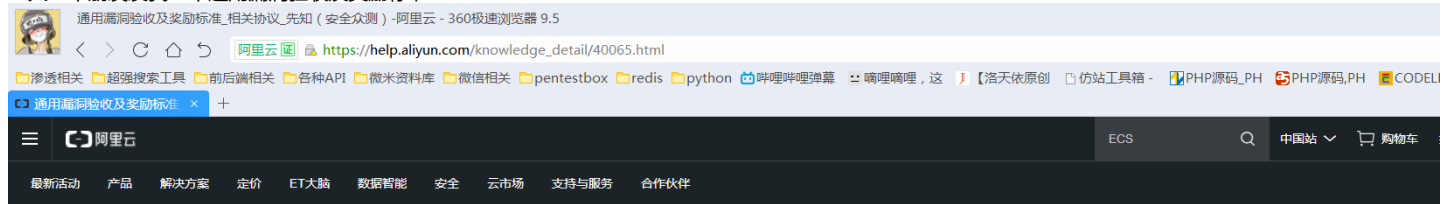


0x01 前言

一天一个朋友发我一个通用漏洞验收及奖励标准



[< 文档首页](#)

[先知 \(安全众测\)](#)

[产品简介](#)
[产品定价](#)
[快速入门](#)
[用户指南](#)
[常见问题](#)
[相关协议](#)
[联系我们](#)
[通用参考](#)

[先知 \(安全众测\) > 相关协议 > 通用漏洞验收及奖励标准](#)

[通用漏洞验收及奖励标准](#)

[更新时间: 2018-07-18 14:05:55](#)

[通用软件漏洞收集及奖励标准](#)

为了更好地保障云上用户的安全,提升安全防护能力,阿里云盾(先知)专门制定了《通用软件漏洞奖励计划》,以提供奖励的方式鼓励白帽子遵循责任的漏洞披露机制,向我们提供通用软件的安全漏洞信息。

云盾先知确认漏洞后,将按照流程向您提供现金奖励和荣誉奖励,同时将漏洞向通用软件官方提交,并向受到影响的合作伙伴共享漏洞信息。如果您发现第三方通用软件的漏洞,欢迎您向我们提交,我们会第一时间响应处理。

漏洞定义

漏洞:攻击者通过操纵某些数据,使得程序偏离设计者的逻辑,进而引发的安全问题。先知计划漏洞平台主要收集应用软件和建站系统程序漏洞。

漏洞名称

白帽子自定义漏洞名称,尽量包含漏洞关键字等信息。

如:PHPTST v1.0.0前台无限制Getshell。

收集的漏洞类型

我们关注的漏洞类型,包括:

XSS跨站;SQL注入;XXE;命令执行;文件包含;任意文件操作;权限绕过;存在后门;文件上传;逻辑漏洞;栈溢出;堆溢

[我的收藏](#)

[新手学堂](#)
[学习路径](#)

[本目录](#)

[通用软件漏洞收集及奖励标准](#)

[漏洞定义](#)

[漏洞名称](#)

[收集的漏洞类型](#)

[漏洞收集范围](#)

[评分规则](#)

[付款条件和限制](#)

[漏洞提交报告要求](#)



看着还可以,一顿突突以后,准备提交的时候发现!!!!



嗯。问题不大:)

一直以来都很少看到有比较完整的cms审计过程，所以特地记录一下自己的审计过程，希望后入门审计的人可以少走点弯路，找到自己的审计方式。

注意：文章可能会字很多很烦，因为你可以看到我一直在哪里BBBBBB。

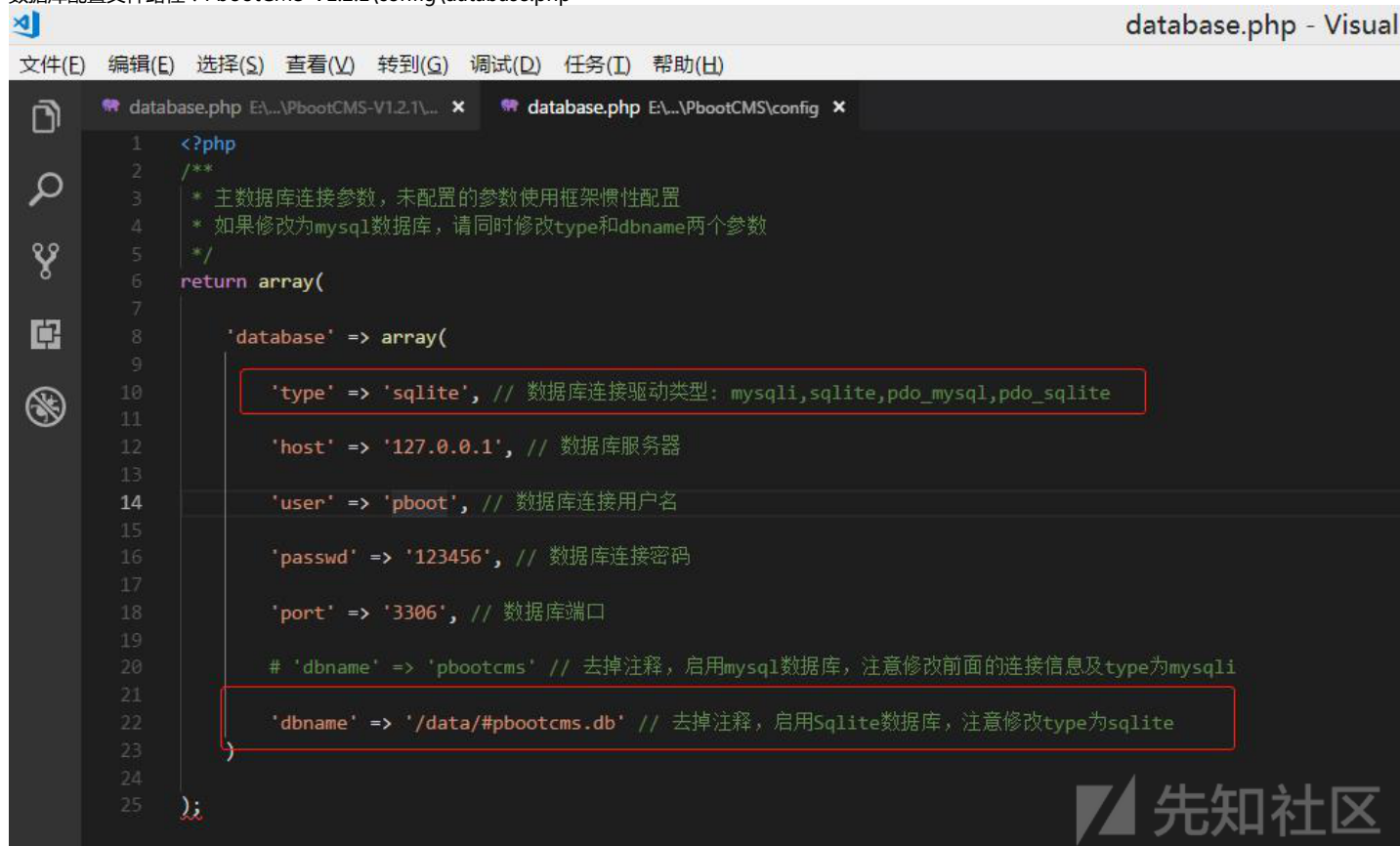
最后希望此文章可以帮助到想学习的人(°□°) /□

0x02 安装系统

这个系统很方便默认情况下，直接下载下来什么都不用做即可使用。

但是系统默认是使用 sqlite 的，我不喜欢、(´▽`)~

数据库配置文件路径：PbootCMS-V1.2.1\config\database.php



```
1 <?php
2 /**
3  * 主数据库连接参数，未配置的参数使用框架惯性配置
4  * 如果修改为mysql数据库，请同时修改type和dbname两个参数
5  */
6 return array(
7
8     'database' => array(
9
10         'type' => 'sqlite', // 数据库连接驱动类型: mysqli,sqlite,pdo_mysql,pdo_sqlite
11
12         'host' => '127.0.0.1', // 数据库服务器
13
14         'user' => 'pboot', // 数据库连接用户名
15
16         'passwd' => '123456', // 数据库连接密码
17
18         'port' => '3306', // 数据库端口
19
20         # 'dbname' => 'pbootcms' // 去掉注释，启用mysql数据库，注意修改前面的连接信息及type为mysqli
21
22         'dbname' => '/data/#pbootcms.db' // 去掉注释，启用Sqlite数据库，注意修改type为sqlite
23     )
24
25 );
```

这里我修改为mysql 数据库来跑

数据库配置文件路径：PbootCMS-V1.2.1\config\database.php

数据库sql保存路径：PbootCMS-V1.2.1\static\backup\sql\20180720164810_pbootcms.sql

然后自己创建个数据库导入即可如图

database.php -

文件(E) 编辑(E) 选择(S) 查看(V) 转到(G) 调试(D) 任务(I) 帮助(H)

database.php E:\...\PbootCMS-V1.2.1\... x database.php E:\...\PbootCMS\config

1 <?php
2 /**
3 * 主数据库连接参数，未配置的参数使用框架惯性配置
4 * 如果修改为mysql数据库，请同时修改type和dbname两个参数
5 */
6 return array(
7
8 'database' => array(
9
10 'type' => 'mysqli', // 数据库连接驱动类型: mysqli,sqlite,pdo_mysql,pdo_sqlite
11
12 'host' => '127.0.0.1', // 数据库服务器
13
14 'user' => 'root', // 数据库连接用户名
15
16 'passwd' => 'root', // 数据库连接密码
17
18 'port' => '3306', // 数据库端口
19
20 'dbname' => 'pbootcms' // 去掉注释，启用mysql数据库，注意修改前面的连接信息及type为mysqli
21)
22
23);

修改为这样既可

先知社区

然后重新打开网站即可



后台默认账户密码

□ 账户：admin

□ 密码：123456

剩下的可以查看帮助手册：PbootCMS-V1.2.1\doc\help.chm

0x03 查看网站目录结构确定基本内容

PbootCMS-V1.2.1

■ apps	■■■■
■ ■ admin	■■■■
■ ■ api	api■■
■ ■ common	■■■■

```

■ ■■ home      ■■■■
■ ■■ config    ■■■■
■ ■■ config.php ■■■■
■ ■■ database.php ■■■■■■
■ ■■ route.php  ■■■■■■■■
■ ■■ core      ■■■■
■ ■■ function  ■■■■■■
■ ■ ■■ handle.php ■■■■■1
■ ■ ■■ helper.php ■■■■■2
■ ■■ template   html■■■
■ ■■ admin.php  ■■■■■■
■ ■■ api.php    api■■■■
■ ■■ index.php  ■■■■■■

```

这里我把一些重要的地方列了出来，在初步审计的时候，可以快速了解系统

0x04 确定路由走向

经过初步的查看，可以得出路由走向。

一种是自定义路由，还有一种是mvc的路由

0x04.1 必须自定义路由才能访问的类

查看路由文件：PbootCMS-V1.2.1\apps\common\route.php

```

route.php - PbootCMS-V1.2.1 - Visual Studio Code
文件(E) 编辑(E) 选择(S) 查看(V) 转到(G) 调试(D) 任务(I) 帮助(H)

资源管理器
  打开的编辑器
    index.php
    route.php apps\common
    AboutController.php apps\home\control... 2
    SitemapController.php apps\home\control... 1
  PBOOTCMS-V1.2.1
    apps
      admin
      api
      common
        AdminController.php
        AdminModel.php
        ApiController.php
        function.php
        HomeController.php
        route.php 1
        version.php
      home
        controller
          AboutController.php 2
          ContentController.php
          DoController.php
          FormController.php
          IndexController.php
          ListController.php
          MessageController.php
          ParserController.php
          SearchController.php

route.php
// =====管理端路由=====
// 系统模块路由
'admin/Area' => 'admin/system.Area',
'admin/Menu' => 'admin/system.Menu',
'admin/Role' => 'admin/system.Role',
'admin/User' => 'admin/system.User',
'admin/Type' => 'admin/system.Type',
'admin/Syslog' => 'admin/system.Syslog',
'admin/Database' => 'admin/system.Database',
'admin/Config' => 'admin/system.Config',
'admin/Upgrade' => 'admin/system.Upgrade',

// 内容发布模块路由
'admin/Site' => 'admin/content.Site',
'admin/Company' => 'admin/content.Company',
'admin/Label' => 'admin/content.Label',
'admin/Model' => 'admin/content.Model',
'admin/ExtField' => 'admin/content.ExtField',
'admin/ContentSort' => 'admin/content.ContentSort',
'admin/Content' => 'admin/content.Content',
'admin/Single' => 'admin/content.Single',
'admin/Message' => 'admin/content.Message',
'admin/Slide' => 'admin/content.Slide',
'admin/Link' => 'admin/content.Link',
'admin/Form' => 'admin/content.Form',

// =====前端路由=====为前端美观，使用了小写URL，此处也用小写
'home/index' => 'home/index/index',
'home/list' => 'home/list/index/scode',
'home/about' => 'home/about/index/scode',
'home/content' => 'home/content/index/id',

```

例如：

<http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/about/1>

因为他的这个文件在系统的自定义路由上所以上面的路由解析以后就是

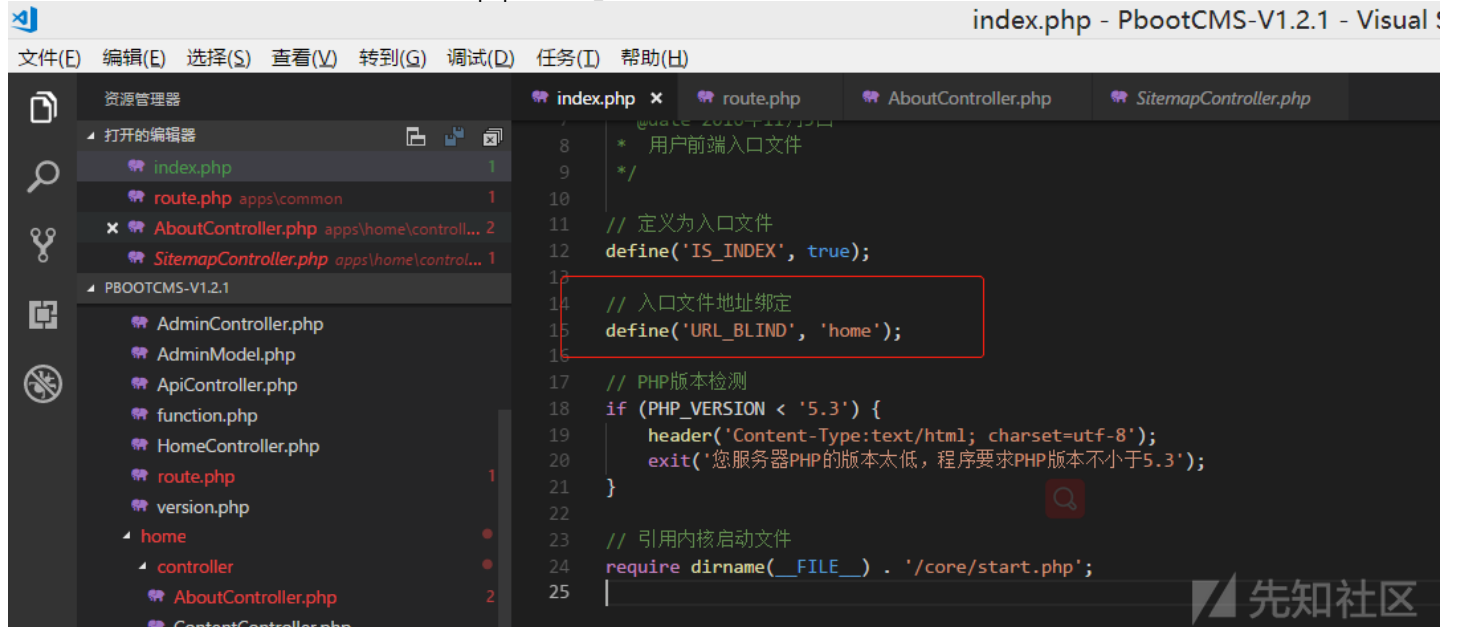
路由：about/1 = home/about/index/scode

文件：PbootCMS-V1.2.1\apps\home\controller\AboutController.php

方法：index

参数：scode

那个 home 是由 对应的入口文件，例如文中的index.php中的URL_BLIND



```
index.php - PbootCMS-V1.2.1 - Visual Studio Code
文件(E) 编辑(E) 选择(S) 查看(V) 转到(G) 调试(D) 任务(T) 帮助(H)

资源管理器
  打开的编辑器
    index.php
    route.php apps\common
    AboutController.php apps\home\control... 2
    SitemapController.php apps\home\control... 1
  PBOOTCMS-V1.2.1
    AdminController.php
    AdminModel.php
    ApiController.php
    function.php
    HomeController.php
    route.php
    version.php
    home
      controller
        AboutController.php
        ContentController.php

index.php
7  * 用户前端入口文件
8  */
9
10 // 定义为入口文件
11 define('IS_INDEX', true);
12
13 // 入口文件地址绑定
14 define('URL_BIND', 'home');
15
16 // PHP版本检测
17 if (PHP_VERSION < '5.3') {
18     header('Content-Type:text/html; charset=utf-8');
19     exit('您服务器PHP的版本太低，程序要求PHP版本不小于5.3');
20 }
21
22 // 引用内核启动文件
23 require dirname(__FILE__) . '/core/start.php';
24
25
```

0x04.2 普通的mvc地址

对于不在自定义路由中的就可以按照普通的mvc模式来访问了

例如：

<http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Message/add>

路径：apps\home\controller\MessageController.php

方法：add

点击收藏 | 1 关注 | 3

[上一篇：nodejs应用中的权限绕过漏洞一...](#) [下一篇：CVE-2018-18921—PH...](#)

1. 3 条回复



[sera](#) 2018-12-17 22:16:09

卧槽我今天才知道这个奖励标准，错亿！！！！

0 回复Ta



于龙gll 2019-09-09 11:01:39

我根据提示修改了,但是pbootcms这个数据库没有,从哪里下载来的

0 回复Ta



于龙gll 2019-09-09 11:03:01

```
6 return array(  
7  
8     'database' => array(  
9  
10         //'type' => 'sqlite', // 数据库连接驱动类型: mysqli, sqlite, pdo_mysql, pdo_sqlite  
11         'type' => 'mysqli', // 数据库连接驱动类型: mysqli, sqlite, pdo_mysql, pdo_sqlite  
12  
13         'host' => '127.0.0.1', // 数据库服务器  
14  
15         //'user' => 'pboot', // 数据库连接用户名  
16         'user' => 'root', // 数据库连接用户名  
17  
18         //'passwd' => '123456', // 数据库连接密码  
19         'passwd' => 'root', // 数据库连接密码  
20  
21         'port' => '3306', // 数据库端口  
22  
23         'dbname' => 'pbootcms', // 去掉注释, 启用mysqli数据库, 注意修改前面的连接信息及type为mysqli  
24  
25         //'dbname' => '/data/#8eaa09e8f7d4254465a12d1f9b144135.db' // 去掉注释, 启用Sqlite数据库, 注意修改type为sqlite  
26     )  
27 );  
28  
29 ;
```



执行SQL发生错误! 错误: Table 'pbootcms.ay_site' doesn't exist, 语句: SELECT * FROM ay_site WHERE(icode='cn') LIMIT 1

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)