

PHP

Internals



A stylized, multi-colored rainbow arching across the top left corner of the slide. The colors are muted and blend into each other, creating a soft, ethereal effect.

`gynvael.coldwind//vx`



Hispasec



`gynvael.coldwind//vx`



gynvael.coldwind//vx

Rev. Eng.

Pentesty

Hispasec

Code

gynvael.coldwind/vx

Vexillium

Rev. Eng.

Pentesty

Hispasec

Code

[gynvael.coldwind//vx](http://gynvael.coldwind.pl/vx)

Vexillium

<http://gynvael.coldwind.pl>

Rev. Eng.

Pentesty

Hispacec

Code

ReverseCraft

gynvael.coldwind//vx

Vexillium

<http://gynvael.coldwind.pl>



PHP ?Externals?

VS.

PHP Internals

Skrypt(y) PHP



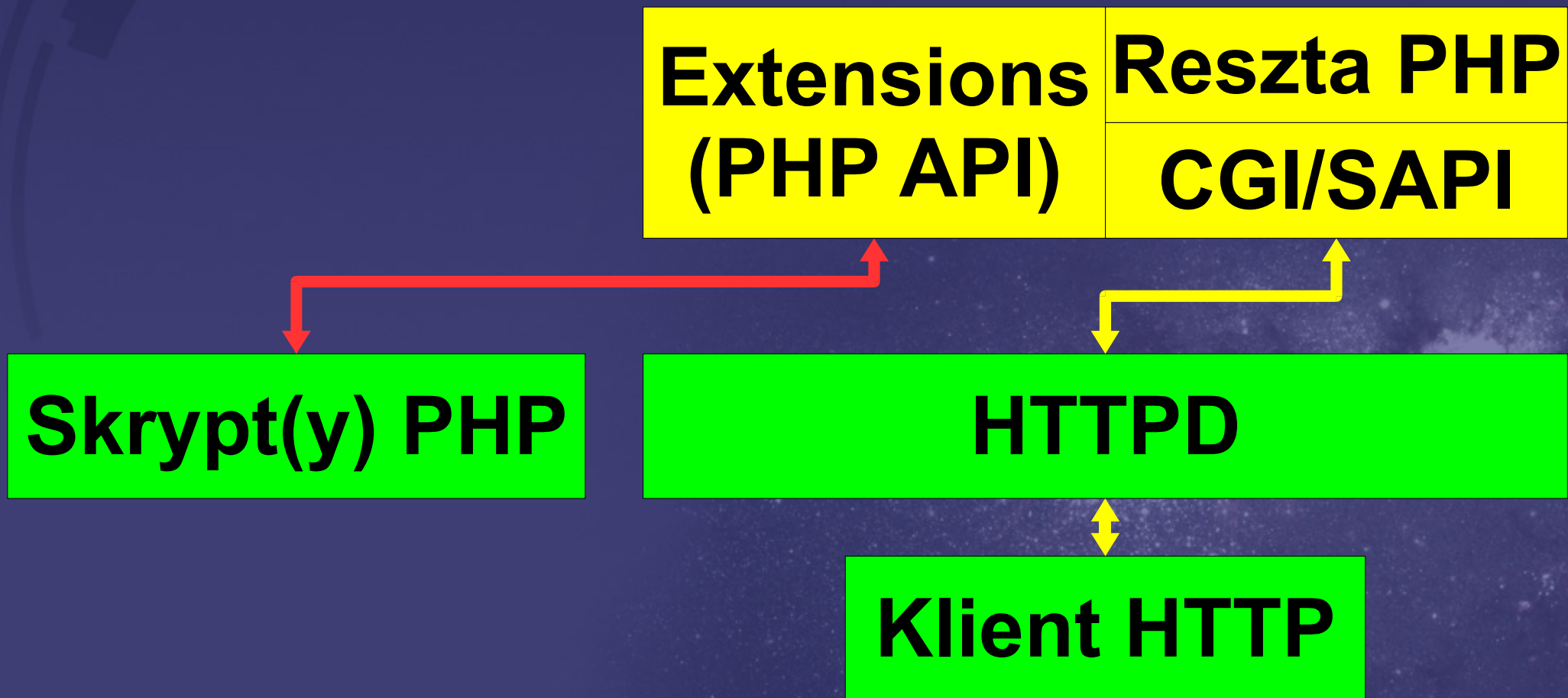
Silnik PHP

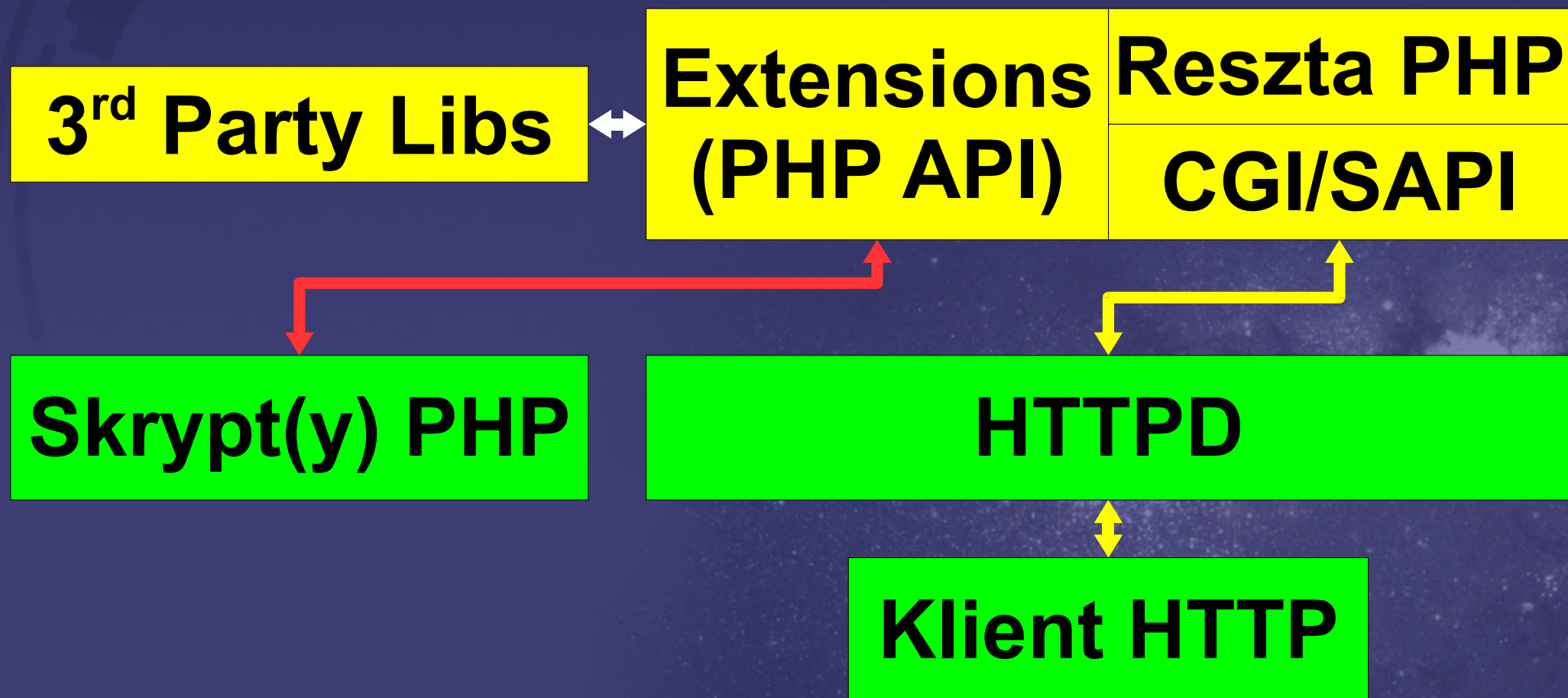
↑ CGI, API

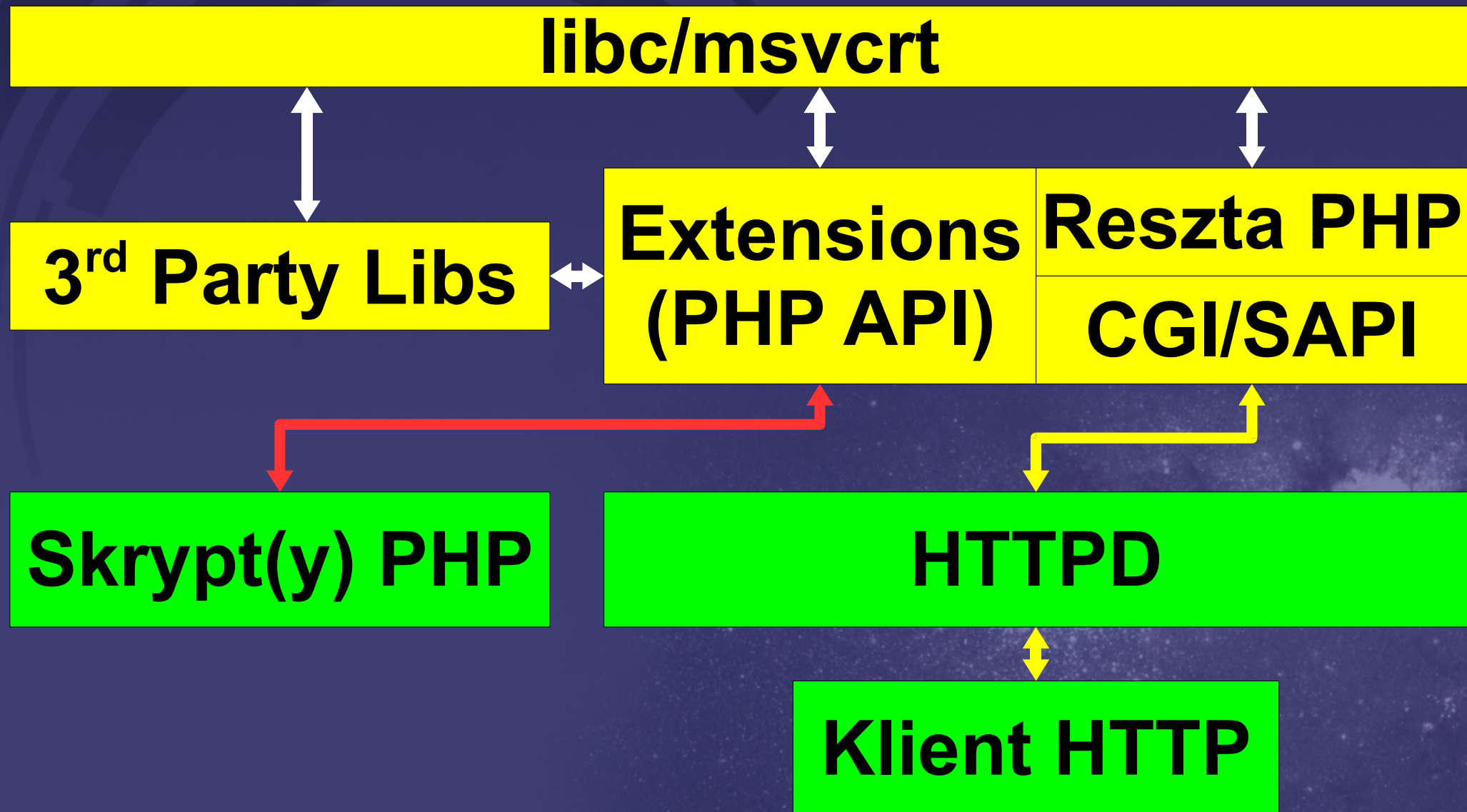
HTTPD

↑ HTTP(S)

Klient HTTP







System Operacyjny

libc/msvcrt

3rd Party Libs

**Extensions
(PHP API)**

**Reszta PHP
CGI/SAPI**

Skrypt(y) PHP

HTTPD

Klient HTTP

Dwa punkty widzenia

...czyli bezpieczeństwo w
PHP od strony admina i
właściciela strony WWW

The background of the slide is a dark blue gradient. In the top-left corner, there is a graphic of several concentric, semi-circular arcs made of small, dark blue rectangular segments, resembling a stylized rainbow or a series of orbits. The bottom-right portion of the slide features a faint, starry pattern, similar to a nebula or a distant galaxy, in a lighter shade of blue.

Punkt pierwszy...

Klient HTTP

A diagram illustrating an HTTP client connection. A yellow box at the top contains the text "Klient HTTP". A yellow double-headed vertical arrow points from this box to a second yellow box below it. The second box contains the text "public_html/asdf.php". The background of the slide is dark blue with faint gear-like patterns on the left and a starry space pattern on the right.

