



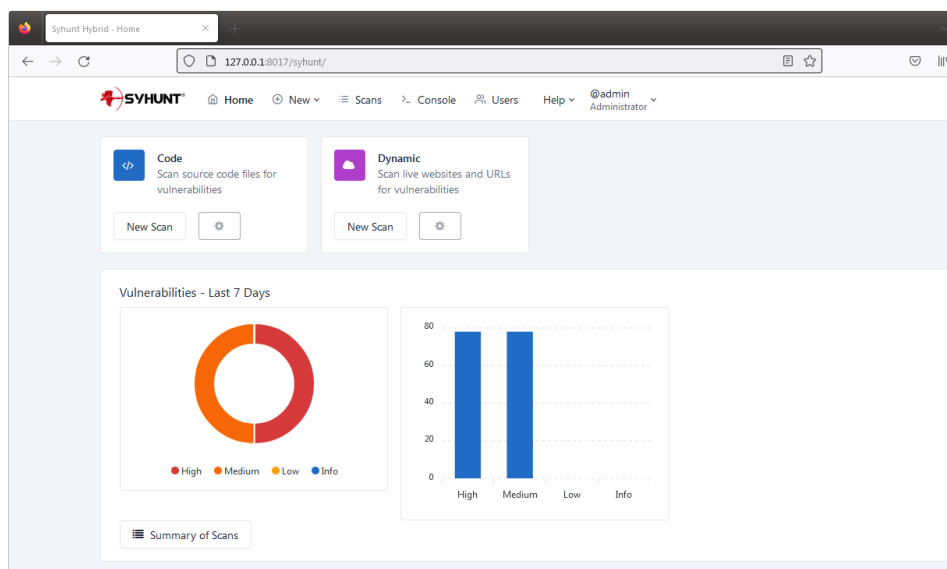
SYHUNT HYBRID: WEB UI

As informações contidas neste documento se aplicam a **versão 7.0.11** do Syhunt Hybrid.

INTRODUÇÃO

A partir da versão 7.0.11, o Syhunt Hybrid vem com uma interface de usuário web e uma API REST que pode ser habilitada em máquinas Windows ou Linux. Embora ainda em evolução, a web UI permite iniciar varreduras DAST, SAST e MAST, visualizar resultados de varreduras (incluindo aquelas iniciadas por meio da GUI, CLI, API REST e agendador, se houver), gerar relatórios e exportações, gerenciar usuários, permissões de usuário e sessões ativas, execute comandos do console e muito mais. A interface web e os relatórios estão atualmente disponíveis em 8 idiomas – inglês, alemão, espanhol, francês, italiano, japonês, coreano e português.

A interface web Syhunt Hybrid foi construída sobre um servidor web robusto - Openresty (Nginx + Lua), usa Bcrypt com um alto fator para hashing de senha, geração segura de ID de sessão e implementa proteção de login contra força bruta.



ATIVANDO A INTERFACE WEB UI

1. Se você estiver em um servidor Linux headless, como Ubuntu Server ou CentOS Minimal, **ative um display e faça com que ele inicie automaticamente na inicialização.**

2. Abra o prompt de comando ou terminal e vá para o local da CLI do Syhunt - a **localização padrão depende do seu sistema operacional**.
3. Configure as principais contas de usuário - a web UI está atualmente no modo preview e permite apenas dois usuários: admin e demo.
 1. Execute o seguinte comando para definir a senha do administrador: **scancore -pwdset:admin**
 2. (Opcional) Execute o seguinte comando para definir a senha da conta demo: **scancore -pwdset:demo**
4. Execute o servidor: **scancore -apisignal:start**
5. Agora você pode acessar a web UI e fazer login em: **http://127.0.0.1:8017/syhunt/** e também usar a **Syhunt REST API**.

ETAPAS ADICIONAIS

1. Em qualquer Linux, se você planeja executar SAST e MAST, certifique-se de que **habilitou as extensões Hybrid Plus**.
2. **Auto-run** - No Windows, uma vez definida a senha do administrador, a web UI é iniciada sempre que o serviço Hybrid Scheduler é iniciado. Isso garante que a web UI continue em execução mesmo que o usuário atual efetue logout. No Linux, use o serviço **cron** para agendar a inicialização do servidor.

CONFIGURANDO FUNÇÕES DE USUÁRIO

Quando você está logado como Administrador, você pode alterar a função de qualquer usuário para Operador, Operador Restrito ou Visualizador. A seguir estão as funções existentes:

- **Administrador** - O administrador pode iniciar e visualizar os resultados de todas as verificações iniciadas, editar as permissões e preferências do usuário e executar comandos do console. Atualmente, apenas uma conta de administrador é permitida.
- **Operador** - Um usuário com esta função pode iniciar e visualizar os resultados de todas as varreduras iniciadas.
- **Operador Restrito** - Um usuário com esta função pode iniciar varreduras, mas apenas visualizar os resultados das varreduras iniciadas por ele mesmo.
- **Visualizador** - Um usuário com esta função pode visualizar os resultados de todas as varreduras iniciadas, mas não é capaz de iniciar nenhuma varredura.

