

path / file:	<input type="text" value="/var/www/"/>		
verbosity level:	<input type="text" value="1. user tainted only"/>	vuln type:	<input type="text" value="All"/>
code style:	<input type="text" value="ayti"/>	<input type="text" value="bottom-up"/>	/regex/: <input type="text"/>

File: /var/www/MISP/MISP/app/Lib/Tools/XMLConverterTool.php**Code Execution**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
174: preg_replace $field = preg_replace('/[^\x{0009}\x{000a}\x{000d}\x{0020}-\x{D7FF}\x{E000}-\x{FFFD}]+/u', '', $field);
```

[hide all](#)**File: /var/www/MISP/MISP/app/Lib/Tools/ComplexTypeTool.php****Code Execution**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
159: preg_replace $ioc = preg_replace('/\p{C}+/u', '', $ioc);
```

requires:

```
153: if(!empty($iocArray))
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
208: preg_replace $inputRefanged = preg_replace($regex, $replacement, $inputRefanged);
207: foreach($this->__refangRegexTable as $regex=>$replacement)
207: foreach($this->__refangRegexTable as $regex=>$replacement)
```

[hide all](#)**File: /var/www/MISP/MISP/app/Lib/Tools/PubSubTool.php****File Disclosure**

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
21: file $settingsFile = new file(APP . 'files' . DS . 'scripts' . DS . 'mispzmq' . DS
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
47: file $pidFile = new file(APP . 'files' . DS . 'scripts' . DS . 'mispzmq' . DS . 'mi
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
51: shell_exec $result = trim(shell_exec('ps aux | awk \'{print $2}\' | grep "^' . $pid
48: $pid = $pidFile->read(true, 'r');
```

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
64: sleep sleep(1);
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
70: shell_exec $result = trim(shell_exec('python ' . APP . 'files' . DS . 'scripts' . DS
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
79: shell_exec shell_exec('python ' . APP . 'files' . DS . 'scripts' . DS . 'mispzmq' .
```

requires:

```
78: if($this->checkifrunning () == false)
```

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
146: sleep sleep(1);
```

requires:

```
139: if($this->checkifrunning ())
```

hide all

File: /var/www/MISP/MISP/app/Lib/Tools/FileAccessTool.php**File Disclosure**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
20: fread $readResult = fread($fileHandle, $fileSize);
    14: $fileHandle = fopen($file, 'rb');
        • 12: ↓ function readfromfile($file, $fileSize = - 1)
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
30: fwrite $writeResult = fwrite($fileHandle, $content);
    28: $fileHandle = fopen($file, 'wb');
        • 26: ↓ function writetofile($file, $content)
        • 26: ↓ function writetofile($file, $content)
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
43: unlink unlink($file);
    • 42: ↓ function deletefile($file)
```

hide all

File: /var/www/MISP/MISP/app/Lib/Tools/RandomTool.php**File Inclusion**

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
8: require_once require_once (APP . 'Lib' . DS . 'random_compat' . DS . 'lib' . DS . 'ra

requires:
    6: if(!function_exists('random_int'))
    7: if(file_exists(APP . 'Lib' . DS . 'random_compat' . DS . 'lib' . DS . 'ran
```

hide all

File: /var/www/MISP/MISP/app/Lib/Export/BroExport.php**Code Execution**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
171: preg_replace $attribute['value'] = preg_replace($this->mapping[$attribute['type']]
['replace'][0], $this->mapping[$attribute['type']]
['replace'][1], $attribute['value']);
```

requires:

```
158: if(isset($this->mapping[$attribute['type']]))
159: if(!$this->checkwhitelist($attribute['value'], $whitelist))
170: if(isset($this->mapping[$attribute['type']]['replace']))
```

hide all

File: /var/www/MISP/MISP/app/Lib/Export/NidsExport.php

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
400: preg_replace $tmpRule = preg_replace('/sid\s*:\s*[0-9]+\s*;', 'sid:' . $sid . ';', $tmpRule, - 1, $replaceCount['sid']);
• 386: ↓ function snortrule($ruleFormat, $attribute, &$sid, $ruleFormatMsg, $ruleForm
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
402: preg_replace $tmpRule = preg_replace('/rev\s*:\s*[0-9]+\s*;', 'rev:1;', $tmpRule, - 1, $replaceCount['rev']);
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
404: preg_replace $tmpRule = preg_replace('/classtype:[a-zA-Z_-]+;', 'classtype:' . $this->classtype . ';', $tmpRule, - 1, $replaceCount['classtyp
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
406: preg_replace $tmpRule = preg_replace('/msg\s*:\s*"(.*)" \s*;', sprintf($ruleFormat rule | $1') . ';', $tmpRule, - 1, $replaceCount['msg']);
• 386: ↓ function snortrule($ruleFormat, $attribute, &$sid, $ruleFormatMsg, $ruleForm
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

408: preg_replace $tmpRule = preg_replace('/reference\s*:
\s*\.+?;/', $ruleFormatReference . ';;', $tmpRule, - 1, $replaceCount['reference']);
• 386: ↓ function snortrule($ruleFormat, $attribute, &$sid, $ruleFormatMsg, $ruleForm

```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

410: preg_replace $tmpRule = preg_replace('/reference\s*:
\s*\.+?;/', $ruleFormatReference . ';;', $tmpRule, - 1, $replaceCount['reference']);
• 386: ↓ function snortrule($ruleFormat, $attribute, &$sid, $ruleFormatMsg, $ruleForm

```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

427: preg_replace $tmpRule = preg_replace('/:s*\)/', ';;' . $extraForRule . ';;', $tmpRu
425: $extraForRule .= $ruleFormatReference . ';;'; // if(0 == $replaceCount),
423: $extraForRule .= $tmpMessage . ';;'; // if(0 == $replaceCount),
421: $extraForRule .= 'classtype:' . $this->classtype . ';;'; // if(0 ==
419: $extraForRule .= 'rev:1;;'; // if(0 == $replaceCount),
417: $extraForRule .= 'sid:' . $sid . ';;'; // if(0 == $repl
415: $extraForRule = "";
• 386: ↓ function snortrule($ruleFormat, $attribute, &$si
• 386: ↓ function snortrule($ruleFormat, $attribute, &$sid, $ruleFormatMsg, $ru

```

hide all

File: /var/www/MISP/MISP/app/Lib/Network/Email/SmimeTransport.php

Protocol Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

59: mail($to, $subject, $message, $headers)
• 56: ↓ function _mail($to, $subject, $message, $headers, $params = null)
• 56: ↓ function _mail($to, $subject, $message, $headers, $params = null)

```

```

requires:
57: if(ini_get('safe_mode'))

```

Protocol Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

64: mail($to, $subject, $message, $headers, $params)
• 56: ↓ function _mail($to, $subject, $message, $headers, $params = null)
• 56: ↓ function _mail($to, $subject, $message, $headers, $params = null)

```

[hide all](#)**File: /var/www/MISP/MISP/app/Plugin/CertAuth/Controller/Component/Auth/CertificateAuthenticate.php****File Disclosure**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
262: file_get_contents $a = file_get_contents($url, false, $ctx);
255: $url .= (('&') : ('?')) . $k . '=' . urlencode(self::$user[$v]); //
if(isset($options), if(isset(self::$user)),
251: $url = $options['url'];
223: $options = Configure::read('CertAuth.restApi'); //
if(is_null($options)),
253: foreach($options['param'] as $k=>$v) // if(isset($options)),
223: $options = Configure::read('CertAuth.restApi'); //
if(is_null($options)),
241: foreach($options['headers'] as $k=>$v) // if(isset($options)),
223: $options = Configure::read('CertAuth.restApi'); //
if(is_null($options)),
226: $user = $user; // if(!is_null($user)),
• 220: ↴ function getrestuser($options = null, $user = null)
```

[hide all](#)**File: /var/www/MISP/MISP/app/View/Helper/XmlOutputHelper.php****Cross-Site Scripting**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
7: echo echo '<' . $k . '>';
5: foreach($array as $k=>$v)
• 4: ↴ function recursiveecho($array)
```

requires:

```
5: ↴ function recursiveecho($array)
6: if(is_array($v))
7: if(empty($v))
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
10: echo echo '<' . $k . '>';
5: foreach($array as $k=>$v)
• 4: ↴ function recursiveecho($array)
```

requires:

```
5: ↴ function recursiveecho($array)
```

```

6: if(is_array($v))
8: if(empty($v)) else

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

12: echo echo '<' . $k . '>';
5: foreach($array as $k=>$v)
    • 4: ↓ function recursiveecho($array)

```

requires:

```

5: ↓ function recursiveecho($array)
6: if(is_array($v))
8: if(empty($v)) else

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

17: echo echo '<' . $k . '>';
5: foreach($array as $k=>$v)
    • 4: ↓ function recursiveecho($array)

```

requires:

```

5: ↓ function recursiveecho($array)
15: if(is_array($v)) else
17: if($v == "" || $v == null)

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

19: echo echo '<' . $k . '>' . $v . '<' . $k . '>';
5: foreach($array as $k=>$v)
    • 4: ↓ function recursiveecho($array)
16: $v = 0;
5: foreach($array as $k=>$v)
    • 4: ↓ function recursiveecho($array)

```

requires:

```

5: ↓ function recursiveecho($array)
15: if(is_array($v)) else
18: if($v == "" || $v == null) else

```

hide all

File: /var/www/MISP/MISP/app/View/Helper/PivotHelper.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

68: echo echo ($v);
67: foreach($data as $k=>$v)
66: $data = array_merge($data, array('</div>'));
65: $data = array_merge($data, $temp);
64: $data = '<div class="pivotElement firstPivot ' . $pivotType .
    array()
59: $pivotType = ' activePivot'; // if($pivot == $currentEv
56: $pivotType = '';
• 63: $height = $height + 50;
    62: $height = $this->__findmaxheight($pivot);
        • 54: ↓ function convertpivottohtml($pivot, $curren
61: $temp = $this->__doconvert ($pivot, $currentEvent, $lookingAtR
    • 54: ↓ function convertpivottohtml($pivot, $currentEvent)
    • 54: ↓ function convertpivottohtml($pivot, $currentEvent)
58: $lookingAtRoot = true; // if($pivot == $currentEvent),

```

hide all

File: /var/www/MISP/MISP/app/Config/routes.php**File Inclusion**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

54: require require CAKE . 'Config' . DS . 'routes.php';

```

hide all

File: /var/www/MISP/MISP/app/Config/core.default.php**Possible Flow Control**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

139: define define('LOG_ERROR', LOG_ERR);

