EYEBALLER

AUTOMATING SECURITY TRIAGE WITH
MACHINE LEARNING

TABLE OF CONTENTS

INTRODUCING EYEBALLER

Sometimes pen testers can recognize the web pages most likely to contain an actionable lead simply by how those pages look. A blocky web app that looks old, an administration login page that could be brute-forced, or even just a web page that looks “interesting” are all prime targets for a hacker. But for larger perimeters, manually reviewing screenshots of every page to find the “interesting” is a laborious task that takes too long for a human to realistically complete. And unfortunately, traditional scanners don’t have the ability to determine which web pages need further inspection.

But, what if there were a different kind of tool that could be “trained” to programmatically identify and categorize those “interesting” pages, so that pen testers could instead focus their time on what they do best: finding vulnerabilities?

Enter **Eyeballer**, a valuable new hacker tool that helps pen testers close gaps in coverage and speed up their security assessments.

SECTION 01

SECURITY TRIAGE AUTOMATION VIA MACHINE LEARNING

SECURITY TRIAGE AUTOMATION VIA MACHINE LEARNING

Eyeballer is a first of its kind, AI-powered pen testing tool designed to assist penetration testers in assessing external perimeters. It identifies pages likely to contain vulnerabilities and pages that can be deprioritized during security assessments. Eyeballer "looks at" rendered web pages and programmatically determines which ones look most "interesting." Aimed at any screenshot repository, Eyeballer's AI automates the heavy lifting of visually inspecting web pages, allowing the testers to maximize their expertise by focusing on exposures and not triage.

WITH EYEBALLER, PENETRATION TESTERS CAN:

- Assess a repository of screenshots for indications of potential vulnerabilities
- Supplement automated scanning methods to close gaps in coverage
- Gauge targeted external perimeters, big or small
- Focus manual review efforts
- Improve testing times and accuracy

This e-book details what Eyeballer does (and doesn't) do, how it works, and the results it generates.

SECTION 02

CATEGORIZING WEB PAGES

EYEBALLER FOCUSES TESTING

EYEBALLER SOLVES GAPS IN COVERAGE

While Eyeballer is a hacking tool, it doesn't actually "hack" into anything. Its job is to take any screenshot repository, identify the websites that are mot likely to contain vulnerabilities, and present those results to a human expert for review. While tools like EyeWitness/Gowitness and Aquatone allow users to take screenshots of sites so that they can quickly identify interesting features, Eyeballer applies this approach at scale.

It's important to note that Eyeballer doesn't replace traditional web scanners, but instead helps focus the manual review of their output. Though HTML scanners work fairly well, they can't scan what they can't see. They cannot identify "old" looking web pages or "Soft 404" pages, where the page returns an error to the user but a 200 OK in the HTTP response.

WHAT EYEBALLER CATEGORIZES

Eyeballer can currently recognize four types of pages: Custom Error Pages, Login and Home Pages, and pages that look "old."

> "Most efforts to develop AI systems for computer security have been defensive in nature, (spam filters, antivirus, intrusion detection, etc...) but we're hackers. So, we wanted to make a machine learning system that could help us break into stuff. Eyeballer does that."
>
> **Dan Petro**
> Senior Security Associate

SOURCE: CUSTOM 404 ERROR PAGE RESPONDING WITH 200 OK

CUSTOM ERROR PAGES

Some custom pages present an error to users but return a 200-level (success) code. These are known as “Soft 404” pages and often have little or no content.

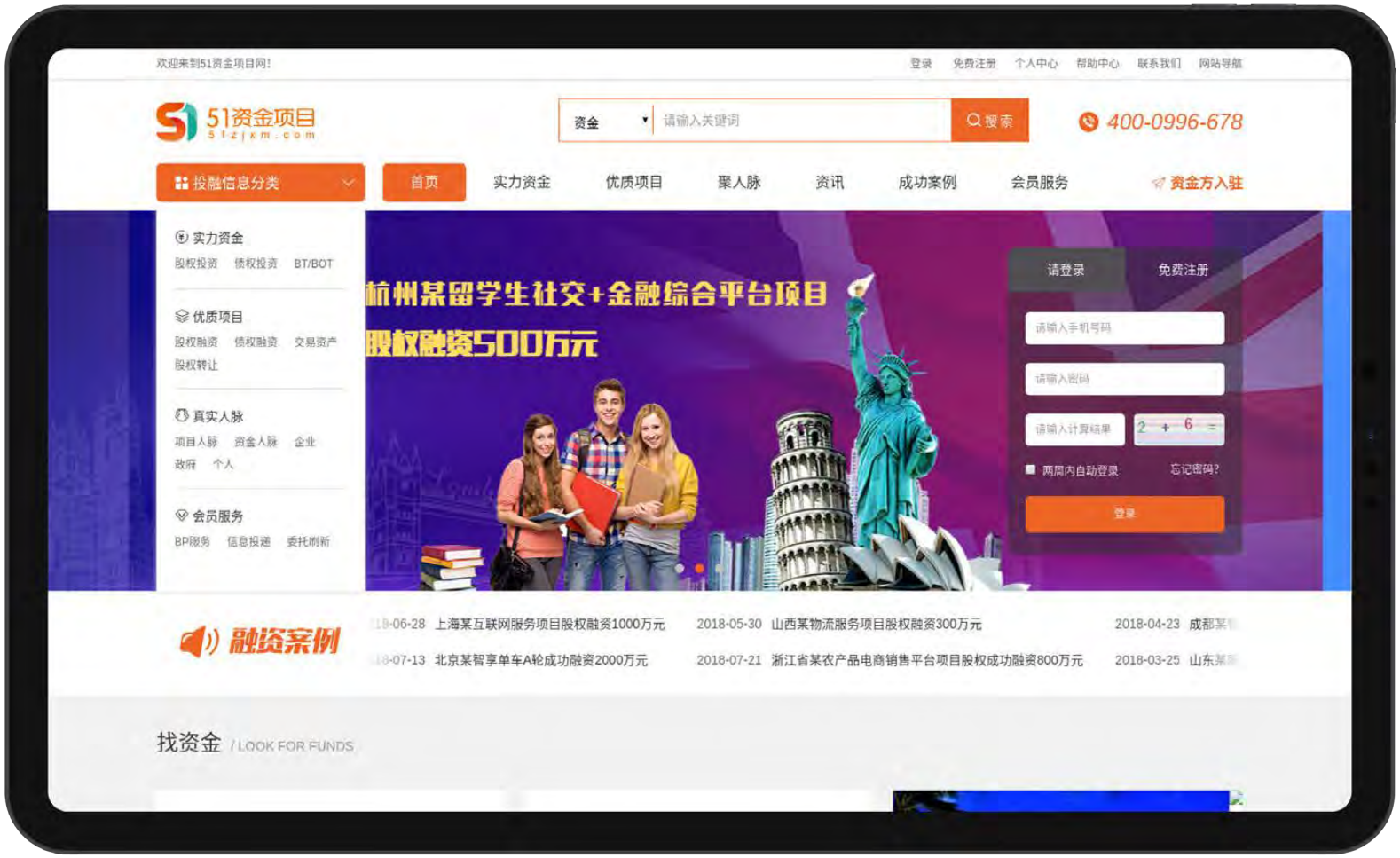
Some 404 pages (as see to the left) return an HTTP 200 status code, making it very hard for an automated scanner to recognize it as a non-existent URL path. Furthermore, the digits “404” are part of an image an obscured, making it challenge for anything but the human eye (and Eyeballer) to categorize it.

SOURCE: THE 2001 VERSION OF MAKEMYTRIP.COM

OLD WEB PAGES

Old-looking web pages, with their broken HTML and blocky frames, have a distinct look-and-feel that a traditional scanner cannot pinpoint. Yet these old-looking pages are very intriguing to those trying to find an initial foothold into a company's environment. After all, the older the website, the more likely it is to be vulnerable. So, identifying orphaned pages that could be vulnerable to new attacks and relic pages that lack patching can help pen testers focus their efforts.

A COMBINATION HOME AND LOGIN PAGE - EYEBALLER ‘SEES’ THAT IT’S BOTH



SOURCE: HTTP://WWW.51ZJXM.COM/

HOME AND LOGIN PAGES

While home and login pages are easy for humans to identify, the same cannot be said for a traditional scanner. Modern web pages are dynamic, constructed with JavaScript and CSS, and often have certain features that can only be recognized once the page is rendered. These complexities make it extremely difficult for any tool to recognize a home or login page programmatically.

These two page types, however, are very important targets for security analysts. Home pages contain links to several endpoints that might be worth exploring, while login pages provide an immediate starting point for injection or brute-force attacks. By being able to recognize both pages on the fly, pen testers can quickly focus their priorities.

SECTION 03

LOOKING THOUGH THE LAYERS: HOW EYEBALLER SEES

LOOKING THOUGH THE LAYERS: HOW EYEBALLER SEES

Eyeballer leverages a Convolutional Neural Network (CNN) to visually sort screenshots. Think of CNNs as automatic feature extractors. Instead of writing a program that searches a general area for a group of pixels that might be a login box, CNNs learn the features of a login box. To a CNN the size, the shape, or the location of the login box doesn't matter; it recognizes the specific features and can pinpoint where in the page it sits. This capability is especially useful when reviewing multiple web pages since common features reside in different places on different sites.

HOW EYEBALLER WORKS:

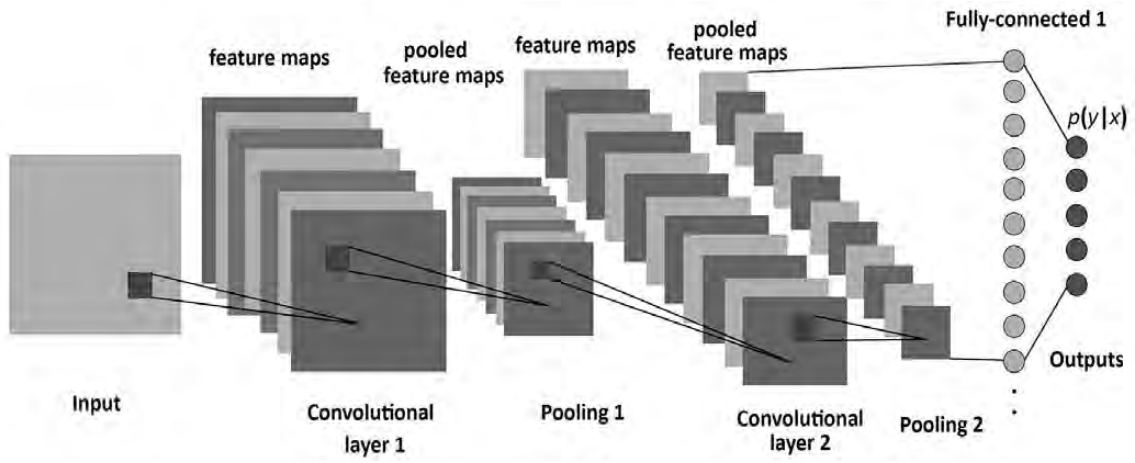
Step 1: Screenshots are split into chunks

Step 2: Eyeballer "looks" at the features of each chunk

Step 3: Each set of inspection results is passed onto the next layer

The final result is a confidence measurement of what features were identified.

A CONVOLUTIONAL NEURAL NETWORK (CNN) LAYOUT

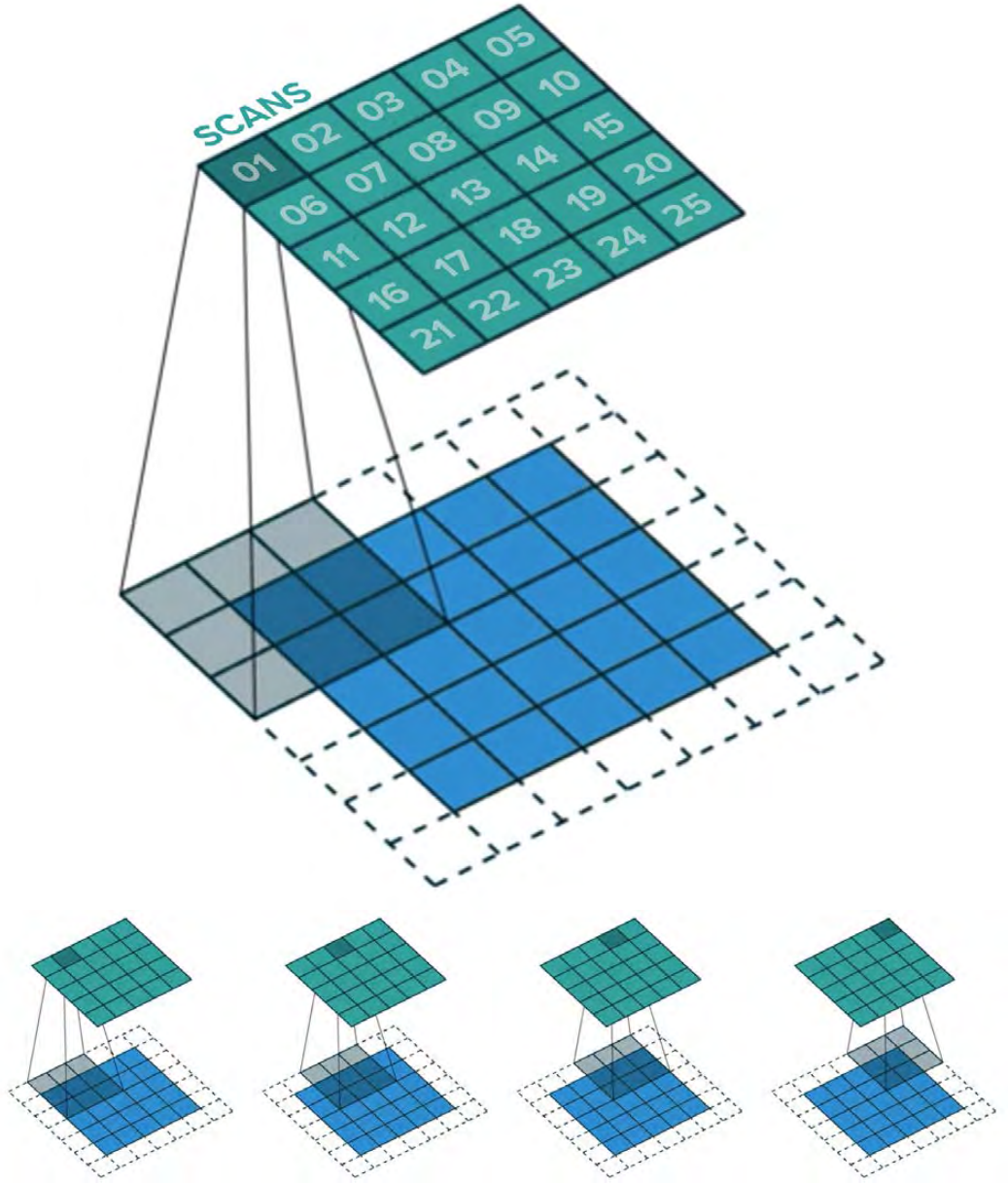


SOURCE:
COURTESY OF WWW.MDPI.COM
(HTTPS://WWW.MDPI.COM/1099-4300/19/6/242) - CREATIVE COMMONS

STEP 01

SCREENSHOTS ARE SPLIT INTO CHUNKS

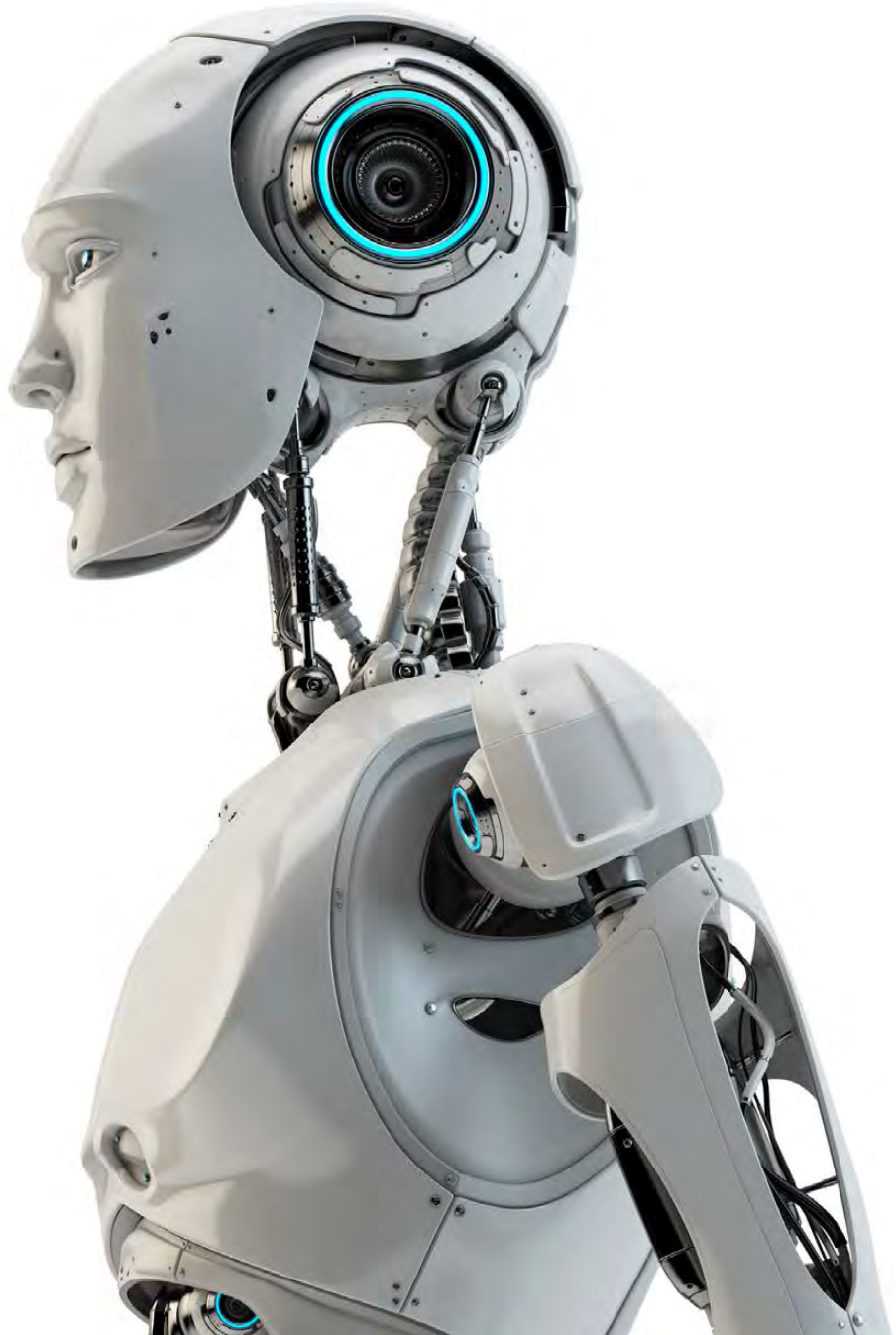
Eyeballer takes an image and breaks it up into chunks. At each layer of the network, it groups neighboring chunks together and looks at their pixel values. It then takes what it learns from one chunk and passes it as the input to the next layer. This process is repeated for each chunk of the image.