EXPONDO A UI DA WEB COM SEGURANÇA

Como o servidor web UI do Syhunt vem pré-configurado e é atualizado toda vez que o Syhunt é atualizado, não é aconselhável modificar suas configurações. Se você precisar expor a UI da web à Internet ou intranet,

recomendamos configurar um proxy Nginx reverso com SSL habilitado. Você precisará gerar um certificado.crt e uma chave privada para ser usado com ele - as instruções abaixo pressupõem que você já tenha os certificados prontos.

No Windows:

1. Baixe o Nginx para Windows: <http://nginx.org/en/download.html>
2. Aplique as alterações de configuração do Nginx nginx.conf descritas abaixo.

No Linux:

1. Instale o Nginx:
 1. No Ubuntu: **sudo apt install nginx**
 2. No CentOS 7: **sudo yum install nginx**
 3. No CentOS 8: **sudo dnf install nginx**
2. Edite o arquivo de configuração do Nginx: **sudo nano /etc/nginx/nginx.conf**
 1. Comente as linhas: **include /etc/nginx/conf.d/*.conf;** e **include /etc/nginx/sites-enabled/;**
 2. Dentro da seção http inclua:

```
server {  
    listen 443 ssl;  
  
    server_name syhuntwebui;  
  
    ssl_certificate /path/to/ssl/certificate.crt;  
    ssl_certificate_key /path/to/ssl/private.key;  
  
    location / {  
        proxy_pass http://127.0.0.1:8017;  
        proxy_set_header Host $host;  
        proxy_set_header X-Real-IP $remote_addr;  
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
        proxy_set_header X-Forwarded-Proto $scheme;  
    }  
}
```

1. Após salvar as alterações, teste a nova configuração: **nginx -t**
2. Permitir tráfego de localhost para a porta 8017 e permitir tráfego de entrada na porta 443:
 1. No Ubuntu:
 1. **sudo ufw allow from 127.0.0.1 to any port 8017**

2. **sudo ufw allow 443**

2. No CentOS:

1. **sudo firewall-cmd --zone=public --add-port=443/tcp**
2. **sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="127.0.0.1" port port=8017 protocol=tcp accept'**
3. **sudo firewall-cmd --reload**

3. Reinicie o servidor Nginx: **systemctl restart nginx**

ATIVANDO O DISPLAY NO HEADLESS LINUX

Se você estiver executando o Ubuntu Server, CentOS Minimal ou outra distribuição Linux headless, antes de tentar iniciar uma varredura através da interface da web ou gerar um relatório em PDF, você precisará instalar e iniciar o xvfb - caso contrário, o Syhunt irá travar enquanto gera um relatório em PDF ou durante a execução de uma varredura.

1. Instale o xvfb:

1. Servidor Ubuntu: **sudo apt-get install xvfb**
2. CentOS 8/7: **sudo yum install xorg-x11-server-Xvfb**
3. RH8: <https://stackoverflow.com/a/65311975>

2. Inicia a exibição do xvfb em uma porta de exibição específica - este exemplo usa a porta 99: **Xvfb :99 &**
3. Diga à sessão do terminal para usar a porta de exibição: **export DISPLAY=:99**
4. Teste a geração do relatório PDF: **./scanurl sometarget.com -out:areport.pdf**

Finalmente, para ter esta tela sempre disponível, você deve configurá-la para iniciar automaticamente na inicialização:

1. Crie um arquivo chamado **/etc/systemd/system/Xvfb.service** com o seguinte conteúdo:

[Unit]

Description=X Virtual Frame Buffer Service

After=network.target

[Service]

ExecStart=/usr/bin/Xvfb :99 -ac -screen 0 1024x768x16

[Install]

WantedBy=multi-user.target


1. Em seguida, habilite e inicie o serviço:
 1. **sudo systemctl ativar Xvfb**
 2. **sudo systemctl iniciar Xvfb**
2. Para finalizar, adicione a linha **export DISPLAY=:99** em **/etc/environment** para tornar a variável de ambiente DISPLAY persistente para todos os processos e usuários.

LIMITAÇÕES

- No Linux, as varreduras de código iniciadas por meio da web UI só podem ter como alvo repositórios GIT públicos. Se você precisar direcionar um repositório privado, use o **comando CLI scancode** para iniciar a varredura após configurar corretamente as credenciais do repositório ou chaves SSH. Além disso, a conexão direta com repositórios Azure TFS não está disponível para máquinas Linux.
- Embora a versão atual não inclua telas que permitem editar preferências globais do scanner ou preferências do site, se você estiver conectado como administrador, a tela do console permite visualizar e editar preferências usando o comando `[Docs.SyhuntIntegrationCLI#cli_prefs|scancore]`.
- No Linux, a geração de relatórios em PDF por meio da web UI não está disponível.

COMPATIBILIDADE COM DIFERENTES SISTEMAS OPERACIONAIS

- ✓ Windows 10 e Windows 11,
- ✓ Ubuntu (GUI) 23.10 e 22.04
- ✓ CentOS 7 (incluindo headless)
- ✓ MacOS Monterey 12.7.2 (Intel)

(*)  No Linux headless, se as varreduras iniciadas pela interface da web terminarem prematuramente no início - nesta situação, o status das varreduras muda de Varredura para Cancelado, então você precisa **habilitar um display**.

CONTATO

 **FALE CONOSCO**

