



**Mark Curphey  
Cyber Coalition,  
15th June**

**The lies, myths,  
unethical practices  
and dodgy truths  
of Software Security**



**The Lies, myths,  
unethical practices  
and dodgy truths  
of Software Security**



The industry  
is out of  
control



**IMMORAL**



**LIE**

**DODGE  
THE  
TRUTH**

**MYTH**

**UNETHICAL**









**Donald J. Trump** ✓

@realDonaldTrump

Following



Putin & I discussed forming an impenetrable Cyber Security unit so that election hacking, & many other negative things, will be guarded..

8:50 AM - 9 Jul 2017

19,157 Retweets 77,052 Likes



37K

19K

77K







**Donald J. Trump** @realDonaldTrump · Jul 9

Putin & I discussed forming an impenetrable Cyber Security unit so that election hacking, & many other negative things, will be guarded..

38K 19K 78K



**WikiLeaks**  
@wikileaks

Follow

Replying to @realDonaldTrump

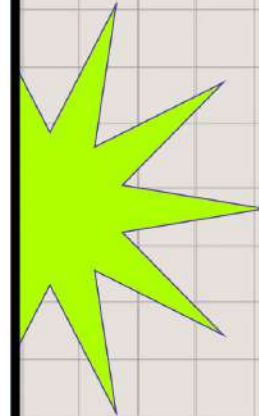
Why not put @JulianAssange in charge of it? He's trusted by the public and has the CIA's best stuff anyway [wikileaks.org/ciav7p1/](http://wikileaks.org/ciav7p1/)

5:38 AM - 9 Jul 2017

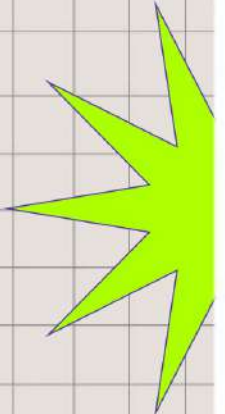
1,688 Retweets 5,579 Likes



291 1.7K 5.6K



UNETHICAL. UNETHICAL.



He's one of the best men in town. While his door may say *Office Hours 2 to 4*, he's actually on call 24 hours a day.

The doctor is energetic, a diplomat, and a friendly sympathetic human being all in one, no matter how long and hard his schedule.

According to a recent *Nationwide survey*:

## MORE DOCTORS SMOKE CAMELS THAN ANY OTHER CIGARETTE

DOCTORS in every branch of medicine—115,000 in all—were queried in this nationwide study of cigarette preferences. These leading research organizations made the survey. The gist of the query was: *What cigarette do you smoke, Doctor?*

The brand named most was Camel!

The rich, full flavor and cool richness of Camel's superb blend of similar tobaccos seem to have the same appeal to the smoking tastes of doctors as to millions of other smokers. If you are a Camel smoker, this preference among doctors will hardly surprise you. If you're not—well, try Camel's now.

Your "T-Zone" Will Tell You...

T for Taste...  
T for Throat...  
That's your proving ground for any cigarette. Now if Camels don't suit your "T-Zone" is a "T."

*"Luckies are easy on my throat"*

There are no finer tobaccos than those used in Luckies, and Luckies' exclusive process is your



UNETHICAL. UNETHICAL. UNETHICAL.

**SKECHERS**  
*Fitness Group*

# Shape-ups

**SHAPE UP WHILE YOU WALK**

**Designed to:**

- Promote weight loss
- Tone muscles
- Improve posture
- Reduce stress on knees and ankles

**WOMEN**

**MEN**

PATENT PENDING

**WANT MORE INFO ON SHAPE-UPS? [GET DETAILS](#)**



UNETHICAL. UNETHICAL.

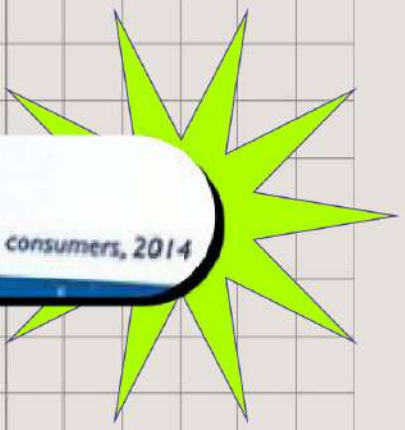
How do you know you have  
**Dandruff Problem?**

Itching  
Redness  
Dry Scalp

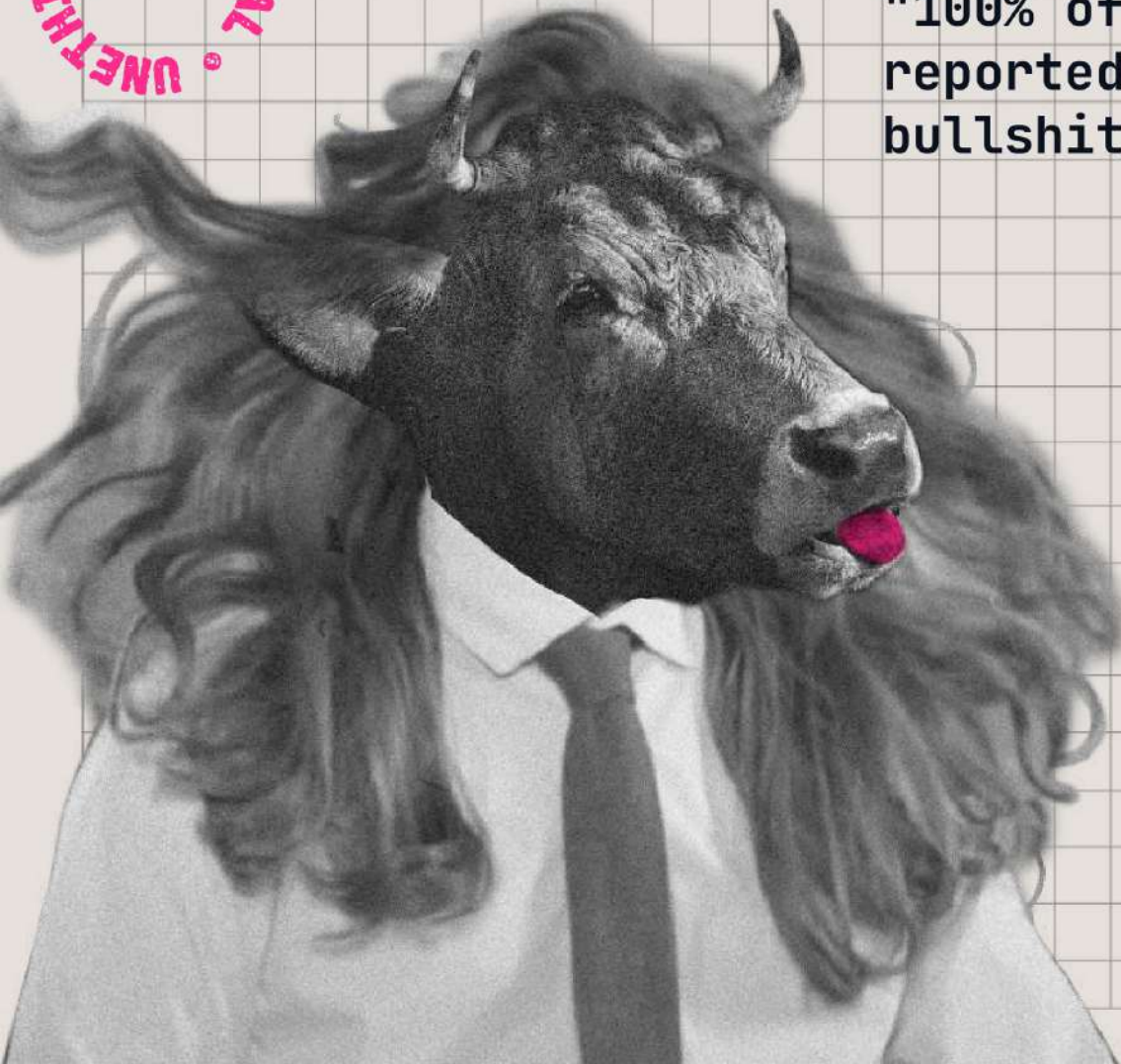
**99%**  
— claims that Selsun Blue is —  
**EFFECTIVE!**

\*Based on internal survey conducted amongst 100 Malaysian consumers, 2014

*\*Based on internal survey conducted amongst 100 Malaysian consumers, 2014*



UNETHICAL. UNETHICAL. UNETHICAL.



