

<bug_bounty> .start()



LUCAS GATES

ISBN: 978-65-00-94469-3

COPYRIGHT © 2024

Seus Primeiros Passos em Bug Bounty

Bem-vindo ao Mundo da Cybersecurity

Opa! Tranquilo futuro bug hunter?

Bem-vindo a este emocionante mundo da segurança cibernética, onde cada dia traz novos desafios e a oportunidade de fazer uma diferença real. Eu me lembro de quando comecei minha jornada, cheio de curiosidade e com muitas perguntas. E é exatamente assim que eu quero que você se sinta: empolgado e pronto para explorar.

Os programas de bug bounty são mais do que apenas uma maneira de ganhar recompensas; eles são uma porta de entrada para aprimorar suas habilidades e contribuir para um ambiente digital mais seguro. Fazer o mundo mais seguro é uma ótima causa... mas a verdade é que fazemos isso porque invadir sistemas é MUITO emocionante! E melhor ainda quando não corremos risco de ser preso!

Este guia é o seu companheiro nessa jornada. Eu compartilharei com você não apenas as ferramentas e técnicas que você precisará, mas também as lições que aprendi ao longo do caminho. Vamos lá que eu quero te mostrar os caminhos secretos dos programas de bug bounty e transformar sua paixão pela segurança cibernética em uma aventura recompensadora.

Preparado? Vamos começar!

Como Funcionam os Programas de Bug Bounty?

Pense em um programa de bug bounty como um convite aberto para uma festa de hackers cibernéticos, onde você é o convidado de honra. Uma empresa basicamente diz: "Aqui estão nossos tesouros digitais. Se você encontrar algum buraco em nossa armadura, vamos te agradecer — e sim, pode até ter uma recompensa!" É uma corrida emocionante contra outros hackers afiados, todos procurando criar um nome para si.

O Papel dos Programas de Bug Bounty na Cybersecurity

Agora, imagine um mundo onde cada um de nós contribui um pouquinho para a segurança na internet. É isso que os programas de bug bounty fazem. Eles nos unem, formando um escudo gigante contra os vilões cibernéticos, garantindo que nossas informações e a de todos estejam seguras. Cada bug que você encontra e relata é como um pedacinho desse escudo se fortalecendo.

Benefícios dos Programas de Bug Bounty

Para as Empresas:

1. **Olhos por toda parte:** Imagine ter um exército de guardiões protegendo seu forte. É isso que as empresas ganham — acesso a mentes brilhantes como a sua, ajudando a manter suas defesas impenetráveis.
2. **Economia Inteligente:** Prevenir é melhor (e mais barato) que remediar. Investir em bug bounties é como comprar um excelente seguro por um preço incrível.
3. **Aprimoramento Constante:** Feedback é um presente, e as empresas recebem toneladas dele, ajudando-as a serem melhores a cada dia.

Para os Pesquisadores de Segurança como Você:

1. **Aprimore seu Arsenal:** Cada desafio é uma lição, tornando-o um mestre em sua arte.
2. **Reconhecimento e Recompensa:** Descobrir aquela falha crítica não só enche seu bolso, mas também eleva seu status na comunidade.
3. **Escolha sua Aventura:** A liberdade de escolher seus projetos significa que você pode seguir sua curiosidade aonde ela levar.

Como Começar em Bug Bounty

Chegar lá parece algo distante. Mas lembre-se, até a jornada mais épica começa com um simples passo. Arme-se com conhecimento, escolha sua arena (plataformas de bug bounty), e então, mergulhe fundo naquilo que faz seu coração bater mais forte. E nunca se esqueça: a prática não só leva à perfeição, ela é a própria jornada.

Escolha uma plataforma e cadastre a sua conta lá. Uma que eu tenho gostado muito, é o Intigriti (<https://www.intigriti.com>). Depois, escolha uma empresa para você testar.

Entendendo o Escopo

Antes de sair à caça, é crucial saber onde você está pisando. O escopo é o seu mapa do tesouro, mostrando onde buscar e onde não se aventurar. Respeitar o escopo é como seguir as regras de um jogo nobre; ele mantém a brincadeira divertida e justa para todos.

