Certificado de Testes de Intrusão

guardsi

Certificado de Pentest

Esta declaração certifica que a **Guardsi Tecnologia LTDA**, pessoa jurídica de direito privado, nome fantasia **GUARDSI**, inscrita no **CNPJ/MF** sob o nº 23.353.677/0001-09, uma empresa especializada em segurança da informação e testes de intrusão, em atividade desde 2015 e com reconhecida experiência em projetos de impacto significativo no território nacional, realizou testes de intrusão (pentest) em cada um dos sistemas da empresa **DOCSPIDER SOFTWARE S.A.**, nome fantasia **Docspider S.A.**, pessoa jurídica de direito privado, inscrita no **CNPJ/MF** sob nº 83.065.805/0001-40.

OBJETIVOS DO PENTEST

O propósito primordial destes testes de intrusão (também conhecido como "Pentest") consiste na identificação, validação e, subsequentemente, na documentação abrangente de vulnerabilidades que pudessem, direta ou indiretamente, comprometer os princípios basilares da segurança da informação. Estes princípios fundamentais, universalmente reconhecidos, incluem a disponibilidade, a confidencialidade e a integridade dos dados. O alcance deste projeto visa não apenas a uma mera detecção dessas falhas, mas também ao fornecimento de análises e recomendações para efetivar todas as correções. Após realizadas todas as correções propostas, a equipe de segurança da Guardsi também realiza novos testes de intrusão (retestes) em cada um dos sistemas para garantir que todas as falhas foram devidamente corrigidas, garantindo assim a completa efetividade de todas as correções propostas para cada vulnerabilidade de segurança encontrada durante os testes.

ESCOPO DOS TESTES

O escopo dos testes abrangeu de forma minuciosa as Aplicações Web e as APIs utilizadas pelos clientes da Docspider, incluindo uma avaliação completa de segurança em cada ponto de interação das plataformas. Essa análise detalhada teve como objetivo garantir que o ambiente estivesse em conformidade com as normas mais rigorosas de segurança, abrangendo desde as funcionalidades principais até os elementos auxiliares que possam expor as aplicações a riscos.

PERÍODO DE EXECUÇÃO DO PENTEST

O pentest teve seu início no dia 19 de janeiro de 2025 e finalização no dia 14 de fevereiro de 2025. Após esse período, a Guardsi iniciou sua consultoria em segurança da informação para acompanhamento da correção de todas as falhas, garantindo assim a correção efetiva de todas as vulnerabilidades encontradas, bem como a implementação de outras sugestões de segurança. Durante esse período, todas as superfícies dos sistemas foram avaliadas de maneira abrangente e detalhada, abrangendo diferentes níveis de criticidade e aplicando diversas metodologias, estratégias e abordagens para simular os mais variados cenários de ataques.

RETESTES DE CONFIRMAÇÃO

Os retestes tiveram início no dia 04 de abril de 2025 e finalizaram no dia 10 de abril de 2025. Durante este período, a equipe de segurança da Guardsi conduziu novos testes de intrusão em cada um dos sistemas para verificar a eficácia das correções implementadas nas vulnerabilidades previamente identificadas. A realização desses retestes garantiu que todas as falhas de segurança fossem devidamente corrigidas e que o ambiente se mantivesse seguro contra possíveis ameaças cibernéticas. Este intervalo foi suficiente para reavaliar todas as superfícies dos sistemas, abordando novamente todos os níveis de criticidade e utilizando diversos métodos e estratégias para assegurar a total eficácia das correções aplicadas.

EXEMPLOS DE TESTES CONDUZIDOS

Foram realizados mais de 90 testes manuais e automatizados, meticulosamente projetados para descobrir vulnerabilidades que pudessem comprometer os pilares de Confidencialidade, Integridade e Disponibilidade dos sistemas da Docspider. Esses testes variaram desde avaliações de segurança de rede até simulações de ataque sofisticadas, visando uma cobertura abrangente de todas as potenciais brechas de segurança.

