Historical Evolution of Security Testing for Web Applications

Maxwell Francis
Independent
Auckland, New Zealand

ABSTRACT

Dynamic Application Security Testing (DAST) has become a core practice in modern cybersecurity, particularly for securing web applications, one of the most common modern software types. This research explores the historical evolution of web application security testing resources and publications over time. A key focus is the chronological focus of these works and the narrative this talks to in regard to security testing.

This study fills a gap in academic literature, as meta-analyses of technical security testing methodologies and related published works are uncommon. The only comparative work that was discovered was Doğan Et al.'s 2014 'A survey on web penetration test'. This work looked at this topic from a quantitative Structured Literature Review (SLR) approach and although effective in answering research questions, the overall study looked more to academic research trends in web security. This research expands on this to rather focus on the historical evolution over time of web security outside of academia.

Findings indicate that the late 90's, specifically around 1997, is where we see the first formal publications primarily for web security.Most formalized methodologies, training, groups and best practices for web application DAST formed between 2002 to 2008, with the use of static published guides and community knowledge being the learning standard until the mid-2010's when the rise of cyber learning and development platforms began maturing. We have plotted a chronological line of these events to better understand this evolution.

The study highlights a shift from static information-sharing mediums (whether online or print) to dynamic, web-based platforms (platforms, source-code community publications) in response to the rapidly changing security landscape. This has allowed improved the ability to access information from centralised locations rather than having to collate web security resources but also has increased the level of commercialisation due to subscriptions and courses within platforms being an increasingly popular source for web security testing thought leadership and training.

This research contributes to the academic understanding of how web application security testing has evolved over time, allowing for expansion for future analysis of application security testing, particularly in evolving education trends and methodologies.

General Terms

Security, Web Application Security Testing, Cybersecurity, Penetration Testing, Dynamic Application Security Testing (DAST), Historical Analysis

Keywords

Security Testing, Methodology, Web Application

1. INTRODUCTION

You can tell a lot about where an industry is going by analysing where it has come from. A key area in the cybersecurity industry is testing computer applications, with a key type of application constantly tested being web applications.

To analyse where web DAST has come from, we first performed a literature review of both the historical and cultural evolution of cybersecurity with focus on testing, and another view specifically on the training and publications both in text and online that teach, inform and guide on web application (DAST). We used the literature review to synthesise a timeline of web security testing that we believe is accurate and informative.

Post literature review analysis, we look to summarise the findings of our literature review and historic analysis to provide commentary in our summary section on what this has meant for security testing from both a performance, educational, and commercialization perspective.

2. LITERATURE REVIEW

2.1 Initial Keyword Searches

When looking at keyword searching for publications and knowledge material, a combination of known publications, and a collection of publications and works were collated through a keyword search across the EBSCO academic search engine using the keywords "**web application hack*" or web application security or"*penetration test*" or "web hack*" or DAST or "ethical hack*"* across all fields. The oldest publication collected in relation to web security testing guidance and methodologies was a Bugtraq posting in February of 1996 looking at CGI vulnerabilities, and the most current publication being the draft 5th version of the OWASP (Open Web Application Security Project) WSTG (Web Security Testing Guide) which was last updated in January of 2025. The unordered list below is for the most relevant literatures for this topic and identified themes:

2.1.1 Theme: Historical and Cultural Evolution of Cybersecurity

This theme looks to describe the historical documentation of how cybersecurity originated and matured as an industry:

- Study 1: **History of US Government Investments in Cybersecurity Research: A Personal Perspective**[1]. Conducted a qualitative analysis through a personal perspective. Landwehr concluded that there was a steady and significant year-on-year increase in U.S. federal cybersecurity funding during that mid-2000s to early-2010s time frame, even if some agencies' budgets fluctuate in specific years.

