

登陆

1.信息收集 (参考lsrc列表列出来的)
都有现成脚本

数据展示

监控域名或IP

主机端口

域名资产

网络资产

排除资产

网页内容

配置信息

1. 项目大厅

项目大厅

我的项目

2.渗透工具

1.邮件钓鱼方案

文章单页

2.WEB免杀

3.自动免杀

3.漏洞探测

1.Awvs13漏洞扫描

添加任务。显示任务。有现成的接口

2.Nessus漏洞扫描

添加任务。显示任务。有现成的接口

Screenshot of a web application security tool interface showing a list of plugins on the left, a configuration panel in the middle, and a response preview on the right.

Plugin List (Left):

- ecshop_sqlinject_3
- ecshop_sqlinject_test
- ii7.6_parsing_test_new
- info_leak_ftp
- info_leak_git
- info_leak_svn
- info_leak_webxml
- info_leak_workspace
- MacOS_v8_getshell
- metinfo_sql_2
- phpcms_auth_key_leak
- phpcms_file_red
- phpcms_user_login_sqlinject
- phpcms_video_for_ck_sqlinject
- phpcms_vote_tag_sqlinject
- phpweb_admin
- phpweb_new_sq
- phpweb_sqlinject
- QiboCMS_v7_file_down
- QiboCMS_v7_test
- seacms_2
- sitedfactory_inject
- southid_sql_1
- southid_sql_2
- southid_sql_cookie_1
- southid_sql_cookie_2
- topsec_change_lab_file_include
- URP通杀第二弹-任意文件读取
- WordPress_download
- WordPress_sql_2
- WordPress_getshell
- zhanzhangquan取文章地址

Configuration Panel (Middle):

测试网址:

插件名称:

1. 检测路径

检测路径:

判断规则: ☐ 状态码 ☐ 禁止跳转 ☒ 急速请求 ☒ 异步请求

2. 模拟请求

请求方式: 请求编码: ☐ 禁止跳转 ☐ 上传协议

请求路径:

判断规则: ☒ 状态码 ☒ 判断包含文本 ☐ 判断排除文本

PHP Version:

3. 处理结果

☐ 过滤html标签 ☐ 结果(正则匹配)

☐ 结果(前后截取) 前面: 后面:

☒ 检测域名+ ☐ 结果(处理后)+

☐ 包含文本不存在!

Response Preview (Right):

```
<!DOCTYPE html>
<!--STATUS OK-->
<html>
<head>
<meta http-equiv="X-UA-Compatible"
content="IE=edge,chrome=1">
<meta http-equiv="content-type"
content="text/html; charset=utf-8">
<meta content="always" name="referrer">
<script
src="https://ssl.bdstatic.com/5eWbjg8AAUfa2zgoT3K/r/www/mocach
e/ingdata/aeErrorRec.js"></script>
<title>页面不存在_百度搜索</title>
<style data-for="result">
body {color: #333; background: #fff; padding: 0;
margin: 0; position: relative; min-width: 700px; font-family:
arial; font-size: 12px;}
p, form, ol, ul, li, dl, dt, dd, h3 {margin: 0;
padding: 0; list-style: none;}
input {padding-top: 0; padding-bottom: 0; width: 100%;
border: 1px solid #ccc; border-radius: 3px; box-sizing:
border-box; outline: none;}
img {border: none;}
.logo {width: 117px; height: 38px; cursor: pointer;}
#wrapper {zoom: 1;}
```

4.自主POC

其实就是请求然后判断返回包存在某个字符

左边是插件列表, 中间是插件定制面板. 右面显示返回数据包

5.APT框架系统 (每个都是文章列表)

12个文章列表 页

6.交流区

类似于留言板。所有用户都可以留言，并且可以评价别人的留言，如果有现成的，那就用现成的套进去

7.账户设置

交流区-我的消息

个人资料

密码修改

网站管理 (管理员权限才可以看到这个)

29