Web xKaliBurr: uma Plataforma Online para Levantamento de Informações em Pentest em Aplicações na Internet

Daniel R. Barros[1], Lucas Cabral[1], João V. A. Oliveira[1], Felipe M. Castro[1], Lucas L. Soares[1], José M. Monteiro[1], Joaquim Bento[1] e Lincoln S. Rocha[1].

[1]Laboratório de Sistemas e Bancos de Dados (LSBD)
Departamento de Computação (DC)
Universidade Federal do Ceará (UFC) – Fortaleza, CE – Brasil.

{daniel.rezende,lucas.cabral,joao.alves,
felipe.moura,lucas.lopes,jose.monteiro,
joaquim.bento}@lsbd.ufc.br e lincoln@dc.ufc.br

Abstract. *The Information Gathering stage in web Pentests is crucial as it lays the foundation for all subsequent activities. However, comprehensive information gathering requires the manual use of various tools that demand advanced technical knowledge. We propose Web xKaliBurr, an open-source web tool that automates the information gathering stage. With a user-friendly interface, the tool performs extensive scans from the site's URL, providing a wide range of information and recommendations, allowing users without advanced knowledge to assess their site's security and detect potential flaws or vulnerabilities.*

Resumo. *A etapa de Levantamento de Informações em Pentests web é fundamental pois estabelece as bases para todas as atividades subsequentes. Contudo, um levantamento abrangente exige o uso manual de várias ferramentas que demandam conhecimento técnico avançado. Propomos o Web xKaliBurr, uma ferramenta online de código aberto que automatiza a etapa de levantamento de informações. Com uma interface amigável, a ferramenta realiza varreduras amplas a partir da URL do site, fornecendo uma gama maior de informações e recomendações de investigação, permitindo que usuários sem conhecimento avançado possam avaliar a segurança de seus sites e detectar possíveis falhas ou vulnerabilidades.*

1. Introdução

O *Pentest* (teste de penetração) é uma simulação controlada de ataques cibernéticos, realizada para identificar e corrigir vulnerabilidades de segurança antes que possam ser exploradas por invasores mal-intencionados [Weidman 2014]. A realização de *Pentests* em sistemas web é uma prática essencial para garantir a segurança e integridade das informações em ambientes online.

As etapas típicas de um *Pentest* incluem Planejamento, Levantamento de Informações, Modelagem de Ameaças, Análise de Vulnerabilidades, Exploração, Pós-Exploração e Relatório Técnico [Weidman 2014]. Entre essas etapas, a de Levantamento de Informações é fundamental, pois envolve a coleta de dados sobre o alvo, como domínios, endereços IP, tecnologias utilizadas e potenciais pontos fracos. Esta fase inicial estabelece a base para todas as atividades subsequentes do *Pentest*, tornando

a abrangência das informações coletadas de vital importância para o sucesso do teste [Stuttard and Pinto 2011].

A etapa de Levantamento de Informações é facilitada pela existência de ferramentas de código aberto que permitem coleta de dados de aplicações web. Contudo, as ferramentas existentes apresentam limitações. Primeiro, cada uma delas realiza a coleta de uma informação específica, de forma que realizar o levantamento completo de informações envolve o trabalho manual de executar sequencialmente várias ferramentas. Segundo, a maior parte dessas ferramentas costumam ser executadas por meio de linhas de comandos em terminais, exigindo um conhecimento técnico avançado [Najera-Gutierrez and Ansari 2018]. Finalmente, a interpretação dos resultados obtidos e a identificação das possíveis vulnerabilidades são dependentes da experiência do analista.

Dado esse contexto, este trabalho propõe uma ferramenta web de código aberto para automação da etapa de Levantamento de Informações de *Pentest* em sites, chamada **Web xKaliBurr**[1]. Esta ferramenta provê uma interface de fácil uso que permite uma varredura extensiva de informações em sites, necessitando apenas do nome do domínio e o protocolo de comunicação como entrada. Além disso, os dados obtidos são apresentados em conjunto com recomendações de segurança, de modo a informar o usuário sobre as possíveis vulnerabilidades relacionadas. Assim, a ferramenta permite que usuários sem conhecimento avançado em segurança da informação consigam realizar uma avaliação inicial das superfícies de ataque existentes em seus domínios.