"100% of security marketing droids reported they smelled fresher using bullshit shampoo"



\* 100% of 0 real people took part in this survey





# Security Bullshit Daily

## The multi-million pound, fake security awards industry

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.



Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.



Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

### Località

#### Una classifica di sicurezza

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

### Internazionale

#### Una classifica di sicurezza

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

Una classifica di sicurezza che non ha mai esistito. Un premio che non si è mai dato. Un'industria che non ha mai esistito.

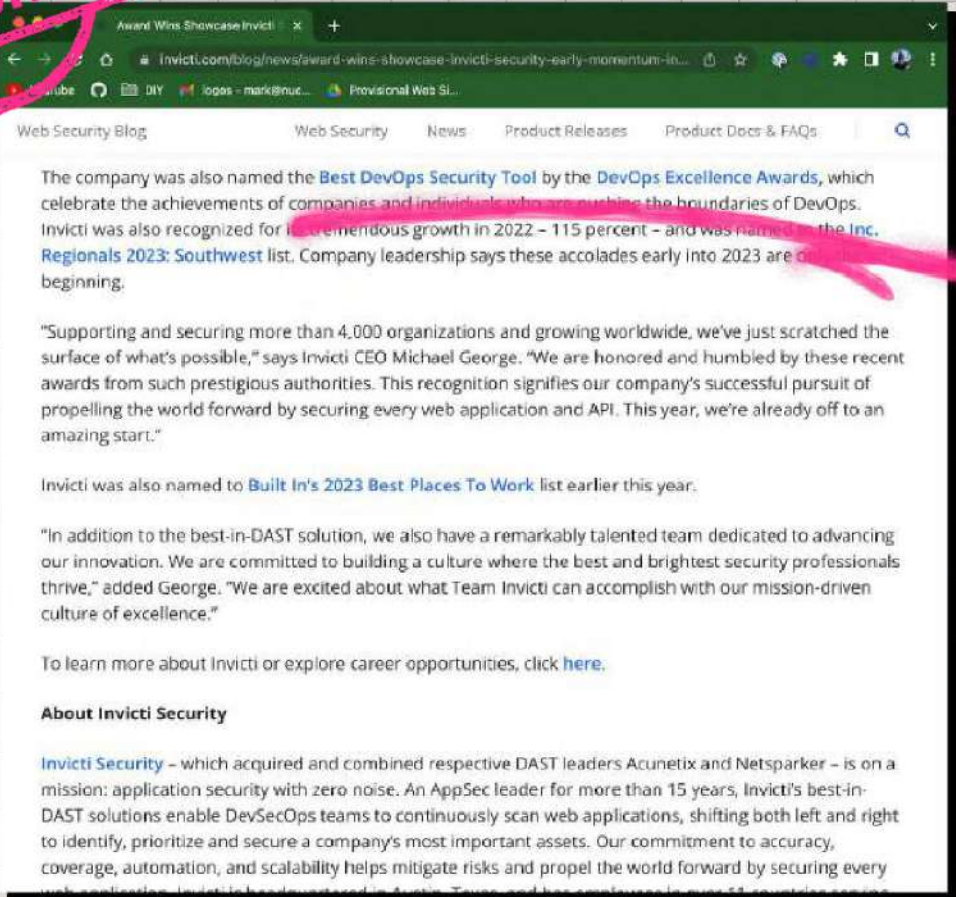


IMMORAL

The screenshot shows a web browser window with the URL `invicti.com/blog/news/award-wins-showcase-invicti-security-early-momentum-in-2023`. The page features the Invicti logo and navigation menu. The main content is a blog post by Chelsea Glosser, dated March 20, 2023. The post text reads: "Invicti Security announces momentum-building success in 2023 as it garners multiple industry awards spotlighting its products and leadership, including Best Application Security Product, Cybersecurity Woman of the Year, and Chief Technology Officer of the Year." Below the text is a subscription form with a "Subscribe" button and a privacy notice: "Your information will be kept private."



IMMORAL



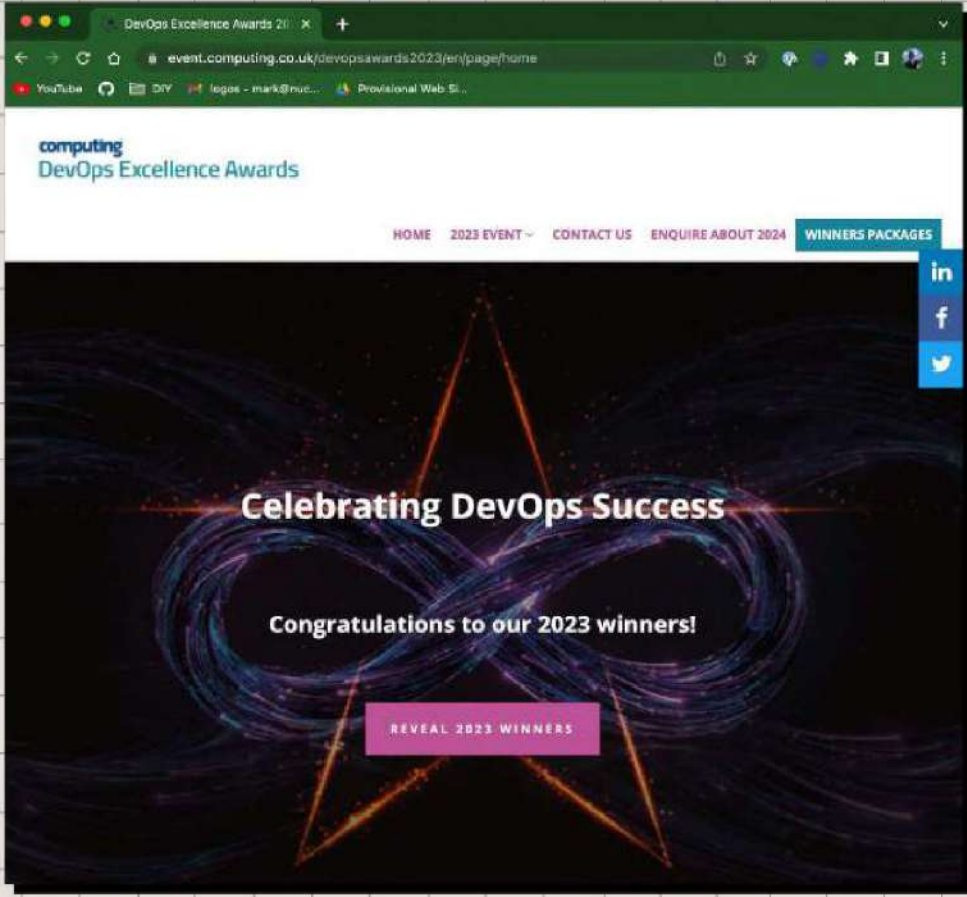
”

The Best DecOps Security tool by the DevOps Excellence Awards





IMMORAL



**IMMORAL**

**Carlisle Bailey**  
Marketing Executive  
c.bailey@thechannelcompany.com  
020 3834 0650

**Zoe Vincent**  
Senior Event Co-Ordinator  
z.vincent@thechannelcompany.com  
020 3834 0609

**Bobby Naipaul**  
Account Manager - Event & Marketing Solutions  
bnaipaul@thechannelcompany.com  
020 3834 0601

Contact Us | Marketing Services | The Channel Company | Terms and Conditions | Policies

**THE CHANNEL COMPANY**  
The Channel Company SMDA, Published by The Channel Company, New London House, 172 Drury Lane, London WC2B 5QR, registered in England and Wales with company registration number 1407011

computing  
DevOps Excellence Awards

HOME 2023 EVENT - CONTACT US ENQUIRE ABOUT 2024 WINNERS PACKAGES

### Winner Packages 2023

Winners can promote their success by purchasing one of our marketing packages below.  
~~Please note, packages included winner logo.~~


If you require any assistance with your booking or would like to view the package options further please contact Bobby Naipaul on 0203 834 0601 or via [bnaipaul@thechannelcompany.com](mailto:bnaipaul@thechannelcompany.com)

**Platinum - £2749 +VAT**

Winners logo with category of the  
Winners social media tile with category name and company logo  
Winners writes interview publication on Computing.co.uk

£2749.00 +VAT (20%)

**BOOK NOW** →



PP

The Channel Company EMEA,  
Published by The Channel  
Company, New London  
House, 172 Drury Lane,  
London WC2B 5QR

PP

Winners can promote their  
success by purchasing one  
of our marketing packages  
below.

