



Relatório de Segurança do Sistema MECRED

Autores

Richard Fernando Heise Ferreira

UNIVERSIDADE FEDERAL DO PARANÁ

SETOR DE CIÊNCIAS EXATAS

DEPARTAMENTO DE INFORMÁTICA

CENTRO DE COMPUTAÇÃO CIENTÍFICA E

SOFTWARE LIVRE

Sumário

1	Introdução	2
2	Infraestrutura de Segurança do Departamento de Informática	3
2.1	Política Interna	3
3	Ferramentas Utilizadas	4
3.1	OWASP ZAP	4
3.2	SecurityHeaders.com	4
4	Resultados	5
4.1	ZAP	5
4.2	SecurityHeaders.com	6
5	Propostas de Melhoria	8
5.1	Infraestrutura Interna	8
5.2	Uniformidade dos Cabeçalhos HTTP	8

1. Introdução

A segurança das interfaces públicas (frontend) de serviços web é fundamental para a proteção de dados, a integridade das interações com usuários e a preservação da confiança em ambientes digitais. Embora camadas de backend geralmente concentrem mecanismos robustos de proteção, o frontend, por estar diretamente exposto a usuários e agentes externos, torna-se um alvo recorrente para ataques. Testar a segurança dessa camada é, portanto, essencial para identificar e mitigar riscos que possam comprometer tanto a funcionalidade do sistema quanto a privacidade e a segurança dos usuários.

Este relatório apresenta os procedimentos adotados e os resultados obtidos durante a análise de segurança da interface pública do frontend do MECRED. Seu objetivo é detalhar as vulnerabilidades encontradas e descrever as ações necessárias para reforçar a postura de segurança do serviço. Os resultados obtidos servirão de base para priorizar correções e orientar melhorias contínuas, assegurando a conformidade com os padrões de segurança e a resiliência frente a ameaças emergentes.

Ainda, parte do objetivo deste relatório é auxiliar no Objetivo 3, Meta 1 do plano de trabalho: Investigar mecanismos de detecção de ataques cibernéticos apropriados para a infraestrutura da plataforma existente e definir metodologia de testes periódicos, reforçando a segurança e a privacidade dos dados e usuários.

2. Infraestrutura de Segurança do Departamento de Informática

Antes da realização dos testes de segurança, é fundamental contextualizar a configuração atual da infraestrutura interna do Departamento de Informática, com ênfase nos mecanismos de proteção da rede local.

2.1 Política Interna

A rede do departamento é estruturada em torno de dois roteadores centrais: a máquina *roble*, que desempenha a função de roteador externo, e a *estrella*, responsável pelo roteamento interno. Em ambos os dispositivos são aplicadas regras de firewall, sendo utilizado o iptables na *roble* e o nftables na *estrella*. Esta última concentra as conexões da maioria das VLANs do Departamento de Informática, com exceção de algumas específicas que não vem ao caso. Por ser o roteador interno, a *estrella* é responsável por intermediar o tráfego de pacotes com endereços IP privados, os quais não são roteáveis fora da rede institucional.

Essa configuração assegura que acessos externos não autorizados sejam devidamente bloqueados pelas regras de firewall definidas, protegendo assim a integridade da rede interna do laboratório e, consequentemente, do projeto MECRED. No entanto, como o foco da análise não está na segurança da rede interna, os testes concentraram-se sobre os pontos de acesso expostos publicamente, em especial a interface web do sistema — o frontend, que é processado no navegador de cada usuário. O capítulo seguinte apresenta os testes realizados e as conclusões extraídas a partir da análise desse vetor de entrada.

3. Ferramentas Utilizadas

Neste capítulo estão apresentadas e descritas as ferramentas de teste utilizadas para assegurar a segurança do sistema.

3.1 OWASP ZAP

O ZAP (Zed Attack Proxy) é uma ferramenta amplamente utilizada para a identificação de vulnerabilidades em aplicações web, oferecendo recursos para testes de segurança tanto automatizados quanto manuais. Neste trabalho, foi realizada uma varredura automatizada por meio da interface gráfica da ferramenta. Esse tipo de varredura executa uma série de testes com o objetivo de detectar falhas como SQL Injection, Cross-Site Scripting (XSS), configurações inadequadas de cabeçalhos de segurança (como Content Security Policy - CSP), entre outras vulnerabilidades comuns.

