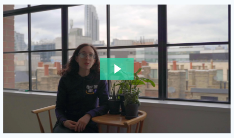
technolog

Faster Than Light

We run security tests on code 80x faster than any competitor

FASTERTHANLIGHT.DEV REDWOOD CITY



Developers want to write high quality, secure code. But no one wants to spend hours doing configuration and waiting for tests to run! We built this tool to make testing easier for developers. Then we realized that it solves an even bigger problem for people with large codebases (large enterprise companies.)

Elissa Shevinsky CEO @ Faster Than Light

ABOUT UPDATES0 GRAPEVINE5 ASK A QUESTION0 ADMIN

OVERVIEW
STORY
INVESTOR
Q&A

Why you may want to support us...

1. CTO cofounded and sold Vindicia for $115M. CEO helped launch Everyday Health (IPO) and Brave ($35M ICO).
2. Made $325K+ in revenue in our first year. Achieved product/market fit with FinTech startups. We built BugCatcher to automate that work.
3. Backed by Techstars London & AI Seed. 1200+ companies applied to Techstars London & only 10 were accepted.
4. Admitted to the Creative Destruction Lab, highly selective program in Toronto for Deep Tech startups worldwide.

Our Team

AND OUR MAJOR ACCOMPLISHMENTS

Elissa Shevinsky
CEO
Launched several successful startups since 1999 - Geekcorps (acquired), Everyday Health (IPO), Daily Steals, and Brave ($35M ICO.) Skills: Building developer communities, Shipping security products, Sales.

Brett Thomas
CTO
Protected 200M+ credit cards as CTO and Co-Founder at Vindicia. Sold Vindicia for $110M to AmDocs. Previously built eMusic (sold to Universal.)

Why people love us

Elissa's ability to bring a product/project to life is incredible. Time and time again, she has demonstrated that she has the competence, knowledge, and skills needed to connect the pieces and people necessary to accomplish her goals. I have worked with Elissa on several projects and she is great at keeping things on track and getting things delivered. She is well-networked and stays in touch with many influential tech contributors. She is an excellent product developer, promoter, and manager and I am completely confident in her ability to bring success to this project as its leader.

Reuven Etzion
Friend

Akul Penugonda Investor

I've found Elissa to be a brilliant, determined, supportive, forward thinking person with a very cool product. She is an extremely passionate founder who always had my back in our accelerator program. I watched as she navigated extremely difficult problems and made it out even stronger. Highly recommended.
Eli Stonberg Friend

See more on Buzz

Some of our investors

Eamonn Carey
Managing Director at Techstars London

In the news

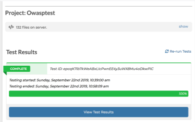
VentureBeat techstars

Downloads

BugCatcher Sample Code Report.pdf
WeFunder Slides Sept9.pdf

Our First Product: BugCatcher

Below is a screenshot from the web application. It's easy to run a test. Those tests are stored in your account, so it's easy to view past results.



Project: Owasptest

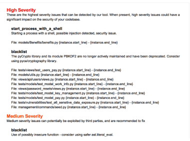
132 files on server.

Test Results

Test ID: epcqK7ib7kWeABxLIcPwnEE4y3uWX8Mu4oDkwPiC

Testing started: Sunday, September 22nd 2019, 10:39:00 am
Testing ended: Sunday, September 22nd 2019, 10:58:09 am

Completed tests can be downloaded on JSON or in a beautiful PDF report. The PDF report is useful for sharing with a manager or teammate. We would create reports similar to this as security consultants for cryptocurrency startups.



High Severity
These are the highest severity issues that can be detected by our tool. When present, high severity issues could have a significant impact on the security of your codebase.

start_process_with_a_shell
Starting a process with a shell, possible injection detected, security issue.

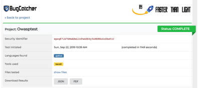
File: models/Benefits/benefits.py {instance.start_line} - {instance.end_line}

blacklist
The pyCrypto library and its module PBKDF2 are no longer actively maintained and have been deprecated. Consider using pyca/cryptography library.