Q

IMMORAL

computing  
DevOps Excellence Awards

HOME 2023 EVENT CONTACT US ENQUIRE ABOUT 2024 WINNERS PACKAGES

place achievable recruitment plans that future proof attraction and retention of the top UK talent.

**Stuart Sumner**  
*Global Vice President - Content Computing*  
Stuart Sumner is Global Vice President - Content of The Channel Company. Previously he spent 10 years as a programme manager in the IT industry, working for companies such as the BBC, COLT, Nortel Networks and Equant. As a journalist he has also worked for Time Out and IPC Media. He is a regular technology pundit and contributor to the BBC News Channel, as well as a published author.

**Terry McGill**  
*Director of Technology Church of England*  
Working in various parts of technology for most of his career Terry has seen the world transform from analogue to Digital several times now. Mostly he gives it a gentle helping hand but sometimes it needs more of a firm shove in the right direction. After years working in the creative industries Terry has, more recently, spent time in the Third Sector and currently leads technology for the Church of England where he has an unhealthy interest in the areas of Cloud Services, Security and Digital Anthropology in order to design agile, secure and modern workplaces and platforms. He has a keen eye for emerging trends in tech, and considers it an honour to be asked to judge these awards.

Contact Us | Marketing Solutions | About The Channel Company | Terms and Conditions | Policies



IMMORAL

Welcome, visitor! [Register] [Login]


**CYBERSECURITY**  
Excellence Awards

**MSC MARKETING**  
Become a marketing leader of tomorrow  
AT NEOMA BUSINESS SCHOOL

NEOMA BUSINESS SCHOOL

NOMINATIONS WINNERS CONTACT US SPONSOR FAQ START NEW NOMINATION

Want to sponsor the awards site or promote your nomination? Click here to learn more

ENTER THE **2023**   
**CYBERSECURITY**  
EXCELLENCE AWARDS

Congratulations  
to all Award Winners!

[Award Winners](#)

**Featured Award Nominations**

Here are the premium sponsorship package details:

- Award winners can request a beautiful award plaque, shipped by mail, to showcase the award win
- Highlight one key nomination / submission on the award homepage
- Create up to three new, custom award categories for your nominations (thereby significantly increasing your odds of an award win)
- Add up to 10 award submissions (an extra fee for the individual nominations)
- ~~Place your company logo on the homepage site (linked to your website for SEO impact)~~
- ~~Feature your brand on the nomination submission page (sidebar)~~
- Benefit from better rankings of your website from the SEO impact of linking back to your website
- Social media promotion of your nomination(s) and award win(s)
- Extend your nomination deadline (for late submissions after the standard deadline)
- Receive 10% discount as a first time client on any Cybersecurity Insiders marketing programs
- Receive premium, 24-hour response, full-service support for any changes, questions or technical issues regarding your nominations

Award sponsorship package = \$1,900

NEXT STEP: Please send your sponsorship request to [info@cybersecurity-excellence-awards.com](mailto:info@cybersecurity-excellence-awards.com) - complete with your company logo file (jpg or png), URL to your website (link will be placed on your


GRSEEE  
Compliance ASAP

BACKTOP

**vmware**

neustar  
Security Services

AKATHENURITY



FF

Create up to three new, custom award categories for your nominations

FF

Want to sponsor the awards site or promote your nomination?

Q

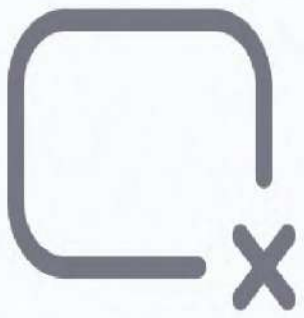
IMMORAL



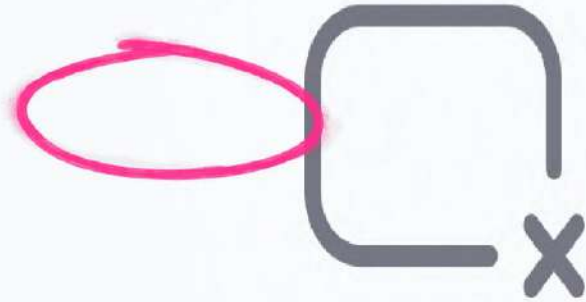
100x



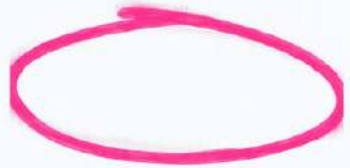
IMMORAL



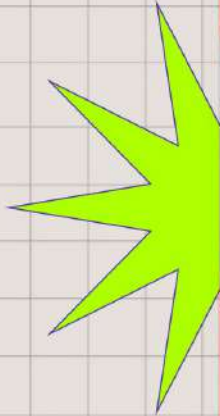
IMMORAL



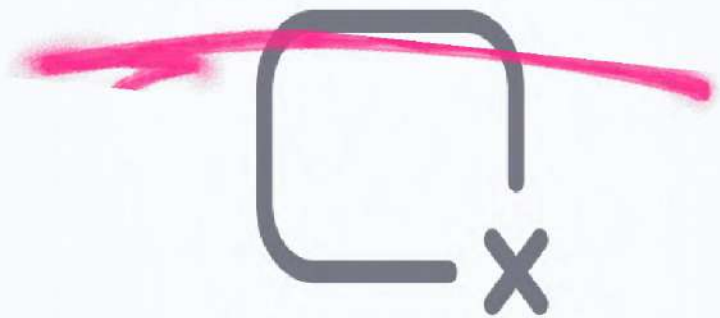
IMMORAL







IMMORAL



IMMORAL

NEWS

### Debricked named leader in the 2023 Gartner Magic Quadrant for Application Security Testing!

21 days ago · 0 replies · 142 views



Community Manager · 0 replies

...ht year was off to a good start, it just keeps getting better! We are happy to  
Debricked has been named a leader in the 2023 Gartner Magic Quadrant for  
Application Security Testing, together with Fortify and OpenText Cybersecurity!

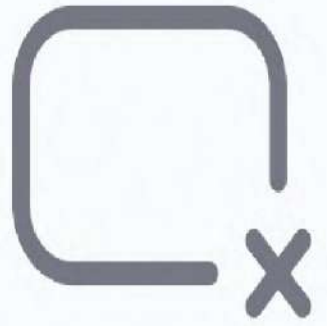
Thanks to critical capabilities such as machine learning, addressing the security of software supply chains with Select and general software composition analysis capabilities, Debricked has largely contributed to Fortify's continued leadership in the Gartner MQ.

*"The acquisition of Debricked provides a number of software supply chain capabilities, including Open Source Select. That product provides insights into data that can be leveraged to assess open source software risks (frequency of updates, size of maintenance team, etc.), and helps guide teams to packages with the least potential for downstream risks."*

This, in couple with other updates and additional capabilities, has made Fortify a leader for the 10th (!!!) year in a row.



IMMORAL



UNETHICAL



As the digital economy grows, digital crime grows with it. Soaring numbers of online and mobile interactions are creating millions of attack opportunities. Many lead to data breaches that threaten both people and businesses. At the current rate of growth, damage from cyberattacks will increase to about \$2.5 trillion annually by 2025, a 300 percent increase from 2015 levels.

Steve Morgan, "2022 Cybersecurity Almanac: 100 facts, figures, predictions, and statistics," *Cybercrime Magazine*, January 19, 2022.

