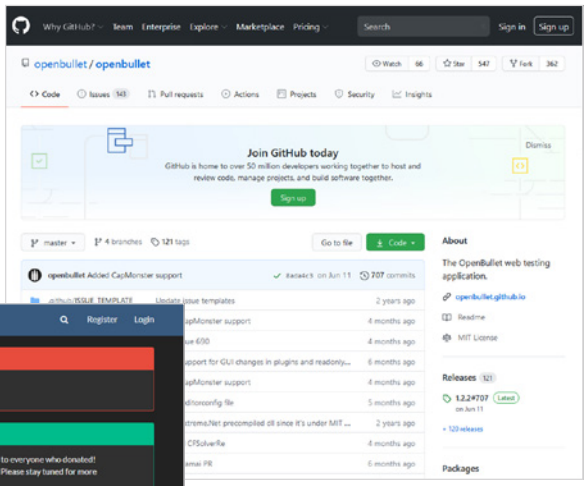
CEQUENCE SECURITY

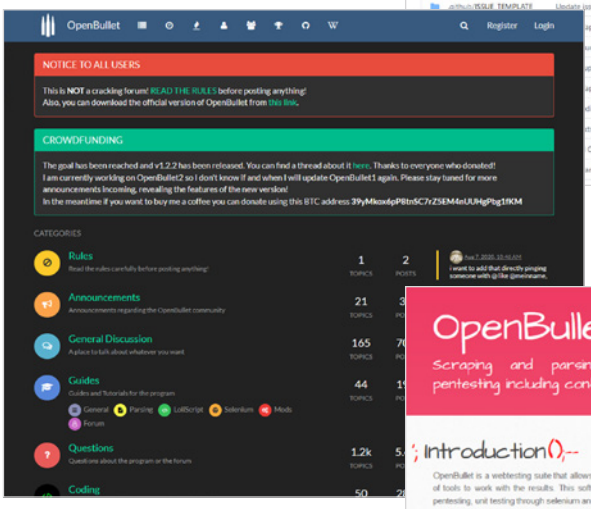
Using OpenBullet Configs to Improve Bot Prevention

Introduction

OpenBullet is an open sourced version of BlackBullet, a commercially available pen testing/hacking tool. Since its launch in March 2019, the popularity of OpenBullet has grown steadily, driven by online forums, how-to videos and publications in dedicated marketplaces. While the project (and all of the marketplaces) say that the tool should only be used for legal purposes, most every online retailer, bank, hospitality site or entertainment site has seen bot traffic originating from OpenBullet. This document provides some recommendations on how to proactively use OpenBullet resources to improve your defenses.

https://github.com/openbullet/openbullet

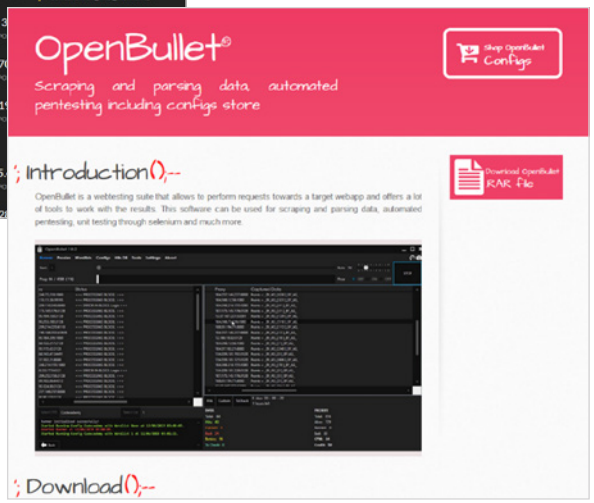




https://forum.openbullet.dev bullet

Finding Attack Configs for Your Site or Brand

Discovering attack configs for your site or brand is a significant step towards improving your defenses. Using variations of operators, keywords, and site/URL selections shown below; combining or separating them (in quotes or without quotes as well) will often times uncover existing configs. These techniques will commonly provide different results that are more valuable or relevant than common search techniques. Note that there is no right or wrong way to use advanced Google searching techniques.



https://openbullet.store/

Search Techniques

- Start with a Google search: YOURCOMPANY config or YOURCOMPANY openbullet
- Use the search operators intext: or allintext: to narrow down the results:
  - intext: YOURCOMPANY config or allintext: YOURCOMPANY openbullet
- Or search one of the hacking sites (below)
  - site:"www.TARGETSITE.WHATEVER" intext:"YOURCOMPANY"
  - intext:"YOURCOMPANY config" inurl: www.TARGETSITE.WHATEVER

Hacking Forums & Marketplace Sites to Research:

- Openbullet.store
- Openbullet.io
- Crackingpro.com
- Cracked.to
- Crackingking.com
- Sickaccountshop.com
- Nulled.to

Other Investigative Resources:

- Dark or Deep Web, Reddit, Telegram, Discord, Twitter, YouTube

You Found a Config – What's Next?

Going after the sites offering the configs is likely a fruitless effort, but there are things you can do to improve your defenses.

- Analyze the config using OpenBullet itself. The Config will give you an idea of which endpoints are being hit - web, mobile or even forgotten legacy APIs. Once you know this you can take steps to add security protections.
- The config will also provide insights into how they are bypassing current protection mechanisms. For example, which capctcha solvers they using, or how they are bypassing JavaScript bot detection measures.
- Always a great idea to share the config information with your peers and your in-place bot protect vendor

If you're currently using JavaScript-based bot mitigation, the OpenBullet configurations are able to evade them in three ways. First, OpenBullet includes bypass techniques for JavaScript. Second, bad actors can see the JavaScript on your site, analyze it and use OpenBullet customization to bypass detection. The third way in which bad actors will bypass your existing bot prevention tool is by using OpenBullet to target APIs directly rather than the web app itself.

How Cequence Security Can Help

As an alternative to JavaScript and SDK-based offerings, consider implementing a bot mitigation tool that is not JavaScript-based like Cequence Bot Defense which relies on CQAI, a patented ML-based analytics engine that accurately identifies bot activity by creating a Behavioral Fingerprint using over 150 customizable rules that encode common behavioral traits of automated attacks. Another recommendation is to reign in your API footprint using Cequence API Sentinel, which provides a complete API inventory (including shadow APIs), API risk assessment, and finds potential sensitive data leakage to help you prioritize areas for improvement which will make tools like OpenBullet less successful.

CEQUENCE® SECURITY

100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai