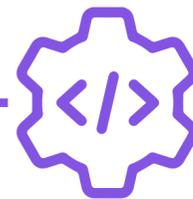


# OpenBullet

---

# OpenBullet

---



**O OpenBullet é um software legítimo de código aberto para testes de páginas na web, que permite realizar solicitações específicas de coleta de informações.** A ferramenta pode ser encontrada no GitHub e pode ser utilizada para diferentes tarefas, como raspagem e análise de dados, pentesting automatizado e testes de unidade usando Selenium – framework utilizado para testar aplicativos web.

Na sua própria página do GitHub, os criadores informam que o uso não autorizado para preenchimento de credenciais e outros tipos de ataque é ilegal e não se responsabilizam pelo uso indevido, porém o software ganhou notoriedade na comunidade de crimes cibernéticos devido sua natureza de código aberto, permitindo que se personalize os métodos usados pela ferramenta em cada ataque.

Também há outros fatores que atraem os cibercriminosos como à sua manutenção constante e o uso reduzido da unidade de processamento gráfico (GPU) no sistema de destino, tornando-se uma ferramenta muito silenciosa.

**Sendo assim, seu código permitiu que desenvolvedores criassem suas próprias versões do software, algumas calibradas para o crime cibernético.**



Devido à popularidade do OpenBullet, todo um mercado para scripts de configuração de negociação se formou no submundo, podendo ser encontrados facilmente online, já outras configurações mais confidenciais são vendidas em sites específicos e mercados fraudulentos.

**Nas imagens ao lado podemos ver algumas configurações para o software sendo vendidas:**



Cod3rMax 🇪🇸 @Cod3rMax · 28 de mai de 2020

Config PAYPAL [OpenBullet]]FullCapture

Starter : HOSEEN

- Api : Yes (IOS)

- Proxy: NO

- FullCapture

- Combo : E:P

Link : [file-upload.com/pua6ftmin2or](https://file-upload.com/pua6ftmin2or)

**Opções de trabalho**



Config: Produtos Globo De @k4k4r0to  
Pool de dados: Wordlist (API 171k)  
Modo proxy: Off  
Fontes de proxy:  
Resultados de hit: Banco de dados  
Pular: 100  
Bots: 10

**Estatísticas de dados**

Testado: 365  
Hits: 3  
Personalizado: 57  
Falhas: 305  
Inválido: 0  
Tentar novamente: 0  
Banido: 341  
Checar: 0  
Erros: 13

#### Produtos Globo

hit = Contas com serviços ativos

Custom = Bloqueada

Extrator de CPF ✓

Sem Proxies ✓

Sem Captcha ✓

Captura todos os produtos globo

Cartola

telecine

Premiere

Globo Play

Globo Play + Canais

Combate

etc

Disponível apenas para Openbullet 2

# Funcionamento

Os ataques de preenchimento de credenciais incluem as seguintes etapas principais:

1

**1.** Um invasor obtém credenciais vazadas (ou seja, um par de nome de usuário e senha) de ataques cibernéticos anteriores.

2

**2.** O invasor usa uma ferramenta de software – OpenBullet – para automatizar o teste de preenchimento dessas credenciais em vários sites e aplicativos móveis.

3

**3.** Se um conjunto de credenciais for autenticado com êxito, ele será sinalizado como uma conta válida.

4

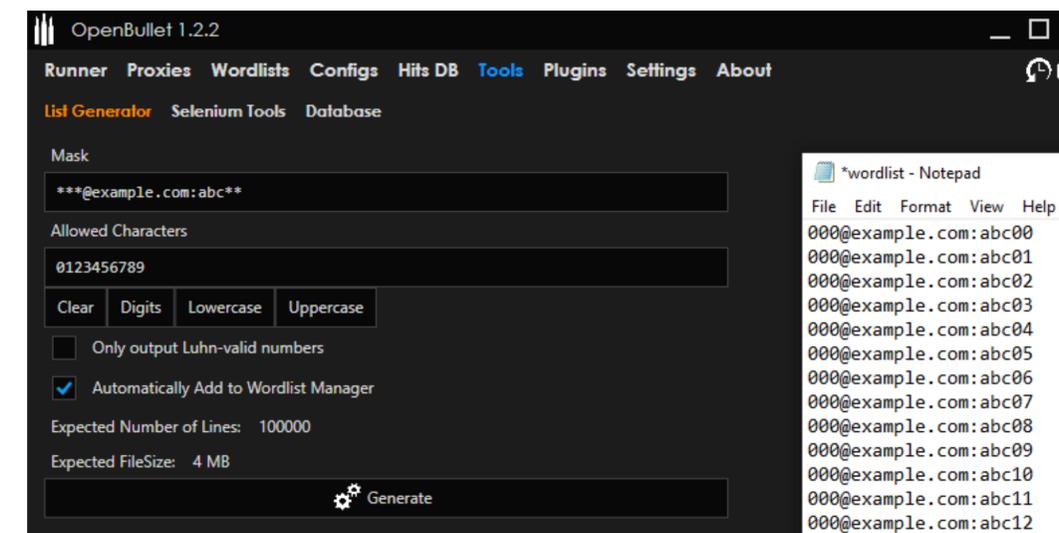
**4.** O invasor agora pode assumir a conta e extrair qualquer valor, incluindo informações de identificação pessoal, informações de cartão de crédito e valor armazenado (como pontos de fidelidade), bem como acessar e-mails, fazer compras fraudulentas e revender a conta.

# Alguns recursos do OpenBullet utilizados ilicitamente



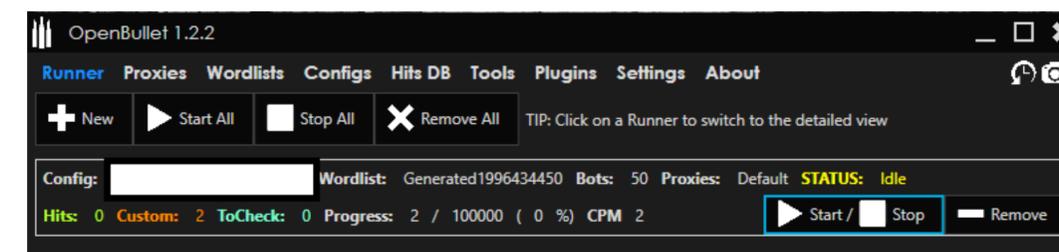
## 1. List Generator

Essa guia permite que o usuário importe milhares de palavras que podem ser usadas ao tentar se conectar a sites segmentados. Uma entrada pode ser tão simples como “endereço de e-mail: senha” ou “login:senha”.



## 2. Runner

Um usuário pode selecionar essa guia para iniciar um ataque de credencial usando o OpenBullet. A guia do corredor mostra o progresso e o número de acessos positivos para cada site que está sendo testado.





### 3. Proxies

Os proxies são uma parte importante do OpenBullet. Eles permitem aos usuários várias tentativas de login usando um endereço IP diferente para cada tentativa. Além disso, eles podem configurar o tempo entre cada tentativa de conexão, para que cada tentativa não gere nenhum alarme no site de destino para uma atividade de login incomum que normalmente seria gerada por um grande número de tentativas em um período muito curto.

