

Manual do Usuário — AutoBounty

Plataforma de gestão de pentest, bug bounty e relatórios Versão 1.0 — Setembro de 2026
Acesso à plataforma: <https://autobounty.com.br>

Este manual não contém endereços IP nem credenciais. Sempre que for necessária uma senha, ela é fornecida fora do canal (pelo administrador ou no momento da instalação).

Sumário

1. Introdução
2. Fundamentos de teste de intrusão (pentest)
3. Fundamentos de bug bounty
4. Conceitos da plataforma
5. Primeiros passos (cadastro, login, MFA)
6. Painéis (dashboards)
7. Clientes e projetos
8. Escopos: definindo o alvo
9. Ferramentas disponíveis
10. Executando os testes no escopo
11. Relatórios
12. Assistente integrado
13. Administração
14. Segurança e boas práticas
15. Perguntas frequentes e solução de problemas
16. Glossário
17. Referências

1. Introdução

1.1. O que é a AutoBounty

A AutoBounty é uma plataforma web para **planejar, executar, acompanhar e relatar** testes de intrusão (pentest) e atividades de bug bounty em um lugar só. Com ela você:

- Cadastra **clientes** e **projetos** de teste;
- Define **escopos** (alvos autorizados: web, rede, mobile, API, cloud);
- Executa **scans** com ferramentas reconhecidas (Nmap, Nuclei, sqlmap, Nikto, entre outras) direto do navegador;
- Revisa e edita os **achados** (severidade, CVSS, CWE, evidências);
- Gera **relatórios profissionais** em HTML e PDF, em português ou inglês;
- Conta com um **assistente integrado** que explica ferramentas, glossário e fluxos de trabalho;
- Gerencia **operadores**, aprovação de cadastros, planos e MFA.

1.2. Para quem é

- **Administradores:** responsáveis pela plataforma, pela aprovação de acessos e pela visão geral de tudo.
- **Operadores:** profissionais que executam os testes nos escopos dos projetos sob sua responsabilidade.

1.3. Como usar este manual

- Se você é **novo em pentest/bug bounty**, leia as seções 2 e 3 primeiro.
- Se você já sabe a teoria e só quer **usar a plataforma**, comece pela seção 5 (primeiros passos) e siga até a seção 10 (executar testes).
- A seção 15 (FAQ) resolve os problemas mais comuns.

1.4. Acesso à plataforma

Abra o navegador em **<https://autobounty.com.br>**. A página inicial (landing) mostra o slogan **Find. Prove. Secure.** e os links para **Sobre, Termo de Uso e Política de Ética** e **Solicitar seu Acesso**. Usuários já logados são levados direto ao painel.

2. Fundamentos de teste de intrusão (pentest)

Esta seção dá a base teórica usada em todo o restante do manual.

2.1. O que é um pentest

Um **teste de intrusão** é uma simulação autorizada de ataque contra um sistema (site, rede, aplicativo mobile, API) com o objetivo de **descobrir vulnerabilidades antes que atacadores mal-intencionados** as exploitem. O resultado é um relatório com os achados, a severidade de cada um e recomendações de correção.

Diferenças importantes:

Conceito	O que é
Pentest	Simulação autorizada, com escopo fechado, relatório e prazo
Bug bounty	Programa contínuo em que a organização recompensa quem achar falhas dentro das regras
Varredura (scan)	Fase automatizada de levantamento; não substitui a análise manual
Vulnerabilidade	Fraqueza explorável (ex.: injeção SQL)
Achado (finding)	Um item registrado na plataforma, com severidade e evidência

2.2. Tipos de caixa

- **Caixa preta (black box):** o tester não conhece a infraestrutura — simula um atacante externo. É o modelo mais comum em bug bounty.
- **Caixa cinza (gray box):** conhece parcialmente (ex.: credenciais de usuário comum, estrutura geral).
- **Caixa branca (white box):** acesso total ao código e à infra — permite cobertura mais profunda em menos tempo.

2.3. Fases de um pentest

1. **Reconhecimento (recon):** coleta de informações do alvo — domínios, subdomínios, tecnologias, portas expostas, registros públicos. Ferramentas típicas: Nmap, WhatWeb, Sublist3r, Amass, The Harvester.
2. **Varredura (scanning):** identificação automatizada de vulnerabilidades — serviços desatualizados, diretórios expostos, configurações erradas, templates de exploits conhecidos. Ferramentas típicas: Nuclei, Nikto, Dirb/Gobuster, SSLscan, WPScan.
3. **Exploração:** confirmação prática de que a falha é real e qual o impacto — ex.: provar que a SQL Injection permite ler dados. Ferramentas típicas: sqlmap, XSSStrike, Metasploit, Hydra.
4. **Pós-exploração e escalção:** avaliar até onde o ataque leva (acesso a outros sistemas, privilégios) **dentro do escopo**.
5. **Relatório:** registrar cada achado com evidência, severidade (CVSS), classificação (CWE/CVE), impacto e recomendação — é o entregável que a plataforma gera para você (seção 11).