Dica de especialista: Reportar uma falha de segurança para uma empresa que não tem programa de bug bounty pode ser uma fria!

Submetendo seu Primeiro Relatório de Vulnerabilidade

Imagina que você acabou de desvendar um segredo cibernético, um bug que ninguém mais viu. Agora, é hora de contar ao mundo – ou melhor, à empresa responsável – sobre sua descoberta. Mas, como você faz isso de uma forma que eles realmente entendam e apreciem o seu trabalho árduo? Aqui está um guia para você brilhar ainda mais.

A Arte de Escrever um Bom Relatório

Pense no seu relatório de vulnerabilidade como uma história que você está contando. Você encontrou o vilão (o bug), entendeu seus movimentos (como ele funciona) e agora você precisa explicar aos mocinhos (a empresa) como capturá-lo.

1. **Resumo Executivo:** Aqui é onde você dá um vislumbre da aventura. Descreva a essência do bug e o impacto que ele pode ter. É como o trailer do seu filme de detetive favorito.
2. **Descrição Detalhada:** Este é o enredo da sua história. Como você encontrou o bug? Que caminhos você percorreu? Seja claro e detalhado para que até mesmo alguém que não estava na jornada com você possa seguir seus passos.
3. **Prova de Conceito (PoC):** Mostre as provas. Capturas de tela, logs, vídeos – são os artefatos que você coletou ao longo do caminho. Eles são a prova irrefutável de que você encontrou algo real.
4. **Impacto e Severidade:** Avalie o perigo. Quão sério é esse bug? É um vilão de nível chefe ou apenas um capanga? Ajude a empresa a entender a urgência do problema.
5. **Sugestões de Remediação:** Se você já tem em mente um plano para capturar o vilão, compartilhe suas ideias. Não é obrigatório, mas mostra que você não só encontrou o problema, como também pensou em uma solução.

Mantendo a Comunicação

Depois de enviar seu relatório, é hora de esperar. Mas mantenha suas linhas de comunicação abertas. Se a empresa precisar de mais informações ou tiver perguntas, esteja pronto para ajudar. É assim que você constrói um relacionamento de respeito e confiança.

Continuando nesse ritmo, vamos mergulhar nas ferramentas que todo caçador de bugs deve ter em seu arsenal. Cada ferramenta que você aprender a usar aumenta suas habilidades e abre novas possibilidades em sua jornada de bug bounty. Vamos explorar algumas das mais cruciais, começando com o Amass.

Ferramenta 1 - Amass

Imagine ter um mapa que não apenas mostra o terreno, mas também revela segredos escondidos. É isso que o Amass faz. Ele vasculha a internet, encontrando pedaços esquecidos do domínio que você está investigando, revelando novas áreas para você explorar.

Por Que o Amass é Importante?

A identificação de subdomínios e ativos é um passo crítico na fase inicial de qualquer teste de penetração ou programa de bug bounty. Ao descobrir o tamanho da superfície de ataque de uma organização, o Amass permite que os bug hunters identifiquem pontos potencialmente vulneráveis que poderiam ser negligenciados.

Utilizando o Amass para Enumeração de Subdomínios

Após instalar o Amass, você pode começar a explorar os ativos de um domínio. Um exemplo comum de uso é a enumeração de subdomínios, que pode ser feita através do seguinte comando no terminal:

```
amass enum -active -d tritoninfosec.com
```

Neste exemplo, -d especifica o domínio que você deseja investigar. O Amass então realizará uma pesquisa abrangente, utilizando várias fontes para descobrir subdomínios associados a tritoninfosec.com.

Veja o exemplo abaixo:

```
lucas@GLaDOS:~$ amass enum -d tritoninfosec.com
tritoninfosec.com
treinamento.tritoninfosec.com
www.tritoninfosec.com
beta.tritoninfosec.com
docs.tritoninfosec.com

OWASP Amass v3.19.2                               https://github.com/OWASP/Amass
-----
5 names discovered - dns: 1, api: 3, scrape: 1
-----
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
172.67.0.0/16          5 Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
lucas@GLaDOS:~$
```

No print acima você pode ver os subdomínios encontrados pelo Amass. Com dominios adicionais, você tem mais possibilidades de achar falhas de segurança.

Ferramenta 2 - Nuclei

Agora, com um mapa em mãos, você precisa de uma ferramenta para achar as falhas. O Nuclei é uma ferramenta ótima para newbies e experts. Ele permite que você examine rapidamente cada ponto no seu mapa em busca de vulnerabilidades conhecidas. Com o nuclei conseguimos automatizar a nossa procura de forma bem rápida. Claro, ela não vai achar tudo. Mas pode achar coisas que passariam despercebidas.

Dominando o Nuclei

1. **Configuração:** Familiarize-se com o Nuclei e seus templates. O nuclei atualiza os templates constantemente. Sabe aquela falha de segurança que saiu recentemente? Pode ser que um novo template consiga identificar ela. Então mantenha o nuclei sempre atualizado.
2. **Criação e Uso de Templates:** Aprenda a criar novos templates baseado em falhas que você for encontrando. Os seus novos templates podem te dar uma grande vantagem sobre os outros bug hunters.
3. **Execução e Análise:** Depois que o Nuclei achou uma falha interessante, dedique tempo para entender tudo sobre a falha de segurança. Com esse conhecimento, você vai entender o impacto da falha. Nem todas as falhas são muito úteis. Mas entendendo como que ela funciona vai aumentar as suas chances de conseguir explorar a falha.

Realizando Scans com o Nuclei

Com o Nuclei instalado, você pode começar a executar scans utilizando templates prontos. Por exemplo, para verificar a presença de vulnerabilidades comuns em um alvo específico, você pode usar o seguinte comando:

nuclei -u http://example.com

Neste comando, -u especifica a URL do alvo. Se você quiser testar mais de um site por vez, você pode criar um arquivo com todos os sites. Nesse caso, o comando seria:

nuclei -l sites.txt

No exemplo acima, o arquivo sites.txt contém uma URL por linha. Abaixo temos o exemplo do resultado do nuclei:

```
lucas@GLaDOS:~$ nuclei -u https://demo.owasp-juice.shop/
____/ /_(_)
 /_ \ / / _\ / \ / v2.9.15
/_/ \_,_\_/_/\_/_/ projectdiscovery.io

[WRN] Found 118 templates with syntax error (use -validate flag for further examination)
[INF] Current nuclei version: v2.9.15 (outdated)
[INF] Current nuclei-templates version: v9.7.5 (latest)
[INF] New templates added in latest release: 106
[INF] Templates loaded for current scan: 7429
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1274 (Reduced 1208 Requests)
[mx-fingerprint] [dns] [info] demo.owasp-juice.shop [5 smtpin.rzone.de.]
[caa-fingerprint] [dns] [info] demo.owasp-juice.shop
[INF] Using Interactsh Server: oast.me
[http-missing-security-headers:permissions-policy] [http] [info] https://demo.owasp-juice.shop/
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://demo.owas
[http-missing-security-headers:clear-site-data] [http] [info] https://demo.owasp-juice.shop/
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://demo.owasp-jui
[http-missing-security-headers:strict-transport-security] [http] [info] https://demo.owasp-juice.
[http-missing-security-headers:content-security-policy] [http] [info] https://demo.owasp-juice.sh
[http-missing-security-headers:referrer-policy] [http] [info] https://demo.owasp-juice.shop/
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://demo.owasp-juice
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://demo.owasp-jui
[prometheus-metrics] [http] [medium] https://demo.owasp-juice.shop/metrics
```

No exemplo acima, vemos várias coisas a nível [info]. Essas informações podem ser úteis, mas não são consideradas falhas de segurança. Pois são coisas informativas. O último item da lista é nível [medium] (risco médio). Falhas de risco médio pode trazer informações úteis, porém geralmente não é crítico o suficiente para ser algo que possa ser explorado sozinho. Muitas vezes, falhas de risco médio são úteis quando são usadas em conjunto com outra falha mais séria.

Este site, <https://demo.owasp-juice.shop>, é uma loja fictícia propositalmente cheio de vulnerabilidades. O objetivo dela é ajudar as pessoas a aprenderem a achar falhas de segurança. Perceba que o nuclei só achou uma falha, mesmo que o site tem dezenas de falhas. Isso é porque o nuclei procura falhas já conhecidas. Ele não é capaz de identificar uma falha nova em um produto novo. Mesmo assim, é uma ferramenta muito útil para te ajudar a encontrar problemas.

A próxima ferramenta, Burp Suite é capaz de encontrar falhas desconhecidas em qualquer plataforma web. Como você já adivinhou, ela é uma ferramenta MUITO mais complexa. Você realmente precisa saber hackear para aproveitar essa ferramenta.

Ferramenta 3 - Burp Suite: O Canivete Suíço do Bug Hunter

Agora, vamos falar da Burp Suite. Se o Nuclei é o seu detector de vulnerabilidades, a Burp Suite é o seu laboratório móvel de hacking. Com um leque de ferramentas que vão desde a interceptação de tráfego até testes automatizados, a Burp Suite é essencial para qualquer um que queira se aprofundar nas entranhas da segurança web.

Por Que a Burp Suite é Essencial?

Ela transforma o tráfego de dados em algo palpável, permitindo que você veja, manipule e, se necessário, altere as comunicações entre o navegador e o servidor. É a ferramenta perfeita para desvendar os mistérios de qualquer aplicativo web. Diferente do Amass e Nuclei, ela não é um simples comando que te retorna resultados. É uma ferramenta para quem realmente sabe hackear. Mas mesmo assim, vale falar um pouco mais dessa ferramenta.

Quer saber usar essa ferramenta como um profissional? No final desse e-book te mostro como.

Primeiros Passos com a Burp Suite

- 1. Abrindo o Navegador:** Na aba Proxy → Intercept, você vai encontrar o botão para abrir o Navegador (“Open Browser”). Esse navegador está conectado ao Burp Suite. Toda navegação que você fizer nela, vai passar pelo Burp Suite. Dessa forma, você pode inspecionar e modificar tudo que passa pelo navegador antes da requisição chegar no site.
- 2. Explorando a Interface:** A Burp Suite é como uma caixa de ferramentas repleta de instrumentos poderosos. Familiarize-se com cada um deles e descubra como podem ajudá-lo em sua jornada. As partes mais importantes para você entender é o Proxy, Repeater, Intruder, Target e o Scanner.
- 3. Interceptação e Análise de Tráfego:** Praticar a arte de interceptar e analisar o tráfego é fundamental. Cada solicitação, cada resposta, pode conter a chave para uma vulnerabilidade não descoberta.

Identificando Vulnerabilidades com a Burp Suite

A Burp Suite é como um conjunto de lentes de aumento que te permite examinar os cantos mais obscuros das aplicações web em busca de falhas. Algumas das áreas que você pode explorar incluem:

- 1. Injeções SQL e XSS:** Use o Intruder ou o Scanner (versão paga) para testar entradas e identificar vulnerabilidades de SQL Injection ou Cross-Site Scripting.
- 2. Quebra de Autenticação:** Analise o gerenciamento de cookies e sessões para testar a robustez dos mecanismos de autenticação.
- 3. Configurações Inseguras:** Fique atento a cabeçalhos HTTP mal configurados ou políticas de segurança frouxas que podem deixar a aplicação vulnerável a ataques.

Dicas Práticas para o Uso da Burp Suite

- Automatize com Cautela:** A automação é uma grande vantagem, mas deve ser usada sabiamente para evitar sobrecarregar os sistemas alvo ou violar o escopo do programa.
- Mantenha-se Ético:** A Burp Suite é poderosa, mas deve ser usada de maneira responsável, respeitando sempre as regras e o escopo dos programas de bug bounty.

Maximizando Seus Ganhos como Caçador de Bugs

Você já se perguntou como transformar sua habilidade de encontrar bugs em uma verdadeira mina de ouro? A chave está em saber onde e como procurar. Aqui estão algumas estratégias para turbinar seus ganhos:

- 1. Escolha Programas Estrategicamente:** Alguns programas oferecem recompensas maiores e têm menos competidores. Pesquise e escolha programas que combinem com suas habilidades e interesses. É como escolher o caminho certo em uma encruzilhada, onde um pode levar a recompensas maiores.
- 2. Especialize-se:** Assim como um artesão se destaca em sua arte, desenvolver uma especialidade, seja em aplicações web, sistemas móveis ou IoT, pode te ajudar a identificar vulnerabilidades mais complexas e valiosas.
- 3. Use Ferramentas e Automação com Sabedoria:** Ferramentas como a Burp Suite, Amass e Nuclei são seus aliados nesta jornada. Aprenda a usá-las eficientemente para aumentar sua eficácia e eficiência.

