Relatório de Serviços

Escopo: Relatório de serviços de auditoria, processo eleitoral do Conselho Federal de Psicologia - CFP - 2019.
Brasília, 19 de setembro de 2019.

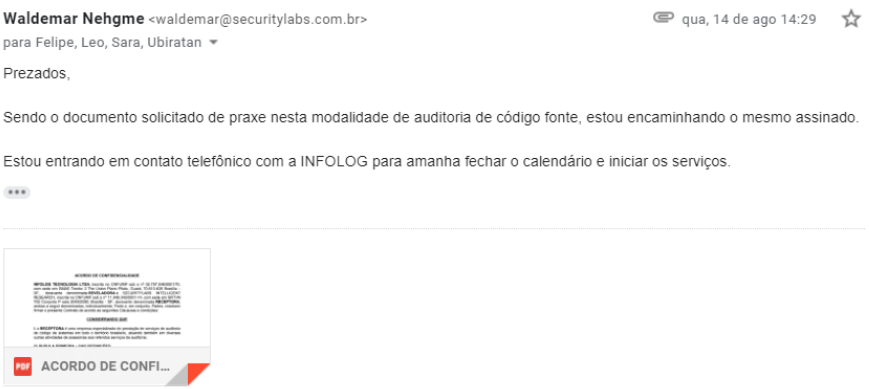
Emissor: SecurityLabs Intelligent Research
Endereço: SRTVN Qd. 702, Conjunto "P", Sala 2049, Brasília - DF
CNPJ:11.046.341/0001-14

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

De acordo com as exigências contratuais, estamos apresentando o relatório final da prestação de serviços referentes ao processo eleitoral do Conselho Federal de Psicologia - CFP - 2019.

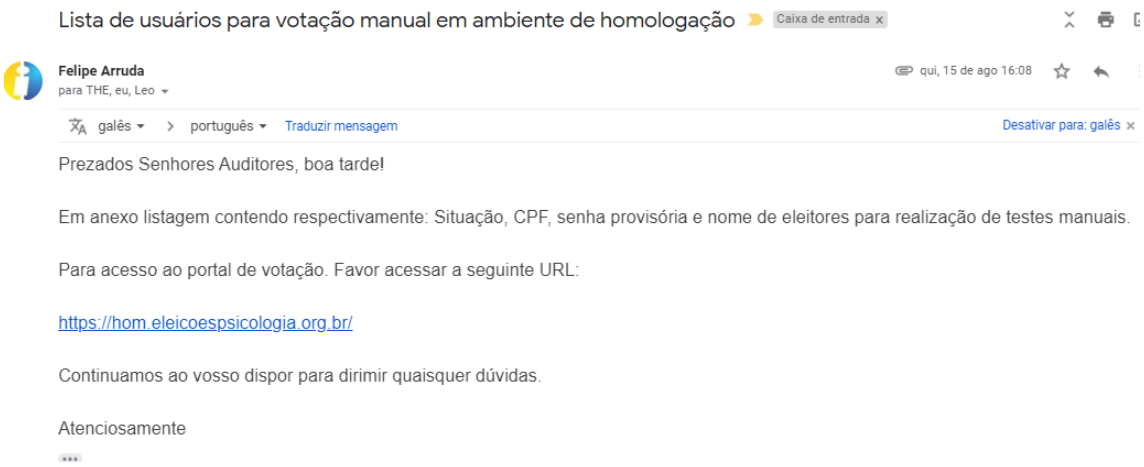
Da cronologia dos serviços:

1.- 14 de agosto de 2019:
Início dos serviços de auditoria de código fonte do sistema "Eleicaoweb"
Participantes:
SecurityLabs: Waldemar Nehgme, Henrique Matos
SCYTL: Ubiratan Soares, Coordenador de TI.
Entre os artefatos produzidos, assinatura do acordo de confidencialidade assinado entre as partes.



Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

2.- 15 de agosto de 2019:
Encaminhamento de lista para realização de testes manuais no ambiente web.


Lista de usuários para votação manual em ambiente de homologação Caixa de entrada x

Felipe Arruda
para THE, eu, Leo
qui, 15 de ago 16:08

galês > português Traduzir mensagem Desativar para: galês x

Prezados Senhores Auditores, boa tarde!

Em anexo listagem contendo respectivamente: Situação, CPF, senha provisória e nome de eleitores para realização de testes manuais.

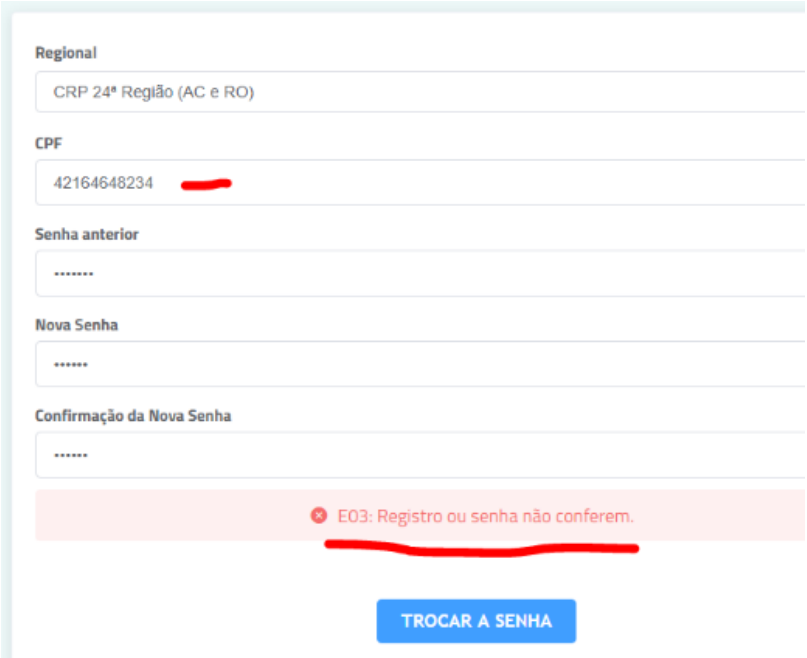
Para acesso ao portal de votação. Favor acessar a seguinte URL:

https://hom.eleicoespsicologia.org.br/

Continuamos ao vosso dispor para dirimir quaisquer dúvidas.

