



47 Ferramentas Hackers

Bem-vindo ao "Hackers Toolbox", onde desvendamos o intrigante mundo de 47 ferramentas digitais essenciais. Este eBook é mais do que um simples guia; é um convite para explorar o vasto arsenal que hackers éticos, analistas de segurança e entusiastas da cibersegurança utilizam para compreender, proteger e, por vezes, desafiar as fronteiras do ciberespaço.

Introdução

1 Exploração Abrangente

Descobriremos ferramentas que vão além da simples defesa cibernética, explorando sentinelas que protegem, sondas que vasculham, iscas que testam e lentes que revelam.

2 Guia Detalhado

Este é um guia abrangente que percorre desde as técnicas fundamentais de segurança até as artimanhas de phishers e os métodos de busca por informações.

3 Jornada Educativa

Prepare-se para uma jornada fascinante e educativa, desvendando o propósito, o uso ético e as nuances destas 47 ferramentas.



Observação Importante

Sistemas Operacionais Recomendados

Para obter o máximo proveito dessas ferramentas e garantir uma utilização eficaz e segura, recomenda-se empregar um sistema operacional adequado, como o Kali Linux ou o Parrot. Ambas as distribuições são especialmente projetadas para atividades de segurança, oferecendo ambientes otimizados e uma variedade de ferramentas pré-instaladas para testes éticos.

Compatibilidade e Disponibilidade

As ferramentas apresentadas podem ser utilizadas em diversos sistemas operacionais, não se limitando ao Kali Linux. Muitas delas são desenvolvidas para serem compatíveis com sistemas Windows, macOS e Linux. Algumas podem ser encontradas dentro do próprio Kali Linux, enquanto outras estão disponíveis em seus respectivos sites oficiais ou no GitHub.

Ferramenta 1 - Burp Suite



1

Scanner de Aplicações Web

Utilize o scanner automático para identificar vulnerabilidades comuns, como injeções SQL, cross-site scripting (XSS) e outras falhas de segurança.

2

Proxy Interativo

Capture e modifique solicitações HTTP entre o navegador e o servidor para analisar e modificar o tráfego em tempo real.

3

Spider e Crawler

Descubra e mapeie automaticamente todas as páginas e funcionalidades de um aplicativo da web.

4

Repeater e Intruder

Repita solicitações para testar vulnerabilidades manualmente e realize ataques de força bruta, fuzzing e testes de carga.

Ferramenta 2 - Nmap



- 1
- 2
- 3
- 4

Varredura de Portas

Identifique portas abertas em hosts para avaliar possíveis pontos de entrada.

Descoberta de Hosts

Localize dispositivos ativos em uma rede para mapear a infraestrutura.

Detectção de Serviços

Identifique os serviços em execução nas portas abertas para avaliar a superfície de ataque.

Scripting Avançado

Use scripts Nmap ou crie os seus para automatizar tarefas específicas de varredura.

Fitoneser/Oeeoe: Car (eraton Cnpinconi)
FizennnenrOnján exarPo88ge Ennocey:
BitnennendOrrrMort: E88eres
Eithennechsteter hñderngon;
Fitnerneecjas8n80Eur p6u

SIM Clotidianos

Genhoir Moddenstere

► Orpio Approuast

Attun, loune — Scèppli — effes "Cpe Ghelenson")
Ditum Scat-Catou — Scatet Scatdrenz - 2000 anndis) / Dethrenz (Ust-6780)

Ferramenta 3 - Metasploit

Exploração de Vulnerabilidades

Utilize exploits existentes para testar sistemas em busca de vulnerabilidades conhecidas.

Desenvolvimento de Exploits

Crie exploits personalizados para vulnerabilidades específicas.

Pós-Exploração

Ganhe acesso e controle a sistemas comprometidos para avaliar o impacto de uma exploração.

Payloads Personalizados

Desenvolva payloads específicos para contornar defesas e atingir objetivos.

Stout
SpacCooer, sennástyntctunt;
S00. S2ASS Jtpren#ton ipieeprotung)
) Rnla Sovw}

Stepmod
Step bid
}

if: Lf S00 Cceve-indleepctrlWSt;798;
fprecertintion. itffststouer;pyat}

Ferramenta 4 - Sqlmap

Identificação de Vulnerabilidades

Utilize a funcionalidade de detecção automática para identificar possíveis vulnerabilidades de injeção de SQL em um aplicativo.

Testes Avançados

Realize testes avançados, como exfiltração de dados, execução de comandos no sistema operacional, entre outros.

1

2

3

4

Exploração de Falhas

Execute ataques de injeção de SQL para explorar e extrair informações do banco de dados subjacente.

Suporte a Diversos Bancos de Dados

O SQLMap oferece suporte para vários bancos de dados, incluindo MySQL, PostgreSQL, Oracle, Microsoft SQL Server, entre outros.

Ferramenta 5 - Dirb



Identificação de Diretórios Ocultos

O Dirb varre um site em busca de diretórios que podem não ser facilmente acessíveis, ajudando a revelar áreas escondidas.



Enumeração de Recursos

Permite aos usuários identificar recursos, scripts e páginas que podem não ser vinculados diretamente, mas que ainda são acessíveis.

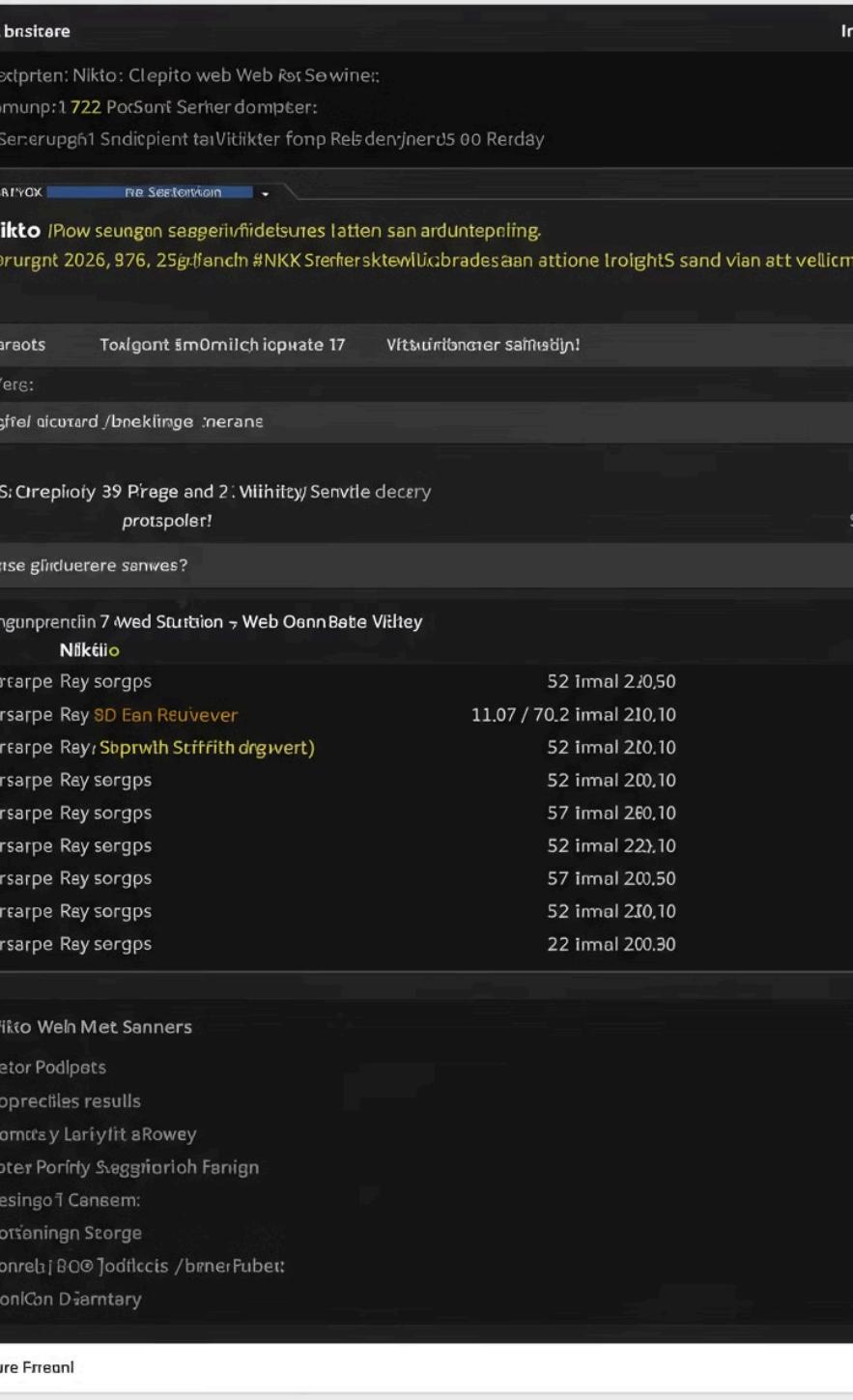


Força Bruta

Pode ser configurado para realizar ataques de força bruta em diretórios protegidos por senha.

Loyel Limenation

Title	New Enumeration	Name	Nationw	Name 24	Content
Por Fian	New Mection	Counter Profecion...	Navie-11	Coutadez.206Z.d6	
20211/2018-18	New Met Files	Cestiver Profescon...	Navie-14	Cmayula22087.d4	
20217/2018-15	New Files Files	Contwer Profescon...	Navie-28	Cmayula22053.d4	
Time	Uls				
20211/2018-16	Curts	Nathew	Navie-12	Dector..	
20211/2018-18	New Files Files	Cestiver Prolkex	Navie-14	Cmayula22052.d4	
20217/2018-18	New Mection...	Cestiver Profescon...	Navie-16	Cmayula22067.d4	
20211/2018-18	New Mestlora..	Tonlertion			
20211/2018-18	New Mection...	Seaterdaye	Navie-17	Cmayula22083.d4	
20211/2018-18	Juli.16				
20211/2018-18	Vde.18				
Time	Nav.11				
Juate, 2028 mestion.	Nux.1				
20217/2018-11	Jue.12				
20217/2018-18	Jule.10				
20211/2016-19	Jue.18				



Ferramenta 6 - Nikto

1

Varredura de Vulnerabilidades

O Nikto realiza uma varredura automatizada em servidores web em busca de vulnerabilidades comuns, como configurações incorretas, scripts desatualizados e outras falhas de segurança.

2

Identificação de Itens Suspeitos

Além de procurar por vulnerabilidades, o Nikto também identifica itens suspeitos no servidor, como diretórios protegidos por senha, scripts CGI e informações de servidor expostas.

3

Supor te a SSL

Oferece suporte a conexões SSL/TLS, permitindo a análise de servidores web seguros.

4

Relatórios Detalhados

Gera relatórios detalhados sobre as descobertas, facilitando a compreensão e a correção das vulnerabilidades identificadas.

The screenshot shows the Acunetix Web Vulnerability Scanner interface. At the top, there's a navigation bar with tabs like 'Home', 'Scans', 'Reports', and 'Logs'. Below the navigation is a search bar and a 'Run Scan' button. The main area is titled 'Website Security Results' and displays a table of vulnerabilities. The table has columns for 'Vulnerability Type', 'Severity', 'Description', 'Location', and 'Recommendation'. A red warning icon is visible next to some rows. On the left side, there's a sidebar with sections for 'Recent Reports' and 'Recent Scans'. At the bottom, there's a footer with links like 'Help & Support', 'Acunetix News', and 'Contact Us'.

Ferramenta 7 - Acunetix



Varredura Automática

O Acunetix realiza varreduras automatizadas em aplicações web em busca de uma ampla variedade de vulnerabilidades, incluindo injeção SQL, cross-site scripting (XSS), e muitas outras.

Varredura de DeepLinks

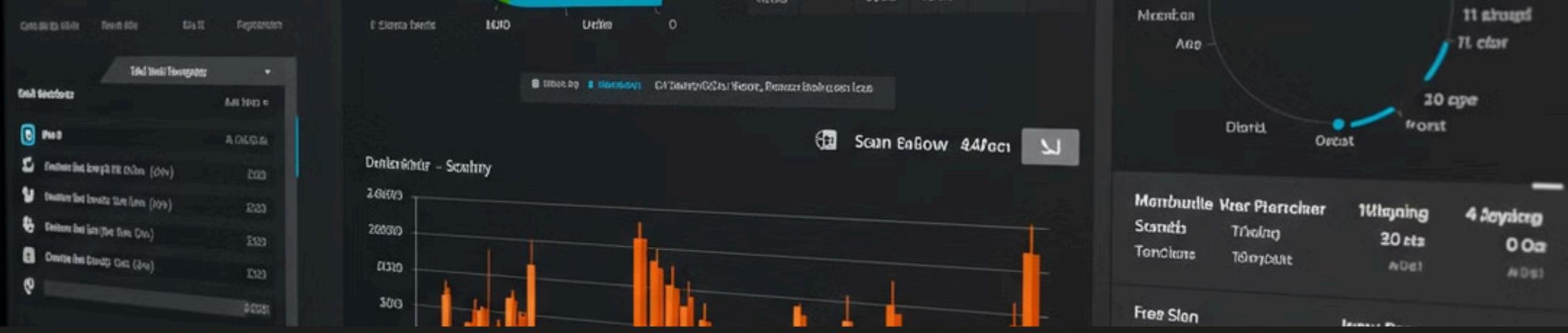
Além da análise superficial, o Acunetix também explora profundamente os links internos e externos da aplicação, identificando possíveis vetores de ataque.

Gerador de Relatórios

Gera relatórios detalhados sobre as vulnerabilidades identificadas, ajudando as equipes de desenvolvimento e segurança a priorizar e corrigir as falhas.

Scanning Incremental

Permite a execução de varreduras incrementais, ajudando a monitorar continuamente a segurança da aplicação e detectar novas vulnerabilidades introduzidas durante o desenvolvimento.



Ferramenta 8 - Nessus

Varreduras de Vulnerabilidades

O Nessus realiza varreduras abrangentes em sistemas e redes, identificando possíveis pontos fracos que podem ser explorados por atacantes.

Compliance Checks

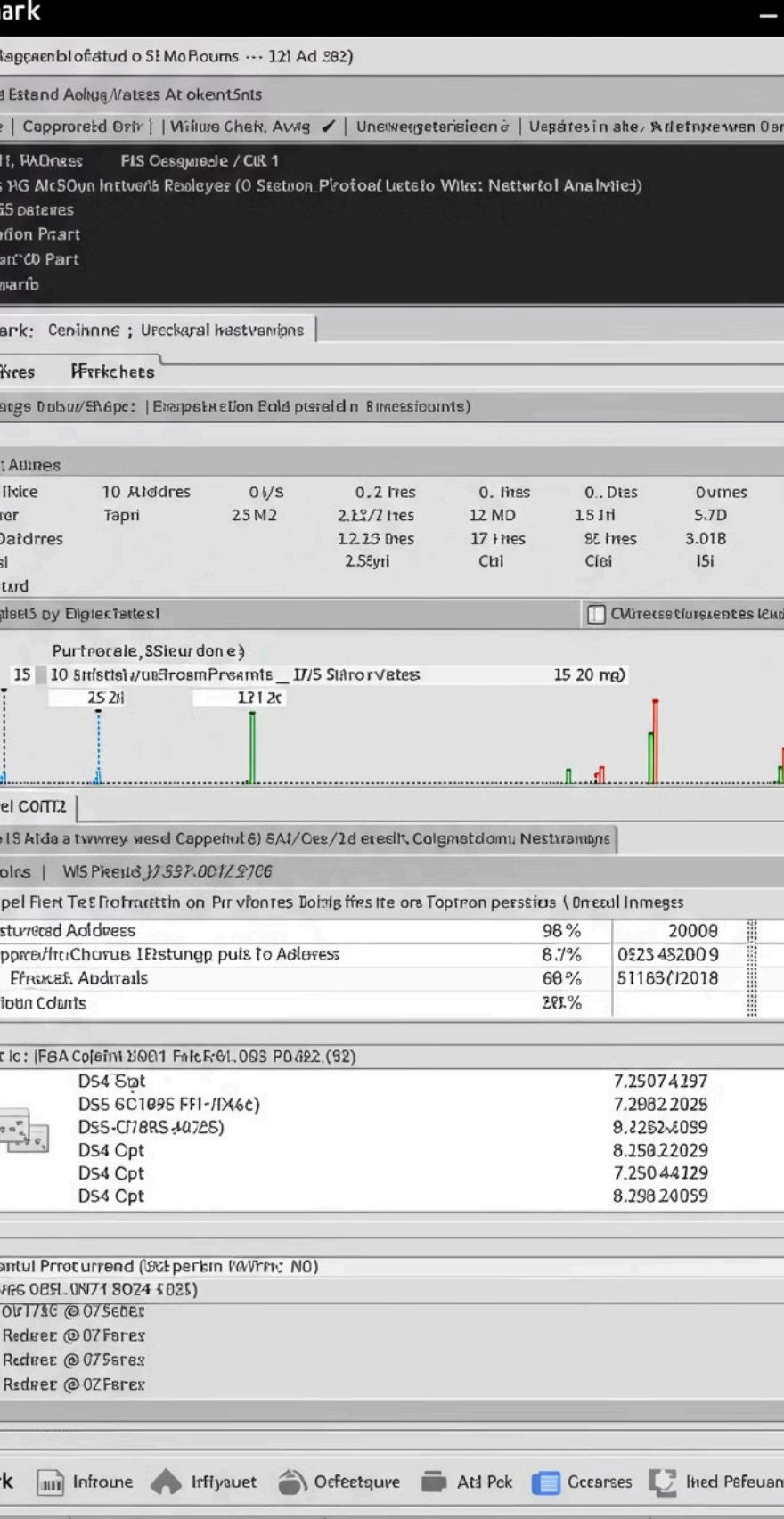
Além de vulnerabilidades, o Nessus verifica a conformidade com padrões de segurança específicos, ajudando as organizações a atender a requisitos regulatórios.

Varreduras Programadas

Permite a programação de varreduras automáticas em horários específicos, garantindo a detecção contínua de ameaças.

Análise de Risco

Classifica as vulnerabilidades detectadas com base na gravidade, impacto e facilidade de exploração, ajudando a priorizar ações corretivas.



Ferramenta 9 - Wireshark

1

Captura de Pacotes em Tempo Real

Wireshark permite capturar e analisar pacotes em tempo real, oferecendo uma visão detalhada das comunicações de rede.

2

Suporte a Diversos Protocolos

Reconhece e decodifica uma ampla gama de protocolos de rede, facilitando a análise de diferentes tipos de tráfego.

3

Filtros Avançados

Permite aplicar filtros para concentrar-se em pacotes específicos, simplificando a análise e resolução de problemas.

4

Visualização Gráfica

Apresenta dados em formatos visuais, como gráficos de fluxo, facilitando a compreensão das interações de rede.

Ferramenta 10 - XSSStrike



Detectção Automática de XSS

O XSSStrike utiliza técnicas avançadas para identificar automaticamente possíveis vulnerabilidades de XSS em aplicações da web.



Variedade de Payloads

Oferece uma ampla gama de payloads (cargas úteis) para testar e explorar diferentes formas de XSS, incluindo ataques persistentes e refletidos.



Relatórios Detalhados

Gera relatórios detalhados sobre as vulnerabilidades encontradas, facilitando a compreensão e a correção por parte dos desenvolvedores.

Strike

XSS Strike

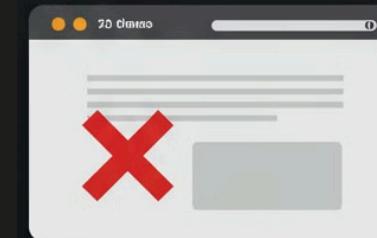
Clonesits Nance Sterit Adoyeyow smod Reonitairis imolke

Jponity Senut

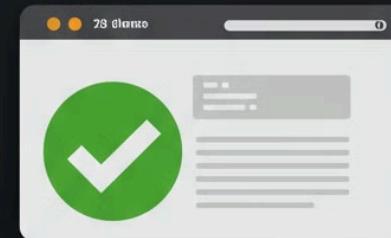


MEED Pipm

Vererte Result?



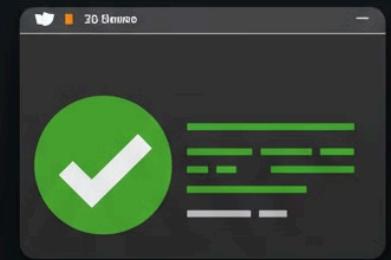
Veilliakle



Uriobubeiity Saan Resultt



Whobedlicy & Result



Cecrcrectey Result

Ferramenta 11 - Recon-**ng**



1

Módulos de Fontes Diversas

O Recon-**ng** possui uma extensa biblioteca de módulos que abrangem várias fontes de informações, como motores de busca, redes sociais, serviços de DNS, entre outros.

3

Reconhecimento Passivo e Ativo

Oferece a capacidade de realizar tanto reconhecimento passivo, onde se coleta informações sem interagir diretamente com o alvo, quanto reconhecimento ativo, que envolve interações mais diretas.

2

Integração com APIs

Permite a integração com APIs públicas e privadas para enriquecer os dados coletados e obter informações específicas de fontes confiáveis.

4

Interface de Linha de Comando (CLI)

Possui uma CLI intuitiva que facilita a configuração de módulos, execução de tarefas e análise de resultados.

Ferramenta 12 - Findomain



1 Enumeração de Subdomínios

O Findomain executa uma busca ampla para encontrar subdomínios associados a um domínio específico.

2 Rápido e Eficiente

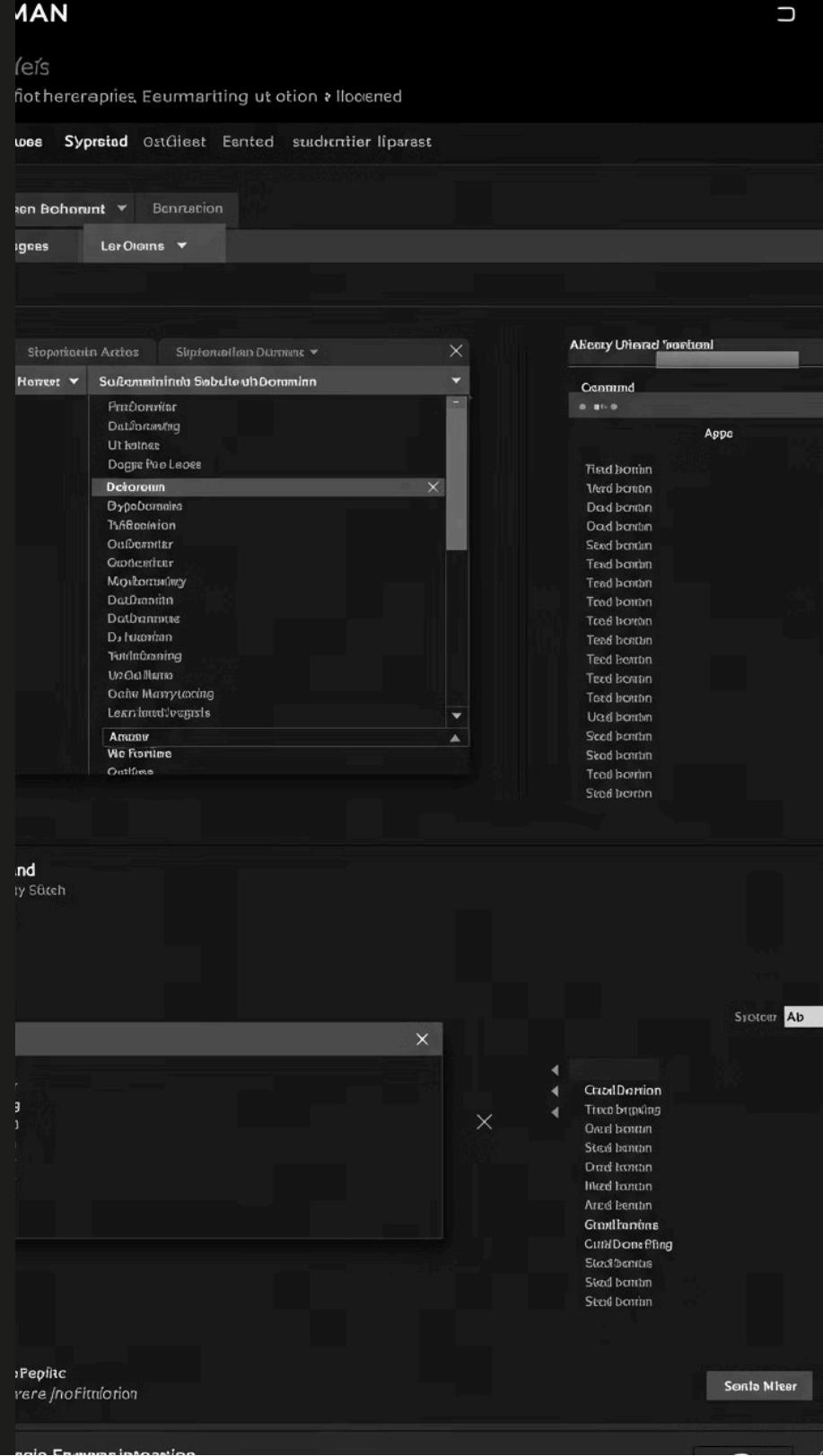
Projetado para ser rápido e eficiente, o Findomain realiza pesquisas de subdomínios de maneira ágil, fornecendo resultados em um curto espaço de tempo.

3 Saída Estruturada

Apresenta os resultados em um formato estruturado, facilitando a análise e a integração com outras ferramentas e scripts.

4 Suporte a Lista de Domínios

Permite a enumeração de subdomínios para vários domínios, possibilitando a análise de uma ampla gama de alvos.



Ferramenta 13 - WPScan

Identificação de Versões do WordPress

O WPScan pode identificar a versão específica do WordPress em execução, permitindo que os usuários saibam se estão usando versões desatualizadas e vulneráveis.

Detecção de Temas e Plugins Vulneráveis

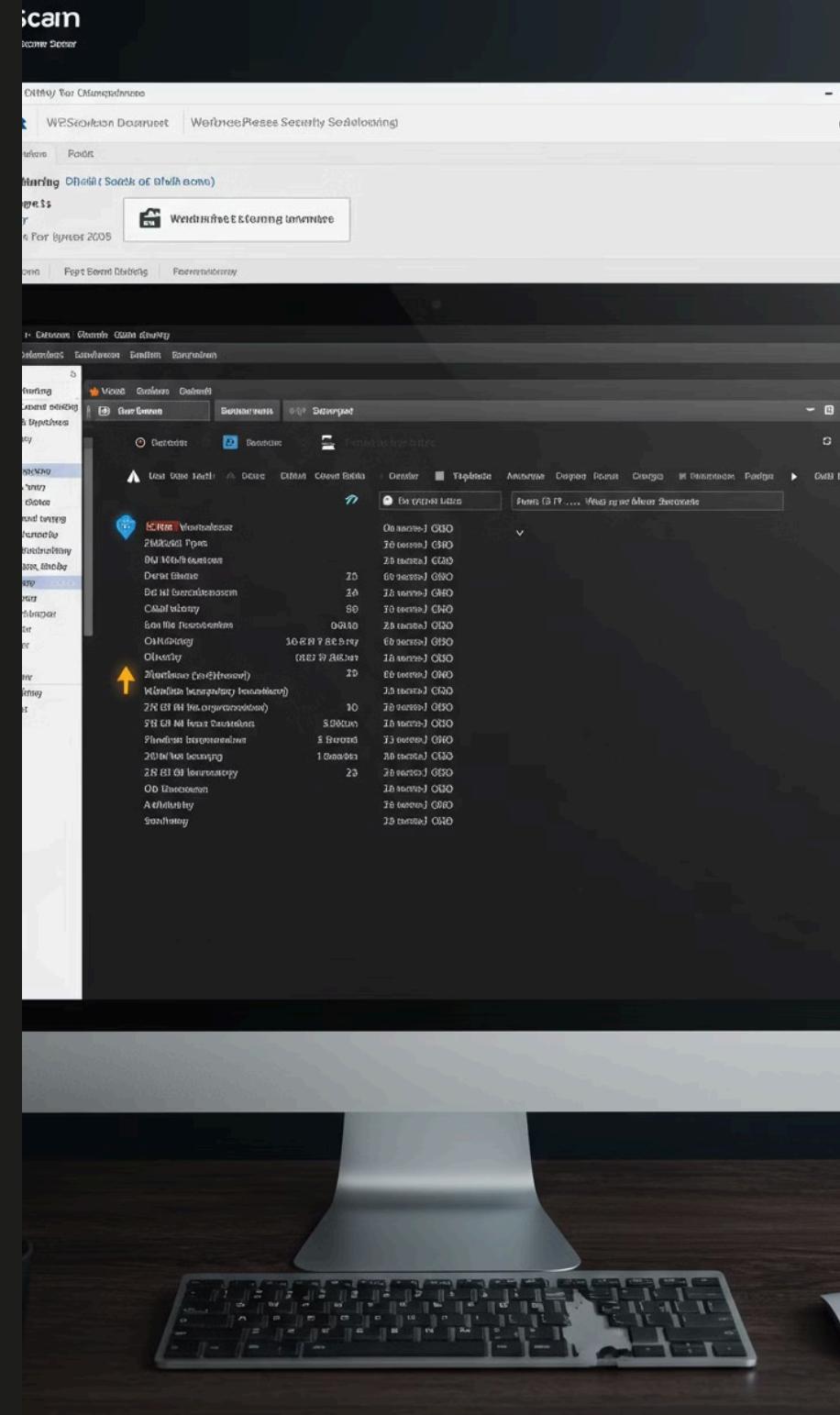
Analisa os temas e plugins instalados, alertando sobre possíveis vulnerabilidades conhecidas ou desatualizações que podem ser exploradas por atacantes.

Força Bruta de Credenciais

Oferece recursos de força bruta para testar a robustez das credenciais de acesso ao WordPress.

Análise de Configurações de Segurança

Verifica as configurações de segurança do WordPress, identificando potenciais problemas de configuração que podem levar a vulnerabilidades.



Ferramenta 14 - Hydra

1

Suporte a Diversos Protocolos

O Hydra suporta uma ampla gama de protocolos de autenticação, incluindo SSH, FTP, HTTP, HTTPS, MySQL, PostgreSQL, entre outros.

2

Ataques de Dicionário e Força Bruta

Permite realizar ataques de dicionário, ataques de força bruta e combinações personalizadas para testar a resistência das credenciais.

3

Multithreading

Utiliza multithreading para otimizar o desempenho, possibilitando a realização rápida de tentativas de autenticação.

4

Integração com Outras Ferramentas

Pode ser integrado a outros frameworks e ferramentas de teste de penetração, como o Metasploit.



The screenshot shows the ffuf tool's user interface. At the top, there's a navigation bar with tabs like 'Discover', 'Findings', 'Access Scan', 'Scan To Start', and 'Logout'. Below the navigation is a toolbar with buttons for 'Analyze & Sort', 'Starts', 'Anset', and 'Inthort'. A large central window is titled 'Discovery Scan' and contains sections for 'Discovery Stunts' (listing 'DirTrigom', 'Sandfire', 'Reportboard ZedP smar ZOM P', and 'MGatting Tad 20z Yuck'), 'Stops Support' (listing 'Topolatice Cope' and 'Tureuetread Inculity TdP'), and 'Anaree Extompuric' (listing 'Vob Mioid' and 'Atecing Toltex'). On the left side, there's a sidebar with 'Word Fuzzing' and 'White BoxTesting' sections, each containing several items. At the bottom, there are social media links for GitHub and LinkedIn.

Ferramenta 15 - ffuf



Fuzzing de Diretórios e Subdomínios

Permite a descoberta de diretórios e subdomínios ocultos em aplicativos da web.

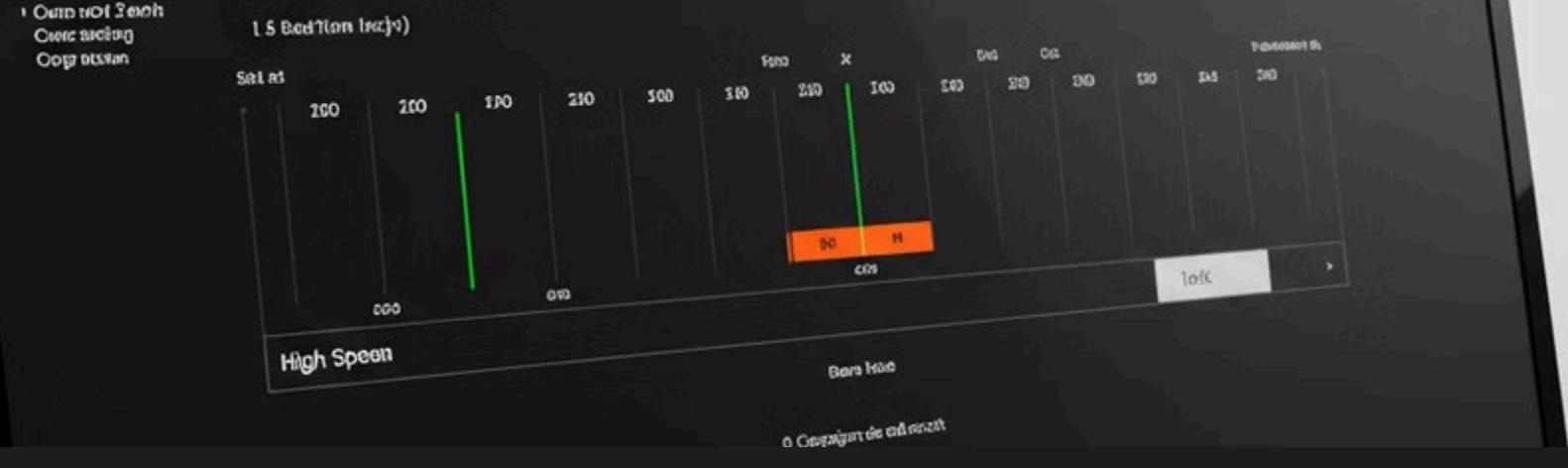
Suporte a Wordlists

Pode utilizar wordlists personalizadas para gerar payloads e realizar testes de fuzzing.



Fuzzing Personalizado

Oferece a capacidade de criar fuzzing personalizado, adaptado às necessidades específicas do teste.



Ferramenta 16 - Masscan

1 Varredura de Alta Velocidade

Utiliza técnicas de varredura otimizadas para atingir altas taxas de transferência.

2 Suporte a Intervalos de IP

Permite especificar intervalos de IP a serem varridos, facilitando a segmentação da varredura.

3 Varredura de Portas Específicas

Permite a varredura de portas específicas ou intervalos de portas em hosts-alvo.

4 Saída Flexível

Gera resultados em formatos como JSON, greppable e XML, facilitando a análise dos dados da varredura.

Ferramenta 17 - Aircrack-ng

- 1
- 2
- 3
- 4

Monitoramento de Pacotes

Permite capturar pacotes de redes sem fio para análise e auditoria.

Quebra de Chaves WEP/WPA/WPA2

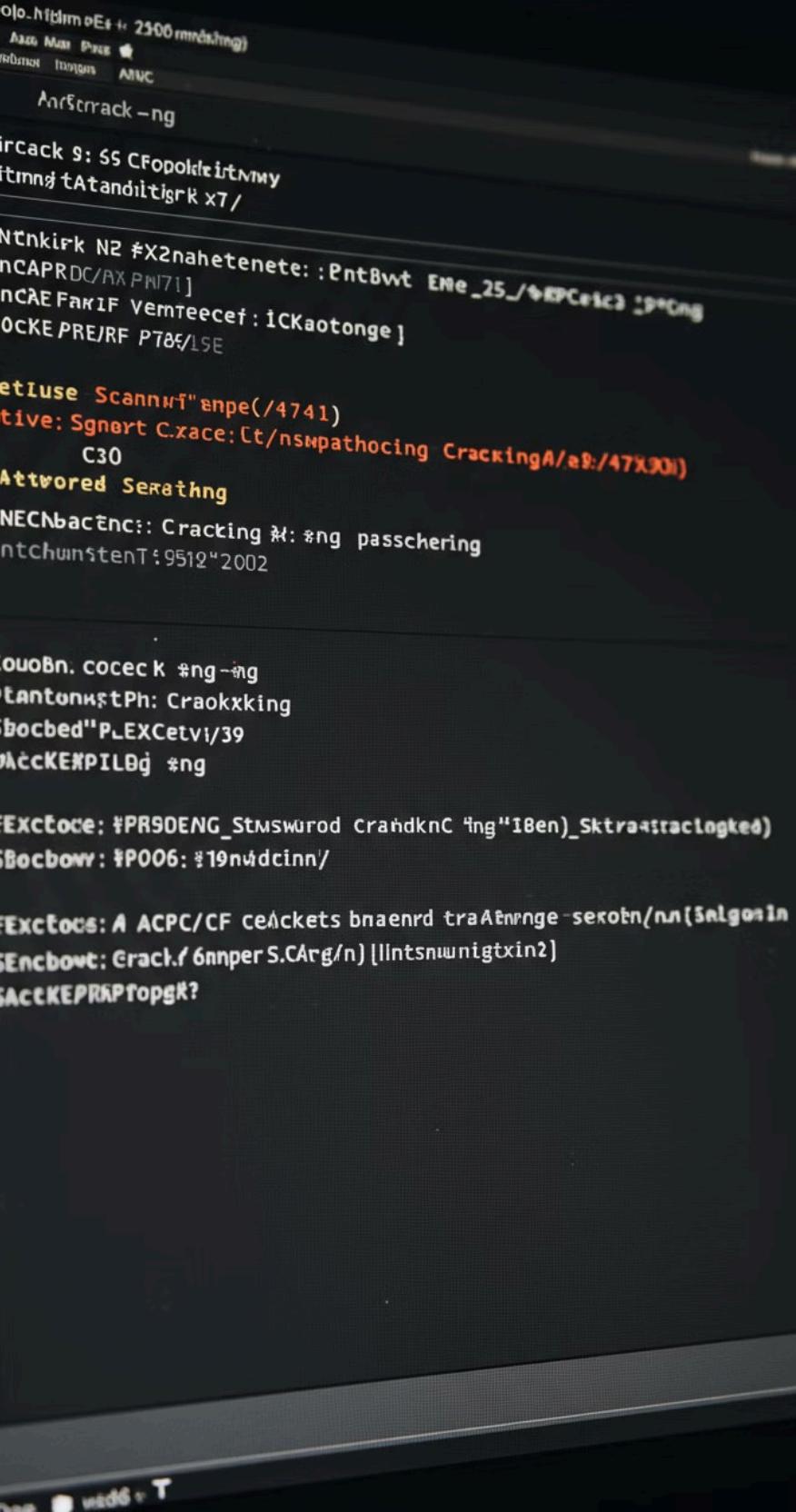
Fornece ferramentas para realizar ataques de força bruta ou ataques de dicionário para quebrar chaves de criptografia.

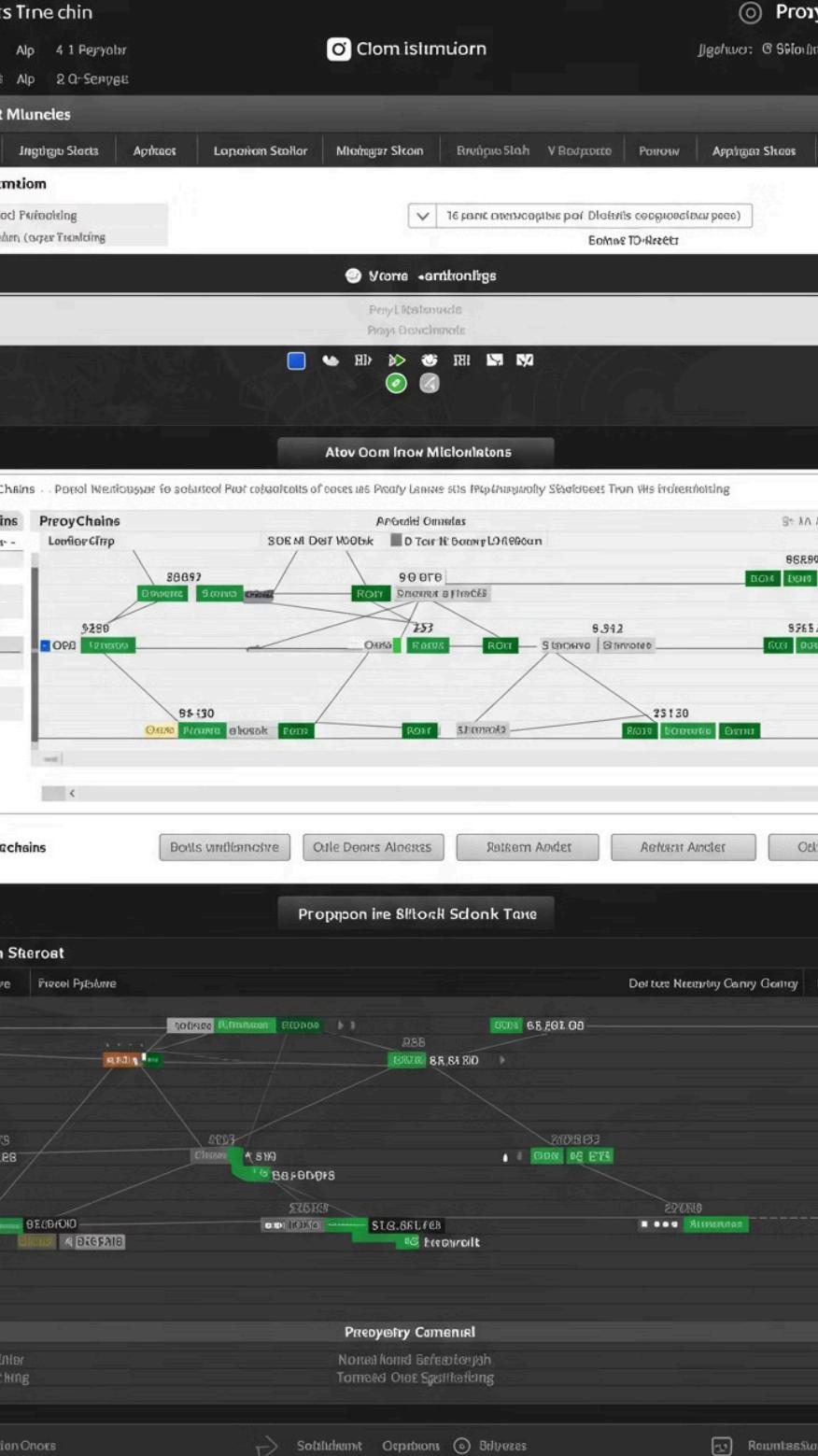
Injeção de Pacotes

Possibilita a injeção de pacotes falsificados na rede para testar a segurança e explorar vulnerabilidades.

Testes de Ataques de Dicionário

Permite realizar ataques de dicionário para tentar quebrar senhas usando listas predefinidas.





Ferramenta 18 - Proxychains

Anonimização

Facilita a anonimização das atividades online ao rotear o tráfego por meio de servidores proxy.

Suporte a Diferentes Protocolos

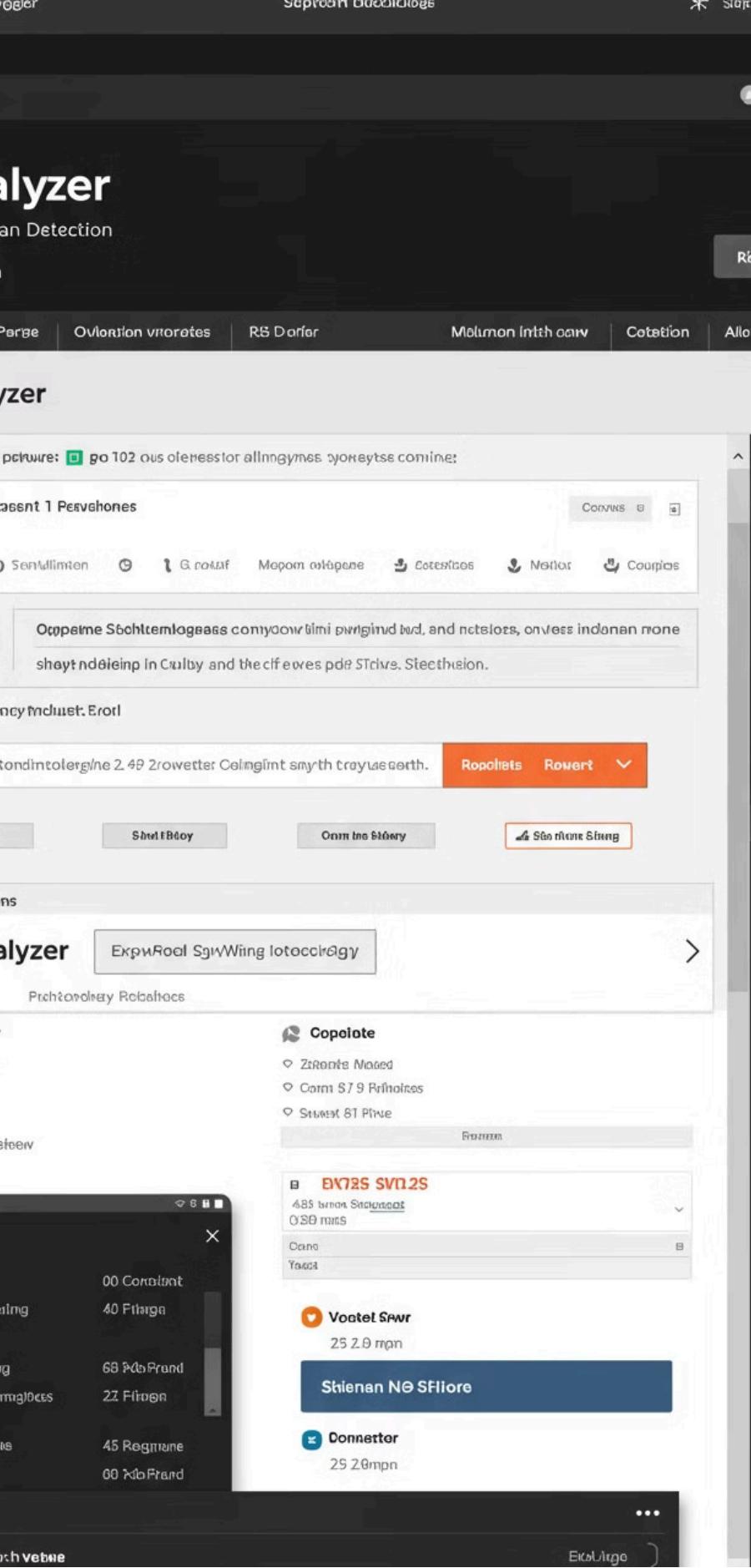
Oferece suporte a diversos protocolos, incluindo HTTP, SOCKS e outros, permitindo a utilização de diferentes tipos de proxies.

Encadeamento de Proxies

Possibilita a configuração de cadeias de proxies, onde o tráfego é direcionado por meio de vários servidores proxy antes de alcançar o destino final.

Configuração Flexível

Permite uma configuração flexível, possibilitando a especificação de proxies específicos para diferentes tipos de tráfego.



Ferramenta 19 - Wappalyzer

1

Identificação de Tecnologias

O Wappalyzer analisa um site e identifica as tecnologias específicas utilizadas, incluindo frameworks, CMS, linguagens de programação, servidores web, e mais.

2

Compatibilidade Ampla

Pode ser usado em uma variedade de navegadores, como Chrome e Firefox, facilitando a integração nas atividades de navegação.

3

Visualização Detalhada

Oferece uma visualização detalhada das tecnologias detectadas, permitindo uma compreensão abrangente da arquitetura de um site.

4

API

Disponibiliza uma API que permite a integração do Wappalyzer em outras ferramentas ou processos automatizados.

Ferramenta 20 - XSSer



Automação de Testes

O XSSer automatiza o processo de identificação e exploração de vulnerabilidades de XSS, economizando tempo e esforço dos testadores de segurança.



Diversidade de Técnicas

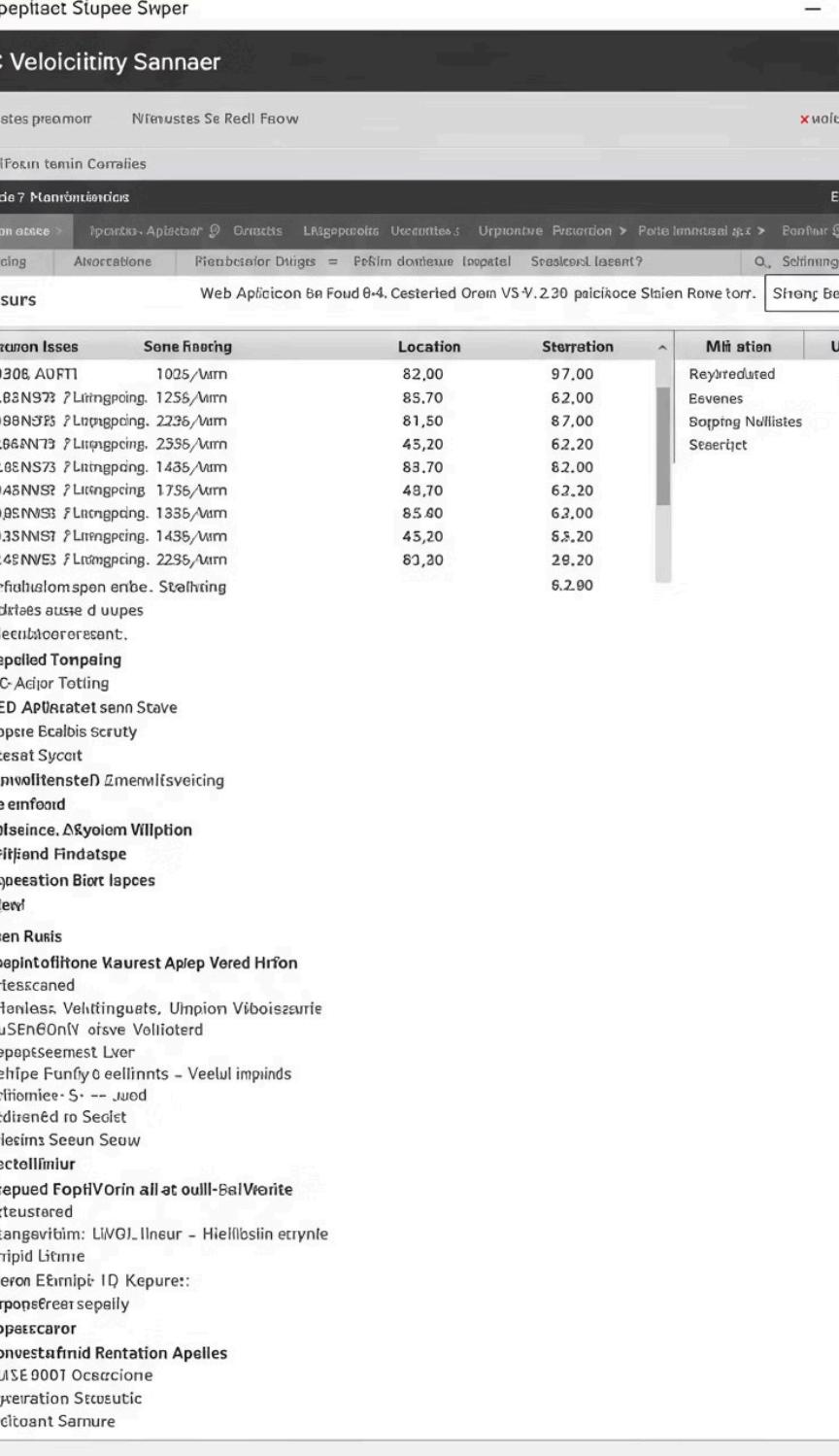
Oferece uma variedade de técnicas e payloads para ajudar na identificação de diferentes tipos de XSS, como Reflected, Stored e DOM-based XSS.



Relatórios Detalhados

Gera relatórios detalhados sobre as vulnerabilidades identificadas, facilitando a compreensão e correção por parte dos desenvolvedores.





Ferramenta 21 - Wapiti

1 Varredura Automática

O Wapiti realiza varreduras automáticas em aplicações web em busca de diversas vulnerabilidades, incluindo injeções SQL, XSS, e outras falhas de segurança comuns.

2 Suporte a Cookies e Autenticação

Permite a configuração de cookies e suporte à autenticação para cenários onde é necessário realizar testes em áreas protegidas por login.

3 Fuzzing de Parâmetros

Oferece funcionalidades de fuzzing para parâmetros, ajudando na identificação de pontos vulneráveis e na execução de ataques controlados.

4 Geração de Relatórios

Gera relatórios detalhados sobre as vulnerabilidades encontradas, facilitando a compreensão e correção por parte dos desenvolvedores.

Ferramenta 22 - DOMinator

1

Análise Estática do DOM

O DOMinator analisa estaticamente e dinamicamente o Document Object Model (DOM) de uma página web para identificar padrões e comportamentos suspeitos relacionados a XSS.

2

Detectção de Vulnerabilidades

Identifica potenciais vulnerabilidades XSS no código JavaScript, ajudando a destacar áreas específicas que podem ser exploradas por atacantes.

3

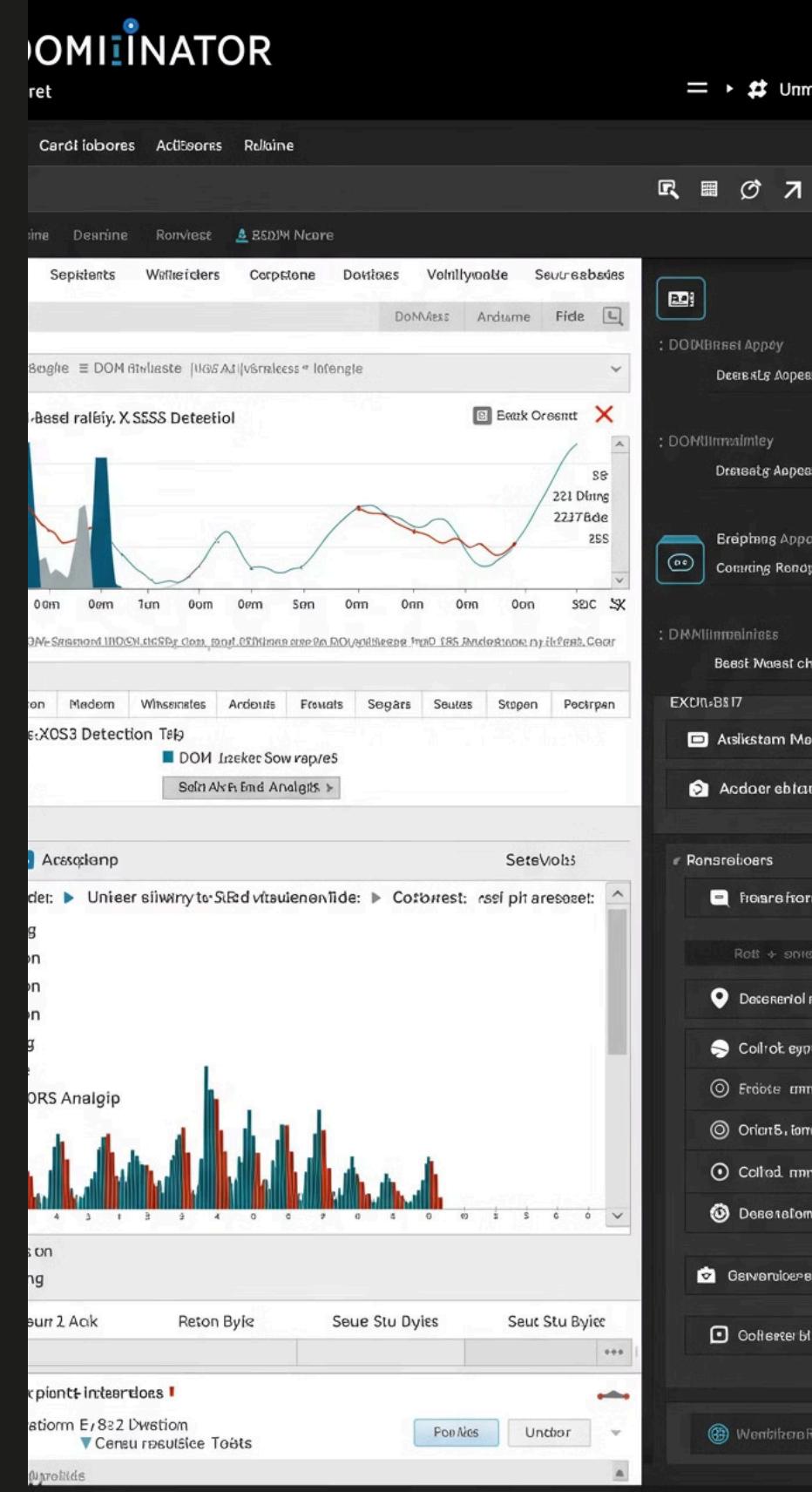
Interatividade com o DOM

Permite aos usuários interagir diretamente com o DOM da página, inspecionando e manipulando elementos para entender melhor o contexto de possíveis vulnerabilidades.

4

Feedback em Tempo Real

Oferece feedback em tempo real durante a navegação, alertando sobre atividades ou códigos suspeitos que podem indicar a presença de XSS baseado em DOM.





Ferramenta 23 - Gowitness

Captura de Screenshots

O Gowitness automatiza a captura de screenshots de várias páginas da web, fornecendo uma visão visual das interfaces e conteúdos dessas páginas.

Análise Visual

A capacidade de análise visual permite que os usuários identifiquem alterações visuais em sites, destacando possíveis modificações ou anomalias.

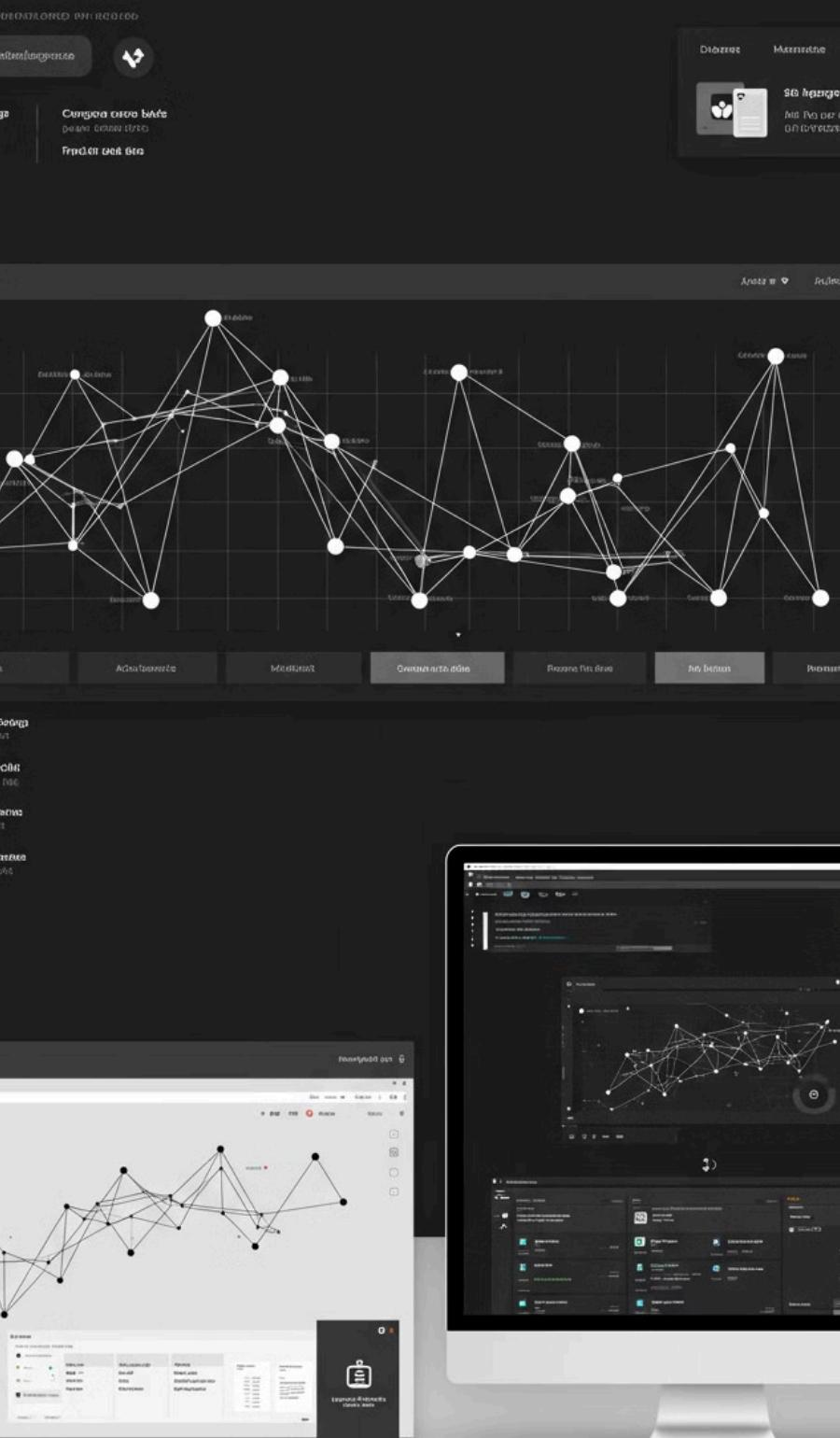
Suporte a Lista de Sites

Aceita listas de sites ou URLs para realizar a captura de screenshots em lote, facilitando a monitoração de diversos alvos simultaneamente.