Transformando Bug Hunting em Carreira

Além dos Bug Bounties: Uma Carreira em Cybersecurity

A participação em programas de bug bounty não é apenas uma maneira de ganhar dinheiro; se você é uma pessoa dedicada e curiosa, você pode transformar esse conhecimento em uma carreira em cybersecurity. Quando eu comecei a estudar infosec, bug bounties não existiam. Se existissem, eu poderia ter começado minha carreira muito mais cedo, pois é uma forma excelente de demonstrar que você realmente sabe.

É muito difícil entrar em cyber sem ter experiência. Como que você vai demonstrar experiência sem um emprego. Te apresento bug bounties. Ele é uma das melhores formas de você adquirir experiência sem ter emprego formal.

Construindo Sua Reputação

1. **Contribuições Consistentes:** A chave para construir uma reputação sólida é a consistência. Contribua regularmente para programas de bug bounty e se esforce para fornecer relatórios de alta qualidade.
2. **Interaja com a Comunidade:** Engaje-se com a comunidade de bug bounty através de fóruns, mídias sociais e conferências. Compartilhar conhecimento e experiências é uma maneira valiosa de construir sua rede.
3. **Aprenda e Evolua:** Mantenha-se atualizado com as últimas tendências e técnicas em cybersecurity. A capacidade de se adaptar e aprender é crucial em um campo que está sempre mudando.

Mantendo a Ética e a Legalidade

Lembre-se, com grandes poderes vêm grandes responsabilidades. Aqui estão algumas diretrizes éticas essenciais:

- **Respeite o Escopo:** Sempre adira estritamente ao escopo definido nos programas de bug bounty. Testar fora do escopo pode ter implicações legais e prejudicar sua reputação.
- **Reporte Responsavelmente:** Quando encontrar uma vulnerabilidade, reporte-a de maneira responsável e detalhada. Trabalhe com a organização para garantir que a falha seja corrigida antes de divulgar qualquer informação publicamente.
- **Integridade Profissional:** Mantenha altos padrões éticos em suas atividades. A integridade é fundamental para o sucesso a longo prazo na comunidade de bug bounty e no campo da segurança cibernética.

Bonus!

Ok, vamos falar sério por um instante. O motivo que eu e (provavelmente) você ficou interessado nesse assunto é porque queremos ser um hacker. É simples. A vontade de fazer algo extraordinário sem que ninguém possa nos impedir é simplesmente intoxicante. Eu pensava que ser um hacker “sem permissão” seria muito mais legal. Mas a realidade é que fazer algo sem permissão não faz bem para a saúde. Invadir sistemas com permissão do cliente é bem melhor porque você pode gabar do que você fez.

Se você quer transformar esse desejo em realidade, eu tenho um convite para te fazer. Comecei uma comunidade onde você tem acesso a material de primeira, em português, que vai te ajudar a ingressar nessa jornada. Como que eu sei que é de primeira? Porque eu tenho mais de duas décadas invadindo sistemas e sei como que as coisas funcionam. Além disso, trabalhei em empresas globais prestando esse tipo de serviço para as maiores empresas do mundo. (Bem melhor do que ser escravo da FBI).

Quer saber o que tem na comunidade? Vou te falar:

- Aulas em vídeo para você aprender a usar cada ferramenta usada em bug bounties.
- Laboratório que emulam sites reais para você aperfeiçoar as suas técnicas.
- Uma comunidade no Discord para você tirar dúvidas. Pra que ficar arrancando os cabelos? Você tem uma comunidade que ajudam uns aos outros a crescerem.
- Quer tirar uma dúvida em particular, me manda uma mensagem lá no Discord que vou ter o maior prazer em te responder!
- E mais! :)

Se interessou?

Visite: <https://bit.ly/bughunter2024>