Atenciosamente

3.- 16 de agosto de 2019:
Testes realizados com a lista encaminhada em 15 de agosto de 2019, somente verificamos que quando um CPF Inapto tentar trocar a senha a mensagem que aparece é “E03-Registro ou senha não conferem” sendo que na verdade confere, porém está inapto.
Solicitamos mudança da mensagem, a empresa INFOLOG Tecnologia Ltda atendeu a solicitação..



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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

4.- 18 de agosto de 2019:
Fiscalização das etapas de implementação da topologia de redes implementada na AWS Amazon para atender os requisitos do processo eleitoral Conselho Federal de Psicologia - CFP 2019.
Participantes:
SecurityLabs: Waldemar Nehgme, Henrique Matos
INFLOG: Ubiratan Soares de Melo.

5.- 18 de agosto de 2019:
Testes de estresse do ambiente de produção, AWS Amazon.
Participantes:
SecurityLabs: Waldemar Nehgme, Henrique Matos
INFLOG: Ubiratan Soares de Melo.

6.- 21 de agosto de 2019:
Entrega de relatório de Teste de intrusão na aplicação “Eleicaoweb”.
Os serviços foram realizados entre os dias 16 e 21 de agosto de 2019 e o mesmo foi bem sucedido.
No workshop foram repassadas a empresa INFOLOG nossas recomendações para correção de problemas encontrados de forma a minimizar o GAP de segurança conforme relatório a seguir:

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

Security labs
Intelligent Research

RELATÓRIO
TESTE DE INTRUSÃO

ELEIÇÕES – CFP 2019

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

Sumário

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

1 SUMÁRIO EXECUTIVO

Foi realizado, durante o período de 16 a 21 de agosto de 2019, um serviço de teste de intrusão na aplicação WEB Eleições CFP e sua infraestrutura com o objetivo de encontrar potenciais vulnerabilidades e problemas de segurança na mesma, bem como testar sua resiliência frente a agentes externos maliciosos.

Foram encontradas algumas falhas de segurança que podem impactar diretamente as contas de usuários e podem levar ao comprometimento dos serviços disponibilizados pela empresa. Nossa equipe foi capaz de explorar essas falhas o que também poderia ser feito por atacantes externos mal-intencionados. Por este motivo, a SecurityLabs entende que a aplicação WEB analisada possui alto risco e comprometimento e que deve ser mitigado o mais rápido possível.

1.1 ESCOPO

Os testes foram realizados nos domínios e intervalos de IPs descritos abaixo:

Domínio ou Local do Datacenter
hom.eleicoespsicologia.org.br

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

1.2 RESUMO DAS FALHAS ENCONTRADAS

Abaixo pode ser encontrado um resumo das falhas descobertas durante a execução do teste de aplicação WEB. Para efeito desse teste, consideramos a classificação de criticidade e impacto, conforme descrito em maiores detalhes na seção 2.1.

Vulnerabilidade	Criticidade	Impacto	Detalhes
Condição de HTML Injection	**ALTA**	**ALTO**	Seção 3.1
Ausência de Cabeçalho HTTP de Segurança – X-Frame-Options	**BAIXA**	**MÉDIO**	Seção 3.12
Ausência de Sistema de Proteção de Intrusão (IPS) e WAF	**BAIXA**	**MÉDIO**	Seção 3.16

1.3 RESUMO DAS RECOMENDAÇÕES

Como demonstrado nesse teste, o cliente deve seguir com um programa de testes constantes no seu ambiente e também uma revisão de seus controles de segurança, visando fortalecer o seu programa de segurança da informação.

As recomendações específicas de cada problema encontrado estão documentadas na sessão “PROBLEMAS ENCONTRADOS” desse documento, mais abaixo, com base nos diversos anos de experiência acumulados pela SecurityLabs e melhores práticas da indústria, enumeramos os principais controles de segurança a serem tomados:

- Utilização de tunning de regras e assinaturas de proteção na camada de aplicação Web, pelo uso de *Web Application Firewall,* que detecte e impeça a execução de ataques WEB nos servidores de aplicação e permita a utilização de eventuais correções virtuais (virtual patching), com ênfase na detecção de ataques de força bruta em formulários de autenticação;
- Utilização de práticas de segurança e programação seguras que eliminem classes de ataques conhecidas;
- Considerar a execução de testes de rede externo que utilizem ataques de “Client-side” como exercícios de Phishing e/ou ataques direcionados que possam simular de maneira mais realista um atacante com foco no ambiente da empresa;
- *Hardening* dos servidores WEB com o objetivo de implementar melhores práticas de segurança, tais como cabeçalhos de segurança HTTP, políticas de controle de acesso, gestão de certificados SSL/TLS, acessos padrão;
- Utilização de sistemas de detecção e resposta a ataques e incidentes em tempo real, tais como IPS (*Intrusion Prevention System*) capazes de detectar

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

scanners de portas e envio de pacotes maliciosos, bem como a execução de ataques de força bruta em serviços contendo autenticação.

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

2 METODOLOGIA

A Execução do Teste de Intrusão obedeceu às principais metodologias utilizadas na atualidade para buscas de vulnerabilidades e exploração de problemas de segurança, tais como ISECOM OSSTMM versão 3, bem como OWASP TOP 10 2017. Maiores informações sobre as mesmas podem ser obtidas nos links abaixo:

- http://www.isecom.org/mirror/OSSTMM.3.pdf
- https://www.owasp.org/index.php/Top_10-2017_Top_10

Os testes de segurança executados na aplicação WEB Farmasis do Conselho Federal de Farmácia seguiram o seguinte fluxo de atividades:

E englobaram uma série de classes de ataque e análise de vulnerabilidades que verificaram, dentre outros, problemas tais como:

- Verificação de Ausência de patches de segurança;
- Busca por problemas relacionados à configuração de serviços;
- Identificação de serviços acessíveis;
- Uso de senha padrão/ausente em serviços de rede e servidores;
- Uso de protocolo de criptografia inseguro.

Problemas relacionados a servidores web, como:

- Acesso a interface administrativas de servidores de aplicação;
- Uso de métodos HTTP inseguros, como TRACE e PUT;
- Uso de certificado inválido/expirado/chave fraca;
- *Basic authentication*;
- Dentre outros.

E problemas em aplicações e servidores de aplicação, tais como:

- Escalação Horizontal de privilégios;
- Escalação Vertical de Privilégios;
- Tentativa de *bypass* do WAF, caso esteja presente;
- Teste de qualidade do *Captcha*;
- *Stack Buffer Overflow;*
- *Heap Overflow;*
- *Integer Overflow;*
- *Vertical Privilege Escalation;*
- *OS command injection;*
- *Blind SQL injection;*

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

- *SQL Injection;*
- *File path traversal;*
- *XML external entity injection;*
- *LDAP injection;*
- *XPath injection;*
- *XML injection;*
- *Stored Cross-site scripting;*
- *HTTP header injection;*
- *Reflected Cross-site scripting;*
- *Flash cross-domain policy;*
- *Silverlight cross-domain policy;*
- *HTML5 cross-origin resource sharing;*
- *Cleartext submission of password;*
- *Referer-dependent response;*
- *User agent-dependent response;*
- *Password returned in later response;*
- *Password field submitted using GET method;*
- *Password returned in URL query string;*
- *Cross-domain POST;*
- *Open redirection;*
- *Cross-domain Referer leakage;*
- *Cross-domain script include;*
- *Session token in URL;*
- *Frameable response (potential Clickjacking);*
- *Browser cross-site scripting filter disabled;*
- *Database connection string disclosed;*
- *Source code disclosure;*
- *Directory listing;*
- *Email addresses disclosed;*
- *Private IP addresses disclosed;*
- *Robots.txt file;*
- *Cacheable HTTPS response;*
- *Multiple content types specified;*
- *HTML does not specify charset;*
- *HTML uses unrecognized charset;*
- *Content type incorrectly stated;*
- *Content type is not specified;*
- *SSL certificate;*
- *CSRF - Cross Site Request Forgery;*
- *Permissive password police;*
- Enumeração de usuários;
- *Session Fixation;*
- *Externally acessible adminstering interface;*
- *Anti-automation mechanism absence;*
- *Recovery / Reset password feature inadequate behavior;*
- *HTTP verb tampering.*

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

2.1 DEFINIÇÃO CRITICIDADE UTILIZADA

Com o objetivo de melhor transmitir a criticidade associada a cada uma das vulnerabilidades identificadas e possibilitar sua priorização quanto as ações emergenciais que devem ser conduzidas no intuito de mitigá-las, segue abaixo um sistema de métricas baseado em alguns padrões abertos como os propostos pelo OWASP *Risk Rating Methodology* e pelo *Common Vulnerability Scoring System* (CVSS v2).

Esse sistema permite a classificação das vulnerabilidades em 03 (três) diferentes níveis de criticidade. Esses valores são calculados com base em 02 (dois) índices: Probabilidade de ocorrência (PO) e Impacto resultante da exploração (IE). A pontuação responsável por definir qual a Criticidade associada a determinada vulnerabilidade é obtida a partir da multiplicação desses dois índices.

A tabela a seguir exibe o conjunto de símbolos juntamente com seu respectivo significado.

CRITICIDADE	SÍMBOLO	DESCRIÇÃO
Maior que 6	ALTA	A vulnerabilidade foi descoberta e foi classificada como crítica, exigindo que seja remediada com urgência ou mitigada em um curto intervalo de tempo.
3 a 5	MÉDIA	A vulnerabilidade foi descoberta e classificada como de média criticidade, devendo ser solucionada como parte das rotinas e/ou tarefas de manutenção da segurança do ambiente.
1 a 2	BAIXA	A vulnerabilidade foi descoberta e classificada como de baixa criticidade, devendo ser remediada como parte do processo de manutenção do ambiente.

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

Vale ressaltar que a Criticidade aqui apresentada pode não representar o risco real ao negócio da organização. Isso pode significar que alguma falha pode ter sido reportada sob o ponto de vista técnico como de alta criticidade, entretanto, devido a existência de algum controle que foge ao conhecimento da análise executada pela SecurityLabs essa mesma falha talvez possa ser visualizada como de baixa criticidade pela empresa.

