I – Definição da Equipe

Equipe responsável pela Auditoria	
Cargo/Função	*Nome do responsável*
Auditor/Auditora Chefe	Yago de Matos
Equipe técnica	Márcio Luis, João Vitor Leão Marques
Equipe de apoio administrativo	Cristofer Cabral, Gabriel Lincoln

II – Pesquisar uma Ferramenta/Programa utilizado para fazer processos de auditoria

Greenbone OpenVAS	
Tipo (generalista/especialista/utilitário)	Generalista
Desenvolvido/disponibilizado por	Greenbone Networks
Endereço/link para acesso	openvas.org
Tipo de Licença	GPL
Vantagens em utilizá-lo (citar 2):	É possível estender as funcionalidades do OpenVAS através de plugin. Base de dados de vulnerabilidades atualizada frequentemente.
Desvantagens em utilizá-lo (citar 2):	Configurar o OpenVAS corretamente pode ser um processo complexo, podendo gerar resultados imprecisos. Requer bastantes recursos quando usado para varreduras em redes muito grandes.

ZAP (Zed Attack Proxy)	
Tipo (generalista/especialista/utilitário)	Especialista
Desenvolvido/disponibilizado por	ZAP
Endereço/link para acesso	zaproxy.org
Tipo de Licença	Apache 2.0
Vantagens em utilizá-lo (citar 2):	Oferece funcionalidades poderosas de varredura automatizada de segurança. Gera relatórios detalhados de vulnerabilidades encontradas, o que facilita a documentação e a correção dos problemas.
Desvantagens em utilizá-lo (citar 2):	Possui algumas limitações em relação a aplicativos móveis. Dificuldade em lidar com aplicativos web complexos.

LibreOffice (Calc)	
Tipo (generalista/especialista/utilitário)	Utilitário
Desenvolvido/disponibilizado por	The Document Foundation
Endereço/link para acesso	libreoffice.org
Tipo de Licença	Mozilla Public License 2.0 (MPL)
Vantagens em utilizá-lo (citar 2):	Possui SDK que pode integrar com a linguagem de programação Python. Pode ser executado a partir de um pen drive (portabilidade).
Desvantagens em utilizá-lo (citar 2):	Não tem como colaborar online com outras pessoas. Pode não ser compatível com outras ferramentas mais populares.

III – Escolher um Aplicativo ou Site utilitário gratuito (funcionalidades básicas gratuitas), que seja utilizado por várias pessoas, que tenha uma funcionalidade e público alvo definidos.
Aplicativo escolhido: X

O X(Twitter) é uma plataforma de mídia social baseada em mensagens curtas e concisas chamadas de "tweets". Cada tweet tem um limite de caracteres, originalmente 140 caracteres, mas posteriormente aumentado para 280 caracteres. Os usuários podem criar uma conta no X e começar a compartilhar seus pensamentos, informações, links, imagens e vídeos por meio de tweets. Esses tweets são exibidos em ordem cronológica inversa, ou seja, os tweets mais recentes aparecem no topo do feed. Algumas das principais funções do X são:

- **Tweeting**: Os usuários podem criar tweets curtos e publicá-los em suas contas para compartilhar informações, opiniões ou atualizações pessoais.
- **Retweet**: Os usuários podem compartilhar tweets de outras pessoas para seus próprios seguidores. Isso ajuda a disseminar informações rapidamente e ampliar o alcance de um tweet.
- **Like**: Os usuários podem "curtir" um tweet para indicar que gostaram do conteúdo. As curtidas são representadas por um ícone de coração.

- **Seguir**: Os usuários podem seguir outras contas para ver os tweets dessas contas em sua linha do tempo. Isso permite que as pessoas acompanhem as atualizações de amigos, celebridades, empresas e outras figuras públicas.
- **Hashtags**: Adicionar "#" seguido por uma palavra-chave cria uma hashtag. As hashtags são usadas para categorizar e organizar tweets relacionados a um tópico específico. Ao clicar em uma hashtag, os usuários podem ver todos os tweets que a usam.
- **Mensagens Diretas (DMs)**: Os usuários podem enviar mensagens privadas para outros usuários. Essas mensagens não são visíveis publicamente e são trocadas apenas entre as contas envolvidas.
- **Twitter Spaces:** Uma funcionalidade mais recente que permite aos usuários participar de salas de áudio ao vivo, onde podem conversar e discutir tópicos em tempo real.

