Análise do Grau de Risco das vulnerabilidades

1. Cookie PHPSESSID Criado sem o Flag HttpOnly

Probabilidade de Exploração: Alta
Impacto: Alto (exposição de sessões de usuário pode levar ao roubo de credenciais e comprometer dados sensíveis) **Risco: Alto**

- **Justificativa:** A ausência da flag `HttpOnly` permite que o cookie seja acessado via JavaScript. Em ataques XSS, um atacante pode roubar sessões, o que leva a um possível comprometimento total da conta do usuário ou do administrador. Isso pode resultar em prejuízos financeiros diretos, como roubo de informações de pagamento ou dados sensíveis.

2. Ausência do Cabeçalho X-Frame-Options (Anti-Clickjacking)

Probabilidade de Exploração: Moderada
Impacto: Médio (ataques de clickjacking podem enganar usuários para executar ações não intencionadas) **Risco: Médio**

- **Justificativa:** Embora clickjacking possa ser utilizado para realizar ações não autorizadas em nome do usuário, o impacto financeiro não é tão direto quanto o roubo de sessões. No entanto, ataques que afetam a confiança do usuário ou comprometem a integridade do sistema podem gerar prejuízos à reputação e à segurança do sistema.

3. Redirecionamento para login.php

Probabilidade de Exploração: Alta
Impacto: Alto (se o login não for protegido adequadamente, pode levar a ataques de força bruta ou exploração de vulnerabilidades na autenticação) **Risco: Alto**

- **Justificativa:** O redirecionamento direto para a página de login pode ser explorado por atacantes para realizar ataques de força bruta. Se o login não for adequadamente protegido (como por autenticação multifatorial), isso pode resultar em compromissos críticos da conta de administração, levando a possíveis danos financeiros ou vazamento de dados sensíveis.

4. Divulgação de ETags com Inodes

Probabilidade de Exploração: Baixa
Impacto: Moderado (divulgação de informações internas pode facilitar outros ataques) **Risco: Médio**

- **Justificativa:** A divulgação de inodes pode fornecer informações sobre a estrutura de arquivos do servidor, mas não leva diretamente a um prejuízo financeiro. Contudo, pode ajudar um atacante a planejar outros ataques, o que pode gerar danos em longo prazo.

5. Indexação de Diretórios de Configuração e Documentação

Probabilidade de Exploração: Alta
Impacto: Alto (exposição de arquivos de configuração pode fornecer informações sensíveis sobre a infraestrutura do servidor) **Risco: Alto**

- **Justificativa:** Se os diretórios de configuração ou documentação contiverem informações sensíveis, como credenciais de acesso ou configurações de servidores, isso pode facilitar a exploração de outras vulnerabilidades no sistema. O impacto financeiro pode ser significativo se informações críticas forem comprometidas.

6. Arquivo README Padrão do Apache Encontrado

Probabilidade de Exploração: Baixa
Impacto: Baixo (informações sobre a instalação do servidor, mas geralmente não crítico) **Risco: Baixo**

- **Justificativa:** O arquivo README pode fornecer informações sobre a instalação do servidor, mas não é uma vulnerabilidade crítica que levaria diretamente a um prejuízo financeiro. No entanto, em um contexto mais amplo, isso pode ser parte de um conjunto de informações que ajudam um atacante.

7. Página de Login Admin Acessível

Probabilidade de Exploração: Alta
Impacto: Muito Alto (se um atacante conseguir comprometer a conta de administrador, isso pode resultar em controle total do sistema) **Risco: Muito Alto**

- **Justificativa:** A página de login do admin acessível sem proteções adequadas é uma vulnerabilidade crítica. Ataques direcionados a contas administrativas podem resultar em comprometimento total do sistema, levando a prejuízos financeiros severos, como perda de dados, roubo de informações sensíveis, e controle total do sistema.

8. CGI Directories

Probabilidade de Exploração: Moderada
Impacto: Moderado (potencial para exploração se diretórios CGI não forem devidamente configurados) **Risco: Médio**

- **Justificativa:** Embora os diretórios CGI possam ser um alvo interessante para atacantes, a probabilidade de exploração depende da configuração do servidor. Em geral, se não configurado adequadamente, pode ser um ponto de entrada para explorar o servidor.

9. Robots.txt

Probabilidade de Exploração: Baixa
Impacto: Baixo (indicação de áreas sensíveis, mas sem exploração direta) **Risco: Baixo**

- **Justificativa:** Embora o conteúdo do `robots.txt` possa dar pistas sobre áreas sensíveis, em si, não representa uma ameaça direta, a menos que seja utilizado em conjunto com outras vulnerabilidades. O risco financeiro é baixo, mas pode ser uma parte de uma exploração mais ampla.

Resumo da Classificação de Risco (de maior para menor risco)

Vulnerabilidade	Probabilidade	Impacto	Risco	Justificativa (Resumo)
Cookie PHPSESSID sem HttpOnly	Alta	Alto	Alto	Permite roubo de sessão via XSS.
Ausência do Cabeçalho X-Frame-Options	Moderada	Médio	Médio	Pode permitir ataques de clickjacking.
Redirecionamento para login.php	Alta	Alto	Alto	Pode facilitar ataques de força bruta.
Divulgação de ETags com Inodes	Baixa	Moderado	Médio	Revela estrutura interna do servidor.
Indexação de Diretórios de Configuração	Alta	Alto	Alto	Pode expor credenciais e informações críticas.
Arquivo README do Apache	Baixa	Baixo	Baixo	Pode revelar detalhes da instalação do servidor.
Página de Login Admin Acessível	Alta	Muito Alto	Muito Alto	Risco crítico de comprometimento total.
CGI Directories	Moderada	Moderado	Médio	Se mal configurado, pode ser explorado.
Robots.txt	Baixa	Baixo	Baixo	Pode dar pistas sobre diretórios sensíveis.