PHP Internals

gynvael.coldwind//vx, Hispasec

gynvael.coldwind//vx

Hispasec

gynvael.coldwind//vx

gynvael.coldwind//vx


Rev. Eng.
Pentesty
Hispasec
Code
gynvael.coldwind//vx
Vexillium

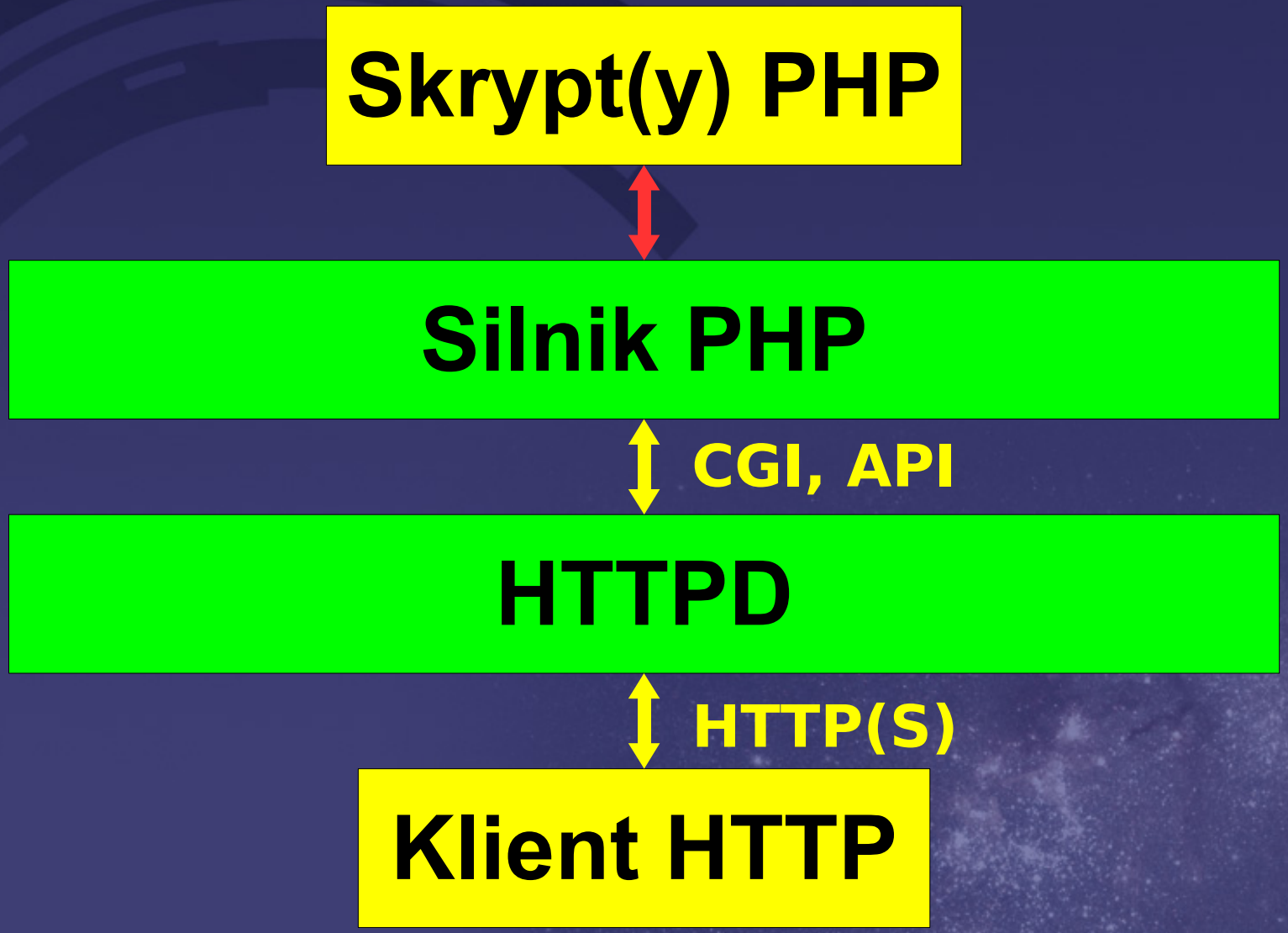

Rev. Eng.
Pentesty
Hispasec
Code
gynvael.coldwind//vx
Vexillium
http://gynvael.coldwind.pl

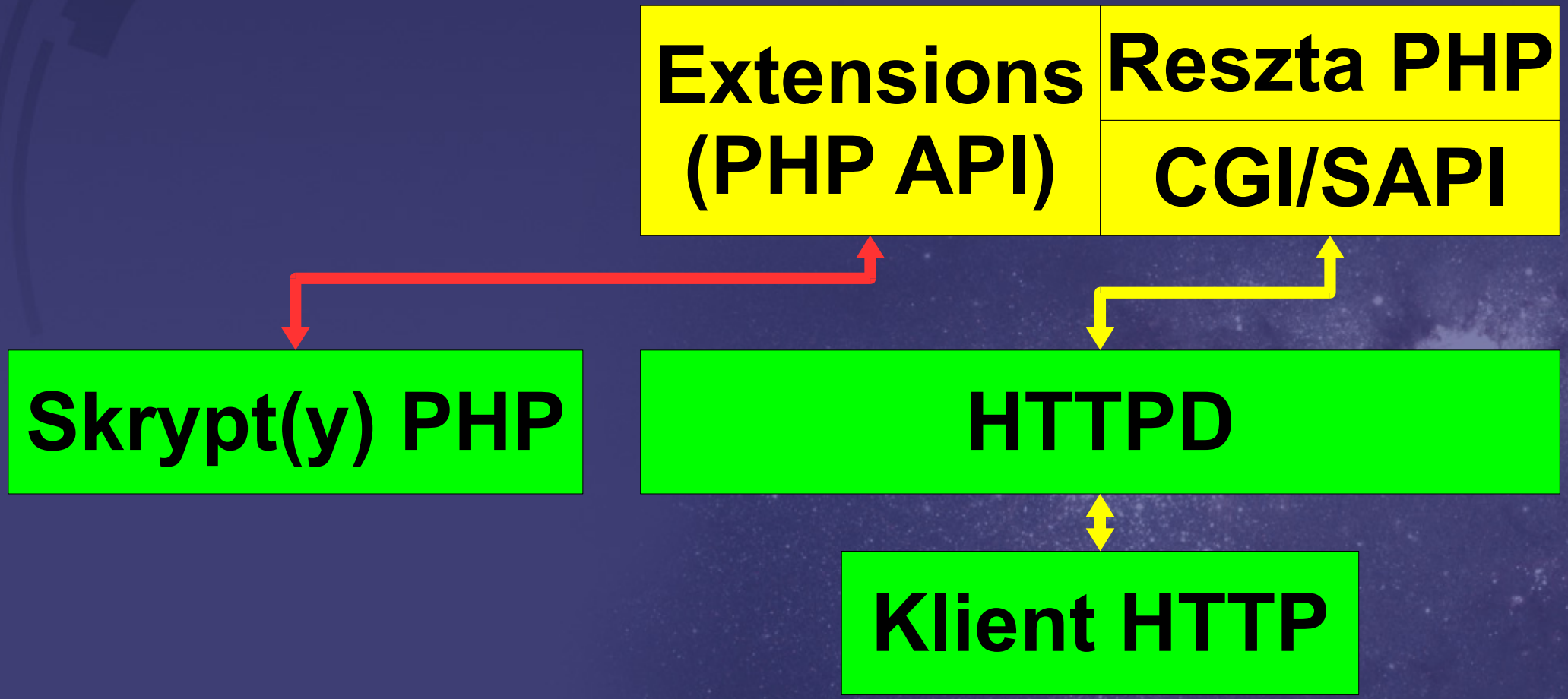

Rev. Eng.
Pentesty
Hispasec
Code
ReverseCraft
gynvael.coldwind//vx
Vexillium
http://gynvael.coldwind.pl

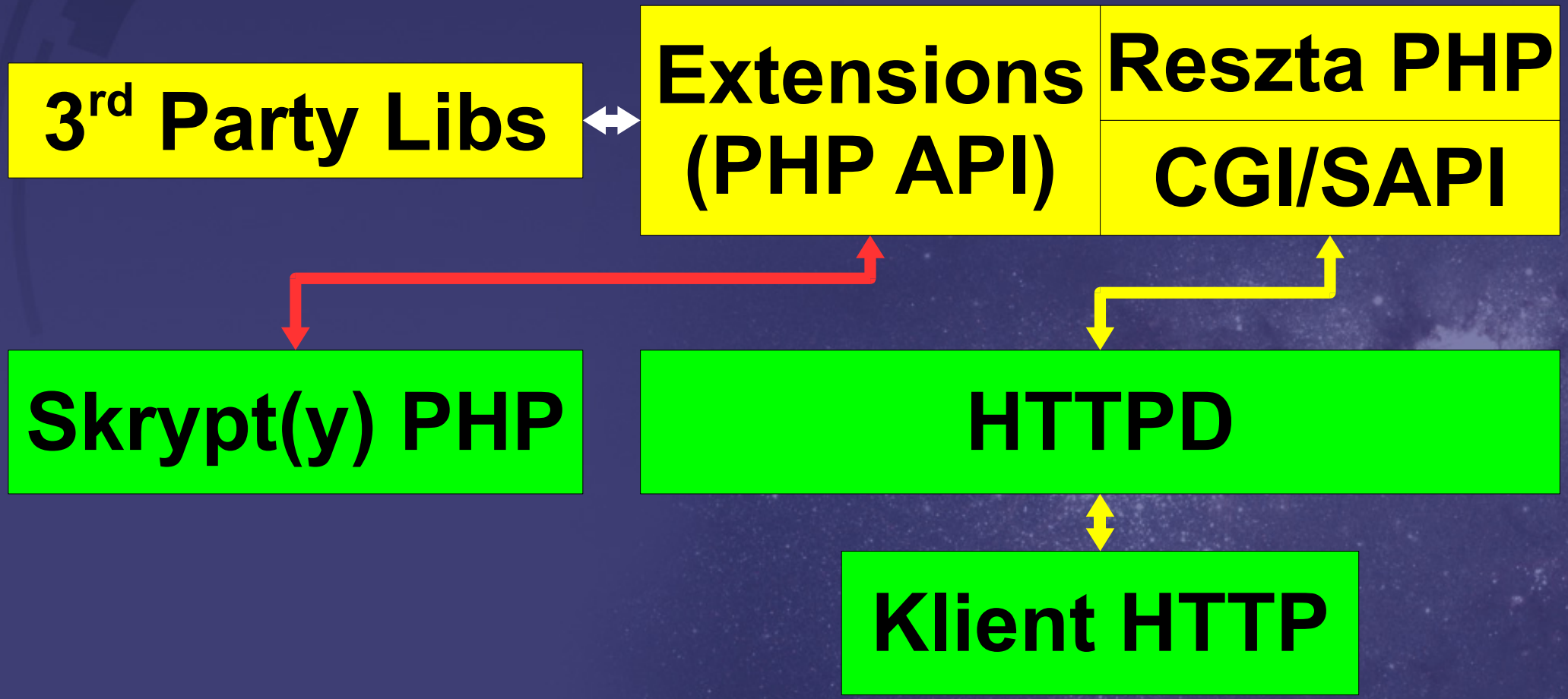
PHP ?Externals?