Entre alguns dos testes realizados, podemos destacar:

1. Cross-Site Request Forgery (CSRF) Test
2. DOM-based Cross-site Scripting (XSS) Test
3. Insecure File Upload Test
4. Clickjacking Test
5. Stored XSS Test
6. File Inclusion (LFI/RFI) Test
7. SQL Injection Pentest
8. Pentest XXE (External Entity Attack) Test
9. XML Injection Test
10. Code Injection Test
11. Reflected XSS Test
12. NoSQL Injection Test
13. LDAP Injection Test
14. Template Injection Test
15. Insecure Deserialization

16. Code Execution via File Upload Test
17. Host Header Injection Verification
18. Server-side Request Forgery (SSRF)
19. Brute-force Authentication Login
20. Remote Code Execution (RCE) vulnerabilities

Esses procedimentos foram essenciais para entender e mitigar os riscos enfrentados pelos sistemas da Docspider, garantindo uma segurança cibernética de alto nível.

QUALIFICAÇÕES TÉCNICAS DA GUARDSI

A Guardsi é uma cybertech com uma sólida reputação, construída sobre a excelência técnica e o compromisso com a ética e a transparência. Ao longo de nossa trajetória, temos orgulho de ter atendido diversas empresas líderes em seus setores, fornecendo serviços de pentest e segurança da informação altamente eficazes e contribuindo para a proteção de seus ativos críticos e a preservação de sua reputação. Por conta dessa grande confiança depositada na Guardsi, frequentemente somos acionados pelas maiores instituições financeiras do país para realização de testes de intrusão em seus sistemas e outros serviços relativos à segurança da informação. A Guardsi se orgulha de ter participado de projetos de impacto nacional, como as aplicações do Auxilio Brasil, Caixa TEM, FGTS e a implementação segura do PIX no Brasil, sistema de transação monetária tido hoje como referência mundial.

Todos os testes são conduzidos por profissionais altamente qualificados, experientes e detentores de diversas certificações amplamente reconhecidas, entre elas a Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH) e Solyd Certified Pentester (SYCP).

Além de possuírem as principais certificações práticas de ethical hacking e pentest do mundo, nossos profissionais acumulam anos na experiência prática na área, como nosso CEO, Guilherme Junqueira, que possui mais de 20 anos de experiência com hacking e segurança da informação. Alguns dos nossos pentesters já reportaram falhas para empresas globais em programas de Bug Bounty, alguns deles já tendo registrado seu nome no hall da fama de segurança dessas empresas, como, por exemplo, o Sócio e Supervisor da Equipe de Pentesters da Guardsi, Luiz Paulo Viana, que contribui ativamente reportando falhas de segurança para instituições mundialmente reconhecidas, como o Departamento de Defesa dos Estados Unidos, Ford, AT&T, Tik Tok e muitas outras. Todo esse histórico pode ser conferido em seu perfil da Hacker One, empresa globalmente reconhecida que

gerencia os maiores programas de “recompensas por vulnerabilidade encontradas” do mundo.

REFERÊNCIA EDUCACIONAL

Além de realizar serviços de pentest e consultoria em segurança da informação para empresas de diversos setores e tamanhos, a Guardsi contribui ativamente com a elevação do padrão de profissionalismo e conscientização de riscos do setor de segurança da informação, contando com seu braço educacional, a Solyd Offensive Security, para o cumprimento dessa importante missão.

A Solyd é a maior escola de treinamentos e certificações em segurança ofensiva da América Latina, contando com mais de 200 mil alunos. Trata-se, portanto, da vertente educacional da Guardsi que fornece para a Docspider treinamentos especializados para a construção e aprimoramento de um time de Red Team interno, bem como treinamentos de conscientização de riscos

cibernéticos para que os demais colaboradores saibam identificar e evitar diversos tipos de ataques, como os de engenharia social.

METODOLOGIAS UTILIZADAS

Na condução dos pentests, a Guardsi adota metodologias rigorosas e amplamente aceitas, consolidando sua abordagem por meio de diretrizes estabelecidas por organizações internacionalmente renomadas na área de segurança da informação. Destacam-se, entre essas entidades e suas metodologias, a Open Web Application Security Project (OWASP), a MITRE Corporation e a Penetration Testing Execution Standard (PTES). Estas organizações são reconhecidas globalmente por sua expertise e liderança na formulação de padrões e melhores práticas para avaliações de segurança.

Ao integrar essas metodologias, garantimos que nossos pentests não apenas atendam, mas superem as expectativas em termos de eficácia e profundidade. A combinação da expertise dessas organizações líderes com a experiência de nossa equipe capacitada resulta em avaliações de segurança de alta qualidade, proporcionando uma visão precisa e abrangente do estado atual da resistência contra ameaças cibernéticas.

METODOLOGIAS PRÓPRIAS

Além de implementar em seu método de trabalho diversas metodologias internacionalmente respeitadas, a Guardsi incorpora sua própria metodologia, desenvolvida e aprimorada ao longo dos anos de experiência em testes de intrusão. Essa metodologia exclusiva complementa e enriquece a análise de vulnerabilidades, garantindo uma abordagem completa e personalizada para atender às necessidades específicas de cada situação. Ao utilizar uma combinação cuidadosamente selecionada de metodologias, a Guardsi assegura uma avaliação minuciosa e confiável da segurança dos sistemas, fornecendo informações valiosas para a tomada de decisões e aprimoramento contínuo da segurança.

LEI GERAL DE PROTEÇÃO DE DADOS

Como consequência das boas práticas de segurança da informação adotadas, a Docspider está em consonância com as exigências legais descritas no Art. 6º, incisos VII e VIII e no Art. 46º da Lei Geral de Proteção de Dados (13.709/2018). A LGPD é uma legislação de importância inquestionável no panorama atual da segurança da informação, visando garantir a integridade e confidencialidade dos dados pessoais, bem como estabelecer princípios sólidos para o seu tratamento responsável.

AVISO LEGAL

É crucial entender que um pentest é uma representação instantânea do cenário de segurança avaliado no momento da avaliação. As descobertas e recomendações feitas nos relatórios são baseadas exclusivamente nas informações coletadas durante o período de avaliação. Elas não levam em consideração quaisquer alterações, atualizações ou modificações que possam ter sido feitas fora deste período específico.

A natureza dinâmica da segurança cibernética significa que as ameaças estão constantemente evoluindo e se adaptando. Portanto, a imagem capturada durante um único teste de penetração pode rapidamente se tornar desatualizada. Isso destaca a importância de uma abordagem proativa e adaptativa à segurança cibernética.

A realização regular de testes de penetração é uma medida prudente e necessária para manter a resiliência do ambiente de segurança de uma organização. Esses testes permitem que uma organização identifique proativamente vulnerabilidades e lacunas em suas defesas e tome medidas para corrigi-las antes que sejam exploradas por atores mal-intencionados.

Por fim, é importante notar que, embora os testes de penetração sejam uma ferramenta valiosa na estratégia de segurança cibernética de uma organização, eles são apenas uma parte de uma abordagem de segurança eficaz. Uma postura de segurança robusta também envolve uma combinação de controles preventivos,

detectivos e corretivos, bem como uma cultura de segurança forte que promova a conscientização e as melhores práticas entre todos os membros da organização.

REPRESENTANTE TÉCNICO

Ao assinar este documento, o representante técnico da Guardsi atesta a execução dos testes de intrusão e demais serviços que estão sendo prestados para a Docspider. Este documento é considerado válido e eficaz a partir da data de assinatura pelo representante técnico, até a data final de duração do contrato de prestação de serviços vigente.

gov.br
Documento assinado digitalmente
LUIZ PAULO VIANA DE SOUZA DORES
Data: 10/04/2025 15:39:31-0300
Verifique em https://validar.iti.gov.br

_____

Luiz Paulo Viana de Souza Dores

GUARDSI CERTIFIED

guardsi