

**QUALIDADE DE SOFTWARE**

Gabriel Amorim da Silva Decarli Roquim

Análise de Qualidade

São Paulo

2023

# Relatório de Testes Vulnerabilidade

Link: localhost:3000

|  |
| --- |
| **CT-**Criar um perfil administrador. |
| Para este cenário vamos usar a ferramenta burp.  Criar o login pelo browser. Vamos criar um login simples para acessar as requisições e respostas. |
| Ferramenta burp. Vamos abrir o browser pela ferramenta e ativar o intercept.  Interface gráfica do usuário, Aplicativo, Word  Descrição gerada automaticamente  Aqui vemos que o login foi realizado. Gerando token em nossa resposta.  Interface gráfica do usuário, Aplicativo  Descrição gerada automaticamente  Acessar a aba Repeater. Aqui alterei a linha 1; Mudei para API.  Interface gráfica do usuário, Texto, Aplicativo  Descrição gerada automaticamente  Voltei para aba PROXY e percebi que temos api/users. Nessa requisição temos “role”: “customer”  Interface gráfica do usuário, Aplicativo  Descrição gerada automaticamente  Então voltei para Repeater, alterei POST /api/users. Inserir “users”  Interface gráfica do usuário, Texto, Aplicativo, Email  Descrição gerada automaticamente  Cliquei em **send** para enviar nossa request e ter nossa reposta. Deu mensagem de erro, pois o email deve ser alterado, para ser um email único.  Interface gráfica do usuário, Texto, Aplicativo, Email  Descrição gerada automaticamente  Mandei novamente a requisição e deu “não autorizado” . Ainda não mudei email.  Interface gráfica do usuário, Texto, Aplicativo, Email  Descrição gerada automaticamente  Alterei o email. E conforme dito percebi que temos “**role**” na resposta. Que nada mais é o papel do usuário.  Interface gráfica do usuário, Texto, Aplicativo, Email  Descrição gerada automaticamente  Em nossa requisição vou inserir “role”: **admin**. Esse **admin** foi escolhido na sorte, por tentativa e erro.  Nossa reposta foi “Sucesso”. Então nosso usuário padrão virou **admin.**  Interface gráfica do usuário, Texto, Aplicativo, Email  Descrição gerada automaticamente  Voltamos para a página para mostrar o resultado  Interface gráfica do usuário, Aplicativo  Descrição gerada automaticamente |

|  |
| --- |
| CT- 5 Vamos acessar a política de privacidade. |
| Texto  Descrição gerada automaticamente  Interface gráfica do usuário, Aplicativo, Word  Descrição gerada automaticamente |

|  |
| --- |
| CT-1 Teste chatBoot cupom |
| URL: [OWASP Juice Shop (owasp-juice.shop)](http://demo.owasp-juice.shop/#/chatbot) |
| Esse teste de vulnerabilidade é para identificar se ao persistir com a mesma pergunta “ se tem cupom de desconto”, o ChatBoot nos daria esse cupom. Foram precisos três pedidos para que conceda. Na segunda tentativa o chat nos retornou algo que não é possível de ler “bug”. Na terceira tentativa o desconto veio.  Print – Pedindo cupom  Interface gráfica do usuário, Texto, Aplicativo  Descrição gerada automaticamente  Cupom recebido  Interface gráfica do usuário, Aplicativo  Descrição gerada automaticamente |

|  |
| --- |
| CT-2- Login |
| Ao efetuar um login pelo portal, com senha ou usuários inválidos, irá nos retornar 401    Ao realizar essa mesma manobra usando postman, nos retornou 200 |

|  |
| --- |
| CT-3 Acessando com senha ou email inválidos |
| Usando a ferramenta burp disponível nesse link <https://portswigger.net/burp/> |
| Para conseguirmos acessar o perfil, segui alguns passos mostrados em aula por Exemplo usar “ ´or 1=1 – “. Neste teste inserindo esse parâmetro consegui acessar o perfil admin desse usuário. Gerando um token inclusiveInterface gráfica do usuário, Texto, Aplicativo  Descrição gerada automaticamente |
|  |
| Ao acessar o devtools ele nos mostra um script SQL que podemos usar para realizar outro login caso desejássemos  Interface gráfica do usuário, Texto, Aplicativo, Email  Descrição gerada automaticamente  Interface gráfica do usuário, Texto  Descrição gerada automaticamente  Navegando pelo DevTools conseguimos encontrar o caminho (path) administrador  Interface gráfica do usuário, Texto, Aplicativo  Descrição gerada automaticamente |

|  |
| --- |
| CT-4 Registrando um usuário sem seguir a regra de segurança senha |
| Aqui na página de registro ele nos mostra algumas regras de senhas a serem criadas.    Para este cenário, acessamos o devtools e apagamos as regras de criação login  Interface gráfica do usuário  Descrição gerada automaticamente |

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente