]=>
  string(224) "Feb 29 16:50:37 datacomm audit: <audit-1112> pid=10773 uid=0 auid=429496
7295 ses=4294967295 msg='op=login acct="(unknown)" exe="/usr/bin/login" hostname=::ffff
:192.168.0.10 addr=::ffff:192.168.0.10 terminal=pts/3 res=failed'"
}
Too Many Offences. Checking Threat Of Offences
00Threat IS Offending Frequently. Blocking
Now Checking Records For Offences That Can Be Unblocked
Now Serializing Content
[root@datacomm 8006-a3-ips]# 
```

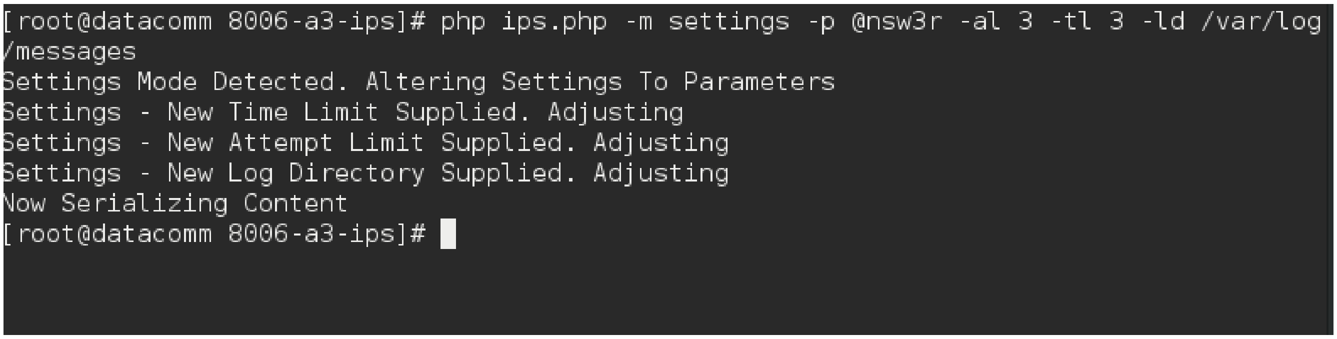
Blocking Released



```
[root@datacomm 8006-a3-ips]# php ips.php -m check -p @nsw3r
Check Mode Activated. Checking For New Threats
array(0) {
}
Now Checking Records For Offences That Can Be Unblocked
Found A Record Whose Block Time Has Exceeded The Time Limit. Unblocking
Now Serializing Content
[root@datacomm 8006-a3-ips]# 
```

G_T2

Settings Changed



```
[root@datacomm 8006-a3-ips]# php ips.php -m settings -p @nsw3r -al 3 -tl 3 -ld /var/log
/messages
Settings Mode Detected. Altering Settings To Parameters
Settings - New Time Limit Supplied. Adjusting
Settings - New Attempt Limit Supplied. Adjusting
Settings - New Log Directory Supplied. Adjusting
Now Serializing Content
[root@datacomm 8006-a3-ips]# 
```