O restante deste trabalho está organizado da seguinte forma: na Seção 2, apresentamos os trabalhos relacionados, destacando as ferramentas existentes com o intuito alinhado com a nossa. Na Seção 3, descrevemos detalhadamente a ferramenta proposta, incluindo sua arquitetura, funcionalidades e o fluxo de execução. Na Seção 4, discutimos os resultados obtidos a partir da aplicação da ferramenta em um cenário de teste, avaliando sua eficácia na identificação de vulnerabilidades. Por fim, na Seção 5, apresentamos as conclusões e sugerimos direções para trabalhos futuros.

2. Trabalhos Relacionados

Encontram-se na literatura e na indústria plataformas online voltadas para análises de segurança da informação que são correlatas ao Web xKaliBurr. Estas ferramentas são acessadas na internet e necessitam de poucas informações para retornarem a análise desejada.

O artigo de [Antunes et al. 2022] apresenta uma plataforma web personalizável para gerenciar a conformidade de aplicações web com padrões de auditoria de cibersegurança. A plataforma recebe como entrada a URL de um site e a importação de listas de verificação do padrão *ISO-27001*, realizando a verificação automática de conformidade aos padrões de segurança. A ferramenta de [Probely 2024] é um recurso online gratuito que realiza uma verificação dos cabeçalhos de segurança que figuram nas comunicações entre clientes e servidores, presentes no tráfego de pacotes na internet. O serviço [DeHashed 2024] é um mecanismo de busca de ativos e mineração de dados na *deep web*, especializado na detecção e coleta de informações vazadas, tais como credenciais de login de usuários e sistemas inteiros.

[1]Repositório: https://github.com/xKaliBurr2024/SBSeg2024

Plataforma	Open-Source	Gratuita	Finalidade
[Antunes et al. 2022]	Não	Não	Verificação de Padrões de Segurança
[Probely 2024]	Não	Sim	Análise de Cabeçalhos de Segurança
[DeHashed 2024]	Não	Não	Vazamento de Dados Sensíveis
Web xKaliBurr	Sim	Sim	Levantamento de Informações

Tabela 1. Comparações entre Plataformas

A Tabela 1 faz uma comparação entre as ferramentas analisadas nesta seção e a nossa proposta. Segundo nosso conhecimento, o Web xKaliBurr é a única plataforma de código-aberto para automação de Levantamento de Informações de sites. Nossa ferramenta é inspirada na proposta de [Barros et al. 2023], se diferenciando pelo incremento do acesso online e as recomendações de pontos de segurança, facilitando o uso para usuários com menor conhecimento técnico.

3. Web xKaliBurr

3.1. Visão Conceitual e Fluxos de Exploração

A ferramenta Web xKaliBurr provê um serviço que realiza um amplo Levantamento de Informações de aplicações online, recebendo como entrada o protocolo de comunicação e o nome de domínio do site. A partir dessa entrada, o Web xKaliBurr inicia seu *pipeline* de exploração, realizando varreduras em busca de mais informações sobre o alvo especificado, revelando possíveis superfícies de ataque. Na Figura 1, são ilustradas as etapas de funcionamento da ferramenta.

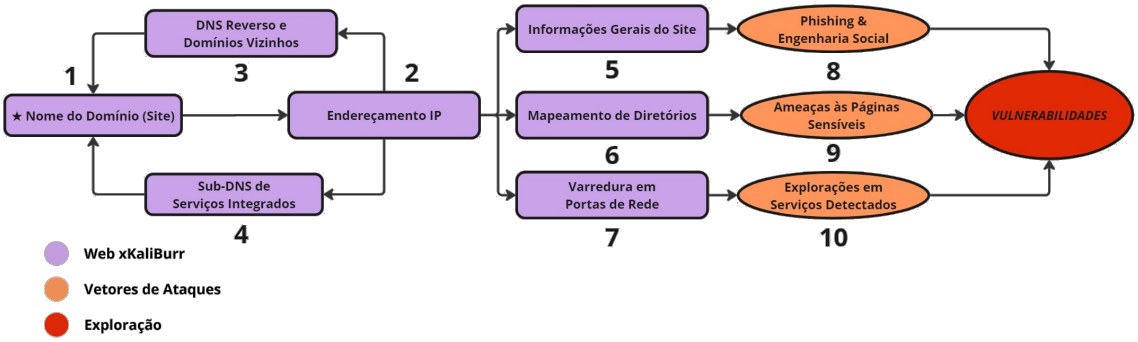

Figura 1. Fluxo de processos do Web xKaliBurr

A ferramenta inicia seu processo com investigações relacionadas à identificação de endereços IP (Protocolo de Internet), à enumeração do DNS (Sistema de Nomes de Domínio) e aos subsistemas integrados ao alvo em análise, conforme retratado nas etapas 2, 3 e 4 da Figura 1. Após obter informações sobre os serviços e endereços IP vinculados ao alvo, o Web xKaliBurr prossegue com buscas mais aprofundadas, abordando quatro principais fluxos de exploração:

1. **Vazamento de Informações:** cenário em que um atacante direciona seus esforços para focar nos funcionários e administradores do serviço. Esses tipos de ataques podem ser caracterizados por golpes de Engenharia Social [Dewan et al. 2014].

Nesses casos, o agente malicioso busca obter informações privilegiadas utilizando dados verdadeiros básicos que podem ser descobertos por meio do Levantamento de Informações. O fluxo de exploração $\{1, 2, 5, 8\}$ da Figura 1 ilustra esse cenário.

2. **Mapeamento de Páginas Sensíveis:** cenário que visa revelar todas as páginas e diretórios ocultos relacionados ao sistema-alvo. Assim, um agente malicioso pode identificar novas superfícies de ataque ao descobrir páginas que não devem ser acessadas por usuários comuns, como painéis de login de funcionários ou serviços de transmissão de arquivos do sistema. O fluxo de exploração $\{1, 2, 6, 9\}$ na Figura 1 ilustra esse cenário.

3. **Detecção de Serviços:** cenário no qual busca-se identificar e obter as versões das tecnologias utilizadas pela infraestrutura do alvo. Neste contexto, um agente malicioso pode capturar essas informações e, a partir delas, realizar abordagens para tentar explorar vulnerabilidades nesses serviços. O fluxo de exploração $\{1, 2, 7, 10\}$ da Figura 1 ilustra essa operação.

4. **Identificação de Vizinhança:** este cenário foca na detecção e identificação de domínios vizinhos, ou seja, páginas e aplicações online presentes no mesmo intervalo de endereçamento IP do alvo analisado. Assim, um atacante pode realizar a "movimentação lateral", quando o ataque direto ao alvo não é possível, mas um domínio conectado a ele está mais vulnerável, aumentando a superfície de ataque dos agentes maliciosos. O fluxo de exploração $\{2, 3, 4\}$ na Figura 1 ilustra essa operação.

As informações referentes a cada fluxo de informação obtidas pela execução da ferramenta são retornadas em páginas web de forma categorizada. Após a execução da ferramenta, são apresentadas para cada fluxo as potenciais vulnerabilidades e recomendações de pontos de atenção relacionados, facilitando a compreensão de usuários com menor conhecimento técnico.

3.2. Implementação

A base para a implementação do Web xKaliBurr reside em recursos encontrados no sistema operacional Kali Linux[2], uma distribuição GNU/Linux baseada na arquitetura Debian, reconhecido como um ambiente completo para testes de penetração e análise de segurança. O sistema utiliza uma arquitetura cliente-servidor, onde o *back-end* é composto por um *container* Docker com uma imagem personalizada baseada no Kali Linux. Esse *container* encapsula todos os softwares e ferramentas que são executadas no Web xKaliBurr, para a realização das atividades de exploração. Uma API serve como canal de comunicação entre as ferramentas no *back-end* e o *front-end*. A API foi construída utilizando a linguagem Python e o *framework* Flask, utilizando seus recursos nativos para realizar as chamadas de execução de cada uma das ferramentas que compõe o sistema. Essa arquitetura é ilustrada na Figura 2.

Os processos e ferramentas utilizadas, de acordo com as etapas ilustradas na Figura 1, são os seguintes:

[2]https://www.kali.org/

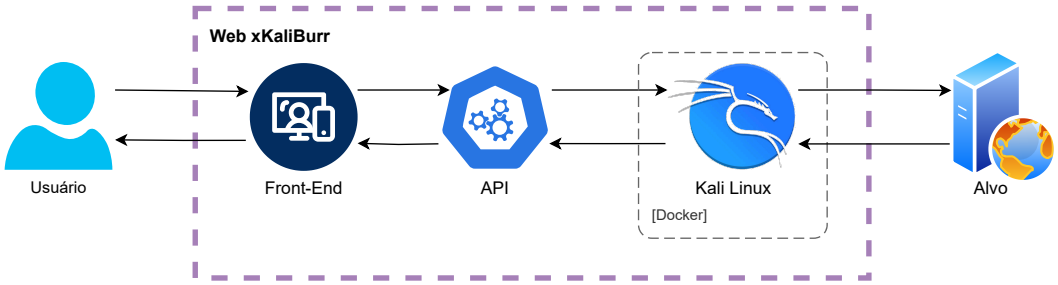

Figura 2. Arquitetura Web xKaliBurr

- **Etapa 1:** Procede-se à inserção dos parâmetros, que incluem o nome de domínio do site e o protocolo de comunicação utilizado (HTTP ou HTTPS).
- **Etapa 2:** Procede-se à descoberta dos endereços IP relacionados ao domínio alvo. Para tal finalidade, empregam-se as ferramentas WhatWeb e Host.
- **Etapas 3 e 4:** Explorações recursivas são realizadas utilizando DNS reverso e sub-DNS, com o objetivo de verificar a existência de sistemas relacionados ao alvo principal. Nessa etapa, são empregados os softwares DNSRecon e DNSMap.
- **Etapas 5 e 8:** Realiza-se a coleta de informações gerais, incluindo dados como nomes de proprietários, empresas ou funcionários, e-mails de contato, e outras informações que podem servir como base para ataques maliciosos. Os buscadores de dados utilizados nesta etapa foram WhatWeb, WhoIs e CURL.
- **Etapas 6, 9:** Procede-se à investigação de diretórios mediante verificações de força bruta em possíveis páginas web, empregando-se os softwares DIRB e GoBuster para a detecção de páginas ocultas suscetíveis a falhas de segurança.
- **Etapas 7, 10:** Utilizando a ferramenta NMAP, identifica-se os serviços empregados na infraestrutura do alvo e suas versões. Potenciais falhas de segurança podem ser identificadas por meio da exploração de vulnerabilidades documentadas, estratégia comumente empregada em sistemas com serviços desatualizados em execução.

4. Demonstração

4.1. Alvo de Exploração

O alvo selecionado foi o ambiente online OWASP Juice Shop[3], desenvolvida pela organização OWASP (Open Web Application Security Project) para treinamentos em segurança da informação. O Juice Shop abrange vulnerabilidades de toda a lista OWASP Top Ten [OWASP Foundation 2021], representando os riscos de segurança mais críticos para aplicações web. Devido ao seu fim educacional, o Juice Shop possui uma série de desafios que envolvem realizar etapas de *Pentest*. Ao completar cada desafio, o progresso é contabilizado no *Score Board* da página.

4.2. Resultados

A análise do Web xKaliBurr inicia ao inserir o domínio e protocolo de comunicação do alvo, conforme exemplificado na Figura 3.

[3]https://juice-shop.herokuapp.com/

Figura 3. Exemplo de Input na Plataforma Web xKaliBurr

Após executar as explorações no Juice Shop, o Web xKaliBurr foi capaz de solucionar 26 dos 169 desafios existentes, que correspondem aos desafios relacionados à etapa de Levantamento de Informações. Esses desafios seriam tipicamente solucionados de forma manual, enquanto que a ferramenta permitiu automatizar esse processo. Os desafios não completos correspondem à etapas subsequentes de *Pentest*, muitos dos quais utilizam informações levantadas na etapa realizada pelo Web xKaliBurr. Além disso, é importante ressaltar que o Web xKaliBurr foi desenvolvido para realizar uma varredura abrangente, não levando em consideração um conhecimento a priori sobre o Juice Shop ou outro alvo em particular. Embora a quantidade de desafios solucionados não seja uma métrica válida para avaliar o desempenho da ferramenta, já que muitos dos desafios fogem do seu escopo, consideramos um resultado satisfatório para ilustrar a sua funcionalidade.

