CCESS - CRYPTOCURRENCY SECURITY STANDARDS

Cryptocurrency Exchange Security Standards - 2018

Relatório Público

Relatório Anual de Segurança das Corretoras Brasileiras de Criptomoedas

São Paulo

2018

CONSELHO

Deivison Franco (Presidente): Perito Forense Computacional Judicial e Extrajudicial. Pesquisador e Consultor em Computação Forense e Segurança de Informações. Membro do IEEE Information Forensics and Security Technical Committee e da Sociedade Brasileira de Ciências Forenses. C|EH, C|HFI, DSFE e ISO 27002 Advanced. Autor e revisor técnico do livro Tratado de Computação Forense, revisor e membro do corpo editorial da Revista Brasileira de Criminalística e colunista das revistas eForensics Magazine, CryptoID e Segurança Digital.

Leonardo Marciano (Membro do board): Empreendedor, presidente da Fundação Marciano e fundador do Sudo Financial. Já participou do time principal das maiores corretoras do mercado de criptomoedas.

Vinicius Valerio (Security Researcher): Pesquisador de segurança da informação, mencionado no Hall of Fame Security Researcher do Netflix. Um dos principais nomes de Bug Bounty do Brasil com empresas como FBI, IBM, Nasa, Nasdaq e Terra em seu portfólio.

Cryptocurrency Exchange Security Standards - 2018

Relatório Anual de Segurança das Corretoras Brasileiras de Criptomoedas

Relatório público sobre segurança das corretoras brasileiras de criptomoedas - referente ao ano de 2018, e funcionamento da Cryptocurrency Exchange Security Standards, tais como serviços prestados e ramos de atuação.

São Paulo

2018

SUMÁRIO

1. CRITÉRIO PARA PARTICIPAÇÃO 4

1.1 Metodologia para Seleção de Corretoras 4

2. CRITÉRIO PARA AVALIAÇÃO 5

2.1 Metodologia para Realização dos Testes..... 5

2.2 Metodologia para Classificação de Riscos 7

3. PRINCIPAIS VULNERABILIDADES ENCONTRADAS 11

3.1 OWASP A3 - Sensitive Data Exposure 11

3.2 OWASP A6 - Security Misconfiguration..... 13

3.3 Vulnerabilidades de Risco Baixo Encontradas 15

3.4 Vulnerabilidades de Risco Médio Encontradas..... 18

3.5 Vulnerabilidades de Risco Alto Encontradas 19

4. SERVIÇOS PRESTADOS 21

5. SELO CCESS 22

6. PRINCIPAIS REFERÊNCIAS UTILIZADAS 26

1. CRITÉRIO PARA PARTICIPAÇÃO

Resumo: Critério de participação e seleção para avaliação de segurança seguindo os padrões impostos pelo conselho de 2018.

Palavras-chave: critério, seleção, corretora, criptomoedas e 2018.

1.1 Metodologia para Seleção de Corretoras

Foram selecionadas corretoras com volume diário acima de 10 (dez) Bitcoins seguindo a lista disponibilizada no site CoinTradeMonitor[1], de forma não sequencial, no dia 07 de agosto de 2018 numa seleção aleatória após as cinco com maior volume, com exceção das corretoras Troca Ninja e Walltime, cuja relação está mostrada na Tabela 1 abaixo.

Tabela 1 – Relação das corretoras testadas.

CORRETORA	WEBSITE
3xBit	https://3xbit.com.br
BitCambio	https://bitcambio.com.br
BitconTrade	https://www.bitcointrade.com.br/
Braziliex	https://braziliex.com/
BTCBolsa	https://btcbolsa.com/
flowBtc	https://www.flowbtc.com.br/
Foxbit	https://foxbit.com.br/
MercaboBitcoin	https://www.mercadobitcoin.com.br/
NegocieCoins	https://www.negociecoins.com.br/
Troca Ninja	https://troca.ninja/
Walltime	https://walltime.info/

[1] https://www.cointradermonitor.com/

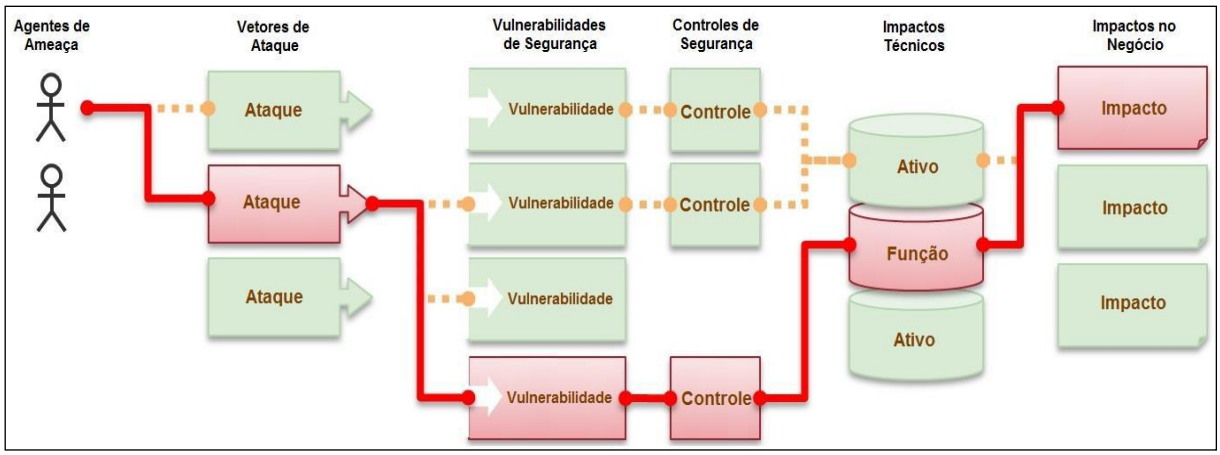
2. CRITÉRIO PARA AVALIAÇÃO

Resumo: Levantamento dos itens avaliados e utilizados na aprovação ou reprovação das corretoras selecionadas durante a avaliação anual de 2018. Todos os testes foram feitos baseando-se em nossa primeira certificação.