STEP 02

EYEBALLER “LOOKS” AT THE FEATURES OF EACH CHUNK

At each layer, Eyeballer generalizes what it sees, first recognizing lines, then shapes, then website features. Toward the end of the network, Eyeballer can recognize entire sections of the page.



STEP 03

THAT INFORMATION IS PASSED ONTO THE NEXT LAYER

Eyeballer repeats this process 22 times within its network, building a deeper picture of what the page contains at each layer.

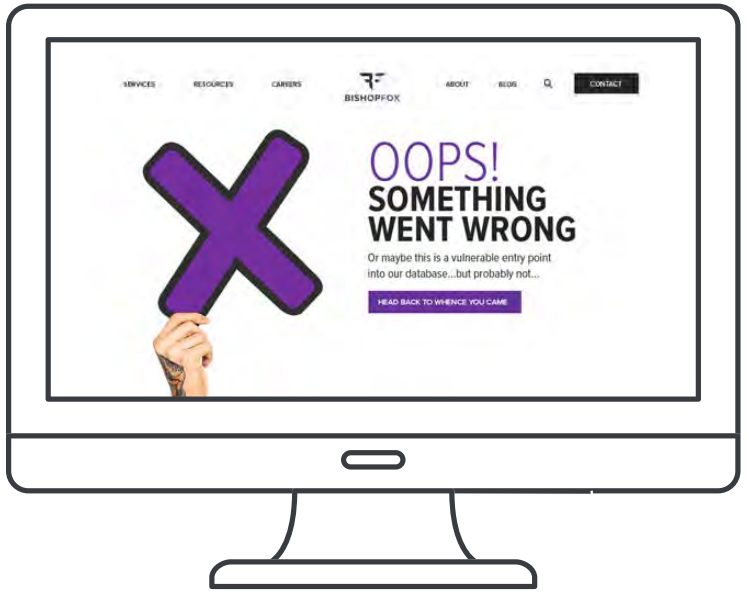
When Eyeballer's CNN is complete, Eyeballer can recognize generalized features of a class of images. Put another way, it means Eyeballer can recognize that two input boxes next to a submit button indicate a login form.

THE RESULTS

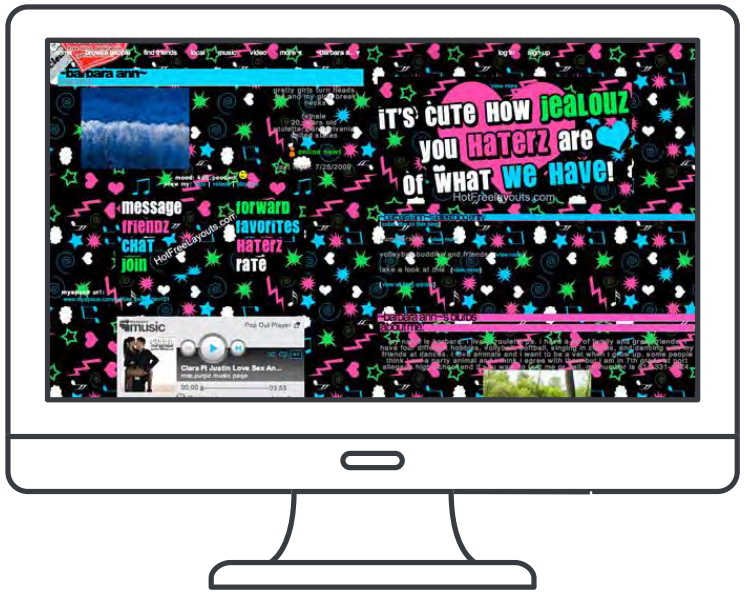
THE FINAL RESULT IS A CONFIDENCE MEASUREMENT OF FEATURES IDENTIFIED

Eyeballer returns a confidence measurement of the types of features it has recognized in the page.
As it learns, Eyeballer tries to answer questions like:

“Does this page have a login prompt?”



“Is this a custom error page?”



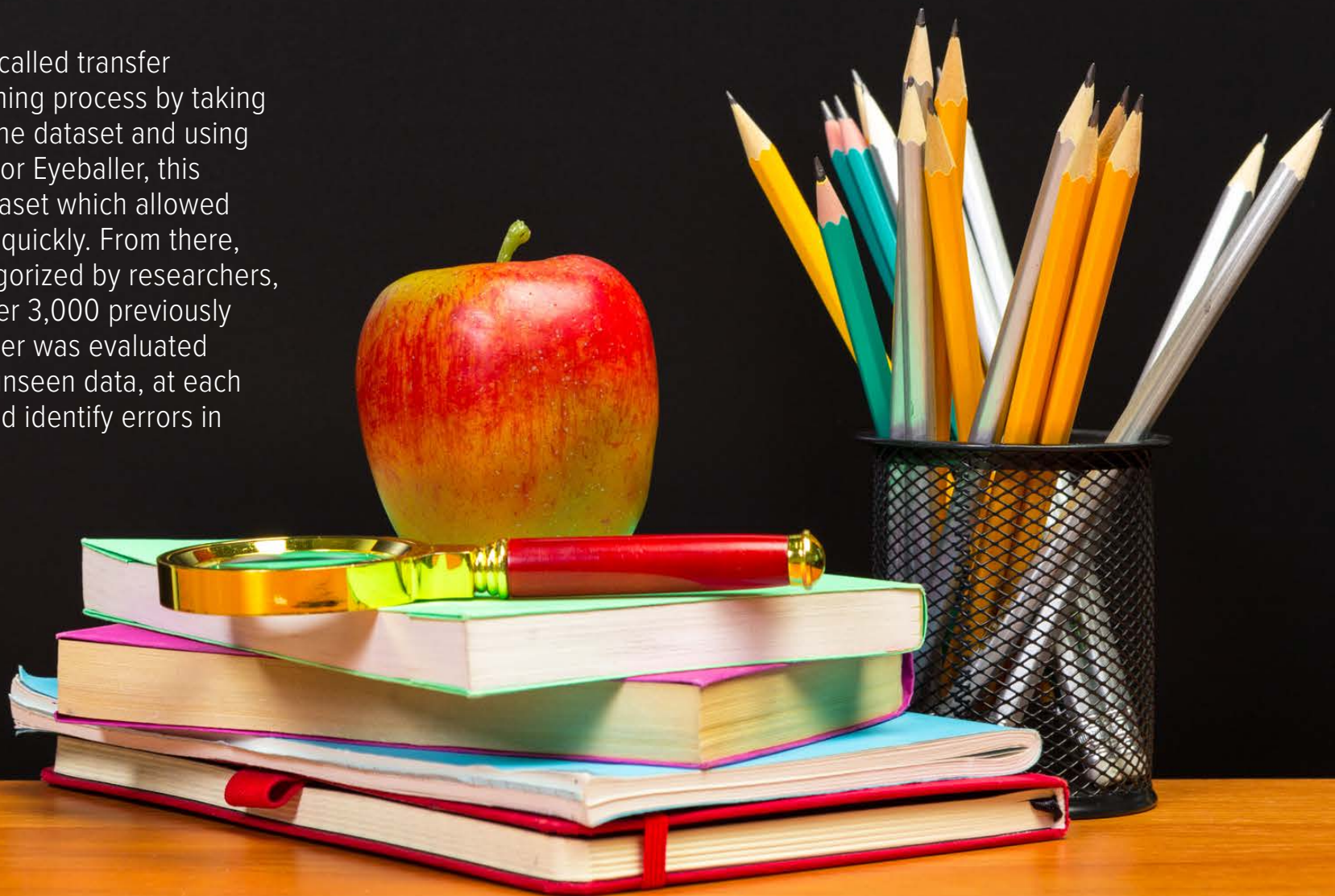
“Does this web page look like it was made in the early 2000s?”

SECTION 04

TRAINING ROUNDS

TRAINING ROUNDS

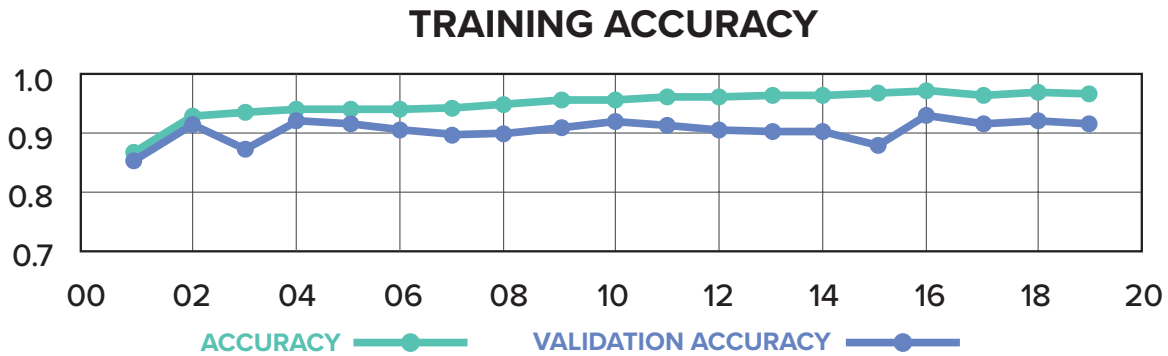
Eyeballer was constructed using a technique called transfer learning. Transfer learning speeds up the training process by taking the knowledge from a pre-trained model of one dataset and using that information to "teach" another dataset. For Eyeballer, this information was taken from the ImageNet dataset which allowed it to recognize lines, curves, and shapes very quickly. From there, Eyeballer was trained on 10,000 images categorized by researchers, and then tested on how well it recognized over 3,000 previously unseen images. As part of its training, Eyeballer was evaluated against a validation dataset, which was also unseen data, at each stop of training. This type of monitoring helped identify errors in training and optimization opportunities.

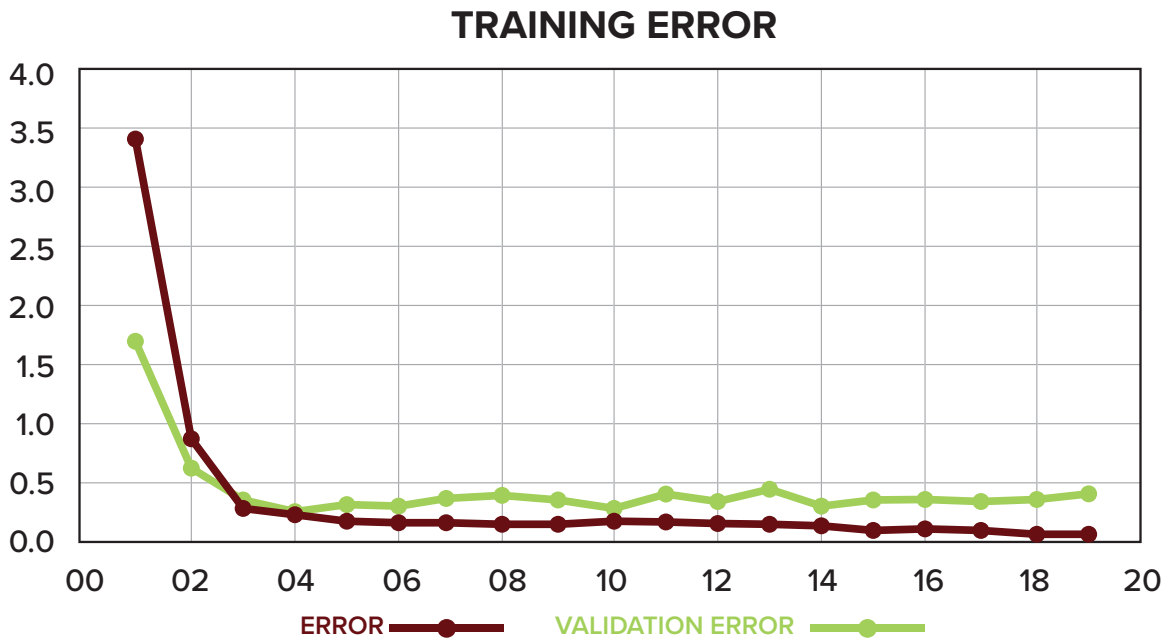


EYEBALLER'S MODEL FILE

Eyeballer comes with a model file, the brain behind its CNN that allows it to successfully classify Home Pages, Login Pages, Custom Error Pages, and Old-looking Web Pages. Should users decide they want to classify more labels, they will need to retrain the model with additional images and specify the new labels (see *Eyeballer research page* for more information).

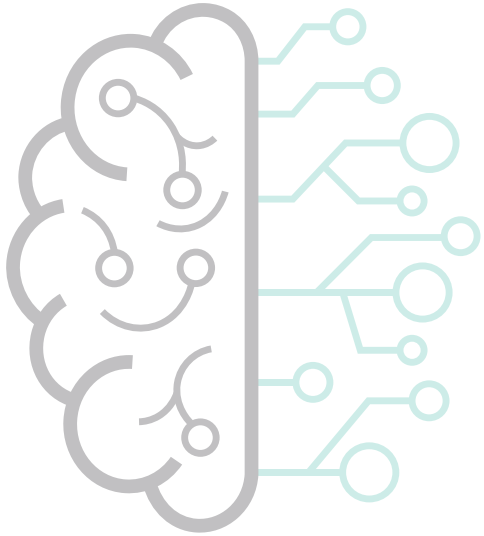
By default, Eyeballer is configured to identify image labels above a threshold of 50%. Since Eyeballer returns a confidence value, this threshold can be modified using the appropriate command line argument when making predictions. Users can set the threshold for recognition as high or as low as their needs demand.





SECTION 05

THE RESULTS



THE RESULTS

Eyeballer can currently recognize several categories of web page features, including Custom 404 Pages, Login Pages, Home Pages, and Old-looking Websites.

Using a real-world evaluation dataset, the latest version of Eyeballer is hitting a benchmark of about 90% overall accuracy.

BEHIND THE SCENES

- Total images hand-labeled:
  - » +13,377 (heh, leet)
- Training samples:
  - » 8,305
- Training validation samples:
  - » 2,076
- Testing samples:
  - » 2,996
- Number of epochs:
  - » 20 epochs that took approximately 2 hours to train (thanks to the model architecture and the transfer learning)
- Time to classify 1,000 images on a standard laptop:
  - » ~120 seconds (2 minutes)

PAGE CATEGORIZATION & CONFIDENCE LEVELS

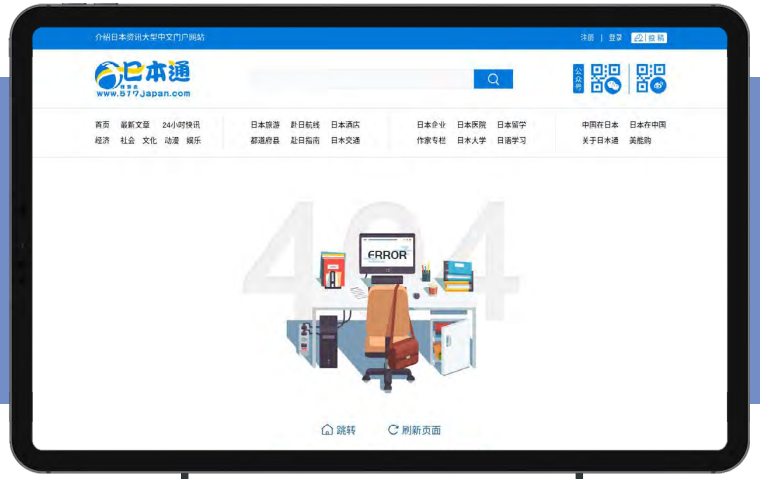
RANKED BY TYPE OF PAGE AND CONFIDENCE LEVELS

Custom 404	0.1%	Homepage	54.3%
Login	65.9%	Old Looking	61.8%

The percentages represent confidence levels. By default, they are set at 50%. These results indicate that this has correctly been identified as a Login, Home, and Old-looking web page. Users can also adjust the confidence level via Eyeballer's command line.

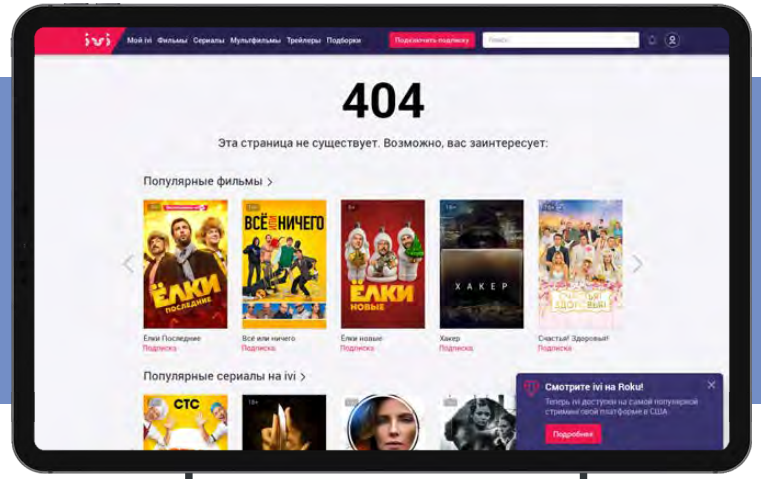
PAGE CATEGORIZATION & CONFIDENCE LEVELS

HIGH SCORING CUSTOM 404 RECOGNITION



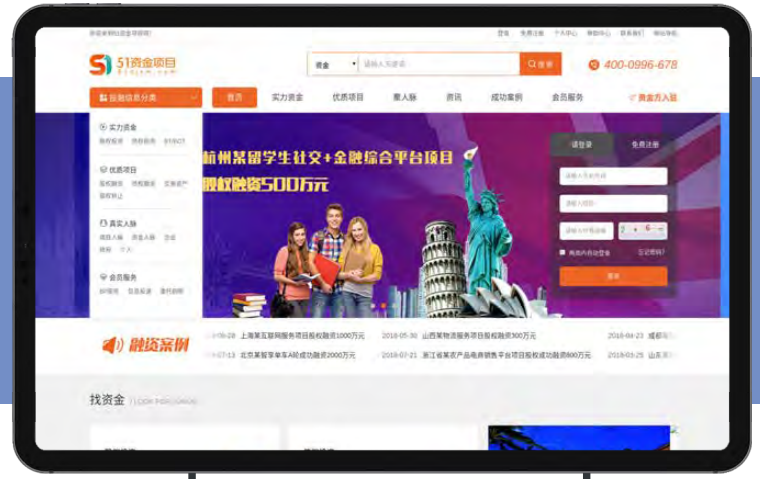
Custom 404	99.5%
Login	0.0%
Homepage	0.0%
Old Looking	0.0%

404 HOMEPAGE WITH HOMEPAGE LOOK & FEEL



Custom 404	52.1%
Login	2.4%
Homepage	55.7%
Old Looking	0.1%

MODERN HOMEPAGE WITH LOGIN



Custom 404	0.0%
Login	87.4%
Homepage	89.5%
Old Looking	0.0%

SECTION 06

EVER-EVOLVING AI

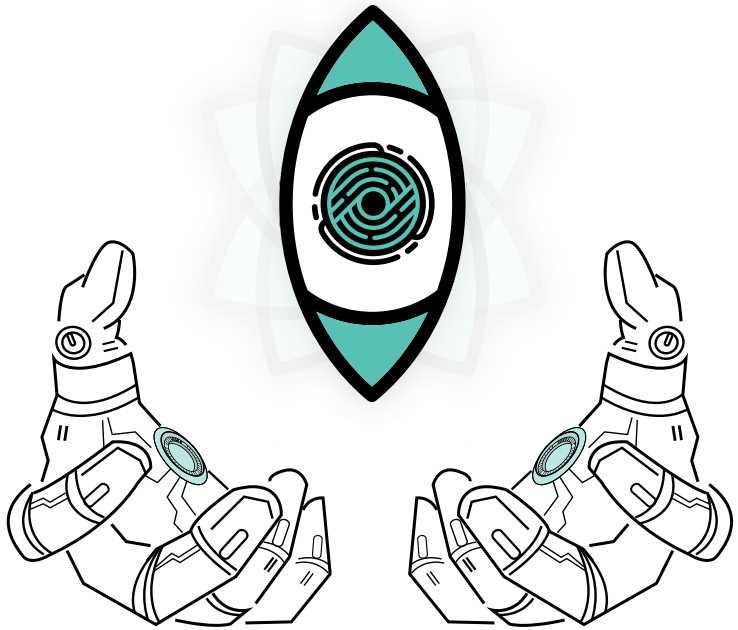
EVER-EVOLVING AI

As security needs evolve, so will Eyeballer. Future enhancements will include improved accuracy, more granular identification buckets, better integration with existing web scanners, and the ability to identify accidentally published pages and internal assets like access point interfaces, printers, and SharePoint routers.

And though Eyeballer comes preconfigured with the ImageNet dataset, it can also be trained from scratch to expand its capabilities and meet specific testing needs. So, whether pen testers are looking to understand the makeup of an external perimeter or looking to optimize their red team or purple team process, Eyeballer makes an excellent addition to any pen testing toolkit.

CYBERSECURITY BREAKTHROUGH AWARD 2019

Eyeballer won the 2019 CyberSecurity Breakthrough Award for Web Filtering and Content Evasion.



GET IT ON GITHUB

Eyeballer is now available as open source software on GitHub.

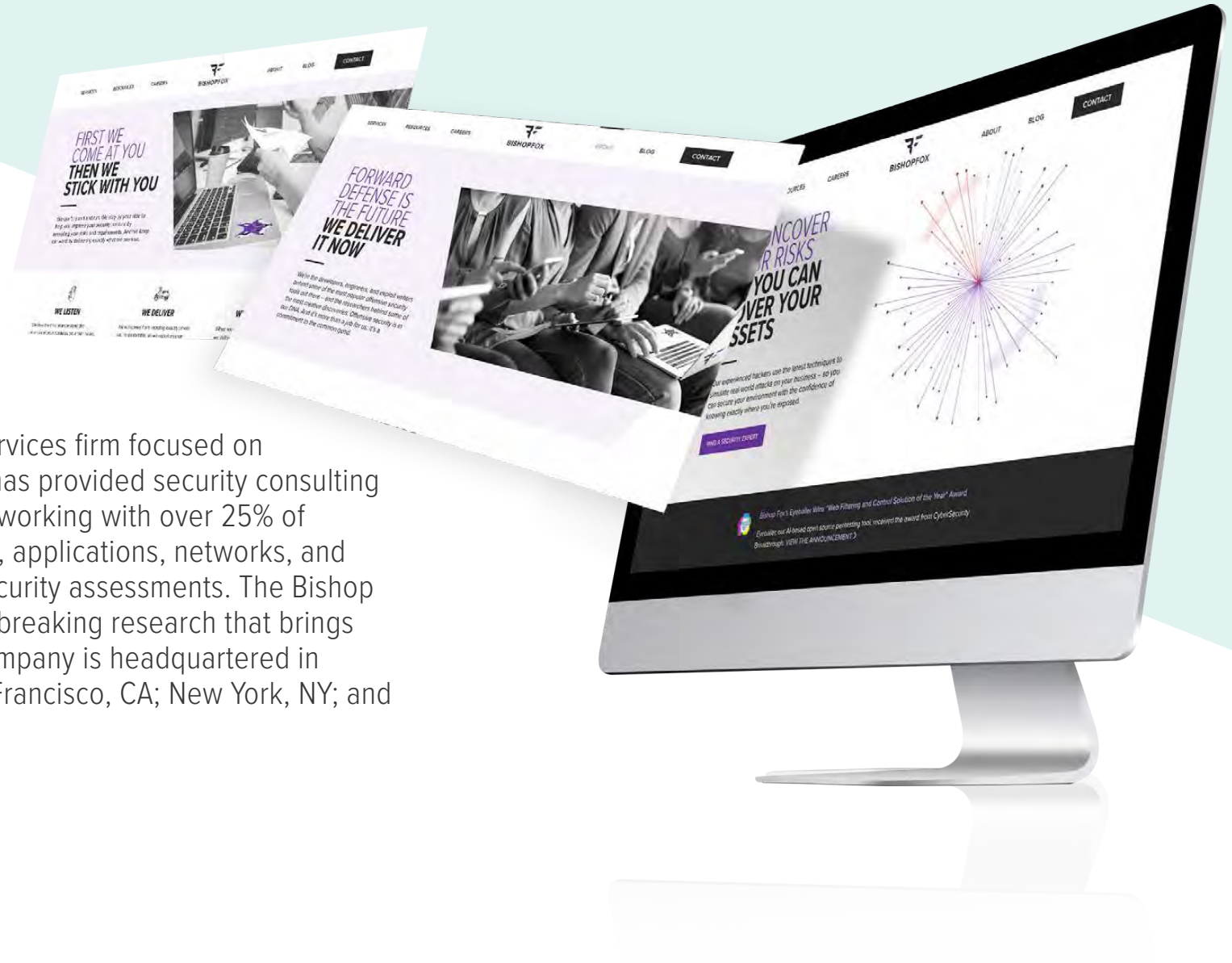
GET INSTRUCTIONS

ABOUT

BISHOPFOX

Bishop Fox is the largest private professional services firm focused on offensive security testing. Since 2005, the firm has provided security consulting services to the world's leading organizations — working with over 25% of the Fortune 100 — to help secure their products, applications, networks, and cloud resources with penetration testing and security assessments. The Bishop Fox R&D team is dedicated to delivering groundbreaking research that brings our vision of offensive security to reality. The company is headquartered in Phoenix, AZ and has offices in Atlanta, GA; San Francisco, CA; New York, NY; and Barcelona, Spain.

Learn more at: **BishopFox.com**



MEET THE BRAINS
BEHIND THE EYEBALLER

DAN PETRO

Dan Petro is a Lead Researcher at Bishop Fox and focuses on application penetration testing (static and dynamic), product security reviews, network penetration testing (external and internal), and cryptographic analysis. Dan has presented at Black Hat USA and DEFCON for the past five years on topics such as hacking smart safes, hijacking Google Chromecasts, and weaponizing AI. Additionally, Dan has been quoted in Wired, The Guardian, Business Insider, and Mashable. Dan holds both a Bachelor of Science and a Master of Science in Computer Science from Arizona State University.

GAVIN STROY

Gavin Stroy (OSCP) is a Senior Security Analyst at Bishop Fox, where he focuses on application assessments (static and dynamic) and network penetration testing (external and internal). Gavin is an active member of the security research community and has published an article on Network Based File Carving in eForensics Magazine. He has spoken on the topic of machine learning at DEFCON China and he presented Eyeballer at Black Hat USA in 2019. He holds a Bachelor of Science in Network and Communications Management from DeVry University and a Master of Computer Science from Arizona State University's Ira A. Fulton School of Engineering.

We provide security consulting services to the Fortune 1000 and high-tech startups.

We help our clients secure their businesses, networks, cloud deployments, applications, and products.

Find out more at bishopfox.com.
Keep in touch with the foxes on Twitter @bishopfox and on LinkedIn.