- Study 2: **Hacking - Tracing the History: What Can India Do with Its Hackers?**[2]. Coupled well-known cybersecurity timeline events with data analysis of Indian CERT (CERT-in) annual report statistics. This report focused on the events of phone phreaking in the 1960's till 2016, and identified the necessity of fostering attackers internal to India to help uplift and grow India's nation state cybersecurity capabilities.
- Book 1: **The History of Information Security**[3]. Was conducted as a first field survey, broken up by twenty-eight contributions. This publication looks at information security at the broadest level, beginning on the first treatise on cryptanalysis prior to computers in the 9th century by the Christian Arab philosopher Al Kindi, and moving throughout history up to the late 90's to early 2000's where cryptography intersected with privacy laws such as the 1990 European Directive on Data Protection. This publication is informative in framing web application security testing within its short timeline in conjunction with the wider history of information security (both with and without computers).
- Book 2: **Hackers: Heroes of the Computer Revolution**[4]describes a cultural tipping point around the tinkering MIT hacker culture and start of the 1975 infamous Homebrew Computer Club. This publication took a humanistic historical account of hacking social groups, with this book initially published seven years prior to the first web application created in 1991.
- Book 3: **Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World**[5]Which is a cultural account which follows after the timeline of Hackers: Heroes of the Computer Revolution to show the forming of hacking interest groups and initial knowledge sharing to collaborate on sophisticated exploits such as the Back Orifice 2000 (BO2k) program released in 1999 DEF CON.

2.1.2 Theme: Web Application Testing and Methodology Publications

This theme looks to describe the practical publications that have been released specifically to aid and educate IT professionals on how to test web applications to discover security vulnerabilities:

- Study 3: **Web application testing: A systematic literature review** [6]
- Book 4: **Web Security, Privacy & Commerce**[7] with the first of two editions being published in 1997 which makes this one of the first ever formal publications related to web security. Although the book does not specifically call out specific testing techniques and methodologies, what Garfinkel and Spafford do is assess the risk of commerce being introduced to the web at the time and mention various security technologies and their subsequent bypasses.
- Book 5**: Hacking Exposed:Web Applications 1st Edition**[8] Having been first published in 2002 is one of the earliest complete education and methodology resources for hacking web applications as web software designs began to become more complicated from a functionality and architecture perspective. Later editions were published with the last publication being the 3rd edition, published in 2010
- Book 6: **How to Break Web Software: Functional and Security Testing of Web Applications and Web Services**[9] is a publication referenced in the later Web Security Testing Cookbook and from initial review is seen to more related to practice hands on testing like the latter The Web Application Hackers Handbook.
- Book 7: **The Web Application Hacker's Handbook**[10] Arrived slightly later but followed the same purpose and format to the Hacking Exposed publication. A lot of the material developed within this publication was used by the author Dafydd Stuttard to later publish the initial Portswigger Web Security Academy web platform.
- Book 8: **Web Security Testing Cookbook**[11]is similarlike the above except with more of a focus of developing security tests on specific areas into repeatable codified software tests in a DevSecOps approach.
- Electronic source 1: **Bugtraq mailing list, specifically 'CGI security: Escape newlines'** [12] in Feb of 1996 was the first discovered mention specifically of web application attacks that featured injection of file inclusion within a URL parameter. Although this is a singular web attack method, this does show that information around web hacking was being disseminated well before OWASP or any formal publication of any kind.
- Electronic Source 2: **The OWASP Testing Project**[13] which by all accounts is the first OWASP testing frameworks published in 2004 and did not include any education on how to test or exploit vulnerabilities but instead assisted in performing higher level web security reviews through selection criteria for when to get a penetration test and understanding elements like operational management reviews and threat modelling. The last commit before the related opensource git repository was archived was in 2015 [14].
- Electronic Source 3: **The OWASP Web Security Testing Guide**[15] was the success to the above testing project which features more specific testing techniques and a defined process through the methodology to select and test specific web applications components and features. The initial source git commit message for the public WSTG repository began in 2017. Much of modern OWASP focuses on a set of core materials with WSTG being one of the most important of these.
- Electronic Source 4: **TryHackMeCyber Training Platform**[17] was first founded in 2018 and is one

of a group of platforms designed to incorporate cloud hosted labs, video, practical testing and online text. TryHackMe utilized the concept of "rooms" where each room covers a theme, topic, or objective, with multiple related official rooms usually making up learning paths.

- Electronic Source 5: **Hack The Box** [17]is a similar training platform to TryHackMe that works on more individualized offerings, such as non-guided rooms, an academy style guided courseware, and certifications. Hack The Box was founded in 2017.

- Electronic Source 6: **Pentesting with Backtrack**[18] is the original 2006 coursework that was the study material alongside the OSCP exam. Although not strictly related to web application testing, every version of this coursework has featured a dedicated section to web attacks and a methodology to test potentially vulnerable systems.

- Electronic Source 7: **HackThisSite**[19] was a pioneer in utilizing a web platform and community to teach and share web application testing techniques. HackThisSite was first introduced in 2003, over a decade before similar competitor platforms would arrive offering a better testing education and development experience.

2.2 SYNTHESIS OF LITERATURE REVIEW

There were three core periods of grouped activity that shaped web application security to be the industry and practice it is today. These being between 1996 to 2000 which saw the beginning of web application publications as evidenced by Bugtraq archives maintained by seclists.org, and Garfinkel and Spafford's Web Security and Commerce via O'Reilly publishing.

The second period activity occurred from 2001 and 2005 which saw the founding of the OWASP according to archived web resources. Additional to OWASP we saw an increase in publishing, and the precursor to web security training platforms in Jeremy Hammond's HackThisSite.org. Stuttard and Pinto also release their initial guidance in The Web Application Hacker's Handbook later in 2008.

Our final evolution occurred in 2017 to 2021 with the majority of modern DAST training platforms both in relation to web and broader systems being released. At the same time literature and internet archive timestamps indicate the release of web security certifications.

Unfortunately, there is little in the way of similar research looking into this area of assessing web security history and research. Of all EBSCO collated research, we only found Doğan Et al.'s 2014 'A survey on web penetration test' [7] to be of relevance. This piece was quite detailed in quantity collected and did well to taxonomise research into web security. The two areas however that this research fills over the above is that we can assess the publication of both books and training platforms to provide commentary due to the more qualitative nature of this study. Additionally, Doğan's work was published in 2014 which between then and now has seen updates in web security training and methodologies.

Looking at the collection of literature in relation to web security DAST, we noticed that initial publications and material were mostly only available through large reference textbooks, with literature moving more to web blogs, articles, and platforms. The core literature collected are mapped below as a time graph.

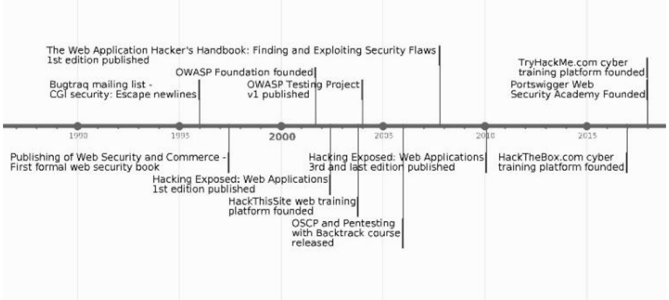

Fig 1: A visual timeline graph of key DAST for Web Application events from 1996 to 2018

We believe the reason the medium of the literature evolved was out of industry necessity. Due to countermeasures, web frameworks, and common attack methods constantly rising (broken access control due to more complex access control and permission systems in apps) and falling (SQL injection due to better ORM's and database query methods), we believe the industry sought to maintain their common body of knowledge via easy to edit and maintain web documents and source controlled projects. It is drastically easier to update a source-controlled text than republish a book.