Palavras-chave: vulnerabilidade, indisponibilidade e código-fonte.

2.1 Metodologia para Realização dos Testes

m atacante pode, potencialmente, usar vários caminhos diferentes através de um sistema para causar danos ao negócio ou organização. Cada um desses caminhos representa um risco que pode, ou não, ser grave o suficiente para justificar atenção. Sendo que, às vezes, esses caminhos são triviais para encontrar e explorar, e em outras, são extremamente difíceis. Da mesma forma, o dano causado pode ter nenhuma consequência, ou resultar em danos sérios, a figura a seguir ilustra esses caminhos.



Para determinar o risco para a organização, pode-se avaliar a probabilidade associada a cada agente de ameaça, vetor de ataque, vulnerabilidade de segurança e combiná-la com uma estimativa dos impactos técnicos e no negócio da empresa. Juntos, esses fatores determinam o risco total.

Diante do exposto, os testes previstos neste documento estão relacionados aos sites e ambientes computacionais das Corretoras testadas e visa atender aos tipos de ataques inerentes à metodologia para realização de testes de intrusão do OWASP, por ordem de criticidade, os quais são apresentados e descritos na Tabela 2 a seguir.

Tabela 2 – Tipo e descrição dos ataques testados.

TIPO DE ATAQUE	DESCRIÇÃO
Injeção de Código	Ocorre quando dados não confiáveis (códigos maliciosos) são enviados para um interpretador como parte de um comando ou consulta.
Gerenciamento de Sessão	Ocorre quando as funções de gerenciamento de sessão são implementadas de forma incorreta.
Cross-Site Scripting (XSS)	Ocorre quando uma aplicação recebe dados não confiáveis e os envia ao navegador sem validação ou filtro.
Referência Insegura e Direta a Objetos	Ocorre quando uma referência à implementação interna de um objeto é exposta.
Configuração Incorreta de Segurança	Ocorre quando configurações de segurança não são implementadas na aplicação.
Exposição de Dados Sensíveis	Ocorre quando aplicações web não protegem devidamente dados sensíveis.
Cross-Site Request Forgery (CSRF)	Ocorre quando uma vítima que possui uma sessão ativa em um navegador envia uma requisição HTTP forjada, incluindo o cookie da sessão, a uma aplicação web vulnerável.
Uso de Componentes Vulneráveis Conhecidos	Ocorre quando componentes como bibliotecas, frameworks e outros módulos de software, são executados com os mesmos privilégios que o sistema.
Redirecionamentos Inválidos	Ocorrem quando a aplicação redireciona os usuários para outros sites usando dados não confiáveis para determinar as páginas de destino.

O cerne do processo de realização dos testes se baseou em aferir a resistência dos sites das corretoras testadas, frente aos ataques indicados pela tabela acima. Para tanto, o Conselho se valeu de um conjunto abrangente de ferramentas para análise de vulnerabilidades e verificações de segurança específicas para testes de intrusão desenvolvidos com base nos padrões do OWASP Testing Project[2,3].

[2] https://www.owasp.org/index.php/OWASP_Testing_Project

A primeira etapa no processo de testes consistiu em avaliar a aplicabilidade dos tipos de ataques contemplados na tabela acima. Sendo assim, objetivou-se com isso extrair uma lista de ataques, e possíveis vulnerabilidades, elegíveis para exploração. Dessa forma, essa atividade considerou características relevantes e inerentes ao funcionamento interno da aplicação tais como as tecnologias e os componentes de backend/frontend empregados em seu processo de desenvolvimento como critério fundamental para eleger as validações que foram efetuadas.

Com base na lista de testes resultantes da etapa anterior, as análises foram então conduzidas para validar a postura de segurança da aplicação verificando sua resistência aos ataques nela contemplados. Vale salientar que o método de análise empregado em cada um dos testes foi cautelosamente desenvolvido pelo corpo técnico do Conselho, sendo constantemente revisado e atualizado. Dessa forma, as técnicas empregadas no desenvolvimento dos testes levaram em consideração a experiência e melhores práticas de mercado. Portanto, o principal objetivo alcançado através da adoção dessa metodologia consistiu em priorizar e otimizar as validações efetuadas, fornecendo garantias em termos de cobertura ao minimizar as chances de uma falha evidente escapar ao processo de análise.

2.2 Metodologia para Classificação de Riscos

A metodologia para realização de testes de intrusão do OWASP tem seu foco na identificação dos riscos mais graves para uma ampla gama de organizações. Para cada um destes riscos, são fornecidas informações genéricas sobre a probabilidade de ocorrência e impacto técnico usando o esquema simples de classificação baseado na metodologia de avaliação de riscos do OWASP.

[3] Cabe ressaltar que os estudos e documentos do OWASP são disponibilizados para toda a comunidade internacional, e adotados como referência por entidades como U.S. Defense Information Systems Agency (DISA), U.S. Federal Trade Commission, várias empresas e organizações mundiais das áreas de Tecnologia, Auditoria e Segurança, e também pelo PCI Council.

Os detalhes de ambiente e de negócio são intrínsecos à organização e apenas os atores envolvidos em seus processos têm conhecimento dos mesmos. Dessa forma, para qualquer aplicação, pode não haver um agente de ameaça que possa executar um ataque relevante, ou o impacto técnico pode não fazer nenhuma diferença para o negócio. Portanto, é necessário avaliar cada risco, focando nos agentes de ameaça, controles de segurança e impactos no negócio da empresa.

