RELATÓRIO DE PENTESTING
CONTATO SEGURO

SUMÁRIO EXECUTIVO

- Este documento apresenta os resultados dos testes de segurança realizados no sistema hospedados nas URLs htttps://portal.tst.contatoseguro.io e https://tst.contatoseguro.io Todos os resultados são referentes ao teste na versão auditada no dia 17/10/2022 e foram gerados através de testes de *pentest* executados através da metodologia da Zero-Defect.

ESCOPO DO PROJETO

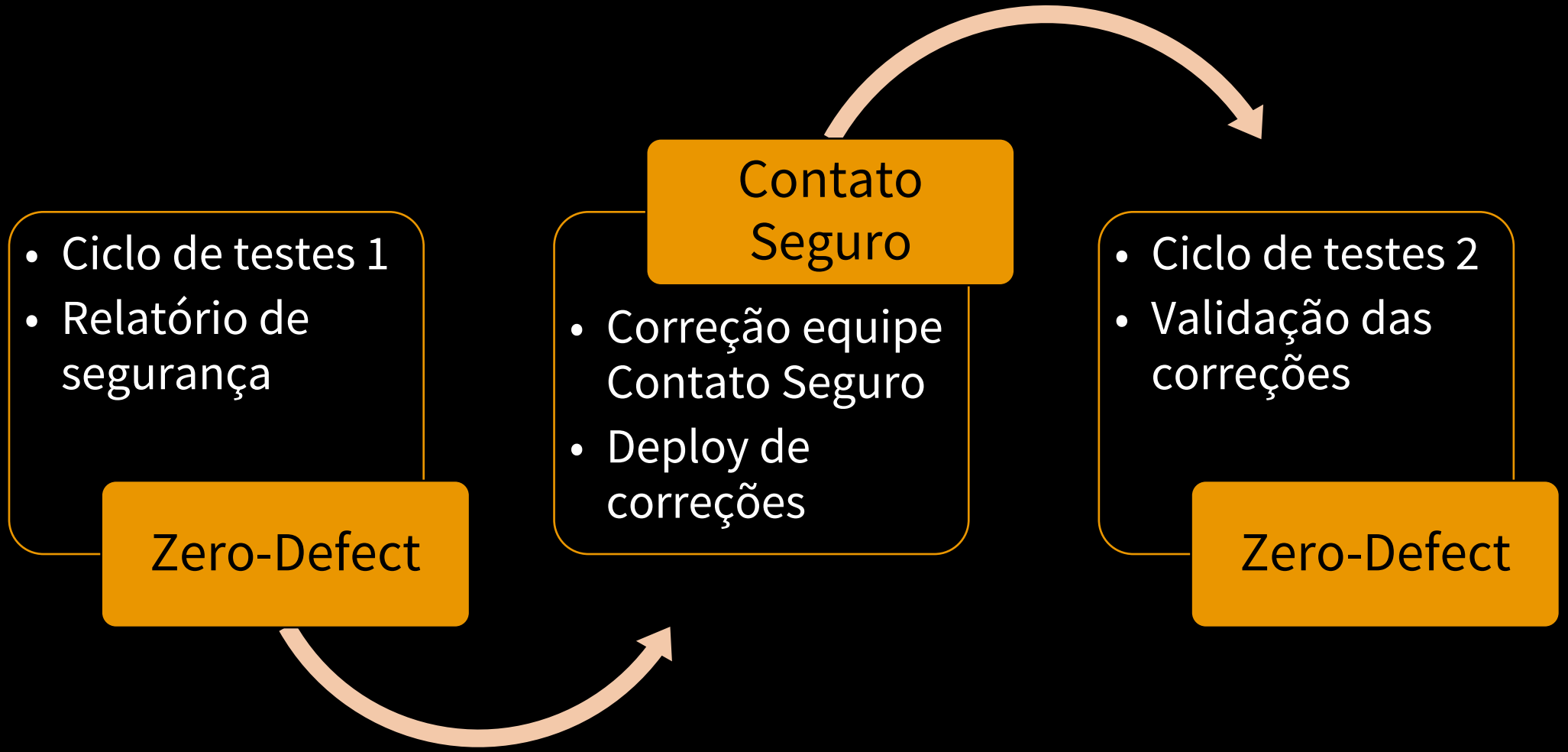
ANÁLISE SEGURANÇA EXTERNA

ANÁLISE DE SEGURANÇA INTERNA

ANÁLISE DE INFRAESTRUTURA

RELATÓRIOS

ESCOPO DO PROJETO



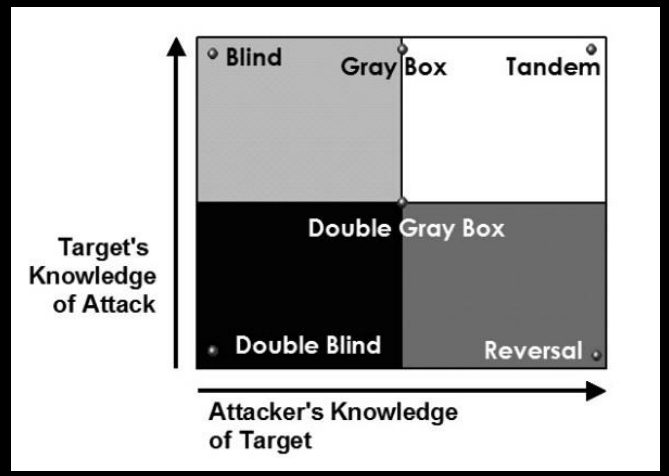
PERSONAS DOS VETORES DE ATAQUE

Usuário **externo** ao ecossistema Contato Seguro. Não gosta da empresa, acredita que pode sabotar os sistemas externos da empresa. É detrator da marca. Pode ser concorrente e gostaria de provar que sistema não é seguro. Busca escândalo e vazar informações

Usuário que foi denunciado no site da contato seguro e quer saber informações de quem fez a denúncia. Se puder, ele irá alterar os dados para se manter incógnito. Não busca se expor e tentará esconder os seus rastros.

Usuário pertencente ao ecossistema Contato Seguro (Auditor de ética ou membro da empresa). Entende que pode tirar vantagem da sua posição junto a empresa e acessar dados de outras pessoas. Não busca destruir o sistema, mas se aproveitar dele sem ser notado. Busca vantagem financeira através de ameaças e chantagem. Se puder encobrir seus rastros irá fazer de forma pensada.

