



# **Relatório de Análise de Vulnerabilidades e Testes de Intrusão**

**Classificação: PÚBLICA.**

**Última Revisão: 16/08/2019.**

**CONTEÚDO**

<b>1</b>	<b>SUMÁRIO EXECUTIVO</b>	<b>3</b>
1.1	Sobre a Access Security Lab	3
1.2	Código de Ética	3
<b>2</b>	<b>INTRODUÇÃO</b>	<b>4</b>
2.1	Aviso Legal	4
2.2	Contexto	4
2.3	Objetivo	5
2.4	Escopo	5
2.5	Não Escopo	6
2.6	Descrição dos Testes	6
<b>3</b>	<b>METODOLOGIA</b>	<b>7</b>
3.1	Identificação de Ameaças	7
3.2	Detecção de Vulnerabilidades	8
3.3	Avaliação das Vulnerabilidades	8
3.4	Exploração das Vulnerabilidades	8
3.5	Relatório	8
3.6	Padrões	8
3.7	Garantia de Qualidade	9
<b>4</b>	<b>EQUIPE TÉCNICA</b>	<b>9</b>
<b>5</b>	<b>CRONOGRAMA DE ATIVIDADES</b>	<b>10</b>
<b>6</b>	<b>NÍVEIS DE CRITICIDADE</b>	<b>10</b>
<b>7</b>	<b>VULNERABILIDADES ENCONTRADAS</b>	<b>11</b>
<b>8</b>	<b>CONCLUSÕES E RECOMENDAÇÕES GERAIS</b>	<b>20</b>
<b>9</b>	<b>PRINCIPAIS REFERÊNCIAS UTILIZADAS</b>	<b>20</b>

## 1 SUMÁRIO EXECUTIVO

Este relatório reflete os resultados da análise de vulnerabilidades e testes de intrusão da plataforma de investimentos em criptomoedas AnubisTrade (<https://anubis.website/>), realizados durante a segunda quinzena de julho de 2019.

A avaliação foi realizada para identificar vulnerabilidades que poderiam ser aproveitadas por invasores, cujo escopo foi definido como o ambiente computacional da plataforma de investimentos.

A maioria dos controles de segurança foi testada manualmente, seguindo uma abordagem padronizada e as vulnerabilidades identificadas foram revisadas para eliminar os falsos positivos e priorizadas de acordo com o risco relacionado.

### 1.1 Sobre a Access Security Lab

A Access Security Lab (ACCESS) surgiu da ideia de se testar a segurança de corretoras (exchanges) brasileiras de criptomoedas. Formado por um grupo especializado de bounty hunters, a iniciativa atua de forma preventiva e já ajudou na correção de mais de 35 vulnerabilidades em plataformas do tipo e prevenindo o roubo de mais de 100 milhões de reais em criptoativos em um curto período.

Assim, o projeto cresceu, tomou forma e hoje está focado em análise de vulnerabilidades, testes de intrusão e perícia digital nos mais variados tipos de ambientes computacionais, especialmente plataformas financeiras.

A empresa conta, ainda, com uma excelente equipe de pesquisadores especializados em White Hat, Offensive Security e Perícia Digital, prestando serviços correlatos de:

- Consultoria em Segurança da Informação;
- Análise de Vulnerabilidades e Testes de Intrusão,
- Perícia Forense;
- Resposta a Incidentes;
- Implementação de Protocolos de Segurança;
- Planejamento Estratégico;
- Treinamentos em Segurança da Informação, Ethical Hacking e Perícia Digital.

### 1.2 Código de Ética

Os profissionais da Access Security Lab aplicam e mantêm os seguintes princípios:

- **Integridade:** a integridade dos pentesters estabelece confiança e, portanto, fornece a base para a confiança em seu julgamento;
- **Objetividade:** os pentesters possuem o mais alto nível de objetividade profissional na coleta, avaliação e comunicação de informações sobre a atividade ou processo que está sendo examinado, fazendo uma avaliação equilibrada de todas as circunstâncias relevantes para suas análises e não são indevidamente influenciados por seus próprios interesses ou por outros na formação de julgamentos;
- **Confidencialidade:** os pentesters respeitam o valor e a propriedade das informações que recebem e não divulgam informações sem a devida autoridade, a menos que haja uma obrigação legal ou profissional de fazê-lo;
- **Competência:** os pentesters aplicam os conhecimentos, habilidades e experiência necessários no desempenho dos serviços de análise de vulnerabilidades e testes de intrusão.

## 2 INTRODUÇÃO

A ACCESS realizou análise de vulnerabilidades e testes de intrusão na plataforma AnubisTrade, conforme definido no "Escopo" deste relatório, cujos resultados serão abordados adiante.

Os testes de segurança foram realizados no período de 22/07/2019 a 30/07/2019 e seu objetivo foi identificar falhas de segurança e propor recomendações para sua correção.

As vulnerabilidades descobertas se valeram de testes de segurança manuais direcionados que foram armazenados em backup com ferramentas que permitem a automação de tarefas.

As fragilidades identificadas foram avaliadas e priorizadas de acordo com seu risco relativo e medidas para sua remediação também foram propostas.

### 2.1 Aviso Legal

Todo o trabalho de avaliação para a elaboração deste documento foi realizado de acordo com as melhores práticas de mercado e em conformidade com as obrigações e regulamentos impostos tanto pela legislação vigente, quanto pelo estabelecido em contrato com a AnubisTrade.

As informações contidas neste relatório estão sujeitas e limitadas pelas condições descritas nas seções de "Escopo" e "Objetivos" e conforme as condições acordadas para a realização das atividades de análise de vulnerabilidades e testes de intrusão.

Em qualquer auditoria ou avaliação autorizada, o tempo e os recursos são naturalmente limitados e, portanto, quando comparado ao tempo e recursos potencialmente ilimitados disponíveis para partes com intenção maliciosa, a existência de vulnerabilidades será verificada, mas a inexistência de todos e quaisquer tipos de fragilidades não pode ser assegurado absolutamente.

Neste contexto, embora tenham sido feitos todos os esforços para auditar e avaliar a segurança do ambiente computacional da AnubisTrade, este relatório não garante de forma alguma o estabelecimento de um sistema impenetrável. Sendo assim, a Access Security Lab não se responsabiliza por qualquer perda ou dano direto ou indireto causado por qualquer falha ou violação dos sistemas desta da plataforma de investimentos em criptomoedas.

Por fim, as informações deste relatório têm classificação PÚBLICA e devem ser usadas apenas pela AnubisTrade e pela Access Security Lab, sendo de inteira e única responsabilidade de ambas.

### 2.2 Contexto

Nascida no começo de 2018, a AnubisTrade é uma plataforma de arbitragem automatizada de criptoativos (Bitcoin) desenvolvida em ASP.NET, na qual o usuário se cadastra e recebe uma carteira única de depósito em Bitcoin. Nela, é possível acompanhar o rendimento de forma centralizada, acessível por computador e smartphone, com dupla autenticação para a realização de saques, através de funções básicas de credenciais, como e-mail e senha.

O projeto nasceu no ambiente open-source como um robô que atuava na corretora Poloniex, após um tempo agindo, o robô foi migrado para as corretoras Binance e Bitmex junto com adaptações em seu modelo de negócio, sendo então fundada a plataforma AnubisTrade, escopo deste relatório.

Hoje, a AnubisTrade constitui-se de um robô que utiliza a análise técnica, price action e tape reading para realizar compras e vendas, ininterruptas e instantâneas, de criptomoedas na Binance e Bitmex, assumindo os papéis de tomada de decisão e de operacionalização e dividindo os lucros (ou prejuízos) com seus clientes, isto é, na plataforma os clientes podem realizar o depósito de Bitcoins para que sejam realizadas as operações de trading de forma automatizada, sem a necessidade de acompanhamento do mercado, cujo maior diferencial é o zelo pela transparência e segurança de seus serviços - motivo pelo qual os testes aqui descritos foram contratados e realizados.

### 2.3 Objetivo

O objetivo dos testes foi fornecer uma opinião independente e confiável sobre a segurança do ambiente computacional da AnubisTrade. Dessa forma, a avaliação identificou vulnerabilidades e quantificou sua criticidade, para que as mesmas possam ser geridas, resolvidas e, conseqüentemente, ajudar a prevenir o mau funcionamento e/ou perda financeira por meio de fraudes, fornecer diligências a regulações a clientes, e proteger a marca contra a perda de reputação.

### 2.4 Escopo

Os testes realizados foram do tipo “black-box” e seguiram uma abordagem baseada em riscos, de tal forma que levaram em consideração a experiência e melhores práticas de mercado. Portanto, o principal objetivo alcançado através da adoção de metodologia, detalha adiante, que consistiu em priorizar e otimizar as validações realizadas, fornecendo garantias em termos de cobertura ao minimizar as chances de uma falha evidente escapar ao processo de análise.

Ademais, também foram realizados testes básicos de verificação de segurança em IPs obtidos indiretamente, isto é, IPs que são públicos e que foram conseguidos através de consulta ao “Censys” e ao “DNSdumpster” - ferramentas de pesquisa de domínio gratuitas que visam descobrir hosts relacionados a um domínio, conforme mostrados na Figura 1 e mapeados na Figura 2 a seguir.

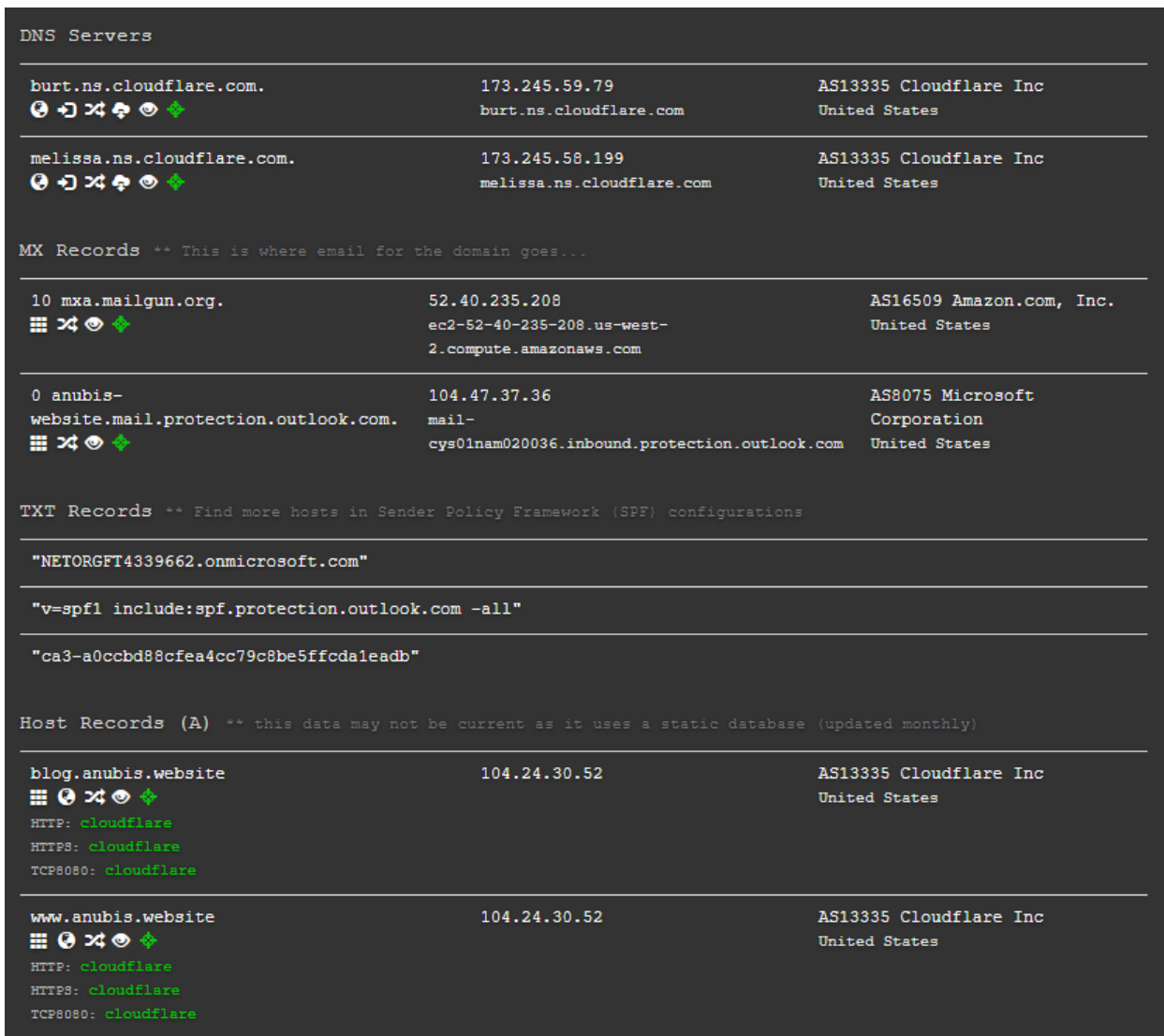


Figura 1. Endereços IP para o domínio “anubis.website”.

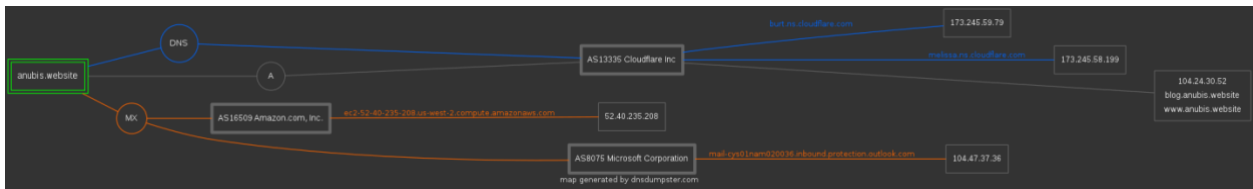


Figura 2. Mapeamento dos endereços IP para o domínio “anubis.website”.

A Tabela 1 apresenta a relação dos IPs da AnubisTrade, obtidos durante os testes de reconhecimento do ambiente, os quais foram analisados.

Tabela 1. Relação de IPs mapeados e testados.

HOSTNAME	IP
email.anubis.website	45.40.130.40
autodiscover.anubis.website	52.97.146.184
sip.anubis.website	52.112.66.139
msoid.anubis.website	40.126.17.39
lyncdiscover.anubis.website	52.112.65.206
anubis.website	104.24.30.52 / 23.245.24.154
www.anubis.website	104.24.30.52 / 23.245.24.154
blog.anubis.website	104.24.31.52

### 2.5 Não Escopo

Todos os devidos cuidados foram tomados para não prejudicar o funcionamento da AnubisTrade, a fim de não causar impacto em seus sistemas ou interferir nos negócios diários da plataforma. Não fazem parte do escopo atividades/ataques de engenharia social e correlatos, que visam a manipulação da confiança de clientes e seu comportamento quanto ao uso dos serviços.

### 2.6 Descrição dos Testes

O cerne do processo de realização dos testes se baseou em aferir a resistência do ambiente computacional e, por conseguinte, dos sistemas que estejam disponibilizados no mesmo, frente aos ataques indicados pela Tabela 2 abaixo. Para tanto, a Access Security Lab se valeu de um conjunto abrangente de ferramentas para análise de vulnerabilidades e verificações de segurança específicas para testes de intrusão e desenvolvidas com base nas metodologias utilizadas.

Tabela 2. Tipo e descrição dos testes realizados.

TIPO DE TESTE	DESCRIÇÃO
Injeção de Código	Ocorre quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta.
Quebra de Autenticação e Gerenciamento de Sessão	Ocorre quando as funções da aplicação relacionadas à autenticação e gerenciamento de sessão estão 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.
Quebra de Controle de Acesso	Ocorre quando não são aplicadas restrições sobre o que os usuários autenticados podem fazer.
Configurações Incorretas de Segurança	Ocorrem quando não há definição de configurações seguras a serem adotadas em redes, aplicações, frameworks, servidores, sistemas operacionais etc.

Exposição de Dados Sensíveis	Ocorre quando não há a devida proteção de dados sensíveis.
Proteção Insuficiente Contra Ataques	Ocorre quando aplicativos e APIs não são capazes de detectar, prevenir e responder a ataques manuais e automatizados.
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 com Vulnerabilidades Conhecidas	Ocorre quando componentes como bibliotecas, frameworks e outros módulos de software, são executados com privilégios de sistema.
APIs Subprotegidas	Ocorrem quando aplicações que possuem APIs estão desprotegidas, as quais podem conter diversas vulnerabilidades.
Injeção de SQL	Ocorre quando é possível manipular uma consulta a bancos de dados, ou seja, quando um atacante consegue manipular e inserir indevidamente instruções dentro de uma consulta a banco de dados.
Fingerprinting / Footprinting	Ocorre quando é possível descobrir/coletar informações de rede, serviços, computador, sistema operacional e/ou usuário(s).
Sistema Operacional Mal Configurado / Protegido	Ocorre quando o sistema operacional está com as configurações padrão ou quando não foi protegido/configurado adequadamente.
Ambiente de Rede Mal Configurado / Protegido	Ocorre quando o ambiente de rede está com as configurações padrão ou quando não foi protegido/configurado adequadamente.
Sniffing	Ocorre quando é possível capturar o tráfego da rede, a fim de se obter e/ou manipular arquivos ou senhas que estejam desprotegidos.

### 3 METODOLOGIA

As etapas a seguir, ilustradas na Figura 3, foram conduzidas para fornecer uma opinião independente e profissional em relação à eficácia e adequação dos controles de segurança do ambiente testado:

- **Identificação de Ameaças:** identificar ameaças e potenciais superfícies de ataques;
- **Detecção de Vulnerabilidade:** avaliar o cenário de segurança;
- **Avaliação:** avaliar e priorizar as vulnerabilidades identificadas;
- **Exploração:** explorar as vulnerabilidades identificadas a fim de se demonstrar seu impacto potencial à confidencialidade e à integridade das informações;
- **Relatório:** determinar medidas apropriadas para eliminar ou minimizar riscos.



Figura 3. Ilustração das etapas do processo de testes de intrusão.

#### 3.1 Identificação de Ameaças

A primeira fase da avaliação concentrou-se na coleta, análise e estruturação de informações sobre os itens do escopo, utilizando principalmente técnicas de análise passiva, além de fontes públicas, como sites, blogs e mecanismos de pesquisa, que foram consultadas para obtenção e reconhecimento de informações sobre o ambiente testado. Isso é feito para identificar a superfície de ataque e coletar informações necessárias para conduzir as demais fases dos testes. Dessa forma, as ameaças potenciais puderam ser identificadas e classificadas de acordo com seu risco.

