

ATESTADO DE CAPACIDADE TÉCNICA

A Senff, inscrita no CNPJ nº 20.150.970/0001-80, com sede Av. Sen. Souza Naves, 1240 - Cristo Rei, Curitiba - PR, ATESTA, para os devidos fins, que a empresa **BESAFEBRASIL CONSULTORIA EM TI E GESTÃO DE RISCOS EIRELI**, inscrita no CNPJ/MF sob o nº 22.414.960/0001-30, sediada na Rua Canadá, 1900, Bacacheri em Curitiba-PR, CEP 82510-290, que nas datas de 04/01/2023 a 17/03/2023, executou a prestação de serviços de PENTEST modalidade Black Box no parque tecnológico, em conformidade ao planejamento abaixo:

- **Análise versão e exploit dos serviços**
 - Enumeração de Usuários;
 - Acesso não autorizado;
 - Escalação de Privilégios;
 - Análise de Protocolos não Criptografados;
 - Análise de Acesso a Dados e Informações Externas;
- **Análise/exploração de vulnerabilidades nas aplicações publicadas**
 - Análise de Acesso;
 - Acesso a Dados não Autorizados;
 - Tratamento de Dados (GET, POST, UPLOAD, DELETE, PUTE);
 - Tratamento de Sessão/Cookies/Tokens;
 - Análise do Código Fronte Front-End;
 - Análise de Configuração Default, Tecnologias obsoletas, ou Utilização de Tecnologias com vulnerabilidades conhecidas;
 - Análise do tratamento e comunicação com o Banco de Dados;
- **Ganho de Informações**
 - Modo Passivo (**Não existe interação direta com o alvo**)

Coleta de informações DNS (dnsenum)

- Coleta de bloco de IPs alocados/utilizado
- Coleta de informações públicas
- Coleta de tecnologias utilizadas
- Modo Ativo - FingerPrint e FootPrint (**Existe interação direta com o alvo**)
 - Coleta de hosts ativos
 - Coleta de Domínios
 - Coleta de Subdomínios
 - URL Fuzzing
 - PortScan

- Enumeração de Sistema Operacional
- Enumeração de Serviços
- Enumeração de ativos de segurança (Firewall/IPS/IDS/WAF)
- **Análise e Planejamento (Não existe interação direta com o alvo)**
 - Configuração de ferramenta(s) automatizada(s) a serem utilizadas
 - MindMap (Correlação de dados adquiridos na fase anterior)
- **Identificação das Vulnerabilidades (Interação direta com o alvo em toda a fase)**
 - Execução da(s) ferramenta(s) automatizadas
 - Teste manual em todas as informações coletadas
 - Ataques a sistemas WEB
 - Owasp Top 10 Web Application 2013 e 2017
 - Análise de Acesso
 - Acesso a Dados não Autorizados;
 - Tratamento de Dados (GET, POST, UPLOAD, DELETE, PUT);
 - Tratamento de Sessão/Cookies/Tokens;
 - Análise do Código Fonte Front-End;
 - Análise de Configuração Default, Tecnologias obsoletas, ou Utilização de Tecnologias com vulnerabilidades conhecidas;
 - Análise do tratamento e comunicação com o Banco de Dados;
 - XSS/CSRF
 - Ataques a serviços públicos
 - HTTP/HTTPS
 - SMTP/POP/IMAP
 - FTP/FTPS
 - DNS
 - MySql/Postgres/Oracle (Banco de dados público)
 - Qualquer outro serviço que se encontre público
 - Análise de Configuração Default, Tecnologias obsoletas, ou Utilização de Tecnologias com vulnerabilidades conhecidas;
 - Ataques a protocolos legados
 - PHP/Ajax/Html/WordPress
 - FTP/Apache/Nginx/IIS
 - Qualquer outro protocolo que se encontre público

- Análise de Configuração Default, Tecnologias obsoletas, ou Utilização de Tecnologias com vulnerabilidades conhecidas;
- **Exploração (Interação direta com o alvo)**
 - Validação dos acessos não autorizados visando identificar seu risco e impacto
 - Validação do impacto que o acesso não autoriza permite em relação aos dados e informações
 - Quebra de Senhas off-line; (Quando existe banco de senhas capturadas)
 - Acesso não autorizado;
 - Escalação de Privilégios;
- **Análise de risco e sugestão de remediação (Não existe interação direta com o alvo)**
 - Levantamento da criticidade vs probabilidade de ocorrência de uma vulnerabilidade
- **Relatórios (Não existe interação direta com o alvo)**
 - Criação do relatório técnico final
 - Criação do relatório executivo final
 - Criação das apresentações
 - Apresentação para o corpo técnico

ATESTA ainda que os serviços foram prestados de acordo com os parâmetros técnicos de qualidade exigidos e nos prazos pactuados e não existem em seus registros fatos que desabonem sua conduta quanto às obrigações assumidas.

Alexsandro Lima – A.lima@senff.com.br

Aldrin Palma - Aldrin.palma@senff.com.br

Atenciosamente,

Banco Senff

CNPJ: 20.150.970/0001-80

NOME: Alexsandro Lima - 

CARGO: Diretor

Banco Senff

CNPJ: 20.150.970/0001-80

NOME: Aldrin Palma - 

CARGO: Coordenador de Segurança da Informação.