Figura 4. Resultados do *Score Board* Juice Shop

Pode-se também analisar os desafios completados de acordo com as seguintes categorias de vulnerabilidade do OWASP Juice Shop:

- **`Exposição de Dados Sensíveis:`** Cenários nos quais informações confidenciais ou privadas são inadvertidamente reveladas ou expostas a indivíduos não autorizados. A identificação dessa vulnerabilidade foi realizada por meio das etapas 3, 4, 6 e 7 do Web xKaliBurr.
- **`Validação de Entrada Imprópria:`** Essa vulnerabilidade ocorre quando um sistema não verifica corretamente os dados fornecidos pelos usuários antes de processá-los, permitindo a injeção de dados maliciosos. A exploração dessa falha ocorreu ao manipular parâmetros em solicitações HTTP, utilizando as ferramentas presentes na etapa 6 do Web xKaliBurr.
- **`Controle de Acesso Quebrado:`** Ocorre quando um sistema não aplica corretamente as restrições de acesso a recursos protegidos, permitindo acesso não autorizado a funcionalidades ou informações. As áreas vulneráveis foram identificadas durante a execução do Mapeamento de Diretórios na etapa 6 do Web xKaliBurr.

- **`Redirecionamentos Inválidos:`** Ocorre quando um aplicativo web redireciona o usuário para uma URL não confiável ou inválida sem realizar as verificações adequadas. A ferramenta CURL, presente na etapa 5 do Web xKaliBurr, pode executar esses redirecionamentos de URL de forma inadequada no alvo.
- **`Autenticação Quebrada:`** Cenário onde medidas de autenticação são mal configuradas, permitindo que atacantes comprometam os mecanismos de segurança para acessar recursos protegidos. Essas vulnerabilidades foram exploradas pela ferramenta NMAP, na etapa 7 do processo de exploração do Web xKaliBurr, durante a varredura de portas de rede na infraestrutura do alvo.
- **`Configuração de Segurança Inadequada:`** Cenário no qual existem configurações inadequadas que tornam o sistema mais suscetível a explorações por parte de atacantes. A ferramenta WhatWeb, utilizada na etapa 5 da exploração, detectou a exposição das interfaces de administração no sistema alvo.

Além da conclusão automática dos desafios, o Web xKaliBurr também obteve informações relacionadas às características da infraestrutura do domínio do Juice Shop, relacionadas aos quatro fluxos de exploração executados pela plataforma, como representados na Figura 5. Através da análise dessas informações, é possível identificar as configurações e tecnologias utilizadas pelo próprio domínio de hospedagem do Juice Shop, coletando informações ocultas sobre a plataforma partindo unicamente dos dados públicos relacionados ao nome do domínio do site. A Figura 5 também ilustra a funcionalidade de recomendação da ferramenta, no qual são aconselhadas ações e pontos de atenção sobre boas práticas de segurança, facilitando a análise para usuários menos experientes.

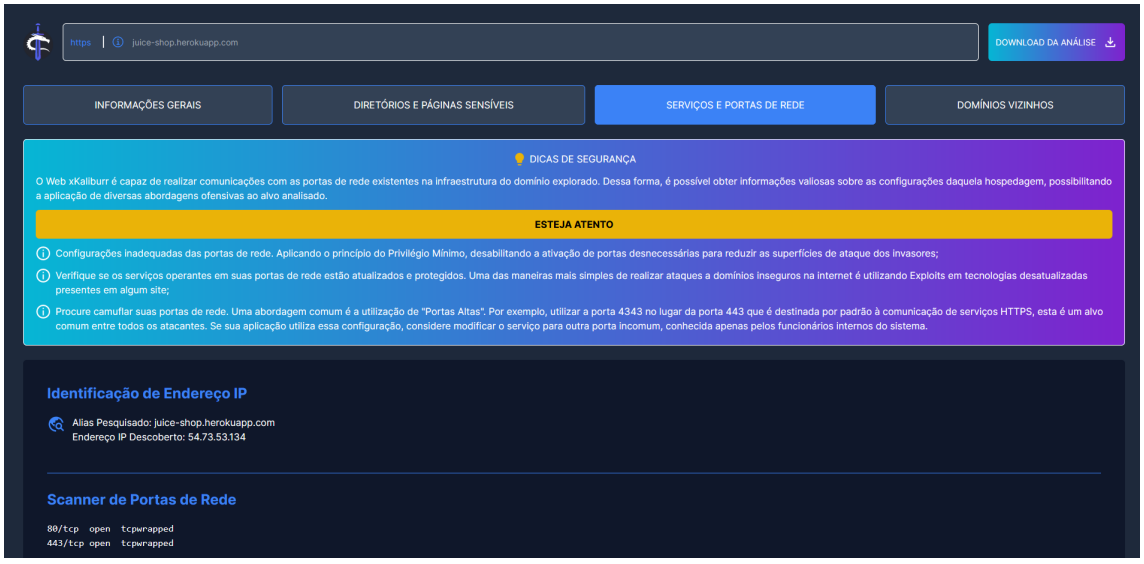

Figura 5. Trecho com Exibição de Resultados

4.3. Apresentação no Salão de Ferramentas

O código fonte, documentação e instruções de instalação estão acessíveis no repositório público do Web xKaliBurr. A demonstração da ferramenta ocorrerá em um ambiente

controlado e provido por um dispositivo próprio dos autores. As funcionalidades da ferramenta serão delineadas pelos seguintes procedimentos: (i) definição de um alvo de exploração; (ii) exemplificação do uso da ferramenta; (iii) exposição dos resultados da execução; (iv) análise e discussão das potenciais vulnerabilidades identificadas.

5. Conclusão

Este trabalho propôs uma ferramenta web de código-aberto para Levantamento de Informações para *Pentests* web, chamada Web xKaliBurr. A ferramenta permite a realização de uma ampla varredura automática, com a coleta de informações que seriam tipicamente coletadas de forma manual. Ela possui uma interface acessível e retorna seus resultados em conjunto com recomendações de segurança, facilitando o uso por usuários menos experientes. Como trabalhos futuros pretendemos executar a ferramenta em uma grande quantidade de sites para coletar um conjunto de dados de informações de sites. Iremos realizar a análise deste conjunto de dados e desenvolver modelos preditivos de aprendizado de máquina para identificação automática de vulnerabilidades conhecidas.

Agradecimentos

Este trabalho foi parcialmente financiado pela Lenovo, como parte de seu investimento em P&D pela Lei de Informática (Lei nº 8.248/1991).

Referências

Antunes, M., Maximiano, M., and Gomes, R. (2022). A customizable web platform to manage standards compliance of information security and cybersecurity auditing. *Procedia Computer Science*, 196:36–43.

Barros, D. R., Pimenta, S. A., Rocha, L. S., and Monteiro, J. M. (2023). Exekaliburr: uma ferramenta exploratória auxiliar para o levantamento de informaçoes em pentests web. In *Anais Estendidos do XXIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 1–8. SBC.

DeHashed (2024). Dehashed. Take your employee security to the next level. Disponível em https://dehashed.com/. Acessado em 04 de Junho de 2024.

Dewan, P., Kashyap, A., and Kumaraguru, P. (2014). Analyzing social and stylometric features to identify spear phishing emails. In *2014 apwg symposium on electronic crime research (ecrime)*, pages 1–13. IEEE.

Najera-Gutierrez, G. and Ansari, J. A. (2018). *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd.

OWASP Foundation (2021). *OWASP Top 10:2021*. OWASP Foundation. Disponível em https://owasp.org/www-project-top-ten/. Acessado em 04 de Junho de 2024.

Probely, S. H. P. (2024). Security headers powered by probely. Probely Cybersecurity Company with Dynamic Application Security Testing (DAST) tools. Disponível em https://securityheaders.com/. Acessado em 04 de Junho de 2024.

Stuttard, D. and Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Wiley.

Weidman, G. (2014). *Penetration Testing: A Hands-on Introduction to Hacking*. Novatec.