Vulnerability Disclosure Program

Tabela de conteúdo:

Introdução

Levamos a Segurança da Informação muito a sério, e por isso estamos comprometidos em aderir às melhores práticas do mercado e regularmente nos submeter a auditorias internas e externas para garantir nossa capacidade de segurança dos dados da empresa. Reconhecemos o impacto positivo que a pesquisa de segurança responsável pode ter em nossos serviços e o papel importante que a comunidade de segurança brasileira desempenha nisso.

Se apesar dos nossos esforços você acredita ter encontrado uma falha em nossos ativos (aplicação, sistema ou APIs), forneça com clareza e detalhes a vulnerabilidade, incluindo as informações necessárias para reproduzir, validar a vulnerabilidade com uma POC (Proof of Concept), ou qualquer outra informação que julga necessária para acessar a falha reportada. Será um prazer trabalhar com você para resolver o problema imediatamente.

Política de divulgação

- Informe-nos o mais breve possível após a descoberta de um possível problema de segurança, e faremos todos os esforços para resolvê-lo rapidamente.
- Forneça um tempo razoável para resolver o problema antes de qualquer divulgação ao público ou a terceiros.
- Faça um esforço de boa fé para evitar violações da privacidade, destruição de dados e interrupção ou degradação do nosso serviço. Interaja apenas com contas que você possui ou com permissão explícita do titular da conta.

Respaldo legal

Quaisquer atividades conduzidas de maneira consistente com esta política serão consideradas conduta autorizada e não iniciaremos uma ação legal contra você. Se uma ação legal for iniciada por terceiros contra você em relação às atividades conduzidas sob esta política, tomaremos medidas para tornar claro que suas ações foram conduzidas em conformidade com esta política. Obrigado por ajudar a manter nossa empresa, aplicações e nossos usuários em segurança!

Escopo

Delimitação de domínios, subdomínios, aplicativos e outros:

1. app.vlow.com.br
2. www.vixting.com.br

Exclusões

Ao procurar por vulnerabilidades, gostaríamos de pedir que você se abstenha da seguinte lista abaixo pois elas não serão consideradas elegíveis em nosso programa:

- Clickjacking em páginas sem informações sensíveis;
- Self-XSS;
- Enumeração de nome de usuário/e-mail por meio da página de login ou através de mensagens de erro na página de "Esqueceu a senha";
- CSRF não autenticado /logout/login;
- CSRF em ações não críticas;
- Falta de cabeçalhos HTTP relacionados à segurança que não levam diretamente a uma vulnerabilidade;
- Vulnerabilidades do lado do cliente baseadas em Flash, como Flash XSS;
- Redirecionamento aberto do Flash ou Injeção de conteúdo do Flash;
- Vulnerabilidades identificadas anteriormente;
- Ataques que exigem acesso físico ou MITM (Man in the middle);
- Bibliotecas com versões vulneráveis conhecidas sem uma PoC funcionando (ex. jQuery Libraries);
- CSV injection attack sem demonstrar uma PoC;

- Melhores práticas de configurações em SSL/TLS;
- Ataques de brute-force em formulários de autenticação;
- Páginas de erros de stack trace (401/403/500) sem uma comprovação de vulnerabilidade;
- Método HTTP OPTIONS habilitado;
- Qualquer atividade que possa levar à interrupção do nosso serviço (ex. DoS);
- Contect spoofing e text injection sem mostrar um vetor de ataque ou sem poder alterar o HTML/CSS;
- Aplicativos, scripts e integrações não oficiais de terceiros;
- Engenharia social (incluindo phishing) na nossa equipe ou terceiros;
- Registros SPF (Sender Policy Framework) inválidos ou ausentes (SPF/DMARC/DKIM incompleto ou ausente);
- Quaisquer tentativas físicas contra nossas propriedades ou data centers;
- Informações de divulgação insensíveis, (ex. versão do software);
- Disclosure de informações com baixo risco;
- Cross-site scripting em navegadores obsoletos;
- Relatórios de scanners automatizados de vulnerabilidades que não são validados (ou seja, falsos positivos);
- Contect spoofing e text injection sem mostrar um vetor de ataque ou sem poder alterar o HTML/CSS;
- Problemas de captura de banner (como encontrar informações como o nome do servidor da web etc.);
- Complexidade da senha;
- Não possui confirmação de e-mail;
- Spamming;
- Negação de serviço;
- Tabnabbing.
- Falta de rate limiting.
- Falta de flags no cookies (ex. HttpOnly, SameSite, Secure).
- Falta de security headers (ex. CSP / HSTS / X-Frame-Options / X-Content-Type-Options).
- Uso de ferramentas automatizadas que podem gerar tráfego significativo e possivelmente prejudicar o funcionamento de nossa aplicação.
- Subresource Integrity (SRI) não implementada.
- Cabeçalho HSTS ausente.
- Bugs divulgados publicamente em software de internet no prazo de 7 dias após sua divulgação.

Observações finais

O report só é determinado como concluído após a correção da vulnerabilidade, solicitamos que o autor do report busque reproduzir a falha após a correção para validar, o mesmo será notificado sobre isso quando necessário.

PEDIMOS AOS PESQUISADORES EXPLICITAMENTE QUE EVITEM:

- Modificação de quaisquer dados;
- Violação de privacidade de dados;
- Vazamento de dados coletados e afins;
- Armazenar qualquer tipo de dados de clientes e afins;
- Divulgar publicamente uma vulnerabilidade sem termos chance prévia de correção em um período de tempo razoável.
- Roubo de identidade ou qualquer outro ataque de engenharia social (ex: phishing, vishing) aos nossos funcionários, comerciantes, parceiros e clientes;
- Qualquer coisa que possa degradar e impossibilitar nossos serviços (por exemplo, ataques de negação de serviço);
- Spamming;
- Ataques de segurança física (ex: em prédios administrativos, lojas, cargas e etc.);

Não entre em contato com funcionários da Vixting através de redes sociais (como LinkedIn) e e-mails pessoais sobre questões relacionadas ao programa de recompensas por bugs, sempre use o e-mail security@vixting.com.br pois desta forma conseguimos seguir o processo aqui definido e assim garantir o melhor resultado possível.