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

3 PROBLEMAS DE SEGURANÇA ENCONTRADOS

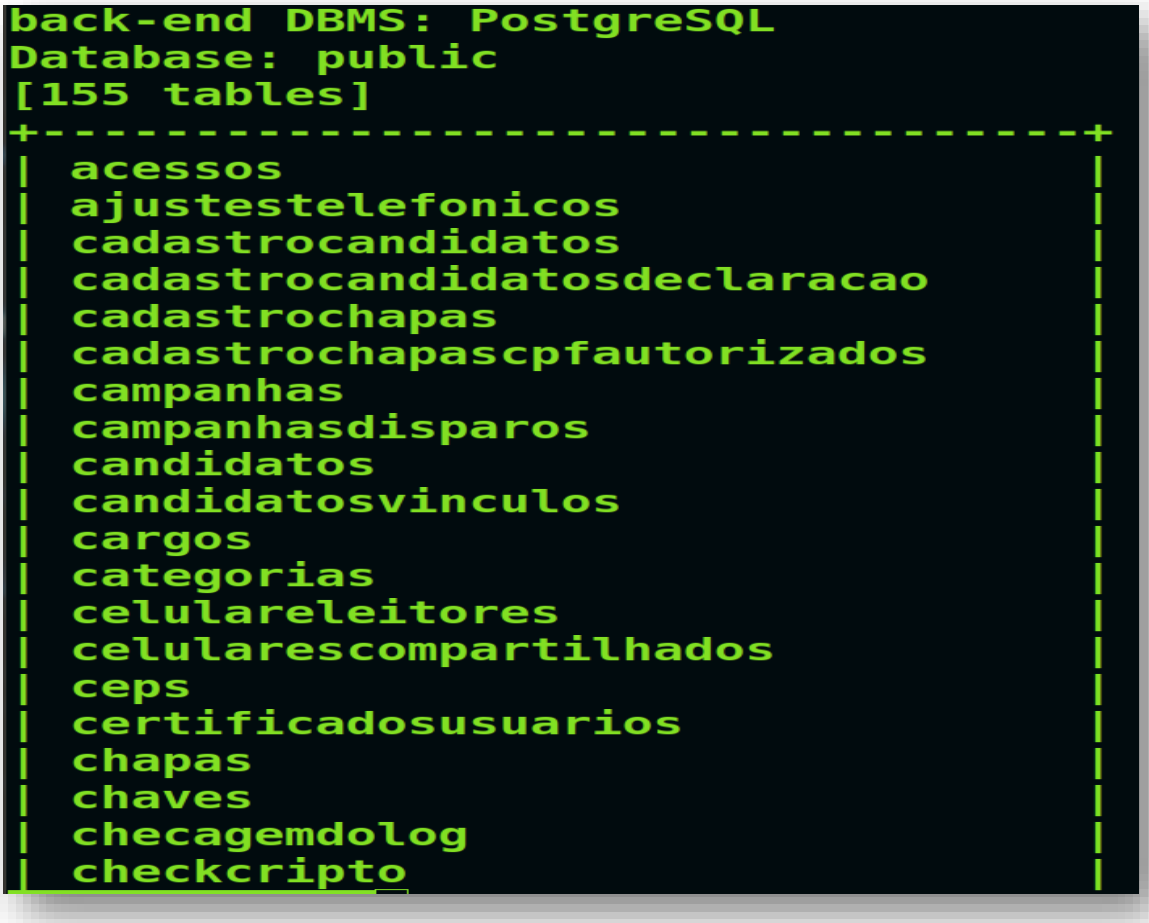
Nesta seção serão apresentadas as falhas de segurança encontradas durante a execução do teste juntamente com as evidências e recomendações.

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

Criticidade: Alta
Impacto: Alto
Descrição:
Foi detectado que a aplicação WEB possui uma condição de SQL Injection que permitiu a extração de dados do banco de dados. Essa condição de encontra em:

https://hom.eleicoespsicologia/adm/api/server/vot/chapas

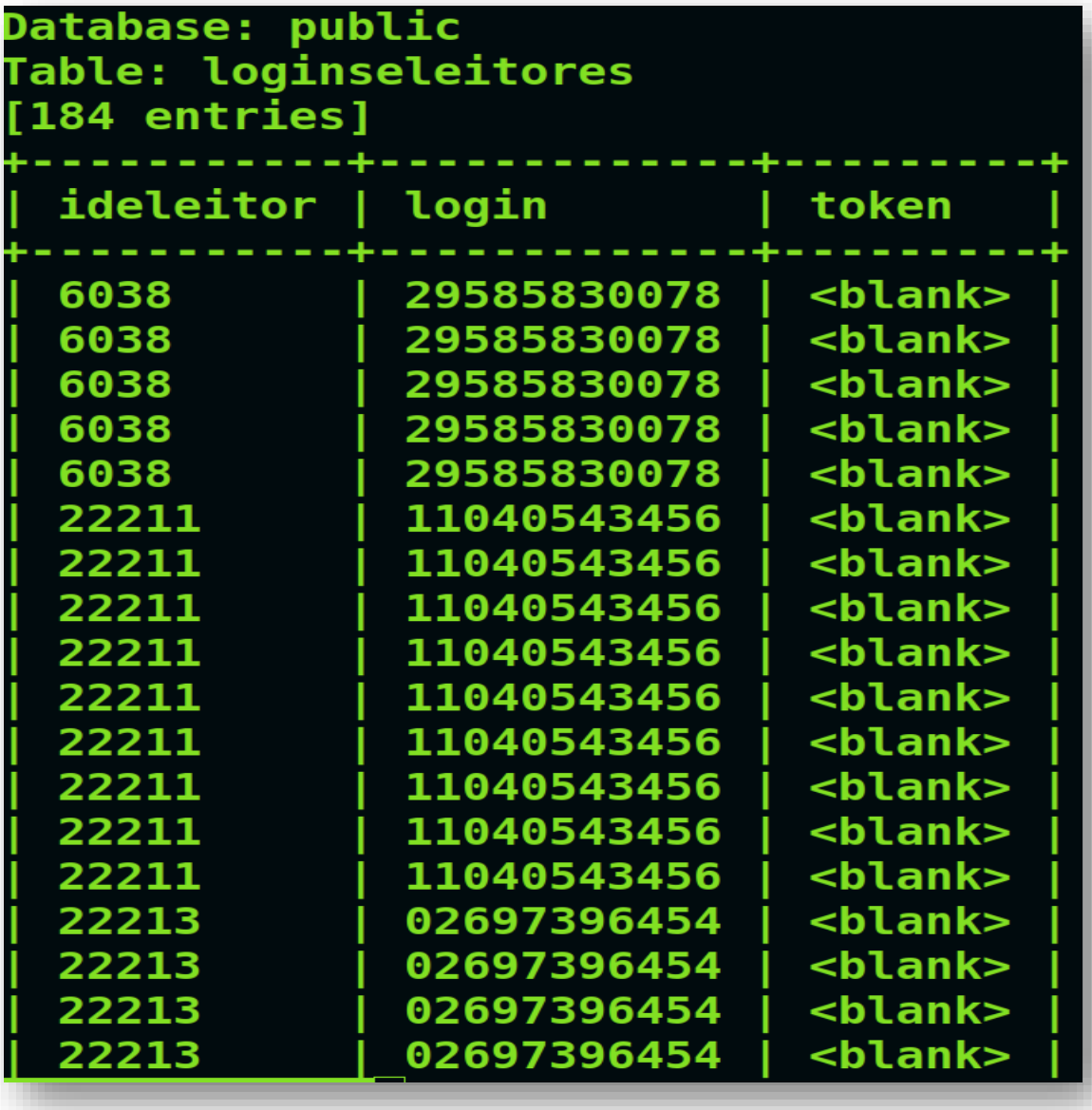
Abaixo demonstramos esse problema.



(Imagem 3.1-1 –Extração de Tabelas via SQL Injection)

Foi possível através dessa falha extrair dados do banco de dados, tais como tabelas, campos, etc. Abaixo vemos mais uma evidência da criticidade desse problema:

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.



```
Database: public
Table: loginseleitores
[184 entries]
+-----------+-------------+---------+
| ideleitor | login       | token   |
+-----------+-------------+---------+
| 6038      | 29585830078 | <blank> |
| 6038      | 29585830078 | <blank> |
| 6038      | 29585830078 | <blank> |
| 6038      | 29585830078 | <blank> |
| 6038      | 29585830078 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22211     | 11040543456 | <blank> |
| 22213     | 02697396454 | <blank> |
| 22213     | 02697396454 | <blank> |
| 22213     | 02697396454 | <blank> |
| 22213     | 02697396454 | <blank> |
```

(Imagem 3.1-2 –Extração de Tabela de Eleitores)

Solução sugerida:
Utilização de progração egura que implemente o conceito de prepared statement ou uso de forte tipagem de entrada de dados.

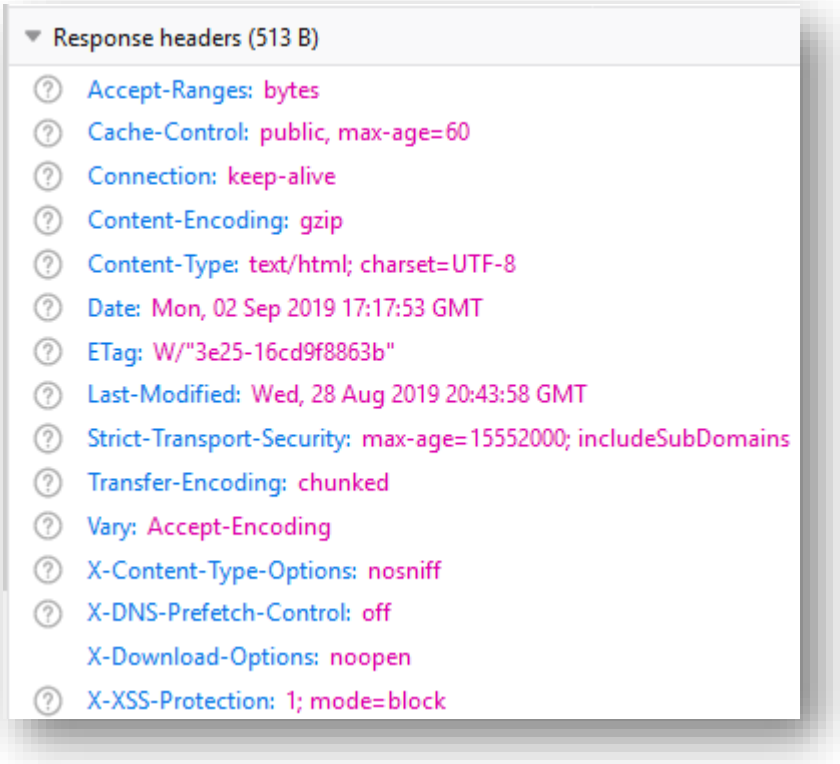
Referências:
https://www.owasp.org/index.php/SQL_Injection

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

3.2 AUSÊNCIA DE CABEÇALHO HTTP DE SEGURANÇA – X-FRAME-OPTIONS

Criticidade: Baixa
Impacto: Médio
Descrição:
O cabeçalho de segurança *X-Frame-Options* tem o objetivo de orientar os navegadores a não carregarem páginas em *tags iframe* sem a devida liberação, com isso evitando ataques do tipo *ClickJacking*.

Foi detectado que o servidor de aplicações não está enviando esse cabeçalho de segurança, conforme evidência abaixo:



(Imagem 3.2-1 – Ausência de envio de cabeçalho *X-Frame-Options*)

Solução Sugerida:
Inserir o cabeçalho *X-Frame-Options* como resposta as requisições HTTP.

