LAUDO DE AUDITORIA

Laudo nº 001
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 FEDERAL DE PSICOLOGIA - CFP
Endereço: SAF Sul, Qd. 02 Lote 02 Bl. "B" Edifício Via Office, sala 104, Brasília/DF
CNPJ: 00.393.272/0001-07

Escopo de Auditoria:

Trabalhos de auditoria de código fonte de aplicação com o objetivo de garantir a confidencialidade e confiabilidade das informações tais como senha, voto e resultado da apuração do processo eleitoral do Conselho Federal de Psicologia – CFP, a ser realizado em 24 de agosto de 2016.

Procedimentos utilizados:

I - Deste Laudo

O presente laudo técnico apresenta uma avaliação de aspectos de segurança de dados relativos ao software (aplicação) que será utilizado no dia 24 de agosto de 2016, para realização das eleições do Conselho Federal de Psicologia - CFP.

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.

Em especial foi fixada a atenção sobre a garantia de sigilo, inviolabilidade do voto, unicidade do voto, senha do eleitor e resultado da apuração, uma vez que os dados são digitados num computador conectado eletricamente à rede mundial de computadores (Internet) no momento da validação e do voto quando da eleição OnLine e no momento da validação e do voto quando da eleição presencial com o uso de Urna.

Para a elaboração deste laudo tivemos livre acesso aos códigos fontes dos programas, ou seja, este parecer técnico foi emitido a partir do resultado obtido após analises sucessivas.

Security labs
Intelligent Research

II – Da Transparência dos trabalhos

Os códigos-fontes das aplicações estão 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 dos programas).

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
-------------------------------------------------------------------
a4bab9fe0fcbe81c4a1b64a974708d13      07eafccfc0e63cdba74792b8b742492c1f42d1fc
c:\temp\cfpeelectionprodsite\site.zip

//
// File Checksum Integrity Verifier version 2.05.
//
                MD5                                SHA-1
-------------------------------------------------------------------
7a4952eccea4d3103bbedf7def1ae307      4d7dfa2df5fe2a527c3ba60c78cd02422ba8a498
c:\temp\cfpeelectionprodsite\site\site\bin\scytl.eelection.site.dll

//
// File Checksum Integrity Verifier version 2.05.
//
                MD5                                SHA-1
-------------------------------------------------------------------
bdd032934617957d93089967ce503f4b      036c577f527544387bb095f016d10a2b85f7136c
c:\temp\cfpeelectionprodbo\fs\site\repository\backoffice\bin\scytl.eelection.backoffice.dll
```

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 final 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 Federal de Psicologia - CFP a ser realizado em 24 de agosto de 2016.

A SecurityLabs Intelligent Research fica à disposição para auxiliar a Justiça ou órgão competente.

Brasília, 12 de agosto de 2016

Atenciosamente,

Waldemar Nehgme Gonzalez
Analista de Segurança
SecurityLabs Intelligent Research

SecurityLabs – Intelligent Research
SRTVN Qd. 702, Conjunto "P" Salas 2049/2050 - CEP: 70.719-900
Brasília/DF - Tel: (61) 3201-1096