```

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

• 287: require_once require_once dirname(__DIR__) . '/Vendor/autoload.php';

```

hide all

File: /var/www/MISP/MISP/app/Console/Command/PasswordShell.php**Cross-Site Scripting**

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
13: echo echo 'MISP password reset command line tool.' . PHP_EOL . 'To assign a new pass
```

requires:

```
13: if(!isset($this->args[0]) || empty($this->args[0]) || !isset($this->args[
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
18: echo echo 'User not found. Make sure you use the correct syntax: /var/www/MISP/app  
/Console/cake Password [email] [password]' . PHP_EOL;
```

requires:

```
14: if(!isset($this->args[0]) || empty($this->args[0]) || !isset($this->args[
```

```
17: if(empty($results))
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
19: exit exit ;
```

requires:

```
14: if(!isset($this->args[0]) || empty($this->args[0]) || !isset($this->args[
```

```
17: if(empty($results))
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
25: echo echo 'Could not update account for User.id = ', $results['User']['id'], PHP_EOL  
16: $results = $this->User->find('first', array('conditions'=>array('email'=>$this->
```

requires:

```
14: if(!isset($this->args[0]) || empty($this->args[0]) || !isset($this->args[
```

```
24: if(!$this->User->save($results))
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
26: echo echo json_encode($this->User->validationErrors) . PHP_EOL;
```

requires:

```
14: if(!isset($this->args[0]) || empty($this->args[0]) || !isset($this->args[
```

```
24: if(!$this->User->save($results))
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
27: print\_r print_r($this->User->invalidfields(), true))
```

requires:

```
14: if(!isset($this->args[0]) || empty($this->args[0]) || !isset($this->args[
24: if(!$this->User->save($results))
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
29: echo echo 'Updated ', PHP_EOL;
```

requires:

```
14: if(!isset($this->args[0]) || empty($this->args[0]) || !isset($this->args[
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
31: exit exit ;
```

hide all

File: /var/www/MISP/MISP/app/Console/Command/Populate023Shell.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
9: sleep sleep(30);
```

hide all

File: /var/www/MISP/MISP/app/Console/Command/LiveShell.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
14: echo echo 'Invalid parameters. Usage: /var/www/MISP/app
/Console/cake Live [0|1]';
```

```
requires:
13: if($live != 0 && $live != 1)
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
19: echo echo $status;
18: $status = 'MISP is now live. Users can now log in.' : 'MISP is now disabled. Or
```

hide all

File: /var/www/MISP/MISP/app/Console/Command/ServerShell.php

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
4: require_once require_once 'AppShell.php'; // AppShell.php
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/Console/Command/EventShell.php

hide all

File: /var/www/MISP/MISP/app/Console/Command/populate20Shell.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
9: sleep sleep(30);
```

hide all

File: /var/www/MISP/MISP/app/Console/Command/EventShell.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
48: file $file = new file($dir->pwd() . DS . 'misp.xml' . '.ADMIN.xml'); //
```

AppShell.php

```
requires:
  47: if($user['Role']['perm_site_admin'])
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
50: file $file = new file($dir->pwd() . DS . 'misp.xml' . '.' . $user['Organisation']
['name'] . '.xml'); // AppShell.php
41: $user = $this->User->getauthuser($userId); // AppShell.php
39: $userId = $this->args[0]; // AppShell.php

requires:
  49: if($user['Role']['perm_site_admin']) else
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
82: file $file = new file($dir->pwd() . DS . 'misp.json' . '.ADMIN.json'); //
AppShell.php

requires:
  81: if($user['Role']['perm_site_admin'])
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
84: file $file = new file($dir->pwd() . DS . 'misp.json' . '.' . $user['Organisation']
['name'] . '.json'); // AppShell.php
75: $user = $this->User->getauthuser($userId); // AppShell.php
73: $userId = $this->args[0]; // AppShell.php

requires:
  83: if($user['Role']['perm_site_admin']) else
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
119: rename rename($result['data'], $stixFilePath); // AppShell.php
115: $result = $this->Event->stix(false, false, Configure::read('MISP.cached_attac
AppShell.php
107: $user = $this->User->getauthuser($userId); // AppShell.php
105: $userId = $this->args[0]; // AppShell.php
106: $id = $this->args[1]; // AppShell.php
113: $stixFilePath = $dir->pwd() . DS . 'misp.stix' . '.' . $user['Organisation']
```

```

107: $user = $this->User->getauthuser($userId); // AppShell.php
105: $userId = $this->args[0]; // AppShell.php
111: $stixFilePath = $dir->pwd() . DS . 'misp.stix' . '.ADMIN.xml'; // AppShell.php

requires:
118: if($result['success'])

```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

120: unlink unlink($result['data']); // AppShell.php
115: $result = $this->Event->stix(false, false, Configure::read('MISP.cached_attach
AppShell.php
107: $user = $this->User->getauthuser($userId); // AppShell.php
105: $userId = $this->args[0]; // AppShell.php
106: $id = $this->args[1]; // AppShell.php

requires:
118: if($result['success'])

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

166: file $file = new file($dir->pwd() . DS . 'misp.' . $extra . '.ADMIN.txt'); //
AppShell.php
160: $extra = $this->args[2]; // AppShell.php

requires:
165: if($user['Role']['perm_site_admin'])

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

168: file $file = new file($dir->pwd() . DS . 'misp.' . $extra . '.' . $user['Organisat
['name'] . '.txt'); // AppShell.php
160: $extra = $this->args[2]; // AppShell.php
157: $user = $this->User->getauthuser($userId); // AppShell.php
156: $userId = $this->args[0]; // AppShell.php

requires:
167: if($user['Role']['perm_site_admin']) else

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

205: file $file = new file($dir->pwd() . DS . 'misp.rpz.ADMIN.txt'); //
AppShell.php

```

```
requires:
  204: if($user['Role']['perm_site_admin'])
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
207: file $file = new file($dir->pwd() . DS . 'misp.rpz.' . $user['Organisation']
['name'] . '.txt'); // AppShell.php
188: $user = $this->User->getauthuser($userId); // AppShell.php
187: $userId = $this->args[0]; // AppShell.php
```

```
requires:
  206: if($user['Role']['perm_site_admin']) else
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
241: file $file = new file($dir->pwd() . DS . 'misp.' . $extra . '.ADMIN.csv'); //
AppShell.php
232: $extra = $this->args[2]; // AppShell.php
```

```
requires:
  240: if($user['Role']['perm_site_admin'])
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
243: file $file = new file($dir->pwd() . DS . 'misp.' . $extra . '.' . $user['Organisat
['name'] . '.csv'); // AppShell.php
232: $extra = $this->args[2]; // AppShell.php
229: $user = $this->User->getauthuser($userId); // AppShell.php
228: $userId = $this->args[0]; // AppShell.php
```

```
requires:
  242: if($user['Role']['perm_site_admin']) else
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
277: file $file = new file($dir->pwd() . DS . 'misp.text_' . $type . '.ADMIN.txt'); //
AppShell.php
274: foreach($types as $k=>$type) // AppShell.php
271: $types = array_keys($this->Attribute->typeDefinitions); //
AppShell.php
```

```

requires:
  274: ↵ function cachetext()
  276: if($user['Role']['perm_site_admin'])

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

279: file $file = new file($dir->pwd() . DS . 'misp.text_' . $type . '.' . $user['Organ
['name'] . '.txt'); // AppShell.php
274: foreach($types as $k=>$type) // AppShell.php
271: $types = array_keys($this->Attribute->typeDefinitions); // AppShell.php
268: $user = $this->User->getauthuser($userId); // AppShell.php
267: $userId = $this->args[0]; // AppShell.php

```

```

requires:
  274: ↵ function cachetext()
  278: if($user['Role']['perm_site_admin']) else

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

305: file $file = new file($dir->pwd() . DS . 'misp.' . $format . '.ADMIN.rules'); //
AppShell.php
300: $format = $this->args[2]; // AppShell.php

```

```

requires:
  304: if($user['Role']['perm_site_admin'])

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

307: file $file = new file($dir->pwd() . DS . 'misp.' . $format . '.' . $user['Organisa
['name'] . '.rules'); // AppShell.php
300: $format = $this->args[2]; // AppShell.php
297: $user = $this->User->getauthuser($userId); // AppShell.php
296: $userId = $this->args[0]; // AppShell.php

```

```

requires:
  306: if($user['Role']['perm_site_admin']) else

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

345: file $file = new file($dir->pwd() . DS . 'misp.bro.ADMIN.intel'); //
AppShell.php

```

```
requires:
  344: if($user['Role']['perm_site_admin'])
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
347: file $file = new file($dir->pwd() . DS . 'misp.bro.' . $user['Organisation']
[name'] . '.intel'); // AppShell.php
335: $user = $this->User->getauthuser($userId); // AppShell.php
334: $userId = $this->args[0]; // AppShell.php

requires:
  346: if($user['Role']['perm_site_admin']) else
```

hide all

File: /var/www/MISP/MISP/app/Console/Command/UserInitShell.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
91: echo $authkey . PHP_EOL;
70: $authkey = $this->User->generateauthkey();

requires:
  69: if($this->User->find('count') == 0)
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
93: echo 'Script aborted: MISP instance already initialised.' . PHP_EOL;

requires:
  92: if($this->User->find('count') == 0) else
```

hide all

File: /var/www/MISP/MISP/app/Console/Command/BaseurlShell.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.


```
14: echo echo 'Baseurl updated. Have a very safe and productive day.', PHP_EOL;
```

[hide all](#)

File: /var/www/MISP/MISP/app/Console/cake.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
24: ini_set ini_set('include_path', $root . $ds . 'lib' . PATH_SEPARATOR . ini_get('incl
23: $root = dirname(dirname(dirname(__FILE__)));
20: $ds = DIRECTORY_SEPARATOR;
```

requires:

```
22: if(function_exists('ini_set'))
```

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
27: include include ($dispatcher)
21: $dispatcher = dirname(__DIR__) . $ds . 'Lib' . $ds . 'cakephp' . $ds . 'lib' .
20: $ds = DIRECTORY_SEPARATOR;
20: $ds = DIRECTORY_SEPARATOR;
20: $ds = DIRECTORY_SEPARATOR;
20: $ds = DIRECTORY_SEPARATOR;
20: $ds = DIRECTORY_SEPARATOR;
20: $ds = DIRECTORY_SEPARATOR;
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
28: trigger_error trigger_error('Could not locate CakePHP core files.', E_USER_ERROR);
```

requires:

```
27: if(!include ($dispatcher))
```

[hide all](#)

File: /var/www/MISP/MISP/app/webroot/index.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
25: define define('DS', DIRECTORY_SEPARATOR);
```

```
requires:
  24: if(!defined('DS'))
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
38: define('ROOT', dirname(dirname(dirname(__FILE__))));
```

```
requires:
  37: if(!defined('ROOT'))
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
45: define('APP_DIR', basename(dirname(dirname(__FILE__))));
```

```
requires:
  44: if(!defined('APP_DIR'))
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
59: define('CAKE_CORE_INCLUDE_PATH', ROOT . DS . APP_DIR . DS . 'Lib' . DS . 'cake');
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
67: define('WEBROOT_DIR', basename(dirname(__FILE__)));
```

```
requires:
  66: if(!defined('WEBROOT_DIR'))
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
70: define define('WWW_ROOT', dirname(__FILE__) . DS);
```

```
requires:
  69: if(!defined('WWW_ROOT'))
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
75: ini_set ini_set('include_path', ROOT . DS . 'lib' . PATH_SEPARATOR . ini_get('include_path'));
38: define('ROOT', dirname(dirname(dirname(__FILE__))))); // define() if(!defined('ROOT'));
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
```

```
requires:
  73: if(!defined('CAKE_CORE_INCLUDE_PATH'))
  74: if(function_exists('ini_set'))
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
77: include include ('Cake' . DS . 'bootstrap.php')) // bootstrap.php
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
```

```
requires:
  73: if(!defined('CAKE_CORE_INCLUDE_PATH'))
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
81: include include (CAKE_CORE_INCLUDE_PATH . DS . 'Cake' . DS . 'bootstrap.php')) // bootstrap.php
59: define('CAKE_CORE_INCLUDE_PATH', ROOT . DS . APP_DIR . DS . 'Lib' . DS . 'cakephp' . DS . 'core' . DS . 'include');
define()
38: define('ROOT', dirname(dirname(dirname(__FILE__)))); // define() if(!defined('ROOT'))
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
45: define('APP_DIR', basename(dirname(dirname(__FILE__)))); // define() if(!defined('APP_DIR'))
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),

requires:
80: if(!defined('CAKE_CORE_INCLUDE_PATH')) else
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
86: trigger_error trigger_error("CakePHP core could not be found. Check the value of CAKE_CORE_INCLUDE_PATH in your /index.php. It should point to the directory containing your " . DS . "cake core directory". bootstrap.php)
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),
25: define('DS', DIRECTORY_SEPARATOR); // define() if(!defined('DS')),

requires:
85: if(!empty($failed))
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/app/index.php

hide all

File: /var/www/MISP/MISP/app/Model/ObjectRelationship.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
44: file $file = new file($relationsFile);
42: $relationsFile = APP . 'files/misp-objects/relationships/definition.json';
```

requires:

```
43: if(file_exists($relationsFile))
```

hide all

File: /var/www/MISP/MISP/app/Model/MispObject.php

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
312: usort usort($template['ObjectTemplateElement'], function ($a, $b){
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
387: file $tmpfile = new file($attribute['Attachment']['tmp_name']);
372: foreach($attributes['Attribute'] as $k=>$attribute)
    • 370: function attributecleanup($attributes)
```

requires:

```
383: if(isset($attribute['Attachment']))
```

hide all

File: /var/www/MISP/MISP/app/Model/Event.php

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
375: unlink unlink($dir);
    • 374: function destroydir($dir)
```

requires:

```
375: if(!is_dir($dir) || is_link($dir))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
376: scandir scandir($dir) as
    • 374: ↓ function destroydir($dir)
```

File Manipulation

Userinput reaches sensitive sink when function *destroydir()* is called. (Blind exploitation)

```
379: chmod chmod($dir . DS . $file, 0777);
    • 374: ↓ function destroydir($dir)
    • 376: foreach(scandir($dir) as $file)
        • 374: ↓ function destroydir($dir)

requires:
    378: if(!$this->destroydir ($dir . DS . $file))
    374: ↓ function destroydir($dir)
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
383: rmdir rmdir($dir);
    • 374: ↓ function destroydir($dir)
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
913: shell_exec $commit = trim(shell_exec('git log --pretty="%H" -n1 HEAD'));

requires:
    912: ↓ function addheaders($request)
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1972: preg_replace $subject = preg_replace("/\r|\n/", "", $event[0]['Event']
    ['info']);

requires:
    1971: if(Configure::read('MISP.extended_alert_subject'))
```

Code Execution

Userinput is used as dynamic function name. Arbitrary functions may be called.

```
2668: $saveMethod $saveMethod($object, $event);
2667: $saveMethod = '__savePrepared' . $object_type;
2665: foreach($objects as $object_type)
2664: $objects[2] = 'EventTag' // array()
2664: $objects[1] = 'ShadowAttribute' // array()
2664: $objects = 'Attribute' // array()
```

requires:

```
2665: ↓ function savepreparedevent($event)
2666: if(!empty($event[$object_type]))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3049: file $tempFile = new file($tmpDir . DS . $randomFileName, true, 0644);
3048: $tmpDir = APP . "files" . DS . "scripts" . DS . "tmp";
3047: $randomFileName = $this->generaterandomfilename();
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

- 3052: shell_exec \$result = shell_exec('python3 ' . \$scriptFile . ' ' . \$tempFile->path .
/exec-errors.log');
- 3051: \$scriptFile = APP . "files" . DS . "scripts" . DS . "stix2" . DS . "misp2sti>

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3055: file $resultFile = new file($tmpDir . DS . $randomFileName . '.out', true, 0644);
3048: $tmpDir = APP . "files" . DS . "scripts" . DS . "tmp";
3047: $randomFileName = $this->generaterandomfilename();
```

requires:

```
3054: if(trim($result) == 1)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3074: file $stixFile = new file($tmpDir . DS . $randomFileName . ".stix");
3073: $tmpDir = APP . "files" . DS . "scripts" . DS . "tmp";
3072: $randomFileName = $this->generaterandomfilename();
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

- 3075: `shell_exec` \$stix_framing = shell_exec('python ' . APP . "files" . DS . "scripts" . /exec-errors.log'
- 3064: `function` stix(\$id, \$tags, \$attachments, \$user, \$returnType = 'xml', \$from =

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3093: file $tempFile = new file($tmpDir . DS . $randomFileName, true, 0644);
3073: $tmpDir = APP . "files" . DS . "scripts" . DS . "tmp";
3072: $randomFileName = $this->generaterandomfilename();
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

- 3114: `shell_exec` \$result = shell_exec('python ' . \$scriptFile . ' ' . \$randomFileName . /exec-errors.log');
- 3113: `$scriptFile` = APP . "files" . DS . "scripts" . DS . "misp2stix.py";
- 3072: `$randomFileName` = \$this->generaterandomfilename();
- 3064: `function` stix(\$id, \$tags, \$attachments, \$user, \$returnType = 'xml', \$from =

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
3123: file $file = new file(APP . "files" . DS . "scripts" . DS . "tmp" . DS . $randomF
3072: $randomFileName = $this->generaterandomfilename());
```

hide all

File: /var/www/MISP/MISP/app/Model/Feed.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
84: file_get_contents $data = file_get_contents($feed['Feed']
['url'] . '/manifest.json');
• 80: function getneweventuuids($feed, $HttpSocket)

requires:
82: if(isset($feed['Feed']['input_source']) && $feed['Feed']
['input_source'] == 'local')
83: if(file_exists($feed['Feed']['url'] . '/manifest.json'))
```


File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
124: file_get_contents $data = file_get_contents($feed['Feed']
['url'] . '/manifest.json');
    • 119: ↓ function getmanifest($feed, $HttpSocket)

requires:
    122: if(isset($feed['Feed']['input_source']) && $feed['Feed']
['input_source'] == 'local')
    123: if(file_exists($feed['Feed']['url'] . '/manifest.json'))
```

Userinput is passed through function parameters.

```
907: ↑ $manifest = $this->getmanifest ($feed, $HttpSocket);
    • 898: ↓ function __cachemispfeed($feed, $redis, $HttpSocket, $jobId = false)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
156: file_get_contents $data = file_get_contents($feed['Feed']['url']);
    • 151: ↓ function getfreetextfeed($feed, $HttpSocket, $type = 'freetext', $page = 1,

requires:
    154: if(isset($feed['Feed']['input_source']) && $feed['Feed']['input_source']
155: if(file_exists($feed['Feed']['url']))
```

Userinput is passed through function parameters.

```
883: ↑ $values = $this->getfreetextfeed ($feed, $HttpSocket, $feed['Feed']
['source_format'], 'all');
    • 875: ↓ function __cachefreetextfeed($feed, $redis, $HttpSocket, $jobId = false)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
162: file $file = new file($feedCache);
159: $feedCache = APP . 'tmp' . DS . 'cache' . DS . 'misp_feed_' . intval($feed['Fe
    • 151: ↓ function getfreetextfeed($feed, $HttpSocket, $type = 'freetext', $page

requires:
    158: if(isset($feed['Feed']['input_source']) && $feed['Feed']['input_source']
161: if(file_exists($feedCache))
```

Userinput is passed through function parameters.

```
883: ↑ $values = $this->getfreetextfeed ($feed, $HttpSocket, $feed['Feed']
['source_format'], 'all');
    • 875: ↓ function __cachefreetextfeed($feed, $redis, $HttpSocket, $jobId = false)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
165: file_get_contents $data = file_get_contents($feedCache);
159: $feedCache = APP . 'tmp' . DS . 'cache' . DS . 'misp_feed_' . intval($feed['Feed']) . '.txt';
    • 151: function getfreetextfeed($feed, $HttpSocket, $type = 'freetext', $page)

requires:
158: if(isset($feed['Feed']['input_source']) && $feed['Feed']['input_source'] == 'file')
161: if(file_exists($feedCache))
163: if(time() - $file->lastchange() < 600)
```

Userinput is passed through function parameters.

```
883: getfreetextfeed ($feed, $HttpSocket, $feed['Feed'], $source_format, 'all');
    • 875: function __cachefreetextfeed($feed, $redis, $HttpSocket, $jobId = false)
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
186: file_put_contents file_put_contents($feedCache, $data);
159: $feedCache = APP . 'tmp' . DS . 'cache' . DS . 'misp_feed_' . intval($feed['Feed']) . '.txt';
    • 151: function getfreetextfeed($feed, $HttpSocket, $type = 'freetext', $page)
185: $data = $response->body;

requires:
158: if(isset($feed['Feed']['input_source']) && $feed['Feed']['input_source'] == 'file')
168: if($doFetch)
179: if($response->code == 200)
```

Userinput is passed through function parameters.

```
883: getfreetextfeed ($feed, $HttpSocket, $feed['Feed'], $source_format, 'all');
    • 875: function __cachefreetextfeed($feed, $redis, $HttpSocket, $jobId = false)
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
286: exec $results = $pipe->exec();
```

```
requires:
266: if($redis !== false)
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
307: exec $feedHits = $pipe->exec();
```

requires:

```
266: if($redis !== false)
296: if(!$overrideLimit && count($objects) > 10000) else
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
380: shell_exec $commit = trim(shell_exec('git log --pretty="%H" -n1 HEAD'));
```

requires:

```
379: ↓ function __createfeedrequest()
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
474: file_get_contents $data = file_get_contents($path);
471: $path = $feed['Feed']['url'] . '/' . $uuid . '.json';
    • 470: ↓ function downloadeventfromfeed($feed, $uuid, $user)
    • 470: ↓ function downloadeventfromfeed($feed, $uuid, $user)

requires:
472: if(isset($feed['Feed']['input_source']) && $feed['Feed']
    ['input_source'] == 'local')
473: if(file_exists($path))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
569: file_get_contents $data = file_get_contents($path);
566: $path = $feed['Feed']['url'] . '/' . $uuid . '.json';
    • 562: ↓ function __addeventfromfeed($HttpSocket, $feed, $uuid, $user, $filterR
    • 562: ↓ function __addeventfromfeed($HttpSocket, $feed, $uuid, $user, $filterR

requires:
567: if(isset($feed['Feed']['input_source']) && $feed['Feed']
    ['input_source'] == 'local')
568: if(file_exists($path))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
594: file_get_contents $data = file_get_contents($path);
591: $path = $feed['Feed']['url'] . '/' . $uuid . '.json';
    • 587: ↓ function __updateeventfromfeed($HttpSocket, $feed, $uuid, $eventId, $u
    • 587: ↓ function __updateeventfromfeed($HttpSocket, $feed, $uuid, $eventId, $u
```

requires:

```
592: if(isset($feed['Feed']['input_source']) && $feed['Feed']['input_source'])
593: if(file_exists($path))
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
704: unlink unlink($feed['Feed']['url'] . $file);
• 700: ↓ function __cleanupfile($feed, $file)
• 700: ↓ function __cleanupfile($feed, $file)
```

requires:

```
701: if(isset($feed['Feed']['input_source']) && $feed['Feed']
['input_source'] == 'local')
702: if(isset($feed['Feed']['delete_local_file']) && $feed['Feed']
['delete_local_file'])
703: if(file_exists($feed['Feed']['url'] . $file))
```

File Disclosure

Userinput reaches sensitive sink when function `__cachemispfeed()` is called.

```
919: file_get_contents $data = file_get_contents($path);
916: $path = $feed['Feed']['url'] . '/' . $uuid . '.json';
• 898: ↓ function __cachemispfeed($feed, $redis, $HttpSocket, $jobId = false)
914: foreach($manifest as $uuid=>$event)
• 907: $manifest = $this->getmanifest($feed, $HttpSocket);
• 898: ↓ function __cachemispfeed($feed, $redis, $HttpSocket, $jobId
• 898: ↓ function __cachemispfeed($feed, $redis, $HttpSocket, $jobId
```

requires:

```
917: if(isset($feed['Feed']['input_source']) && $feed['Feed']
['input_source'] == 'local')
918: if(file_exists($path))
898: ↓ function __cachemispfeed($feed, $redis, $HttpSocket, $jobId = false)
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
956: exec $pipe->exec()
```

requires:

```
935: if($data)
937: if(!empty($event['Event']['Attribute']))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the

left side.

```
1045: file_get_contents $json = file_get_contents(APP . 'files/feed-metadata/defaults.json');
```

hide all

File: /var/www/MISP/MISP/app/Model/User.php

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
307: require_once require_once 'Crypt/GPG.php';
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
346: mkdir mkdir($dir, 0750, true))
344: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
339: if(openssl_x509_read($check['certif_public']))
345: if(!file_exists($dir))
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
353: unlink unlink($msg_test);
349: $msg_test = $fileAccessTool->writetofile ($tempFile, 'test');
348: $tempFile = $fileAccessTool->createtempfile($dir, 'SMIME');
344: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
339: if(openssl_x509_read($check['certif_public']))
352: if(openssl_pkcs7_encrypt($msg_test, $msg_test_encrypted, $check['certif_
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
354: unlink unlink($msg_test_encrypted);
350: $msg_test_encrypted = $fileAccessTool->createtempfile($dir, 'SMIME');
344: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
339: if(openssl_x509_read($check['certif_public']))
352: if(openssl_pkcs7_encrypt($msg_test, $msg_test_encrypted, $check['certif_
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
371: unlink unlink($msg_test);
349: $msg_test = $fileAccessTool->writetofile ($tempFile, 'test');
348: $tempFile = $fileAccessTool->createtempfile($dir, 'SMIME');
344: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
339: if(openssl_x509_read($check['certif_public']))
370: if(openssl_pkcs7_encrypt($msg_test, $msg_test_encrypted, $check['certif_
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
372: unlink unlink($msg_test_encrypted);
350: $msg_test_encrypted = $fileAccessTool->createtempfile($dir, 'SMIME');
344: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
339: if(openssl_x509_read($check['certif_public']))
370: if(openssl_pkcs7_encrypt($msg_test, $msg_test_encrypted, $check['certif_
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
376: unlink unlink($msg_test);
349: $msg_test = $fileAccessTool->writetofile ($tempFile, 'test');
348: $tempFile = $fileAccessTool->createtempfile($dir, 'SMIME');
344: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
339: if(openssl_x509_read($check['certif_public']))
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
377: unlink unlink($msg_test_encrypted);
350: $msg_test_encrypted = $fileAccessTool->createtempfile($dir, 'SMIME');
344: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
339: if(openssl_x509_read($check['certif_public']))
```

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
474: require_once require_once 'Crypt/GPG.php';

requires:
473: if(!$gpg)
```

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
512: require_once require_once 'Crypt/GPG.php';
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
546: mkdir mkdir($dir, 0750, true))
544: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
538: function verifycertificate()
545: if(!file_exists($dir))
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
577: unlink unlink($msg_test);
549: $msg_test = $fileAccessTool->writetofile ($tempFile, 'test');
548: $tempFile = $fileAccessTool->createtempfile($dir, 'SMIME');
544: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
538: function verifycertificate()
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
578: unlink unlink($msg_test_encrypted);
550: $msg_test_encrypted = $fileAccessTool->createtempfile($dir, 'SMIME');
544: $dir = APP . 'tmp' . DS . 'SMIME';
```

requires:

```
538: function verifycertificate()
```

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
724: require_once require_once 'Crypt/GPG.php';
```

requires:

```
722: if($scanEncryptGPG)
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
776: mkdir mkdir($dir, 0750, true))
774: $dir = APP . 'tmp' . DS . 'SMIME';
```

requires:

```
768: if(!$failed && !$scanEncryptGPG && $scanEncryptSMIME)
775: if(!file_exists($dir))
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
789: unlink unlink($msg);
780: $msg = $fileAccessTool->writetofile ($tempFile, $prependedBody);
779: $tempFile = $fileAccessTool->createtempfile($dir, 'SMIME');
774: $dir = APP . 'tmp' . DS . 'SMIME';
770: $prependedBody = 'Content-Transfer-Encoding: 7bit' . PHP_EOL . 'Content-
755: $body = $gpg->encrypt($body, true); // if(!$failed && $scanEncrypt
728: $body = $gpg->sign($body, Crypt_GPG::SIGN_MODE_CLEAR); // if
720: $body = str_replace('\n', PHP_EOL, $body);
718: $body = $bodyNoEnc; // if(Configuration::read('GnuPG.
• 692: function sendemail($user, $body, $bodyNoEnc)
```

requires:

```
768: if(!$failed && !$scanEncryptGPG && $scanEncryptSMIME)
785: if($canSign)
787: if(openssl_pkcs7_sign($msg, $signed, 'file:/// . Configuration::read('SMIME.
```


File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left sid

```

790: unlink unlink($signed);
786: $signed = $fileAccessTool->createtempfile($dir, 'SMIME');
774: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
768: if(!$failed && !$scanEncryptGPG && $scanEncryptSMIME)
785: if($scanSign)
787: if(openssl_pkcs7_sign($msg, $signed, 'file://' . Configure::read('SMIME.

```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left sid

```

792: unlink unlink($msg);
780: $msg = $fileAccessTool->writetofile ($tempFile, $preppedBody);
779: $tempFile = $fileAccessTool->createtempfile($dir, 'SMIME');
774: $dir = APP . 'tmp' . DS . 'SMIME';
770: $preppedBody = 'Content-Transfer-Encoding: 7bit' . PHP_EOL . 'Content-
755: $body = $gpg->encrypt($body, true); // if(!$failed && $scanEncrypt
728: $body = $gpg->sign($body, Crypt_GPG::SIGN_MODE_CLEAR); // if
720: $body = str_replace('\n', PHP_EOL, $body);
718: $body = $bodyNoEnc; // if(Configure::read('GnuPG.
    • 692: ↓ function sendemail($user, $body, $bodyNoEn

requires:
768: if(!$failed && !$scanEncryptGPG && $scanEncryptSMIME)
785: if($scanSign)
791: if(openssl_pkcs7_sign($msg, $signed, 'file://' . Configure::read('SMIME.

```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left sid

```

793: unlink unlink($signed);
786: $signed = $fileAccessTool->createtempfile($dir, 'SMIME');
774: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
768: if(!$failed && !$scanEncryptGPG && $scanEncryptSMIME)
785: if($scanSign)
791: if(openssl_pkcs7_sign($msg, $signed, 'file://' . Configure::read('SMIME.

```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left sid

```

806: unlink unlink($msg_signed);
800: $msg_signed = $msg; // if($scanSign) else ,
780: $msg = $fileAccessTool->writetofile ($tempFile, $preppedBody);
779: $tempFile = $fileAccessTool->createtempfile($dir, 'SMIME');
774: $dir = APP . 'tmp' . DS . 'SMIME';
770: $preppedBody = 'Content-Transfer-Encoding: 7bit' . PHP_EOL . 'Cor

```

```

Type: text/plain;' . PHP_EOL . ' charset=us-ascii' . PHP_EOL . PHP_EOL
755: $body = $gpg->encrypt($body, true); // if(!$failed && $scanEn
728: $body = $gpg->sign($body, Crypt_GPG::SIGN_MODE_CLEAR);
720: $body = str_replace('\n', PHP_EOL, $body);
718: $body = $bodyNoEnc; // if(Configuration::read('
&& !$scanEncryptGPG && $bodyNoEnc),
    • 692: ↓ function sendemail($user, $body, $bod

requires:
768: if(!$failed && !$scanEncryptGPG && $scanEncryptSMIME)
804: if(openssl_pkcs7_encrypt($msg_signed, $msg_signed_encrypted, $user['User
['certif_public'], $headers_smime, 0, OPENSSL_CIPHER_AES_256_CBC))

```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```

807: unlink unlink($msg_signed_encrypted);
802: $msg_signed_encrypted = $fileAccessTool->createtempfile($dir, 'SMIME');
774: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
768: if(!$failed && !$scanEncryptGPG && $scanEncryptSMIME)
804: if(openssl_pkcs7_encrypt($msg_signed, $msg_signed_encrypted, $user['User
['certif_public'], $headers_smime, 0, OPENSSL_CIPHER_AES_256_CBC))

```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

814: unlink unlink($msg_signed);
800: $msg_signed = $msg; // if($scanSign) else ,
780: $msg = $fileAccessTool->writetofile ($tempFile, $prependedBody);
779: $tempFile = $fileAccessTool->createtempfile($dir, 'SMIME');
774: $dir = APP . 'tmp' . DS . 'SMIME';
770: $prependedBody = 'Content-Transfer-Encoding: 7bit' . PHP_EOL . 'Cor
Type: text/plain;' . PHP_EOL . ' charset=us-ascii' . PHP_EOL . PHP_EOL
755: $body = $gpg->encrypt($body, true); // if(!$failed && $scanEn
728: $body = $gpg->sign($body, Crypt_GPG::SIGN_MODE_CLEAR);
720: $body = str_replace('\n', PHP_EOL, $body);
718: $body = $bodyNoEnc; // if(Configuration::read('
&& !$scanEncryptGPG && $bodyNoEnc),
    • 692: ↓ function sendemail($user, $body, $bod

requires:
768: if(!$failed && !$scanEncryptGPG && $scanEncryptSMIME)
813: if(openssl_pkcs7_encrypt($msg_signed, $msg_signed_encrypted, $user['User
['certif_public'], $headers_smime, 0, OPENSSL_CIPHER_AES_256_CBC)) else

```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```

815: unlink unlink($msg_signed_encrypted);

```

```

802: $msg_signed_encrypted = $fileAccessTool->createtempfile($dir, 'SMIME');
774: $dir = APP . 'tmp' . DS . 'SMIME';

requires:
768: if(!$failed && !$canEncryptGPG && $canEncryptSMIME)
813: if(openssl_pkcs7_encrypt($msg_signed, $msg_signed_encrypted, $user['User
['certif_public'], $headers_smime, 0, OPENSSL_CIPHER_AES_256_CBC)) else

```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

915: preg_replace $temp['address'] = preg_replace('/\s{2,}/', PHP_EOL, trim($temp['address']

```

```

requires:
904: ↓ function __extractpgpinfo($lines)

```

hide all

File: /var/www/MISP/MISP/app/Model/Warninglist.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

44: glob $directories = glob(APP . 'files' . DS . 'warninglists' . DS . 'lists' . DS . '

```

File Disclosure

Userinput reaches sensitive sink when function *update()* is called.

```

47: file $file = new file($dir . DS . 'list.json');
46: foreach($directories as $dir)
    • 44: $directories = glob(APP . 'files' . DS . 'warninglists' . DS . 'lists' .

```

```

requires:
46: ↓ function update()
43: ↓ function update()

```

Code Execution

Userinput is used as dynamic function name. Arbitrary functions may be called.

```

321: $function $function($value, $lv)
    • 318: ↓ function __evalcidr($value, $listValues, $function)

```

```

requires:
320: ↓ function __evalcidr($value, $listValues, $function)

```

[hide all](#)**File: /var/www/MISP/MISP/app/Model/AppModel.php****File Disclosure**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
963: glob $files = array_merge($files, glob(CACHE . 'models' . DS . 'myapp*'));
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
964: glob $files = array_merge($files, glob(CACHE . 'persistent' . DS . 'myapp*'));
```

File Manipulation

Userinput reaches sensitive sink when function `cleancachefiles()` is called. (Blind exploitation)

```
967: unlink unlink($f);
965: foreach($files as $f)
    • 964: $files = array_merge($files, glob(CACHE . 'persistent' . DS . 'myapp*'))
    • 963: $files = array_merge($files, glob(CACHE . 'models' . DS . 'myapp*'))
      962: $files = array();
```

requires:

```
965: function cleancachefiles()
966: if(is_file($f))
959: function cleancachefiles()
```

Call triggers vulnerability in function `cleancachefiles()`

```
1057: $this->cleancachefiles ()
```

requires:

```
1056: if(empty($cleanDB) || $cleanDB['AdminSetting']['value'] == 1)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
974: file $file = new file(ROOT . DS . 'VERSION.json', true);
```

[hide all](#)

File: /var/www/MISP/MISP/app/Model/Behavior/RegexpBehavior.php**Code Execution**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
32: preg_replace $value = preg_replace($regexp['Regexp']
['regexp'], $regexp['Regexp']['replacement'], $value);
30: foreach($this->__allRegexp as $regexp)
30: foreach($this->__allRegexp as $regexp)

requires:
31: if(!empty($regexp['Regexp']
['replacement']) && !empty($regexp['Regexp']
['regexp']) && ($regexp['Regexp']['type'] === 'ALL' || $regexp['Regexp']
['type'] === $type))
```

[hide all](#)**File: /var/www/MISP/MISP/app/Model/Server.php****Cross-Site Scripting**

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
1690: print_r $fails[$eventId] = 'Failed (partially?) because of validation errors: ' .
```

```
requires:
1623: if(!empty($eventIds))
1625: if(null != $eventIds)
1633: if(null != $event)
1684: if(!$existingEvent)
1689: if($result) else
```

File Disclosure

Userinput reaches sensitive sink when function *disablecacheafterhook()* is called.

```
2518: file $file = new file($dir->pwd() . DS . $file);
• 2518: $file = new file($dir->pwd() . DS . $file);
2517: foreach($files as $file)
2516: $files = $dir->find('.*' . $settings['extension']);
2510: foreach($this->Event->export_types as $type=>$settings)

requires:
2505: if($value)
2504: function disablecacheafterhook($setting, $value)
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side
(Blind exploitation)

```

2612: file_put_contents file_put_contents(APP . 'Config' . DS . 'config.php', $settingsS
2611: $settingsString = '<?php' . "\n" . '$config = ' . $settingsString . '';
2610: $settingsString = var_export($settingsArray, true);
2608: $settingsArray[$setting] = Configure::read($setting);
2607: foreach($settingsToSave as $setting)
2605: $settingsToSave[14] = 'ApacheSecureAuth' // array()
2605: $settingsToSave[13] = 'ApacheShibbAuth' // array()
2605: $settingsToSave[12] = 'CertAuth' // array()
2605: $settingsToSave[11] = 'Plugin' // array()
2605: $settingsToSave[10] = 'site_admin_debug' // array()
2605: $settingsToSave[9] = 'Session.autoRegenerate' // array
2605: $settingsToSave[8] = 'Session.timeout' // array()
2605: $settingsToSave[7] = 'Session.defaults' // array()
2605: $settingsToSave[6] = 'Security' // array()
2605: $settingsToSave[5] = 'SecureAuth' // array()
2605: $settingsToSave[4] = 'Proxy' // array()
2605: $settingsToSave[3] = 'SMIME' // array()
2605: $settingsToSave[2] = 'GnuPG' // array()
2605: $settingsToSave[1] = 'MISP' // array()
2605: $settingsToSave = 'debug' // array()

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

2681: file $f = new file($item['path'] . DS . $file);
2677: foreach($validItems as $k=>$item)
2674: $validItems = $this->getfilerules();
2680: foreach($files as $file)
2679: $files = $dir->find($item['regex'], true);
2677: foreach($validItems as $k=>$item)
2674: $validItems = $this->getfilerules();

```

requires:

```
2677: ▯ function grabfiles()
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

2746: file_get_contents $testFile = file_get_contents(APP . 'files/scripts
/test_payload.txt');

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

2803: file $file = new file(ROOT . DS . 'VERSION.json', true);

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2970: file $file = new file($path . DS . 'test.txt', true);
2967: foreach($writeableDirs as $path=>$error)
2950: $writeableDirs[15] = // array()
2950: $writeableDirs[APP.'tmp'.DS.'bro'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'logs'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'files'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'xml'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'text'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'suricata'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'snort'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'sha1'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'md5'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'csv_sig'] = 0 // array()
2950: $writeableDirs[APP.'tmp'.DS.'csv_all'] = 0 // array()
2950: $writeableDirs[APP.'files'.DS.'scripts'.DS.'tmp'] = 0 // array()
2950: $writeableDirs[APP.'files'] = 0 // array()
2950: $writeableDirs[APP.'tmp'] = 0 // array()
2950: $writeableDirs['/tmp'] = 0 // array()
```

requires:

```
2967: function writeabledirsdiagnostics(&$diagnostic_errors)
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3013: shell_exec $scriptResult = shell_exec('python ' . APP . 'files' . DS . 'scripts' .
```

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3041: require_once require_once 'Crypt/GPG.php';
```

requires:

```
3038: if(Configure::read('GnuPG.email') && Configure::read('GnuPG.homedir'))
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3156: shell_exec $currentUser = trim(shell_exec('whoami'));
```

requires:

```
3155: if(function_exists('posix_getpwnuid')) else
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3213: shell_exec shell_exec('ps -p ' . $pid))
    • 3206: ↯ function killworker($pid, $user)

    requires:
      3211: if(isset($workers[$pid]))
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
3214: shell_exec shell_exec('kill ' . $pid . ' > /dev/null 2>&1 &');
    • 3206: ↯ function killworker($pid, $user)

    requires:
      3211: if(isset($workers[$pid]))
      3213: if(substr_count(trim(shell_exec('ps -p ' . $pid)), PHP_EOL) > 0 true : f
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3251: shell_exec $currentUser = trim(shell_exec('whoami'));

    requires:
      3251: if(function_exists('posix_getpuid')) else
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
3254: shell_exec $pidTest = substr_count(trim(shell_exec('ps -p ' . $pid)), PHP_EOL) > 0
3252: foreach($workers as $pid=>$worker)
3246: $workers = $this->ResqueStatus->getworkers();
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3574: exec $results['cli'] = exec('php ' . APP . '/files/scripts/selftest.php');

    requires:
      3573: if(!is_readable(APP . '/files/scripts/selftest.php')) else
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3589: exec exec('git ls-remote https://github.com  
/MISP/MISP | head -1 | sed "s/HEAD//"');
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3594: exec $status['commit'] = exec('git rev-parse HEAD');
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3601: exec exec("git symbolic-ref HEAD | sed 's!refs\*/heads\*/!!'");
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3606: exec exec('git checkout ' . $mainBranch);  
3605: $mainBranch = '2.4';
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3614: exec exec($command1, $output);  
3611: $command1 = 'git pull origin ' . $status['branch'] . ' 2>&1';  
• 3609: ↴ function update($status)
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
3618: exec exec($command2, $output);  
3612: $command2 = 'git submodule init && git submodule update 2>&1';
```

hide all

File: /var/www/MISP/MISP/app/Model/ObjectTemplate.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
49: glob $directories = glob($objectsDir . '/*', GLOB_ONLYDIR);
48: $objectsDir = APP . 'files/misp-objects/objects';
```

File Disclosure

Userinput reaches sensitive sink when function *update()* is called.

```
59: file $file = new file($objectsDir . DS . $dir . DS . 'definition.json');
48: $objectsDir = APP . 'files/misp-objects/objects';
55: foreach($directories as $dir)
    52: $directories[$k] = $dir; // functionupdate($user),
    51: $dir = str_replace($objectsDir, '', $dir); //
        functionupdate($user),
    48: $objectsDir = APP . 'files/misp-objects/objects';
    50: foreach($directories as $k=>$dir)
        • 49: $directories = glob($objectsDir . '/*', GLOB_ONLYDIR);
          48: $objectsDir = APP . 'files/misp-objects
            /objects';
```

requires:

```
47: ↓ function update($user)
```

Call triggers vulnerability in function *update()*

```
189: ↑ $this->update ($user)
    • 183: ↓ function populateifempty($user)
```

requires:

```
188: if(empty($result))
```

hide all

File: /var/www/MISP/MISP/app/Model/Galaxy.php**File Disclosure**

Userinput reaches sensitive sink when function *__load_galaxies()* is called.

```
34: file $file = new file($dir->pwd() . DS . $file);
    • 34: $file = new file($dir->pwd() . DS . $file);
    33: foreach($files as $file)
    31: $files = $dir->find('.*\.json');
```

requires:

```
33: ↓ function __load_galaxies()
29: ↓ function __load_galaxies()
```

Call triggers vulnerability in function *__load_galaxies()*

```
68: ↑ $galaxies = $this->__load_galaxies ();
```

File Disclosure

Userinput reaches sensitive sink when function *update()* is called.

```
73: file $file = new file($dir->pwd() . DS . $file);
• 73: $file = new file($dir->pwd() . DS . $file);
72: foreach($files as $file)
70: $files = $dir->find('.*\.json');
```

requires:

```
72: ↓ function update()
67: ↓ function update()
```

[hide all](#)
File: /var/www/MISP/MISP/app/Model/Regexp.php**Code Execution**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
43: preg_replace preg_replace($this->data['Regexp']
['regexp'], 'success', $this->data['Regexp']['regexp']) !=
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
81: preg_replace $string = preg_replace($regexp['Regexp']
['regexp'], $regexp['Regexp']['replacement'], $string);
79: foreach($allRegexp as $regexp)
• 77: ↓ function replacespecific($string, $allRegexp = null, $type)
79: foreach($allRegexp as $regexp)
• 77: ↓ function replacespecific($string, $allRegexp = null, $type)
```

requires:

```
79: ↓ function replacespecific($string, $allRegexp = null, $type)
80: if(strlen($regexp['Regexp']
['replacement']) && strlen($regexp['Regexp']
['regexp']) && ($regexp['Regexp']['type'] === 'ALL' || $regexp['Regexp']
['type'] === $type))
```

[hide all](#)
File: /var/www/MISP/MISP/app/Model/Organisation.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

209: file $logFile = new file($dirPath . DS . 'merge_' . $currentOrg['Organisation'])['i
207: $dirPath = APP . 'tmp' . DS . 'logs' . DS . 'merges';
194: $currentOrg = $this->find('first', array('recursive'=> - 1, 'conditions'=>arra
    • 193: ↓ function orgmerge($id, $request, $user)
196: $targetOrg = $this->find('first', array('fields'=>array('id', 'name', 'uuid',
    195: $targetOrgId = $request['Organisation']['orgsLocal'] : $request['Organis
        • 193: ↓ function orgmerge($id, $request, $user)
        • 193: ↓ function orgmerge($id, $request, $user)

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

211: file $backupFile = new file($dirPath . DS . 'merge_' . $currentOrg['Organisation']
207: $dirPath = APP . 'tmp' . DS . 'logs' . DS . 'merges';
194: $currentOrg = $this->find('first', array('recursive'=> - 1, 'conditions'=>arra
    • 193: ↓ function orgmerge($id, $request, $user)
196: $targetOrg = $this->find('first', array('fields'=>array('id', 'name', 'uuid',
    195: $targetOrgId = $request['Organisation']['orgsLocal'] : $request['Organis
        • 193: ↓ function orgmerge($id, $request, $user)
        • 193: ↓ function orgmerge($id, $request, $user)

```

hide all

File: /var/www/MISP/MISP/app/Model/Attribute.php**File Disclosure**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

598: file $file = new file($filepath);
597: $filepath = $attachments_dir . DS . $this->data['Attribute']
    ['event_id'] . DS . $this->data['Attribute']['id'];
595: $attachments_dir = $my_server->getdefaultattachments_dir(); //
    if(empty($attachments_dir)),
592: $attachments_dir = Configure::read('MISP.attachments_dir');

requires:
590: if($this->typeisattachment($this->data['Attribute']['type']))

```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

1164: preg_replace $value = preg_replace('/[^0-9]+/', '', $value);

requires:
1115: switch($type)

```

```
1163: case 'bin' :
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1169: preg_replace $value = preg_replace('/[^0-9A-Z]+/', '', $value);
```

requires:

```
1115: switch($type)
1167: case 'bic' :
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1175: preg_replace $value = preg_replace('/\.(0)/', '', $value);
```

requires:

```
1115: switch($type)
1173: case 'phone-number' :
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1176: preg_replace $value = preg_replace('/[^\+0-9]+/', '', $value);
```

requires:

```
1115: switch($type)
1173: case 'phone-number' :
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1179: preg_replace $value = preg_replace('/^http/i', 'http', $value);
```

requires:

```
1115: switch($type)
1178: case 'url' :
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1180: preg_replace $value = preg_replace('/\[\.\.]/', '.', $value);
```

requires:

```
1115: switch($type)
1178: case 'url' :
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
1317: file $file = new file($filepath);
1316: $filepath = $attachments_dir . DS . $attribute['event_id'] . DS . $attribute['id'];
1314: $attachments_dir = $my_server->getdefaultattachments_dir(); //
if(empty($attachments_dir)),
1311: $attachments_dir = Configure::read('MISP.attachments_dir');
• 1310: ↓ function base64encodeattachment($attribute)
• 1310: ↓ function base64encodeattachment($attribute)
```

Userinput is passed through function parameters.