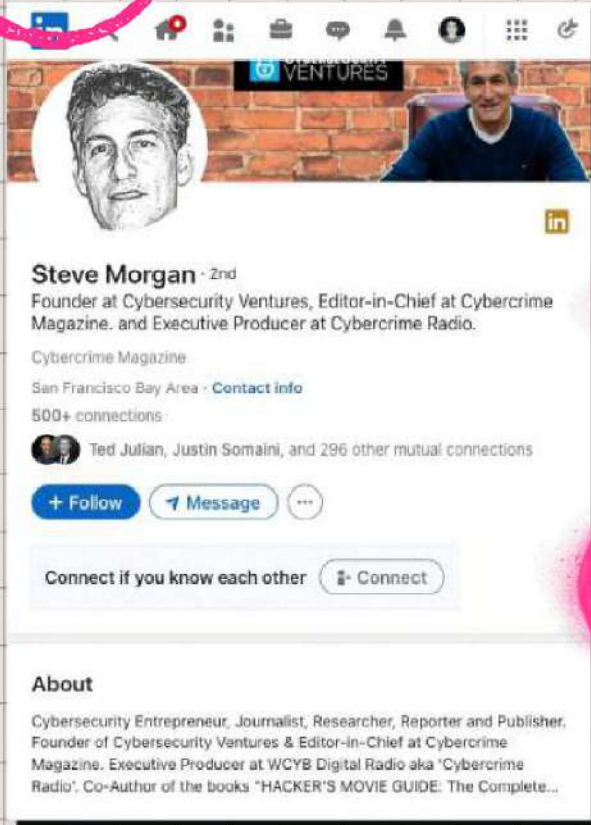
However, set against the scale of the problem, even this

”

Steve Morgan,  
"2022 Cybersecurity Almanac:  
100 facts, figures,  
predictions and statistics."  
*Cybercrime Magazine*, January  
19, 2022



UNETHICAL



Steve Morgan · 2nd  
Founder at Cybersecurity Ventures, Editor-in-Chief at Cybercrime Magazine, and Executive Producer at Cybercrime Radio.

Cybercrime Magazine  
San Francisco Bay Area · [Contact info](#)  
500+ connections  
Ted Julian, Justin Somaini, and 296 other mutual connections

[+ Follow](#) [Message](#) [...](#)

Connect if you know each other [Connect](#)

**About**  
Cybersecurity Entrepreneur, Journalist, Researcher, Reporter and Publisher, Founder of Cybersecurity Ventures & Editor-in-Chief at Cybercrime Magazine. Executive Producer at WCYB Digital Radio aka 'Cybercrime Radio'. Co-Author of the books 'HACKER'S MOVIE GUIDE: The Complete...

## 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics



The past, present, and future of cybercrime  
Sponsored by [Cisco](#)

- [Steve Morgan](#), Editor-in-Chief

SecurityWeek - Jan. 19, 2022

If it were measured as a country, then cybercrime – which was predicted to inflict damages totaling \$6 trillion USD globally in 2021 – would be the world's third-largest economy after the U.S. and China, [Chuck Robbins](#), Chair and CEO at [Cisco](#), informed, citing research from Cybersecurity Ventures, when he [delivered a keynote](#) at last year's RSA Conference.

Cybersecurity Ventures is excited to release this special second annual [2022 Cybersecurity Almanac](#), a handbook containing the most pertinent statistics and information for

computer programmer Bob Thomas. BBN, Bold, Beranek, and Newman, now Raytheon BBN Technologies, developed packet switching networks for ARPANET.

- Brain is the industry standard name for a computer virus that was released in its first form in Jan. 1986, and is considered to be the first computer virus for the IBM Personal Computer (IBM PC) and compatibles.

### ACCORDING TO CISCO

- 39 percent of security technologies used by organizations are considered outdated, according to a report from Cisco.
- Cisco asked over 5,100 IT and security professionals across 27 countries about staying resilient when disaster strikes. Key findings include: Organizations with board-level oversight of business continuity and disaster recovery are the most likely (11 percent above average) to report having strong programs; Organizations that regularly test their business continuity and disaster recovery capabilities in multiple ways are 2.5 times more likely to maintain business resiliency; Organizations that make chaos engineering standard practice are



**UNETHICAL**

## **CAUTION**

**Name, shame and vocalise. Please stop buying products from companies that participate in this bullshit**

**Lobby for the practice of these type of awards to be regulated like the advertising standards authority**



MYTH

# Security Bullshit Daily

## Shift left phenomenon is based on fake survey



La ricerca ha dimostrato che il fenomeno del shift left non è supportato da dati reali. Invece, si basa su una survey fasulla che ha chiesto ai rispondenti di indicare se il loro team di sicurezza si è spostato verso sinistra. Il risultato è stato che il 70% dei rispondenti ha risposto di sì, il che è chiaramente falso.



La ricerca ha dimostrato che il fenomeno del shift left non è supportato da dati reali. Invece, si basa su una survey fasulla che ha chiesto ai rispondenti di indicare se il loro team di sicurezza si è spostato verso sinistra. Il risultato è stato che il 70% dei rispondenti ha risposto di sì, il che è chiaramente falso.





**MYTH**

### The exponential cost of fixing bugs

Source: January 20, 2019

The cost of detecting a bug increases exponentially with time in the software development lifecycle. Fixing an issue in the field is several orders of magnitude more expensive than fixing it during development. The cost of a bug increases exponentially over time because of the impact of the bug on the business and the customer's experience.

"Many defects end up costing more than it would have cost to prevent them. Defects are inevitable when they occur, but the financial costs of fixing the defects and the related costs because of damaged relationships, lost business, and lost development time..."

The following graph courtesy of the NIST helps in illustrating how the effort in detecting and fixing software bugs increases exponentially through the development lifecycle.

The relative cost of fixing bugs increases exponentially through the development lifecycle.

### Calculating the ROI of SAST

Cost			
Maintenance	\$8,000,000	\$1,166,667	\$6,833,333
Costs 1 <sup>st</sup> Year			
Savings from High Quality	\$15,012,287		

Table 3. Savings from a mature, quality and security focused development approach versus average organizations on a large project.

Based on Jones' research, it's clear that the ROI in security and quality is tied to maturing the development process, like DevSecOps, to a state of high quality delivered products. These companies not only reduce their maintenance costs, they reduce their overall maintenance costs as well.

For more specific ROI numbers for shift-left test automation, Veracode's SAST plays an important role. Forrester Research found an ROI of 206% over three years, with a real dollar return of almost \$7 million on a \$3.3 million investment. These benefits from shift-left automation included increased output per developer, decreased testing time, improved risk avoidance and bug remediation. In the Forrester Study, the tools studied removed about 20% of the bugs from the software which aligns with the direct cost avoidance savings noted in Table 3.

### The Exponential Cost of Failure

As seen above, best practices such as DevSecOps and automating SAST throughout the SDLC can produce significant savings by finding and fixing defects and vulnerabilities. The results are higher quality and more secure code that forms the foundation of the software applications or software powering your business. You will see in this section is that there are other cost considerations when measuring the ROI of using SAST solution.

### The Importance of Finding and Fixing Bugs Early

CERT Vulnerability database last year. While ensuring security and preventing possible breaches is the primary and main reason for wanting to find as many vulnerabilities in application code during development, rather than in production, there are actually other reasons why an organization would want to find and remediate as many vulnerabilities as possible during the development cycle.

The first additional reason and maybe one of the most compelling is the increased cost to remediate vulnerabilities that have made it to production. According to the NIST (the National Institute of Standards and Technologies), the cost of fixing a security defect once it's in production can be up to 60 times more expensive than during the development cycle. This is a significant increase in cost, and one that should concern most organizations.

The second additional reason to fix a defect during development is the length of time required to fix a defect once it is discovered. Veracode's 2019 "State of Software Security" report, indicated that the average amount of time to fix a software defect has gone from 59 days ten years ago, to an astounding 171 days in 2019. That's almost half a year that a vulnerability would be in production before it gets fixed if it were discovered in production, rather than during the development cycle, where it would be remediated before going to production.

DevOps Onramp

### The Shift-Left Approach to Software Development

This also isn't surprising, because typically you find bugs when you start testing, and it can be difficult without a proper infrastructure to begin testing before everything is ready.

But what we also see here is that while bugs are mostly introduced during coding, they are almost never found at that phase. What does it cost to fix these bugs?

It becomes important to understand the difference in cost to fix defects at each phase of development. This is represented in the following graph.

Now it starts to get really interesting, as we see a nasty progression of cost that dramatically increases the later the defect is found. Letting a bug sneak through to system testing is forty times the cost of finding it during coding, or ten times more costly than finding that same bug during unit testing. And it



**MYTH**

The cost to address bugs post-release costs \$16,000 to address, but a bug found at the design phase costs \$25

- Capers and Jones, Applied Software Measurement, 1997



References an earlier IBM Systems study



**MYTH**

The original project data, if any exist, are not more recent than 1981, and probably older; and could be as old as 1967

- Laurent Bossavit, Degrees of Dishonesty



**MYTH**



High-quality software is not expensive. High-quality software is faster and cheaper to build and maintain than low-quality software, from initial development all the way through total cost of ownership.

— *Capers Jones* —

**AZ QUOTES**



MYTH



High-quality software is not expensive. High-quality software is faster and cheaper to build and maintain than low-quality software, from initial development all the way through total cost of ownership.

— Capers Jones —

AZ QUOTES



**MYTH**

## CAUTION

Build your security program using facts and not myths

Think about the era of DevOps & the best appsec is the collab between developers and security teams



ODG  
TRUTH  
FLARE



# Security Bullshit Daily

## SBOMs are going to save the world

Sei un po' stanco? Se non ce ne sono abbastanza, ecco un'altra notizia che non ha nulla di nuovo e di originale. In questo mondo di notizie e di informazioni, è sempre più difficile trovare qualcosa di nuovo e di interessante. In questo mondo di notizie e di informazioni, è sempre più difficile trovare qualcosa di nuovo e di interessante.



La notizia è che, in un mondo dove la sicurezza è sempre più importante, è sempre più difficile trovare qualcosa di nuovo e di interessante. In questo mondo di notizie e di informazioni, è sempre più difficile trovare qualcosa di nuovo e di interessante.



La notizia è che, in un mondo dove la sicurezza è sempre più importante, è sempre più difficile trovare qualcosa di nuovo e di interessante. In questo mondo di notizie e di informazioni, è sempre più difficile trovare qualcosa di nuovo e di interessante.

La notizia è che, in un mondo dove la sicurezza è sempre più importante, è sempre più difficile trovare qualcosa di nuovo e di interessante. In questo mondo di notizie e di informazioni, è sempre più difficile trovare qualcosa di nuovo e di interessante.

La notizia è che, in un mondo dove la sicurezza è sempre più importante, è sempre più difficile trovare qualcosa di nuovo e di interessante. In questo mondo di notizie e di informazioni, è sempre più difficile trovare qualcosa di nuovo e di interessante.

La notizia è che, in un mondo dove la sicurezza è sempre più importante, è sempre più difficile trovare qualcosa di nuovo e di interessante. In questo mondo di notizie e di informazioni, è sempre più difficile trovare qualcosa di nuovo e di interessante.



PODGY  
TRIAL

Apache Log4j Security Vulnerabilities

This page lists all the security vulnerabilities fixed in released versions of Apache Log4j 2. Each vulnerability is given a security impact rating by the Apache Logging security team. Note that this rating may vary from platform to platform. We also list the versions of Apache Log4j the flaw is known to affect, and where a flaw has not been verified list the version with a question mark.

Log4j 1.x has reached End of Life in 2015 and is no longer supported. Vulnerabilities reported after August 2015 against Log4j 1.x were not checked and will not be fixed. Users should upgrade to Log4j 2 to obtain security fixes.

Binary patches are never provided. If you need to apply a source code patch, use the building instructions for the Apache Log4j version that you are using. For Log4j 2 these can be found in [BUILDING.md](#) located in the root subdirectory of the source distribution.

If you need help on building or configuring Log4j or other help on following the instructions to mitigate the known vulnerabilities listed here, please [subscribe to ML](#), and send your questions to the public Log4j [Users mailing list](#).

If you have encountered an unlisted security vulnerability or other unexpected behaviour that has security impact, or if the descriptions here are incomplete, please report them privately to the [Log4j Security Team ML](#). Note that reports assuming attacker's access to the Log4j configuration will not qualify as a vulnerability. Thank you for your understanding and help!

**Fixed in Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) and 2.3.2 (Java 6)**

WH.GOV

MAY 12, 2021

### Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM  
PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Section 1. Policy.** The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to

THE WHITE HOUSE

Executive Order on Improving the Nation's Cybersecurity

(1) The term "Software Bill of Materials" or "SBOM" means a formal listing containing the details and supply chain relationships of various components used in building software. Software developers and providers often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. An SBOM is useful to those who develop or manufacture software, those who select or purchase software, and those who operate software. Developers often use available open source and third-party software components to create a product. An SBOM allows the builder to make sure those components are up to date and to respond quickly to new vulnerabilities. Businesses use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product. Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability. A widely used, machine-readable SBOM format allows for greater benefits through automation and tool integration. The SBOM gains greater value when effectively stored in a repository that can be easily queried by other applications and systems. Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.

(2) The term "Zero Trust Architecture" means a security model, set of system design principles, and a coordinated cyber security and system management strategy based on an acknowledgment that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple

aqua

## Gartner® Report

**Gartner® Report: Innovation Insight for SBOMs**

Get the Report

### Innovation Insight for SBOMs Report

"SBOMs improve the visibility, transparency, security and integrity of proprietary and open-source code in software supply chains.

To realize these benefits, software engineering leaders should integrate SBOM throughout the software delivery life cycle





**MYTH**

## CAUTION

FOR TRANSPARENCY AND SO I AM NOT A HYPOCRITE, I WROTE THE OPEN SOURCE SECURITY FOUNDATION 'SBOM EVERYWHERE' SECTION OF 'THE OPEN SOURCE SECURITY MOONSHOT' THAT WE TOOK THE WHITE HOUSE



BOGGY  
TRUTH



BODGY  
TRUTH



How do they  
actually work ?

Package managers are non  
deterministic \*

There is no build provenance \*

SBOMs don't bind source code  
to binary code

Hot-loading, pot build hooks  
... sudo su

**CRITICAL:** Make Up Anything you  
want





**That's a big smelly  
CVE**





CVE & NVD data is far from complete. Far, far, far away..

The CNA is a shield for vendors

Very few developers report bugs

CVE and NVD doesn't have the data to validate or reproduce an issue and it doesn't do it!

The VAST majority of vulnerable methods in vulnerable libraries are never called

Managed by US government ?





CVE-2022-38392 - Certain 5400 RPM hard drives, for laptops and other PCs in approximately 2005 and later, allow physically proximate attackers to cause a denial of service (device malfunction and system crash) via a resonant-frequency attack with the audio signal from the Rhythm Nation music video.

A reported product is Seagate STDT4000100763649053447.





## CAUTION

We need build provenance

We need code provenance

We need robust vulnerability data



**UNETHICAL**

## **CAUTION**

**FOR TRANSPARENCY AND SO I AM NOT A HYPOCRITE, I AM BUILDING A CODE TAGGING COMPANY USED FOR SECURITY PROVENANCE AND I AM TALKING HERE BECAUSE IT RAISES THE PROFILE OF MY COMPANY.**





UNETHICAL

# Security Bullshit Daily

## Security tool benchmarks exposed as false information



Security tool benchmarks exposed as false information. The article discusses how security tool benchmarks have been found to be false information, potentially misleading users.

Security tool benchmarks exposed as false information. The article continues to discuss the implications of these findings for security professionals and users.



Security tool benchmarks exposed as false information. The article concludes with a discussion on the importance of verifying security tool performance and the potential risks of relying on unverified benchmarks.

Locali. I dati sono stati... Security tool benchmarks exposed as false information. The article discusses how security tool benchmarks have been found to be false information, potentially misleading users.

Locali. I dati sono stati... Security tool benchmarks exposed as false information. The article continues to discuss the implications of these findings for security professionals and users.





LOSER

100x

Lets win at benchmarks



UNETHICAL

Web Vulnerability Scanners Comparison - Invicti (formerly Netsparker) Confirmed a Market Leader

Table of Contents

- 1. What is the Web Application Security Scanner (DAST) Benchmark?
  1. How Are Tests Performed?
  2. Testing Vulnerability Management & Assessment Solutions
  3. The Negative Impact of False Positives
  4. False Positives Make Scaling Up Web Security Impossible
  5. Evaluation Criteria
- 2. The Benchmark Results - Global Results
  1. How Many Vulnerabilities Did the Scanners Detect?
  2. How Many False Positives Were Reported?
  3. Graph with Global Detection & False Positives Rates
- 3. The Benchmark Results - Individual Tests Results
  1. OS Command Injection Detection
  2. Remote File Inclusion / SSRF
  3. Path Traversal
  4. SQL Injection
  5. Reflective Cross-site Scripting (XSS)
  6. Unvalidated Redirect
- 4. Are Web Security Scanner Comparisons Useful & Realistic?
  1. Which is the Best Web Application Security Scanner?
  2. Can Invicti Identify Security Flaws in Your Web Applications and APIs?
- 5. Best Comparisons Between Automated Web

sectooladdict / wavsep

The Web Application Vulnerability Scanner Evaluation Project

File	Initial Commit	Time
.settings	Initial Commit v1.5	9 years ago
WebContent	Initial Commit v1.5	9 years ago
build/classes/co...	Initial Commit v1.5	9 years ago
docs	Initial Commit v1.5	9 years ago
licenses	Initial Commit v1.5	9 years ago
scripts	Initial Commit v1.5	9 years ago
src/com/sectoola...	Initial Commit v1.5	9 years ago
.classpath	Initial Commit v1.5	9 years ago
.project	Initial Commit v1.5	9 years ago
LICENSE.md	Initial Commit v1.5	9 years ago
README.md	Initial Commit v1.5	9 years ago
VERSION.md	Initial Commit v1.5	9 years ago

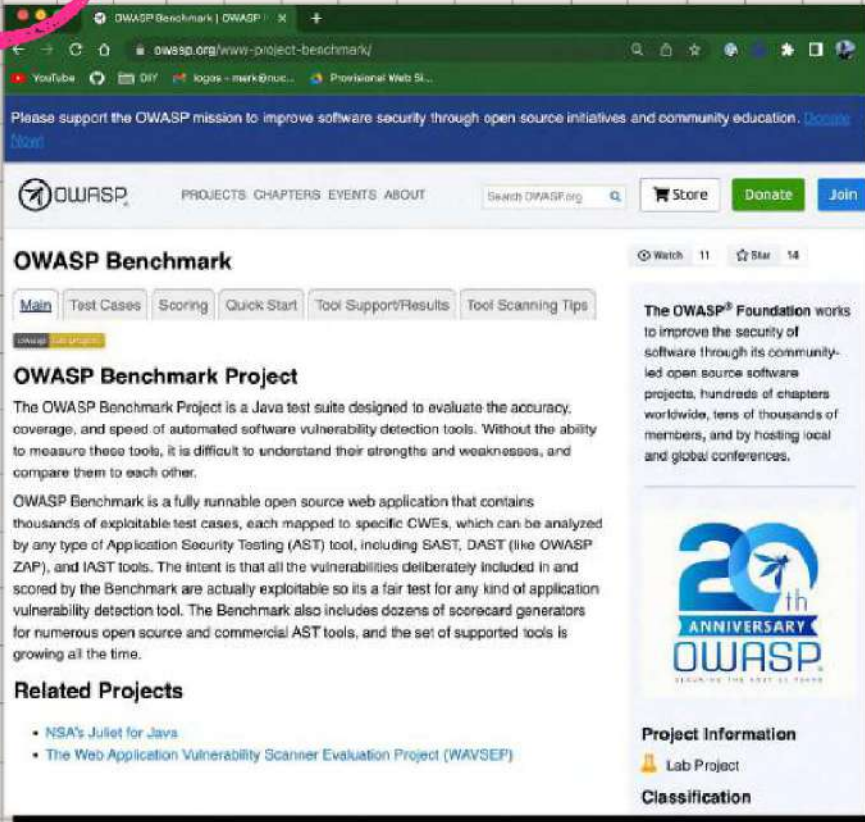
Releases: 2

- wavsep-v1.5-war (Latest) on Jun 12, 2015

Packages: No packages published



UNETHICAL



OWASP Benchmark | OWASP

Please support the OWASP mission to improve software security through open source initiatives and community education. [Donate](#)

OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Store Donate Join

## OWASP Benchmark

Main Test Cases Scoring Quick Start Tool Support/Results Tool Scanning Tips

### OWASP Benchmark Project


The OWASP Benchmark Project is a Java test suite designed to evaluate the accuracy, coverage, and speed of automated software vulnerability detection tools. Without the ability to measure these tools, it is difficult to understand their strengths and weaknesses, and compare them to each other.

OWASP Benchmark is a fully runnable open source web application that contains thousands of exploitable test cases, each mapped to specific CWEs, which can be analyzed by any type of Application Security Testing (AST) tool, including SAST, DAST (like OWASP ZAP), and IAST tools. The intent is that all the vulnerabilities deliberately included in and scored by the Benchmark are actually exploitable so its a fair test for any kind of application vulnerability detection tool. The Benchmark also includes dozens of scorecard generators for numerous open source and commercial AST tools, and the set of supported tools is growing all the time.

### Related Projects

- NSA's Juliet for Java
- The Web Application Vulnerability Scanner Evaluation Project (WAVSEP)

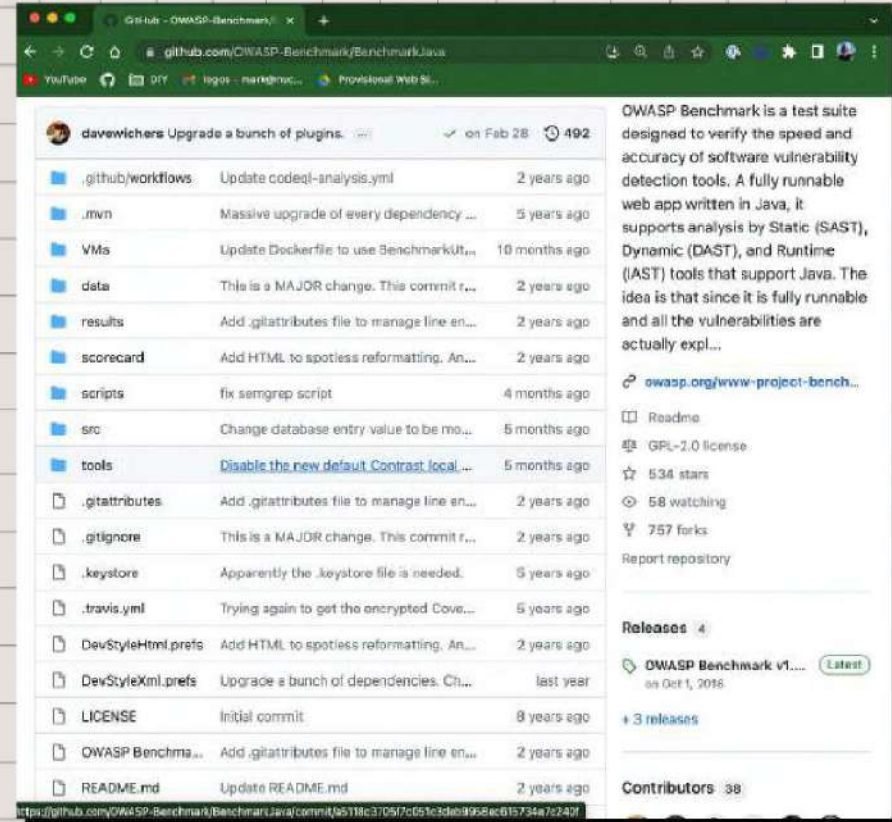
The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.



