Security labs
Intelligent Research

LAUDO DE AUDITORIA

Laudo nº 003
Escopo: Auditoria de Códigos

Emissor: SECURITYLABS RESEARCH INTELLIGENCE
Endereço: SRTVN Qd. 702 BL. "P" Salas 2049/2050 Brasília - DF
CNPJ:11.046.341/0001-14

Empresa: CONSELHO NACIONAL DE TÉCNICOS EM RADIOLOGIA
Endereço: SRTVN 702, Bloco P, sala 2062 – Ed. Brasília Rádio Center, Brasília-DF.
CNPJ: 03.635.323/0001-40

Escopo de Auditoria:

Trabalhos de auditoria de código fonte de aplicação, programa denominado "Webvoto" com o objetivo de garantir a confidencialidade e confiabilidade das informações tais como senha, voto e resultado da apuração do processo eleitoral do Conselho Nacional de Técnicos em Radiologia, a ser realizado em 11 de maio de 2017.

Procedimentos utilizados:

I - Deste Laudo

O presente laudo técnico apresenta uma avaliação de aspectos de segurança de dados relativos ao software (aplicação) denominado "Webvoto" que será utilizado no dia 11 de maio de 2017, para realização das eleições do Conselho Nacional de Técnicos em Radiologia.

Em especial foi fixada a atenção sobre a garantia de sigilo, inviolabilidade do voto e da senha do eleitor, uma vez que os dados são digitados num computador conectado eletricamente à rede mundial de computadores (Internet) no momento do voto.

Para a elaboração deste laudo tivemos livre acesso aos códigos fontes do programa (aplicação), ou seja, este parecer técnico foi emitido a partir do resultado obtido após analises sucessivas e completas de códigos fontes e programas utilizados pela aplicação (programa de computador).

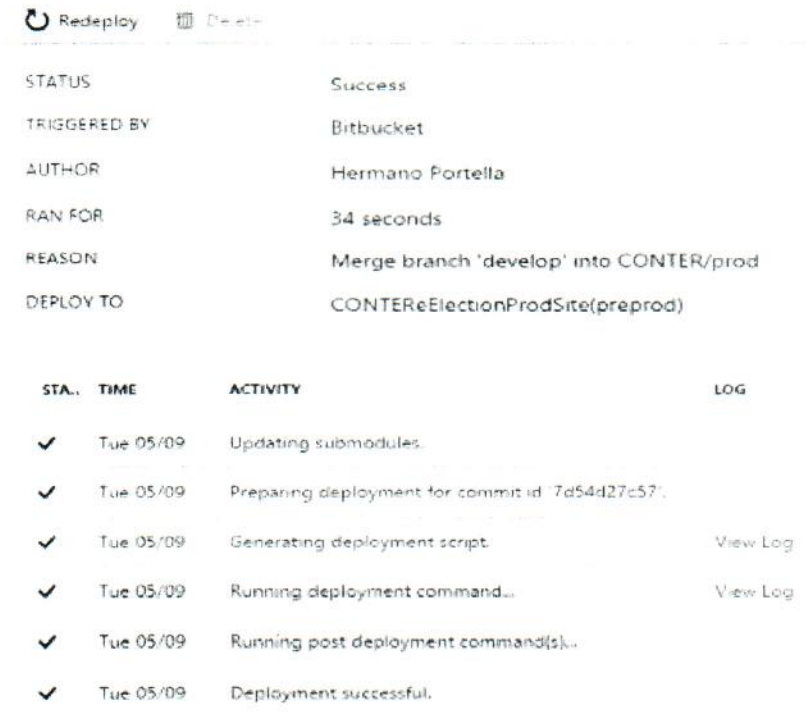
II – Da Transparência dos trabalhos

Os códigos-fontes da aplicação está a disposição dos candidatos participantes do processo eleitoral para análise por empresas independentes de auditoria e de confiança pessoal dos candidatos (pasta reservada na SCYTL, detentora da propriedade intelectual do programa).

A versão final auditada do programa (aplicação), códigos fontes é a versão com assinatura digital:

```
//
// File Checksum Integrity Verifier version 2.05.
//
                    MD5                                 SHA-1
-------------------------------------------------------------------------
6d6ac0ffdf5feab7f550cacfa8b84537
3b664b814a36f05589b955251b275a165f647624 wwwroot.zip
```

Que foram utilizados para gerar o binário (programa executável) instalado no Servidor de Aplicação (hardware) com HASH de DEPLOYMENT conforme imagem a seguir nos servidores Cloud Computing AZURE Microsoft.



SecurityLabs Intelligent Research
SRTVN Quadra 702 conj. P sala 2049/2050 Brasília – DF
CEP: 70.719-900 Telefone: (61) 3201-1096

Security labs
Intelligent Research

III – Do Trabalho

Os serviços de auditoria de código foram divididos em 03 (três) módulos conforme a seguir:

Módulo 1:
Busca de falhas em aplicação e que poderiam ser exploradas por atacantes danificando ou modificando o sistema e o resultado final das eleições.

Módulo 2:
Garantias ao eleitor de que o voto é secreto.

Módulo 3:
Garantias ao eleitor de que seu voto realmente foi computado para o candidato escolhido.

IV – Da Execução dos trabalhos

Módulo 1:
Busca de falhas em Aplicação e que poderiam ser exploradas por atacantes danificando ou modificando o sistema e o resultado final das eleições:

Por ser um processo eleitoral que utilizará a rede de computadores como base de seu desenvolvimento, uma página Web como camada de apresentação e trabalhará fundamentalmente sob a camada 7 do modelo OSI, sendo assim realizamos o processo de auditoria de segurança de aplicação utilizando testes específicos para aplicações Web incluindo os testes do TOP 10 OWASP, requisitos do PCI-DSS, ISO27001, entre outros.

Nesta etapa do projeto procuramos falhas específicas de aplicação, como erros de design e erros de programação tais como:

- SQL Injection;
- XPATH Injection;
- OS Command Execution;
- Senhas frágeis(brute force);
- Leak Informations;
- Input Validations;
- Race Conditions;
- XSS;
- XSRF;
- Ataques de Reflection;
- Erros em Criptografia;
- URL Redir;

- Iframe Injection;
- Ajax Hijacking;
- Session ID Brute Force;
- Session Hijacking;
- Cookie manipulations;
- Flaws in Web Services;

Resultado:
A aplicação, não apresenta nenhuma das falhas listadas acima.

Módulo 2:
Garantias ao eleitor de que o voto é secreto:

Premissa:
O voto é secreto e o sistema tem a obrigatoriedade de assegurar o sigilo e inviolabilidade do voto do eleitor.

Resultado:
Após analises e testes de inclusão de dados no sistema, verificamos que na versão assinada digitalmente não existe a possibilidade de rastrear o voto dos eleitores, ou seja, não há como associar um voto a um eleitor.

Módulo 3:
Garantias ao eleitor de que seu voto realmente foi computado para o candidato escolhido:

Foram realizadas com exaustão diversas análises nos códigos fontes da aplicação assinada digitalmente à procura de falhas ou códigos maliciosos que pudessem modificar o resultado das eleições.

Resultado:
A equipe de auditores da SecurityLabs Intelligent Research, não encontrou nada nocivo que pudesse manipular o resultado das eleições nos códigos fontes em nenhuma das versões auditadas e nem na versão assinada digitalmente neste laudo.

Laudo:

Desta forma entendemos que o processo eleitoral como foi projetado e executado oferece todas as garantias que o estado da arte permite quanto ao sigilo, inviolabilidade do voto e confiabilidade no resultado apurado pela aplicação no processo eleitoral do Conselho Nacional de Técnicos em Radiologia a ser realizado em 11 de maio de 2017.

A SecurityLabs Intelligent Research fica à disposição para auxiliar as empresas independentes de auditoria de sistemas que porventura venham a periciar o sistema por ordem do próprio Conselho Nacional de Técnicos em Radiologia por ordem da Justiça ou órgão competente.

Brasília, 09 de maio de 2017

Atenciosamente,

Waldemar Nehgme
Analista de segurança

SecurityLabs Intelligent Research
SRTVN Quadra 702 conj. P sala 2049/2050 Brasília – DF
CEP: 70.719-900 Telefone: (61) 3201-1096