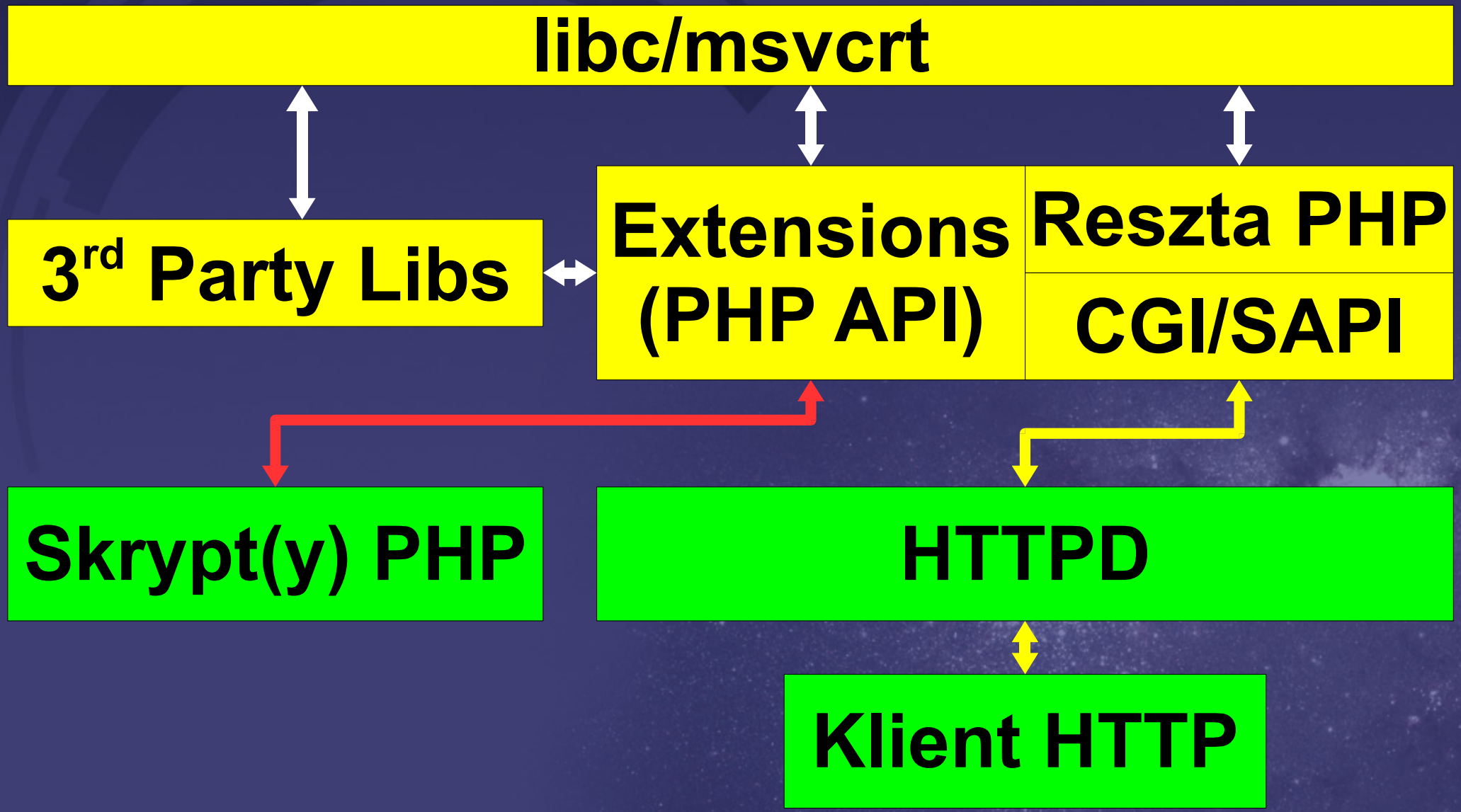
vs.

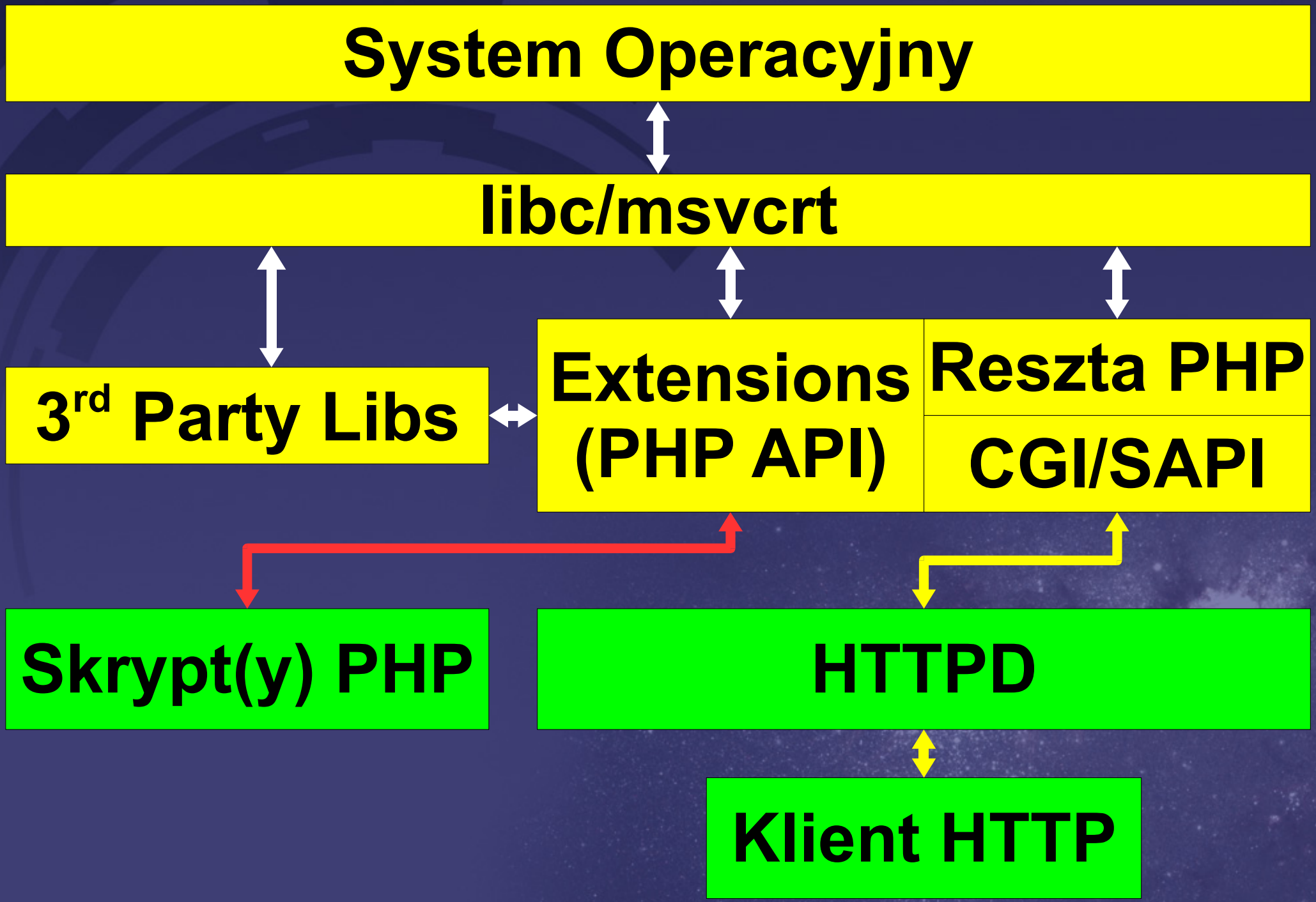
PHP Internals


Skrypt(y) PHP
Silnik PHP
CGI, API
HTTPD
HTTP(S)
Klient HTTP


Extensions
(PHP API)
Reszta PHP
CGI/SAPI
Skrypt(y) PHP
HTTPD
Klient HTTP


3rd Party Libs
Extensions (PHP API)
Reszta PHP
CGI/SAPI
Skrypt(y) PHP
HTTPD
Klient HTTP