Exportação de Resultados

Oferece opções para exportar os resultados, permitindo que os usuários armazenem as capturas de screenshots e os dados de análise visual para referência futura.

Ferramenta 24 - Maltego



Coleta de Dados

O Maltego permite a coleta de informações de fontes variadas, incluindo registros públicos, redes sociais, bancos de dados de segurança, WHOIS, e outros.

2

Análise Visual

Apresenta os dados de maneira visualmente intuitiva, usando grafos para representar as relações entre entidades, como pessoas, organizações, endereços IP e domínios.

3

Integração de Fontes

Suporta a integração de várias fontes de dados, proporcionando uma visão holística e abrangente sobre o alvo da investigação.

4

Transformações

Utiliza transformações para realizar consultas e análises específicas nos dados coletados, permitindo explorar relações complexas entre entidades.

Lodery	O	Security Issues	\$
Undumieng	C	Socoplication Issues Security Issues	\$
Podutimil Indone	C	Sporculation Issues Security Issues	\$
OnintheniusSense	C	Ferpolation Issues Security Issues	\$

Ferramenta 25 - Goofuzz



Varredura de Vulnerabilidades

O Goofuzz realiza uma varredura abrangente em um aplicativo web em busca de vulnerabilidades conhecidas, incluindo falhas de segurança comuns.



Busca de Arquivos Sensíveis

Além de vulnerabilidades, o Goofuzz procura por arquivos sensíveis ou mal configurados que possam expor informações confidenciais.



Ferramenta de Teste de Segurança

Pode ser utilizado como parte de um conjunto de ferramentas de teste de segurança para garantir que um aplicativo web seja robusto contra ameaças conhecidas.



Ferramenta 26 - OpenVAS

1 Varredura de Vulnerabilidades em Rede

O OpenVAS realiza varreduras em redes para identificar vulnerabilidades comuns e potenciais ameaças de segurança.

2 Banco de Dados de Vulnerabilidades Atualizado

A ferramenta utiliza um banco de dados extenso e atualizado regularmente, contendo informações sobre uma ampla variedade de vulnerabilidades conhecidas.

3 Análise de Resultados Detalhada

Após a conclusão da varredura, o OpenVAS fornece relatórios detalhados que incluem informações sobre as vulnerabilidades encontradas, sua gravidade e recomendações de mitigação.

4 Configuração Flexível

Permite aos usuários configurar varreduras de acordo com suas necessidades específicas, incluindo a escolha de perfis de varredura, exclusões de hosts e personalização de parâmetros.

Ferramenta 27 - XSSer

1

Automatização de Testes

O XSSer é projetado para simplificar o processo de teste de XSS, tornando-o automatizado. Ele utiliza diversas técnicas e payloads para identificar e explorar vulnerabilidades em aplicações web.

2

Variedade de Técnicas

Oferece uma variedade de técnicas para detecção e exploração de XSS, adaptando-se a diferentes contextos e tipos de vulnerabilidades.

3

Payloads Personalizáveis

Permite aos usuários criar e utilizar payloads personalizáveis, proporcionando flexibilidade para testar diferentes cenários de XSS.

4

Relatórios Detalhados

Gera relatórios detalhados sobre as vulnerabilidades encontradas, incluindo informações sobre a localização e o tipo de vulnerabilidade.



Vantagens Curing TSIV Arete	200.000	750.000g	150.000
Técnica de Vantagem	250.000g	250.000g	160.000
Detecção de vulnerabilidades:			
Ute Site	2 Comunidades	550 Dap	✓
Técnica de Vantagem	150.000	1.760	
Ute Site	450.000	0.480	
Ute Site			
Doll Vantagem	Sesfim	500 Dap	✓
Vantagem	150.000	8.700	

Relatório de Vulnerabilidades				
Ace	328.9600g	500 Dap	90 Dap	Ace
28AP	128.9600g	90 Dap	90 Dap	1CONF
Pgo	728.6500g	190 Dap		
Pgs	228.9800g	90 Dap	29.0Dap	2CS

Ferramenta 28 - wnXSS

Interface Gráfica Simples

O wnXSS oferece uma interface gráfica de usuário (GUI) intuitiva e fácil de usar. Isso facilita a navegação e a execução de testes de XSS, especialmente para usuários que preferem uma abordagem mais visual.

Identificação Automática de Vulnerabilidades

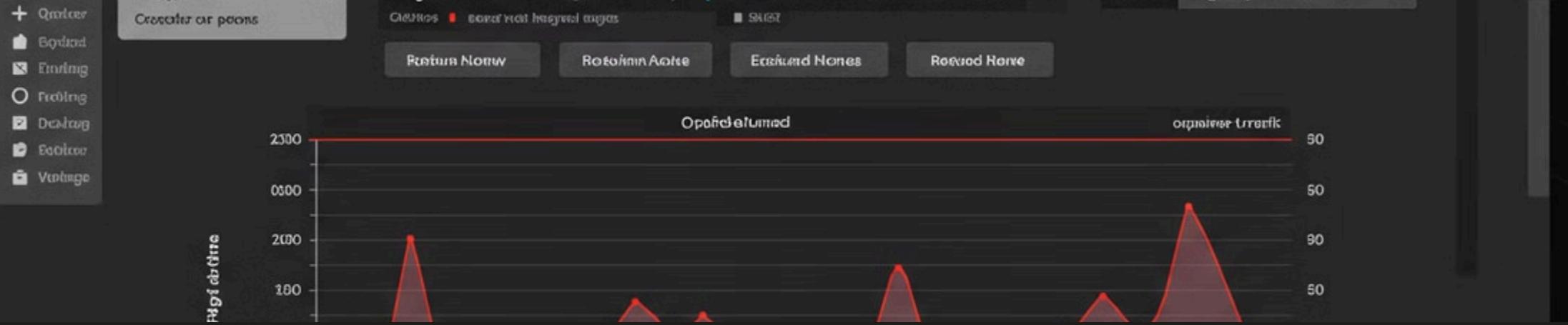
A ferramenta é capaz de identificar automaticamente possíveis vulnerabilidades de XSS em páginas da web, simplificando o processo de detecção.

Exploração de XSS

Após a identificação de vulnerabilidades, o wnXSS fornece opções para explorar e testar essas vulnerabilidades, ajudando a entender o impacto potencial e a gravidade da falha.

Relatórios de Resultados

Gera relatórios detalhados sobre as vulnerabilidades encontradas, oferecendo informações úteis para os profissionais de segurança corrigirem os problemas detectados.



Ferramenta 29 - ngrok

Exposição de Servidores Locais

Permite expor servidores locais hospedados em sua máquina para a Internet, mesmo quando por trás de firewalls ou em redes privadas.

Redirecionamento de Tráfego

Facilita o redirecionamento de tráfego da Internet para servidores locais, permitindo o acesso remoto a aplicativos web, APIs e outros serviços hospedados localmente.



Túneis Seguros

Estabelece conexões seguras usando TLS/SSL para proteger a transferência de dados entre o servidor local e a interface web do ngrok.

Geração de URLs Temporárias

Atribui URLs exclusivos e temporários para cada túnel, facilitando a compartilhamento temporário de acesso a servidores locais.

Ferramenta 30 - DOMPurify



Sanitização de Conteúdo

DOMPurify foca em sanitizar (limpar) conteúdo HTML/JavaScript, removendo quaisquer elementos ou código malicioso que possam ser explorados para ataques XSS.



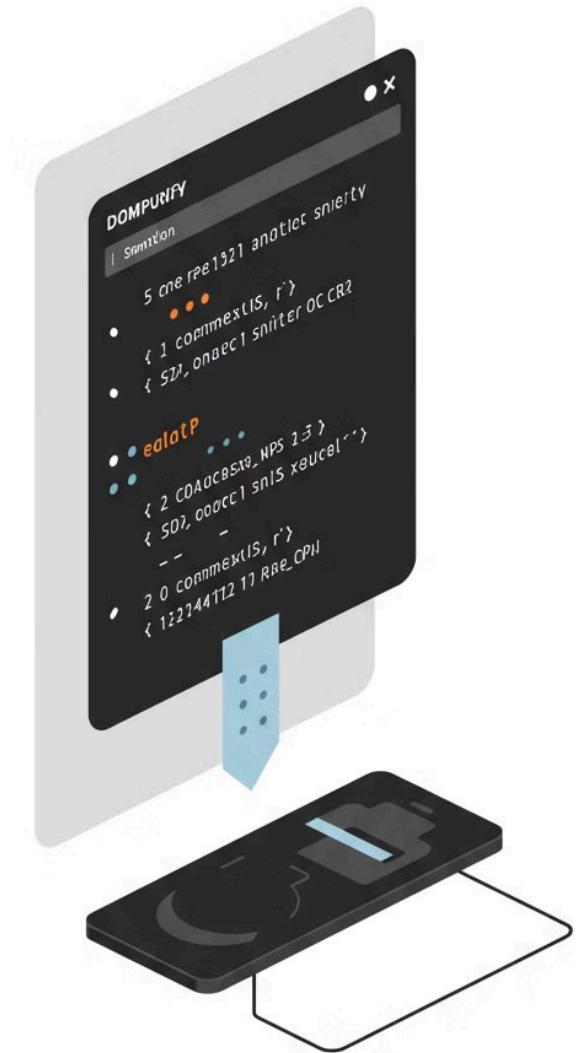
Prevenção contra XSS

Oferece uma camada adicional de segurança ao analisar e filtrar código inserido dinamicamente, garantindo que apenas conteúdo seguro seja renderizado.



Proteção Baseada em Regras

Utiliza um conjunto de regras predefinidas para analisar e filtrar tags, atributos e eventos, garantindo que o conteúdo final seja seguro para renderização.





Ferramenta 31 - Osintgram

1 Coleta de Dados do Instagram

Osintgram possibilita a coleta de informações públicas disponíveis em perfis do Instagram, como detalhes de perfil, postagens, seguidores, seguidos, entre outros.

3 Extração de Dados

Oferece recursos para extrair dados relevantes, facilitando a análise de informações coletadas a partir de perfis do Instagram.

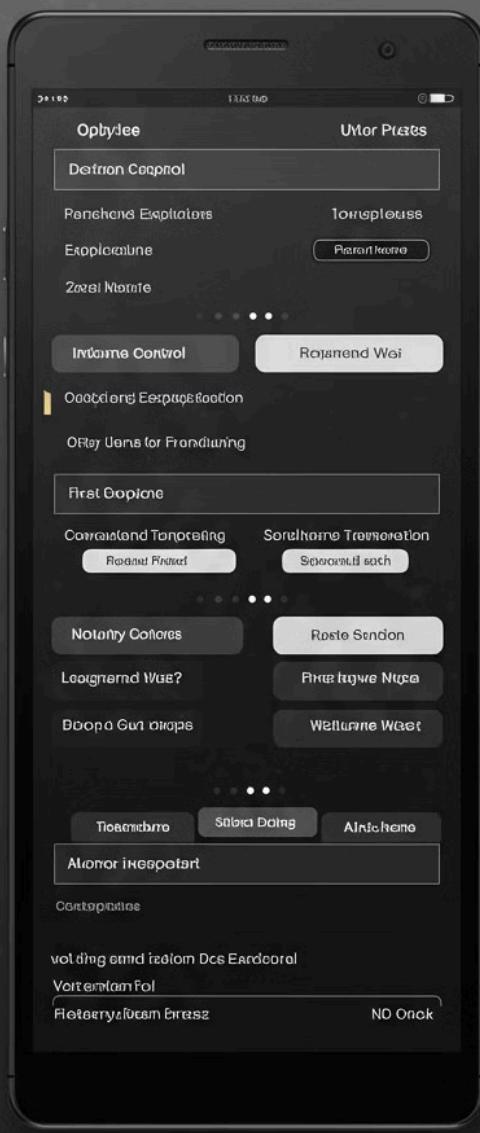
2 Pesquisa por Usuário

Permite realizar buscas específicas por nomes de usuários do Instagram, recuperando dados associados a esses perfis.

4 Interface de Linha de Comando (CLI)

Apresenta uma interface de linha de comando amigável que simplifica o processo de interação com a ferramenta.

Ferramenta 32 - Ghost



Exploração de Dispositivos Android

Ghost oferece módulos para explorar e comprometer dispositivos Android, permitindo a execução de ataques controlados pelo invasor.

Engenharia Social

Inclui recursos relacionados à engenharia social, visando manipular usuários para realizar ações que beneficiem o invasor.

Funcionalidades Variadas

O conjunto de ferramentas abrange uma variedade de funcionalidades, desde a obtenção de informações sobre o dispositivo até a execução de comandos remotos.

Persistência e Acesso Remoto

Ghost busca estabelecer persistência nos dispositivos comprometidos, garantindo acesso remoto contínuo para o invasor.

Ferramenta 33 - Saycheese

Captura Remota de Fotos

O Saycheese facilita a captura de fotos da câmera frontal de dispositivos remotos, sem o conhecimento da vítima.