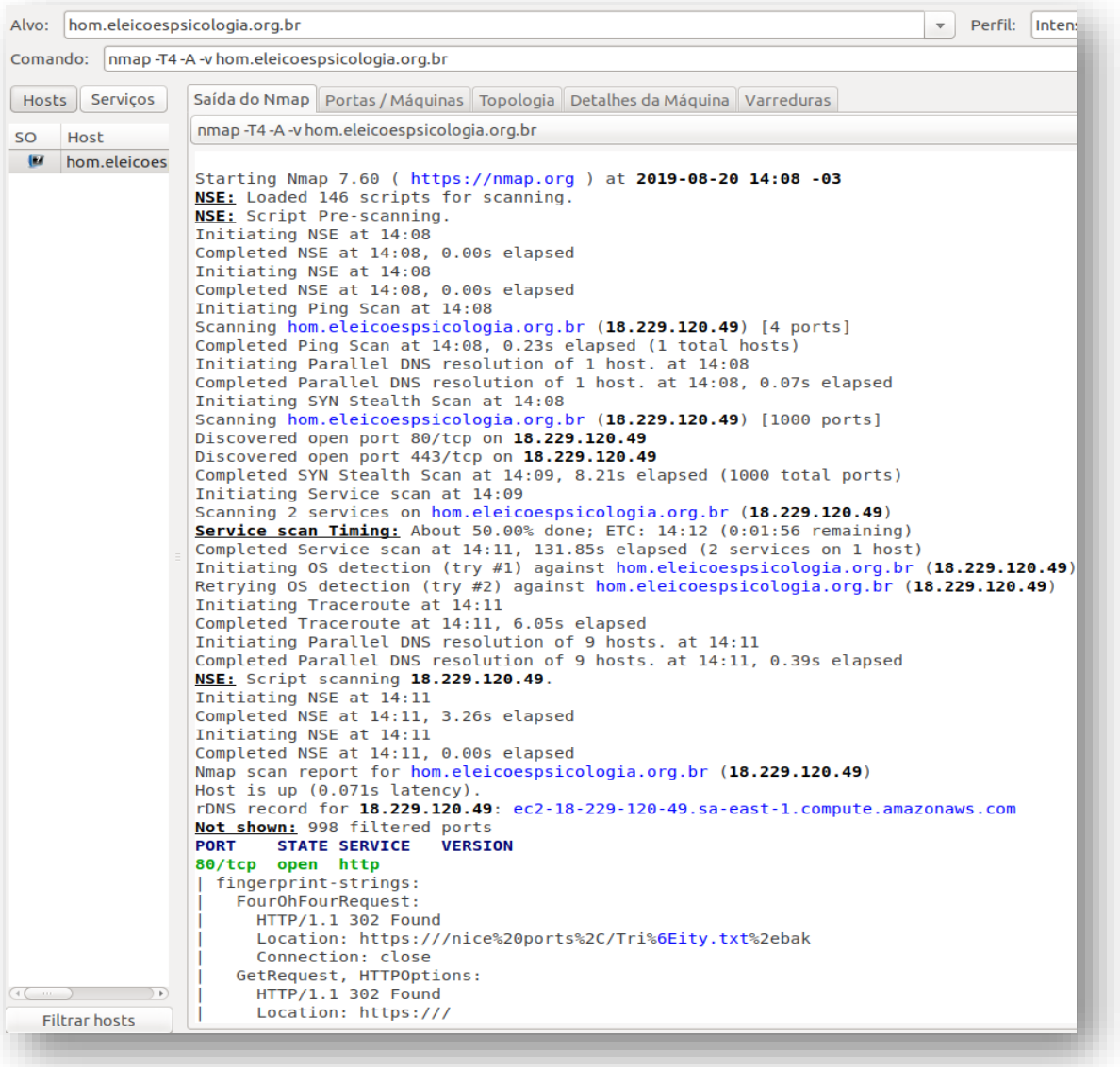
Referências:
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xfo
https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers
https://www.owasp.org/index.php/Clickjacking

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

3.3 AUSÊNCIA DE SISTEMA DE PROTEÇÃO DE INTRUSÃO (IPS) E HARDENING

Criticidade: Baixa
Impacto: Médio
Descrição:
Durante a execução do teste de intrusão foi verificado a ausência de recursos avançados de segurança de rede que bloqueiem ataques em tempo real.

Abaixo repassamos uma evidência desse problema:



(Imagem 3.3-1 –Execução de Portscan)

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

Acima, vemos a execução de um ataque de portscan não ser bloqueado.

Além disso, no ataque de SQL Injection, nenhum Web Application Firewall foi detectado.

Solução Sugerida:
Instalação de configuração de sistemas de IPS, NIDS e SIEM para detecção e bloqueio de ataques em tempo real. Utilização de um Web Application Firewall (WAF) para bloqueio de ataques WEB.

Referências:
https://www.owasp.org/index.php/Web_Application_Firewall
https://www.owasp.org/index.php/Intrusion_Detection

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

4 CONCLUSÃO

Este relatório apresentou diversos problemas de segurança detectados durante a execução de um teste de intrusão (blackbox) na aplicação Eleições CFP.

Foram repassadas instruções quanto a solução dos mesmos. E recomendamos que essas soluções sejam implementadas o mais rápido possível.

O serviço de teste de intrusão representa apenas uma fotografia da segurança de um sistema em um dado momento e não devem ser vistos como um processo final de busca de vulnerabilidades de uma aplicação.

É recomendável a execução periódica de tanto de análises de vulnerabilidades bem como testes de intrusão aliada a outras práticas de validação e análise de segurança.

Nome	E-mail	Função
Glaudson Ocampos	glaudson@securitylabs.com.br	Analista de Segurança
Waldemar Nehgme	waldemar@securitylabs.com.br	Analista de segurança

7.- 22 de agosto de 2019:

Teste de intrusão na aplicação “Eleicaoweb” com o objetivo de certificar a retirada de vulnerabilidades apontadas no teste de intrusão, a empresa INFOLOG seguindo nossas recomendações modificou a aplicação retirando do GAP de segurança as falhas apontadas.

¶
¶

Sumário¶

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

8.- 22 de agosto de 2019:
Testes de estresse do ambiente de produção, AWS Amazon.
Testes de estresse do ambiente de votação presencial utilizando diversas listas em conjunto ao Jmetter.
Participantes:
SecurityLabs: Waldemar Nehgme.
INFLOG: Ubiratan Soares de Melo.

9.- 22 de agosto de 2019:
Analises “anti-fraude” da Base de Dados utilizada para a realização das eleições do Conselho Federal de Psicologia - CFP processo 2019 e supervisão da entrada em produção do sistema “Eleicaoweb”
Participantes:
SecurityLabs: Waldemar Nehgme.
INFLOG: Ubiratan Soares de Melo.

10.- 22 de agosto de 2019:
Supervisão da entrada em produção do sistema “Eleicaoweb” utilizando os códigos auditados pela SecurityLabs, eleição CFP 2019 conforme laudo de auditoria.

11.- 22 de agosto de 2019:
Assinatura laudo de auditoria de código fonte, sistema eleitoral aplicação “Eleicaoweb” 2019 CFP.
Participantes:
SecurityLabs: Waldemar Nehgme.
INFLOG: Ubiratan Soares de Melo.

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

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 empresa Infolog Tecnologia Ltda, detentora da propriedade intelectual do programa).

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

faf46d0a72bf6a72a508a1fd74d0f169
_2019_08_22_22_49_16/_2019_08_22_22_49_16_ip-172-30-0-134_api_md5.txt
(app)

faf46d0a72bf6a72a508a1fd74d0f169
_2019_08_22_22_49_50/_2019_08_22_22_49_50_ip-172-30-0-53_api_md5.txt
(app)

faf46d0a72bf6a72a508a1fd74d0f169
_2019_08_22_22_48_41/_2019_08_22_22_48_41_ip-172-30-0-116_api_md5.txt
(app)

12.- 23 de agosto de 2019:
Verificação manual da tabela de votos (vazia) no início do pleito eleitoral, backup da base de dados e assinatura digital da mesma.
SecurityLabs: Waldemar Nehgme.
INFLOG: Ubiratan Soares de Melo.

13.- 23 de agosto de 2019:
Lacre da base de dados do ambiente de produção.
Participantes:
SecurityLabs: Waldemar Nehgme.
INFLOG: Ubiratan Soares de Melo.

Hash do Documento

2283DD63A772335E529AF78FD6BB3869C325E60F111E25ABB8BE461247EE02D8

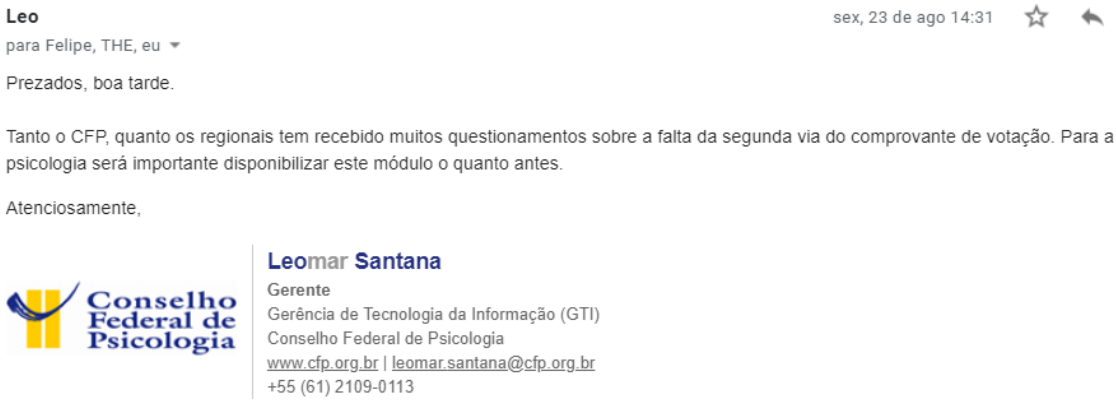
O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 23/08/2019 é(são) :

☑ Waldemar Nehgme Gonzalez (Signatário) - 490.385.241-53 em 23/08/2019 00:18 UTC-03:00
Tipo: Certificado Digital - SECURITYLABS SERVICOS DE DESENVOLVIMENTO E LICENC - 11.046.341/0001-14

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

14.- 23 de agosto de 2019:
Solicitação do CFP conforme e-mail para disponibilização do modulo de comprovante de votação.



Leo sex, 23 de ago 14:31
para Felipe, THE, eu

Prezados, boa tarde.

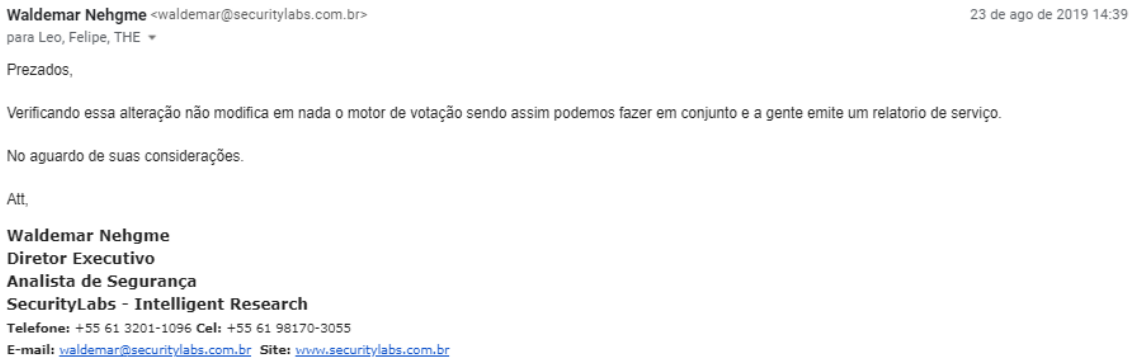
Tanto o CFP, quanto os regionais tem recebido muitos questionamentos sobre a falta da segunda via do comprovante de votação. Para a psicologia será importante disponibilizar este módulo o quanto antes.

Atenciosamente,

Conselho Federal de Psicologia

Leomar Santana
Gerente
Gerência de Tecnologia da Informação (GTI)
Conselho Federal de Psicologia
www.cfp.org.br | leomar.santana@cfp.org.br
+55 (61) 2109-0113

14.- 23 de agosto de 2019:
Após reunião com a empresa INFOLOG e analisando a solicitação do CFP, verificamos que a mudança em nada afeta o motor de votação e supervisionamos a mesma junto ao fornecedor.



Waldemar Nehgme <waldemar@securitylabs.com.br> 23 de ago de 2019 14:39
para Leo, Felipe, THE

Prezados,

Verificando essa alteração não modifica em nada o motor de votação sendo assim podemos fazer em conjunto e a gente emite um relatorio de serviço.

