文件包含

北京联合大学 glzjin

能力要求

- 了解常见的文件包含点
- 会基本利用文件包含点，包括伪协议等

成因

```php
<?php
/** Created by PhpStorm. ...*/

$_GET['file'] = "13_2.php";
require_once $_GET["file"];
// include $_GET["file"];
```

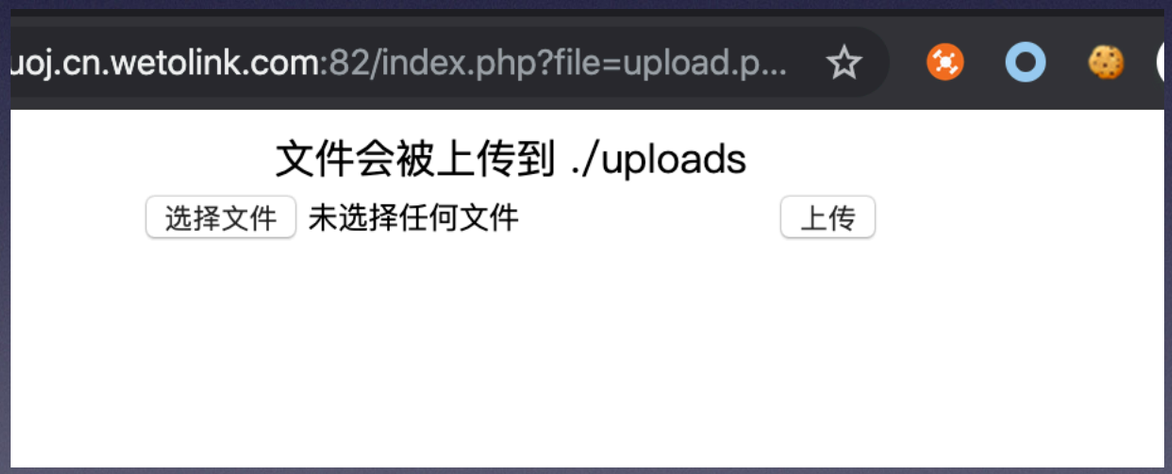
- 被包含的文件如果含有 <?php <? 等 php 头，里面的 php 代码就会被执行。