O OWASP lista agentes de ameaça como específicos da aplicação, e impactos no negócio como específicos do negócio/aplicação para indicar que estes são claramente dependentes dos detalhes sobre os diversos sistemas de uma empresa. Sendo assim, os nomes dos riscos na metodologia para realização de testes de intrusão derivam-se do tipo de ataque, do tipo de vulnerabilidade, ou do tipo de impacto causado.

A Tabela 3, a seguir, apresenta um resumo dos principais riscos de segurança em aplicações e os fatores de risco que foram atribuídos a cada um. Esses fatores foram determinados com base nas estatísticas disponíveis e na experiência da equipe. Para compreender esses riscos em uma aplicação, é necessário considerar os próprios agentes de ameaça e impactos no negócio, pois mesmo falhas flagrantes de software podem não representar um risco sério se não houver agentes de ameaça em uma posição de realizar o ataque necessário, ou o impacto no negócio é insignificante para os ativos envolvidos.

Tabela 3 – Mensuração de riscos do OWASP.

AGENTES DE AMEAÇA	EXPLORAÇÃO DA VULNERABILIDADE	PREVALÊNCIA DA VULNERABILIDADE	DETECÇÃO DA VULNERABILIDADE	IMPACTOS TÉCNICOS	IMPACTOS AOS NEGÓCIOS
Específicos da Aplicação	**Fácil**	**Generalizada**	**Fácil**	**Severo**	Específicos do Negócio / Aplicação
	Média	**Comum**	**Média**	**Moderado**	
	Difícil	**Rara**	**Difícil**	**Pequeno**	

Procurando melhor transmitir o impacto associado às vulnerabilidades identificadas e possibilitar sua priorização quanto às ações que devem ser conduzidas no intuito de mitigá-las, desenvolveu-se uma métrica baseada no OWASP Risk Rating Methodology[4] e no Common Vulnerability Scoring System[5] (CVSS v3.0). Sendo assim, para cada tipo de ataque realizado (especificados na Tabela 1), estimou-se o risco típico que cada vulnerabilidade introduz no sistema testado, verificando fatores comuns de probabilidade e fatores de impacto para cada vulnerabilidade comum. Em seguida, classificamos de forma ordenada de acordo com as vulnerabilidades que normalmente apresentam o risco mais significativo para a aplicação testada.

A metodologia proposta inclui três fatores de probabilidade para cada vulnerabilidade (prevalência, detecção e facilidade de exploração) e um fator de impacto (impacto técnico). A prevalência de uma vulnerabilidade é um fator que normalmente não precisa ser calculado, pois são fornecidos pelo OWASP através de estatísticas a partir de diferentes organizações para se chegar a uma lista da probabilidade de existência por prevalência de uma determinada vulnerabilidade. Estes dados são então combinados com os dois outros fatores de probabilidade (detecção e facilidade de exploração) para se calcular uma classificação de probabilidade para cada vulnerabilidade encontrada. Este valor é então multiplicado pelo impacto técnico médio estimado para cada item para se chegar a uma classificação de risco global.

Nesse contexto, a métrica proposta permite a classificação das vulnerabilidades em 03 (três) diferentes níveis de criticidade, cujo valor é calculado a partir da soma dos fatores de risco de sua respectiva explorabilidade, prevalência, detecção e impacto. Dessa forma, a pontuação responsável por definir qual a criticidade associada à determinada vulnerabilidade é obtida a partir do resultado da soma desses fatores, os quais são apresentados na Tabela 4, a seguir.

[4] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[5] https://www.first.org/cvss/specification-document

Tabela 4 – Fatores de risco.

EXPLORAÇÃO	PREVALÊNCIA	DETECÇÃO	IMPACTO	FATOR DE RISCO
Fácil	Generalizada	Fácil	Severo	3
Média	Comum	Média	Moderado	2
Difícil	Rara	Difícil	Pequeno	1

As corretoras passaram por até três testes envolvendo APIs, infraestrutura, criptografia, encapsulamento e pentest, para os quais foi proposto um índice de vulnerabilidade. Sendo assim, a Tabela 5, a seguir, exibe o nível de criticidade da vulnerabilidade encontrada, de acordo com o resultado da soma de seus fatores de risco, juntamente com seu respectivo significado. Tais níveis foram utilizados no decorrer deste documento para representar o risco e a criticidade calculados para cada uma das vulnerabilidades identificadas.

Tabela 5 – Índice de Risco x Vulnerabilidade.

PONTUAÇÃO	RISCO	VULNERABILIDADE	IMPACTO	RECOMENDAÇÃO
Maior que 10 pontos	Alto	Vulnerabilidades mais perigosas, que colocam o site em risco máximo de invasão e roubo de dados.	O sucesso de seu ataque pode resultar em grandes perdas financeiras, de ativos ou de recursos, além de poder causar danos significativos à imagem da organização, impedindo que ela cumpra suas tarefas junto aos clientes.	Exige que seja remediada com urgência ou mitigada em curto intervalo de tempo.
De 6 a 10 pontos	Médio	Vulnerabilidades que são causadas por erros de configuração do servidor e falhas de codificação de sites.	O sucesso de seu ataque pode resultar em perdas financeiras, de ativos ou de recursos, além de poder causar danos à imagem da organização, impedindo que ela cumpra suas tarefas junto aos clientes.	Deve ser solucionada como parte das rotinas e/ou tarefas de manutenção de segurança do site/ambiente.
De 1 a 5 pontos	Baixo	Vulnerabilidades derivadas da falta de criptografia de tráfego de dados ou de divulgação de caminho de diretório.	O sucesso de seu ataque pode resultar em perda de ativos ou recursos, além de afetar, de forma perceptível, as tarefas da organização e sua reputação.	Deve ser remediada como parte do processo de manutenção do site/ambiente.