No aguardo de suas considerações.

Att,

Waldemar Nehgme
Diretor Executivo
Analista de Segurança
SecurityLabs - Intelligent Research
Telefone: +55 61 3201-1096 **Cel:** +55 61 98170-3055
E-mail: waldemar@securitylabs.com.br **Site:** www.securitylabs.com.br

15.- 23 de agosto de 2019:
Acompanhamento presencial da habilitação do modulo de comprovante de votação e mudanças no aprimoramento do sistema que em nada afetam o motor de votação e a lisura do pleito.
As mudanças foram supervisionadas e emitido o laudo de auditoria V1 para o CFP.

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

Procedimentos utilizados:

I - Deste Laudo

O presente laudo técnico apresenta uma avaliação de aspectos de segurança de dados relativos ao software (aplicação) denominado "EleiçãoWeb" após modificações nas camadas de:

- Modulo de segunda via ativado;
- Melhoria na mensagem de quando há falha de comunicação do dispositivo do usuário;
- Recomendação de substituição de octeto para PDF ou list para melhorar download em Iphones;
- Recomendação de melhoria na comunicação de aguardando encaminhamento na urna;

16.- 25 de agosto de 2019:

Acompanhamento presencial da mudança na codificação na rota das mensagens após detecção de ataque direcionado a infraestrutura de votação.
A equipe de resposta a incidente da SecurityLabs realizou analises em tempo real dos log de ataque e recomendou a mudança na codificação para minimizar o impacto do ataque.
A empresa INFOLOG acatou as recomendações e modificou a codificação.
O aprimoramento do sistema em nada afeta o motor de votação e a lisura do pleito.
As mudanças foram supervisionadas e emitido o laudo de auditoria V2 para o CFP.

Da tentativa de exploração:

No dia 25 de agosto de 2019, foram detectados ataques intensos ao sistema na rota de mensagens, ainda que nenhum deles com sucesso, como forma preventiva a SecurityLabs recomendou e autorizou a remoção de caracteres especiais na rota de mensagens conforme a seguir:

```
tipo = tipo.split("""").join("""").split('=').join('')
```

Estas alterações conforme assinatura de código foram processada em 25 de agosto de 2019 e a mesma não modifica em nada o restante dos códigos fontes do sistema eleitoral utilizado.

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

17.- 27 de agosto de 2019.
Participação na cerimônia de encerramento do processo eleitoral do Conselho Federal de Psicologia – CFP 2019, entrega em mãos do resultado final das eleições para a Comissão Eleitoral na sede do Conselho Federal.

Eleições /Apuracao/CFP
Resultado - 01 CRP 1ª Região (DF)
Consulta: Conselho Federal de Psicologia 01

Opção	Votos	Percentual	% Válidos
Frente em Defesa da Psicologia Brasileira	1005	30.60	35.50
Fortalecer a Profissão	1004	30.60	35.40
Renovação da Psicologia	221	6.70	7.80
Movimento Psicólogos em Ação	323	9.80	11.40
Avançar a Profissão no Brasil	281	8.60	9.90
Branco	189	5.80	
Nulo	261	7.90	
Total	**3284**	**100.00**	
Apurado em 27/08/19 19:57:02 - Emitido em 27/08/19 20:01:58			

18.- 28 de agosto de 2019.
Backup da base de dados utilizada no pleito eleitoral e assinatura digital da mesma. A assinatura digital da base de dados consta da ata técnica de encerramento contendo as assinaturas iniciais e finais da base de dados utilizada no pleito eleitoral.
O resultado gerou o laudo de auditoria V3.

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

Security labs
Intelligent Research

Security labs
Intelligent Research

LAUDO DE AUDITORIA V3

Escopo: Ata de Abertura e Fechamento da Base de Dados.
Referência: Processo Eleitoral 2019.
Brasília-DF, 28 de agosto de 2019.

Emissor: SecurityLabs Intelligent Research
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

Este documento tem como objetivo garantir a integridade da base de dados no início e no termino do processo eleitoral do CONSELHO FEDERAL DE Psicologia – CFP 2019.

Backup base de dados inicial:

c76d3b4c6b87c98c34a8b8c32be15e22 backup_cfp_www.dump

Backup base de dados final:

b997982f160623eeb17036e085ef7929 backup_cfp_www_final.dump

Dos serviços:

Conforme cronograma de serviço todas as etapas foram concluídas com êxito e sempre dentro de nossa competência respondemos todos os questionamentos.

O processo eleitoral transcorreu de acordo com as expectativas e sem nenhum incidente técnico ou de segurança reportado.

Cabe destacar que nossos serviços de auditoria de código fonte de sistemas, não validam informações de cadastro nem de registro de candidatos, focando principalmente nos aspectos de segurança no que se refere a "trafego de informação na rede de computadores, sigilo do voto e garantias do voto ao candidato de acordo com as melhores práticas em segurança da informação.

No momento do encerramento deste relatório não se reportou nenhuma contestação jurídica.

Atenciosamente,

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

Este documento foi assinado digitalmente por Waldemar Nehgme Gonzalez.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código 5859-A885-6968-88A7.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas Certisign. Para verificar as assinaturas clique no link: https://www.portaldeassinaturas.com.br/Verificar/5859-A885-6968-88A7 ou vá até o site https://www.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 5859-A885-6968-88A7

Hash do Documento

EED3F5B2F6BA63AB366BC3E97DE17803827FC914BEBE9121F09406C86E5DC56A

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 19/09/2019 é(são) :

- Waldemar Nehgme Gonzalez (Testemunha) - 490.385.241-53 em 19/09/2019 10:42 UTC-03:00
  Tipo: Certificado Digital - SECURITYLABS SERVICOS DE DESENVOLVIMENTO E LICENC - 11.046.341/0001-14