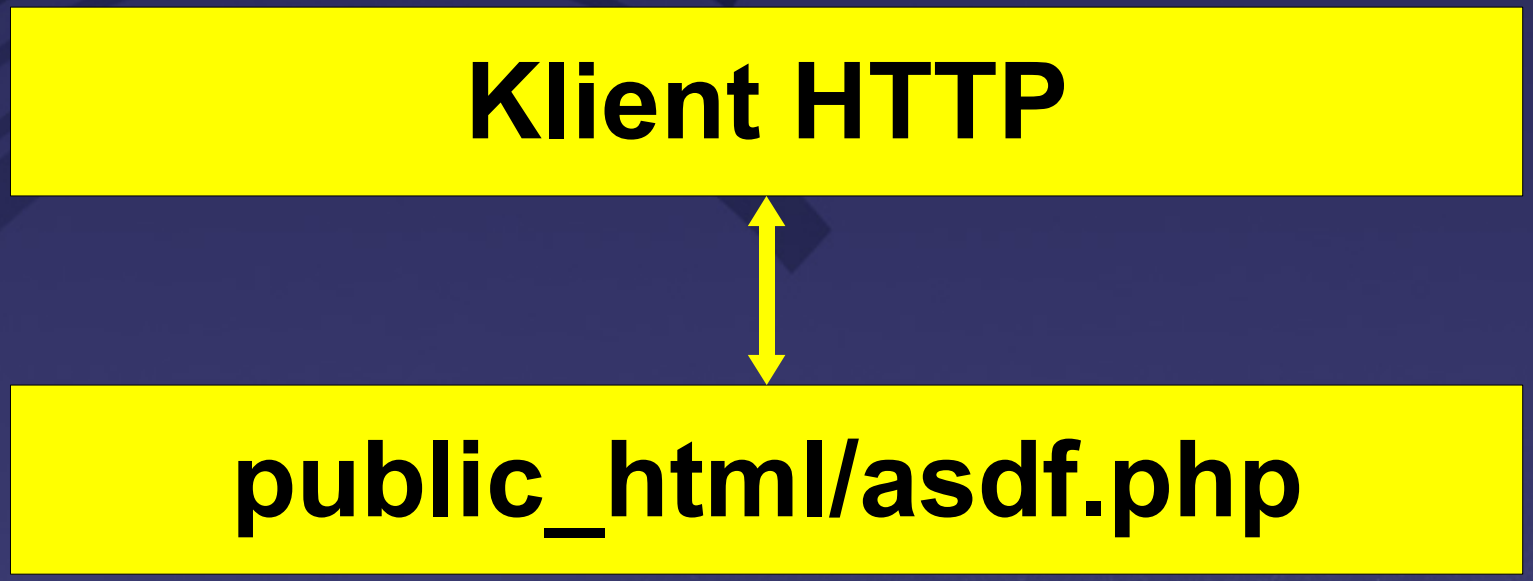

libc/msvcrt
3rd Party Libs
Extensions (PHP API)
Reszta PHP
CGI/SAPI
Skrypt(y) PHP
HTTPD
Klient HTTP