public_html/asdf.php

Klient HTTP



public_html/asdf.php



/etc/passwd

C99

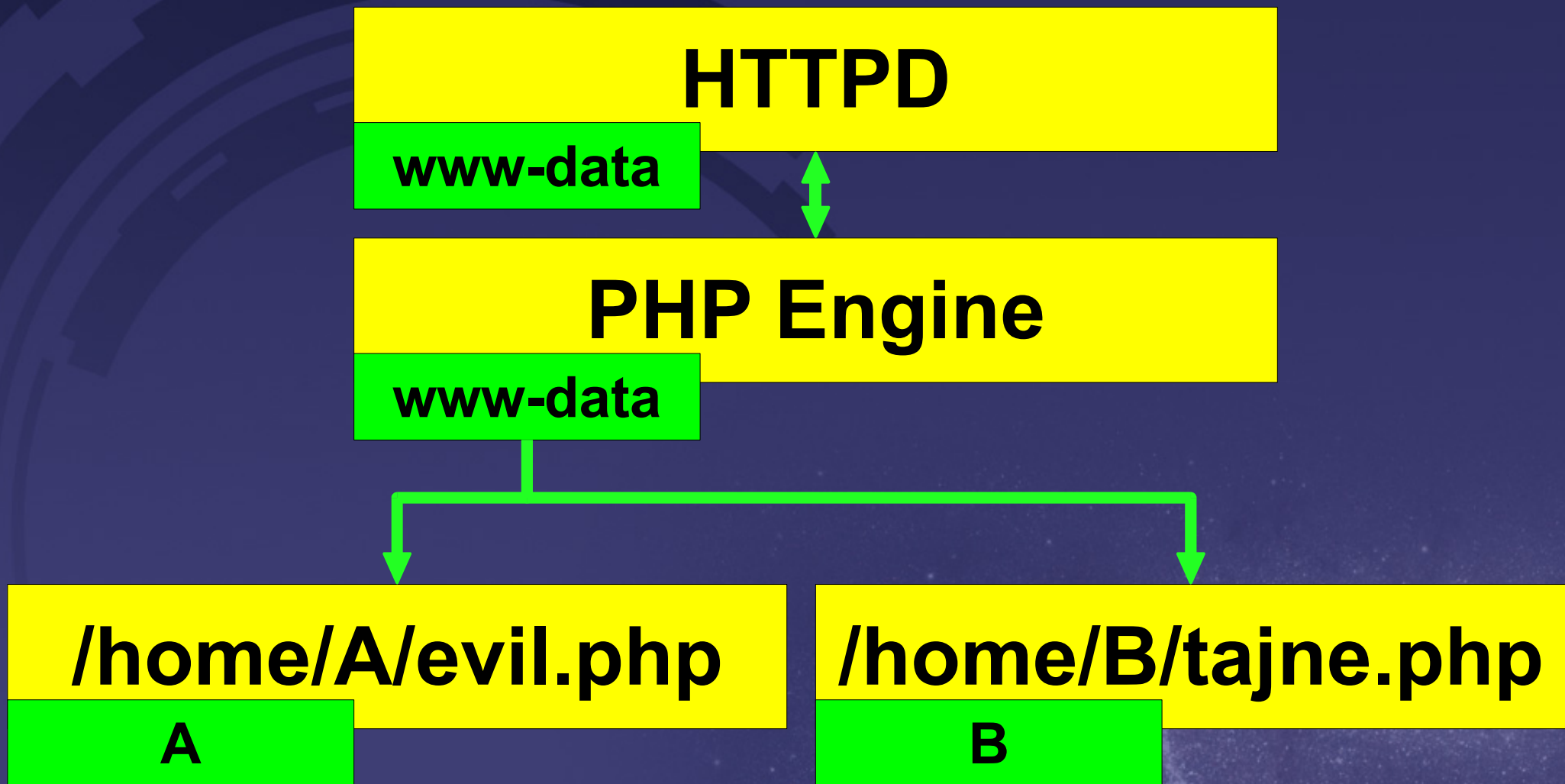
SQLI

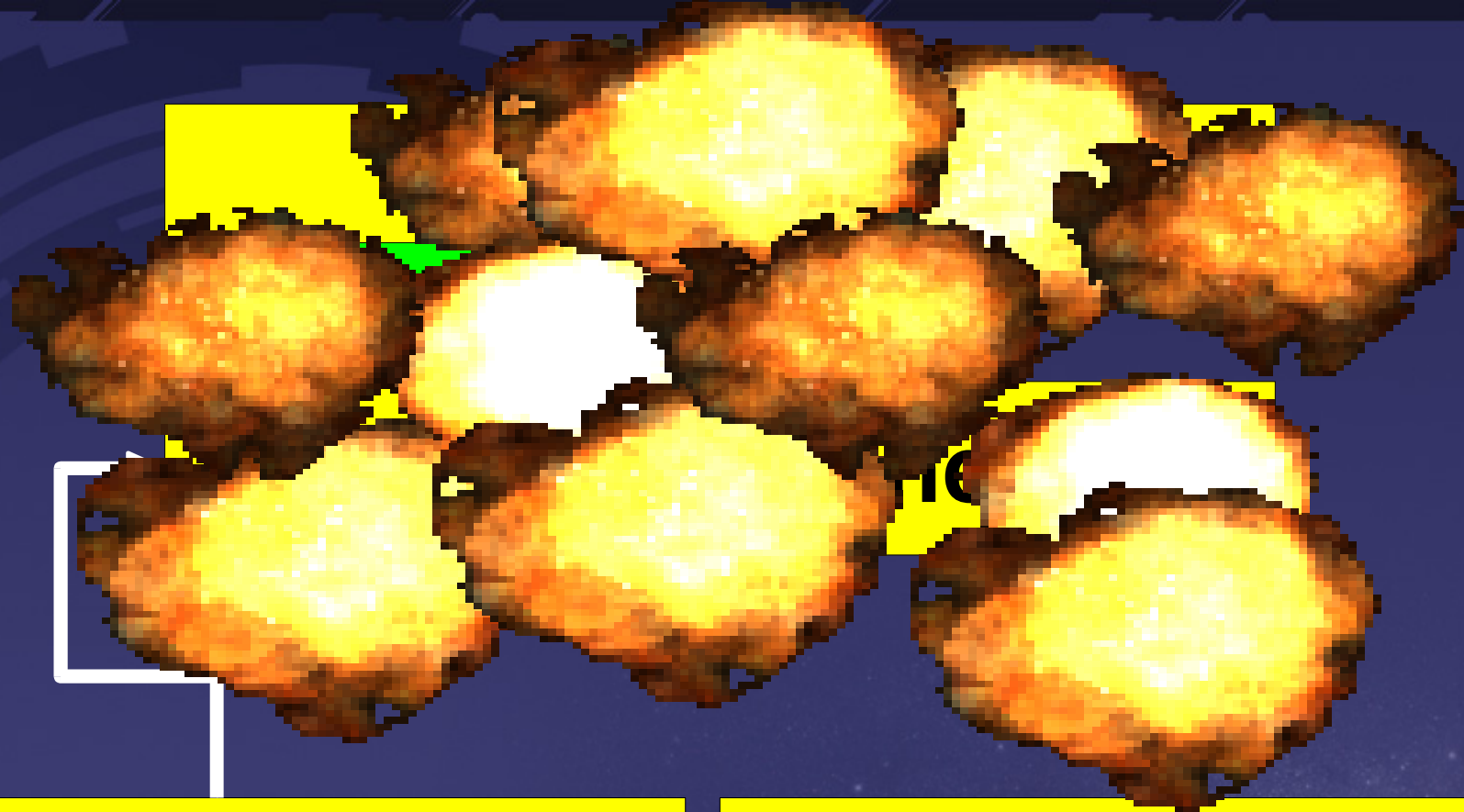
LFI

RFI

The background is a dark blue gradient. In the top-left corner, there are several concentric, semi-circular arcs made of a dashed or segmented pattern. In the bottom-right corner, there is a faint, starry pattern resembling a galaxy or nebula.

Punkt drugi...