Geração de Links Maliciosos

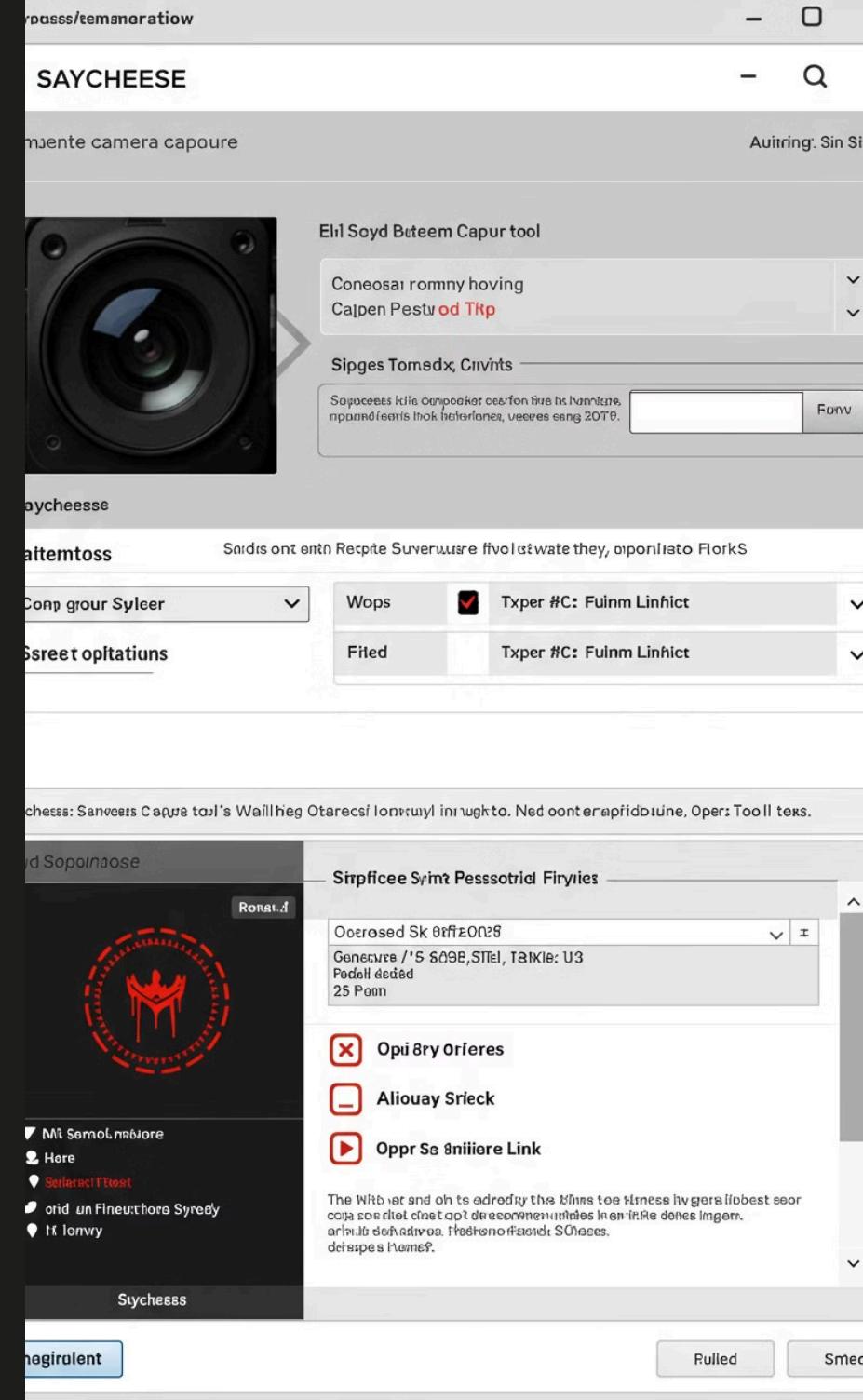
A ferramenta cria links maliciosos que, ao serem abertos pela vítima, açãoam a câmera frontal do dispositivo para capturar a imagem.

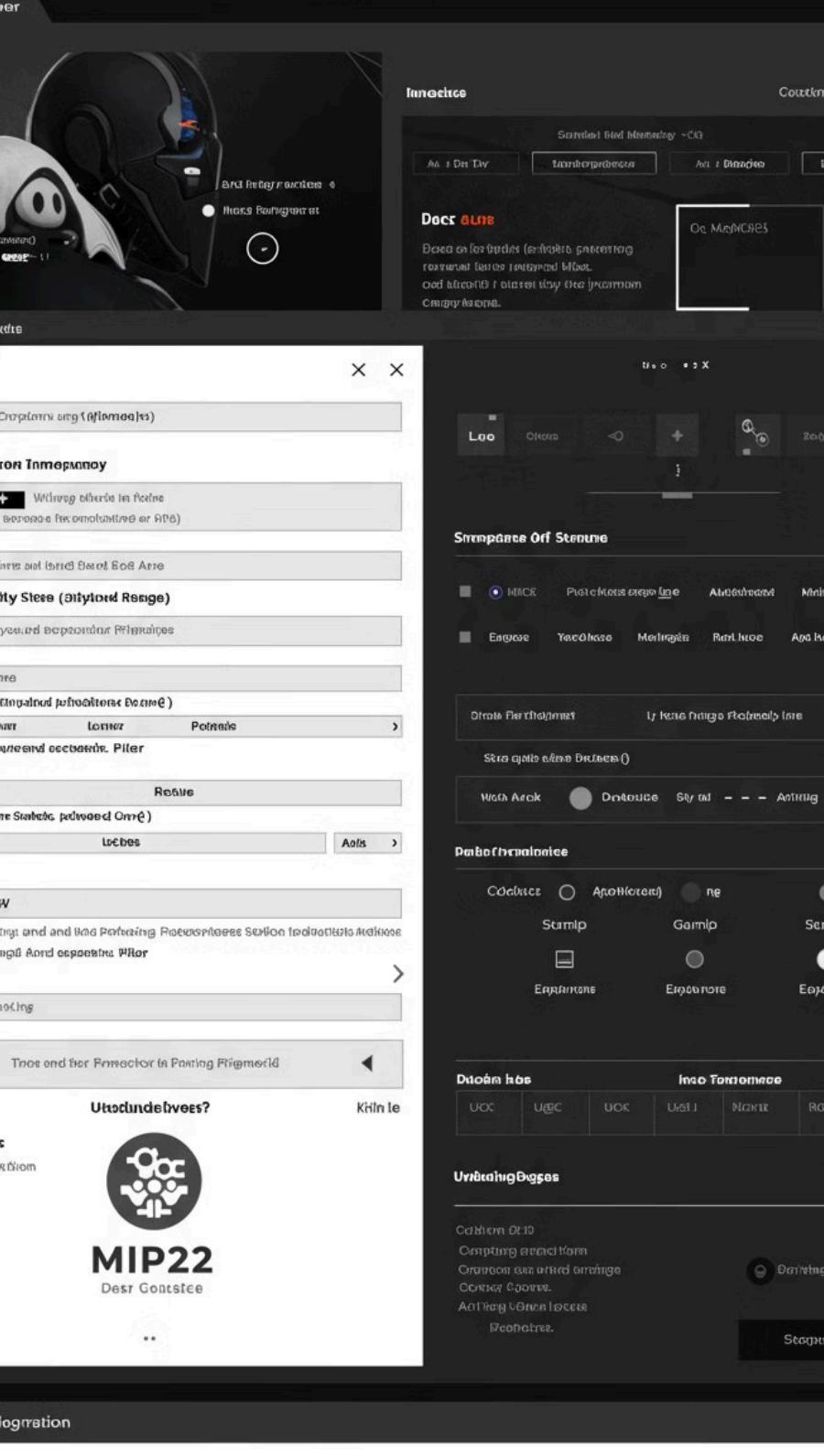
Acesso Discreto

Operando de maneira discreta, o Saycheese permite realizar a captura de imagens sem alertar a vítima sobre a atividade.

Compartilhamento do Link

Após a configuração, o link gerado pode ser compartilhado com a vítima de maneira a induzi-la a acessar o conteúdo.





Ferramenta 34 - Mip22

1

Framework de Phishing

O Mip22 é baseado no Zphisher e oferece recursos de phishing automatizado para simplificar a criação e implantação de ataques.

2

Opções Extras

Esta versão personalizada pode incluir opções extras que aprimoram a eficácia e a flexibilidade do framework.

3

Inclusão de Jogos

A adição de jogos pode ser uma estratégia para atrair potenciais vítimas, utilizando elementos de entretenimento para induzi-las a interagir com o conteúdo malicioso.

4

Personalização

Explore as opções extras e recursos adicionados nesta versão personalizada para ajustar o framework de acordo com seus objetivos.



Ferramenta 35 - Spiderfoot



Coleta de Informações OSINT

O Spiderfoot é especializado em reunir dados de fontes abertas, fornecendo informações sobre IPs, domínios, e-mails, nomes de usuários, entre outros.



Fontes Diversificadas

A ferramenta utiliza uma variedade de fontes, como motores de busca, bancos de dados públicos e redes sociais para adquirir dados relevantes.



Análise de Relacionamentos

Além de coletar informações, o Spiderfoot analisa e exibe relacionamentos entre os dados, oferecendo uma visão abrangente do alvo.

Ferramenta 36 - Sherlock

1 Busca Automatizada

O Sherlock automatiza o processo de busca por perfis de usuário em redes sociais populares, utilizando nomes de usuário.

2 Ampla Cobertura

Oferece suporte para uma variedade de plataformas, incluindo redes sociais, fóruns, sites e outros locais onde os usuários podem ter presença online.

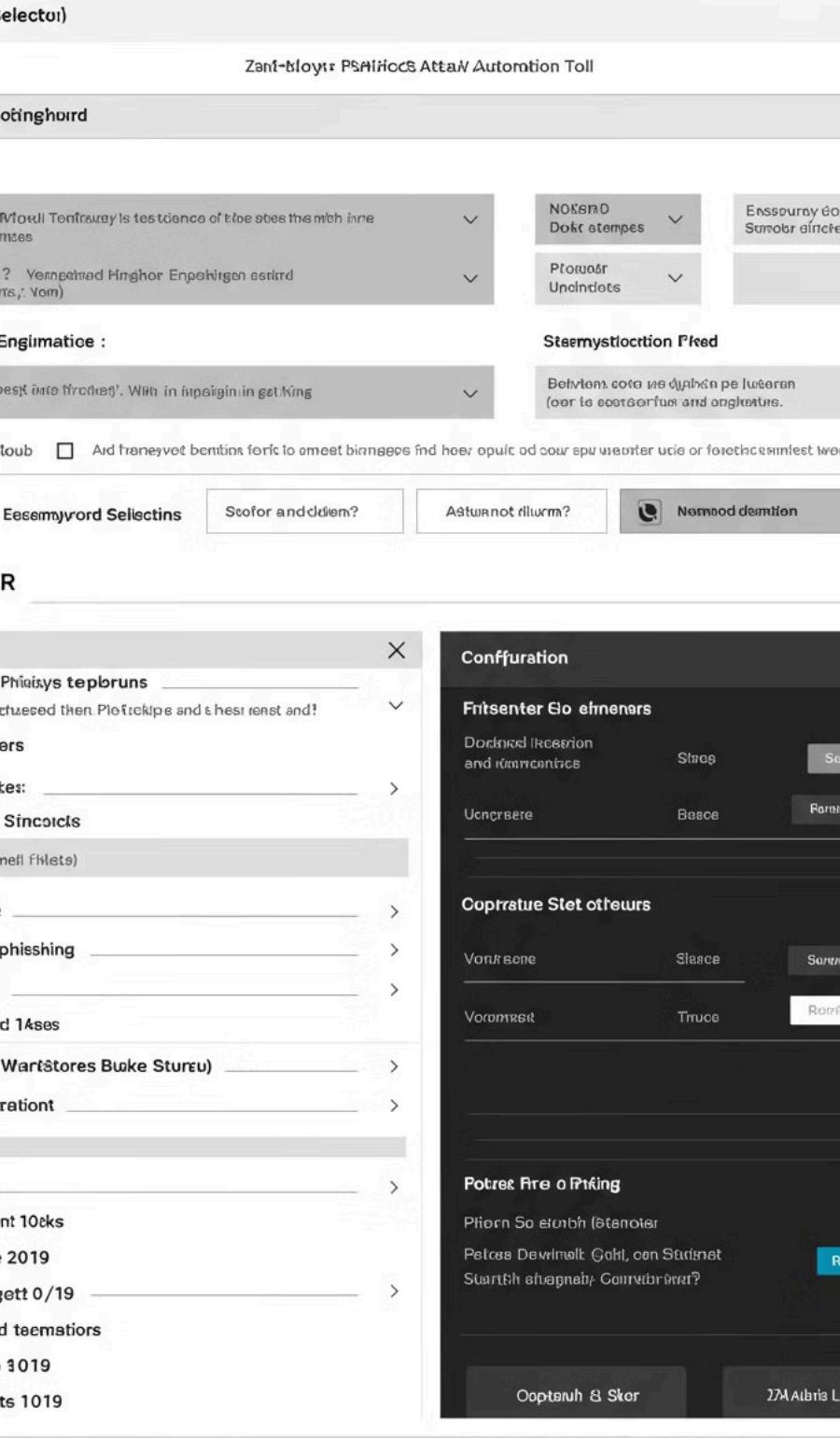
3 Utilização de Nomes de Usuário

Baseia-se em nomes de usuário para realizar buscas, permitindo a localização de perfis mesmo quando o nome real não é conhecido.

4 Busca Rápida e Eficiente

Agiliza o processo de investigação, economizando tempo ao automatizar a busca em diferentes plataformas simultaneamente.





Ferramenta 37 - Zphisher



Phishing Automatizado

O Zphisher simplifica o processo de criação e execução de ataques de phishing, tornando-o acessível a usuários com diversos níveis de habilidade.

Diversidade de Opções

Oferece uma variedade de modelos de phishing para diferentes sites e serviços populares, incluindo redes sociais, serviços de e-mail e plataformas de login.

Facilidade de Uso

Sua interface simples e amigável torna o Zphisher uma escolha conveniente para usuários iniciantes ou aqueles que desejam realizar testes de conscientização em segurança.

Métodos de Redirecionamento

Permite redirecionamento para páginas de login reais após a submissão de credenciais falsas, aumentando a autenticidade do ataque.

Ferramenta 38 - Seeker

Rastreamento de Geolocalização

O Seeker se concentra em rastrear a localização de alvos usando informações de redes sociais, permitindo a criação de páginas de phishing para capturar dados de geolocalização.

Criação de Páginas de Phishing

Gera páginas de phishing personalizadas que exploram a curiosidade da vítima, incentivando-a a compartilhar sua localização.

Integração com ngrok

Pode ser combinado com o ngrok para criar túneis seguros e expor as páginas de phishing para a internet.

Acesso Remoto

Permite o acesso remoto aos dados de geolocalização capturados, proporcionando uma visão abrangente dos movimentos da vítima.



Test case	Test cases	Mutation	Mutations	Mutations	Coverage
9.1M	2.8%	2.5%	Intabpis.	Intenviomz	Coverage

180 ↗

Ferramenta 39 - PyJFuzz

Teste de Mutação Automatizado

PyJFuzz automatiza o processo de teste de mutação, gerando inputs mutados para aplicativos Python a fim de descobrir falhas de segurança.

Compatibilidade com Aplicações Python

Projetado especificamente para testar aplicações escritas em Python, abrangendo uma variedade de tipos de projetos e cenários de uso.

1

2

3

4

Identificação de Falhas de Software

Utiliza a técnica de teste de mutação para gerar inputs que podem revelar falhas de software, como exceções inesperadas, vazamentos de informações e outros problemas de segurança.

Configurações Personalizadas

Permite configurações personalizadas para ajustar o nível de mutação, o escopo do teste e outras opções, proporcionando flexibilidade aos testadores.



Ferramenta 40 - Faraday



Integração de Ferramentas

Oferece integração com diversas ferramentas populares de teste de segurança, como scanners de vulnerabilidade, frameworks de exploração e análise de resultados.



Centralização de Dados

Permite centralizar e organizar todos os dados relacionados aos testes de segurança, facilitando a análise e o acompanhamento de resultados ao longo do tempo.



Colaboração em Equipe

Suporta colaboração entre membros da equipe de segurança, permitindo o compartilhamento de informações, resultados e tarefas.

Ferramenta 41 - CyberChef

1 Manipulação de Dados

Permite realizar uma ampla gama de operações em dados, como conversões de codificação, criptografia, compressão, análise hexadecimal e muito mais.

3 Conversão de Codificação

Suporta conversões entre diferentes formatos de codificação, como Base64, hexadecimal, URL, entre outros.

2 Visualização de Dados

Fornece uma interface gráfica intuitiva para visualização de dados e resultados, facilitando a compreensão das transformações aplicadas.

4 Análise de Strings

Ajuda na análise e manipulação de strings, tornando mais fácil extrair informações específicas de dados complexos.



Ferramenta 42 - Empire

1

Controle Remoto

Permite o controle remoto de sistemas comprometidos, facilitando a execução de comandos, transferência de arquivos e outras operações.

2

Módulos de Exploração

Oferece uma variedade de módulos para explorar sistemas, incluindo a execução de exploits, enumeração de informações e identificação de vulnerabilidades.

3

Persistência

Possui recursos para estabelecer persistência nos sistemas comprometidos, garantindo que o acesso seja mantido mesmo após reinicializações.

4

Extensibilidade

Permite a adição de módulos personalizados, ampliando a funcionalidade do framework para atender a cenários específicos.



Ferramenta 43 - BeEF

Exploração de Navegadores

O BeEF concentra-se em explorar vulnerabilidades e fraquezas nos navegadores da web, aproveitando seus recursos e execução de código arbitrário.

Módulos Extensíveis

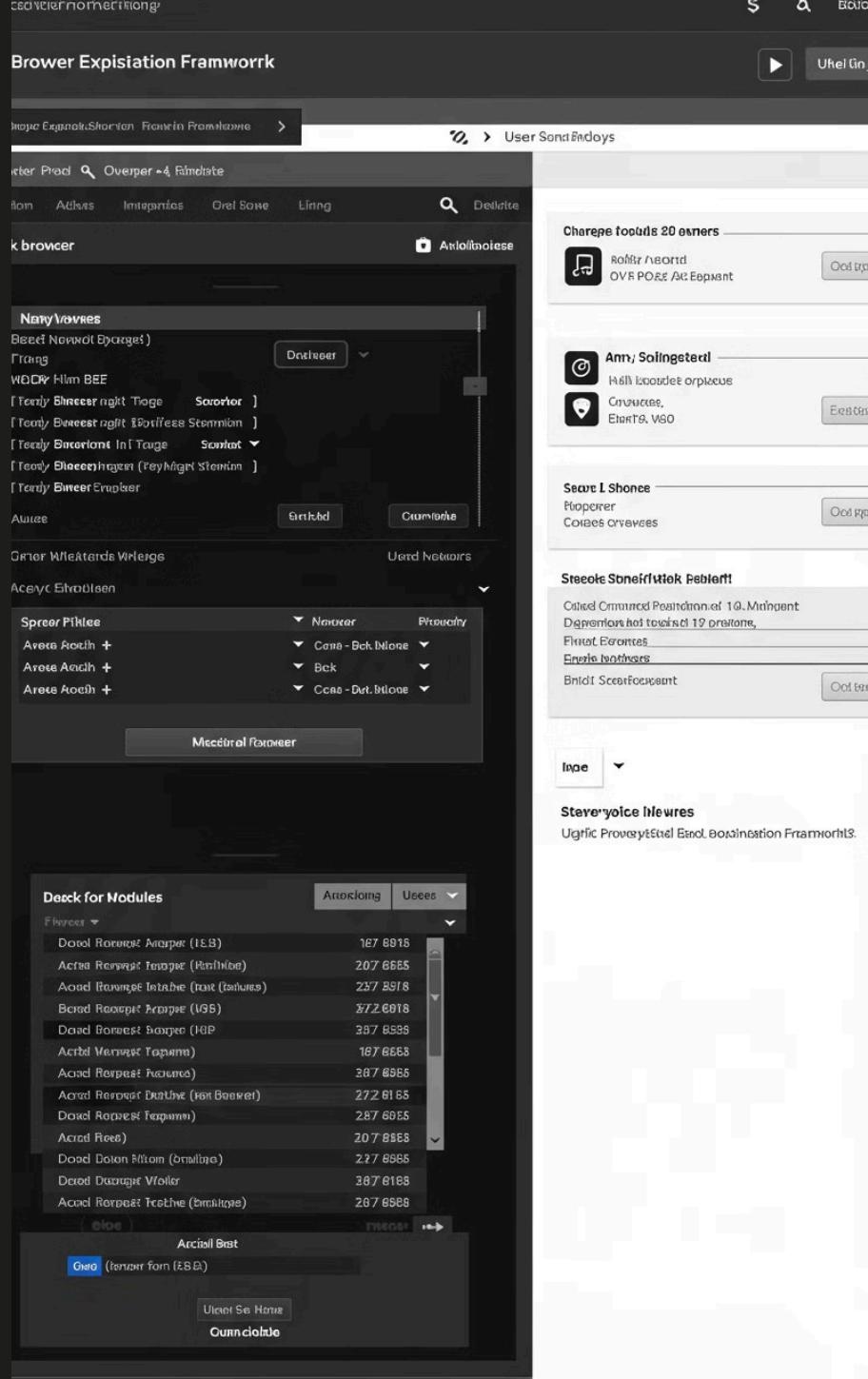
Oferece uma arquitetura modular com uma ampla variedade de módulos para diferentes tipos de ataques e explorações, tornando-o altamente extensível.

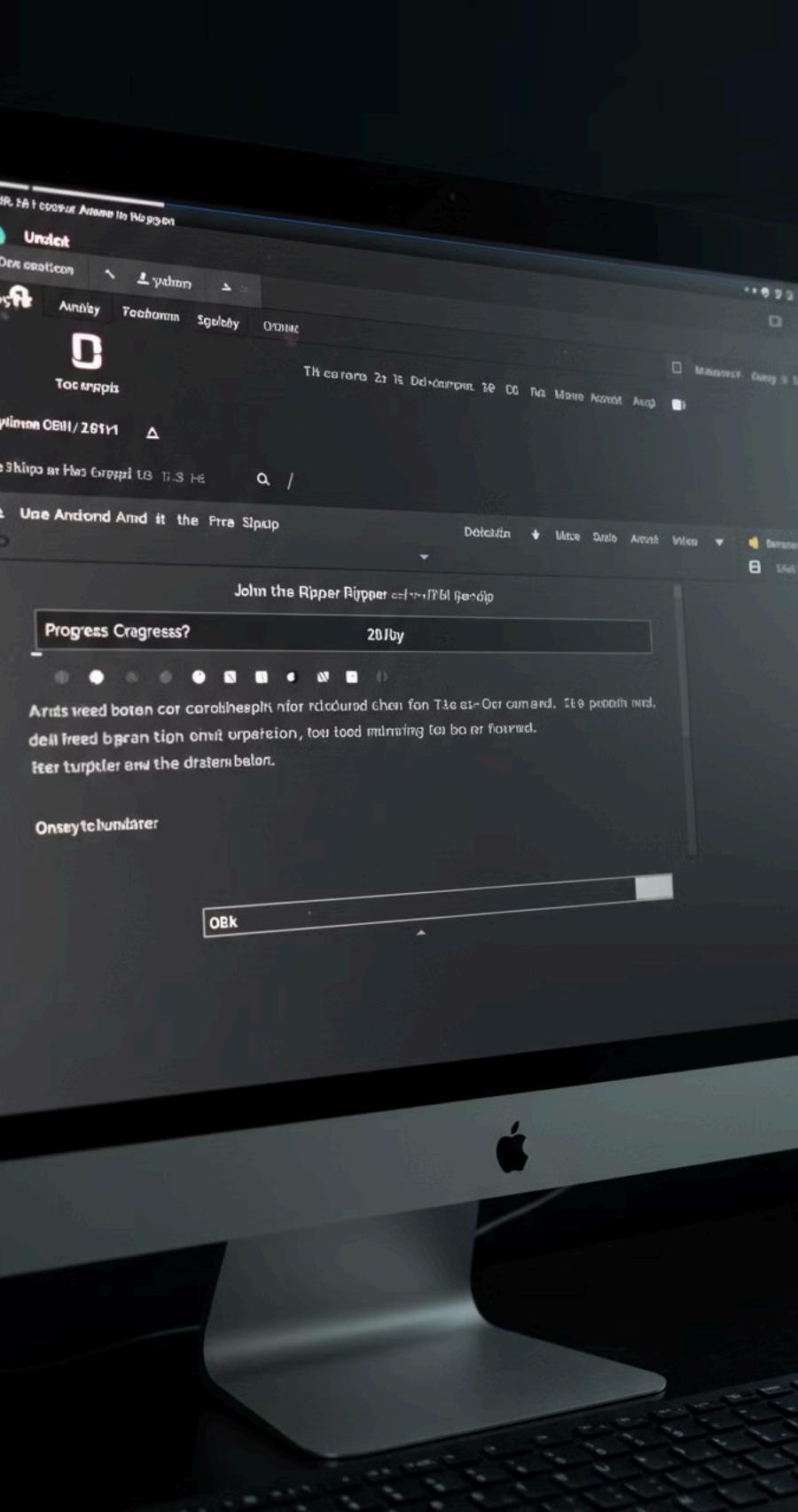
Interface Gráfica e Painel de Controle

Possui uma interface gráfica intuitiva e um painel de controle que permite aos usuários interagirem com os navegadores comprometidos em tempo real.

Ataques Persistentes

O BeEF é capaz de estabelecer conexões persistentes com navegadores comprometidos, permitindo ataques contínuos e interações com as vítimas.





Ferramenta 44 - John the Ripper

1

Quebra de Senhas

Projetado para quebrar senhas por meio de ataques de força bruta, ataques de dicionário e outros métodos.

2

Suporte a Vários Algoritmos

Oferece suporte a uma variedade de algoritmos de hash, incluindo DES, MD5, SHA-1, SHA-256, entre outros.

3

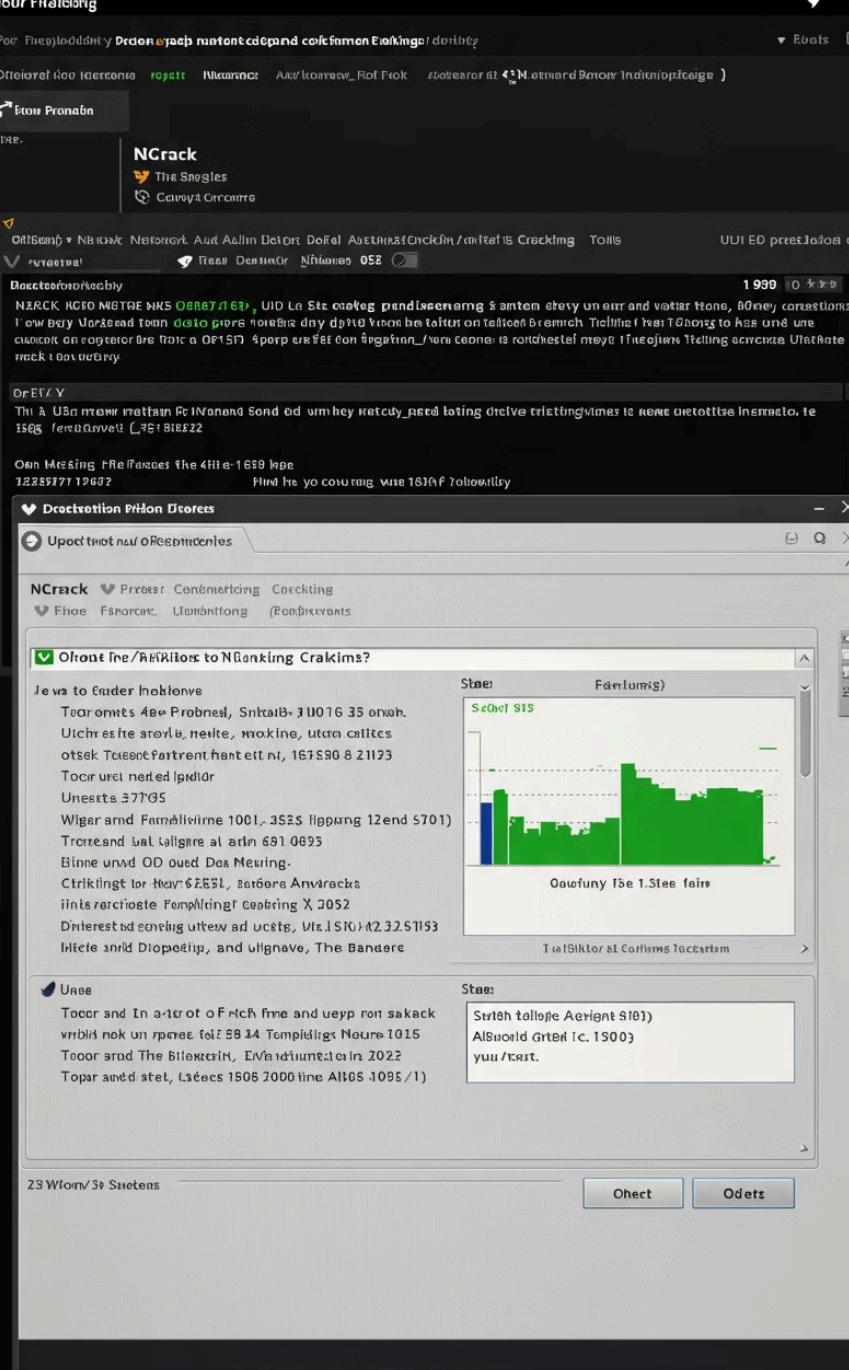
Modos de Ataque

Permite a execução de diferentes modos de ataque, como ataques de dicionário, ataques incrementais e ataques baseados em regras.

4

Personalização de Ataques

Os usuários podem personalizar os ataques usando regras específicas para gerar combinações de senhas.



Ferramenta 45 - Ncrack



Quebra de Autenticação

Desenvolvido para realizar ataques de força bruta e ataques de dicionário contra diferentes protocolos de autenticação.



Supo rte a Diversos Protocolos

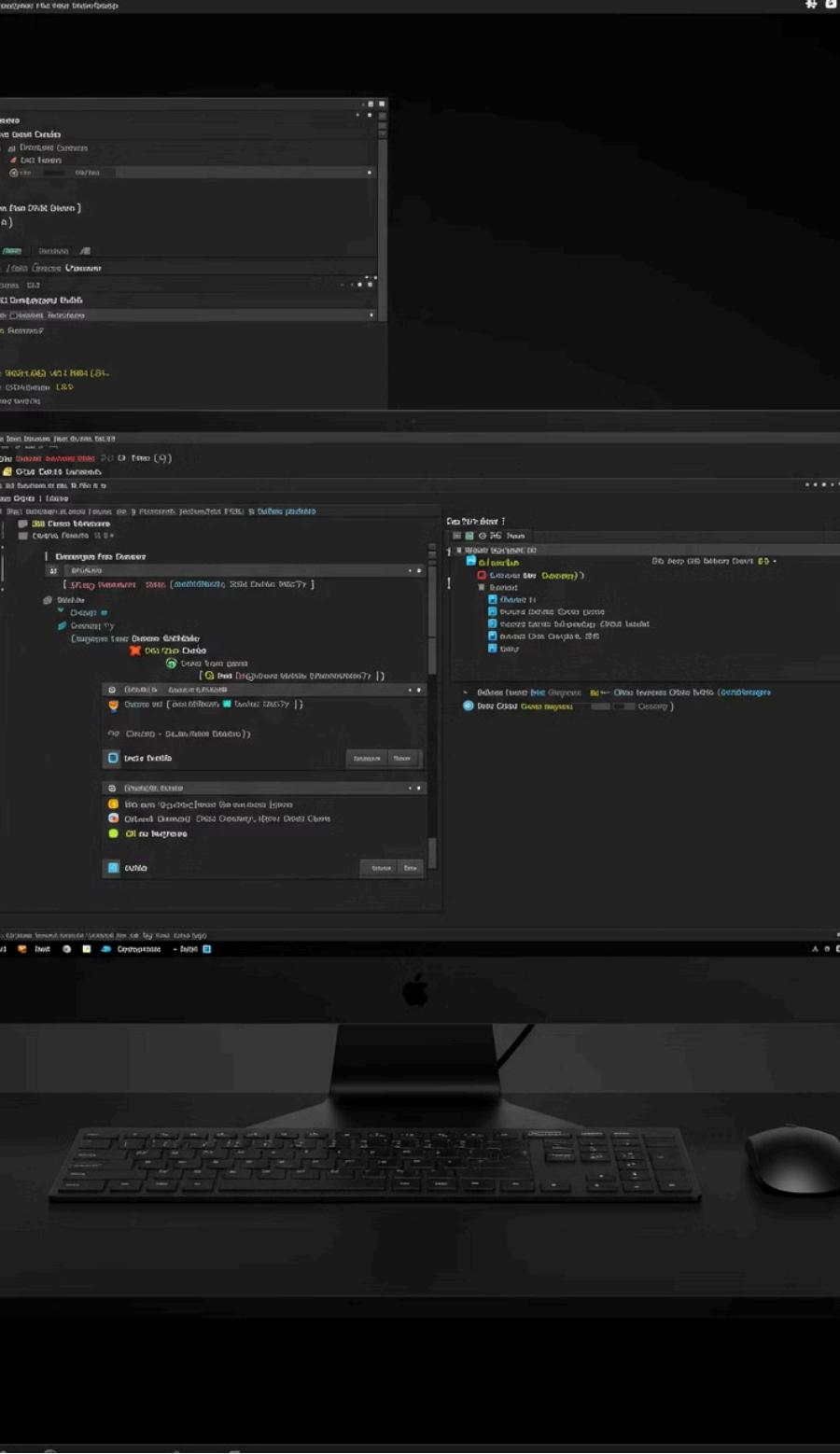
Oferece suporte a uma ampla variedade de protocolos de rede, incluindo SSH, RDP, FTP, Telnet, HTTP(S) e muitos outros.



Detecção de Bloqueio

Implementa técnicas inteligentes para evitar bloqueios por parte do alvo, ajustando automaticamente a velocidade do ataque.

Ferramenta 46 - Kali Linux



1

Foco em Segurança

Projetado para fornecer uma plataforma dedicada a testes de segurança, avaliação de vulnerabilidades e investigações forenses.

2

Ampla Gama de Ferramentas

Vem pré-instalado com uma vasta coleção de ferramentas de segurança, abrangendo desde scanners de vulnerabilidade até frameworks de exploração.

3

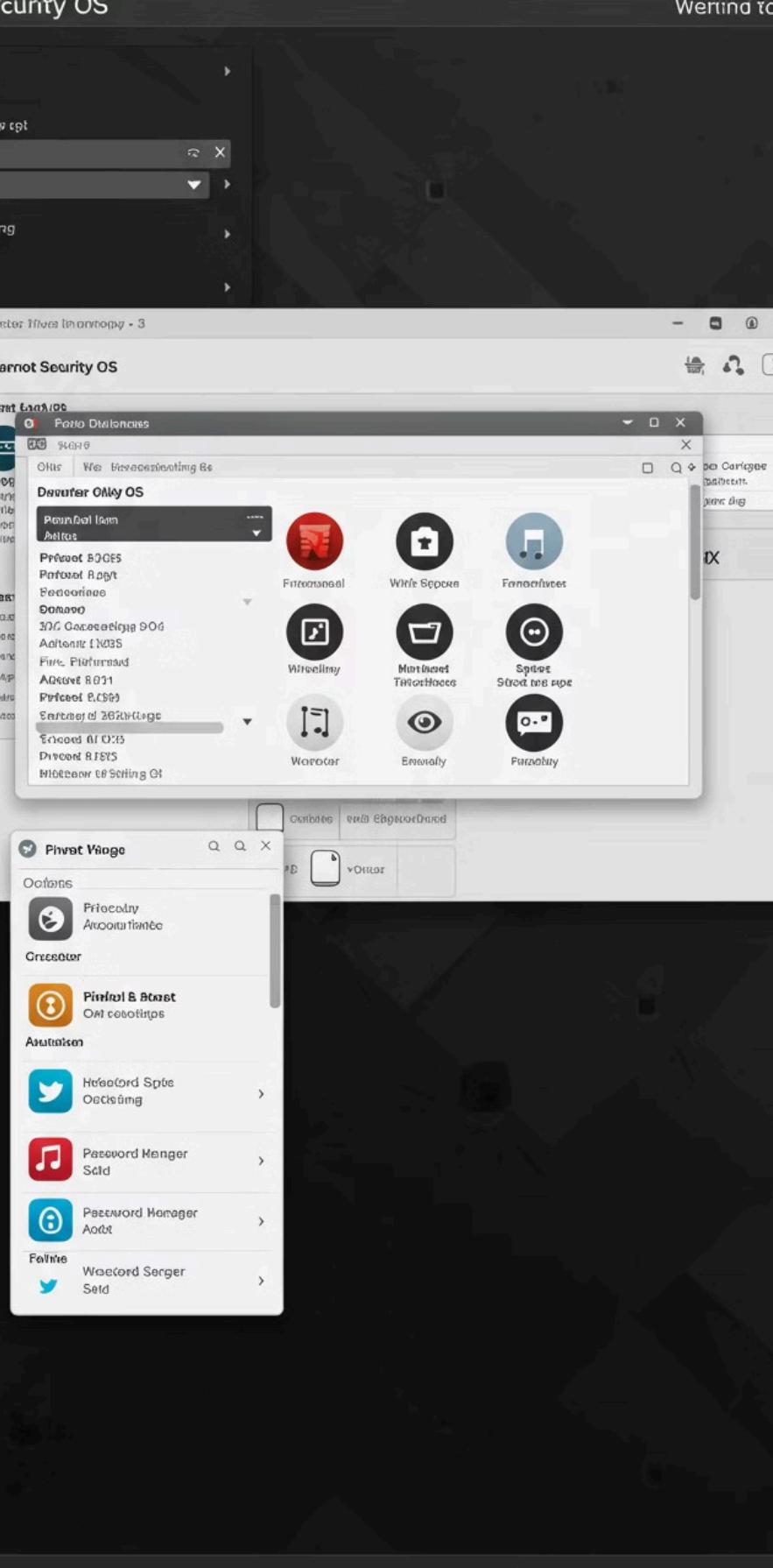
Ambiente de Testes Seguro

Possui um ambiente seguro e controlado, permitindo que os profissionais de segurança realizem testes sem impactar sistemas reais.

4

Constantes Atualizações

Mantido ativamente pela comunidade de segurança cibernética, garantindo que as ferramentas e os componentes estejam atualizados com as últimas tecnologias.



Ferramenta 47 - Parrot Security OS

Segurança e Privacidade

Oferece ferramentas avançadas para testes de segurança, análise forense, preservação de privacidade online e proteção contra ameaças cibernéticas.

Base Debian

Construído sobre a base do Debian, garantindo estabilidade e compatibilidade com uma vasta gama de pacotes e software.

Múltiplos Ambientes de Desktop

Suporta vários ambientes de desktop, incluindo MATE, KDE Plasma, Xfce e outros, permitindo que os usuários escolham a interface que melhor atende às suas preferências.

Ferramentas de Anonimato

Integra ferramentas para navegação anônima, como a rede Tor, proporcionando maior privacidade online.

```
se(ap=Tomd  
stal_opa install pypton;
```

```
ite ap:_int wime aytorn enines);
```

```
pe: = appare a_apt letatt 'ofeenim ar ign: =uston;  
od?
```

```
nonur: yni Oitival orc/anopeye/remontnrrdesue sstiggs_  
titure_youre426_!0608(!N:/eorenatum aceprafexe_  
ptcine_votvegren jatc} 1.311, cdege dsesrlsingrtsteniaggs_  
tetplesy 1 batal pyton!?"
```

```
noiunt / apt JInstall pyton'apirnntmesh/, syplafnrciep Setren;  
(43estnyofl rnsual jeum? 16g::
```

Termux: Emulador de Terminal para Android

Ambiente Linux Completo

Oferece um ambiente Linux funcional no Android, permitindo a execução de comandos e a instalação de pacotes como se estivesse em um sistema Linux tradicional.

Gerenciador de Pacotes

Possui um gerenciador de pacotes próprio, semelhante aos sistemas Linux, permitindo a instalação fácil de ferramentas, utilitários e linguagens de programação.

Acesso à Raiz (Root)

Para dispositivos com root, o Termux oferece maior controle e acesso ao sistema Android, permitindo a execução de comandos como superusuário (root).

Desenvolvimento e Scripting

É uma ferramenta valiosa para desenvolvedores e entusiastas que desejam programar, executar scripts e realizar tarefas de administração de sistemas diretamente em seus dispositivos Android.

Encerramento

Neste eBook, exploramos um vasto conjunto de 47 ferramentas que abrangem diversas áreas do universo da segurança digital. Desde ferramentas essenciais para testes de penetração e avaliação de vulnerabilidades até utilitários dedicados à coleta de informações e exploração ética, cada uma desempenha um papel crucial no arsenal de profissionais de segurança, hackers éticos e entusiastas de tecnologia.

Lembre-se, o conhecimento e o uso dessas ferramentas devem ser conduzidos de maneira ética e responsável. A segurança digital é um campo dinâmico, e a constante evolução dessas ferramentas reflete a necessidade de profissionais bem treinados e dedicados.



Responsabilidade Ética



1

Uso Ético

À medida que você explora e utiliza essas ferramentas, lembre-se do imperativo ético de respeitar a privacidade e agir em conformidade com as leis e regulamentações locais.

3

Contribuição para Segurança

Ao aprofundar-se na exploração dessas soluções, você contribui para a construção de um ambiente digital mais seguro e resiliente.

2

Aprendizado Contínuo

A segurança cibernética é uma jornada contínua, e a compreensão dessas ferramentas é apenas o ponto de partida.

4

Adaptação e Evolução

Continue aprendendo, adaptando-se e explorando novas fronteiras na vasta paisagem da segurança cibernética.

Importância da Segurança Cibernética



1

Proteção de Dados

A segurança cibernética é crucial para proteger informações sensíveis e dados pessoais contra ameaças digitais.

2

Integridade de Sistemas

Garante a integridade e o funcionamento adequado de sistemas e redes, prevenindo interrupções e danos.

3

Confiança Digital

Promove a confiança em transações e comunicações digitais, essencial para o funcionamento da economia moderna.

4

Inovação Segura

Permite o avanço tecnológico e a inovação, garantindo que novos desenvolvimentos sejam seguros e confiáveis.

Desafios Futuros em Segurança Cibernética

1

Ameaças Emergentes

Novas formas de ataques e ameaças surgem constantemente, exigindo vigilância e adaptação contínuas.

2

Complexidade Crescente

Sistemas e redes tornam-se cada vez mais complexos, aumentando a superfície de ataque e os desafios de proteção.

3

Privacidade vs. Segurança

Equilibrar as necessidades de segurança com o direito à privacidade continua sendo um desafio significativo.

4

Escassez de Talentos

A demanda por profissionais qualificados em segurança cibernética supera a oferta, criando um gap de habilidades no setor.





Tendências em Segurança Cibernética



Inteligência Artificial

Uso crescente de IA e aprendizado de máquina para detecção e resposta a ameaças em tempo real.



Segurança em Nuvem

Foco aumentado na proteção de dados e aplicações em ambientes de nuvem.



IoT Security

Maior atenção à segurança de dispositivos conectados à Internet das Coisas (IoT).

Melhores Práticas em Segurança Cibernética

Atualizações Regulares

Manter sistemas e software atualizados com as últimas correções de segurança.

Educação Contínua

Treinar regularmente funcionários e usuários sobre ameaças cibernéticas e práticas seguras.

Autenticação Forte

Implementar autenticação de múltiplos fatores e senhas fortes em todos os sistemas.

Backup e Recuperação

Manter backups regulares e testar planos de recuperação de desastres.



Software Update



Multi-Factor Authentication



User Education Practitioners



Usability



O Papel da Colaboração em Segurança Cibernética

1 Compartilhamento de Informações

Colaboração entre organizações para compartilhar informações sobre ameaças e melhores práticas.

2 Parcerias Público-Privadas

Cooperação entre governos e setor privado para fortalecer a segurança cibernética nacional.

3 Pesquisa e Desenvolvimento

Esforços conjuntos em P&D para desenvolver novas tecnologias e soluções de segurança.

4 Comunidade Open Source

Contribuições da comunidade open source para ferramentas e frameworks de segurança.

O Futuro da Segurança Cibernética

1

Segurança Quântica

Desenvolvimento de criptografia resistente a ataques quânticos e uso de computação quântica para segurança.

2

Automação Avançada

Maior automação em detecção, resposta e remediação de ameaças usando IA avançada.

3

Biometria Aprimorada

Uso de biometria avançada e tecnologias de reconhecimento para autenticação mais segura.

4

Segurança Descentralizada

Adoção de tecnologias blockchain e descentralizadas para melhorar a segurança e privacidade.



Conclusão: Um Chamado à Ação

À medida que concluímos nossa jornada através do vasto mundo das ferramentas de segurança cibernética, é crucial lembrar que a segurança é uma responsabilidade compartilhada. Cada indivíduo, organização e nação tem um papel a desempenhar na construção de um ciberespaço mais seguro e resiliente.

Continue aprendendo, adaptando-se e contribuindo para o campo da segurança cibernética. Seu conhecimento e habilidades são essenciais para enfrentar os desafios em constante evolução do mundo digital. Juntos, podemos criar um futuro digital mais seguro para todos.