3. PRINCIPAIS VULNERABILIDADES ENCONTRADAS[6]

3.1 OWASP A3 - Sensitive Data Exposure

Agentes de Ameaça / Vetores de Ataque		Fraqueza de Segurança		Impactos	
Específico	Explorabilidade: 2	Prevalência: 3	Detectabilidade: 2	Técnico: 3	Negócio: ?
Em vez de atacar diretamente a criptografia, os atacantes roubam chaves, executam ataques de intermediários ou roubam dados de texto não criptografado do servidor, enquanto em trânsito ou do cliente do usuário, por exemplo, navegador. Um ataque manual é geralmente necessário. Os bancos de dados de senhas recuperados anteriormente podem ser forçados a bruto pelas unidades de processamento de gráficos (GPUs).		Nos últimos anos, esse foi o ataque de impacto mais comum. A falha mais comum é simplesmente não criptografar dados confidenciais. Quando a criptografia é empregada, a geração e o gerenciamento de chaves fracas e o uso fraco de algoritmos, protocolos e cifras são comuns, particularmente para técnicas de armazenamento de hash com senhas fracas. Para dados em trânsito, os pontos fracos do servidor são principalmente fáceis de detectar, mas difíceis de armazenar dados.		Falha frequentemente compromete todos os dados que deveriam ter sido protegidos. Normalmente, essas informações incluem dados de informações pessoais confidenciais (PII), como registros de saúde, credenciais, dados pessoais e cartões de crédito, que geralmente exigem proteção, conforme definido por leis ou regulamentos, como o GDPR da UE ou leis locais de privacidade.	

[6] **Obs.: Durante a apresentação das vulnerabilidades e provas de ato não mencionaremos nomes ou como chegar até a vulnerabilidade.**

EXEMPLOS DE CENÁRIOS DE ATAQUE:

- **Cenário 1:** um aplicativo criptografa números de cartão de crédito em um banco de dados usando a criptografia automática do banco de dados. No entanto, esses dados são descriptografados automaticamente quando recuperados, permitindo que uma falha de injeção de SQL recupere números de cartão de crédito em texto não criptografado;

- **Cenário 2:** um site não usa ou aplica o TLS para todas as páginas ou oferece suporte a criptografia fraca. Um invasor monitora o tráfego de rede (por exemplo, em uma rede sem fio insegura), faz downgrade de conexões de HTTPS para HTTP, intercepta solicitações e rouba o cookie de sessão do usuário. O invasor então reproduz esse cookie e intercepta a sessão do usuário (autenticada), acessando ou modificando os dados privados do usuário. Em vez do acima, eles poderiam alterar todos os dados transportados, por exemplo: o destinatário de uma transferência de dinheiro;

- **Cenário 3:** o banco de dados de senhas usa hashes simples ou sem salt para armazenar as senhas de todos. Uma falha de upload de arquivo permite que um invasor recupere o banco de dados de senhas. Todos os hashes sem salt podem ser expostos com uma tabela de arco-íris de hashes pré-calculados. Os hashes gerados por funções hash simples ou rápidas podem ser decompostos por GPUs, mesmo que tenham SALT.

3.2 OWASP A6 - Security Misconfiguration

AGENTES DE AMEAÇA / VETORES DE ATAQUE		FRAQUEZA DE SEGURANÇA		IMPACTOS	
ESPECÍFICO	EXPLORABILIDADE: 3	PREVALÊNCIA: 3	DETECTABILIDADE: 3	TÉCNICO: 2	NEGÓCIO: ?
Os invasores frequentemente tentam explorar falhas não corrigidas ou acessar contas padrão, páginas não utilizadas, arquivos e diretórios desprotegidos, etc. para obter acesso não autorizado ou conhecimento do sistema.		A configuração incorreta de segurança pode acontecer em qualquer nível de uma pilha de aplicativos, incluindo serviços de rede, plataforma, servidor da Web, servidor de aplicativos, banco de dados, estruturas, código personalizado e máquinas virtuais, contêineres ou armazenamentos pré-instalados. Scanners automatizados são úteis para detectar configurações incorretas, uso de contas ou configurações padrão, serviços desnecessários, opções legadas, etc.		Tais falhas frequentemente dão aos invasores acesso não autorizado a alguns dados ou funcionalidades do sistema. Ocasionalmente, essas falhas resultam em um comprometimento total do sistema. O impacto nos negócios depende das necessidades de proteção do aplicativo e dos dados.	

EXEMPLOS DE CENÁRIOS DE ATAQUE:

- **Cenário 1:** o servidor de aplicativos é fornecido com aplicativos de amostra que não são removidos do servidor de produção. Esses aplicativos de amostra têm falhas de segurança conhecidas que os invasores usam para comprometer o servidor. Se um desses aplicativos for o Admin Console e as contas padrão não tiverem sido alteradas, o invasor fará login com as senhas padrão e assumirá o controle;

- **Cenário 2:** a listagem de diretórios não está desabilitada no servidor. Um atacante descobre que eles podem simplesmente listar diretórios. O invasor localiza e faz o download das classes Java compiladas, as quais elas descompilam e fazem engenharia reversa para exibir o código. O atacante então encontra uma séria falha no controle de acesso no aplicativo;

