Relatório Final de Auditoria

Apresentação do Sistema

No dia 16 de setembro de 2022 às 14 horas participei de uma reunião em conjunto com o auditor Marcelo Sampaio (perito), Ronaldo (Gerente de TI da OAB) e o fornecedor da aplicação para o entendimento do sistema e coleta de informações para a preparação de um roteiro de testes.

O Sistema foi explicado através de slides por aproximadamente 3 horas. Compreendi que o núcleo do sistema é o Helios (www.heliosvoting.org), um sistema de votação de código aberto, bastante utilizado em votações pequenas e com baixo nível de coerção. O sistema é bastante conhecido na comunidade e passou por diversas auditorias independentes que asseguram que para o modelo de ataque acima, Helios já foi avaliado por especialistas qualificados e por isso utilizado por grandes organizações, incluindo sociedades científicas e profissionais além de inúmeras Instituições de Ensino Superior. No Brasil, pode-se citar alguns exemplos de Instituições de Ensino Superior que usam o sistema Helios em eleições internas, tais como: Universidade de São Paulo (USP), Universidade de Campinas (UNICAMP), Universidade Federal de Santa Catarina (UFSC), Universidade Federal de Minas Gerais (UFMG), Universidade Federal da Grande Dourados (UFGD), Universidade Federal de São Carlos (UFSCar). Helios é usado também por Institutos Federais, tais como: Instituto Federal do Pará (IFPA), Instituto Federal de Goiás (IFG), Instituto Federal de Rondônia (IFRO), Instituto Federal de Minas Gerais (IFMG), Instituto Federal de Santa Catarina (IFSC), Instituto Federal Fluminense (IFF), entre outros. Organizações públicas como Defensoria Pública da União e Tribunal de Justiça de Minas Gerais além de sociedades científicas como Sociedade Brasileira de Computação (SBC) e a Associação Brasileira de Métodos Computacionais em Engenharia (ABMEC).

No que se refere à segurança da votação eletrônica o sistema protege o segredo do voto. A criptografia, nos mesmos moldes da tecnologia de serviços bancários, traduz a escolha do eleitor numa forma codificada antes de enviá-la ao servidor de dados, impedindo que o voto seja revelado de forma individualizada, alterado ou excluído. A cada eleição, o sistema envia uma mensagem automática para a conta de e-mail cadastrada, contendo o token de acesso para votação. O token enviado para cada eleitor não é de conhecimento de nenhum administrador do sistema, pois é gerada eletronicamente.

Testes

No dia 18 de Setembro de 2022 às 9 horas foi disponibilizado o ambiente de testes onde de imediato dei inicio a examinação do sistema começando às 9 horas e 10 minutos, testes nos quais enumero abaixo:

Teste 1 - Obter token de acesso do eleitor alterando os headers da requisição	
Objetivo	Manipular a url de envio do token do o e-mail para quando o eleitor clicar no token esse token ser enviado para o servidor controlado por outro usuario e assim obter acesso ao token do eleitor
Protocolo	Por meio de um proxy altero os headers Origin: https://oab-validation.votus.app e Referer: https://oab-validation.votus.app para Origin: https://meuservidor.com e Referer: https://meuservidor.com/
Resultado	A aplicação ignora os headers alterado e mantém seus headers originais fazendo com que o token chegue ao seu destino com segurança

Teste 2 - Burlar o painel de login e realizar a votação sem o token	
Objetivo	Conseguir logar na aplicação sem nenhum token de acesso e realizar a votação
Protocolo	Por meio de um proxy tento manipula o responde no qual troco {"success":false,"msg":"Credenciais inv\u00e1lidas para concluir sua solicita\u00e7\u00e3o."} por {"msg":"Autenticado com sucesso","success":true}
Resultado	A aplicação me redireciona para tela de login novamente

Teste 3 – Obter o token de acesso e credencias durante o envio para o backend	
Objetivo	Verificar se pessoas conectadas na mesma rede conseguem capturar credencias e o token do eleitor trafegando em rede
Protocolo	Ativo a ferramenta bettercap e monitoro todos os dados que estão sendo enviados na rede
Resultado	A aplicação utiliza um certificado seguro e dessa forma nem um dado apareceu no monitoramento apenas a sua url "https://oab-validation.votus.app/" , sendo possível verificar um comportamento normal.

Teste 4 – Capturar a identificação do eleitor e a identificação do voto durante a votação	
Objetivo	Verificar se pessoas conectadas na mesma rede conseguem capturar a identificação do eleitor e a identificação do voto, quebrando assim o sigilo do voto
Protocolo	Ativo a ferramenta bettercap e monitoro todos os dados que estão sendo enviados na rede
Resultado	A aplicação utiliza um certificado seguro e dessa forma nem um dado apareceu no monitoramento apenas a sua url "https://oab-validation.votus.app/" , sendo possível verificar um comportamento normal.

Teste 5 – Alterar os dados do eleitor	
Objetivo	Alterar dados do eleitor e se passar por ele no momento do voto, assim impedindo que o eleitor realize a votação.
Protocolo	Por meio de um proxy realizo a votação e capturo a requisição do voto antes dela ser enviada para o servidor
Resultado	A aplicação retorna um erro "{"success":false,"msg":"N\u00e3o autenticado."}" e é mostrado ao usuário a mensagem "Não autenticado"

Teste 5 – Alterar os dados do Voto	
Objetivo	Alterar dados do eleitor e se passar por ele no momento do voto, assim impedindo que o eleitor realize a votação.
Protocolo	Por meio de um proxy realizo a votação e capturo a capturo a requisição do voto antes dela ser enviada para o servidor
Resultado	A aplicação retorna um erro "{"success":false,"msg":"N\u00e3o autenticado."}" e é mostrado ao usuario a mensagem "Não autenticado"

Teste 6 – Votar em um mesmo candidato várias vezes	
Objetivo	Conseguir votar em uma única cédula, múltiplas vezes em um mesmo candidato
Protocolo	Por meio de um proxy recupero as informação de headers e body da sessão anterior na qual realizei todo procedimento de autenticação e votação e tento votar novamente no mesmo candidato.
Resultado	A aplicação retorna uma mensagem "Não foi possível acessar sua cédula de votação. Eleitor já votou"

Teste 7 – Votar várias vezes com o mesmo token (reutilização do token)	
Objetivo	Conseguir com o mesmo token votar várias vezes e o voto ser computado
Protocolo	Clico no botão votar no browser até chegar no login com o token e tento efetuar novamente o login, e também tento com um proxy mandibular o header e body de autenticação do token.
Resultado	A aplicação retorna uma mensagem “Não foi possível acessar sua cédula de votação. Eleitor já votou”

Teste 8 – Manter duas sessões utilizando browsers diferentes (Google Chrome, Mozilla Firefox)	
Objetivo	Manter duas sessões ativas e realizar votações múltiplas
Protocolo	Copio o link do token que recebi através do e-mail e uso um no “Google Chrome” e outro no “Mozilla Firefox”
Resultado	A aplicação teve dois comportamentos: • **Comportamento 1:** a aplicação automaticamente encerrou a sessão no browser Google Chrome e manteve a sessão no browser Mozilla Firefox e vise versa. • **Comportamento 2:** manteve as duas sessões mais no momento da votação gerou um erro com a mensagem “Não autenticado.” impedindo a votação pois o mesmo já votou no outro browser

Teste 9 – Fuzzing para identificar possíveis pontos de ataques e pastas públicas	
Objetivo	Localizar outros pontos que possam comprometer a votação e o sigilo do voto
Protocolo	Através da ferramenta feroxbuster tento buscar pastas ou arquivos que possam dar acesso ao banco de dados e ao Script de apuração, chaves e credencias que possam estar públicas
Resultado	A ferramenta retornou algumas pastas como “System/, Config/, controllers/, core/, helpers/, i18n/, libraries/, views/” nada que possa comprometer ou manipular a votação ou a aplicação, essas descobertas foram relatadas ao fornecedor e ele de imediatamente realizou as correções.

Análise do código

No dia 19/09/2022 às 14 horas dei inicio a análise do código junto com o fornecedor e o Ronaldo (gerente de TI da OAB), onde o fornecedor explicou em detalhes o funcionamento de cada linha de código, esse exame durou aproximadamente 4 horas, e não foram identificadas falhas óbvias, vícios ou funcionalidades suspeitas.

Parecer final

1. Considero que a arquitetura, a infraestrutura proposta nos slides, utilizando a AWS, é bastante robusta e escalável sendo teoricamente capaz de suportar o fluxo de votantes e possíveis ataques;
2. O representante da empresa, compreendia os principais vetores de ataque e as medidas de proteção;
3. Para o núcleo do sistema de votação, o fornecedor afirmou utilizar o Helios Voting. Que é um sistema de votação que já foi auditado diversas vezes, e que utiliza um modelo sólido de criptografia, atendendo perfeitamente para o tipo de votação da OAB;
4. Foram executados todos os testes e não foram encontrados problemas.

Considero que o sistema testado no dia 18 de Setembro de 2022 é seguro e será capaz de atender o pleito do Quinto Constitucional sem problemas.

Salvador, 20 de setembro de 2022

TÁSSIO CERQUEIRA DIAS

Engenheiro de cibersegurança