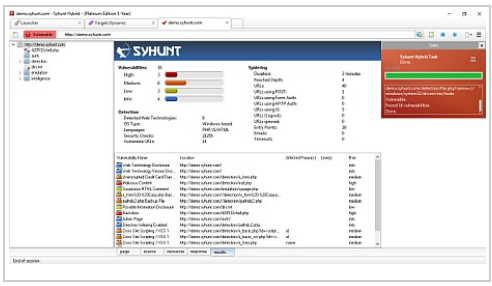
SYHUNT

DYNAMIC AUGMENTED



O Syhunt Dynamic Augmented 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, incluindo ataques inferenciais, in-band e out-of-band através de Análise Dinâmica Aumentada.

ANÁLISE DINÂMICA DA SEGURANÇA

- **5700+** vulnerabilidades em aplicações web em mais de 70 categorias, incluindo ataques **inferenciais**, **in-band** e **out-of-band** que detectam vulnerabilidades invisíveis.
- Testa qualquer tipo de aplicação web em funcionamento, em especial aplicações escritas em **ASP.Net (C# & VB.Net), Java (JEE / JSP), JavaScript, Node.js, Lua, Perl, PHP, Python & Ruby**, realizando um teste completo de penetração na camada web.
- **Mapeamento profundo** (através de spidering), automático e completo da estrutura de um website, reconhecendo os pontos de entrada (links, formulários, requisições XHR, etc), com suporte para **HTML5** e **JS**
- Otimizado para testar sites com frameworks diversas, rodando em servidores (**Apache, Tomcat, IIS, Nginx**, etc) e plataformas diversas (Windows, Unix, etc).

COBERTURA E INTEGRAÇÕES

- Verifica pelas Dez Vulnerabilidades Mais Críticas de Segurança em Aplicações, Top 5 de PHP e outras listas do OWASP, XSS (Cross-Site Scripting), Injeção de SQL, Inclusão de Arquivos, Execução de Comandos, e mais, via análise estática ou dinâmica.
- Reconhece vulnerabilidades de SQL envolvendo os principais tipos de bancos de dados.
- Compatível com o **GitHub**, **GitLab**, **Jenkins** e **JIRA**para Integração Contínua e rastreamento de bugs, **Imperva**, **F5 BIG-IP ASM** e **ModSecurity** para correção virtual de falhas.

ANÁLISE DINÂMICA AUMENTADA

- Detecta variantes **invisíveis** (out-of-band) de vulnerabilidades como Execução de Comandos, Inclusão Remota de Arquivos, Falsificação de Requisição do lado do servidor, Injeção de SQL e de XXE.
- Tais vulnerabilidades não são detectadas por ferramenta de DAST convencional.
- Observa requisições forçadas provenientes de um servidor web vulnerável ao longo de uma varredura.
- Demonstra a exfiltração de dados de um servidor web vulnerável alvo de análise.
- Retorna **zero falsos positivos**.

GERAÇÃO DE RELATÓRIOS

- Cria relatórios contendo todos os detalhes sobre as vulnerabilidades identificadas, gráficos, estatísticas, referências **CVE, CWE** e vetores de **CVSS3**, que comunicam a gravidade das vulnerabilidades e ajudam a determinar a urgência e prioridade da resposta.
- Informações sobre conformidade relacionadas com o Top 10 do OWASP, Top 5 de PHP, Top 25 do CWE/SANS, WASC Threat Classification, o padrão PCI DSS, e etc.
- Acompanhamento da evolução das vulnerabilidades.
- Suporte para os formatos de arquivo mais utilizados, incluindo **HTML, PDF, JSON, XML, texto** e **CSV**.

Para mais informações sobre o Syhunt, visite:

www.syhunt.com.br