- **Cenário 3:** a configuração do servidor de aplicativos permite mensagens de erro detalhadas, por ex. rastreamentos de pilha, a serem devolvidos aos usuários. Isso potencialmente expõe informações confidenciais ou falhas subjacentes, como versões de componentes que são conhecidas como vulneráveis;

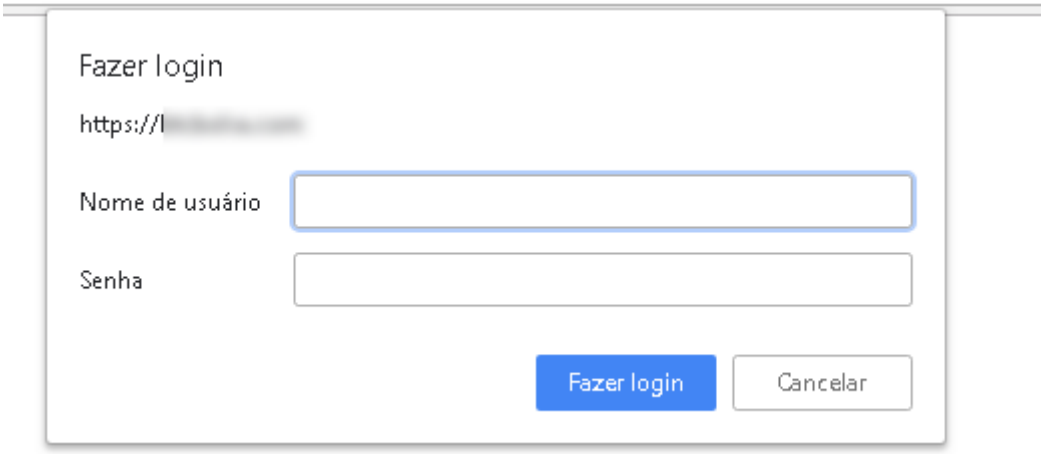
- **Cenário 4:** um provedor de serviços em nuvem tem permissões de compartilhamento padrão abertas para a Internet por outros usuários do CSP. Isso permite que dados confidenciais armazenados no armazenamento em nuvem sejam acessados.

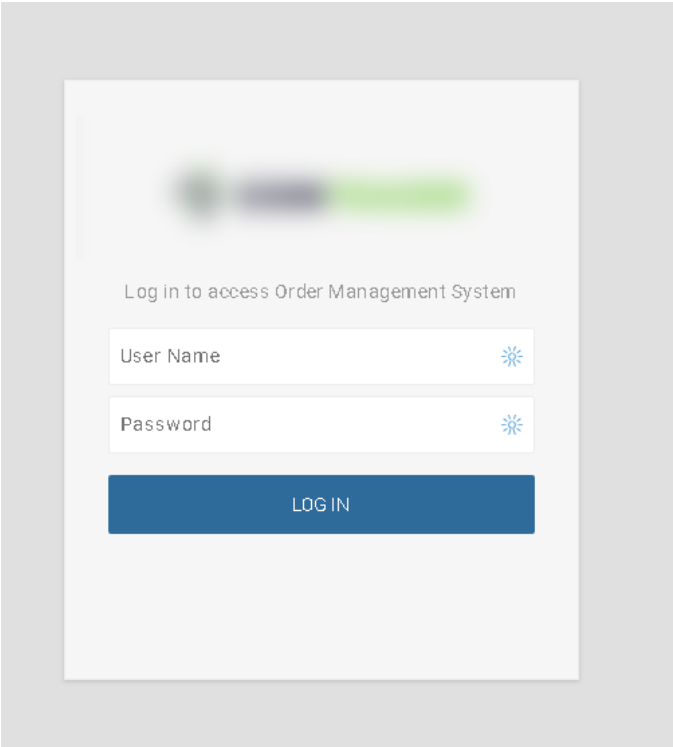
3.3 Vulnerabilidades de Risco Baixo Encontradas

- Deixar arquivos com informações confidenciais acessíveis ao provedor pode facilitar para o atacante encontrar vulnerabilidades em módulos utilizados na construção da plataforma, é recomendado remover ou restringir acesso a arquivos como *package.json e .gitignore* ou pastas como */.git/*, encontradas conforme abaixo;

```
{
  "name": "[illegible]",
  "version": "[illegible]",
  "description": "[illegible]",
  "repository": "[illegible]",
  "main": "[illegible]",
  "scripts":
    "test": "[illegible]o \"Error: no test specified\" && exit 1",
    "build": "[illegible] -rf build && mkdir build",
    "library": "cd components/library && sudo npm run build && cp -R build/. ../../js && cd ../..",
    "[illegible]": "cd components && sudo npm run build && cp -R build/. ../js && cd ..",
    "[illegible]": "node-sass --output-style compressed scss/shift/styles.scss assets/css/shift-styles.css",
    "[illegible]": "node-sass --output-style compressed scss/shift/wallet.scss assets/css/shift-wallet.css",
    "[illegible]": "node-sass --output-style compressed scss/shift/trade.scss assets/css/shift-trade.css",
    "[illegible]styles": "node-sass --watch --output-style compressed scss/shift/styles.scss assets/css/shift-styles.css",
    "[illegible]wallet": "node-sass --watch --output-style compressed scss/shift/wallet.scss assets/css/shift-wallet.css",
    "[illegible]trade": "node-sass --watch --output-style compressed scss/shift/trade.scss assets/css/shift-trade.css",
    "[illegible] admin && sudo npm run build && mkdir -p ../build/admin && cp -R build/. ../build/admin && cd ..",
    "[illegible]": "live-server",
    "[illegible]do npm run dev:server | sudo npm run watch-shiftstyles | sudo npm run watch-shiftwallet | sudo npm run watch-shifttrade",
    "[illegible]ld": "webpack --config webpack.config.js",
    "[illegible]components": "live-server --port=3030 --proxy=/js/widgets.min.js:http://localhost:8080/widgets.min.js --proxy=/js/widgets.min.js.map:http://localhost:8080/widgets.min.js.map"
  "[illegible]":
    "[illegible]": "[illegible]",
    "[illegible]": "[illegible]",
    "[illegible]":
      "[illegible]": "[illegible]",
      "[illegible]": "[illegible]",
      "[illegible]": "[illegible]",
```

Usuário:
Senha:
Acessar

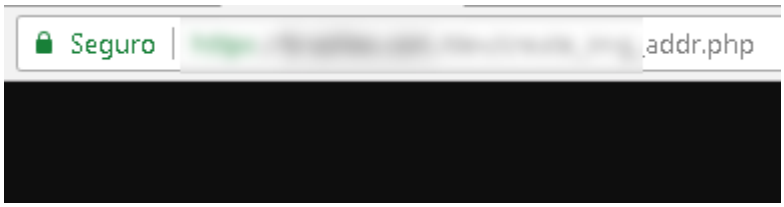

Fazer login
https://
Nome de usuário
Senha
Fazer login
Cancelar


Log in to access Order Management System
User Name
Password
LOG IN

- Não deixar exposto a página de acesso do PhpMyAdmin e/ou documentações que exponha a versão do mesmo, com essas informações é possível fazer ataques contra o gerenciador, conforme pode-se verificar abaixo;

Obs.: Esta corretora estava vulnerável ao CVE-2017-1000499[7].

- Foram encontrados endpoints que possibilitam uploads de arquivos em diversas corretoras, conforme pode se constatar abaixo, o que poderia ser utilizado de maneira mal intencionada;



[7] https://nvd.nist.gov/vuln/detail/CVE-2017-1000499

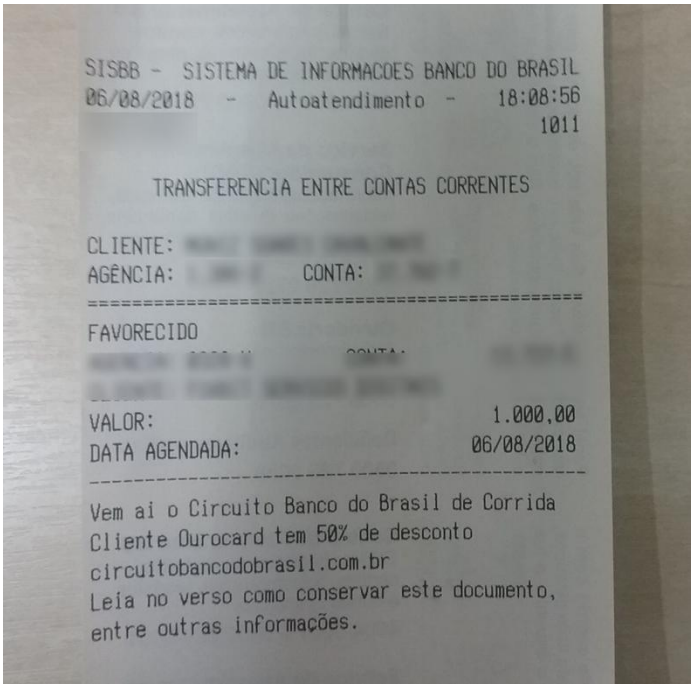
3.4 Vulnerabilidades de Risco Médio Encontradas

- Algumas corretoras estão com o modo DEBUG ativo - um dos principais recursos do modo de depuração é a exibição de páginas de erro detalhadas.
- É possível obter os dados de administradores, tais como logins de CMS utilizados em páginas institucionais de algumas corretoras, conforme comprovado abaixo;

- Foram encontradas credenciais de acesso a servidores, com dados privilegiados de clientes, em arquivos acessíveis publicamente, conforme evidenciado abaixo;

3.5 Vulnerabilidades de Risco Alto Encontradas

- Foram encontrados servidores com autenticação fraca e vulnerável a ataques para obtenção das credenciais de acesso;
- Foi encontrado Bucket da Amazon sem autenticação, contendo selfies de clientes com seus documentos pessoais e contas bancárias, conforme pode ser constatado abaixo;



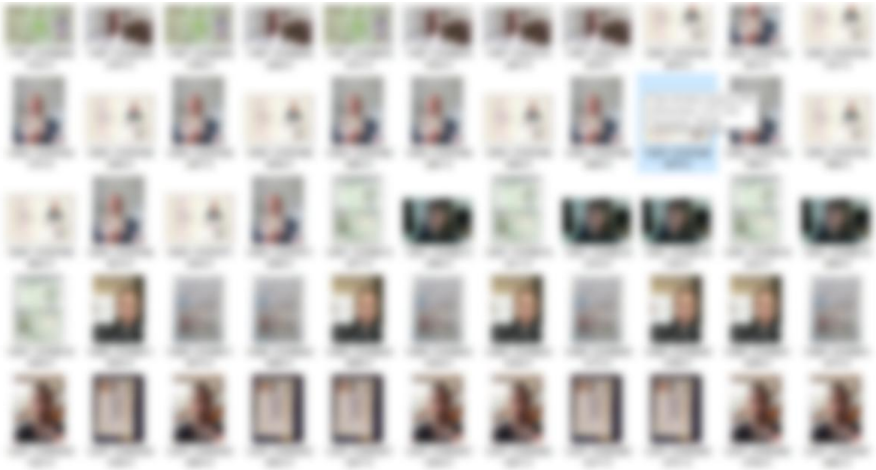
SISBB - SISTEMA DE INFORMACOES BANCO DO BRASIL
06/08/2018 - Autoatendimento - 18:08:56
1011