### 3.2 Detecção de Vulnerabilidades

Testes automatizados e manuais foram combinadas para cobrir a maioria das vulnerabilidades potenciais. Sendo assim, ao testar manualmente os aspectos críticos, as falhas de segurança que não são cobertas pela abordagem de testes automatizados puderam ser descobertas, além da avaliação em relação às melhores práticas de mercado para segurança da informação.

### 3.3 Avaliação das Vulnerabilidades

Os resultados das análises manuais e automatizadas foram verificados quanto à sua integridade e razoabilidade a fim de se diminuir o risco de vulnerabilidades não identificadas (falsos negativos) para um nível aceitável. Com isso, as descobertas foram avaliadas e reavaliadas individualmente para verificar se elas representavam, de fato, vulnerabilidades. Logo após, é atribuída às descobertas uma pontuação com base no OWASP Risk Rating Methodology<sup>1</sup> e no Common Vulnerability Scoring System<sup>2</sup> para categorizar seus impactos.

### 3.4 Exploração das Vulnerabilidades

A exploração das vulnerabilidades encontradas consistiu em avaliar a aplicabilidade dos tipos de ataques contemplados na Tabela 2. Sendo assim, objetivou-se, com isso, extrair uma lista de ataques e possíveis fragilidades, elegíveis para exploração, tendo como alvo o ambiente computacional da AnubisTrade e, por conseguinte, dos sistemas que estejam disponibilizados no mesmo. Dessa forma, essa fase levou em conta características relevantes e inerentes ao ambiente como um todo, a fim de se eleger as validações que foram efetuadas.

### 3.5 Relatório

O cliente foi regularmente informado sobre o status e o andamento dos testes, que consistia em um resumo do progresso geral e informações sobre quaisquer questões que interferissem e gerassem problemas tanto para a AnubisTrade, em relação a seus serviços e clientes, quanto para a Access Security Lab, quando da realização dos testes. Sendo que os resultados da avaliação foram aqui documentados e serão entregues na forma deste relatório.

### 3.6 Padrões

Os padrões utilizados 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. Sendo que os trabalhos relacionados mais conhecidos reúnem os riscos de ataques críticos exploráveis a partir de vulnerabilidades em aplicações web e em ambientes computacionais que fazem uso de criptomoedas, nos quais os testes basearam-se:

---

<sup>1</sup> [https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)

<sup>2</sup> <https://www.first.org/cvss/specification-document>



- Os 10 principais riscos de segurança de aplicações do OWASP (OWASP Top 10<sup>3</sup>);
- Guia de testes de intrusão do OWASP (OWASP Testing Guide<sup>4</sup>);
- Publicação Especial 800-115 do NIST (NIST SP 800-115<sup>5</sup>);
- Padrão de Segurança para Criptomoeda (CCSS<sup>6</sup>).

Sendo assim, além de identificar os ataques de maior risco e criticidade, foram feitas recomendações de segurança para que cada um deles seja evitado a partir das etapas do desenvolvimento das aplicações e de sua disponibilização em produção.

### 3.7 Garantia de Qualidade

Todos os testes, assim como o relatório, foram conduzidos e elaborados por especialistas experientes e certificados na área. De tal forma que o processo de garantia de qualidade foi executado em paralelo com as fases dos testes, as quais foram individualmente acompanhadas e verificadas a fim de se obter integridade e precisão em seu andamento e condução.

## 4 EQUIPE TÉCNICA

NOME	RESPONSABILIDADES	QUALIFICAÇÕES
Bruno da Silva.	Testes de estresse e penetração invasivos e elaboração de provas de conceito.	Analista de redes com experiência em testes de intrusão e transações com criptomoedas.
Carlos Giovanella.	Reconhecimento, testes de CVEs relacionados e OWASP.	Bug Hunter com mais de 40 vulnerabilidades críticas relatadas na BugCrowd e na Hackerone. Hall of fame da Jet.com.
Deivison Franco.	Elaboração do relatório, consultoria geral, cálculo e análises de vetores de ataque e riscos associados.	Mestre em Inovação Tecnológica e em Ciência da Computação. Consultor em Segurança da Informação e Perícia Digital. Autor e revisor do livro Tratado de Computação Forense e das revistas eForensics Magazine, Hakin9 Magazine e Pentest Magazine.
Leandro Trindade.	Coordenação de operações, testes, hipóteses, provas de conceito e relatoria.	Bacharel em Ciência da Computação especializado em segurança de sistemas computacionais.
Leonardo Marciano.	Teste de CVEs relacionados, OWASP e produção do relatório.	Vencedor de mais de 17 hackathons, com destaque para o “Nasa Space Apps CWB”.
Vinicius Valério.	Reconhecimento do ambiente, testes de penetração invasivos, hipóteses, elaboração de conceitos e consultoria.	Bug Hunter com mais de 285 vulnerabilidades relatadas no OpenBugBounty. Hall of fame da Netflix, IBM e NASA.

<sup>3</sup> [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_2017\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project)

<sup>4</sup> [https://www.owasp.org/index.php/OWASP\\_Testing\\_Guide\\_v4\\_Table\\_of\\_Contents](https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents)

<sup>5</sup> <https://csrc.nist.gov/publications/detail/sp/800-115/final>

<sup>6</sup> <https://cryptoconsortium.github.io/CCSS/>

## 5 CRONOGRAMA DE ATIVIDADES

ATIVIDADE	DATA DE REALIZAÇÃO
Pesquisas e reconhecimento de sistemas computacionais envolvidos no escopo.	22 de julho de 2019.
Testes de penetração semiautomáticos e manuais, elaboração e teste de hipóteses.	29 de julho de 2019.
Provas de conceito e conclusão dos testes.	30 de julho de 2019.
Avaliação de riscos, vetores e esboço do relatório.	03 de agosto de 2019.
Conclusão e revisão final do relatório.	07 de agosto de 2019.

## 6 NÍVEIS DE CRITICIDADE

Para categorizar o impacto e a exploração de vulnerabilidades, os níveis de criticidade usados na seção “Vulnerabilidades Encontradas” estão de acordo com a Versão 3 do Common Vulnerability Scoring System (CVSS v3.1) do NIST, o qual utiliza a pontuação básica composta pelo tipo de acesso, a complexidade de acesso e o nível de autenticação exigido para explorar uma determinada vulnerabilidade, bem como o impacto relacionado à confidencialidade, integridade e disponibilidade.

A pontuação aplicada às vulnerabilidades varia de 0 a 10 pontos e é normalizada categorizando-as em níveis críticos, altos, médios e baixos de criticidade. Além disso, o vetor exato é fornecido para calcular a pontuação específica, a fim de se garantir sua transparência, ou seja, o vetor é construído com base nas seguintes métricas:

- **Vetor de Acesso (AV):** descreve a fonte necessária de ataque para explorar uma vulnerabilidade, cujos valores possíveis são Local (L), Rede Adjacente (A) ou Rede (N);
- **Complexidade do Acesso (AC):** está relacionado à complexidade das condições que precisam estar em vigor para uma exploração bem-sucedida. Os valores possíveis são Alto (H), Médio (M) e Baixo (L);
- **Autenticação (AU):** refere-se aos níveis de autenticação que um invasor precisa transmitir para explorar uma vulnerabilidade. Os valores possíveis são Requer Várias Instâncias (M), Requer Instância Única (S) e Nenhum Requerido (N);
- **Confidencialidade (C), Integridade (I), Disponibilidade (A):** quando há impacto na confidencialidade, integridade ou disponibilidade, e cujos possíveis valores são Nenhum (N), Parcial (P) e Completo (C).

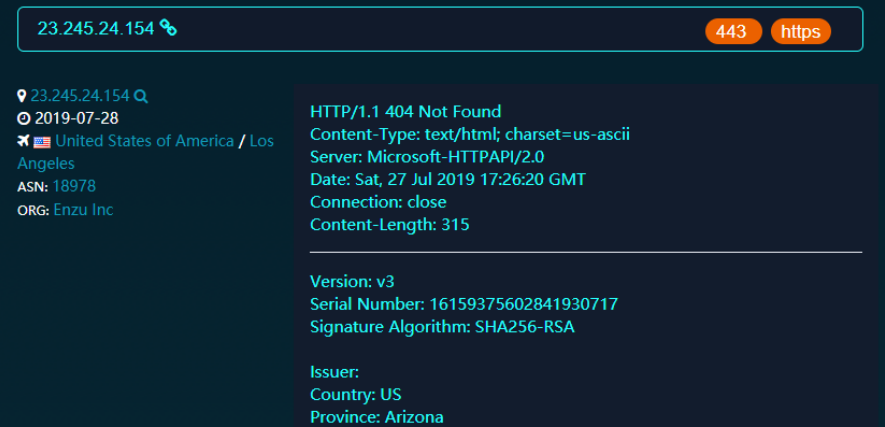

Diante do exposto, os níveis de criticidade definidos podem ser visualizados na Tabela 3, a seguir, de acordo com o resultado da soma de seus fatores de risco, juntamente com seu respectivo significado. Tais níveis foram utilizados para representar o risco e a criticidade calculados para cada uma das vulnerabilidades que identificadas.

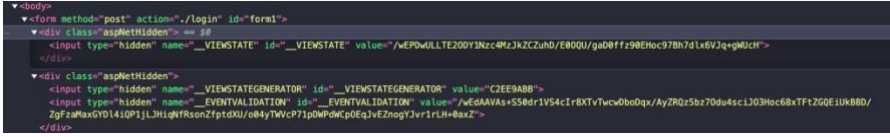
Tabela 3. Níveis de criticidade e descrição.

CRITICIDADE	DESCRIÇÃO
<b>Crítica</b>	<ul style="list-style-type: none"> <li>• Pontuação Base do CVSS: 8 a 10 pontos;</li> <li>• Exploração trivial;</li> <li>• Perda de confidencialidade, integridade e disponibilidade.</li> </ul> <p><b>A remediação imediata é crítica para os negócios.</b></p>
<b>Alta</b>	<ul style="list-style-type: none"> <li>• Pontuação Base do CVSS: de 6 a 7.9 pontos;</li> <li>• Exploração quase trivial;</li> <li>• Perda ou de confidencialidade, ou de integridade ou de disponibilidade.</li> </ul> <p><b>A remediação é crítica para os negócios.</b></p>
<b>Média</b>	<ul style="list-style-type: none"> <li>• Pontuação Base do CVSS: de 4 a 5.9 pontos;</li> <li>• Exploração possível e comum, mas requer habilidades;</li> <li>• Sério impacto na confidencialidade, integridade e disponibilidade.</li> </ul> <p><b>Ações corretivas são exigidas dentro de um prazo razoável.</b></p>
<b>Baixa</b>	<ul style="list-style-type: none"> <li>• Pontuação Base do CVSS: de 0.1 a 3.9 pontos;</li> <li>• Exploração possível, mas difícil e improvável;</li> <li>• Impacto mensurável na confidencialidade, integridade e disponibilidade.</li> </ul> <p><b>Ações corretivas são recomendadas.</b></p>
<b>Informativa</b>	<p><b>Nenhuma vulnerabilidade real foi identificada, mas há informações que podem ser relevantes para melhorar a segurança do ambiente.</b></p>

## 7 VULNERABILIDADES ENCONTRADAS

ID da Vulnerabilidade	1
<b>Criticidade</b>	<b>Informativa</b>
<b>Título</b>	IP real exposto, via certificado, e respondendo a requisições diretas.
<b>Descrição</b>	<p>O IP real do servidor está exposto através do certificado, e ao realizar uma conexão com a porta 443 é possível descobrir a qual servidor pertence aquele endereço de IP.</p> <p>Além disso, o servidor está respondendo a conexões na porta 80 e, alterando-se o URL do request para “anubis.website”, o sistema responde normalmente com a página, permitindo um bypass completo das proteções oferecidas pela CDN da Cloudflare.</p>
<b>URL Afetado</b>	<a href="https://23.245.24.154:443">https://23.245.24.154:443</a>