Type	Host	Port	Username	Password	Country	Working	Ping	Chain	Last Checked
Socks4a	.1	8008				YES	2327	False	3/2/2021 3:44:44 PM
Socks4a	.137	9160				YES	2542	False	3/2/2021 4:18:21 PM
Socks4a	.042	8080				YES	1624	False	3/2/2021 4:15:51 PM
Socks5	.9.199	8080				YES	2183	False	3/2/2021 3:46:57 PM
Socks4		23				YES	2644	False	3/2/2021 4:06:06 PM
Socks4a	.5	2222				YES	1921	False	3/2/2021 4:23:38 PM
Socks4a	.186	9200				YES	7029	False	3/2/2021 4:15:08 PM
Socks5	.8.215	8080				YES	1553	False	3/2/2021 3:46:54 PM
Http	.77	5432				YES	1877	False	3/2/2021 3:30:26 PM
Socks4	.137	9000				YES	5361	False	3/2/2021 4:00:55 PM
Socks4	.254	8080				YES	1547	False	3/2/2021 3:37:43 PM
Socks4a	.59	9095				YES	1352	False	3/2/2021 4:22:14 PM
Socks4a	.241	9051				YES	5458	False	3/2/2021 4:14:09 PM
Socks4a	.8.130	9080				YES	1205	False	3/2/2021 4:14:48 PM
Socks5	.8.242	9080				YES	6165	False	3/2/2021 9:52:43 PM
Socks5	.241	9080				YES	2691	False	3/2/2021 9:55:31 PM
Socks5	.8.130	9070				YES	3591	False	3/2/2021 9:56:05 PM
Socks5	.8.130	9084				YES	2228	False	3/2/2021 9:56:09 PM
Socks5	.8.130	9090				YES	3198	False	3/2/2021 9:56:12 PM
Socks5	.8.130	9103				YES	3305	False	3/2/2021 9:56:14 PM
Socks5	.1.109	9051				YES	5508	False	3/2/2021 9:57:54 PM
Socks5	.4.193	9200				YES	2200	False	3/2/2021 9:58:15 PM
Socks5	.3.11	9999				YES	6566	False	3/2/2021 9:58:36 PM
Socks5	.0.123	8001				YES	1386	False	3/2/2021 9:59:38 PM

Progress: [Progress Bar] Bots: 1 [Slider]

Test On:  Success Key:

CHECK

Import Export Delete Delete All More Actions Del. Not Working Del. Duplicates Del. Untested

STATISTICS

Total: 35  
Tested: 35  
Working: 35  
Not Working: 0  
HTTP: 1  
SOCKS4: 3  
SOCKS4a: 8  
SOCKS5: 23  
Chain: 0

OPTIONS

Only Untested



### 4. Ferramentas, plug-ins e configurações

Os plug-ins podem ser facilmente importados para o OpenBullet para diferentes propósitos. As possibilidades são aparentemente infinitas, desde que a finalidade do usuário envolva enviar e coletar dados para um site direcionado. Na guia de configurações, os usuários do OpenBullet podem ajustar as configurações do sistema, como ignorar CAPTCHAs, por exemplo.

Runner Proxies Wordlists Configs Hits DB Tools Plugins Settings About

RuriLib OpenBullet

General Proxies Captchas Selenium

Captcha Service in use: TwoCaptcha

2Captcha API Key: TwoCaptcha

Bypass Balance C

Check Balance Your

Timeout for captcha res

- AntiCaptcha
- CustomTwoCaptcha
- DeathByCaptcha
- DeCaptcha
- ImageTyperz
- CapMonster
- AzCaptcha
- CaptchasIO
- RuCaptcha
- SolveCaptcha

# Maneiras de se proteger contra-ataques de preenchimento de credenciais

---

1

**Boas práticas na criação de senhas.** Os usuários devem evitar usar senhas fracas, enquanto as organizações devem implementar uma lista de bloqueio de senhas comumente usadas para impedir que os usuários as criem. Os usuários também devem evitar a reutilização de credenciais para várias contas e serviços online.

2

**Habilite a autenticação multifator – MFA em sites e serviços.**

3

**Crie um PIN ou responda a perguntas de segurança adicionais.** Alguns sites permitem que os usuários respondam a perguntas de segurança adicionais ou forneçam um PIN exclusivo para autenticação adicional.

4

**Habilite a análise de tentativas de login.** Alguns sites e serviços, como provedores de serviços de e-mail, executam análises de tentativas de login. Estes são baseados em diferentes fatores, incluindo:

- I. Informações do navegador. Uma tentativa de login com um navegador diferente, que nunca foi escolhido por um usuário, pode indicar uma tentativa de login fraudulenta.
- II. Endereço IP. Os usuários que alteram repentinamente o endereço IP e/ou o país de origem podem ser um bom indicador de tentativa fraudulenta.

