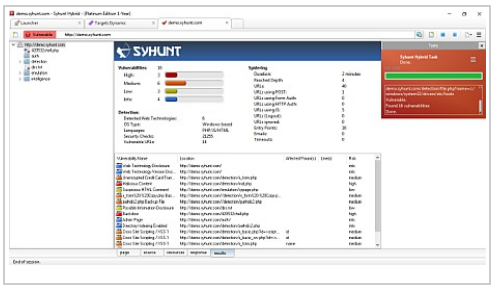
SYHUNT (HYBRID)

SCANNER DE SEGURANÇA PARA APLICAÇÕES WEB

Syhunt Hybrid® (formalmente conhecido como o scanner Sandcat) é uma ferramenta híbrida de avaliação da segurança de aplicações web para múltiplas linguagens. Através da combinação de diferentes abordagens, o Syhunt protege sites pró-ativamente contra ameaças de segurança nas aplicações, simulando ataques e rapidamente localizando as vulnerabilidades existentes antes dos hackers.

UM SCANNER METADE DINÂMICO, METADE ESTÁTICO

Com o Syhunt Hybrid, você pode:



- Realizar testes de penetração em websites, escanear aplicações web em funcionamento por múltiplas classes de vulnerabilidades - uma abordagem conhecida como caixa-preta, que se equivale a perspectiva de um hacker.
- Realizar o scan do código-fonte das aplicações buscando os mesmos tipos de vulnerabilidades - uma revisão interna do código (também conhecida como caixa-branca).
- Combinar ambas as abordagens, realizando o que é conhecido como análise híbrida (ou caixa-cinza)
- Realizar mais de **1500** verificações nas aplicações, com uma cobertura de mais de **100** tipos de ataques de segurança e todos os tipos de bancos de dados.

SCANNER DINÂMICO

O Syhunt injeta dinamicamente dados nas aplicações e analisa sua resposta para determinar se o código está vulnerável, automatizando o teste de segurança e defendendo de maneira pró-ativa a infraestrutura Web de sua organização contra diversos tipos de ameaças de segurança. Inclui um mapeador de sites que reconhece HTML5 e executa JavaScript.

SCANNER DE CÓDIGO-FONTE

Projetado para analisar aplicações web por diversos tipos de problemas, como Cross-Site Scripting (XSS), Inclusão de Arquivos, Injeção de SQL, Execução de Comandos e validação fraca, o scanner de código é um complemento perfeito para o já extenso conjunto de capacidades de auditoria presentes no scanner dinâmico da Syhunt.

COBERTURA DE TODOS OS ASPECTOS DA SEGURANÇA

Com o Syhunt Hybrid, digitando um simples URL, você pode:

- Detectar mais de **5700** vulnerabilidades em mais de 70 categorias de ataques, incluindo:
- XSS (Cross-Site Scripting), Injeção de SQL, Inclusão de Arquivos, Execução de Comandos, e etc.
- as Dez Vulnerabilidades Mais Críticas de Segurança em Aplicações, as Cinco Principais Vulnerabilidades de PHP e outras listas do OWASP.
- Realizar milhares de verificações dinâmicas adicionais de vulnerabilidades que conhecidamente afetam aplicações ou servidores específicos.
- Realizar uma análise profunda (através de spidering), mapeando de maneira automática e completa a estrutura de um website e executando verificações através de injeção e força bruta de diretórios.
- Testar qualquer tipo de aplicação web.

Através da simples seleção de um diretório contendo código-fonte, você pode:

- Detectar mais de **1300** vulnerabilidades de código-fonte, cobrindo 21 tipos de ataques de segurança.
- Realizar o scan do código-fonte de aplicações escritas em ASP.NET (C# & VB.Net), Java (JEE / JSP), JavaScript, Node.js, Lua, Perl, PHP, Python e Ruby por vulnerabilidades.
- Identificar áreas chave do código, como tags chave de HTML, JavaScript, requisições XHR, pontos de entrada e palavras-chave interessantes

Algumas das principais tecnologias suportadas pelo Syhunt Hybrid:

RELATÓRIOS DETALHADOS

O Syhunt Hybrid vem com a habilidade de criar relatórios contendo todos os detalhes sobre as vulnerabilidades identificadas. Depois de examinar a resposta da aplicação aos ataques, se um ponto alvo é confirmado como vulnerável, ele é adicionado ao relatório. Os relatórios do Syhunt também possuem gráficos, estatísticas e informações sobre conformidade com padrões - um conjunto de modelos de relatórios desenvolvidos para diferentes tipos de audiência está disponível no produto.

