Web xKaliBurr: Uma Plataforma Online para Levantamento de Informações para Pentests em aplicações na Internet

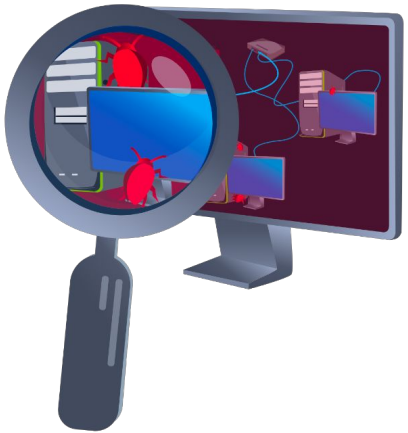
UFC

lsbd

Lenovo

Daniel R. Barros, Lucas Cabral, João V. Alves, Felipe M. Castro, Lucas L. Soares, Lincoln S. Rocha, José M. Monteiro, Joaquim B. Cavalcante-Neto.

Motivação



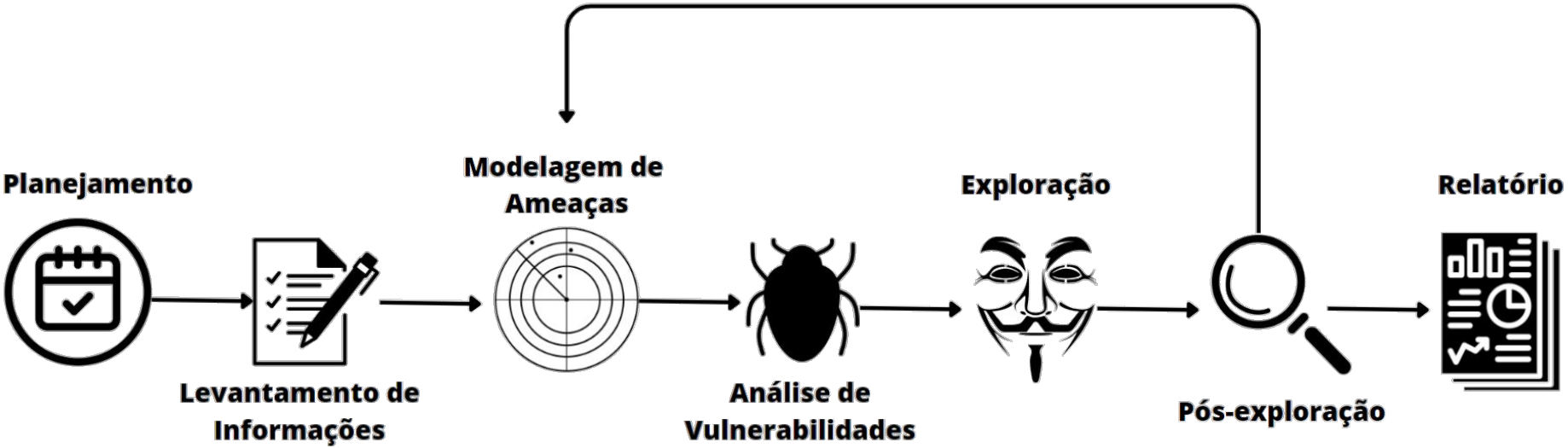
Segurança Ofensiva

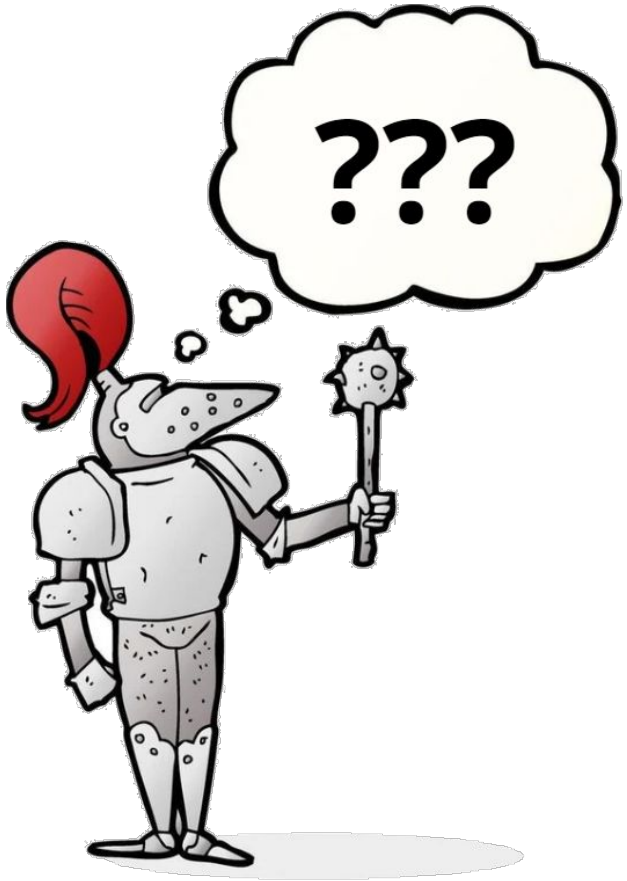
Abordagem que se concentra na criação de técnicas e estratégias para proteger uma organização ou sistemas por meio de ações proativas destinadas a identificar, explorar e neutralizar potenciais ameaças.

O Pentest

Uma das principais estratégias empregadas em verificações de segurança, geralmente conduzida por especialistas em Segurança Ofensiva.

As Etapas de um Pentest





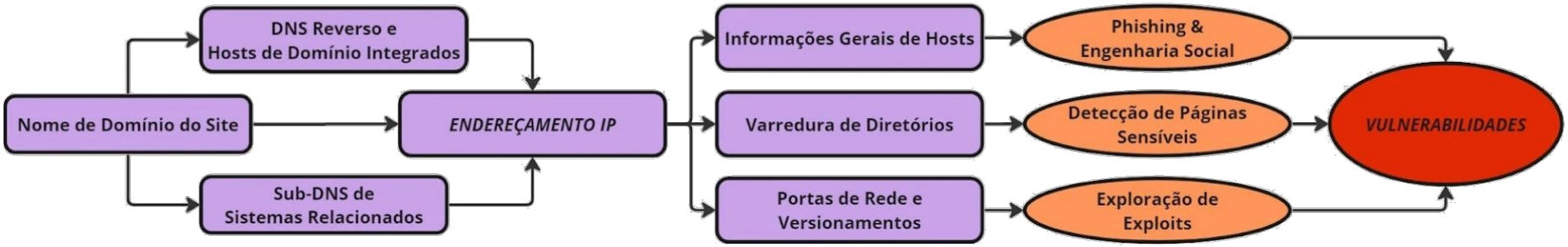
Desafios e Dificuldades

- Processo Manual
- Escolha de Ferramentas Adequadas
- Duração da Execução
- Experiência e Competência

A Solução

Ferramenta auxiliar de exploração destinada a apoiar profissionais de Segurança Ofensiva na condução de um Pentest Web, na modalidade Black Box.

Framework de Exploração



- Web xKaliBurr
- Vetores de Ataques
- Exploração de Vulnerabilidade

Demonstração

OWASP

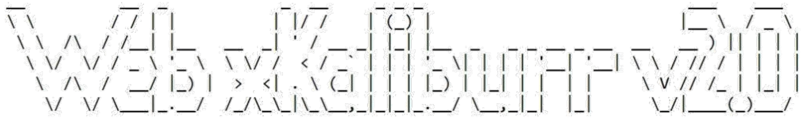
Open Web Application Security Project

Alvo: Juice Shop

- Aplicação vulnerável integrante do Projeto OWASP Vulnerable Web Applications Directory (VWAD).
- Ambiente de treinamento e testes utilizado por profissionais para a avaliação de ferramentas de hacking e técnicas ofensivas.

Web xKaliBurr

by
round table team



```
By round table team

###########################################
###     Identificação de Endereço IP    ###
###########################################

Alias usado: juice-shop.herokuapp.com
Endereço IP Descoberto: 54.220.192.176

Outras Informações Relacionadas aos Endereçamentos IP do Alvo:
WhatWeb report for http://juice-shop.herokuapp.com/
Status     : 200 OK
Title      : OWASP Juice Shop
IP         : 46.137.15.86
Country    : IRELAND, IE

Summary    : HTML5, HTTPServer[Cowboy], JQuery[2.2.4], Script[module], UncommonHeaders[report-to,reporting-endpoints,nel,access-control-allow-origin,x-content-type-option

Detected Plugins:
[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Cowboy (from server string)

[ JQuery ]
        A fast, concise, JavaScript that simplifies how to traverse
        HTML documents, handle events, perform animations, and add
        AJAX.

        Version      : 2.2.4
        Website     : http://jquery.com/

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : module
```

```
[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : report-to,reporting-endpoints,nel,access-control-allow-origin,x-content-type-options,feature-policy,x-recruiting (from headers)

[ Via-Proxy ]
        This plugin extracts the proxy server details from the Via
        param of the HTTP header.

        String       : 1.1 vegur

[ X-Frame-Options ]
        This plugin retrieves the X-Frame-Options value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : SAMEORIGIN

HTTP Headers:
        HTTP/1.1 200 OK
        Server: Cowboy
        Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1719020727&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=ZM343WXor5xO4qi6nS8qIa5LtgY5XWmcdsmrX0X1B1g%3D"}]}
        Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1719020727&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=ZM343WXor5xO4qi6nS8qIa5LtgY5XWmcdsmrX0X1B1g%3D
        Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
        Connection: close
        Access-Control-Allow-Origin: *
        X-Content-Type-Options: nosniff
        X-Frame-Options: SAMEORIGIN
        Feature-Policy: payment 'self'
        X-Recruiting: /#/jobs
        Accept-Ranges: bytes
        Cache-Control: public, max-age=0
        Last-Modified: Sat, 22 Jun 2024 00:39:12 GMT
        Etag: W/"ea4-1903d6203ad"
        Content-Type: text/html; charset=UTF-8
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Date: Sat, 22 Jun 2024 01:45:27 GMT
        Transfer-Encoding: chunked
        Via: 1.1 vegur


##############################################
###      Scanner de Portas de Redes      ###
##############################################

80/tcp  open  http      heroku-router
443/tcp open  ssl/https heroku-router

#################################
###   Varredura de Diretórios   ###
#################################
```

Trabalhos Futuros

- Automatização e execução das demais etapas de Pentest.
- Execução simultânea em múltiplos alvos.
- Geração de conjuntos de dados científicos e colaborativos das vulnerabilidades mais encontradas.
- Incorporação de modelos de aprendizado de máquina para interpretação e priorização dos resultados.

Obrigado!

SBSeg24
SÃO JOSÉ DOS CAMPOS

UFC

lsbd

Lenovo