File: tests/views/test_users_pay.py {instance.start_line} - {instance.end_line}
File: models/utils.py {instance.start_line} - {instance.end_line}
File: views/api/users/views.py {instance.start_line} - {instance.end_line}
File: tests/models/test_model_work_info.py {instance.start_line} - {instance.end_line}
File: views/password_resets/views.py {instance.start_line} - {instance.end_line}
File: tests/models/test_model_key_management.py {instance.start_line} - {instance.end_line}
File: tests/models/test_model_pay.py {instance.start_line} - {instance.end_line}
File: tests/vulnerabilities/test_a6_sensitive_data_exposure.py {instance.start_line} - {instance.end_line}
File: management/commands/seed.py {instance.start_line} - {instance.end_line}

Medium Severity
Medium severity issues can potentially be exploited by third parties, and are recommended to fix

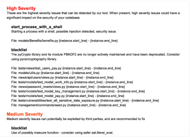
blacklist
Use of possibly insecure function - consider using safer ast.literal_eval.



Project: Owasptest

Security identifier	epcqK7ib7kWeABxLIcPwnEE4y3uWX8Mu4oDkwPiC
Test initiated	Sun, Sep 22, 2019 10:39 AM (completed in 1149 seconds)
Languages found	python
Tools used	bandit
Files tested	show files
Download Results	JSON PDF

BugCatcher reports are well organized, and easy to read. We show the highest priority bugs first, at the top. (Many tools show the bugs in the order that they were found, which is less helpful.)



High Severity
These are the highest severity issues that can be detected by our tool. When present, high severity issues could have a significant impact on the security of your codebase.

start_process_with_a_shell
Starting a process with a shell, possible injection detected, security issue.

File: models/Benefits/benefits.py {instance.start_line} - {instance.end_line}

blacklist
The pyCrypto library and its module PBKDF2 are no longer actively maintained and have been deprecated. Consider using pyca/cryptography library.

File: tests/views/test_users_pay.py {instance.start_line} - {instance.end_line}
File: models/utils.py {instance.start_line} - {instance.end_line}
File: views/api/users/views.py {instance.start_line} - {instance.end_line}
File: tests/models/test_model_work_info.py {instance.start_line} - {instance.end_line}
File: views/password_resets/views.py {instance.start_line} - {instance.end_line}
File: tests/models/test_model_key_management.py {instance.start_line} - {instance.end_line}
File: tests/models/test_model_pay.py {instance.start_line} - {instance.end_line}
File: tests/vulnerabilities/test_a6_sensitive_data_exposure.py {instance.start_line} - {instance.end_line}
File: management/commands/seed.py {instance.start_line} - {instance.end_line}

Medium Severity
Medium severity issues can potentially be exploited by third parties, and are recommended to fix

blacklist
Use of possibly insecure function - consider using safer ast.literal_eval.

What Makes BugCatcher special?

Whether you are an individual developer or a large enterprise, testing code is an annoying part of software development. A common complaint is that tests take too long to run.

It takes most companies with a large code base 8-10 hours or more to complete their security scans. Some companies solve this by just doing less scans, or not running these tests at all. This comes with some security risk. There were 3,813 data breaches reported in the first six months of 2019, according to a report by Risk Based Security. That report details how most of those hacks, impacting both large and small companies, happened because companies failed to implement basic security best practices. In one case, American Medical Collection Agency is filing for bankruptcy following an expensive data breach.

It's clear that security best practices, including testing code for possible security issues, matters. Most Fortune 1000 companies aren't willing to cut corners on information security, so they simply deal with the bottlenecks and expenses that come with following best practices.

BugCatcher solves this problem, by running these scans in half an hour or less.

How do we do it? Traditional software scanning tools (think of Veracode or Sonarqube, or open source tools like Pylint or PyTest) scan files one at a time. That's why the tests take so long to run. If there are 999 files, each of those files has to wait for its turn to be scanned. BugCatcher uses a revolutionary, innovative, proprietary process to scan multiple files at the same time. (We do this by running the scans inside Docker containers, inside AWS, for those interested in more technical details. For a technical deep dive, message Elissa @ fasterthanlight.dev to set up a chat with the CTO or member of the dev team.)

