HEITORGOUVEA.ME

Pesquisador Independente de Segurança

Relatório de Segurança de Aplicações

06/06/2023 - Versão 1.1
Tipo: relatório executivo

Preparado para: Kaique Bonato
Preparado por: Heitor Gouvêa

COMUNICADO DE CONFIDENCIALIDADE

Para a publicação de forma aberta desse documento, alguns cuidados foram tomados como por exemplo a omissão de detalhes de vulnerabilidades e entre outras informações, logo, apenas o conteúdo desse documento em si é de visibilidade pública não refletindo o conteúdo completo de toda a análise envolvida. Embora tenham sido tomadas precauções na preparação deste documento, o editor e o(s) autor(es) não assumem nenhuma responsabilidade por erros, omissões ou danos resultantes do uso das informações aqui contidas.

ISENÇÃO DE RESPONSABILIDADE

Observe que esta avaliação pode não revelar todas as vulnerabilidades presentes nos sistemas dentro do escopo do trabalho. Como um exercício de melhor esforço e com limite de tempo, ele não garante que não haja outros problemas de segurança no aplicativo. Quaisquer alterações feitas no ambiente durante ou após o período de teste podem afetar os resultados da avaliação.

TABELA DE CONTEÚDOS

COMUNICADO DE CONFIDENCIALIDADE	2
ISENÇÃO DE RESPONSABILIDADE	2
CONTROLE DO DOCUMENTO	4
CARTA DE APRESENTAÇÃO DOS AUDITORES	5
OBJETIVO	6
CONTEXTO	6
SUMÁRIO EXECUTIVO	7
ESCOPO	8
METODOLOGIA DE TESTES	9
DEFINIÇÃO DE CLASSIFICAÇÕES	11
VULNERABILIDADES ENCONTRADAS	12
TRABALHOS FUTUROS	13
CONCLUSÃO	14

CONTROLE DO DOCUMENTO

Informações sobre a versão

Versão	Data	Descrição
0.9	03/06/2023	Rascunho para análise de qualidade.
1.0	05/06/2023	Relatório inicial.
1.1	06/06/2023	Ajustes após revisão da contratante.

Distribuição do documento

Nome	Cargo	Organização	Contato
Kaique Bonato	Diretor	Vantico	kaique@vantico.com.br
Heitor Gouvêa	Pesquisador de Segurança	heitorgouvea.me	hi@heitorgouvea.me

CARTA DE APRESENTAÇÃO DOS AUDITORES

Heitor Gouvêa - Pesquisador Independente em Segurança da Informação

Como pesquisador independente, sem vínculo com empresas ou investidores, é neutro na avaliação de fabricantes de produtos de segurança e sem interesses comerciais, para garantir que as auditorias tenham foco na qualidade e entreguem resultados que superem as expectativas; Com formação em Engenharia de Software e 7 anos de experiência na indústria de segurança ofensiva o foco da pesquisa de Gouvêa é a descoberta de vulnerabilidades em aplicações/serviços e desenvolvimento de exploits - já tendo reportado vulnerabilidades para empresas incríveis como Activision, Nubank (e outras fintechs brasileiras), Adobe, Oracle e outras empresas não tão famosas, mas tão incríveis quanto.

OBJETIVO

O objetivo deste trabalho foi realizar um teste de intrusão e identificar a existência de vulnerabilidades exploráveis no ambiente. Para isso foi utilizado técnicas automatizadas e manuais direcionadas para partes específicas das tecnologias/serviços mapeados para validar a existência de vulnerabilidades.

CONTEXTO

A Vantico é uma empresa no ramo de Segurança da Informação, mais especificamente a mesma possuí um produto SaaS definido como plataforma de *Pentest as a Service*; Executando testes de segurança sob demanda, tal plataforma é responsável por gerir os relatórios completos, permitindo visualização em atualizações em tempo real. Sendo uma prestadora de serviço no ramo de Segurança da Informação, a mesma é extremamente interessada em avaliar a sua maturidade no seguinte aspecto e em casa de identificação de algum risco, realizar a correção para assim proteger as informações de seus clientes.

SUMÁRIO EXECUTIVO

Depois de realizada uma avaliação de segurança do aplicativo do cliente, onde o teste de invasão simulou uma tentativa de ataque de um agente de ameaça externo tentando obter acesso aos sistemas: o objetivo dessa avaliação era descobrir e identificar vulnerabilidades na infraestrutura e nos aplicativos, então sugerir métodos para remediar as vulnerabilidades. Identificamos um total de 9 vulnerabilidades no escopo do trabalho, discriminadas por gravidade na tabela abaixo.

CRÍTICO	ALTO	MÉDIO	BAIXO	INFORMATIVO
1	2	2	4	0

As vulnerabilidades de maior gravidade dão aos potenciais invasores a oportunidade de comprometer os dados dos clientes, acessando seus projetos e consequentemente as informações sigilosas contidas em cada um deles. Para garantir a confidencialidade, integridade e disponibilidade dos dados, as correções de segurança foram implementadas ainda durante a execução dos testes posteriores.

Observe que esta avaliação pode não divulgar todas as vulnerabilidades presentes nos sistemas dentro do escopo. Quaisquer alterações feitas no ambiente durante o período de teste podem afetar os resultados da avaliação.

ESCOPO

Todos os testes foram baseados no escopo definido nas comunicações escritas oficiais. O período de testes disponibilizado foi com início em *20/05/2023* e finalização *30/05/2023*, despendendo um esforço total de **40 horas** fragmentadas durante esse espaço de tempo. Os itens no escopo estão listados abaixo.

Aplicações

URL	Descrição
pentest.vantico.com.br	Ambiente dedicado exclusivamente para os testes, provisionado durante o período descrito e sem dados reais.

Credenciais providenciadas

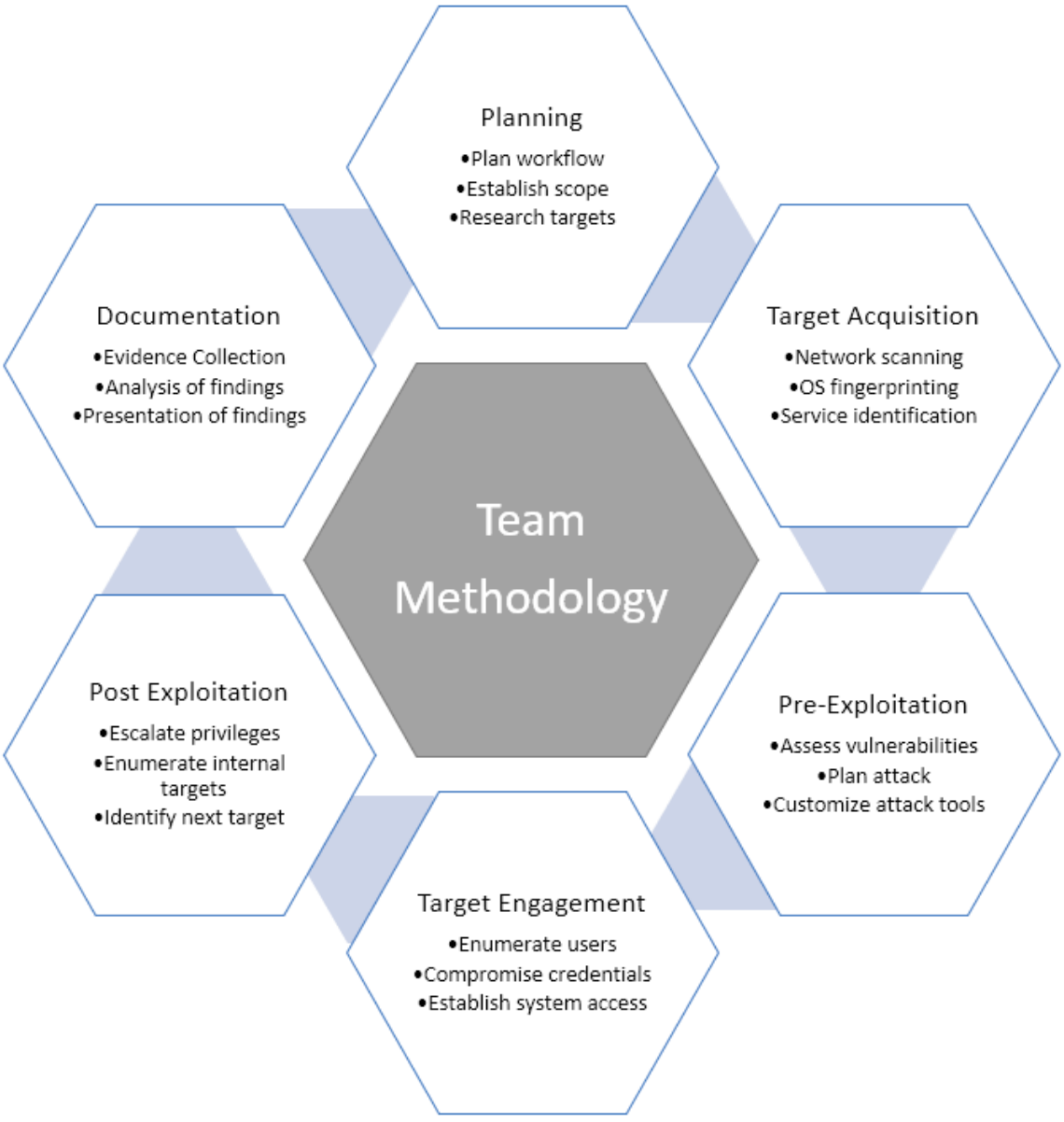
O cliente forneceu as seguintes credenciais e acesso para facilitar a avaliação de segurança listada abaixo.