TRANSFERENCIA ENTRE CONTAS CORRENTES

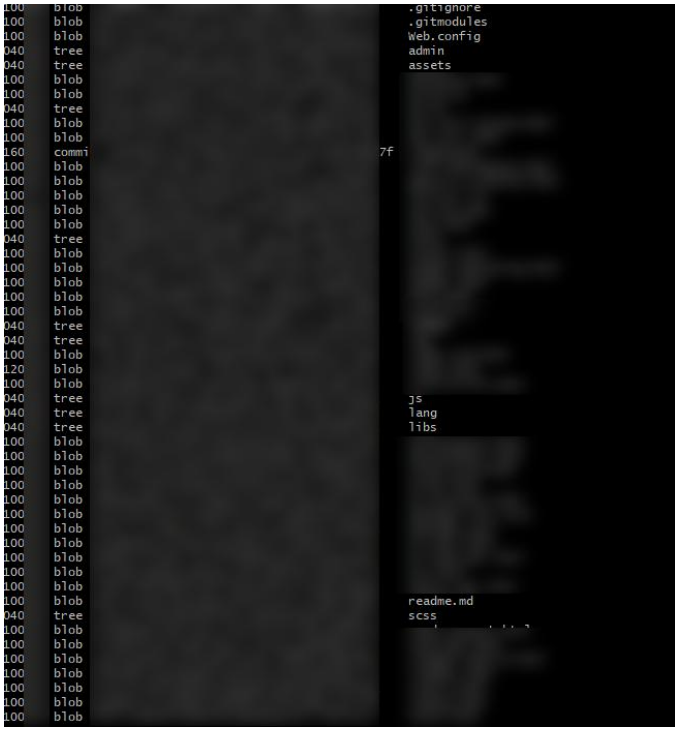
CLIENTE:
AGÊNCIA: CONTA:
==========
FAVORECIDO

VALOR: 1.000,00
DATA AGENDADA: 06/08/2018

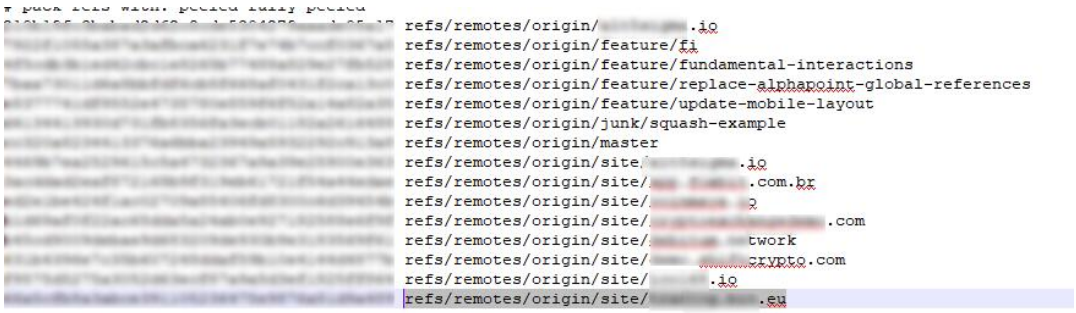
Vem ai o Circuito Banco do Brasil de Corrida
Cliente Ourocard tem 50% de desconto
circuitobancodobrasil.com.br
Leia no verso como conservar este documento,
entre outras informações.

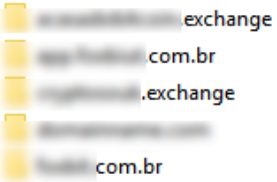


- Foram encontrados repositórios GIT em pastas de acessos públicos, onde foi possível montar a árvore de envio e chegar até o código-fonte da corretora, onde era possível ter acesso inclusive a chave privada da hot/cold wallet e todos os fundos da corretora através de uma montagem de repositório das alterações enviadas para o servidor, conforme pode-se comprovar a seguir;



- Foi encontrada vulnerabilidade em tecnologia de terceiros[8] utilizados como base de software de corretoras que possibilitou acesso aos repositórios de todos os clientes da mesma, inclusive de versões betas, conforme se pode verificar abaixo;





[8] Esta tecnologia de terceiro também é utilizada em uma das maiores corretoras nos Estados Unidos que também apresenta os mesmos problemas.

4. SERVIÇOS PRESTADOS

A Cryptocurrency Security Standards é um conselho, os serviços prestados são definidos anualmente por todos os membros e empresas filiadas.

Com um time de resposta rápida, peritos forenses licenciados e formalizados foi definido que no ano de 2018 estaremos exercendo as seguintes atividades:

Segurança da Informação

- Consultoria em Segurança da Informação e Comunicações;
- Elaboração de Políticas e Estratégias para Segurança da Informação e Comunicações;
- Elaboração de Relatórios de Segurança da Informação e Comunicações;
- Setor terceirizado de segurança da informação;
- Auxílio para certificação PCI-DSS.

Forense Computacional

- Análise de Incidentes de Segurança da Informação;
- Perícia Digital e Investigação de Crimes Cibernéticos;
- Elaboração de Laudos Periciais em Forense Computacional.

Pesquisas e Análise de Vulnerabilidades

- Análise de Vulnerabilidades e Testes de Intrusão em Ambientes Computacionais;
- Resposta a Incidentes Computacionais;
- Elaboração de Relatórios de Análise de Vulnerabilidades e de Testes de Intrusão em Ambientes Computacionais;
- Análise e planejamento de infraestrutura;
- Análise e planejamento de infraestrutura interna;
- Pesquisa e análise de aplicativos nativos (Android e iOS).

