

ibos oa v4.5.5 SQL injection

SQL injection vulnerability exists in ibos oa v4.5.5

version:4.5.5

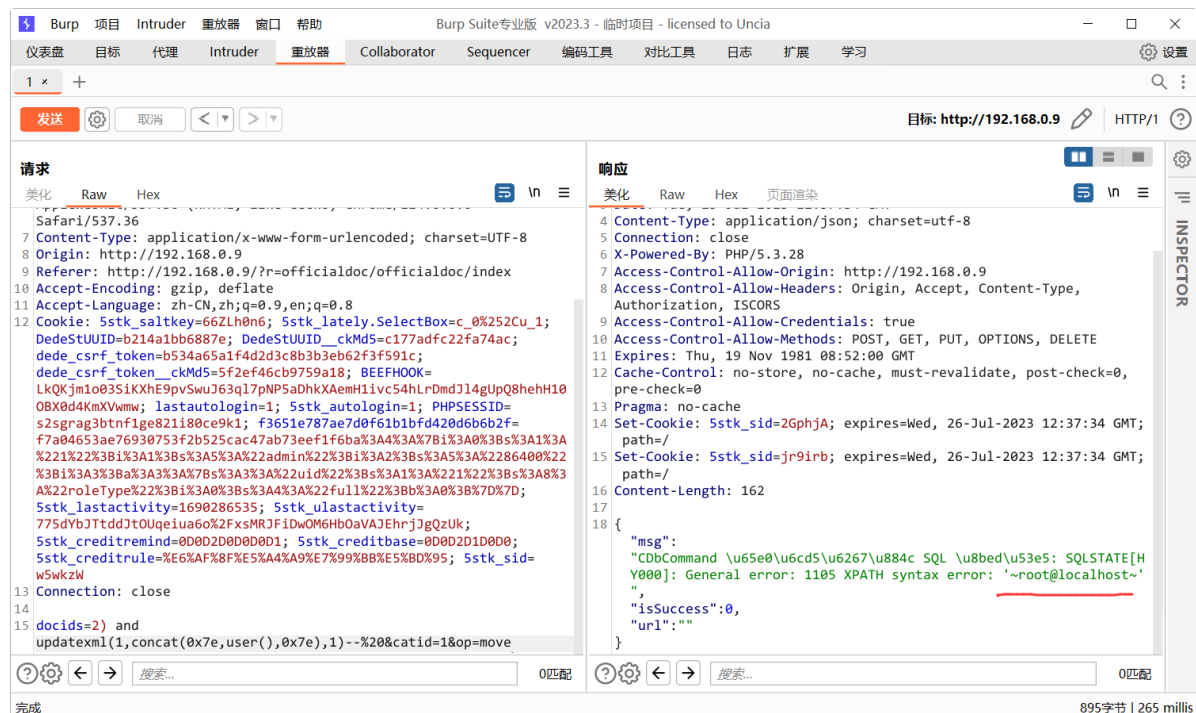
Function point: Integrated office ==> Notification Announcement



POC

Routing: r = officialdoc/officialdoc/edit

Successfully burst the user name by reporting an error injection



We can also use the sqlmap tool for testing.

Omit here

Analyze

It's routed here and it calls the `actionEdit()` method, it selects the function point by passing in the `op` parameter.



```
236
237
238
239
240 public function actionEdit()
241 {
242     $op = Env::getRequest('op');
243     $option = empty($op) ? 'default' : $op;
244     $routes = array('default', 'update', 'top', 'highLight', 'move', 'verify',
245         'back');
246     if (!in_array($option, $routes)) {
247         $this->error(Ibos::lang('Can not find the path'), $this->createUrl('officialdoc/index'));
248     }
249     if ($option == 'default') { ...
282
283     } else {
284         $this->$option();
285     }
286 }
```

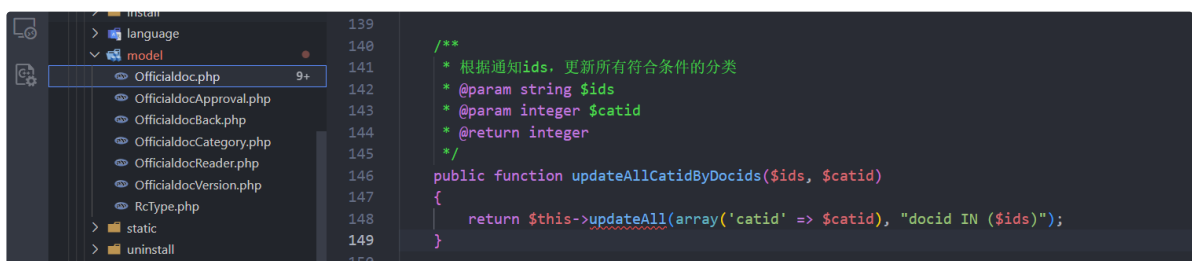
We chosen the `move` function because it has a small amount of code and simple parameters,

Two arguments `docids` and `catid` are passed in the `move()` method where `docids` is injected, bringing the values of both arguments into the `updateAllCatidByDocids()` method.



```
970
971
972
973
974
975 private function move()
976 {
977     if (Ibos::app()->request->isAjaxRequest) {
978         $docids = Env::getRequest('docids');
979         $catid = Env::getRequest('catid');
980         if (!empty($docids) && !empty($catid)) {
981             Officialdoc::model()->updateAllCatidByDocids(ltrim($docids, ','), $catid);
982             $this->ajaxReturn(array('isSuccess' => true));
983         } else {
984             $this->ajaxReturn(array('isSuccess' => false));
985         }
986     }
987 }
988 }
```

The SQL statement is executed using the `updateAll()` wrapper function



```
139
140
141
142
143
144
145
146 public function updateAllCatidByDocids($ids, $catid)
147 {
148     return $this->updateAll(array('catid' => $catid, "docid IN ($ids)");
149 }
150 }
```