常见可在服务器上生成文件的功能

- 文件上传
- 服务器日志（/var/log/apache2/access.log 等）
- 程序本身的自带备份功能（MyWebSQL 等）

BUU UPLOAD COURSE 1

- 观察地址，有 file 参数，指向 upload.php。

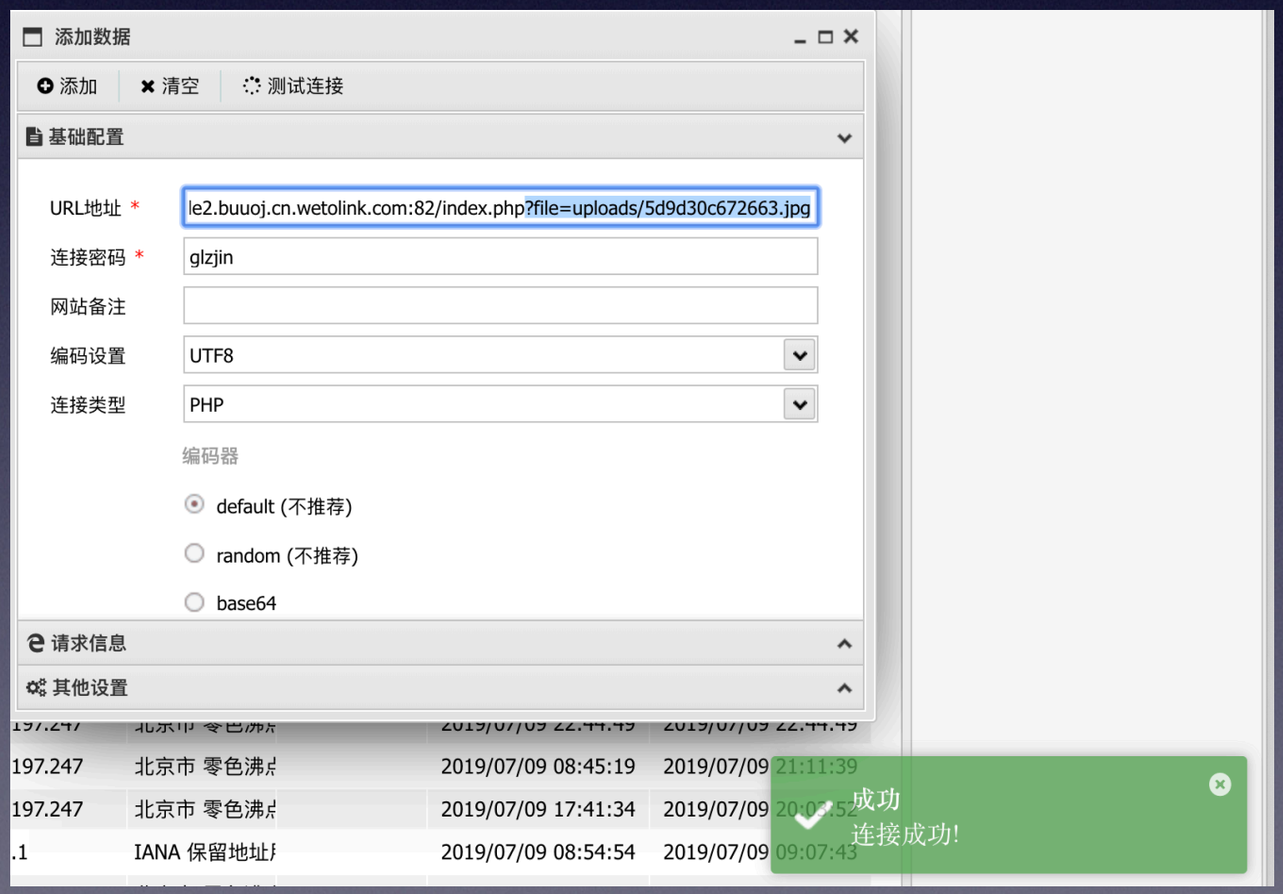


BUU UPLOAD COURSE 1

- 上传的文件保存到的文件名随机，后缀都会被改成 jpg

BUU UPLOAD COURSE 1

- 将 file 参数改为这个路径，即可将这个文件包含进来，使其作为 php 文件执行

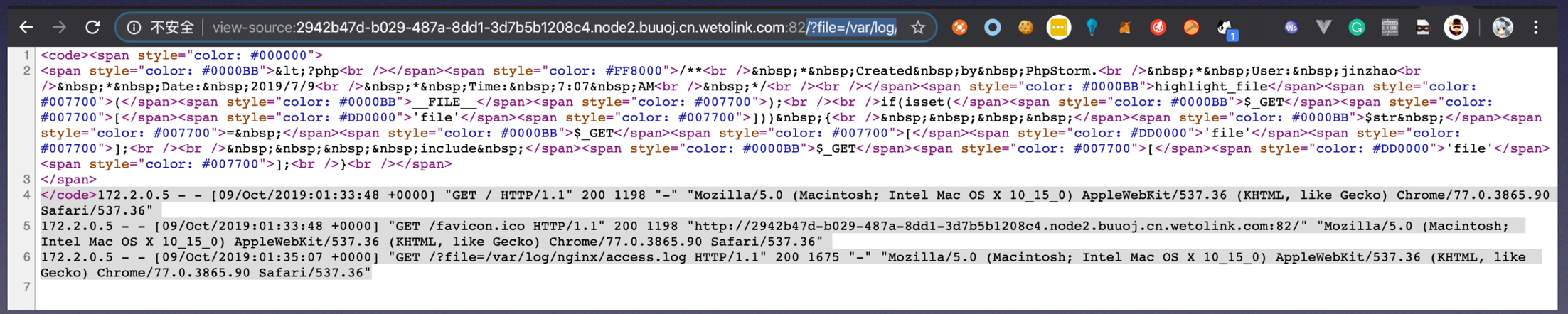


BUU LFI COURSE 1

- 无上传点，使用服务器日志包含。

BUU LFI COURSE 1

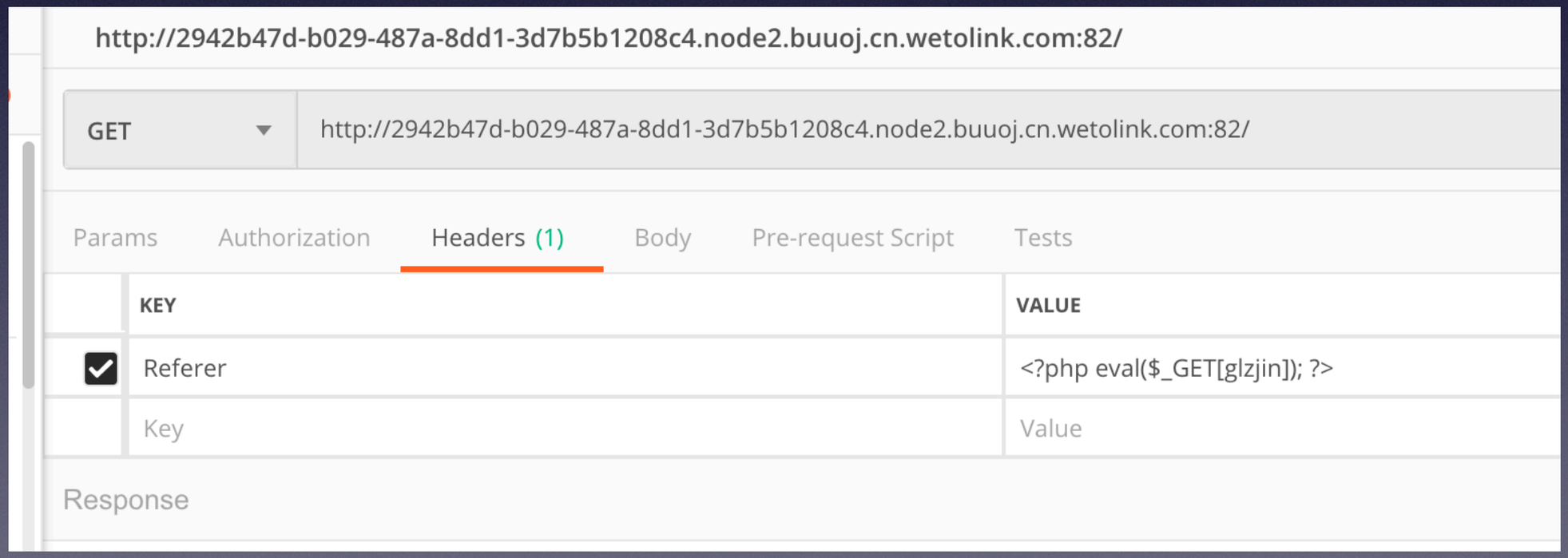
- /?file=/var/log/nginx/access.log




```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br /></span><span style="color: #FF8000">/**<br /> * Created by PhpStorm.<br /> * User: jinzhao<br /> * Date: 2019/7/9<br /> * Time: 7:07 AM<br /> */<br /><br /></span><span style="color: #0000BB">highlight_file</span><span style="color: #007700">(</span><span style="color: #0000BB">__FILE__</span><span style="color: #007700">);<br /><br />if(isset(</span><span style="color: #0000BB">$_GET</span><span style="color: #007700">[</span><span style="color: #DD0000">'file'</span><span style="color: #007700">])) {<br />    </span><span style="color: #0000BB">$str </span><span style="color: #007700">= </span><span style="color: #0000BB">$_GET</span><span style="color: #007700">[</span><span style="color: #DD0000">'file'</span><span style="color: #007700">];<br /><br />    include </span><span style="color: #0000BB">$_GET</span><span style="color: #007700">[</span><span style="color: #DD0000">'file'</span><span style="color: #007700">];<br />}<br /></span>
</span>
</code>172.2.0.5 - - [09/Oct/2019:01:33:48 +0000] "GET / HTTP/1.1" 200 1198 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36"
172.2.0.5 - - [09/Oct/2019:01:33:48 +0000] "GET /favicon.ico HTTP/1.1" 200 1198 "http://2942b47d-b029-487a-8dd1-3d7b5b1208c4.node2.buuoj.cn.wetolink.com:82/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36"
172.2.0.5 - - [09/Oct/2019:01:35:07 +0000] "GET /?file=/var/log/nginx/access.log HTTP/1.1" 200 1675 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36"
```

BUU LFI COURSE 1

- 尝试修改 Referer 头来在日志里插入不被转义的内容。



BUU LFI COURSE 1

- 再次包含日志文件并加上 glzjin 参数即可 RCE。
- /?file=/var/log/nginx/access.log&glzjin=phpinfo();

StarCTF 2019-mywebsql

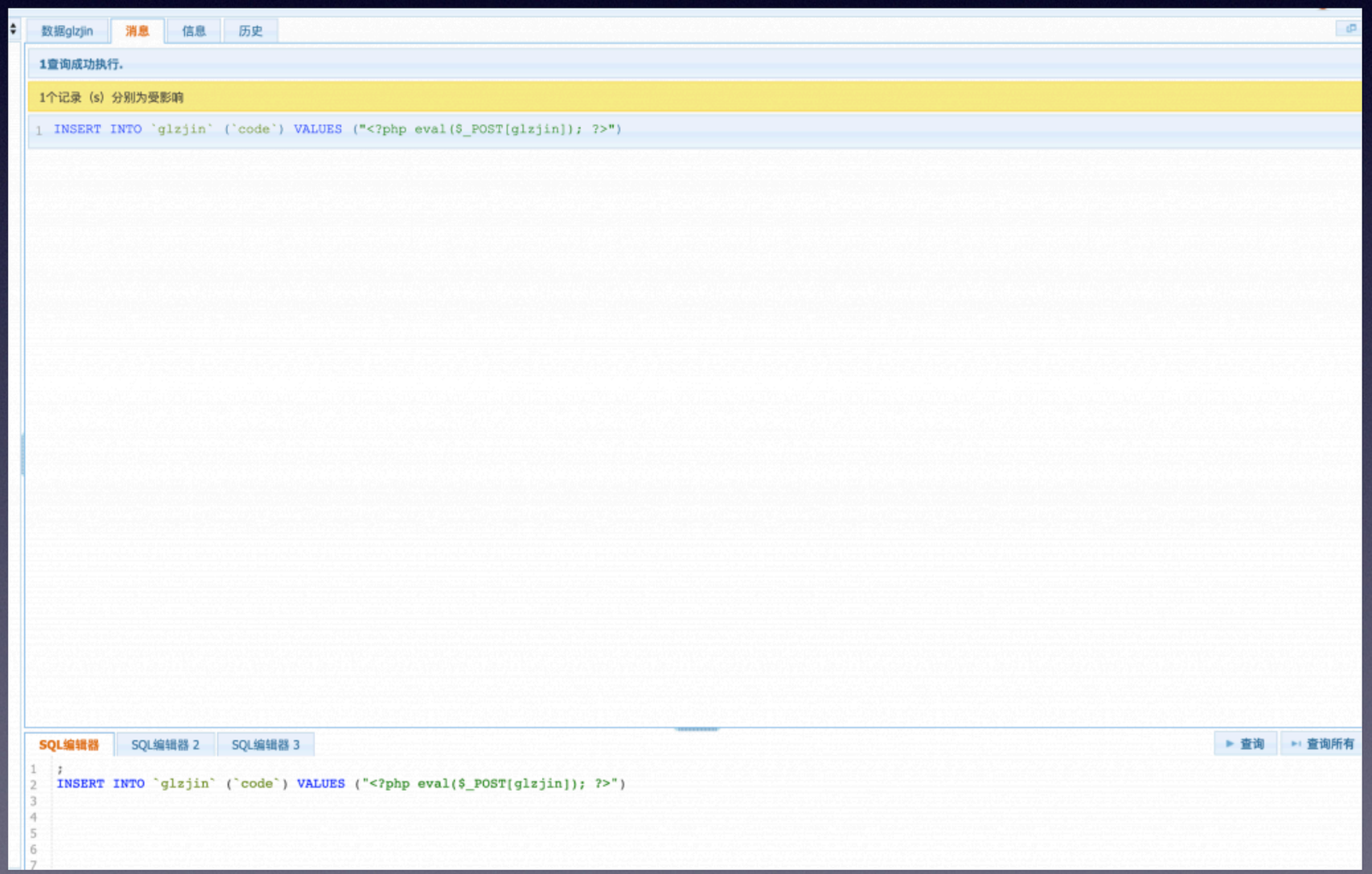
- 本题无复现环境。其实也不是文件包含，但挺有意思，也是个思路，在这里一起分享了。
- https://www.zhaoj.in/read-5479.html

StarCTF 2019-mywebsql

- https://nvd.nist.gov/vuln/detail/CVE-2019-7731

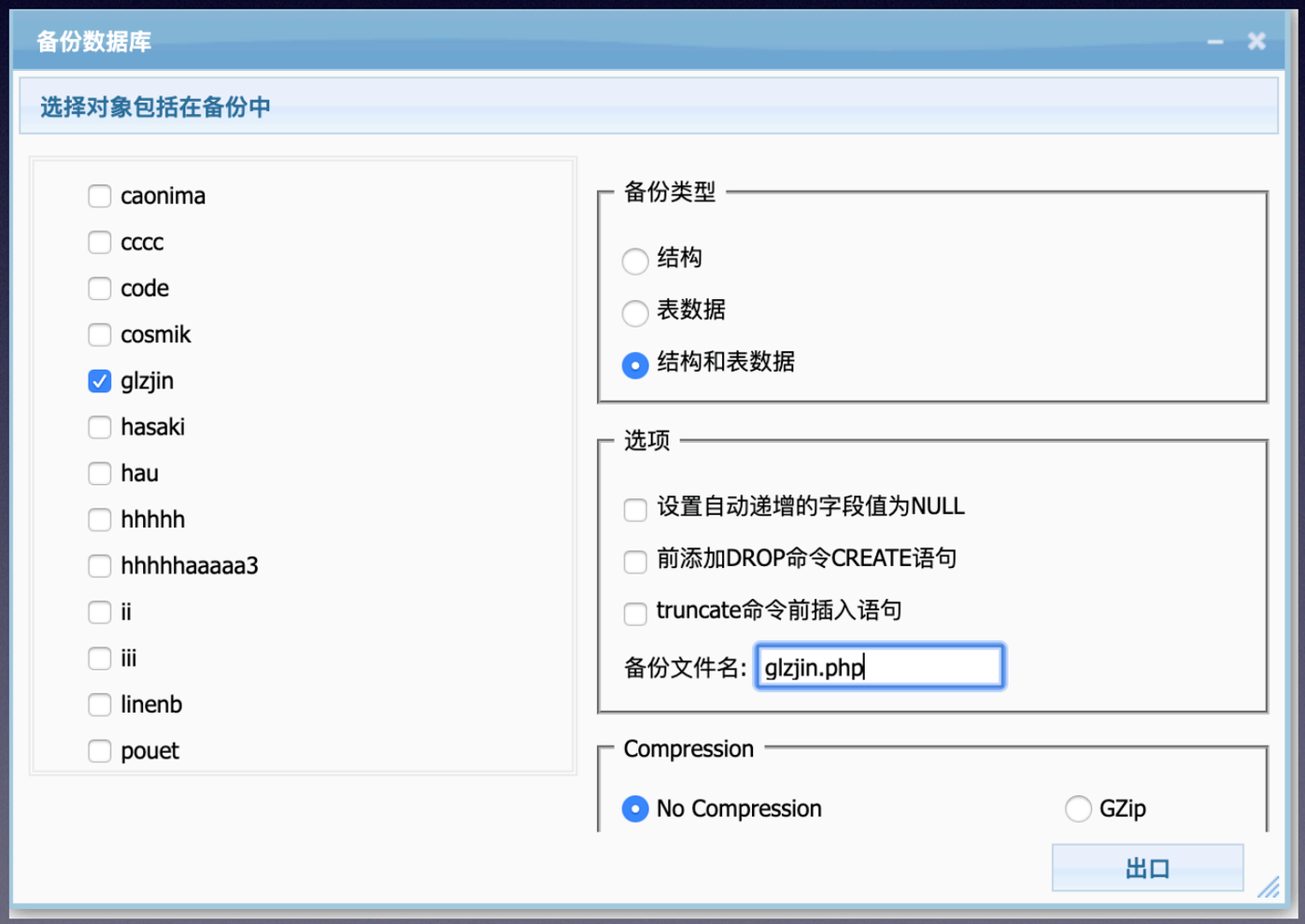
StarCTF 2019-mywebsql

- 往数据库里写 Webshell Code。