METODOLOGIAS UTILIZADAS



Usuário Externo: Double Blind

Usuário Interno: Reverso

Double Blind: A empresa não está ciente dos tipos de ataque que irá sofrer e o vetor de ataque não conhece a estrutura da empresa. Ambos os atores não sabem o que pode acontecer durante o ataque.
Reversal: O vetor de ataque tem conhecimento e acesso ao sistema, mas a empresa não sabe quais técnicas serão utilizadas para poder mitigar o ataque.

ZERO DEFECT

METODOLOGIAS UTILIZADAS

OWASP

- Web Crawling Analysis
- Port Scanning e Banner Grabbing
- GHDB Check (Google Hacking Database Check)
- Light Web code scan (Input fields)
- RFC Compliance CHECK.
- Buffer Overflow
- Brute force attacking
- Fuzzer de Parâmetros
- Medium Code Scan (XSS simple/SQL Injection simple)
- Heavy Code scan (Variables check, reverse injection)
- Blind SQL Injection
- Time SQL Injection
- Transversal attack
- Service exploit
- WebServer Global variable checks
- XSS (Cross-site Scripting)
- CSRF (Cross-site request forgery)
- XST (Cross Site Trace)
- DoS.(Deny of Service com uma máquina)
- Sniffing

METODOLOGIAS UTILIZADAS

Etapa 1 – ATAQUE PERSONA EXTERNA

- Ataque de *brute force* na área de login;
- Ataque de *brute force* na área de recuperação de senha;
- Ataque de *buffer overflow* em serviços de autenticação;
- Validação de possíveis fraquezas criptográficas dos protocolos de sistema;