Perfil	Usuário	Descrição
Pentester	henrique.melo@vantico.com.br	Utilizado para visualizar projetos e realizar a escrita de relatórios de vulnerabilidades.
Desenvolvedor	hromdn2003@vantico.com.br	Perfil responsável pelo entendimento das vulnerabilidades e correção.
Gestor	gestao@vantico.com.br	Capaz de gerir os projetos na plataforma.
Gestor	gestao3@vantico.com.br	Capaz de gerir os projetos na plataforma.

Outro perfil existente é o de “Administrador”, utilizado pela contratante na administração de alguns recursos da plataforma. No entanto, o acesso a esse perfil não foi disponibilizado durante os testes, limitando algumas possibilidades.

METODOLOGIA DE TESTES

Para execução destes trabalhos, adotamos a metodologia própria mesclada com padrões existentes e solidamente reconhecidos, tais como PTES (Penetration Testing Execution Standard) e OWASP Top Ten nas quais foram executados nas seguintes fases:



Coleta de informações: tem como objetivo mapear a superfície de ataque, identificando informações sobre blocos de IP, subdomínios e ambientes digitais de propriedade do cliente em questão.

Varredura: consiste em identificar portas abertas, serviços ativos e possíveis mecanismos de defesa.

Enumeração: permite identificar detalhes sobre os serviços ativos, identificando possíveis versões, fornecedores, usuários e informações que possam ser uteis para o sucesso de um ataque.

Exploração: tem como objetivo explorar as possíveis vulnerabilidades identificadas nos serviços e sistemas identificados nas fases anteriores e obter acesso ao sistema.

Pós exploração: tem como objetivo aprofundar o ataque obtendo mais privilégios e aumentando o nível de acesso, se deslocando para outros sistemas afim de controlar ou extrair dados mais sensíveis.

Documentação: consiste em relatar todos os resultados obtidos nas fases anteriores.

