



TRIBUNAL DE JUSTIÇA MILITAR DE SP
Rua Doutor Vila Nova, 285 - Bairro Vila Buarque - CEP 01222-020 - São Paulo - SP - www.tjmisp.jus.br

ATESTADO DE CAPACIDADE TÉCNICA

São Paulo, 15 de maio de 2024.

PROCESSO SEI Nº 22.1.000002518-7

O TRIBUNAL DE JUSTIÇA MILITAR DO ESTADO DE SÃO PAULO, inscrito no CNPJ sob o nº 60.265.576/0001-02, com sede na Rua Doutor Vila Nova, nº 285, Vila Buarque - São Paulo/SP - CEP: 01222-020, neste ato representado por seu funcionário Emerson Ribeiro Araujo, matrícula nº 61.111-1, Coordenador de Gestão Administrativa deste Egrégio (emerson.araujo@tjmisp.jus.br - (11) 3150-5386), atesta para os devidos fins que a empresa BESAFE BRASIL CONSULTORIA EM TI E GESTAO DE RISCOS, inscrita no CNPJ sob nº 22.414.960/0001-30, com sede na Rua Canadá, 1900 - Bacacheri - Curitiba/PR, executou o objeto constante no Processo SEI supracitado, conforme abaixo relacionado:

1) Contrato TJMSP nº 378/2023
2) Objeto: - Prestação de serviços de PENTEST, modalidade Black Box, Planejamento, Descoberta, Exploração e Apresentação de resultados com relatórios (técnico e executivo) e reteste no parque tecnológico desse Tribunal, em conformidade com o EDITAL DE PREGÃO ELETRÔNICO TJMSP Nº 003/2023, e seus anexos.
3) Especificações técnicas - Detalhamento do escopo - DESCOBERTA Coleta passiva, caracterizada pela obtenção de informações utilizando se, no mínimo, as seguintes técnicas/serviços/ferramentas, quando aplicáveis: Whois e nslookup (consultas DNS); Sites de busca; Listas de discussão; Blogs de colaboradores; Dumpster diving ou trashing; Informações livres; Packet sniffing “passive eavesdropping”; Captura de banner. Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas, quando aplicáveis: Port scanning (Mapeamento de rede); Varredura de vulnerabilidade, que deverá verificar/identificar no mínimo: Hosts ativos na rede; Portas e serviços em execução; Serviços ativos e vulneráveis nos hosts; Fingerprinting de Sistemas operacionais dos hosts; Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas; Configurações feitas nos hosts, sem observância de boas práticas em segurança computacional; Identificação de rotas e estimativa de impacto, caso estas sejam modificadas ou reconfiguradas; Identificação de vetores de ataque e cenários para exploração; Vulnerabilidades Detectadas (CVE), classificadas com Alto, Médio ou Baixo Risco. Informações a serem aplicadas na fase de ataques; Em relação a serviços e aplicações web: Uso indevido de sistema de arquivos e arquivos temporários; Evasão de informação por configurações padrão de tratamento de erros; Tratamento indevido de entrada; Problemas relacionados à má configuração dos serviços; e

Gerenciamento inseguro de sessões web.

- **EXPLORAÇÃO**

Violações do protocolo HTTP;
SQL Injection;
LDAP Injection;
Cookie Tampering;
Cross-Site Scripting (XSS);
Directory Transversal;
Buffer Overflow;
OS Command Execution;
Command Injection;
Remote Code Inclusion;
Server Side Includes (SSI) Injection;
File disclosure;
Information Leak;
Ataques contra protocolo TCP:
Sequestro de conexões;
Prognóstico de número de sequência do protocolo TCP;
Source routing.
Ataques em nível da aplicação:
Buffer Overflow; e
Problemas com o SNMP.

4) Vigência contratual

- 03/04/2023 a 02/04/2024

5) Valor do contrato

- R\$ 84.000,00 (oitenta e quatro mil reais).

Outrossim, atesta que os referidos serviços foram recebidos e tomados satisfatoriamente e que todas as cláusulas contratuais foram respeitadas e cumpridas, não havendo, até a presente data, nada que desabone a referida empresa.



Documento assinado eletronicamente por **Emerson Ribeiro Araújo, Coordenador**, em 16/05/2024, às 11:57, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.tjmsp.jus.br/sei/verifica.php> informando o código verificador **0485967** e o código CRC **4AD91E3B**.