Ameaças e Ataques

Como todo grande serviço virtual, o X está constantemente exposto a ameaças e ataques, que podem prejudicar a plataforma e/ou seus usuários. Algumas das mais notáveis são:

- **Phishing e Engenharia Social**: Ataques de phishing envolvem tentativas de enganar os usuários para revelarem informações confidenciais, como senhas, através de mensagens ou sites falsos. A engenharia social explora a manipulação psicológica para obter acesso não autorizado a contas.
- **Contas Falsas e Bots**: Contas falsas e bots automatizados são usados para disseminar desinformação, spam, links maliciosos e para fins de engajamento falso. Isso pode afetar a autenticidade e a confiabilidade da plataforma.
- **Roubo de Contas**: Hackers podem tentar acessar contas de usuários legítimos por meio de invasões ou explorações de vulnerabilidades. Uma vez que uma conta é comprometida, os invasores podem enviar tweets maliciosos, roubar informações pessoais ou prejudicar a reputação do titular da conta.
- **Vazamentos de Dados**: A exposição acidental ou intencional de dados dos usuários, como endereços de e-mail e senhas, pode resultar em violações de privacidade e acesso não autorizado.
- **Ameaças à Privacidade**: As configurações de privacidade inadequadas podem levar à exposição indevida de informações pessoais, como localização, dados de contato e interações.
- **Ataques de Denegação de Serviço (DDoS)**: Ataques DDoS visam sobrecarregar os servidores do X com tráfego excessivo, tornando a plataforma inacessível para os usuários legítimos.
- **Exploração de Vulnerabilidades:** Vulnerabilidades em sistemas e aplicativos podem ser exploradas por hackers para obter acesso não autorizado ou para realizar atividades maliciosas.

- **Conteúdo Malicioso:** Links e anexos maliciosos podem ser compartilhados através de tweets, mensagens diretas ou perfis de usuário, levando a downloads de malware ou páginas de phishing.

Pontos de Controle

- **Autenticação:** É necessário garantir que todo usuário tenha acesso a sua conta, e que outros não possam invadi-la por qualquer motivo que seja. O X utilizava a autenticação de dois fatores (2FA) exigindo que os usuários forneçam uma segunda forma de autenticação, como um código enviado para o celular, além da senha, para acessar suas contas.
- **Segurança:** Como principal ponto de controle, é necessário que haja segurança, para que os usuários utilizem o X sem preocupação. O X estabelece regras e políticas de uso que definem o que é permitido e o que não é permitido na plataforma. Isso inclui restrições sobre discurso de ódio, assédio, spam e outros comportamentos inadequados. Monitora atividades maliciosas, como bots, contas falsas e atividades coordenadas, para proteger a integridade da plataforma e etc.
- **Privacidade:** No X, usuários têm direito a serem anônimos, e para tal o site possui algumas ferramentas que buscam garantir a privacidade do usuário. Como medidas de criptografia para proteger as comunicações e os dados dos usuários.
- **Qualidade:** Como um produto, o X deve manter um ambiente propício para uso, que seja confortável e seguro, que agrade os usuários os incentivando a continuar utilizando a plataforma. Através de relatórios e denúncias, onde usuários podem denunciar tweets, contas ou comportamentos que violem as políticas do X. Esse sistema permite que os usuários denunciem abusos, spam e outras violações. Mecanismos anti spam, que identificam e combatem contas de spam e atividades suspeitas, ajudando a manter a qualidade da plataforma. Estabelecendo limites de uso para evitar comportamentos abusivos ou automatizados em massa, como o envio excessivo de tweets ou seguidores.

IV – Desenvolver uma Matriz de Riscos para identificar possíveis riscos analisando os pontos de controle que o aplicativo possui:

Ameaças

Phishing e Engenharia Social (Ph)

- Probabilidade Moderada(50%), Impacto Baixo. Não afeta diretamente o sistema ou integridade do site, porém afeta os usuários que caem nele e a reputação do serviço em si, uma vez que pessoas evitariam utilizar uma plataforma onde golpes são constantes.

Bots (B)

- Probabilidade Muito Alta(90%), Impacto Muito Alto. Pode afetar o sistema, já que pode sobrecarregar os servidores, ser usado para marketing injusto e afins.

Roubo de Contas (RC)

- Probabilidade Moderada(50%), Impacto Muito Alto. Se uma figura importante ou famosa tiver a conta roubada, o impacto imediato pode ser enorme

Roubo/Vazamento de dados pessoais

Oportunidades

Sistema de Denúncia (SD)

- Probabilidade Muito Alta(90%), Impacto Moderado. O X deve ser um ambiente próprio para usuários, dar a eles uma ferramenta de denúncia ajudaria não só a punir usuários que utilizam serviço de maneira indevida, mas de garantir um bom ambiente para os usuários.

Avisos de Segurança (AS)

- Probabilidade Muito Alta(90%), Impacto Moderado. Ter avisos de que usuários não devem mandar informações privadas, que links não vinculados ao X não são seguros e etc.

Mecanismos de Detecção e Banimento de Bots (MDB)

- Probabilidade Muito Alta(90%), Impacto Muito Alto. É extremamente necessário aplicar mecanismos para combater o uso de bots, levando em conta seu impacto.

Autenticação de 2 Fatores (2F)

- Probabilidade Alta(70%), Impacto Alto. A verificação de dois fatores ajuda a prevenir roubos e invasões de contas, uma vez que oferece identificação aos usuários através da combinação de dois componentes diferentes.