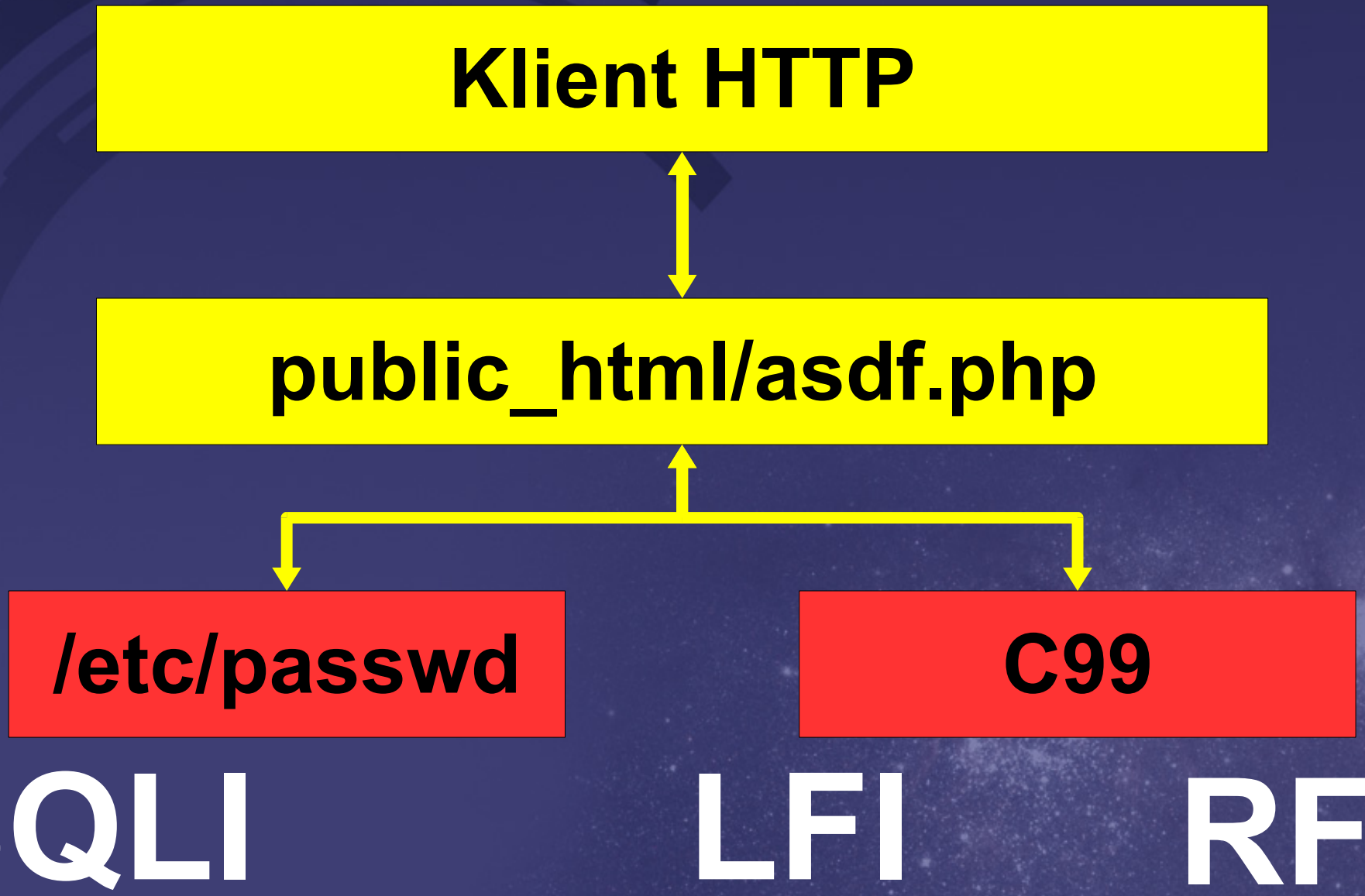

System Operacyjny
libc/msvcrt
3rd Party Libs
Extensions (PHP API)
Reszta PHP
CGI/SAPI
Skrypt(y) PHP
HTTPD
Klient HTTP

Dwa punkty widzenia

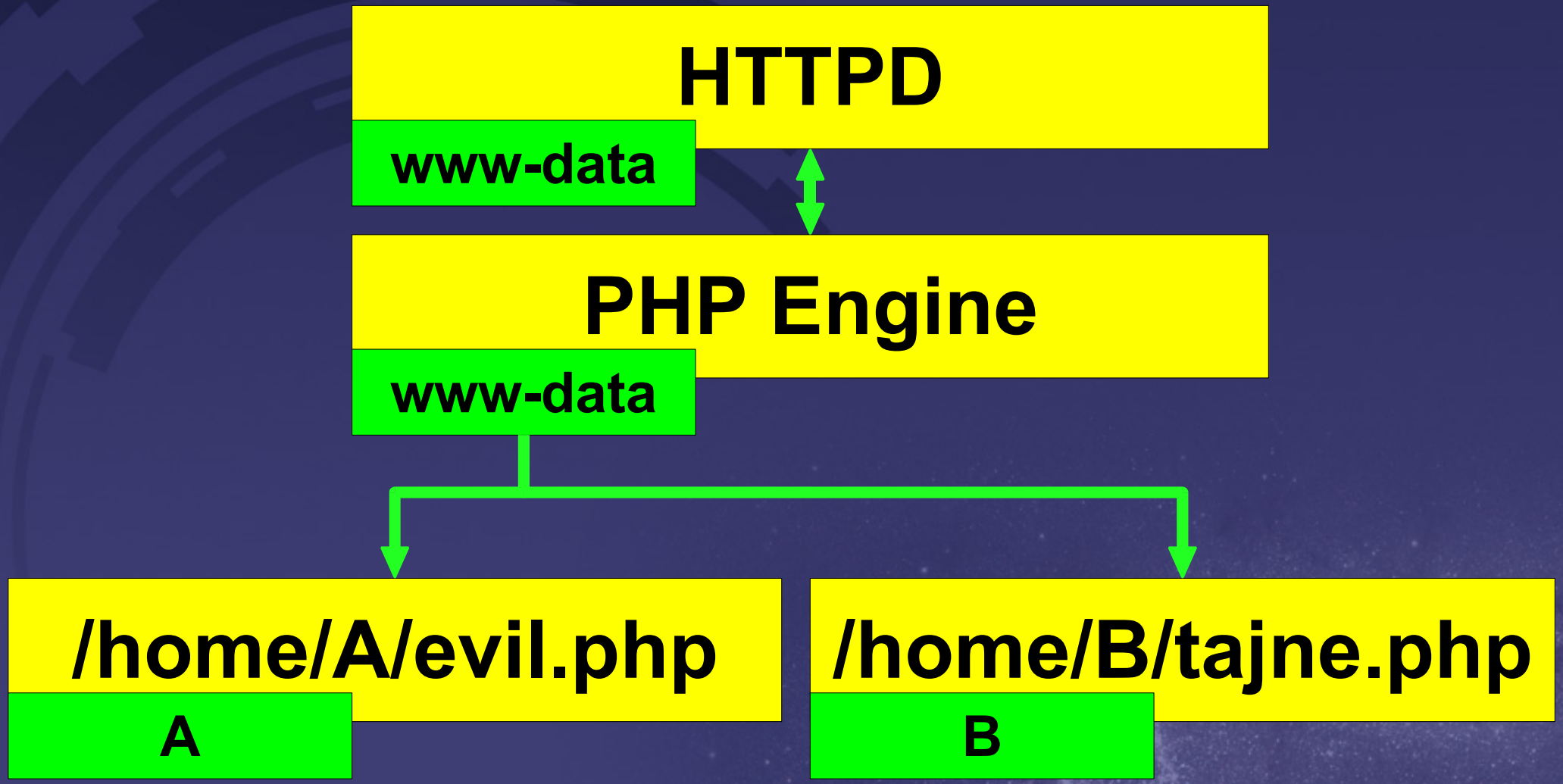
...czyli bezpieczeństwo w PHP od strony admina i właściciela strony WWW

