

**Departamento de Engenharias e Tecnologias**

**MULTIMÉDIA**

2022/2º Semestre

**RELATÓRIO**

**Elaborado por**

Andreia Brito

Budy Vieira

Helder da Costa

**Curso:** Engenharia Informática

**Turma:** EINF8\_T1

**Docente:** Bongo Cahisso

26/06/2022

**Índice**

[1. Introdução 5](#_Toc106044517)

[2. Fundamentação Teórica 6](#_Toc106044518)

[2.1 Sobre a Startup 6](#_Toc106044519)

[2.2 Cibersegurança 6](#_Toc106044520)

[2.3 Ferramenta utilizada 7](#_Toc106044521)

[2.3.1. Exploits 7](#_Toc106044522)

[2.3.2 Carga útil ou payload 8](#_Toc106044523)

[2.4 Tecnologias Implementadas 8](#_Toc106044524)

[3. Conclusão 9](#_Toc106044525)

[4. Referências bibliográficas 10](#_Toc106044526)

# Introdução

Se antes da pandemia de Covid-19 já vivíamos em um mundo conectado, o salto digital entre 2020 e 2021 acelerou todas as estimativas sobre a produção e troca de dados cibernéticos. O home office e outras práticas de trabalho a distância, como espaços colaborativos e compartilhados, vieram para ficar e empresas de todo o planeta já manifestaram intenção de incorporar novos modelos de atendimento e de manter os seus colaboradores a trabalhar, pelo menos parcialmente, a partir de casa.

Por outro lado, também cresceram vertiginosamente os crimes e as ameaças virtuais. Os hackers se aproveitam das vulnerabilidades de nossos dispositivos eletrônicos e das redes que utilizamos para realizar ataques que podem gerar prejuízos incalculáveis.

A segurança cibernética, assim como a segurança digital, é um braço da segurança da informação que tem como objetivo prevenir os ataques, realizados por sistemas maliciosos que se aproveitam de falhas sistêmicas para invadir dispositivos, roubando, manipulando e tornando indisponível uma série de dados ou arquivos.

Os profissionais de cibersegurança são responsáveis por desenvolver e executar soluções de rede seguras, realizando uma série de testes a partir do uso de diferentes ferramentas com o objetivo de proteger a empresa contra ameaças virtuais e ataques de hackers criminosos. E um dos testes mais utilizados para descobrir vulnerabilidades de um sistema são os testes de penetração, conhecidos como PenTest.

* 1. **Objectivo geral**
* Realizar testes de penetração no servidor da startup.
  1. **Objectivos específicos**
* Identificar as vulnerabilidades do sistema;
* Avaliar os requisitos de segurança da startup;
* Supervisionar os dispositivos da startup para proteger a integridade dos dados.

# Fundamentação Teórica

## 2.1 Sobre a Startup

E-barato consiste numa startup cujo o objectivo é tornar a interação entre mercados e clientes mais agradável.

O e-barato vem dar solução a situações como as filas enormes nos mercados e os problemas de pouca afluência de clientes em mercados menos conhecidos. Outro problema a ser resolvido, é a procura exaustiva pelo preço mais barato dos produtos por parte dos clientes.

Uma parte essencial para o desenvolvimento da startup são as parcerias com os mercados, e sendo essas instituições de todos os portes (pequenas, médias ou grandes) um dos pontos cruciais para a colaboração com os mercados é a segurança, visto que a startup terá de trabalhar com informações de stock e outras para o desempenho das suas funcionalidades. Neste âmbito, proteger o sistema da startup contra as ameaças do ciberespaço é de extrema importância para o cumprimento dos objectivos estratégicos do E-Barato.

## 2.2 Cibersegurança

Segundo a CISCO, a cibersegurança é a prática de proteger sistemas, redes e programas contra-ataques digitais. Esses ataques cibernéticos geralmente visam acessar, alterar ou destruir informações confidenciais; extorquir dinheiro dos usuários; ou interromper processos normais de negócios.

A implementação de medidas eficazes de segurança cibernética é particularmente desafiadora hoje porque há mais dispositivos do que pessoas e os invasores têm se tornando mais inovadores.

O tema tem ganhado cada vez mais importância tendo em vista o crescente número de ataques a pessoas e empresas de todos os portes, demonstrando a vulnerabilidade do mundo virtual, que conta com uma vasta rede de dados. A cibersegurança já é um dos principais temas da agenda de executivos e líderes em todo mundo.

Na era da Indústria 4.0 a cibersegurança é fundamental, já que tudo está conectado e, mais que nunca, é necessário desenvolver práticas e mecanismos capazes de eliminar e/ou reduzir riscos e falhas para se defender de hackers e criminosos virtuais. E é preciso um conjunto de estratégias para atuar nos vários momentos da cadeia de valor, sendo capaz de prevenir, monitorar e defender as empresas, organizações governamentais e cidadãos contra os ataques à segurança cibernética.

Os ataques virtuais são realizados por diferentes motivos e mostram que qualquer um está suscetível a esses crimes digitais. Um hacker pode invadir uma rede com intenções que vão desde o ganho financeiro até o terrorismo de Estado.

Algumas motivações para os ataques cibernéticos são:

* Extorquir dinheiro por meio de ameaças de divulgação de dados confidenciais, o chamado sequestro de dados;
* Interromper processos produtivos ou comerciais, paralisando negócios e arranhando a reputação de empresas;
* Alterar ou destruir alguma informação de processos e de bancos de dados;
* Roubar dados do perfil, dos hábitos de consumo ou do histórico de saúde de pessoas;
* Objetivos políticos;
* Protesto;
* Gerar caos;

## 2.3 Tecnologia utilizada

A tecnologia utilizada para o desenvolvimento da aplicação foi o Symfony, uma estrutura PHP líder para criar sites e aplicativos da web. Construído sobre os componentes do Symfony, um conjunto de componentes desacoplados e reutilizáveis ​​nos quais os melhores aplicativos PHP são construídos, como Drupal, Prestashop e Laravel.

A ideia por trás do Symfony: Não se tranque dentro do Symfony. Permite criar aplicações que atendam precisamente as necessidades. O Symfony respeita os “padrões de fato” existentes do PHP: PHPUnit, convenções de nomenclatura para classes, etc. necessariamente usando o framework em sua totalidade.

Além disso, o Symfony é tão interoperável que, na sua essência, ele próprio usa blocos de construção de software externos (ORM Doctrine, Swiftmailer, etc.).

Também utilizou-se ORM (Object Relational Mapper) é uma técnica de mapeamento objeto relacional que permite fazer uma relação dos objetos com os dados que os mesmos representam. Ele faz o mapeamento da sua classe para o banco de dados e cada ORM tem suas particularidades para gerar o SQL referente a inserção do objeto que corresponde a uma tabela no banco de dados e realizar a operação. Utilizando um ORM, também se ganha produtividade, pois deixa-se de escrever os comandos SQL para deixar que o próprio ORM.

### **2.3.1. Exploits**

G

# Conclusão

Com auxílio do Metasploit conseguiu-se fazer uma análise sobre o estado da segurança da startup tendo sido identificadas algumas vulnerabilidades que poderão causar posteriores problemas. Como já foi mencionado, garantir a segurança no ciberespaço é de sua importância pois evita a ocorrência de acidentes variados que resultam no vazamento de dados e informações e paralisação ou perda de rendimento das suas actividades. É de extrema importância que as vulnerabilidades encontradas possam ser ultrapassadas para garantir a protecção da empresa contra ameaças maliciosas e possíveis violações de segurança eu possam gerar grandes impactos na organização e também, co mais segurança para operar no mercado, será possível estabelecer parcerias comerciais ainda mais saudáveis com os mercados para atingir os objectivos estratégicos da startup.

# Referências bibliográficas

CISCO. **What is CyberSecurity.** 2022. Acessado a 13/06/2022. Disponível em: <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>

BRANCO, Dácio. **O que é exploit?** Acessado a 13/06/2022. Disponível em: https://canaltech.com.br/seguranca/o-que-e-exploit-203850/