Etapa 2 – ATAQUE PERSONA INTERNA

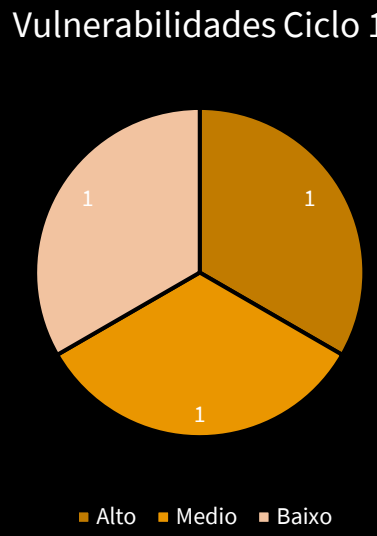
- Tentativa de escalada de privilégio utilizando-se de credenciais válidas de sistema;
- Ataques de XSS
- Ataques de SQL-Injection
- Ataques de buffer-overflow
- Criação de pacotes de dados maliciosos para comprometer o sistema (Remote File Inclusion, Local File inclusion);
- Manipulação de parâmetros de URLs

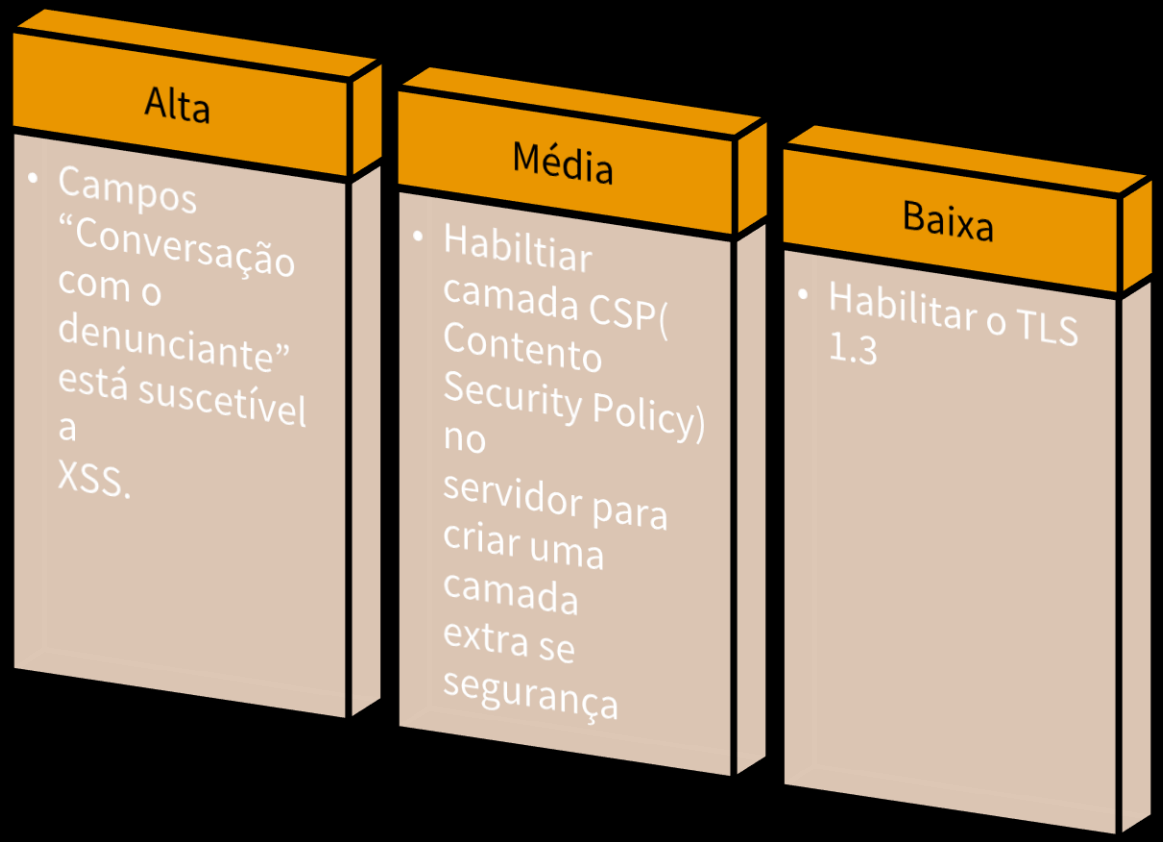
Etapa 3 – ANÁLISE INFRAESTRUTURA

- Validação de WAF
- Validação de atualização de serviços web
- Validação de certificados digitais
- Validação de políticas de Firewall
- Validação de criptografia de sistema
- Validação de proteção de ataques a negação de serviço por pacotes maliciosos

Relatório de segurança

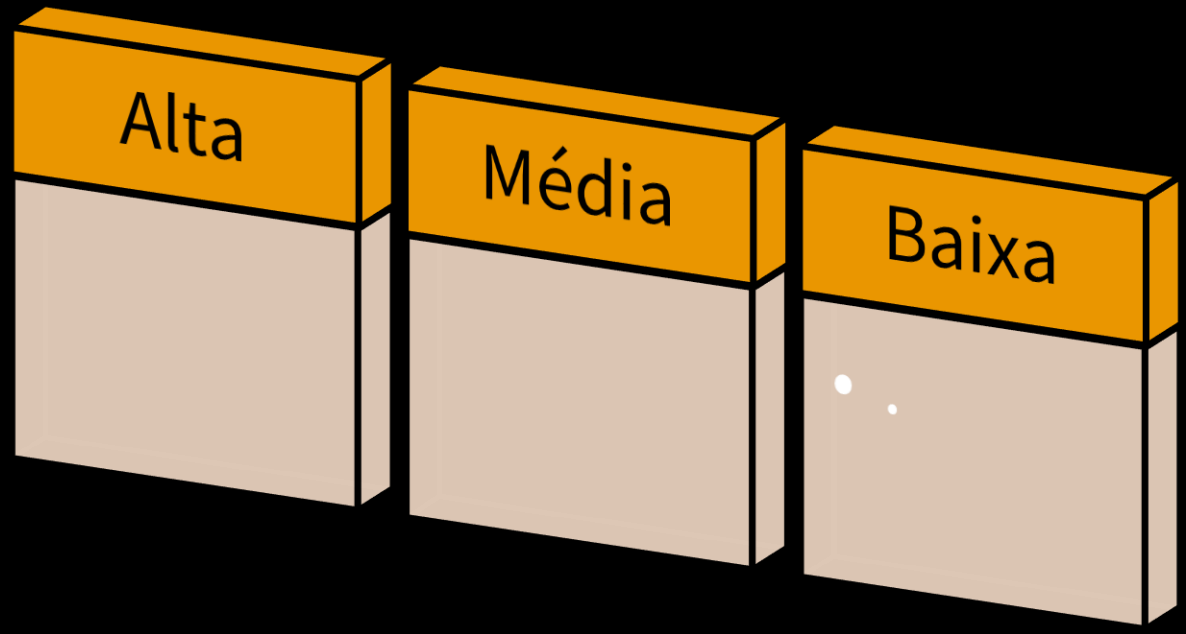
RELATÓRIO CICLO 1





RELATÓRIO CICLO 2

Sem vulnerabilidades



CONCLUSÃO

- Durante o primeiro ciclo de testes verificou-se diversas vulnerabilidades que poderiam afetar a segurança como um todo do sistema Contato Seguro. A presença de XSS encontrada através da persona de ataque vinda de um usuário interno ao sistema foi encontrada através da nossa metodologia e mitigada para a execução do segundo ciclo. As outras vulnerabilidades foram sanadas pela equipe da Contato Seguro para os retestes. Dessa forma, a Zero-Defect considera que a segurança do sistemas contatoseguro e portal para a versão testada no dia 17/10/2022 está aceitável. Recomendamos sempre que os testes de invasão sejam realizados de forma periódica a medida que novos códigos sejam implementados dentro da solução do cliente. Sistemas de informação necessitam serem atualizados periodicamente de forma a garantir uma qualidade aceitável dos seus níveis de serviço e segurança.