How much money can we make, as we bring this technology to market? The pricing page for Sonarqube's parent company, Sonarsource, is relevant here. It's common for enterprises to do pilot programs for $10k - $100k for testing software. It's also typical for the leading testing companies to do annual on-premise contracts (meaning that the enterprise companies are running the software on-site, rather than relying on AWS or Google to host the software) for over $500K. Pricing is based partly on the size of the code base.

For developers: BugCatcher is built on top of existing open source tools. It's free, and it's very fast to sign up. Just go to the BugCatcher website, click for Google authentication, and you're in! Developers can either use our beautiful web interface or our CLI tool.

The free tier of BugCatcher currently supports Python and Java. This tier is most useful for developers, open source projects and small businesses.

But How Good are Our Tests? Very good!

In truth, our tests are currently EXACTLY as good as the leading open source tests. That's because we built on top of open source tools like Bandit and Findbugs. Our results are exactly as good as the leading open source tools (which are widely regarded to be excellent.) These tools take a long time to set up. That's extremely frustrating for junior developers. Even senior developers can struggle with getting open source testing tools up and running, as there can be any number of reasons why set-up won't complete. (It could be that the project is undergoing maintenance, or that the tools require the latest versions of certain software packages etc.) BugCatcher eliminates the frustration and the time spent setting up and configuring these tools. And we offer this free of charge to the developer community. We hope that the community finds this useful!

But excellent test quality isn't good enough. One of the leading complaints about static analysis tests are that they have too much noise. This is similar to the experience of using Grammarly or Spellcheck. With Grammarly, the results are useful - but there's so much noise to sort through.

We believe that we have a unique insight, about how to make these tests more accurate. We're going back to our roots (see story below) and are focusing on FinTech companies. In the next year, we plan to collect data from volunteer customers about which security issues they consider to be highest priority. We're also going to gather data about which issues are the most frequent. We can use this data to produce more accurate results in the future, specifically for FinTech companies. That's just one slice of the market but it's a huge slice. The FinTech market is estimated to grow to USD 305.7 billion by 2023. Besides market size, it makes sense to start in FinTech because banks (and other companies handling funds) understand the importance of securing their code. The stakes are high, and so FinTech companies are prepared to spend the time and money on best practices.

Getting to Product/Market Fit in 2018: Securing FinTech Startups

We got our start doing security scans and reports for Cryptocurrency startups, under the name Soho Token Labs. We've spent the last year automating that work, and the result is the BugCatcher software. We also changed our name to "Faster Than Light." This better reflects our focus on efficiency and speed for developers and companies.

Our first customer was a month long "audit" for the 0x project. The 0x project is one of the most highly regarded companies in the Ethereum space. They blogged about our involvement (you can see one such post here.) This was followed by several months working with The Graph.

Most recently, we did an audit for Roll, whose tagline is "The New Standard for Social Money." Below is a testimonial from Bradley Miles, CEO at Roll:

We were interviewing several firms to audit our codebase and it became clear pretty quickly that Elissa and her team were the best choice for the job. The entire process from start to finish was extremely simple. If you're building secure applications that intend to serve a wide audience, I'd highly recommend reaching out to Elissa.

Investor Q&A

– COLLAPSE ALL

What does your company do?

BugCatcher is like spellcheck but for developers. Every Fortune 1000 company uses a tool like this to secure their code. These security tests are required for compliance and defending against hackers. We've solved the biggest complaint that companies have about these tools, which is "tests are too slow to run." Our tool is faster than anything else on the market, for companies with a large code base. We're using machine learning to make it the most accurate as well.

Where will your company be in 5 years?

We want to be the market leader for "Code Quality" tools. This is a huge market - we aim

We want to be the market leader for "Code Quality" tools. This is a huge market - we aim to hit $100M in annual revenue within five years. We have a clear path to revenue, based on scaling enterprise sales over the next five years. We'll start by selling a pilot into a friendly enterprise company (via our network) and leverage that for a case study and testimonials. That will help us to sell into five enterprises in 2021, which we can leverage to sell into twenty enterprises in 2022.

Why did you choose this idea?

Developers want to write high quality, secure code. But no one wants to spend hours doing configuration and waiting for tests to run! We built this tool to make testing easier for developers. Then we realized that it solves an even bigger problem for people with large codebases (large enterprise companies.)

Why is this a good idea, right now? What changed in the world? Why wasn't this done a few years ago?

Developers are more empowered than ever before, especially when it comes to choosing software. That creates an opportunity for us to help them ship higher quality code. We're leveraging the #DevSecOps movement, where developers become security evangelists inside their organizations.

We are also at a moment where large enterprises want to ship new code every day. There is a window of opportunity to help them, by reducing bottlenecks & improving code security.

On a more technical note - our application uses Docker containers to run multiple tests asynchronously and in parallel (rather than consecutively, which can take a long time.) This technology wasn't available ten years ago.

What is your proudest accomplishment?

Brett Thomas protected 200M credit cards at Vindicia without incident - and then he & his cofounder sold the company for $115M.

CEO Elissa Shevinsky was featured on the cover of the NY Times Sunday Business, named "Woman of the Decade" by Williams College, and was invited to teach Computer Science at Williams College (for "Winter Study" session.) Now she is keynoting one of the largest events in our space - DevSecCon in both London and Tel Aviv.

How far along are you? What's your biggest obstacle?

We've completed the MVP for individual developers, and are working on completing the SMB/enterprise versions.

We're focusing on shipping the MVP individual developers over the next few weeks. This version makes it fast and easy to test Python and Java code using open source tools. We also give the developer a beautiful report, which makes it easy to share results with colleagues and management.

We're working towards shipping the parallelization (speed) technology. Completing the "speed tech" is a rather complex problem (and a significant challenge.) Managing the various integrations and language-specific packages is extremely complex. The good news here is that we have a significant moat against competitors.

Who are your competitors? Who is the biggest threat?

The largest competitors are VeraCode, SonarQube, Rapid7, Codacy ShiftLeft and a few others. Our biggest threat is the length of enterprise sales cycles. It could take us a very long time to sell into big customers. We're focusing on individual developers and startups in the short term, which is the classic way to scale up to enterprise sales. We're also working on selling into relatively friendly enterprises, for examples via Techstars partnerships.

What do you understand that your competitors don't?

We understand the importance of community in the dev tools market. Most of the larger players stay away from open source, and don't have a significant presence in community events like Meetups or DevOpsDays.

We also see the potential for collaboration between developers and security engineers. We're working on tools to empower developers and security engineers to solve problems and fix bugs collaboratively.

How will you make money?

We plan to make money selling our software to SMBs (and eventually enterprise customers) via SaaS licenses. We'll start out by offering three pricing tiers: a free tier for individual developers, a pro tier for small businesses at a price point of $79.99/month, and a $550/month tier that includes significant support from our technical team.

The real monetization will come when we are able to support enterprise customers, who pay $90K - $1M+/year for this type of software and services.

What are the biggest risks? If you fail, what would be the reason? What has to go right for you to succeed?

The classic startup risks are team, product and market.

We've solved for team risk (we've all worked together before and can get things done.) We have an MVP for developers and are close to shipping our "speed tech" to businesses and pro users.

We still need to prove that we can make money selling our software. We plan to use some of the money from our upcoming seed raise to do sponsorships and content marketing at Meetups and PyCon events. We'd also like to hire a salesperson with experience selling dev tools, and a developer advocate with experience running security or testing workshops. I can do all of these things (hooray for founder selling) but we'll sell more faster by growing the team.

What do you need the most help with?

We could use beta testers (a great way to help if you're a developer) and introductions to customers. We're interested in talking to decision makers and developers at small to medium size tech companies, and doing informational interviews with potential enterprise customers.

We could also use support on social media and Github. We have a Twitter account, and are on Twitch. We could use likes, follows and retweets, to give those new channels some initial traction.

What would you do with the money you raise?

This campaign is part of a larger pre-seed raise. Funding will go towards:

1. Runway for the current team & operating expenses. Paying our bills FTW!

2. Hiring a developer advocate to write technical documentation and give educational workshops to drive adoption.

3. Hiring a part time or full time Python developer, to accelerate development of key features (expansion into additional languages, helpful integrations, etc.)

4. Paying back an interest-free loan. (We bought out our first investor. That's a long story but tldr they wanted us to focus on blockchain consulting and we had a different vision.) Happy to share more details - that was an important step in becoming a scalable software business.