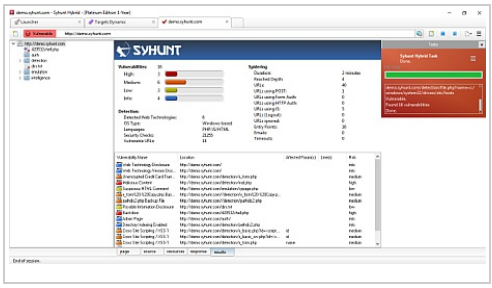
# ../SYHUNT/DYNAMIC

## SCANNER DE SEGURANÇA DE APLICAÇÕES WEB

**Syhunt Dynamic® (formalmente conhecido como o scanner Sandcat) é um scanner de segurança de aplicações web que automatiza de forma completa os testes de segurança, protegendo de maneira pró-ativa a infraestrutura e aplicações Web de sua organização contra todos os tipos de ameaças.**

## CARACTERÍSTICAS PRINCIPAIS



**Com o Syhunt Dynamic, digitando um simples URL, você pode:**

- Realizar mais de **800** verificações dinâmicas 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.

### MAPEADOR PROFUNDO

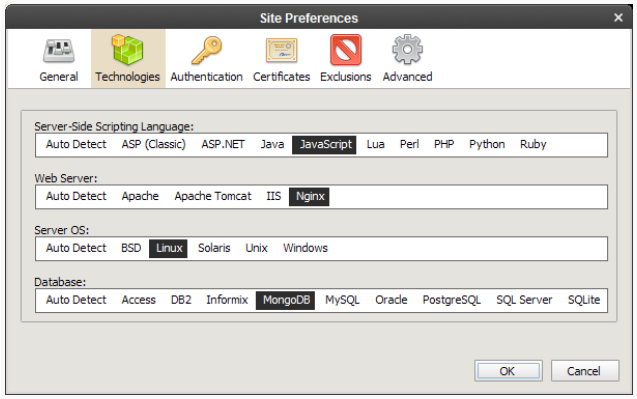
O Syhunt Dynamic mapeia completamente a estrutura do website (todos os links, formulários, requisições XHR e outros pontos de entrada) e localiza vulnerabilidades únicas da aplicação através da simulação de um conjunto amplo de ataques e do envio de milhares de requisições.

### INJETOR AVANÇADO

Testa por Injeção de SQL, XSS, Inclusão de Arquivos e muitas outras classes de vulnerabilidade de aplicações web. Enquanto realiza uma auditoria, o Syhunt Dynamic injeta dados nas aplicações web para em seguida analisar a resposta da aplicação e determinar se o código da aplicação está de fato vulnerável.

# ANALISE QUALQUER TIPO DE AMBIENTE WEB

O Syhunt Dynamic oferece o grau de flexibilidade necessário para suportar qualquer ambiente web, em qualquer lugar. Ele foi projetado para lidar de forma inteligente com sites grandes e complexos, adaptando-se automaticamente a diferentes ambientes e tecnologias da web. Enquanto navega pelo website alvo e caça vulnerabilidades, o Syhunt Dynamic emula um navegador moderno, com suporte ao HTML 5, garantindo que toda aplicação web seja completamente testada. Tal extenso conjunto de recursos para a emulação de navegador inclui:




- Análise inteligente de HTML (lida até mesmo com HTML deformado como um navegador faria)
- Emulação de JavaScript (capacidade de se comportar como Chrome, Firefox e IE), com suporte para requisições XHR
- Simulação de interação do usuário (pressionar de teclas, cliques de mouse, etc)
- Compatível com HTML 5 e CSS 3
- Preenchimento automático de formulários e login
- Isolamento de processos/Escaneamento Multi-Processo (cada escaneamento de website que você inicia é um processo diferente no seu sistema operacional)
- Suporte de cookies
- Suporte de HTTPS (SSL 2/SSL 3/TLS 1)
- Suporte de Certificados
- Suporte de autenticação básica & NTLM
- Suporte de HTTP 1.0 e 1.1
- Suporte de Keep-Alive
- Suporte de redirecionamento de HTTP

**Algumas das principais tecnologias suportadas pelo scanner Syhunt Dynamic:**

HTML JS Java ASP.NET php mongoDB.

## RELATÓRIOS DETALHADOS

O Syhunt Dynamic vem com a habilidade de criar relatórios contendo todos os detalhes sobre as vulnerabilidades localizadas. 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. Um 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 em diversos formatos - incluindo HTML, PDF, XML, texto, CSV, RTF, XLS, DOC e NBE. Os resultados podem ser convertidos a qualquer momento para HTML ou múltiplos formatos disponíveis, e comparados para determinar vulnerabilidades novas, que continuam presentes ou que foram removidas.

## 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

### CVE E CWE

O Syhunt Dynamic 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

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.

> Foi capaz de descobrir um número de vulnerabilidades de injeção de SQL e XSS que teríamos perdido se fizessemos testes manuais

**Arthur Donkers, Security Officer**

> Ferramentas como o Syhunt tornam uma vulnerabilidade na aplicação muito simples de se detectar, não mais exigindo um conjunto de habilidades de nível hacker.

**SC Magazine**

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