DEFINIÇÃO DE CLASSIFICAÇÕES

Classificações de Risco

Nível	Pontos	Descrição
Crítico	**10**	A vulnerabilidade representa uma ameaça imediata para a organização. A exploração bem-sucedida pode afetar permanentemente a organização. A correção deve ser realizada imediatamente.
Alto	**7-9**	A vulnerabilidade representa uma ameaça urgente para a organização e a correção deve ser priorizada.
Médio	**4-6**	A exploração bem-sucedida é possível e pode resultar em interrupção notável da funcionalidade do negócio. Essa vulnerabilidade deve ser corrigida quando possível.
Baixo	**1-3**	A vulnerabilidade representa uma ameaça insignificante/mínima para a organização. A presença dessa vulnerabilidade deve ser observada e corrigida, se possível.
Informativo	**0**	Essas descobertas não representam uma ameaça clara para a organização, mas podem fazer com que os processos de negócios funcionem de maneira diferente do desejado ou revelar informações confidenciais sobre a empresa.

VULNERABILIDADES ENCONTRADAS

Identificador	Vulnerabilidades	Risco	Status
1	Quebra de controle de acesso	**Crítico**	**Corrigida**
2	Quebra no controle de acesso	**Alto**	**Corrigida**
3	Quebra no controle de acesso	**Alto**	**Corrigida**
4	Logs fracos e insuficientes	**Médio**	**Corrigida**
5	Cross Site Request Forgery	**Médio**	**Corrigida**
6	Erro de lógica	**Baixo**	**Corrigida**
7	Referências de objeto direto inseguras	**Baixo**	**Corrigida**
8	Política de senhas permissível	**Baixo**	**Corrigida**
9	Enumeração de usuários	**Baixo**	**Corrigida**

NOTA: (Classificação por pontuação de risco decrescente);

TRABALHOS FUTUROS

Aconselhamos fortemente que todas as vulnerabilidades sejam corrigidas e que a equipe responsável também faça a busca por variações dessas mesmas vulnerabilidades em outras partes da aplicação para garantir uma maior cobertura dos testes. Durante o período do teste de invasão as mitigações foram aplicadas e a realização de novos testes foram feitos no ambiente controlado descrito no escopo.

Também aconselhamos que em um futuro próximo, seja feito um teste de invasão utilizando uma abordagem white-box para assim garantir maior profundidade e qualidade da análise.

Sugerimos que seja adotada uma estratégia de longo prazo quanto a implementação de um ciclo de desenvolvimento seguro, utilizando ferramentas como SCA, SAST, DAST e outras; pois assim será possível identificar vulnerabilidades em estágios anteriores ao de produção, diminuindo agressivamente as chances de uma vulnerabilidade ser explorada “in-the-wild”.

CONCLUSÃO

Através da identificação das vulnerabilidades de “Quebra de controle de acesso” podemos entender que o objetivo foi atingido em sua máxima, pois foi possível localizar uma vulnerabilidade capaz de comprometer todo o sistema, possibilitando então sua correção para que atacantes não o fizessem.

Também podemos afirmar que os principais riscos e pontos de atenção no escopo estão relacionados ao controle de acesso, onde o mesmo precisa ganhar mais maturidade para evitar vulnerabilidades futuras.

Foi possível notar que a segurança já é uma preocupação da Vantico, isso se dá pela presença de funcionalidades obrigatórias como o Multi Authenticator Factor, utilização de algoritmos de rate limit e geração randômica de identificadores únicos como UUID V4.

Agradecemos fortemente ao cliente por toda parceria e assistência durante os testes, esclarecendo pontuais dúvidas e se colocando à disposição. A proatividade na correção das vulnerabilidades por parte da Vantico também vale receber uma pontuação específica pois a equipe da mesma fez movimentações em tal sentido com muita agilidade.

APÊNDICE A - FERRAMENTAS UTILIZADAS

FERRAMENTA	DESCRIÇÃO
Burp Suite Professional	Usado como apoio para testar aplicativos da web.
Firefox Browser	Navegador moderno adotado.
Nmap	Usado para escanear portas em hosts.

TABELA A.1: *ferramentas escolhidas durante a análise.*