Project Information

- Lab Project

Classification



GitHub - OWASP-Benchmark/BenchmarkJava

davewichers Upgrade a bunch of plugins. on Feb 28 492

.github/workflows	Update codeql-analysis.yml	2 years ago
.mvn	Massive upgrade of every dependency ...	5 years ago
VMs	Update Dockerfile to use BenchmarkUT...	10 months ago
data	This is a MAJOR change. This commit r...	2 years ago
results	Add .gitattributes file to manage line en...	2 years ago
scorecard	Add HTML to spotless reformatting. An...	2 years ago
scripts	fix semgrep script	4 months ago
src	Change database entry value to be mo...	5 months ago
tools	Disable the new default Contrast local...	5 months ago
.gitattributes	Add .gitattributes file to manage line en...	2 years ago
.gitignore	This is a MAJOR change. This commit r...	2 years ago
.keystore	Apparently the .keystore file is needed.	5 years ago
.travis.yml	Trying again to get the encrypted Cove...	5 years ago
DevStyleHtml.prefs	Add HTML to spotless reformatting. An...	2 years ago
DevStyleXml.prefs	Upgrade a bunch of dependencies. Ch...	last year
LICENSE	Initial commit	8 years ago
OWASP Benchma...	Add .gitattributes file to manage line en...	2 years ago
README.md	Update README.md	2 years ago

OWASP Benchmark is a test suite designed to verify the speed and accuracy of software vulnerability detection tools. A fully runnable web app written in Java, it supports analysis by Static (SAST), Dynamic (DAST), and Runtime (IAST) tools that support Java. The idea is that since it is fully runnable and all the vulnerabilities are actually expl...

[owasp.org/www-project-bench...](https://owasp.org/www-project-bench...)

Readme

GPL-2.0 license

534 stars

58 watching

757 forks

Report repository

### Releases 4

OWASP Benchmark v1.0... Latest  
on Oct 1, 2018

3 releases

### Contributors 38

https://github.com/OWASP-Benchmark/BenchmarkJava/commit/95186c37057c051c3d0e9968ec615734476242f



UNETHICAL

Cyber Security Benchmark Highlights Legacy Product Failures

US Department of Homeland Security-funded project documents weak performance of application security solutions

NEWS PROVIDED BY Contrast Security → Sep 23, 2015, 08:05 ET

SHARE THIS ARTICLE

PALO ALTO, Calif., Sept. 23, 2015 /PRNewswire/ -- In August 2015, with funding support from the US DHS, the Open Web Application Security Project (OWASP) published an open source Benchmark Project on application security accuracy. The Benchmark Project allows organizations to measure the effectiveness of application security solutions by providing an application with over 21,000 test cases across 11 different attack categories; it also uses code that looks vulnerable, but isn't, to check for false alarms.

The new Benchmark Project exposes the failings of the Static Source Code (or SAST) and Dynamic Web Scanning (or DAST) product categories. The best performing products in those groups scored a discouragingly poor 33% accuracy on the

High Failure Rates of Existing AppSec Products, with One Significant Exception

Applying the benchmark application consistently across application security products produced astonishing results on the accuracy front:

- 18% accurate – Most accurate open source Dynamic Application Security Testing (DAST) product
- 17% accurate – Most accurate commercial DAST product
- 33% accurate – Most accurate open source Static Application Security Testing (SAST) product
- 33% accurate – Most accurate commercial SAST product
- 92% accurate – Contrast Enterprise, an Interactive Application Security Testing (IAST) product

Figure 1: Benchmark Accuracy Results (September 17, 2015) Accuracy scores for products across all 11 Benchmark Project vulnerability categories.

Reevaluate Application Security Products and Programs

Using the benchmark, organizations should evaluate the strengths and weaknesses of their current application security solutions, and reconsider their options. Contrast Enterprise, which the OWASP Benchmark demonstrated is both fast and accurate, is a natural choice to augment or replace existing SAST and DAST solutions. Ask your application security vendor for their benchmark results, and contact Contrast Security ([benchmark@contrastsecurity.com](mailto:benchmark@contrastsecurity.com)) to learn more about Contrast Enterprise.

About Contrast Security

Contrast Security is the world's only application security software that quickly and accurately stops hackers from stealing data via web applications – the most successful attack vector. Industry research shows that application security



**UNETHICAL**

## **CAUTION**

**We need regulated, independent security tools testing that works for today's software engineering world.**



UNETHICAL

DODGY  
TRICK

# The top ten list of bullshit top tens



**Laurea senza merito**  
Secondo un sondaggio la maggioranza dei moduli ha ammesso di aver fatto il voto per paura di contagio e non per la serietà della materia. In alcuni casi si è anche votato per non averlo.

Un sondaggio condotto da un'azienda di ricerca di mercato ha rivelato che il 70 per cento degli studenti universitari ha ammesso di aver fatto il voto per paura di contagio e non per la serietà della materia. In alcuni casi si è anche votato per non averlo.

Un sondaggio condotto da un'azienda di ricerca di mercato ha rivelato che il 70 per cento degli studenti universitari ha ammesso di aver fatto il voto per paura di contagio e non per la serietà della materia. In alcuni casi si è anche votato per non averlo.



Un sondaggio condotto da un'azienda di ricerca di mercato ha rivelato che il 70 per cento degli studenti universitari ha ammesso di aver fatto il voto per paura di contagio e non per la serietà della materia. In alcuni casi si è anche votato per non averlo.

La Repubblica 1 gennaio 2021

**Lo scudo**  
**UNA SOSTA**

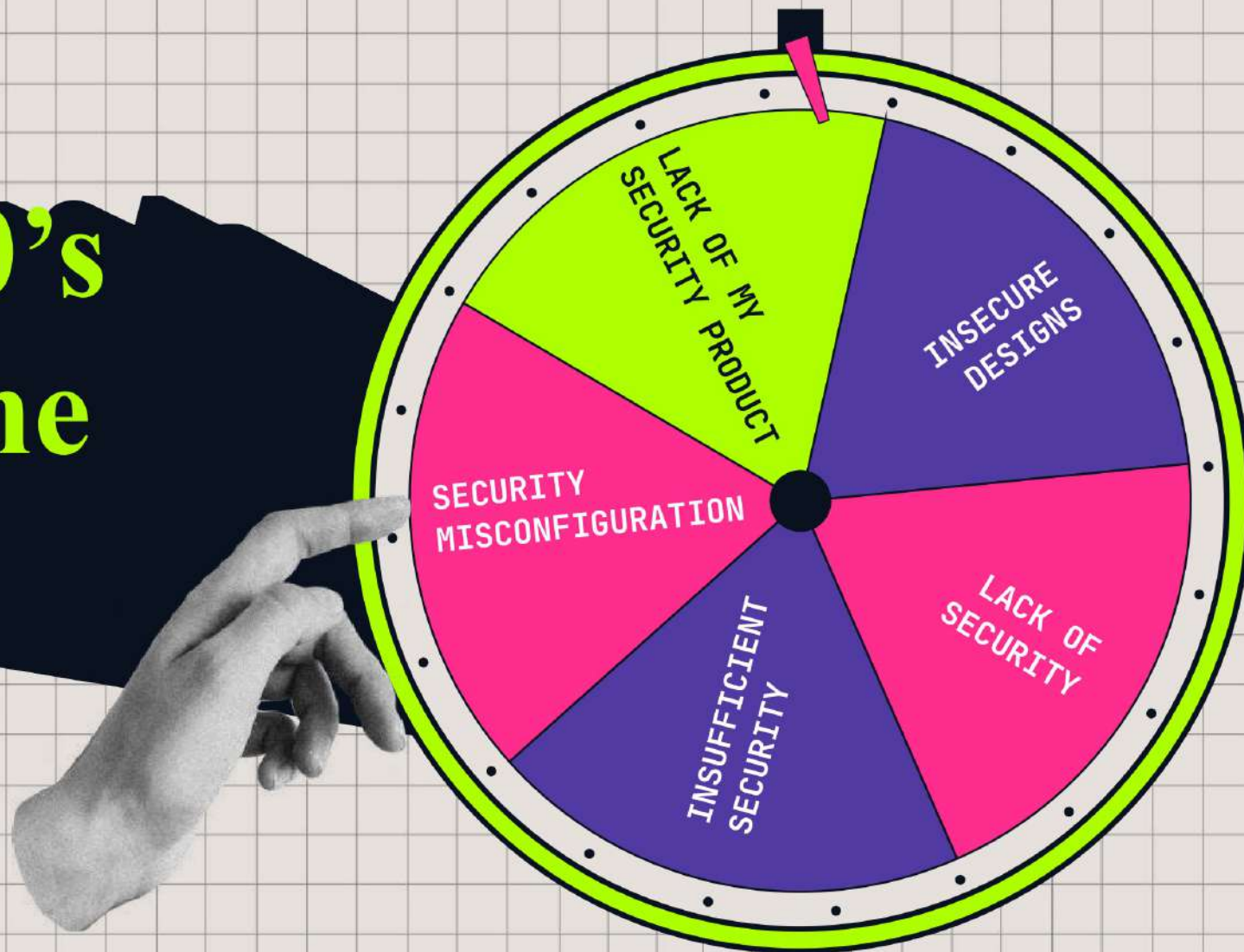
Un sondaggio condotto da un'azienda di ricerca di mercato ha rivelato che il 70 per cento degli studenti universitari ha ammesso di aver fatto il voto per paura di contagio e non per la serietà della materia. In alcuni casi si è anche votato per non averlo.

**Laurea senza merito**  
**CRISTINA RISPUGLIANI E SILVANO DI MAMMÀ**

Un sondaggio condotto da un'azienda di ricerca di mercato ha rivelato che il 70 per cento degli studenti universitari ha ammesso di aver fatto il voto per paura di contagio e non per la serietà della materia. In alcuni casi si è anche votato per non averlo.



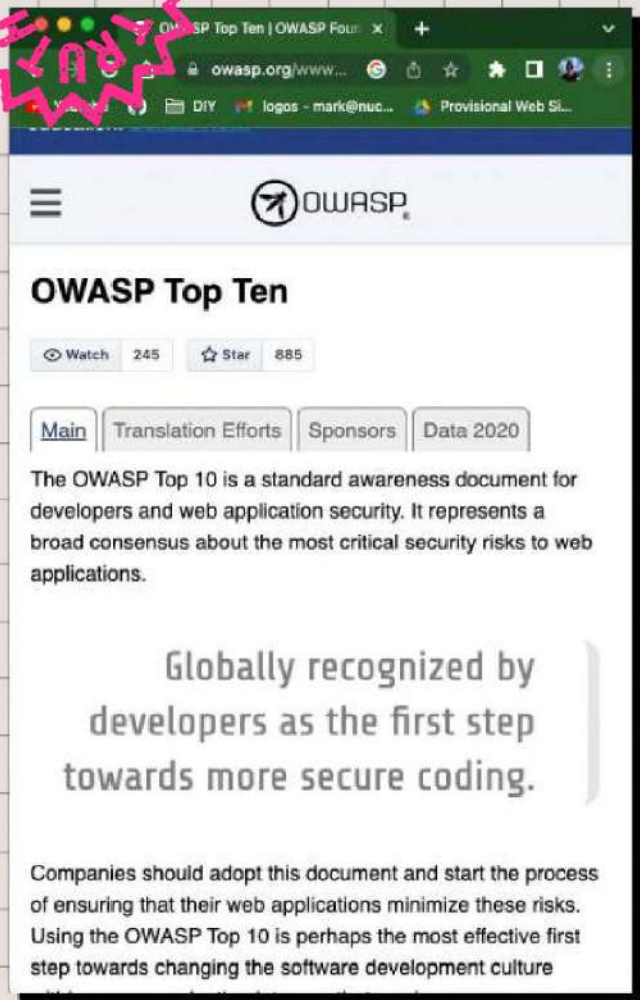
# Top 10's Fortune Wheel





UNETHICAL

DODGE  
LABS



OWASP Top Ten | OWASP Four

owasp.org/www...

DIY logos - mark@nuc... Provisional Web Sl...

Home

# OWASP

## OWASP Top Ten

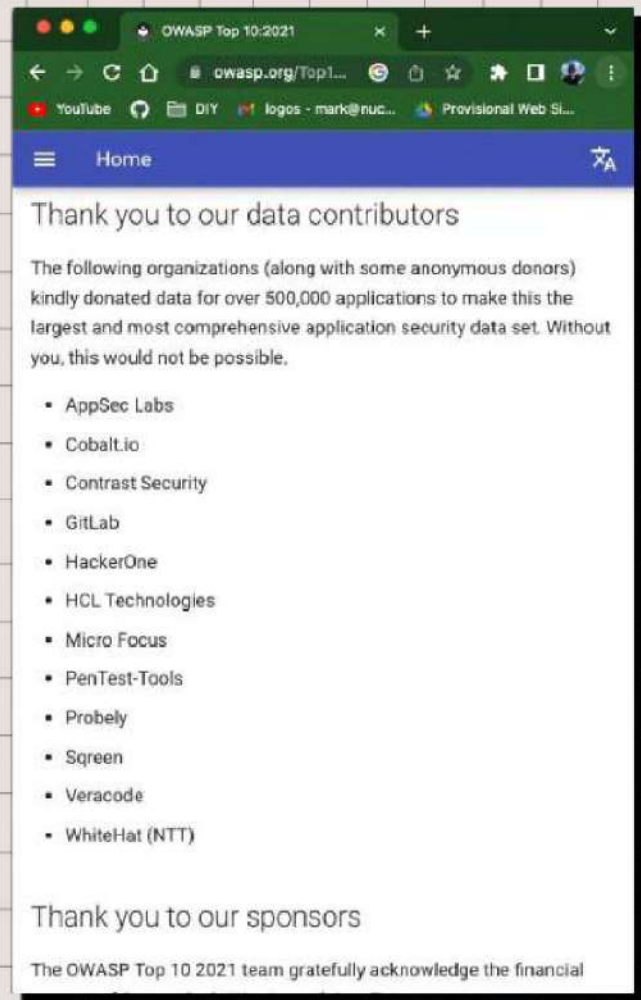
Watch 245 Star 885

Main Translation Efforts Sponsors Data 2020

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture



OWASP Top 10:2021

owasp.org/Top1...

YouTube DIY logos - mark@nuc... Provisional Web Sl...

Home

## Thank you to our data contributors

The following organizations (along with some anonymous donors) kindly donated data for over 500,000 applications to make this the largest and most comprehensive application security data set. Without you, this would not be possible.

- AppSec Labs
- Cobalt.io
- Contrast Security
- GitLab
- HackerOne
- HCL Technologies
- Micro Focus
- PenTest-Tools
- Probely
- Sqreen
- Veracode
- WhiteHat (NTT)

## Thank you to our sponsors

The OWASP Top 10 2021 team gratefully acknowledge the financial



UNETHICAL

DODGY  
TRICKS

OWASP API Security Project

What is API Security?

API Security Top 10 2019

- API1: 2019 Broken Object Level Authorization

OWASP API Security Project

Leaders

2023 Sponsors

- SEQUENCE SECURITY
- IMPART
- SALT
- TRACEABLE

2023 Contributors

2019 Contributors

OWASP Kubernetes Top Ten

About the Kubernetes Top 10

Top 10 Kubernetes Risks - 2022

- K00: Welcome to the Kubernetes Security Top Ten
- K01: Insecure Workload Configurations
- K02: Supply Chain Vulnerabilities
- K03: Overly Permissive RBAC Configurations
- K04: Lack of Centralized Policy Enforcement
- K05: Inadequate Logging and Monitoring
- K06: Broken Authentication Mechanisms
- K07: Missing Network Segmentation Controls
- K08: Secrets Management Failures
- K09: Misconfigured Cluster Components
- K10: Outdated and Vulnerable Kubernetes Components

OWASP Kubernetes Top Ten

- K06: Broken Authentication Mechanisms
- K07: Missing Network Segmentation Controls
- K08: Secrets Management Failures
- K09: Misconfigured Cluster Components
- K10: Outdated and Vulnerable Kubernetes Components
- Other Risks to Consider

Getting Involved

Licensing

Project Leaders

- Jimmy Mesiti, Co-founder & CTO at KSOC

Project Information

- Incubator Project
- Defender
- Builder
- Documentation



UNETHICAL

## CAUTION

Top Tens need to be driven by operators. Operators needs to tell consults and vendors what the biggest issues are. We can not be driven by circulation causation.





*"That's all Folks!"*