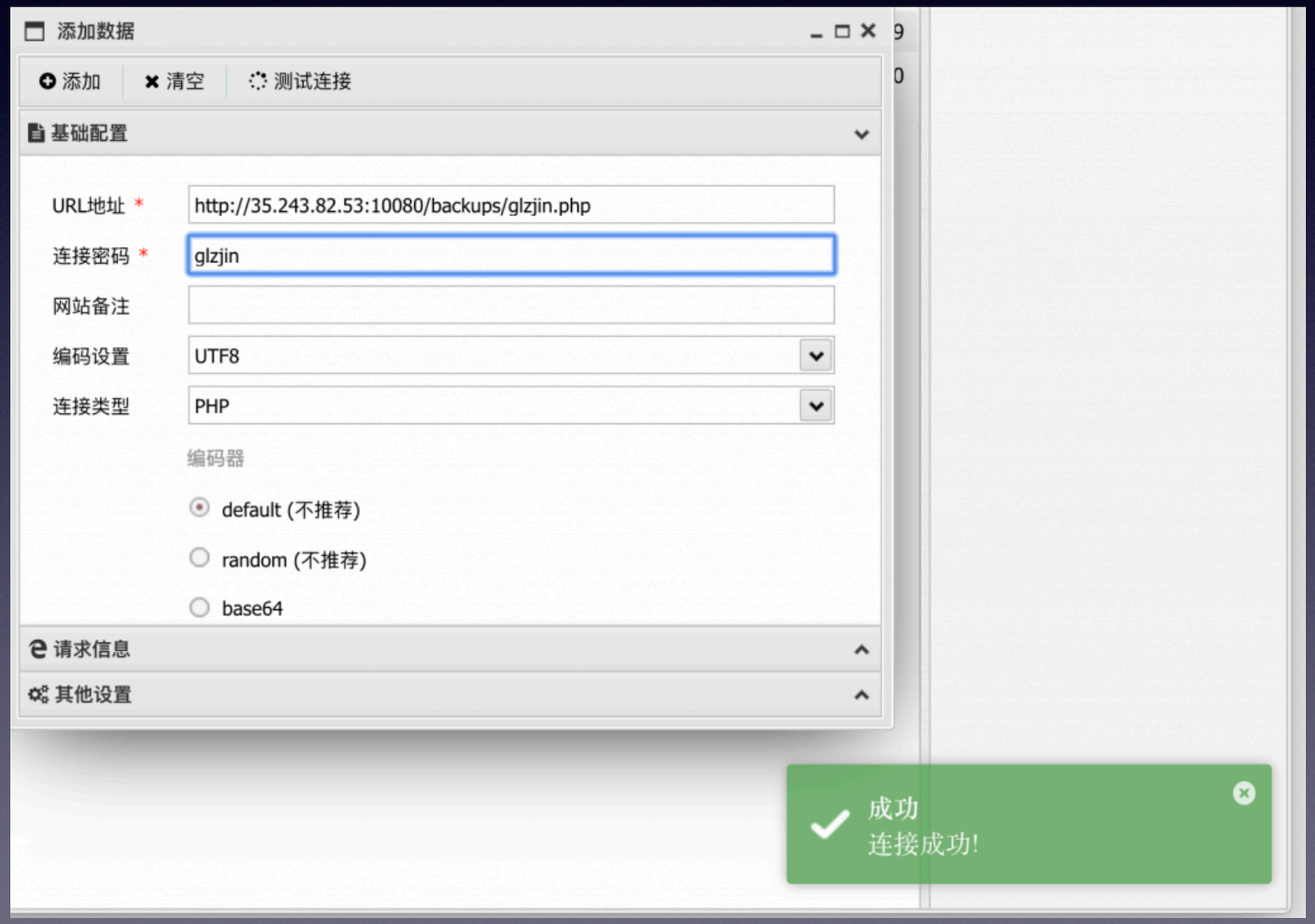
StarCTF 2019-mywebsql

- 导出备份文件。



StarCTF 2019-mywebsql

- 测试连接。



总结与练习

- 还是那句话，姿势多种多样，多练习多总结，不变应万变。
- 练习：
  - [PWNHUB 公开赛 2018]傻 fufu 的工作日