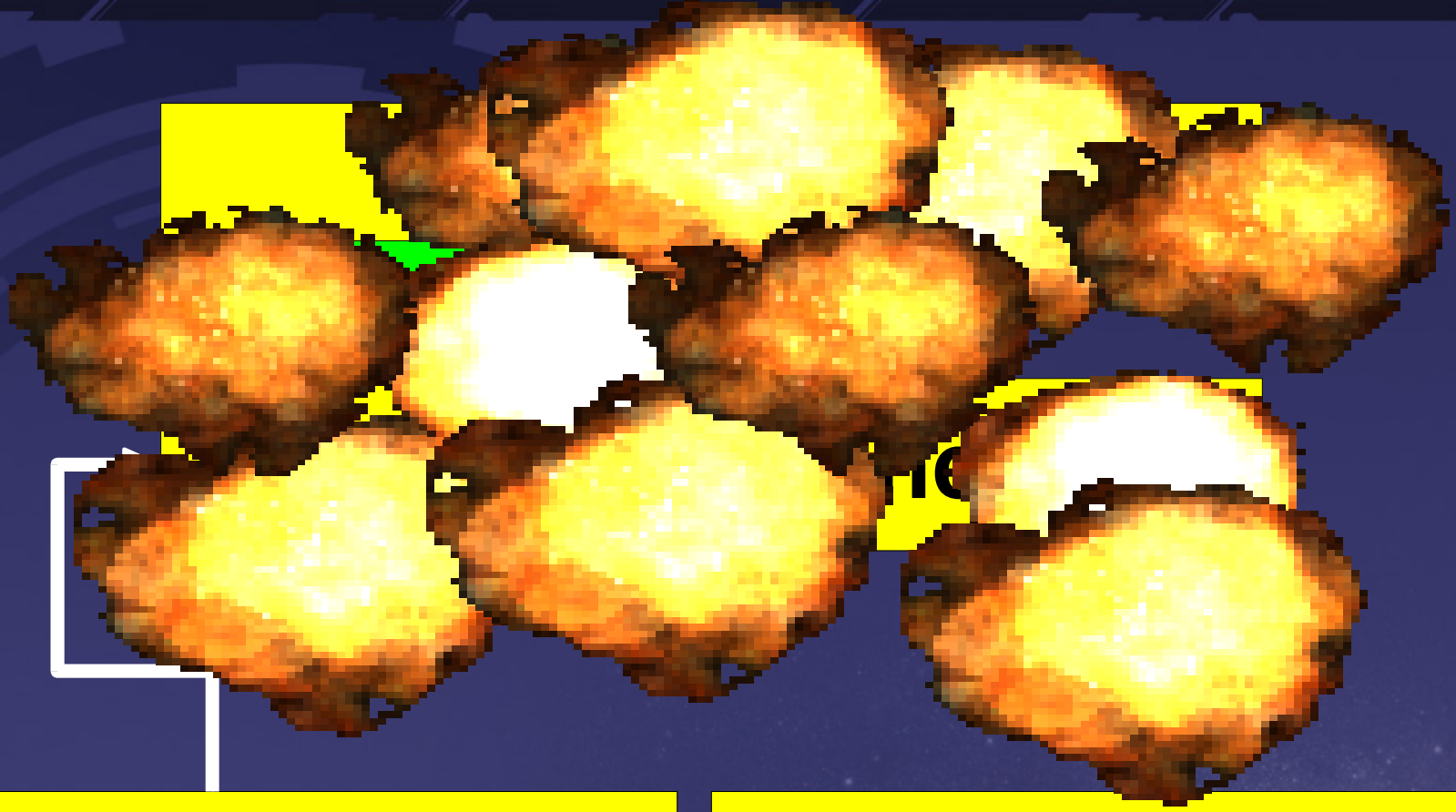
Punkt pierwszy...


Klient HTTP
public_html/asdf.php


Klient HTTP
public_html/asdf.php
/etc/passwd
C99
SQLI
LFI
RFI

Punkt drugi...


HTTPD
www-data
PHP Engine
www-data
/home/A/evil.php
A
/home/B/tajne.php
B



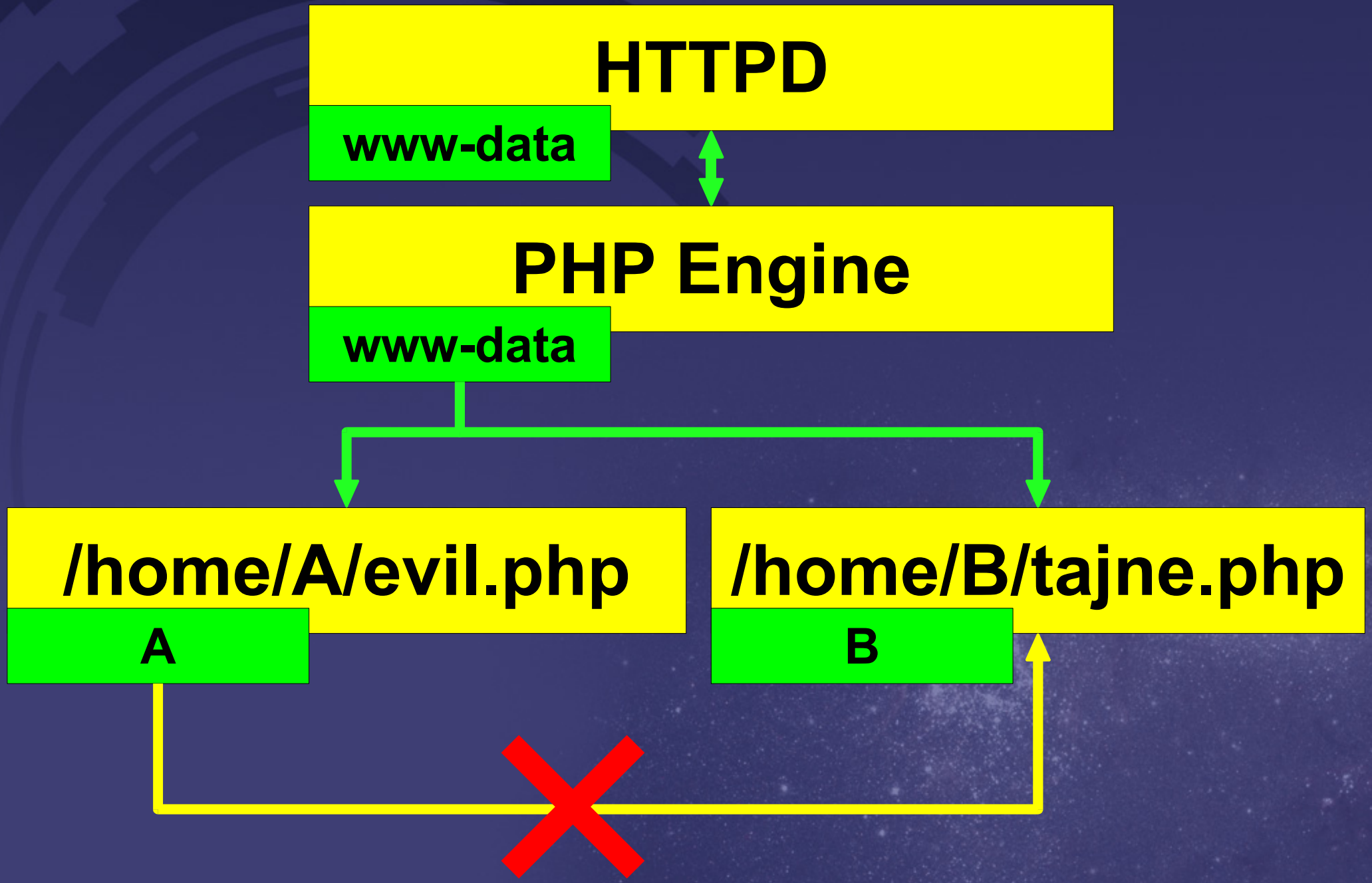
/home/A/evil.php

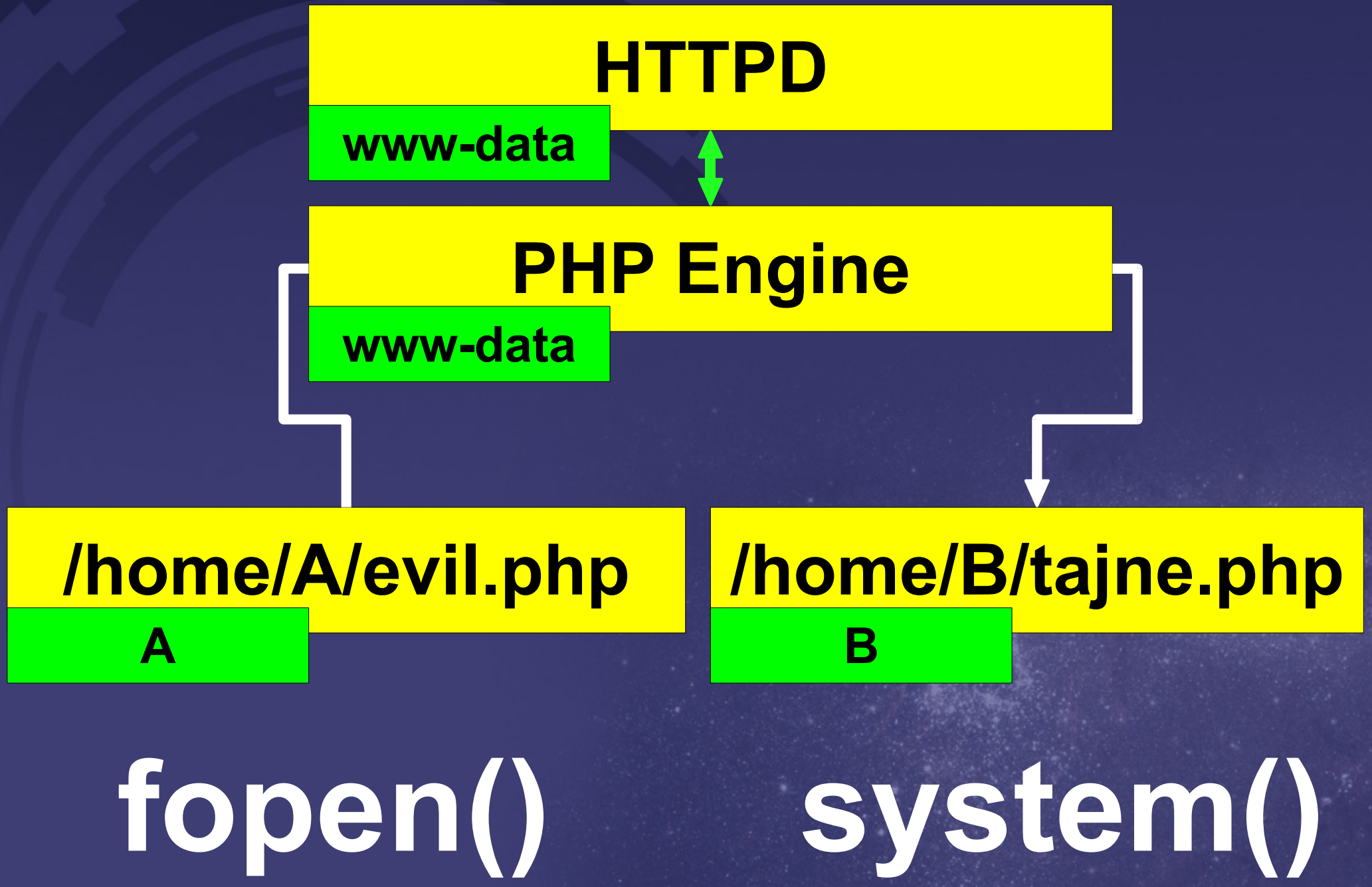
A

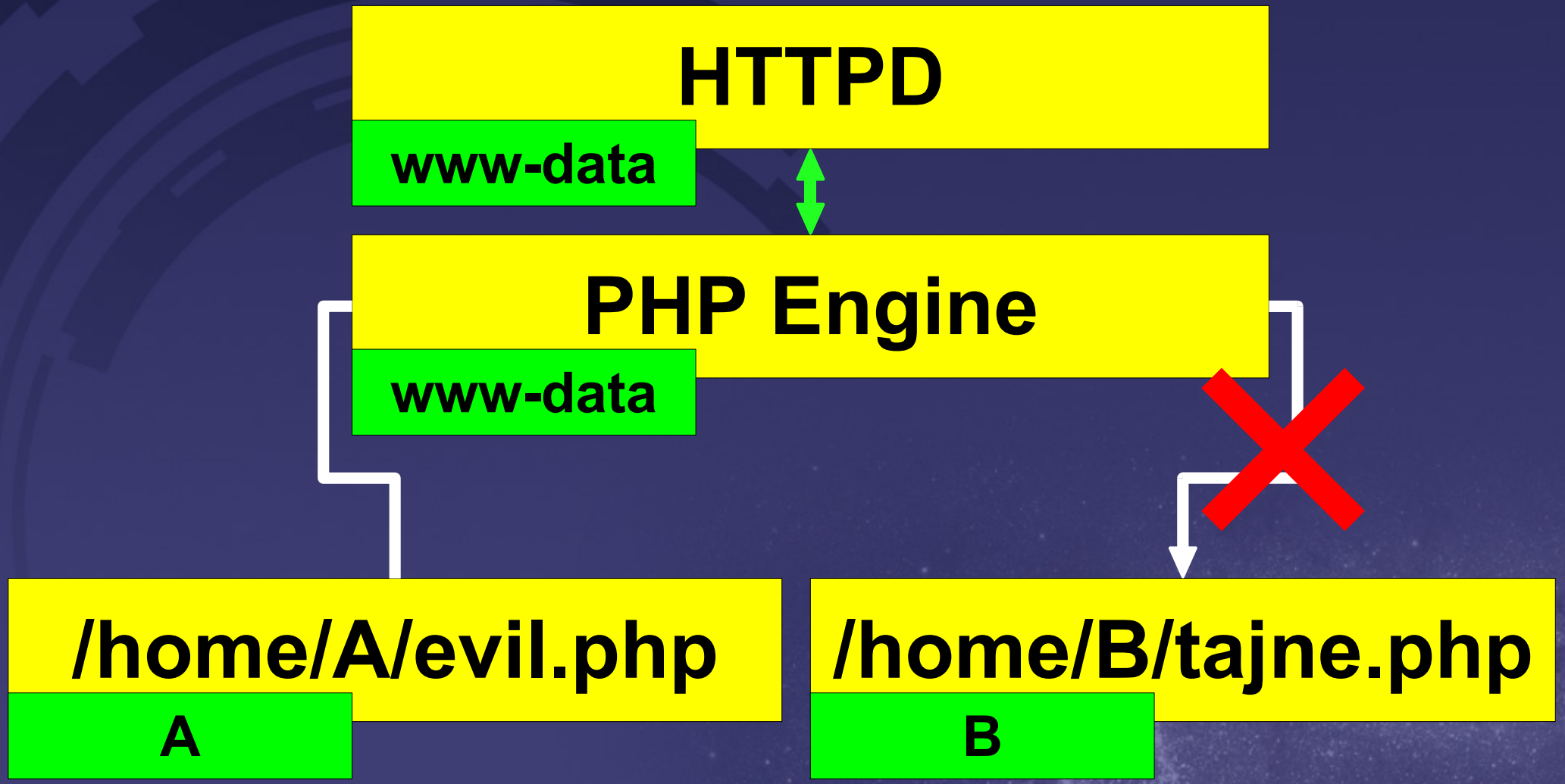
/home/B/tajne.php

B

DoS


HTTPD
www-data
PHP Engine
www-data
/home/A/evil.php
A
/home/B/tajne.php
B


HTTPD
www-data
PHP Engine
www-data
/home/A/evil.php
A
/home/B/tajne.php
B
fopen()
system()



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

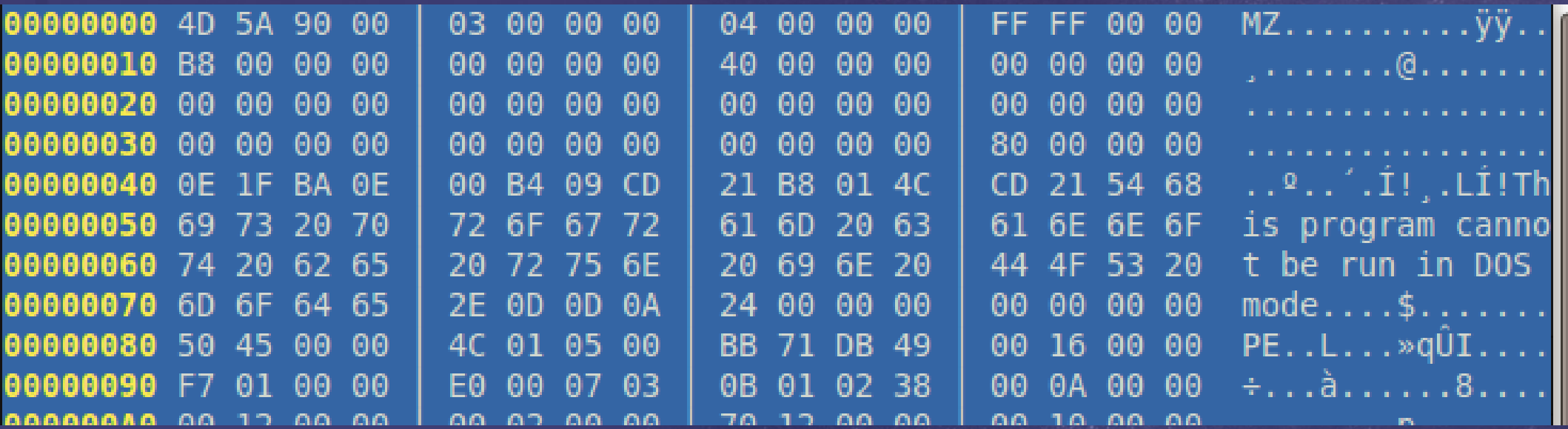
Metody zapisu stringów

1. Terminator

[dane] [terminator]

np. asdf\0 lub asdf$

(z/bez escape'owania)



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([…] ”ssl|br”,
  &filename, &filename_len, […]
  &(char*)   &(int)

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

Skrypt PHP vs C (implementacja)

```
fopen("asdf\0xxx");
```

to dla systemu

```
fopen("asdf");
```

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)

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

Ktoś 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;
[…]
```

Tablica Tablic Tablic :)

(5.2.6 convert_cyr_string)

BLACK SHEEP WALL

```php
<?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(„”)
```

HINT: Warning is evil!

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...

```php
<?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

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

Dziękuje za uwagę :)

Pytania?

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