Na AutoBounty, as fases 1-3 são apoiadas pelas ferramentas de scan (seção 10); a exploração manual e o relatório completam o trabalho.

2.4. OWASP Top 10 (visão geral)

O **OWASP Top 10** é a lista dos riscos mais críticos em aplicações web. Conhecer ajuda a interpretar achados:

1. **Broken Access Control** — usuário acessa dados/funções que não deveria.
2. **Cryptographic Failures** — dados sensíveis mal protegidos (senhas em texto claro, TLS fraco).
3. **Injection** — SQL Injection, XSS, comandos injetados em entradas não sanitizadas.
4. **Insecure Design** — falhas de arquitetura (sem limite de tentativas, lógica de negócio explorável).
5. **Security Misconfiguration** — padrões inseguros, diretórios expostos, debug ligado em produção.
6. **Vulnerable and Outdated Components** — bibliotecas/serviços com CVEs conhecidos.
7. **Identification and Authentication Failures** — MFA fraco, sessões previsíveis, força bruta sem trava.
8. **Software and Data Integrity Failures** — updates sem verificação, dependências comprometidas.
9. **Security Logging and Monitoring Failures** — nada é registrado, incidentes passam despercebidos.
10. **Server-Side Request Forgery (SSRF)** — servidor induzido a requisitar endereços internos.

2.5. Severidade: CVSS, CWE e CVE

- **CVE (Common Vulnerabilities and Exposures):** identificador único público de uma vulnerabilidade conhecida (ex.: CVE-2021-44228).

- **CWE (Common Weakness Enumeration)**: classificação da **fraqueza** (ex.: CWE-89 = SQL Injection, CWE-79 = XSS, CWE-326 = criptografia fraca). A AutoBounty usa CWE nos achados e nos relatórios.
- **CVSS (Common Vulnerability Scoring System)**: escore de **0 a 10** com vetor (ex.: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). Quanto maior, mais grave.

Escala de severidade usada na plataforma:

Severidade	Faixa CVSS (referência)	Significado prático
Crítico	9,0 - 10,0	Exploração remota total, dados massivos expostos
Alto	7,0 - 8,9	Impacto sério com condições simples
Médio	4,0 - 6,9	Exploração com alguma limitação
Baixo	0,1 - 3,9	Impacto reduzido
Informativo	0,0	Contexto/interesse técnico, sem impacto direto

Interprete sempre o **contexto**: um “médio” em sistema crítico pode valer mais que um “alto” em ambiente de testes.

3. Fundamentos de bug bounty

3.1. O que é um programa de bug bounty

Um **programa de bug bounty** é uma iniciativa contínua em que uma organização convida pesquisadores a encontrar vulnerabilidades em seus sistemas, **dentro de regras públicas**, em troca de reconhecimento e recompensa financeira. Diferente do pentest (projeto fechado com prazo), o programa roda o ano inteiro e qualquer pesquisador elegível pode participar.

3.2. Escopo do programa

Cada programa publica um **escopo** dizendo:

- **In scope**: domínios, URLs, apps e tipos de falha aceitos;
- **Out of scope**: tudo que não será aceito (ex.: subdomínios de terceiros, redes internas, phishing, DoS);
- **Regras específicas**: quais classes de vulnerabilidade contam, se é permitido fuzzing agressivo, quais ferramentas são proibidas, etc.

Regra de ouro: se não está no escopo, não teste. Testar alvos fora do escopo — mesmo que a falha seja real — é violação das regras e pode ter consequências legais.

3.3. Autorização e regras de engenharia

- A autorização **vem do próprio programa** (ou de um contrato de pentest assinado com o cliente). Sem ela, qualquer teste é crime (no Brasil, tipificado na Lei 12.737/2012 — “Lei Carolina Dieckmann”).
- **Safe harbor** (porto seguro): a maioria dos programas se compromete a não processar pesquisadores que agiram de boa-fé e dentro das regras.
- **Proibido sempre**: causar indisponibilidade (DoS), exfiltrar dados reais de usuários, modificar dados, usar phishing, pivôtar para sistemas de terceiros, vender a falha a terceiros.
- Respeite **limite de impacto**: prove a falha com o menor dano possível (ex.: mostrar que consegue ler **um** registro, não baixar a base toda).

3.4. Classificação e recompensa

A severidade (seção 2.5) costuma definir a recompensa. Programas usam escalas próprias (“Critical/High/Medium/Low”) e podem pagar por **bônus** (primeiro a reportar, falha em componente crítico, qualidade do relatório). Um bom relatório inclui:

1. Título objetivo e resumo do impacto;
2. Passos de reprodução (pré-requisitos, requisições, capturas);
3. Evidência (sem dados reais de terceiros);
4. Severidade sugerida com justificativa (vetor CVSS);
5. Recomendação de correção.

3.5. Divulgação responsável (disclosure)

- **Divulgação coordenada**: você reporta ao programa e espera a correção antes de publicar — é o padrão e o que os programas preferem.
- **Divulgação pública**: só quando há acordo (ou após prazo do programa de divulgação). Nunca publique antes disso.
- **Regra básica**: nunca divulgue dados de usuários expostos; demonstre o risco com dados sintéticos.

3.6. Ética, responsabilidade e legalidade

- Teste **apenas alvos autorizados** — a AutoBounty exige o aceite do Termo de Uso e Política de Ética no cadastro justamente por isso.
- Guarde as evidências com cuidado; trate tudo como confidencial.
- Se descobrir uma falha que expõe dados de pessoas reais, priorize o canal seguro de reporte e a remediação.
- O uso da plataforma para testar alvos não autorizados **viola os termos e acarreta banimento** (e responsabilização civil/criminal).

4. Conceitos da plataforma

4.1. Objetos principais

Objeto	O que é	Onde fica
Cliente	Organização/pessoa para quem o teste é feito	Menu Clientes
Projeto	Um engajamento de pentest/bug bounty de um cliente, com status e datas	Menu Projetos
Escopo	Um alvo autorizado dentro de um projeto (URL, domínio, IP, rede) com tipo, dificuldade e portas	Dentro do projeto
Ferramenta	Software de scan disponível no servidor (Nmap, Nuclei...)	Menu Ferramentas
Tarefa de scan	Uma execução de ferramenta contra um escopo, com status, saída bruta e achados	Resultados dos Scans
Achado	Um resultado relevante registrado num scan (título, severidade, CVSS, CWE, evidência)	Detalhe do scan
Relatório	Documento do projeto em HTML/PDF com resumo executivo, achados e conclusões	Botão Relatório

4.2. Papéis de acesso

Papel	O que pode fazer
Administrador	Tudo: dashboards globais, operadores, aprovação de cadastros, planos, resets de senha/MFA, todos os clientes/projetos/relatórios
Operador	Seus clientes, seus projetos e seus scans; cria escopos, executa scans, edita achados e gera relatórios

O administrador vê os projetos de **todos** os operadores; o operador vê apenas os que são de sua responsabilidade.

4.3. Planos de acesso

O cadastro público pede um plano, e o administrador aprova:

Plano	Duração
Mensal	30 dias a partir da aprovação

Plano	Duração
Anual	365 dias
Vitalício	Não expira
Sem plano	Acesso ainda não liberado/avulso

Plano **expirado** impede o login até que o administrador renove.

4.4. Status e severidades

- **Status do projeto:** Planejamento → Ativo → Em Varredura → Concluído (ou Cancelado). Durante a execução de scans ele muda para **Em Varredura** e volta sozinho ao status anterior.
- **Status da tarefa de scan:** Pendente → Em Execução → Concluído / Falhou (ou Cancelado).
- **Severidade dos achados:** Crítico, Alto, Médio, Baixo, Informativo (cores mantidas em toda a plataforma e nos relatórios).

5. Primeiros passos

5.1. Solicitar cadastro

1. Em <https://autobounty.com.br>, clique em **Solicitar seu Acesso** (ou acesse /accounts/signup/).
2. Preencha usuário, e-mail, telefone, **senha** (siga as regras exibidas) e escolha o **plano** desejado.
3. Leia o **Termo de Uso e Política de Ética** (link na página) e marque o aceite — o botão só é liberado depois disso. O aceite é registrado com data e versão do termo (auditoria).
4. Envie. A conta é criada **inativa** e uma solicitação de acesso entra na fila do administrador. Você verá a mensagem **“Cadastro solicitado! Aguarde a aprovação...”**.

Enquanto a solicitação estiver pendente, o login não é liberado.

5.2. Aprovação pelo administrador

O administrador abre **Solicitações de Acesso** no menu superior, revisa cada pedido (usuário, e-mail, plano, termo aceite) e clica em **Aprovar** (com ajuste do plano, se necessário) ou **Rejeitar** (com motivo). Na aprovação a conta é ativada e o plano começa a contar a partir daquele dia.

5.3. Login

1. Acesse <https://autobounty.com.br/accounts/login/> (ou o botão **Entrar** da landing).
2. Informe **usuário** e **senha**.
3. Se o MFA já estiver ativo, informe o **código de 6 dígitos** do app autenticador. O login só termina depois do MFA.
4. Se a senha tiver sido redefinida pelo administrador, a tela **Troca de senha obrigatória** aparece antes de qualquer coisa — escolha uma nova senha para seguir.

Entrar com GitHub: se o administrador tiver configurado o OAuth, o botão **Entrar com GitHub** usa sua conta do GitHub no lugar da senha (o MFA continua valendo). E-mail desconhecido na plataforma gera uma nova solicitação de acesso, como no cadastro comum.

5.4. MFA obrigatório (primeiro login)

A plataforma exige **MFA por TOTP** de todos os usuários:

1. Logo após a senha, a tela **Ative o MFA** mostra um **QR code**.
2. Use um aplicativo autenticador (Google Authenticator, Authy, Microsoft Authenticator, 1Password...), escaneie o QR e informe o código de 6 dígitos para confirmar.
3. Na sequência, a tela **Códigos de Recuperação** mostra **8 códigos**. **Salve-os em local seguro** (imprima, gerenciador de senhas): cada um serve uma única vez quando você não tiver o celular por perto.

Observações:

- As tentativas erradas de código são limitadas por sessão; ao exceder, a sessão MFA é reiniciada e você precisa logar de novo.
- **Perdeu o celular?** Use um código de recuperação ou peça ao administrador para **resetar o MFA** (seção 13.3).

5.5. Idioma

No canto superior direito, o seletor **globe / idioma** alterna **(BR) Português** e **(US) English** na hora (o relatório também tem as duas versões). O padrão é o português.

6. Painéis (dashboards)

Após o login você cai no painel adequado ao seu papel.

6.1. Dashboard administrativo (/dashboard/admin/)

- **KPIs**: operadores (total/ativos), clientes, projetos, escopos e scans;
- **Gráfico de visão geral** com a distribuição de recursos e o estado dos scans (concluídos, em execução, pendentes, falhos);
- **Solicitações de acesso** pendentes com aprovação rápida;
- **Histórico** de decisões de cadastro e **seção de planos** de todos os usuários (editar plano, expirar agora);
- **Listas**: projetos recentes, clientes recentes, últimos 10 scans;
- **Atalhos**: novo operador, novo cliente, novo projeto, ferramentas;
- **Cards de notícias e CVEs** (feeds atualizados sob demanda).

6.2. Dashboard do operador (/dashboard/operator/)

- **KPIs** dos seus recursos: clientes, projetos, escopos, scans e **total de achados**;
- **Gráfico** de visão geral dos seus recursos;
- Seus **projetos recentes** (com contagem de escopos) e seus **últimos scans** com link para o detalhe;
- Atalhos para criar cliente/projeto e abrir as ferramentas.

6.3. Feeds de notícias e CVEs

Os cards mostram manchetes de notícias de segurança e vulnerabilidades recentes (CVE com escore CVSS), buscados de fontes públicas (RSS/NVD). Eles são atualizados pelo painel (/dashboard/feeds/) sem recarregar a página. São apenas informativos — não substituem o acompanhamento das fontes oficiais.

6.4. Monitoramento de ataques (card e mapa)

Os dashboards incluem o card **Monitoramento de Ataques**, que mostra o que está batendo contra o próprio servidor em tempo quase real:

- **Totais dos últimos 7 dias** por categoria: banimentos de SSH (força bruta), varreduras web, bloqueios de firewall (UFW) e tentativas de login inválidas na própria plataforma;
- **Lista dos eventos recentes** com IP, país, tipo e contagem;
- **Mapa animado** com a origem geográfica dos ataques e o marcador do servidor; os arcos destacam os eventos mais recentes.

Como funciona: um coletor roda a cada minuto (collect_threats, via timer do systemd), lê o log do fail2ban, o journal do UFW e os access logs do Apache, registra os IPs (com geolocalização em cache) e o card se atualiza sozinho a cada 30 segundos. Os logins inválidos da própria plataforma entram em tempo real, direto na tela de login.

Interpretação típica: brute force SSH de botnets (banido pelo fail2ban), port scans de varredores automáticos (bloqueados pelo UFW) e scanners web caçando /.env, wp-admin, backups etc. Nada disso deve chegar ao aplicativo — o card serve para **conferir que as barreiras estão funcionando**.

7. Clientes e projetos

7.1. Cadastrar um cliente

1. Menu **Clientes** → **Novo Cliente** (/projects/clients/create/).
2. Preencha **Nome**, **Empresa**, **E-mail** (obrigatório), **Telefone**, **Pessoa de contato** e o **Responsável** (usuário da plataforma que cuidará do cliente).
3. Salve. O operador responsável enxerga o cliente na sua lista; o administrador vê todos.

7.2. Criar um projeto

1. Menu **Projetos** → **Novo Projeto** (/projects/create/).
2. Campos: - **Nome do Projeto** e **Descrição**; - **Cliente** (obrigatório — se não existir, o formulário oferece o link para cadastrá-lo); - **Operador responsável** (quem executará os testes); - **Status**: Planejamento, Ativo, Em Varredura, Concluído ou Cancelado (comece por **Planejamento** ou **Ativo**); - **Data de início** e **Data de término** (opcionais).
3. Salve. Você vai para a lista de projetos e pode abrir o detalhe.

7.3. Detalhe, edição e exclusão

Na lista de projetos, use **Ver** (abre o detalhe), **Editar** e, no ícone de lixeira, **Remover** (com tela de confirmação). O detalhe do projeto mostra:

- Cabeçalho com status, cliente, operador e datas;
- Cartões com **escopos** e **últimos scans**;
- Botões **Novo escopo**, **Resultados dos Scans** e **Relatório**.

8. Escopos: definindo o alvo

O **escopo** é o coração do teste: é ele que diz **o que pode ser testado**. Cuidado ao defini-lo — é a linha entre um teste legítimo e um teste não autorizado.

8.1. Criar um escopo

No detalhe do projeto → **Novo escopo** (/projects/<id>/scopes/create/):

Campo	O que é	Exemplo de valor
Nome do Escopo	Identificação amigável	Site institucional
Alvo (URL/IP/Domínio)	O alvo exato a ser testado	https://exemplo.com.br
Tipo de Escopo	Aplicação Web, Rede, Aplicação Mobile, API ou Cloud	Aplicação Web
Nível de Dificuldade	Fácil, Médio, Difícil, Especialista	Médio
Portas	Para scans de rede: 80, 443, 8080 ou vazio (padrão)	443, 8443
Notas Adicionais	Restrições, credenciais de teste, avisos	Ambiente de homologação

8.2. Regras para um bom escopo

- **Só alvos autorizados:** em bug bounty, copie literalmente o escopo do programa; em pentest contratado, use o alvo do contrato/escritório de trabalho. Nunca inclua “de curiosidade” um domínio que não é do cliente.
- **Um escopo por alvo lógico:** separe app web, API e admin em escopos distintos — isso organiza os scans e o relatório final.
- **Delimite subdomínios:** decida se api.exemplo.com.br está dentro; deixe registrado nas **Notas**.
- **Portas com moderação:** listar todas as portas deixa o Nmap lento; informe as relevantes.
- **Restrições operacionais:** registre janelas de manutenção, alvos que não podem receber fuzzing agressivo etc.

8.3. Editar e remover

No card do escopo, use **Editar** ou **Remover** (confirmação obrigatória). Scans já executados permanecem no histórico do projeto.

9. Ferramentas disponíveis

Menu **Ferramentas** (/projects/tools/) lista o catálogo do servidor, com filtro por categoria:

Categoria	Ferramentas	Para quê
Reconhecimento	Nmap, Sublist3r, Amass, The Harvester, WhatWeb, HTTPX	Portas/serviços, subdomínios, e-mails públicos, tecnologias
Varredura Web	Nikto, Nuclei, WPScan, SSLscan	Configurações erradas, CVEs conhecidas, WordPress, TLS
Exploração	sqlmap, XSSStrike, Metasploit, Hydra	Confirmar SQLi, XSS, exploits, força bruta (autorizada)
Fuzzing	Dirb, Gobuster, Wfuzz, FFuf	Diretórios, arquivos e parâmetros ocultos
Pós-Exploração	Buster	Enumeração adicional após acesso inicial

Notas importantes:

- O instalador da plataforma já instala as ferramentas essenciais (Nmap, Nikto, sqlmap, Dirb, Gobuster, WhatWeb, SSLscan, Hydra e **Nuclei**). Ferramentas não instaladas **ainda aparecem no catálogo**: ao executar, a saída bruta explica o que falta e como instalar.
- O catálogo é gerido pelo administrador (comando `seed_tools` na instalação/atualização).
- Ferramentas pesadas (Metasploit, Amass) exigem mais recursos — execute com paciência e dentro do escopo.

10. Executando os testes no escopo

Esta é a seção central do manual: o fluxo completo de um teste na plataforma.

10.1. Visão geral do fluxo

Cliente → Projeto → Escopo → Selecionar ferramentas → Executar pendentes
→ Resultados → Detalhe do scan → Editar achados → Relatório

10.2. Passo 1 — Abrir o seletor de ferramentas

No **detalhe do projeto**, no card do escopo desejado, clique em **Executar Scan** (`/projects/<projeto>/scan/<escopo>/`). A tela lista as ferramentas ativas com checkbox, agrupadas por categoria.

- Marque **as ferramentas adequadas ao tipo de escopo** (veja a tabela da seção 9 e a recomendação da 10.8), ou
- Marque **Executar todas** para criar tarefas com todas as ferramentas ativas.

Clique em **Executar**. As tarefas são criadas com status **Pendente** e você é levado a **Resultados dos Scans**.

10.3. Passo 2 — Executar as tarefas pendentes

Em **Resultados dos Scans** (`/projects/<id>/scan/results/`):

1. Confira o filtro de status e as estatísticas no topo (total de achados e contador por severidade);
2. Clique em **Executar Pendentes** (somente esse botão inicia execução);
3. Um aviso confirma que os scans começaram **em segundo plano** — a página pode ser fechada; o servidor continua trabalhando;
4. **Para cada ferramenta que entra em execução, um mini-terminal abre na própria linha da tabela**, mostrando a saída dos logs **em tempo real** (atualizada a cada ~2 segundos), com o comando no topo e a barra de status girando; ao terminar, status, badges e totais são atualizados na hora.

Detalhes de comportamento:

- O botão **Executar Pendentes** mostra **Executando...** e ignora cliques repetidos; a primeira submissão sempre é enviada ao servidor;
- As janelas de terminal podem ser abertas/fechadas a qualquer momento pelo botão **Ver log** (ícone de terminal) na coluna **Ações** — também para scanners já concluídos, que mostram a saída final gravada; as janelas que você deixou abertas são restauradas após uma atualização da página;
- O projeto fica **Em Varredura** durante a execução e **volta ao status anterior** ao terminar;
- Duplo clique não duplica tarefas (elas são “reservadas” ao iniciar);
- Uma ferramenta que falhar **não derruba as demais**;
- Cada ferramenta tem tempo limite próprio (1–5 minutos); scan que estourar o limite é marcado como falho com a saída do timeout.

10.4. Passo 3 — Acompanhar e inspecionar resultados

Na lista de scans, cada linha mostra ferramenta, escopo, status, hora e badges de severidade. O botão **Ver log** (ícone de terminal) reabre o mini-terminal daquela ferramenta com a saída completa. Clique em **Ver** para o **detalhe do scan**:

- **Comando executado** (ex.: `nmap -sV -sC <alvo> -p 443`) — bom para auditar o que a plataforma rodou;
- **Saída bruta** completa da ferramenta;
- **Tabela de achados**: título, badge de severidade, **CVSS**, **CWE** e evidência;
- Botão **Editar** (✎) em cada achado.

O que cada ferramenta costuma entregar:

Ferramenta	Achados típicos
Nmap	Portas/serviços abertos (informativo); serviços inseguros (médio); assinatura de vulnerabilidade (alto)
Nikto	Itens de configuração insegura, XSS refletido, divulgação de informação (médio/alto)
Nuclei	Achados ricos: nome, descrição, CVSS + vetor , CWE , CVE , referências e comando de prova — a fonte mais completa
sqlmap	Parâmetros injetáveis (CWE-89 , crítico)

Ferramenta	Achados típicos
Dirb/Gobuster	Conteúdo oculto encontrado — diretórios admin, backup, .env (médio); arquivos com segredos (alto)
SSLscan	Protocolos SSL/TLS obsoletos (CWE-326), cifrões fracos (CWE-327), sem certificado
WhatWeb	Tecnologias identificadas (informativo); versões antigas notáveis (médio)
Sublist3r	Subdomínios descobertos (informativo)
Hydra	Placeholder — brute force exige configuração manual (veja 10.7)

Os parsers são heurísticos. Todo achado automático precisa de **validação humana** antes do relatório: confira a saída bruta, confirme a falha de forma não destrutiva e edite o achado se necessário.

10.5. Passo 4 — Editar um achado

Na tela do scan, clique em  **Editar** (.../findings/<n>/edit/). Você pode corrigir:

- **Título** — objetivo e específico;
- **Severidade** — Crítico/Alto/Médio/Baixo/Informativo (com a régua da seção 2.5);
- **Detalhe** — o que foi encontrado, impacto e contexto;
- **CVSS (score e vetor)** — ex.: 7,5 + CVSS:3.1/AV:N/AC:L/...;
- **CWE** — aceita 89 e normaliza para CWE-89;
- **Confiança** — quão certo o scanner está (ajude quem lê).

Ao salvar, o **resumo de severidade** é recalculado e já aparece nos badges, nos gráficos e no relatório. Boas práticas:

- Remova/rebaixe falsos positivos (ex.: porta interpretada como vulnerabilidade);
- Suba a severidade quando a evidência mostrar impacto real maior;
- Sempre que possível, deixe a **evidência** objetiva (trecho da resposta, requisição reproduzível).

10.6. Passo 5 — Revisar tudo antes do relatório

1. Filtre por **Crítico/Alto** e confirme cada um;
2. Padronize títulos (padrão: “ **em** ”);
3. Garanta que todo achado tem CWE ou CVSS preenchido;
4. Rode as ferramentas complementares para os escopos que ficaram vagos (ex.: SSLscan se só houve Nmap).

10.7. Exploração manual (quando a plataforma não faz)

Alguns testes são **manuais por natureza**. A plataforma não executa automaticamente:

- **Força bruta (Hydra)**: monte o comando você mesmo com wordlist e credenciais de teste autorizadas — ex.: `hydra -l usuario -P /caminho/wordlist.txt ssh://alvo;`

- **Exploração com Metasploit** e pós-exploração: use no servidor dentro do escopo e registre o resultado como achado manual no relatório;
- **Testes lógicos** (IDOR, quebra de autorização, fluxo de pagamento): sempre manuais — descreva passo a passo no relatório.

10.8. Combos recomendados por tipo de escopo

Tipo	Combo sugerido
Aplicação Web	Nuclei + Nikto + Dirb/Gobuster + WhatWeb (+ sqlmap se houver parâmetros)
Rede	Nmap (+ SSLscan se houver TLS)
API	Nuclei + WhatWeb (+ sqlmap nas endpoints com parâmetro)
Cloud	Nmap + Nuclei (revise achados manualmente)
Mobile	WhatWeb no backend da API + Nuclei; o APK em si é análise manual

10.9. Ciclo de vida dos achados e reteste

Cada achado **nasce como um registro próprio** (o objeto **Finding**), derivado da saída do scan mas com estado que a ferramenta não tem: status, responsável, histórico e datas. O fluxo completo é:

Aberto → Em Correção → Corrigido → Reteste → Fechado

Transição	Quando usar
Iniciar Correção	alguém assumiu o achado
Marcar como Corrigido	o cliente/time confirmou a correção
Solicitar Reteste	pedir a validação (carimba a data do pedido)
Reteste Aprovado	o reteste não reproduziu → fecha com evidência
Reteste Reprovado	ainda reproduz → volta para Aberto
Fechar / Reabrir	descarte (falso positivo) ou retorno do achado

Como usar:

1. No projeto, clique em **Achados** — a lista traz filtros por status e severidade, ordenada do mais grave para o mais leve;
2. Abra o achado para ver descrição, evidência, request/response, passos de reprodução, **histórico completo** (quem mudou o quê e quando) e definir o **responsável**;
3. Use os botões do **Ciclo de Vida** com uma nota opcional (ex.: “não reproduzido após o patch de 12/10”).

Regras importantes:

- As transições são validadas no servidor: não dá para pular etapas (ex.: direto de Aberto para Reteste);
- Se um achado **corrigido reaparecer num novo scan**, ele volta para Aberto automaticamente, com o evento **Reapareceu em Novo Scan**;
- Achados duplicados (mesmo título/endpoint no mesmo escopo) são **deduplicados** entre execuções — o registro é atualizado, não copiado;
- A edição técnica (seção 10.5) atualiza o registro sem duplicar, e o relatório continua lendo a mesma fonte de dados.

11. Relatórios

11.1. Visualizar e exportar

- No detalhe do projeto ou na tela de resultados, clique em **Relatório** (/reports/<projeto>/).
- Na página do relatório, use **PDF em Português** e **PDF em Inglês** (/reports/<projeto>/pdf/?lang=pt e ?lang=en) para baixar o documento pronto para o cliente.

11.2. Seções do relatório

1. **Informações do Projeto** — cliente, operador, status, datas;
2. **Resumo** — totais por severidade e cartões de estatística;
3. **Escopo do Teste** — alvos, tipos, dificuldade e quantidade de scans por escopo;
4. **Resumo Executivo** — texto para a liderança: nível de risco geral, achados por severidade, destaques e recomendações prioritárias;
5. **Achados Detalhados** — cada achado com evidência, CVSS, CWE, referências e recomendação;
6. **Conclusão e Recomendações por Ativo** — um veredito por escopo (aprovado/com ressalvas/crítico) com o que corrigir primeiro;
7. **Metodologia** — fases aplicadas e ferramentas utilizadas;
8. **Isenção de Responsabilidade** — limites e uso do documento.

Refaça a revisão de achados (seção 10.6) **antes** de gerar o PDF: o relatório usa exatamente os dados registrados na plataforma.

12. Assistente integrado

Em todas as telas logadas há um **painel de chat** (canto inferior direito). Ele funciona **sem internet** com uma base local:

- **“Como usar o Nuclei?”** — explica a ferramenta e dá exemplos de uso;
- **“O que é CWE-89?”** — respostas do glossário de segurança;
- **“Quero fazer um pentest web”** — sugere o fluxo de trabalho passo a passo;
- **“Me dê sugestões”** — dicas contextuais para o projeto/escopo atual;
- **“Lembre-se: ...”** — guarda observações na memória do assistente (visível no botão de memória; item apagável individualmente);
- +/- em respostas corrige a base; **Limpar conversa** zera o histórico.

O administrador pode, opcionalmente, liberar conversa livre com um LLM configurando `AI_PROVIDER=openai`, `AI_API_KEY` (e `AI_API_BASE` para outros provedores compatíveis) no ambiente do servidor. Sem isso, o assistente responde apenas da base local.

O assistente é educacional: **não substitui** sua validação técnica nem as regras de escopo.

13. Administração

Tudo abaixo exige perfil **administrador**.

13.1. Operadores

Menu **Operadores** (`/accounts/operators/`):

- **Novo operador** — usuário, e-mail, senha provisória, papel;
- **Editar** — dados e status (ativo/inativo);
- **Remover** — com confirmação;
- Coluna **MFA** mostra quem já ativou.

13.2. Reset de senha pelo administrador

Na lista de operadores ou no dashboard, o botão **Redefinir senha** (`/accounts/users/<pk>/password-reset/`):

1. O admin **digita uma nova senha** provisória;
2. As **sessões ativas do usuário são revogadas** na hora;
3. No próximo login, a **troca é obrigatória** antes de usar a plataforma;
4. O admin também pode alterar a própria senha em `/accounts/password-change/`.

13.3. MFA e recuperação

- **Resetar MFA** (`/accounts/users/<pk>/mfa-reset/`): apaga o segredo — o usuário será obrigado a configurar o MFA de novo no login;
- **Reset de hardware** (`/accounts/users/<pk>/hardware-reset/`): limpa os códigos de recuperação antigos; novos são gerados no fluxo do usuário;
- O próprio usuário pode regenerar códigos em `/accounts/mfa/codes/` após o login.

13.4. Solicitações de acesso

Solicitações de Acesso (`/accounts/signup-requests/`): fila com usuário, e-mail, plano, status do termo e data. **Aprovar** ativa a conta com o plano escolhido; **Rejeitar** descarta com registro de quem decidiu e quando (auditoria completa).

13.5. Planos de acesso

No dashboard administrativo, na seção de usuários:

- **Editar plano** — Mensal/Anual/Vitalício/Sem plano, com revalidação da data de expiração a partir de hoje;
- **Expirar agora** — bloqueia o acesso imediatamente (útil para auditorias e cancelamentos);
- Plano expirado → o login é barrado com aviso até a renovação.

13.6. Administração avançada (Django)

/admin/ abre o painel nativo do Django (login pelo **mesmo fluxo de senha + MFA**). Serve para manutenção fina: usuários, ferramentas, tarefas de scan e migrações. Prefira as telas da plataforma no dia a dia.

13.7. Publicação de novos idiomas

As traduções do painel ficam em `translations/en.json` e são compiladas com `python scripts/il18n_tool.py build`. O seletor de idioma só mostra o que estiver publicado.

14. Segurança e boas práticas

- **MFA sempre ligado** — nunca compartilhe o segredo nem os códigos de recuperação; guarde-os em cofre/gerenciador de senhas.
- **Senhas fortes e únicas** — a plataforma exige complexidade e o admin força a troca quando redefini.
- **HTTPS obrigatório** — o endereço usa TLS com HSTS; se o navegador reclamar, não ignore o aviso.
- **Princípio do menor privilégio** — crie operadores só para quem precisa e desative contas inativas.
- **Escopo autorizado** — revise sempre o alvo antes de executar qualquer ferramenta; registre restrições nas Notas do escopo.
- **Evidências sensíveis** — trate saídas de scan e relatórios como informação confidencial do cliente.
- **Backup** — o administrador do servidor faz cópias periódicas do banco (ver `README.md` do projeto); combine uma rotina de restore testada.
- **Auditoria** — decisões de cadastro, resets e trocas de senha ficam registradas; revise periodicamente.

15. Perguntas frequentes e solução de problemas

Não consigo logar / “aguardando aprovação”.

Sua solicitação ainda está pendente. Aguarde o administrador aprovar em **Solicitações de Acesso**.

Meu plano expirou.

O login é barrado com aviso. Peça ao administrador para renovar o plano (seção 13.5).

Esqueci a senha.

A plataforma não envia e-mail de redefinição: o **administrador redefine** pelo botão de redefinição e você é obrigado a escolher nova senha no login (seção 13.2).

Perdi o celular com o MFA.

Use um **código de recuperação** (seção 5.4) ou peça o **reset de MFA** ao administrador (seção 13.3).

O scan não inicia.

Só tarefas **Pendentes** executam — use o botão **Executar Pendentes** na tela de resultados. Se estiverem **Em Execução**, a página atualiza sozinha.

Scan falhou / “ferramenta não está instalada”.

Abra o detalhe do scan e leia a saída bruta: ela diz qual pacote falta e o comando de instalação. Peça ao administrador do servidor para instalar e reexecute a tarefa.

Os achados parecem errados ou repetidos.

São heurísticas — filtre, valide na saída bruta e **edite os achados** (seção 10.5). Remova falsos positivos antes do relatório.

Não vejo os projetos de outro operador.

Comportamento esperado: operador vê os próprios; administrador vê todos.

O PDF saiu sem achados.

Não há achados registrados ou os scans ainda rodam — conclua a execução e a revisão antes de gerar.

Quero a plataforma em inglês.

Use o seletor de idioma (globe) no topo; o relatório também tem versão EN.

Posso testar qualquer alvo?

Não. Só alvos autorizados — dentro do escopo do programa/contrato (seções 3.2 e 8.2). Fora disso é infração e crime.

16. Glossário

Termo	Significado
Achado (finding)	Vulnerabilidade/observação registrada com evidência
Bug bounty	Programa contínuo de recompensas por falhas dentro de regras
CVSS	Escore 0–10 de gravidade de uma vulnerabilidade
CWE	Classificação da fraqueza (ex.: CWE-89 = SQL Injection)
CVE	Identificador público de vulnerabilidade conhecida
Escopo	Conjunto de alvos autorizados para o teste
Fuzzing	Envio massivo de entradas para achar falhas
MFA/2FA	Segunda etapa de login (aqui: TOTP de 6 dígitos)
OWASP	Organização que publica padrões de segurança web
Pentest	Teste de intrusão autorizado e contratado

Termo	Significado
Recon	Fase de coleta de informações do alvo
Scan	Execução automatizada de ferramenta contra o alvo
TOTP	Algoritmo de código temporário (30 s) usado no MFA
XSS / SQLi	Cross-Site Scripting / SQL Injection
Safe harbor	Compromisso do programa de não processar boa-fé
Resumo executivo	Seção do relatório para a liderança

17. Referências

- **OWASP Top 10** — <https://owasp.org/www-project-top-ten/>
- **OWASP Testing Guide** — <https://owasp.org/www-project-web-security-testing-guide/>
- **NIST SP 800-115** — Technical Guide to Information Security Testing
- **CVSS (FIRST)** — <https://www.first.org/cvss/>
- **CWE (MITRE)** — <https://cwe.mitre.org/>
- **CVE (MITRE)** — <https://cve.mitre.org/>
- **Termo de Uso da AutoBounty** — <https://autobounty.com.br/accounts/termos/>
- **README de operação do projeto** — README.md na raiz do pacote (instalação, backup, atualização).

Fim do manual — AutoBounty © 2026. Documento sem IP nem credenciais.