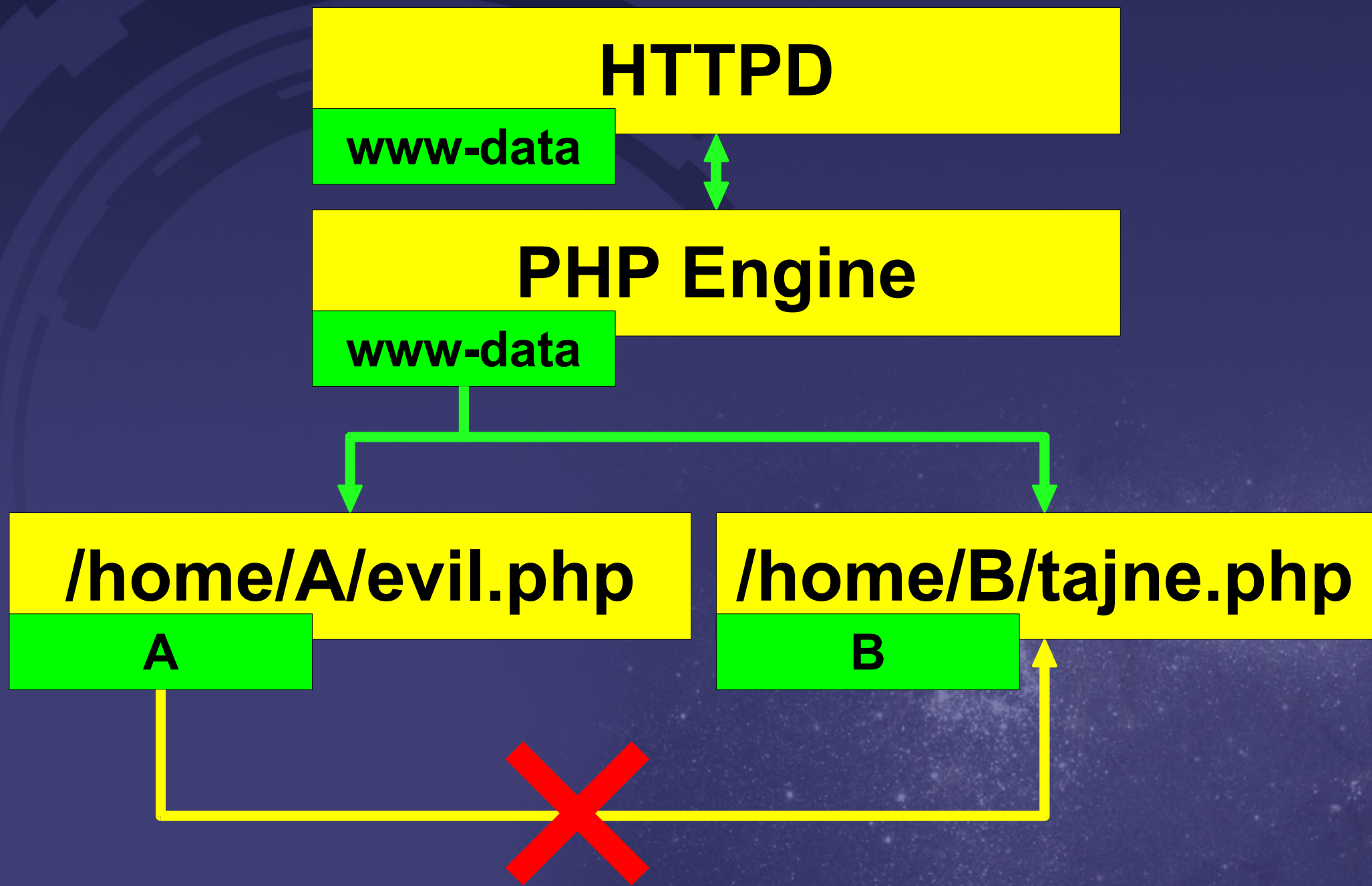
/home/A/evil.php

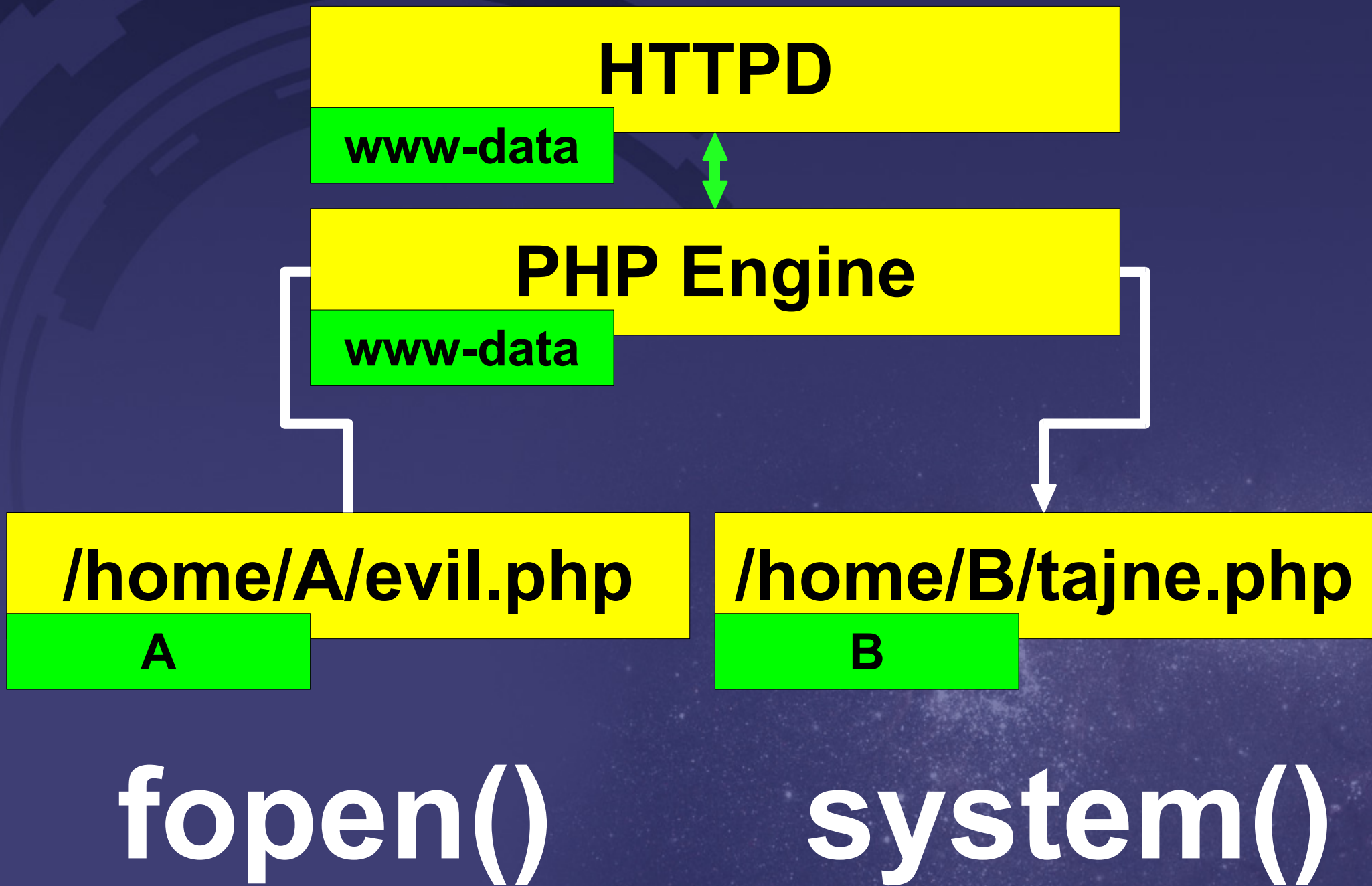
A

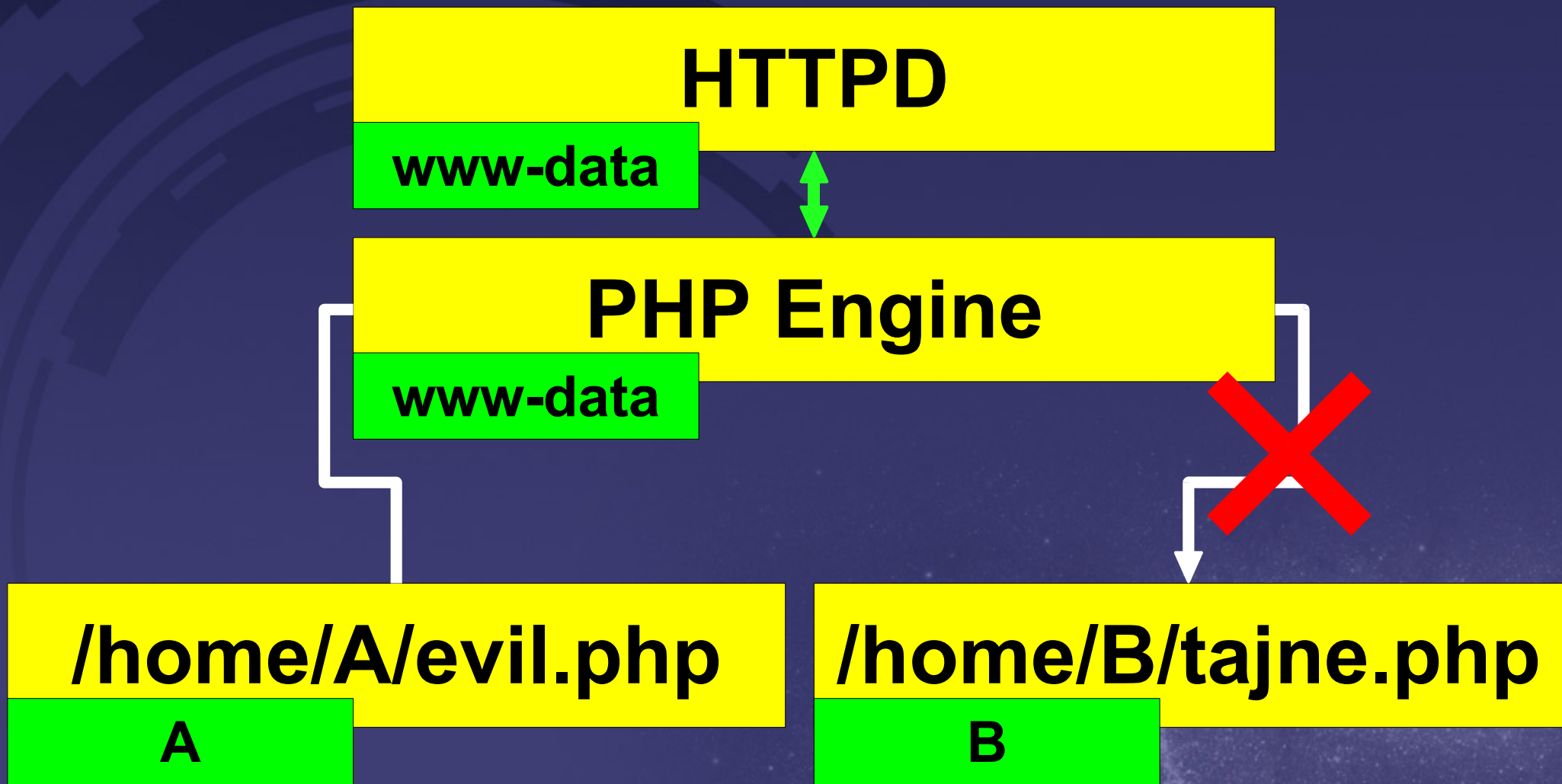
/home/B/tajne.php

B

DoS







**open base dir
restriction**

safe mode

Czas na „internals”



R U PHP?

(to nie błąd, to feature)

Czyli czy asdf.html to skrypt PHP ?

BLACK SHEEP WALL

```
ext/standard/info.h:#define PHP_LOGO_GUID  
"PHPE9568F34-D428-11d2-A769-00AA001ACF42"
```

```
ext/standard/info.h:#define PHP_EGG_LOGO_GUID  
"PHPE9568F36-D428-11d2-A769-00AA001ACF42"
```

```
ext/standard/info.h:#define ZEND_LOGO_GUID  
"PHPE9568F35-D428-11d2-A769-00AA001ACF42"
```

Null Byte **Poison**

Olaf Kirch (1998)

...czyli o różnicach w
kodowaniu stringów

Plik z hasłem: **asdf.pass**

```
<?php  
$f = fopen('..' . $_GET['x'] . '.txt', 'r');  
echo @fread($f, 1024);
```

BLACK SHEEP WALL

Metody zapisu stringów

1. Terminator

[dane] [terminator]

np. asdf\0 lub asdf\$
(z/bez escape'owania)

00000000	4D 5A 90 00	03 00 00 00	04 00 00 00	FF FF 00 00	MZ.....ÿÿ..
00000010	B8 00 00 00	00 00 00 00	40 00 00 00	00 00 00 00@.....
00000020	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
00000030	00 00 00 00	00 00 00 00	00 00 00 00	80 00 00 00
00000040	0E 1F BA 0E	00 B4 09 CD	21 B8 01 4C	CD 21 54 68	..²..'.'Í!.,.LÍ!Th
00000050	69 73 20 70	72 6F 67 72	61 6D 20 63	61 6E 6E 6F	is program canno
00000060	74 20 62 65	20 72 75 6E	20 69 6E 20	44 4F 53 20	t be run in DOS
00000070	6D 6F 64 65	2E 0D 0D 0A	24 00 00 00	00 00 00 00	mode....\$.
00000080	50 45 00 00	4C 01 05 00	BB 71 DB 49	00 16 00 00	PE..L....»qÛI....
00000090	F7 01 00 00	E0 00 07 03	0B 01 02 38	00 0A 00 00	÷...à.....8....
000000A0	00 12 00 00	00 02 00 00	70 12 00 00	00 10 00 00

Metody zapisu stringów

1. Terminator

[dane] [terminator]

np. asdf\0 lub asdf\$
(z/bez escape'owania)

DOS (\$)

C (\0)

Kernel Linux (\0)

Metody zapisu stringów

2. Length + Data

[długość] [dane]

np. **[4]**asdf lub **[1][4]**asdf
(z/bez escape'owania)

PHP

Java

MySQL protocol

Kernel Windows

Metody zapisu stringów

2. Length + Data

[długość] [dane]

np. **[4]**asdf lub **[1][4]**asdf
(z/bez escape'owania)

```
typedef union _zvalue_value {  
    [...]  
    struct {  
        char *val;  
        int len;  
    } str;  
    [...]
```

Skrypt PHP vs C (implementacja)

```
$f = fopen(„asdf\0xxx”);
```

```
val → „asdf\0xxx”
```

```
len → 8
```



**implementacja
fopen()**

```
zend_parse_parameters([...] “s|br”,  
    &filename, &filename_len, [...]  
    &(char*)    &(int))
```

```
f = fopen(new_state.cwd, mode);
```

Skrypt PHP vs C (implementacja)

```
f open( „as df \0xxx” );
```

to dla systemu

```
f open( „as df ” );
```

Path truncation (5.2.10)

*Francesco “ascii” Ongaro
Giovanni “evilaliv3” Pellerano*

Schodzimy niżej...

Plik z hasłem: **asdf.pass**

```
<?php  
$x = addslashes($_GET['x']);  
include(„$x.txt”);
```

BLACK SHEEP WALL

Bo bufor był za mały...
(4096)



Bo bufor był za mały

Tokenizacja po separatorze katalogów + zignorowanie tokenów „obecnego katalogu”

```
ptr = tsrm_strtok_r(path_copy, '/', &tok);  
while(ptr) { ...
```

dla IS_DIRECTORY_CURRENT nic nie jest
wykonywane

mail.log (5.3.0)

Maksymilian „cxib” Arciemowicz

Czyli o wykorzystaniu logów
po raz n-ty...

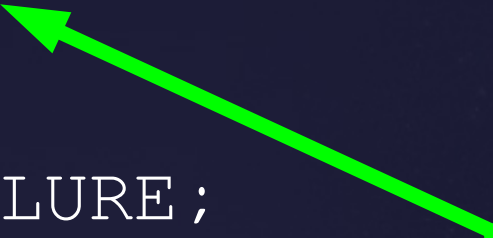
Plik z hasłem:
`/home/test/public_html/asdf.pass`

- Utrudnienia:
1. deny from all dla \.pass\$
 2. skonfigurowany open_basedir

BLACK SHEEP WALL

Kt oś zapomniał o sprawdzeniu open_basedir :

```
if (PG(open_basedir) &&  
    php_check_open_basedir(new_value TSRMLS_CC))  
{  
  
    return FAILURE;  
  
}
```



Kod którego nie było

(main/main.cpp)

NTFS ADS*

Czyli dwukropek zła...

*Alternate Data Streams

```
if(file_exists('config.php'))  
    readfile('asdf.pass');  
  
$filename = addslashes($_GET['f']);  
$f = fopen('./' . $filename . '.txt', 'w');  
if($f)  
{  
    fwrite($f, "Sth!");  
    fclose($f);  
}
```

BLACK SHEEP WALL

ADS

Nazwa.Pliku:Strumień.Danych

asdf.txt

asdf.txt:\$DATA

asdf.txt:costam.exe

asdf.txt:costam.exe:\$DATA

Array
(greetz to adam_i)

*„Nikt nie spodziewa się
hiszpańskiej inkwizycji!”*

Monty Python

main/php_variables.c

```
[...]  
} else if (*p == '[') {  
    is_array = 1;  
[...]
```

Tabl i ca Tabl i c Tabl i c :)
(5.2.6 *convert_cyr_string*)

BLACK SHEEP WALL

```
<?php
if($_GET['a'] != $_GET['b'])
{
    if(md5($_GET['a']) == md5($_GET['b']))
        echo(„Haslo to ...");
}
else
{
    die(„'a' != 'b'");
}
```

BLACK SHEEP WALL

```
$x = addslashes($_GET['x']);  
if($x !== 'HASLO')  
    die(„“)
```

H I N T: W a r n i n g i s e v i l !

BLACK SHEEP WALL

```
$a = addslashes($_GET['a']);  
$b = $_GET['b'];  
if($b == 0)  
    die("Null byte not allowed!");  
  
readfile('./' . $a . chr($b) . '.txt');
```

BLACK SHEEP WALL

```
if (zend_parse_parameters_ex(
    ZEND_PARSE_PARAMS_QUIET,
    [...], "l", &c) == FAILURE) {
    c = 0;
}
```

```
temp[0] = (char)c;
temp[1] = '\0';
```



`session_start()`

Warningi, warningi...

A large, stylized gear or circular arrow graphic in the top left corner, composed of several concentric arcs and segments, suggesting a cycle or process.

```
<?php  
session_start();
```

BLACK SHEEP WALL

`session_start()`

Dygresja o LFI → RFI

`/tmp/sess_NAZWA`
`/tmp/sess_Array`

getimagesize()

Warningi, warningi...

*If accessing the filename image is impossible, or if it **isn't a valid picture**, getimagesize() will generate an error of level E_WARNING. On read error, getimagesize() will generate an error of level E_NOTICE.*

Returns an array with 7 elements.

```
if (result->bits != 0) {  
    add_assoc_long(return_value, "bits",  
result->bits);  
}  
if (result->channels != 0) {  
    add_assoc_long(return_value, "channels",  
result->channels);  
}
```

BLACK SHEEP WALL

JPC

```
$data = "\xff\x4f\xffHi!";
```

JP2

```
$data = "\x00\x00\x00\x0c\x6a\x50".  
        "\x20\x20\x0d\x0a\x87\x0a";
```

PNG

```
$data = "\x89\x50\x4eALAMAKOTA";
```

BLACK SHEEP ICEWALL

getimagesize()
(a ico jest udokumentowane)

*Awatar musi mieć
maksymalnie 80 na 80
pikseli...*

regulamin losowego forum

BLACK SHEEP WALL

getimagesize()

„Note: The information about icons are retrieved from the icon with the highest bitrate.”

getimagesize()

Czy ten obrazek jest
obrazkiem?

PNG

```
"\x89\x50\x4e\x47\x0D\x0A\x1A\x0A".  
„XXXXYYYY\4\0\0\0\3\0\0\0\0“
```

GIF

```
"GIFxxx\0\4\0\3\xff"
```

XBM

```
„#define asdf_width 123\n".  
„#define asdf_height 123\n“
```

BLACK SHEEP WALL

Po co udawać obrazek?

Trzy powody:

1. LFI i C99

Po co udawać obrazek?

Trzy powody:

1. LFI i C99
2. LFI i C99

Po co udawać obrazek?

Trzy powody:

1. LFI i C99
2. LFI i C99
3. LFI i C99

A large, stylized gear or arc graphic in the top-left corner, composed of several concentric, slightly offset segments.

Kod PHP w danych

Kod PHP po danych

Imagecreatefrom*



image*

Trochę bezpieczniej...



mysqlnd

Czyli jak wysadzić PHP...

„BOOM!”

Oscar Wilde

<http://uncyclopedia.wikia.com>



mysqlnd

Atakujemy klienta SQL :)

BLACKEST SHEEP WALL



**Dziękuję za uwagę :)
Pytania?**

<mailto:gynvael@coldwind.pl>
<http://gynvael.coldwind.pl>
<http://re.coldwind.pl/>