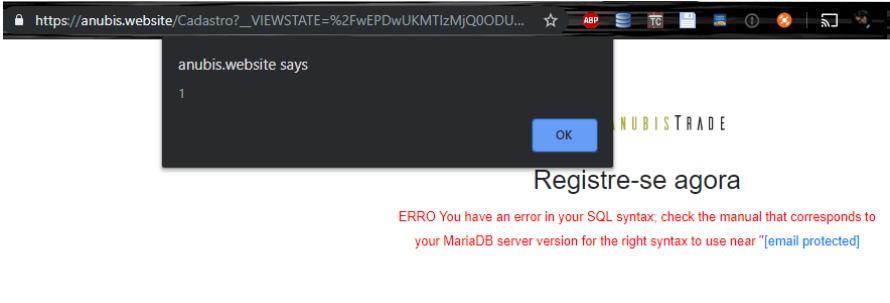
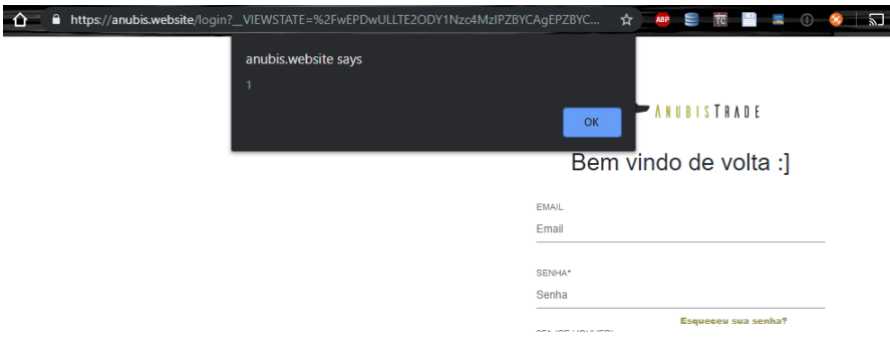
<p>Evidência/PoC</p>	 <p>23.245.24.154 443 https</p> <p>23.245.24.154 2019-07-28 United States of America / Los Angeles ASN: 18978 ORG: Enzu Inc</p> <p>HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sat, 27 Jul 2019 17:26:20 GMT Connection: close Content-Length: 315</p> <p>Version: v3 Serial Number: 16159375602841930717 Signature Algorithm: SHA256-RSA</p> <p>Issuer: Country: US Province: Arizona</p> <p>DNS Names: anubis.website www.anubis.website</p> <p>Certificate Signature Algorithm: SHA256-RSA Certificate Signature: 94:B0:FB:82:AF:7A:A1:33:F1:2D:49:D8:84:A4:AA:2D: 84:37:D3:3E:11:2C:CA:9C:54:7E:50:29:0C:3E:1E:12:</p> <p>General Request URL: https://anubis.website/ Request Method: GET Status Code: 200 Remote Address: 23.245.24.154:443 Referrer Policy: no-referrer-when-downgrade</p> <p>Response Headers cache-control: private content-length: 85861 content-type: text/html; charset=utf-8 date: Mon, 05 Aug 2019 04:38:02 GMT server: Microsoft-IIS/10.0 status: 200 x-aspnet-version: 4.0.30319 x-powered-by: ASP.NET</p> <p>Request Headers :authority: anubis.website</p>  <p>Dificuldades para investir? Conheça a forma mais simples e segura de investir em Criptomoedas. *Taxa de 0% para depósitos e saques. COMECE AGORA SAIBA MAIS</p>
<p>Recomendação</p>	<p>Utilizar intranet para o consumo de serviços de terceiros expostos, junto com uma autenticação de usuário e senha.</p>
<p>Referência</p>	<p><a href="https://citadelo.com/en/blog/cloudflare-how-to-do-it-right-and-do-not-reveal-your-real-ip/">https://citadelo.com/en/blog/cloudflare-how-to-do-it-right-and-do-not-reveal-your-real-ip/</a></p>

<b>ID da Vulnerabilidade</b>	<b>2</b>
<b>Criticidade</b>	<b>Informativa</b>
<b>Título</b>	ViewState sem criptografia.
<b>Descrição</b>	<p>A aplicação utiliza ViewState sem criptografia, o que pode permitir a um invasor estudar a lógica de gerenciamento de estado do aplicativo para possíveis vulnerabilidades.</p> <p>Dessa forma, se a aplicação armazenar informações críticas para o aplicativo no ViewState, ele também será revelado.</p>
<b>URL Afetado</b>	<a href="https://anubis.website/Panel">https://anubis.website/Panel</a>
<b>Evidência/PoC</b>	
<b>Recomendação</b>	Criptografar todos os estados da aplicação.
<b>Referência</b>	<a href="https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/viewstate-is-not-encrypted/">https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/viewstate-is-not-encrypted/</a>

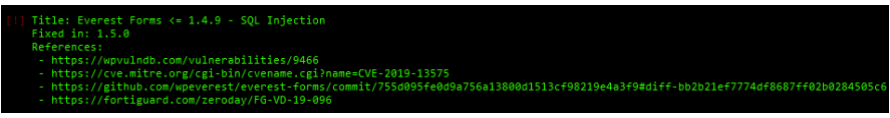
<b>ID da Vulnerabilidade</b>	<b>3</b>
<b>Criticidade</b>	<b>Informativa</b>
<b>Título</b>	Vazamento de usuários do WordPress.
<b>Descrição</b>	<p>Detectou-se um endpoint do WordPress vulnerável, o qual permite a listagem de usuários da plataforma, facilitando ataques de bruteforce.</p>
<b>URL Afetado</b>	<a href="http://blog.anubis.website/wp-json/wp/v2/users/">http://blog.anubis.website/wp-json/wp/v2/users/</a>
<b>Evidência/PoC</b>	
<b>Recomendações</b>	<p>Ocultar endpoints que não sejam necessários à aplicação e retornar erros ao serem acessados;</p> <p>Desativar a API REST do wordpress.</p>
<b>Referências</b>	<p><a href="https://wordpress.org/support/topic/rest-api-exposed-user-data-for-all-users/">https://wordpress.org/support/topic/rest-api-exposed-user-data-for-all-users/</a></p> <p><a href="https://wordpress.stackexchange.com/questions/252328/wordpress-4-7-1-rest-api-still-exposing-users">https://wordpress.stackexchange.com/questions/252328/wordpress-4-7-1-rest-api-still-exposing-users</a></p>






	<p><a href="https://anubis.website/Forgot?__VIEWSTATE=%2FwEPDwULLTEyNTUzOTM3MzQPZBYCAgEPZBYCAgMPDxYCHgRUZXh0BcQBRVJSTyBZb3UgaGF2ZSBhbiBlcnJvciBpb3VlIFNRTCBzeW50YXg7IGNoZWNRlHRoZSBtYW51YWwgdGhhdCBjb3JyZXNwb25kcyB0byB5b3VyIE1hcmlhRElqc2VydmVlIHZlcnNpb24gZm9yIHRoZSByaWdodCBzeW50YXggdG8gdXNlIG5lYXlqJydsdWx6QGdtYWlsLmNvbTwwPjxzdhIsZS9vbmxxvYWQ9YWxlc nQoMSk%2BXCcnIGF0IGxpbmUgMWRkZAI0Ck4rSPBbbnmk5xOa%2B7uSiagreOoV0vna164l1d9y">https://anubis.website/Forgot?__VIEWSTATE=%2FwEPDwULLTEyNTUzOTM3MzQPZBYCAgEPZBYCAgMPDxYCHgRUZXh0BcQBRVJSTyBZb3UgaGF2ZSBhbiBlcnJvciBpb3VlIFNRTCBzeW50YXg7IGNoZWNRlHRoZSBtYW51YWwgdGhhdCBjb3JyZXNwb25kcyB0byB5b3VyIE1hcmlhRElqc2VydmVlIHZlcnNpb24gZm9yIHRoZSByaWdodCBzeW50YXggdG8gdXNlIG5lYXlqJydsdWx6QGdtYWlsLmNvbTwwPjxzdhIsZS9vbmxxvYWQ9YWxlc nQoMSk%2BXCcnIGF0IGxpbmUgMWRkZAI0Ck4rSPBbbnmk5xOa%2B7uSiagreOoV0vna164l1d9y</a></p>
<p><b>Evidência/PoC</b></p>	 
<p><b>Recomendações</b></p>	<p>Realizar a filtragem em todos os campos da aplicação, não apenas nos de login, mas os campos em área logada como observação, carteira de saque etc., os quais estão permitindo a inclusão de tags html, conteúdo desnecessário para seu funcionamento;</p> <p>Usar a flag HTTPOnly na criação de cookies de sessão.</p>
<p><b>Referências</b></p>	<p><a href="https://cwe.mitre.org/data/definitions/79.html">https://cwe.mitre.org/data/definitions/79.html</a></p> <p><a href="https://www.owasp.org/index.php/Top_10-2017_A7-Cross-Site_Scripting_(XSS)">https://www.owasp.org/index.php/Top_10-2017_A7-Cross-Site_Scripting_(XSS)</a></p> <p><a href="https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)">https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)</a></p>



<b>ID da Vulnerabilidade</b>	6
<b>Criticidade</b>	Alta
<b>Título</b>	SQL Injection no blog através de vulnerabilidade no Everest Forms (CVE 2019-13575).
<b>Descrição</b>	<p>Vulnerabilidade descoberta recentemente no plugin Everest Forms que permite a um usuário autenticado realizar ataques de SQL Injection para escalar privilégios.</p> <p>De acordo com os testes realizados, esse ataque é feito no parâmetro "form_id" durante a geração de um relatório CSV.</p>
<b>Vetor CVSS</b>	AV:N / AC:L / PR:H / UI:N / S:C / C:L / I:L / A:L
<b>Pontuação CVSS</b>	6.6
<b>URL Afetado</b>	<a href="http://blog.anubis.website/wp-content/plugins/everest-forms/includes/evf-entry-functions.php">http://blog.anubis.website/wp-content/plugins/everest-forms/includes/evf-entry-functions.php</a>
<b>Evidência/PoC</b>	 <pre> [!] Title: Everest Forms &lt;= 1.4.9 - SQL Injection Fixed in: 1.5.0 References: - https://wpvulndb.com/vulnerabilities/9466 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13575 - https://github.com/wpeverest/everest-forms/commit/755d095fe0d9a756a13800d1513cf98219e4a3f9#diff-bb2b21ef7774df8687ff02b0284505c6 - https://fortiguard.com/zeroday/FG-VD-19-096           </pre>
<b>Recomendações</b>	<p>Atualizar os componentes de wordpress frequentemente;</p> <p>Seguir as listas de discussão a respeito para realizar a correção/mitigação de vulnerabilidades assim que forem descobertas;</p> <p>Atualizar o Everest Forms para a versão 1.5.0.</p>
<b>Referências</b>	<p><a href="https://cwe.mitre.org/data/definitions/89.html">https://cwe.mitre.org/data/definitions/89.html</a></p> <p><a href="https://wpvulndb.com/vulnerabilities/9466">https://wpvulndb.com/vulnerabilities/9466</a></p> <p><a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13575">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13575</a></p> <p><a href="https://github.com/wpeverest/everest-forms/commit/755d095fe0d9a756a13800d1513cf98219e4a3f9#diff-bb2b21ef7774df8687ff02b0284505c6">https://github.com/wpeverest/everest-forms/commit/755d095fe0d9a756a13800d1513cf98219e4a3f9#diff-bb2b21ef7774df8687ff02b0284505c6</a></p> <p><a href="https://fortiguard.com/zeroday/FG-VD-19-096">https://fortiguard.com/zeroday/FG-VD-19-096</a></p>