O relatório completo do Syhunt normalmente inclui:

- Informações completas de vulnerabilidades com referências - CVE, NVD, CWE, Bugtraq e OSVDB
- Informações de vetores e pontuação de CVSS3/CVSS2.
- Comparação - Evolução das vulnerabilidades com o tempo através da comparação com resultados de análises executadas anteriormente.
- Informações sobre conformidade - Como por exemplo relacionadas com o Top 10 do OWASP, Top 5 de PHP, Top 25 do CWE/SANS, o padrão PCI DSS, e etc.

Atualmente, o Syhunt Hybrid é capaz de gerar relatórios e exportar os resultados nos mais diversos formatos - incluindo HTML, PDF, XML, texto, CSV, RTF, XLS, DOC e NBE. Os resultados de um scan podem ser convertidos a qualquer momento para HTML ou múltiplos formatos disponíveis, e comparados para determinar vulnerabilidades novas, que continuam presentes ou que foram remediadas.

SUPORTE AO CVSS

O Syhunt Hybrid vem com suporte completo ao CVSS (Common Vulnerability Scoring System), um padrão da indústria criado para comunicar a gravidade de uma vulnerabilidade e ajudar a determinar a urgência e prioridade da resposta. Quando um relatório é gerado, as vulnerabilidades são ordenadas com base na pontuação de CVSS3.

VERIFICAÇÃO DAS PRINCIPAIS VULNERABILIDADES

O Syhunt Hybrid permite que você realize scans que identificam as principais vulnerabilidades usadas por hackers para comprometer aplicações web.

DEZ MAIS DO OWASP

As Dez Mais do OWASP é uma lista de vulnerabilidades que necessitam de remediação imediata. Códigos existentes devem ser verificados por estas vulnerabilidades de maneira imediata, já que estas falhas estão sendo ativamente exploradas por invasores. A Fundação OWASP encoraja as empresas a adotarem as Dez Mais do OWASP como um padrão mínimo para tornar aplicações web seguras.

VINTE MAIS DO SANS

As Vinte Mais do SANS incluem instruções passo-a-passo e links para informações adicionais úteis para corrigir falhas de segurança. O Instituto SANS atualiza a lista e as instruções na medida em que mais ameaças críticas e mais métodos de proteção atuais e convenientes são identificados. É um documento de consenso da comunidade.

AUDITORIA DE CONFORMIDADE

O Syhunt Hybrid pode ajudar sua organização a lidar com os problemas de conformidade mais urgentes, como:

- Ato de Portabilidade e Responsabilização do Seguro de Saúde (HIPAA)
- Gramm-Leach-Bliley (GLBA)
- Padrão PCI de Segurança de Dados (Payment Card Industry)
- CA-SB1
- Sarbanes-Oxley

CVE E CWE

O scanner da Syhunt suporta de maneira completa o CVE (Exposições e Vulnerabilidades Comuns) e o CWE (Enumeração de Fraquezas Comuns), sendo capaz de identificar as principais entradas CWE relacionadas com aplicações web. O Syhunt também está na lista de produtos e serviços compatíveis com CVE da Mitre Corporation, que desenvolveu o padrão.

> “...a melhor ferramenta de auditoria de segurança de aplicações web atualmente no mercado. Rapidamente atualizada e muito fácil de usar.
>
> **Robert Davies, CEO, Stealth-ISS, EUA**

> “...uma das ferramentas mais eficazes e valiosas no mercado hoje.
>
> **Matt McDermott, Engenheiro de Segurança II, Solutionary, EUA**

Para mais informações sobre a Syhunt, visite **www.syhunt.com.br**