Treinamentos

- Ambiente de trabalho seguro.

5. SELO CCESS

O selo **C**rypto**c**urrency **E**xchange **S**ecurity **S**tandards (CCESS) foi desenvolvido para garantir que a corretora segue padrões de segurança impostos pelo conselho anual que abrange as áreas mais importantes de segurança da informação.

Há dois níveis do selo:

- **DAS:** corretora de destaque na verificação anual de segurança da informação para o desenvolvimento do relatório;
- **Seal I:** enquadra-se no **Selo I** das corretoras que cumprem todos os seguintes requisitos:

Carteira:

- As chaves e seeds são criadas pelo sistema que as usará;
- Endereços exclusivos devem ser gerados pela carteira para cada transação, os endereços podem seguir um padrão de negócio próprio ou Extended Public Key;
- Deve-se existir um backup da chave / seed das carteiras fortemente criptografado;
- O acesso à chave primária / seed requer um identificador 2FA;
- As chaves primárias / seed devem estar em um documento que descreve as ações específicas que devem ser tomadas por cada utilizador em um Sistema de Informações para regenerar o conjunto de chaves do sistema no caso de uma chave ter sido comprometida.

Concessão / Revogação de Políticas e Procedimentos

- A validação precisa ser manual para revogação de qualquer instrumento de acesso.

Auditorias de Segurança

- A corretora precisa passar por um mês de consultoria e testes padrões, definidos pelo Conselho.

Política de Saneantes de Dados

- Seguir um padrão de exclusão avançado.

Prova de Custódia

- Promover uma ou mais vias de comprovação de fundos.

Armazenamento de Informações

- Manter uma configuração de firewall para proteger os dados de clientes;
- Não usar os padrões de sistemas pré-instalados de sistema para a criptografia de senhas e outros parâmetros de segurança;
- Todos os dados dos clientes devem estar fortemente criptografados;
- Criptografar a transmissão dos dados de seus clientes;
- Atribuir um ID exclusivo para cada pessoa com computador de acesso para retorno de qualquer informação.

- **Seal II:** enquadra-se no **Selo II** das corretoras que cumprem todos os seguintes requisitos:

Carteira:

- A chave ou seed é gerada usando um Determinative Random Bit Generator (DRBG) que está em conformidade com NIST SP 800-90A, e foi semeado com pelo menos duas fontes separadas criptograficamente seguras de entropia que foram combinadas de uma maneira criptograficamente segura (por exemplo, SHA256 [UnguessableFactor1 + UnguessableFactor2]);
- Todas as chaves que possuem autoridade de assinatura em uma única carteira devem ser armazenadas por várias entidades ou um cofre bancário;
- Os backups das chaves necessita ser resistente a ondas eletromagnéticas, de material resistente e armazenada em um cofre de aço;
- Endereços exclusivos devem ser gerados pela carteira para cada transação, os endereços podem seguir um padrão de negócio próprio ou Extended Public Key;
- O acesso à chave primária / seed requer um identificador 2FA;
- As chaves primárias / seed devem estar em um documento que descreve as ações específicas que devem ser tomadas por cada utilizador em um Sistema de Informações para regenerar o conjunto de chaves do sistema no caso de uma chave ter sido comprometida.

Concessão / Revogação de Políticas e Procedimentos

- A validação precisa ser manual para revogação de qualquer instrumento de acesso.

Auditorias de Segurança

- A corretora precisa passar por um mês de consultoria e treinamento, também é necessário passar por testes padrões definidos pelo conselho.

Política de Saneantes de Dados

- Seguir um padrão de exclusão avançado;
- O disco de armazenamento precisa funcionar na arquitetura; RAID 1 e ser trocado a cada um ano.

Prova de Custódia

- Promover uma ou mais vias de comprovação de fundos a cada três meses.

Armazenamento de Informações

- Manter uma configuração de firewall para proteger os dados de clientes;
- Não usar os padrões de sistemas pré-instalados de sistema para a criptografia de senhas e outros parâmetros de segurança;
- Todos os dados dos clientes devem estar fortemente criptografados ;
- Criptografar a transmissão dos dados de seus clientes;
- Atribuir um ID exclusivo para cada pessoa com computador de acesso para retorno de qualquer informação;

6. PRINCIPAIS REFERÊNCIAS UTILIZADAS

OWASP. **OWASP Top 10 - The Ten Most Critical Web Application Security Risks (OWASP Top 10 - 2013)**. 2015. Disponível em: <https://www.owasp.org/index.php/Top_10_2013-Top_10>. Acesso em setembro de 2018.

OWASP. **OWASP Top 10 - The Ten Most Critical Web Application Security Risks (OWASP Top 10 - 2017)**. 2017. Disponível em: <https://www.owasp.org/index.php/Top_10_2017-Top_10>. Acesso em setembro de 2018.

OWASP. **OWASP Testing Guide v4 - Table of Contents**. 2017. Disponível em: <https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents>. Acesso em setembro de 2018.

OWASP. **Web Application Penetration Testing**. 2014. Disponível em: <https://www.owasp.org/index.php/Web_Application_Penetration_Testing>. Acesso em setembro de 2018.

OWASP. **OWASP Risk Rating Methodology**. 2016. Disponível em: <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology>. Acesso em setembro de 2018.

OWASP. **Threat Risk Modeling**. 2017. Disponível em: <https://www.owasp.org/index.php/Threat_Risk_Modeling>. Acesso em setembro de 2018.

FIRST. **Common Vulnerability Scoring System v3.0 - Specification Document**. 2017. Disponível em: <https://www.first.org/cvss/specification-document>. Acesso em setembro de 2018.

Cryptocurrency Security Standards

ccss@marciano.io