<b>ID da Vulnerabilidade</b>	7
<b>Criticidade</b>	<b>Crítica</b>
<b>Título</b>	Injeção de conteúdo no e-mail de login e recuperação de conta através do cabeçalho "X-Forwarded-For".
<b>Descrição</b>	<p>Ao realizar uma tentativa de login malsucedida ou uma recuperação de senha o sistema envia um e-mail alertando o cliente do IP que originou a mesma (o IP, neste caso, está sendo obtido através do cabeçalho "X-Forwarded-For").</p> <p>Esse cabeçalho, no entanto, não está sendo filtrado ou validado corretamente, permitindo que o mesmo seja manipulado por um atacante para injetar conteúdo HTML ou javascript em um e-mail.</p> <p>Esse tipo de ataque pode ser aproveitado para se realizar campanhas de phishing com alto índice de confiança, uma vez que o phishing partiria do próprio endereço de e-mail da AnubisTrade.</p> <p>Alguns clientes de e-mail vulneráveis permitem ainda a execução de código javascript, o que possibilita a um atacante a extração do código de redefinição de senha para roubo de conta.</p>
<b>Vetor CVSS</b>	AV:N / AC:L / PR:N / UI:R / S:C / C:H / I:H / A:N
<b>Pontuação CVSS</b>	9.3
<b>URLs Afetados</b>	<a href="https://anubis.website/Forgot">https://anubis.website/Forgot</a> <a href="https://anubis.website/login">https://anubis.website/login</a>
<b>Evidência/PoC</b>	<pre> POST /Login HTTP/1.1 Host: anubis.website Connection: close Content-Length: 743 Pragma: no-cache Cache-Control: no-cache Origin: https://anubis.website Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i Referer: https://anubis.website/Login Accept-Encoding: gzip, deflate Accept-Language: pt-BR,pt;q=0.9 X-Forwarded-For: &lt;h1&gt;HTML INJECT ON E-MAIL&lt;/h1&gt; Cookie: __cfduid=d4f9000bd5132f780f602b2b0e7f71c2f1559213296; _ ASP.NET_SessionId=todgi3nnihskryxdeghrzqzkt  __VIEWSTATE=%2FwEPDwULLTE2ODY1Nzc4MzJrZCZuhD%2FE00QU%2FgaD0ffz9 qx%2FAyZRQz5bz70du4sciJ03Hoc68xTFtZGQEIUrB8D%2FZgFzaMaxGYD14iQP kT0uS3x&amp;txt2FA=&amp;g-recaptcha-response=03A0LTBLTgmPZfVHr00jAL5PIz Ca0ja-JaKlL6-S42u3UXwj3BWx6Yf-dfcBRnyfbBkriNaGMf_WTxxg-gVzbZlGD yAB2LmD53Z8T54gMczMTF&amp;Button=Acessar+agora           </pre>

	 <p>Acompanhe nossos resultados</p> <p><b>Atenção Usuário, ERRO AO ACESSAR A SUA CONTA!</b></p> <p>Você acessou sua conta AnubisTrade com usuário ou senhas inválidos!</p> <p>IP de acesso:</p> <p><b>HTML INJECT ON E-MAIL</b></p> <p>Para sua segurança, enviamos um e-mail notificando sobre qualquer atividade em sua conta. Em caso de atividades suspeitas, altere a senha clicando <a href="#">aqui</a>.</p> <p>Recomendamos o uso de 2FA em todas as contas!</p> <p>Atenciosamente, <b>AnubisTrade</b>.</p> <p>Acompanhe o AnubisTrade nas redes sociais</p>
<p><b>Recomendações</b></p>	<p>Não utilizar o cabeçalho “X-Forwarded-For” para obter o IP do visitante;</p> <p>Utilizar dados diretos da conexão ou, em caso de uso de CDN Cloudflare, utilizar o cabeçalho “CF-Connecting-IP” provido pelo serviço;</p> <p>Realizar a filtragem de todos os dados vindos de entradas não confiáveis, principalmente os destinados ao e-mail, mesmo que estes sejam originados do banco de dados.</p>
<p><b>Referências</b></p>	<p><a href="https://cwe.mitre.org/data/definitions/79.html">https://cwe.mitre.org/data/definitions/79.html</a></p> <p><a href="https://cwe.mitre.org/data/definitions/345.html">https://cwe.mitre.org/data/definitions/345.html</a></p> <p><a href="https://capec.mitre.org/data/definitions/148.html">https://capec.mitre.org/data/definitions/148.html</a></p> <p><a href="https://www.owasp.org/index.php/Content_Spoofing">https://www.owasp.org/index.php/Content_Spoofing</a></p>

## 8 CONCLUSÕES E RECOMENDAÇÕES GERAIS

Conforme detalhado no item 6, e de acordo com as vulnerabilidades encontradas nos testes, é possível concluir que o sucesso de um ataque pode resultar em perdas financeiras, de ativos ou de recursos, além de causar danos à imagem da plataforma. Portanto, sua remediação é crítica para os negócios, exigindo que seja providenciada com urgência e em curto intervalo de tempo.

A abordagem dos testes realizados não considera a probabilidade do agente de ameaça, nem responde por qualquer um dos vários detalhes técnicos associados à sua aplicação específica. Qualquer um desses fatores poderia afetar significativamente a probabilidade global de um atacante encontrar e explorar uma vulnerabilidade particular. Esta classificação também não leva em conta o impacto real sobre o negócio. É necessário que a área específica de segurança da plataforma defina qual o grau de risco de segurança das aplicações que está disposta a aceitar.

Cabe ressaltar, por fim, que novas vulnerabilidades surgem a cada dia, através da implantação de novos softwares, mudanças nos códigos dos sistemas desenvolvidos internamente, e até mesmo com a descoberta de novas falhas em softwares já testados. Por isso, recomenda-se que rotinas de análises de vulnerabilidades e testes de intrusão sejam realizadas periodicamente.

## 9 PRINCIPAIS REFERÊNCIAS UTILIZADAS

C4. **CryptoCurrency Security Standard.** 2016. Disponível em: <<https://cryptoconsortium.github.io/CCSS>>. Acesso em julho de 2019.

FIRST. **Common Vulnerability Scoring System.** 2019. Disponível em: <<https://www.first.org/cvss/specification-document>>. Acesso em julho de 2019.

NIST. **SP 800-115 - Technical Guide to Information Security Testing and Assessment.** 2008. Disponível em: <<https://csrc.nist.gov/publications/detail/sp/800-115/final>>. Acesso em julho de 2019.

OWASP. **OWASP Risk Rating Methodology.** 2019. Disponível em: <[https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)>. Acesso em julho de 2019.

OWASP. **OWASP Testing Guide.** 2017. Disponível em: <[https://www.owasp.org/index.php/OWASP\\_Testing\\_Guide\\_v4\\_Table\\_of\\_Contents](https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents)>. Acesso em julho de 2019.

OWASP. **OWASP Top Ten.** 2017. Disponível em: <[https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_2017\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project)>. Acesso em julho de 2019.