```
2428: ↑ $encodedFile = $this->base64encodeattachment ($attribute['Attribute']);
2411: foreach($results as $key=>$attribute)
2409: $results = array_values($results);
2404: $results = $this->find('all', $params);
2385: $params['conditions']['AND']
[[1,'Event.orgc_id'] = $user['org_id'] // array()
• 2344: ↓ function fetchattributes($user, $options = array())
```

requires:

```
2426: if($options['withAttachments'])
2427: if($this->typeisattachment($attribute['Attribute']['type']))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1334: file $file = new file($destpath, true);
1333: $destpath = $rootDir . DS . $attribute['id'];
1331: $rootDir = $attachments_dir . DS . $attribute['event_id'];
1329: $attachments_dir = $my_server->getdefaultattachments_dir(); //
if(empty($attachments_dir)),
1326: $attachments_dir = Configure::read('MISP.attachments_dir');
• 1325: ↓ function savebase64encodedattachment($attribute)
• 1325: ↓ function savebase64encodedattachment($attribute)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
1348: file $tmpfile = new file($fileP);
• 1344: ↓ function uploadattachment($fileP, $realFileName, $malware, $eventId = null,
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

1385: file $file = new file($destpath);
1384: $destpath = $rootDir . DS . $this->getid();
1381: $rootDir = $attachments_dir . DS . $eventId;
1379: $attachments_dir = $my_server->getdefaultattachments_dir(); // if
1376: $attachments_dir = Configure::read('MISP.attachments_dir');
• 1344: function uploadattachment($fileP, $realFileName, $malware, $sever

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

1386: file $zipfile = new file($destpath . '.zip');
1384: $destpath = $rootDir . DS . $this->getid();
1381: $rootDir = $attachments_dir . DS . $eventId;
1379: $attachments_dir = $my_server->getdefaultattachments_dir(); // if
1376: $attachments_dir = Configure::read('MISP.attachments_dir');
• 1344: function uploadattachment($fileP, $realFileName, $malware, $sever

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

1387: file $fileInZip = new file($rootDir . DS . $extraPath . $filename);
1381: $rootDir = $attachments_dir . DS . $eventId;
1379: $attachments_dir = $my_server->getdefaultattachments_dir(); // if(empt
1376: $attachments_dir = Configure::read('MISP.attachments_dir');
• 1344: function uploadattachment($fileP, $realFileName, $malware, $eventId =
• 1344: function uploadattachment($fileP, $realFileName, $malware, $eventId = null,
1347: $filename = basename($fileP);
• 1344: function uploadattachment($fileP, $realFileName, $malware, $eventId =

```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

- 1393: **exec** exec('zip -j -P infected ' . escapeshellarg(\$zipfile->path) . ' ' . escapeshe

requires:

```
1390: if($malware)
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
1398: rename rename($zipfile->path, $file->path);
```

requires:

```
1390: if($malware)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1400: file $fileAttach = new file($fileP);
    • 1344: function uploadattachment($fileP, $realFileName, $malware, $eventId = null,

requires:
    1399: if($malware) else
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
1401: rename rename($fileAttach->path, $file->path);

requires:
    1399: if($malware) else
```

HTTP Response Splitting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1939: header $export->header)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2170: file $tmp_file = new file(APP . 'tmp/files/' . $file['tmp_name']);
2163: foreach($files as $file)
    • 2152: function __resolveelementfile($element, $files)

requires:
    2168: if($element['malware'])
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2186: file $tmp_file = new file(APP . 'tmp/files/' . $file['tmp_name']);
2163: foreach($files as $file)
    • 2152: function __resolveelementfile($element, $files)

requires:
    2184: if($element['malware']) else
```


File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
2452: file $tmpFile = new file($dir->path . DS . $this->generaterandomfilename(), true,
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
2458: file $contentsFile = new file($dir->path . DS . $hashes['md5']);
2456: $hashes[$hash] = $this->__hashrouter($hash, $tmpFile->path);
2455: foreach($hash_types as $hash)
    • 2440: ↓ function handlemaliciousbase64($event_id, $original_filename, $!
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
2459: rename rename($tmpFile->path, $contentsFile->path);
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
2460: file $fileNameFile = new file($dir->path . DS . $hashes['md5'] . '.filename.txt')
2456: $hashes[$hash] = $this->__hashrouter($hash, $tmpFile->path);
2455: foreach($hash_types as $hash)
    • 2440: ↓ function handlemaliciousbase64($event_id, $original_filename, $!
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
2463: file $zipFile = new file($dir->path . DS . $hashes['md5'] . '.zip');
2456: $hashes[$hash] = $this->__hashrouter($hash, $tmpFile->path);
2455: foreach($hash_types as $hash)
    • 2440: ↓ function handlemaliciousbase64($event_id, $original_filename, $!
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
• 2464: exec exec('zip -j -P infected ' . escapeshellarg($zipFile->path) . ' ' . escapeshe
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the

left side.

```
2712: exec $pipeline->exec()
```

requires:

```
2705: if($redis)
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2831: shell\_exec $result = shell_exec('python ' . APP . 'files/scripts
/generate_file_objects.py -p ' . $tmpfile->path);
```

hide all

File: /var/www/MISP/MISP/app/Model/Taxonomy.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
38: glob $directories = glob(APP . 'files' . DS . 'taxonomies' . DS . '*', GLOB_ONLYDIR)
```

File Disclosure

Userinput reaches sensitive sink when function *update()* is called.

```
49: file $file = new file(APP . 'files' . DS . 'taxonomies' . DS . $dir . DS . 'machine
45: foreach($directories as $dir)
42: $directories[$k] = $dir; // functionupdate(),
40: $dir = str_replace(APP . 'files' . DS . 'taxonomies' . DS, '', $dir);
39: foreach($directories as $k=>$dir)
    • 38: $directories = glob(APP . 'files' . DS . 'taxonomies' . I
```

requires:

```
37: function update()
```

hide all

File: /var/www/MISP/MISP/app/Model/Sighting.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
267: file $tempFile = new file(APP . "files" . DS . "scripts" . DS . "tmp" . DS . $rand
266: $randomFileName = $this->generaterandomfilename();
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
274: shell_exec $result = shell_exec('python ' . $scriptFile . ' ' . $randomFileName);
272: $scriptFile = APP . "files" . DS . "scripts" . DS . "stixsighting2misp.py";
266: $randomFileName = $this->generaterandomfilename();
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
280: file $file = new file(APP . "files" . DS . "scripts" . DS . "tmp" . DS . $randomFi
266: $randomFileName = $this->generaterandomfilename());
```

requires:

```
279: if($result['success'] == 1)
```

hide all

File: /var/www/MISP/MISP/app/Model/ShadowAttribute.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
238: file $file = new file($filepath);
237: $filepath = $attachments_dir . DS . 'shadow' . DS . $sa['ShadowAttribute']['ev
[id'];
235: $attachments_dir = $my_server->getdefaultattachments_dir(); // if(empty
232: $attachments_dir = Configure::read('MISP.attachments_dir');
229: $sa = $this->find('first', array('conditions'=>array('ShadowAttribute.id
[id']), 'recursive'=> - 1, 'fields'=>array('ShadowAttribute.id', 'ShadowAttr
229: $sa = $this->find('first', array('conditions'=>array('ShadowAttribute.id
[id']), 'recursive'=> - 1, 'fields'=>array('ShadowAttribute.id', 'ShadowAttr
```

requires:

```
228: if(isset($this->data['ShadowAttribute']['deleted']) && $this->data['Shad
230: if($this->typeisattachment($sa['ShadowAttribute']['type']))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
270: file $file = new file($filepath);
269: $filepath = $attachments_dir . DS . 'shadow' . DS . $this->data['ShadowAttribu
```

```

    ['event_id'] . DS . $this->data['ShadowAttribute']['id'];
    267: $attachments_dir = $my_server->getdefaultattachments_dir(); //
    if(empty($attachments_dir)),
    264: $attachments_dir = Configure::read('MISP.attachments_dir');

requires:
    262: if($this->typeisattachment($this->data['ShadowAttribute']['type']))

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

368: file $file = new file($filepath);
367: $filepath = $attachments_dir . DS . 'shadow' . DS . $attribute['event_id'] . I
365: $attachments_dir = $my_server->getdefaultattachments_dir(); // if(empty
362: $attachments_dir = Configure::read('MISP.attachments_dir');
• 361: ↓ function base64encodeattachment($attribute)
• 361: ↓ function base64encodeattachment($attribute)

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

385: file $file = new file($destpath, true);
384: $destpath = $rootDir . DS . $attribute['id'];
382: $rootDir = $attachments_dir . DS . 'shadow' . DS . $attribute['event_id'
380: $attachments_dir = $my_server->getdefaultattachments_dir(); //
    if(empty($attachments_dir)),
377: $attachments_dir = Configure::read('MISP.attachments_dir');
• 376: ↓ function savebase64encodedattachment($attribute)
• 376: ↓ function savebase64encodedattachment($attribute)

```

hide all

File: /var/www/MISP/MISP/app/index.php

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

17: require require 'webroot' . DIRECTORY_SEPARATOR . 'index.php'; // index.php

```

hide all

File: /var/www/MISP/MISP/app/files/scripts/selftest.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
8: echo echo json_encode($results);
6: $results['extensions'][$extension] = extension_loaded($extension);
5: foreach($extensions as $extension)
2: $extensions = 'redis' // array()
```

[hide all](#)

File: /var/www/MISP/MISP/app/Controller/ShadowAttributesController.php

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
190: rename rename($pathOld, $pathNew)
188: $pathOld = APP . "files" . DS . $eventId . DS . "shadow" . DS . $shadowId;
    • 187: ↓ function _movefile($shadowId, $newId, $eventId)
    • 187: ↓ function _movefile($shadowId, $newId, $eventId)
189: $pathNew = APP . "files" . DS . $eventId . DS . $newId;
    • 187: ↓ function _movefile($shadowId, $newId, $eventId)
    • 187: ↓ function _movefile($shadowId, $newId, $eventId)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
488: file response->file($path . $file, array('download'=>true, 'name'=>$filename . '.');
473: $path = "files" . DS . "shadow" . DS . $shadowAttribute['event_id'] . DS;
    • 472: ↓ function __downloadattachment($shadowAttribute)
474: $file = $shadowAttribute['id'];
    • 472: ↓ function __downloadattachment($shadowAttribute)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
501: file $tmpfile = new file($this->request->data['ShadowAttribute']['value']
    ['tmp_name']);
```

```
requires:
496: if($this->request->is('post'))
```