3.2 SecurityHeaders.com

O SecurityHeaders.com é uma ferramenta online gratuita que permite analisar e avaliar os cabeçalhos de segurança HTTP configurados por um site. Esses cabeçalhos são fundamentais para reforçar a proteção contra ameaças como injeção de scripts (XSS), clickjacking, entre outras vulnerabilidades comuns em aplicações web. Para esta análise, foi utilizado o endereço mecred.mec.gov.br, cuja configuração foi inspecionada a fim de identificar possíveis melhorias na política de segurança aplicada pelo servidor.

4. Resultados

Este capítulo apresenta e analisa os resultados obtidos por meio das ferramentas descritas no capítulo anterior.

4.1 ZAP

A análise realizada com o ZAP revelou alguns alertas relacionados à configuração de cabeçalhos HTTP, que, em um primeiro momento, indicam possíveis vulnerabilidades na interface pública do sistema. A Figura 4.1 resume os alertas identificados, classificando-os por gravidade e atribuindo a cada um deles um nível de confiança — métrica utilizada pela ferramenta para indicar a probabilidade de o alerta representar uma vulnerabilidade real, e não um falso positivo.

		Confidence				
		User				
		Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	5 (29.4%)	2 (11.8%)	0 (0.0%)	7 (41.2%)
	Low	0 (0.0%)	2 (11.8%)	3 (17.6%)	1 (5.9%)	6 (35.3%)
	Informational	0 (0.0%)	0 (0.0%)	1 (5.9%)	3 (17.6%)	4 (23.5%)
	Total	0 (0.0%)	7 (41.2%)	6 (35.3%)	4 (23.5%)	17 (100%)

Figura 4.1: Resumo de alertas gerados pelo ZAP.

Entretanto, uma análise mais aprofundada dos resultados demonstra que nem todos os alertas representam riscos concretos para o sistema MECRED. Em diversos casos, tratam-se de decisões arquiteturais conscientes, adotadas para garantir a compatibilidade e o funcionamento da aplicação. Um exemplo é apresentado na Figura 4.2, que mostra cinco alertas referentes ao cabeçalho Content-Security-Policy (CSP). Embora o cabeçalho esteja presente, ele inclui a diretiva `style-src 'unsafe-inline'`, considerada insegura pela ferramenta. Essa

configuração, no entanto, é necessária para permitir a execução de estilos embutidos gerados automaticamente pelo framework Next.js durante o processo de renderização das páginas da aplicação. Assim, tais alertas podem ser classificados como falsos positivos.

Alert type	Risk	Count
CSP: Failure to Define Directive with No Fallback	Medium	17 (100.0%)
CSP: Wildcard Directive	Medium	17 (100.0%)
CSP: script-src unsafe-inline	Medium	17 (100.0%)
CSP: style-src unsafe-inline	Medium	17 (100.0%)
Content Security Policy (CSP) Header Not Set	Medium	12 (70.6%)
Cross-Domain Misconfiguration	Medium	1 (5.9%)
Missing Anti-clickjacking Header	Medium	10 (58.8%)
Cross-Domain JavaScript Source File Inclusion	Low	14 (82.4%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	14 (82.4%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	137 (805.9%)
Strict-Transport-Security Header Not Set	Low	138 (811.8%)

Figura 4.2: Alertas específicos referentes ao cabeçalho CSP.

Os demais alertas identificados apresentam risco baixo ou caráter apenas informativo. A maioria dessas ocorrências pode ser corrigida de forma simples, por meio de ajustes na configuração do proxy reverso.

4.2 SecurityHeaders.com

De maneira semelhante à ferramenta ZAP, foi utilizada uma solução online especializada na avaliação de cabeçalhos HTTP para identificar possíveis vulnerabilidades na camada de frontend da aplicação. A análise foi conduzida com base na inspeção dos cabeçalhos retornados pelo endereço `mecred.mec.gov.br`, e os resultados obtidos indicam que a plataforma está em

conformidade com as principais práticas de segurança recomendadas, tendo recebido a nota máxima de avaliação, classificada como A.

A resposta HTTP da aplicação revela a presença de importantes mecanismos de proteção. Entre eles, destaca-se o cabeçalho `Strict-Transport-Security`, configurado com a diretiva `max-age=31536000`; `includeSubDomains`, que reforça a obrigatoriedade do uso de conexões HTTPS e protege contra ataques de downgrade. Outro ponto relevante é a política definida pelo cabeçalho `Content-Security-Policy` (CSP), que impõe restrições sobre as origens de scripts, estilos, fontes, imagens e conexões. Apesar da inclusão da diretiva `'unsafe-inline'` em `script-src` e `style-src` — medida necessária para compatibilidade com o framework Next.js —, a política geral é bem estruturada e específica, abrangendo somente os domínios utilizados pela aplicação, como `plausible.c3sl.ufpr.br` e `api.mecred.c3sl.ufpr.br`.

A segurança também é reforçada pela presença do cabeçalho `X-Content-Type-Options`, com valor `nosniff`, que evita que navegadores realizem detecção de tipo de conteúdo (MIME sniffing), mitigando ataques baseados em execução indevida de arquivos. O cabeçalho `X-Frame-Options`, definido como `sameorigin`, protege a aplicação contra ataques do tipo *clickjacking*, restringindo seu carregamento em *iframes* de domínios externos.

Além desses, observam-se práticas adequadas no uso dos cabeçalhos `Cache-Control` e `ETag`, que contribuem para a otimização do desempenho da aplicação sem comprometer sua segurança. A presença dos cabeçalhos `Cross-Origin-Embedder-Policy`, `Cross-Origin-Opener-Policy` e `Cross-Origin-Resource-Policy` evidencia uma preocupação com o isolamento entre contextos de origem, protegendo contra vazamentos de dados entre diferentes abas ou janelas do navegador.

De maneira geral, a configuração atual dos cabeçalhos demonstra uma abordagem madura e consciente em relação à segurança na camada de apresentação da aplicação, atendendo às recomendações das principais ferramentas de análise automatizada.

5. Propostas de Melhoria

Nesta seção final deste relatório são apresentadas as ideias para tornar o sistema ainda mais robusto e seguro.

5.1 Infraestrutura Interna

Embora a configuração atual dos firewalls nos roteadores tenha se mostrado eficaz na mitigação de ataques, identificou-se a necessidade de um monitoramento mais detalhado do tráfego de rede recebido diariamente pelo Departamento. Nesse sentido, está em análise a implantação de um sistema de detecção de intrusões (IDS), com ênfase na análise estatística dos pacotes que atravessam o firewall. A adoção dessa solução viabilizará a geração de relatórios especializados em segurança, proporcionando uma visão mais aprofundada do comportamento da rede e permitindo a detecção proativa de anomalias e padrões suspeitos.

Cabe destacar que a segurança não se resume a uma implementação pontual, mas sim a um processo contínuo, minucioso e em constante evolução, ajustando-se progressivamente às demandas e vulnerabilidades identificadas ao longo do tempo — e o projeto MECRED não é uma exceção a essa regra.

Além disso, o C3SL conta com uma equipe interna de roots, composta por bolsistas responsáveis por atender às demandas de infraestrutura e segurança tanto dos projetos desenvolvidos no laboratório quanto do Departamento como um todo. Essa equipe encontra-se em constante processo de expansão e capacitação, com o objetivo contínuo de aprimorar sua atuação, garantir uma formação de excelência e contribuir para a melhoria da qualidade dos projetos executados.

5.2 Uniformidade dos Cabeçalhos HTTP

Apesar da adoção dos cabeçalhos de segurança mencionados anteriormente, a arquitetura atual do sistema pode ser aprimorada por meio da padronização dessas diretivas para os demais sistemas mantidos pelo C3SL, realizando os devidos ajustes conforme as particularidades de cada aplicação. Com esse objetivo, propõe-se a implantação do MECRED em um *pod* Kubernetes, o que permitirá maior controle sobre a infraestrutura e facilitará a aplicação uniforme de cabeçalhos HTTP seguros. Além disso, sugere-se a capacitação de bolsistas na configuração e manutenção dessas práticas, promovendo autonomia e sustentabilidade técnica no ambiente do laboratório.

Cabe ressaltar que segurança é um conceito abstrato, contínuo e processual, não se limitando à aplicação de soluções pontuais. A prática de testes recorrentes e a produção de relatórios

técnicos permitem a definição de padrões robustos, como os discutidos, que asseguram a consistência e a resiliência do sistema. Nesse sentido, planeja-se a adoção dessas diretrizes como parte da cultura organizacional do laboratório, de forma a garantir que a aplicação continue segura no futuro, assim como se encontra no presente.