Relatório de Pentest - Vulnerabilidades Identificadas com Nikto

---

Data da Análise: 1 de abril de 2025
Endereço de IP do Alvo: 10.0.0.6/24 - Servidor Web
Porta: 8080
Versão do Nikto: 2.1.5
Serviço Web: Apache/2.4.10 (Debian) - DVWA

Visão Geral

Através da execução do Nikto, um scanner de vulnerabilidades, foi identificado um conjunto de possíveis falhas de segurança no servidor web hospedado no endereço IP 10.0.0.6, porta 8080. Algumas dessas vulnerabilidades podem expor o sistema a riscos de exploração, sendo essencial implementar correções e mitigação.

Vulnerabilidades Identificadas

1. **Cookie PHPSESSID Criado sem o Flag HttpOnly**
   - **Descrição**: O cookie PHPSESSID foi encontrado sem a flag `HttpOnly`. Isso significa que o cookie pode ser acessado via JavaScript, o que facilita ataques de XSS (Cross-Site Scripting) que visem roubar sessões do usuário.
   - **Recomendação**: Configurar o servidor para adicionar a flag `HttpOnly` aos cookies de sessão para evitar o acesso via scripts.
2. **Ausência do Cabeçalho X-Frame-Options (Anti-Clickjacking)**
   - **Descrição**: O cabeçalho `X-Frame-Options` não foi encontrado na resposta HTTP, o que permite que a página seja carregada dentro de um iframe. Isso torna o site vulnerável a ataques de Clickjacking.
   - **Recomendação**: Adicionar o cabeçalho `X-Frame-Options` com valor `DENY` ou `SAMEORIGIN` para prevenir ataques de Clickjacking.
3. **Redirecionamento para login.php**
   - **Descrição**: A página raiz (`/`) realiza um redirecionamento para `login.php`, sugerindo que há uma área de login exposta que pode ser alvo de ataques de brute-force ou outras tentativas de exploração.
   - **Recomendação**: Garantir que o mecanismo de login esteja protegido com autenticação forte e implementações adequadas de controle de acesso.
4. **Divulgação de ETags com Inodes**
   - **Descrição**: O servidor web está vazando inodes através do cabeçalho `ETag`, o que pode fornecer informações sobre a estrutura de arquivos internos do servidor.
   - **Recomendação**: Configurar o servidor Apache para desabilitar ou modificar a geração de ETags que incluam inodes, de modo a proteger informações sensíveis do sistema de arquivos.
5. **Indexação de Diretórios de Configuração e Documentação**
   - **Descrição**: O servidor apresenta diretórios com indexação habilitada, como `/config/` e `/docs/`, que podem expor arquivos de configuração ou documentação sensível.
   - **Recomendação**: Desabilitar a indexação de diretórios no servidor Apache e revisar a configuração para garantir que diretórios sensíveis não sejam acessíveis.
6. **Arquivo `README` Padrão do Apache Encontrado**
   - **Descrição**: O arquivo `README` padrão do Apache foi encontrado no diretório `/icons/`, o que pode fornecer informações sobre a instalação do servidor e possíveis vulnerabilidades.

- **Recomendação**: Remover arquivos de exemplo e documentação padrão do Apache, que podem fornecer informações úteis para um atacante.

7. **Página de Login Admin Acessível**
   - **Descrição**: A página `/login.php` foi identificada como uma página de login admin, o que pode ser um ponto de entrada crítico para ataques direcionados a privilégios administrativos.
   - **Recomendação**: Proteger a página de login com autenticação multifatorial (MFA) e limitar tentativas de login para evitar ataques de força bruta.

Outros Detalhes

- **CGI Directories**: Nenhum diretório CGI foi encontrado, mas a recomendação é usar o parâmetro `-C all` para realizar uma verificação mais profunda de possíveis diretórios CGI.
- **Robots.txt**: O arquivo `robots.txt` contém 1 entrada que deveria ser visualizada manualmente. O conteúdo desse arquivo pode fornecer pistas sobre áreas sensíveis ou ocultas do site.

Conclusões e Recomendações Gerais

O servidor web identificado apresenta diversas vulnerabilidades que podem ser exploradas para comprometer a segurança do sistema. A principal recomendação é realizar as configurações apropriadas no servidor Apache, como a habilitação de segurança em cookies, proteção contra clickjacking e a remoção de diretórios sensíveis. Além disso, é crucial realizar uma revisão mais aprofundada do código do servidor e aplicar práticas recomendadas de segurança.

Ações Prioritárias:

- Habilitar a flag `HttpOnly` para os cookies.
- Adicionar o cabeçalho `X-Frame-Options`.
- Remover a indexação de diretórios sensíveis.
- Desabilitar a geração de ETags com inodes.

Próximos Passos:

- Revisão do servidor Apache para garantir a configuração adequada.
- Testes de penetração mais aprofundados, com foco nas páginas de login e na exploração de diretórios sensíveis.
- Monitoramento contínuo da segurança do servidor para mitigar ataques futuros.

Data de Conclusão do Teste: 2025-04-01
Analista de Segurança: Silas Marques