[hide all](#)

File: /var/www/MISP/MISP/app/Controller/FeedsController.php

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side (exploitation)

```
223: unlink unlink($feedCache);
221: $feedCache = APP . 'tmp' . DS . 'cache' . DS . 'misp_feed_' . intval($feedId)
    • 170: function edit($feedId)

requires:
187: if($this->request->is('post') || $this->request->is('put'))
220: if($result)
222: if(file_exists($feedCache))
```

hide all

File: /var/www/MISP/MISP/app/Controller/UsersController.php

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1019: uasort uasort($data, function ($a, $b){
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side (exploitation)

```
1061: file response->file($termsFile, array('download'=>true, 'name'=>Configure::read('M
1059: $termsFile = APP . 'files' . DS . 'terms' . DS . Configure::read('MISP.terms_
if(!Configure::read('MISP.terms_file')) else ,
1057: $termsFile = APP . "View/Users/terms"; // if(!Configure::read('MISP.terms_fi
```

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1443: uksort uksort($orgs, 'strcasecmp');
```

hide all

File: /var/www/MISP/MISP/app/Controller/SightingsController.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
27: file\_get\_contents $result = $this->Sighting->handlestixsighting
    (file_get_contents('php://input'));
```

```
requires:
  21: if($this->request->is('post'))
  26: if($id === 'stix')
```

[hide all](#)

File: /var/www/MISP/MISP/app/Controller/EventsController.php

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
343: array_map $orgArray = array_map('strtoupper', $orgArray);
```

```
requires:
  270: if(substr($k, 0, 6) === 'search')
  276: switch($searchTerm)
  339: case 'org' :
```

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
786: array_map $filterValue = array_map('trim', explode(",", $filterColumns));
```

```
requires:
  784: if(!empty($this->params['named']['searchFor']))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1189: file $file = new file($this->data['Event']['submittedgfi']['name']);
```

```
requires:
  1174: if($this->request->is('post'))
  1185: if(!empty($this->data))
  1187: if(isset($this->data['Event']['submittedgfi']))
```

HTTP Response Splitting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
1267: header response->header('Location', Configure::read('MISP.baseurl') . '/events/' .
```

```
requires:
  1174: if($this->request->is('post'))
```

```

1185: if(!empty($this->data))
1195: if(isset($this->data['Event']
['submittedgfi']) && ($ext != 'zip') && $this->data['Event']['submittedgfi']
['size'] > 0 && is_uploaded_file($this->data['Event']['submittedgfi']
['tmp_name'])) else
1264: if($add === true && !is_numeric($add)) else
1265: if($this->isrest ())
1266: if(is_numeric($add))

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

1885: file $file = new file($dir->pwd() . DS . 'misp.text_md5.' . $org_name . $type['ex
1854: $org_name = $this->'ADMIN' : $this->Auth->user('Organisation')['name'];
1868: foreach($this->Event->export_types as $k=>$type)

```

requires:

```

1850: if(Configure::read('MISP.background_jobs') && !Configure::read('MISP.di
1883: if($k === 'text')

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

1887: file $file = new file($dir->pwd() . DS . 'misp.' . $k . '.' . $org_name . $type['
1868: foreach($this->Event->export_types as $k=>$type)
1854: $org_name = $this->'ADMIN' : $this->Auth->user('Organisation')['name'];
1868: foreach($this->Event->export_types as $k=>$type)

```

requires:

```

1850: if(Configure::read('MISP.background_jobs') && !Configure::read('MISP.di
1886: if($k === 'text') else

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side
exploitation)

```

1949: file response->file($path, array('download'=>true))
1948: $path = 'tmp/cached_exports/' . $type . DS . 'misp.' . strtolower($this->Ever
['type']) . $extra . '.' . $org . $this->Event->export_types[$type]['extension'];
    • 1939: ↓ function downloadexport($type, $extra = null)
    • 1939: ↓ function downloadexport($type, $extra = null)
1946: $extra = '_' . $extra;
1944: $org = $this->Auth->user('Organisation')['name'];
    • 1939: ↓ function downloadexport($type, $extra = null)

```

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

2297: array_walk array_walk($requested_obj_attributes, ↓ function (&$value, $key){

```



```
requires:
    2296: if(!empty($requested_obj_attributes))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2331: file $zipFile = new file($rootDir . $this->data['Event']['submittedgfi']
['name']);
2325: $rootDir = $attachments_dir . DS . "GFI" . DS . $id . DS;
2323: $attachments_dir = $this->Server->getdefaultattachments_dir(); //
if(empty($attachments_dir)),
2320: $attachments_dir = Configure::read('MISP.attachments_dir');
• 2312: ↳ function _addgfizip($id)

requires:
2314: if(!empty($this->data) && $this->data['Event']['submittedgfi']
['size'] > 0 && is_uploaded_file($this->data['Event']['submittedgfi']
['tmp_name']))
```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2338: exec exec("unzip " . $zipFile->path . ' -d ' . $rootDir, $execOutput, $execRetVal)
2325: $rootDir = $attachments_dir . DS . "GFI" . DS . $id . DS;
2323: $attachments_dir = $this->Server->getdefaultattachments_dir(); //
if(empty($attachments_dir)),
2320: $attachments_dir = Configure::read('MISP.attachments_dir');
• 2312: ↳ function _addgfizip($id)

requires:
2314: if(!empty($this->data) && $this->data['Event']['submittedgfi']
['size'] > 0 && is_uploaded_file($this->data['Event']['submittedgfi']
['tmp_name']))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2375: file $iocFile = new file($destPath . DS . $this->data['Event']['submittedioc']
['name']);
2373: $destPath = $rootDir . 'ioc';
2370: $rootDir = $attachments_dir . DS . $id . DS;
2368: $attachments_dir = $this->Server->getdefaultattachments_dir(); //
if(empty($attachments_dir)),
2365: $attachments_dir = Configure::read('MISP.attachments_dir');
• 2353: ↳ function _addiocfile($id)

requires:
2355: if(!empty($this->data) && $this->data['Event']['submittedioc']
['size'] > 0 && is_uploaded_file($this->data['Event']['submittedioc']
```

```
['tmp_name'])))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```
2598: file $file = new file($actualFile);
2596: $actualFile = $rootDir . DS . 'Analysis' . DS . 'proc_' . $index . DS . 'modi
2551: $rootDir = $attachments_dir . DS . $id . DS;
2543: $attachments_dir = $this->Server->getdefaultattachments_dir(); //
2540: $attachments_dir = Configure::read('MISP.attachments_dir');
• 2505: function _readgfixml($data, $id)
2590: $index = (string)$val;
2589: foreach($result[0]->attributes() as $key=>$val)
2580: $actualFileName = $file['val'] . $ext;
2574: foreach($files as $file)
2569: $files[['val']] = $arrayItemValue // array() if($arrayItemSi
2565: $arrayItemValue = (string)$val;
2563: foreach($result[0]->attributes() as $key=>$val)
2579: $ext = substr($file['key'], strpos($file['key'], '.'));
2574: foreach($files as $file)
2569: $files[['val']] = $arrayItemValue // array() if($array:
2565: $arrayItemValue = (string)$val;
2563: foreach($result[0]->attributes() as $key=>$
2574: foreach($files as $file)
2569: $files[['val']] = $arrayItemValue // array() if($array:
2565: $arrayItemValue = (string)$val;
2563: foreach($result[0]->attributes() as $key=>$
```

Code Execution

Userinput is used as dynamic function name. Arbitrary functions may be called.

```
2708: $tool $tool();
2707: $tool = strtoupper($type) . 'ConverterTool';
2705: $type = 'xml';
```

Code Execution

Userinput is used as dynamic function name. Arbitrary functions may be called.

```
2846: $converters $converters[$responseType]();
2833: $converters['json'] = 'JSONConverterTool' // array()
```

Possible Flow Control

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2996: ini_set ini_set('max_execution_time', 3600);
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side (Blind exploitation)

```

3399: unlink unlink($tmpdir . '/' . $tempFile[0]);
3393: $tmpdir = Configure::Configure::read('MISP.tmpdir') : '/tmp';
3394: $tempFile = explode('|', $attribute['data']);
3385: foreach($$source as $k=>$attribute)
3384: foreach($attributeSources as $source)
3382: $attributeSources[1] = 'onthe-fly-attributes' // array()
3382: $attributeSources = 'attributes' // array()

requires:
3370: if($this->request->is('post'))
3390: if($attribute['type'] == 'malware-sample')
3391: if(!isset($attribute['data_is_handled']) || !$attribute['data_is_handled'])

```

File Disclosure

Userinput reaches sensitive sink when function `upload_sample()` is called.

```

3949: file $tmpfile = new file($tmpfile);
• 3949: $tmpfile = new file($tmpfile);
3947: $tmpfile = $fileAccessTool->createTempfile($tmpdir, $prefix = 'MISP_upload_sample');
3946: $tmpdir = Configure::Configure::read('MISP.tmpdir') : '/var/www/MISP/tmp';

requires:
3823: function upload_sample($event_id = null, $advanced = false)

```

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

4046: array\_walk\_recursive array_walk_recursive($json, function (&$item, $key){

```

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

4219: call\_user\_func\_array $validation = call\_user\_func\_array(array($this->Module, $this->validation), array($this->request->data['Event']['config'][$configName]));
4212: foreach($module['mispattributes']['userConfig'] as $configName=>$config)
4200: $module['mispattributes']['inputSource'] = 'paste' // array()
4198: $module = $this->Module->getEnabledModule($module, 'Import');
• 4195: function importModule($module, $eventId)

requires:
4201: if($this->request->is('post'))
4213: if(!$fail)
4218: if(isset($config['validation'])) else

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
4246: file $tmpfile = new file($fileupload['tmp_name']);
4245: $fileupload = $this->request->data['Event']['fileupload'];

requires:
4201: if($this->request->is('post'))
4235: if(!$fail)
4236: if(!empty($module['mispattributes']['inputSource']))
4241: if($this->request->data['Event']['source'] == '1')
4244: if(!isset($this->request->data['Event']
['fileupload']) || empty($this->request->data['Event']
['fileupload'])) else
```

hide all

File: /var/www/MISP/MISP/app/Controller/AppController.php

Code Execution

Userinput is used as dynamic function name. Arbitrary functions may be called.

```
381: $debugType $debugType($content))
    • 376: function queryacl($debugType = 'findMissingFunctionNames', $content = false)
```

HTTP Response Splitting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
404: header request->header('Accept')
```

hide all

File: /var/www/MISP/MISP/app/Controller/TemplatesController.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
330: file $file = new file(APP . 'tmp/files/' . $attribute['data']);
328: foreach($attributes as $k=>$attribute)
325: $attributes = json_decode($this->request->data['Template']['attributes']

requires:
294: if($this->request->is('post'))
324: if(isset($this->request->data['Template']['attributes']))
329: if(isset($attribute['data']) && $this->Template->checkfilename($attribut
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
378: move_uploaded_file move_uploaded_file($file['tmp_name'], APP . 'tmp/files/' . $fn);
374: foreach($this->request->data['Template']['file'] as $k=>$file)
377: $fn = $this->Template->generaterandomfilename();
```

requires:

```
368: if($this->request->is('post'))
375: if($file['size'] > 0 && $file['error'] == 0)
376: if($this->Template->checkfilename($file['name']))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
406: file $file = new file(APP . 'tmp/files/' . $filename);
• 401: ↓ function deletetemporaryfile($filename)
```

requires:

```
405: if($this->Template->checkfilename($filename))
```

hide all

File: /var/www/MISP/MISP/app/Controller/OrganisationsController.php**File Manipulation**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
106: move_uploaded_file $result = move_uploaded_file($this->request->data['Organisation'
['logo']['tmp_name'], APP . 'webroot/img/orgs/' . $filename);
103: $filename = basename($this->request->data['Organisation']['name'] . '.png');
```

requires:

```
82: if($this->request->is('post'))
101: if($this->Organisation->save($this->request->data))
102: if(isset($this->request->data['Organisation']['logo']
['size']) && $this->request->data['Organisation']['logo']
['size'] > 0 && $this->request->data['Organisation']['logo']['error'] == 0)
104: if(preg_match("/^[0-9a-z\-\_\.\]*\.(png)$/i", $filename))
105: if(!empty($this->request->data['Organisation']['logo']
['tmp_name']) && is_uploaded_file($this->request->data['Organisation']
['logo']['tmp_name']))
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

164: move_uploaded_file $result = move_uploaded_file($this->request->data['Organisation']
['logo']['tmp_name'], APP . 'webroot/img/orgs/' . $filename);
161: $filename = basename($this->request->data['Organisation']['name'] . '.png');

requires:
138: if($this->request->is('post') || $this->request->is('put'))
159: if($this->Organisation->save($this->request->data))
160: if(isset($this->request->data['Organisation']['logo']
['size']) && $this->request->data['Organisation']['logo']
['size'] > 0 && $this->request->data['Organisation']['logo']['error'] == 0)
162: if(preg_match("/^[0-9a-z\-\_\.\]*\.(png)$/i", $filename))
163: if(!empty($this->request->data['Organisation']['logo']
['tmp_name']) && is_uploaded_file($this->request->data['Organisation']
['logo']['tmp_name']))

```

hide all

File: /var/www/MISP/MISP/app/Controller/ThreadsController.php**Code Execution**

Userinput is used as dynamic function name. Arbitrary functions may be called.

```
29: $array $array(), $this->response->type());
```

requires:

```

23: if($result)
27: if($thread_id) else
28: if($this->isrest ())

```

hide all

File: /var/www/MISP/MISP/app/Controller/ServersController.php**File Disclosure**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

636: file $file = new file($server['Server'][$subm]['name']);
• 618: function __savecert($server, $id, $client = false, $delete = false)

```

requires:

```
628: if(!$delete)
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

648: file $pemfile = new file($destpath . $id . $ins . '.' . $ext);
646: $destpath = APP . "files" . DS . "certs" . DS;

```

```

• 618: ↓ function __savecert($server, $id, $client = false, $delete = false)
626: $ins = ''; // if($client) else ,
622: $ins = '_client'; // if($client),
637: $ext = $file->ext();

```

```

requires:
628: if(!$delete)

```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

774: shell_exec $advanced_attachments = shell_exec('python ' . APP . 'files/scripts
/generate_file_objects.py -c');

```

```

requires:
701: if($this->request->is('Get'))
771: if($tab == 'diagnostics' || $tab == 'download')

```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

913: shell_exec shell_exec($prepend . APP . 'Console' . DS . 'cake CakeResque.CakeResque
912: $prepend = 'export PATH=$PATH: "/opt/rh/rh-php56/root/usr/bin:/opt/rh/rh-php56,
• 907: ↓ function startworker($type)

```

```

requires:
913: if($type != 'scheduler')

```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

914: shell_exec shell_exec($prepend . APP . 'Console' . DS . 'cake CakeResque.CakeResque
912: $prepend = 'export PATH=$PATH: "/opt/rh/rh-php56/root/usr/bin:/opt/rh/rh-php56,

```

```

requires:
914: if($type != 'scheduler') else

```

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

1039: call_user_func_array $beforeResult = call_user_func_array(array($this->Server, $fo
['value']));

```

```

973: $found = $s; // if(isset($s)) else , if($setting == $k),
961: foreach($serverSettings as $k=>$s)
958: $serverSettings = $this->Server->serverSettings ;
966: $found = $es; // if(isset($s)), if($ek != 'branch'), if($setting == $k . '.')
963: foreach($s as $ek=>$es) // if(isset($s)),
961: foreach($serverSettings as $k=>$s)

```

```

958: $serverSettings = $this->Server->serverSettings ;

requires:
1003: if($this->request->is('post'))
1038: if(isset($found['beforeHook']))

```

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

1095: call_user_func_array $afterResult = call_user_func_array(array($this->Server, $found['value']));
973: $found = $s; // if(isset($s)) else , if($setting == $k),
961: foreach($serverSettings as $k=>$s)
958: $serverSettings = $this->Server->serverSettings ;
966: $found = $es; // if(isset($s)), if($ek != 'branch'), if($setting == $k . '.')
963: foreach($s as $ek=>$es) // if(isset($s)),
961: foreach($serverSettings as $k=>$s)
958: $serverSettings = $this->Server->serverSettings ;

requires:
1003: if($this->request->is('post'))
1079: if(!$forceSave && $testResult !== true) else
1094: if(isset($found['afterHook']))

```

Command Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

1134: shell_exec shell_exec($prepend . APP . 'Console' . DS . 'worker' . DS . 'start.sh
1131: $prepend = Configure::read('MISP.rh_shell_fix_path'); //
if(Configure::read('MISP.rh_shell_fix')), if(Configure::read('MISP.rh_shell_fix_pat
1129: $prepend = 'export PATH=$PATH:"/opt/rh/rh-php56/root/usr/bin:/opt/rh/rh-php56
/usr/sbin"; '; // if(Configure::read('MISP.rh_shell_fix')),
1127: $prepend = '';

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

1149: file $existingFile = new file($validItems[$type]
['path'] . DS . $filename);
1147: $validItems = $this->Server->getfilerules();
• 1144: ↓ function deletefile($type, $filename)

requires:
1146: if($this->request->is('post'))

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.


```

1183: file $existingFile = new file($validItems[$type]['path'] . DS . $filename);
1167: $validItems = $this->Server->getfilerules();
1171: $filename = basename($this->request->data['Server']['file']['name']);

```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

1189: move_uploaded_file $result = move_uploaded_file($this->request->data['Server']
['file']['tmp_name'], $validItems[$type]['path'] . DS . $filename);
1167: $validItems = $this->Server->getfilerules();
1171: $filename = basename($this->request->data['Server']['file']['name']);

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

1253: file $file = new file(ROOT . DS . 'VERSION.json', true);

```

requires:

```

1249: if($result['status'] == 1)
1251: if(isset($version['version']) && preg_match('/^[0-9]+\.[0-9]+
\.[0-9]+$/ ', $version['version']))

```

hide all

File: /var/www/MISP/MISP/app/Controller/AttributesController.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side (exploitation)

```

328: file response->file($path . $file, array('download'=>true, 'name'=>$filename . '.');
313: $path = $attachments_dir . DS . $attribute['event_id'] . DS;
311: $attachments_dir = $this->Server->getdefaultattachments_dir(); //
if(empty($attachments_dir)),
308: $attachments_dir = Configure::read('MISP.attachments_dir');
• 307: ↓ function __downloadattachment($attribute)
314: $file = $attribute['id'];
• 307: ↓ function __downloadattachment($attribute)

```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

349: file $tmpfile = new file($value['tmp_name']);
345: foreach($this->request->data['Attribute']['values'] as $k=>$value)

```

```
requires:
  332: if($this->request->is('post'))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
490: file $tmpfile = new file($this->request->data['Attribute']['value']
    ['tmp_name']);
```

```
requires:
  477: if($this->request->is('post'))
```

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
512: fgetcsv $row = fgetcsv($handle, 0, ',', '"') !=
511: $handle = fopen($filename, 'r') !=
508: $filename = $tmpfile->path;
```

```
requires:
  477: if($this->request->is('post'))
  511: if(($handle = fopen($filename, 'r')) != false)
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2204: echo echo '&nbsp;';
```

```
requires:
  2202: if($field == 'timestamp')
  2204: if(isset($result)) else
```

Reflection Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
2321: array_map $newValues = array_map('trim', $newValues);
```

```
requires:
  2300: if($this->request->is('post'))
```

Code Execution

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

2556: preg_replace $attribute['Attribute']
['value'] = preg_replace($regex, $rC['to'], $attribute['Attribute']['value']);
2555: $regex .= 'i';
2554: $regex .= '/';
2553: $regex .= '$';
2552: $regex .= $rC['from'];
2551: $regex .= '^';
2550: $regex = '/';
2543: foreach($replaceConditions as $rC)
2534: $replaceConditions[2] = // array() switch($scrip
case 'urlSanitisation' : ,
2534: $replaceConditions[false,'condition'] = 'contains
array() switch($script), case 'urlSanitisation' : ,
2534: $replaceConditions[true,'condition'] = 'startsWit
array() switch($script), case 'urlSanitisation' : ,
2543: foreach($replaceConditions as $rC)
2534: $replaceConditions[2] = // array() switch($script), case 'urlSanitisa
: ,
2534: $replaceConditions[false,'condition'] = 'contains' // array()
switch($script), case 'urlSanitisation' : ,
2534: $replaceConditions[true,'condition'] = 'startsWith' // array()
switch($script), case 'urlSanitisation' : ,

```

hide all

File: /var/www/MISP/MISP/app/Controller/Component/Auth/ApacheAuthenticate.php

Protocol Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

52: ldap_connect $ldapconn = ldap_connect(Configure::read('ApacheSecureAuth.ldapServer'))

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

53: die $ldapconn = ldap_connect(Configure::read('ApacheSecureAuth.ldapServer')) or die

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

63: die ("LDAP bind failed");

```

requires:

```

58: if($ldapconn)
62: if(!$ldapbind)

```

LDAP Injection

Userinput reaches sensitive sink when function *authenticate()* is called.

```

75: ldap_search $result = ldap_search($ldapconn, $ldapdn, $filter, $getLdapUserInfo) or
70: $filter = '(' . Configure::read('ApacheSecureAuth.ldapSearchAttribut') . '=' .
    else ,
68: $filter = '(&' . $ldapSearchFilter . '(' . Configure::read('ApacheSecureAuth.ldapSearchFilter') .
    if(!empty($ldapSearchFilter)),
    50: $ldapSearchFilter = Configure::read('ApacheSecureAuth.ldapSearchFilter');

requires:
58: if($ldapconn)
40: function authenticate(CakeRequest$request, CakeResponse$response)

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

76: die $result = ldap_search($ldapconn, $ldapdn, $filter, $getLdapUserInfo) or die ('Error
52: $ldapconn = ldap_connect(Configure::read('ApacheSecureAuth.ldapServer')) or die
    stopped

requires:
58: if($ldapconn)

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

85: die die ("User not found in LDAP");

requires:
58: if($ldapconn)
84: if(isset($ldapUserData[0]['mail'][0])) else

```

hide all

File: /var/www/MISP/MISP/app/Controller/Component/ACLComponent.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side

```

491: file_get_contents $fileContents = file_get_contents(APP . 'Controller' . DS . $file
487: foreach($files as $file)
    485: $files = $dir->find('.*\.\php');

requires:
487: function __findallfunctions()

```

[hide all](#)

File: /var/www/MISP/MISP/app/Controller/Component/IOCImportComponent.php**Reflection Injection**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
302: array\_filter array_filter(array_keys($array), 'is_string'))
```

[hide all](#)

File: /var/www/MISP/MISP/INSTALL/ansible/roles/misp/templates/misp/config/core.php**Possible Flow Control**

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
139: define define('LOG_ERROR', LOG_ERR);
```

Vulnerability is also triggered in:
/var/www/MISP/MISP/travis/core.php

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

- 286: [require_once](#) require_once dirname(__DIR__) . '/Vendor/autoload.php';

[hide all](#)