Another trend that we noticed is the sudden commercialization of knowledge and methodologies for web security testing and training. Before when one could 'own' the information via a publication or OWASP guideline, we are now seeing subscription-based platforms and a push to technical certifications. We believe this is to absorb the modernization cost and due to the value these groups provide in continuously updating techniques and methodologies, and then providing this information along with other features such as labs, videos, and performance tracking. For the uninitiated looking to 'break into' security, the ease in which to find and apply web security DAST methodologies and techniques has improved drastically in 2025 when compared to 2016 and earlier.

3. SUMMARY

Web application Dynamic Application Security Testing (DAST) first came into the public sphere in 1996 and since then has seen evolutions with a first stage of publications and pioneers in 2002 to 2005, and later a commercialization and introduction of security testing training and development platforms a decade later in 2015 onwards.

With the accessibility of guidance and methodologies we see a positive future towards more researchers and contributors learning and developing how we test one of societies most utilised software types. A bleaker perspective is due to the adoption of certifications and subscription based platforms, coupled with increasing complexity, there may be a increased difficulty spike from both an effort and financial perspective to learn and contribute to web application DAST.

3.1 Proposed Future Research

This research was done within the focused tunnel of only analysing the history and evolution of web application testing (specifically hands on exploitation), however there are other areas that could be looked at, if not the whole discipline of penetration testing and/or 'red teaming'. There is scope to investigate new novel security testing methodologies. One such example could be leveraging known methods of design and agile practices based on security testing requirements. Specific exploitation methods (i.e. Log4j injection via LDAP and JNDI) come and go, while methodologies afford themselves better to academic rigor in conjunction with applying said methodologies into practice to ensure academic ideas reflect reality.

4. ACKNOWLEDGMENTS

It’s noticeable through doing this research that multiple people and organisations have offered training and material for web testing for free or at low cost to aid society, and feel this selflessness needs acknowledgement.I’dalso like to thank my mum Colleen, my sister Elise, my partner Kathleen, and the New Zealand Cybersecurity Community.

5. REFERENCES

[1] C. E. Landwehr, "History of US Government Investments in Cybersecurity Research: A Personal Perspective," in 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA , 2010.

[2] E. Dilipraj, "Hacking - Tracing the History: What Can India Do with Its Hackers?," Liberal Studies 1 Liberal Stud, vol. 1, no. 2, pp. 239-258, 2016.

[3] K. De Leeuw and J. Bergstra, The History of Information Security - A Comprehensive Handbook, Amsterdam: Elsevier B.V, 2007. Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] S. Levy, Hackers: Heroes of the Computer Revolution, New York City: Anchor Press, 1984.

[5] C. o. t. D. C. H. t. O. H. S. M. J. S. t. World, Menn, Joseph, PublicAffairs, 2019. Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[6] S. Doğan, A. Betin-Can and V. Garousi, “Web application testing: A systemic literature review” Journal of Systems and Software, vol. 91, pp. 174-201, May. 2014, doi: 10.1016/j.jss.2014.01.010

[7] G. Spafford and S. Garfinkel, Web Security, Privacy & Commerce, Sebastopol: O'Reily , 1997.

[8] J. Scambray and M. Shema, Hacking Exposed: Web Applications, New York: McGraw-Hill Osborne Media, 2002.

[9] M. Andrews and J. Whittaker, How to Break Web Software: Functional and Security Testing of Web Applications and Web Services, Boston: Addison-Wesley Professional, 2006.

[10] D. Stuttard and M. Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley, 2007.

[11] P. Hope and B. Walther, Web Security Testing Cookbook, Sebastopol: O'Reilly Media, 2008.

[12] C. s. E. newlines., "CGI security: Escape newlines.," 5 Feb 1996. [Online]. Available: https://seclists.org/bugtraq/1996/Feb/16.

[13] The OWASP Foundation, "The OWASP Testing Project," The OWASP Foundation, Maryland, 2004.

[14] andrewwmuller, "Commit 8193439 - Create 4.2.10 Map Application Architecture (OTG-INFO-010).md," 1 Sep 2015. [Online]. Available: https://github.com/OWASP/OWASP-Testing-Guide/commit/8193439baa2359d79fc59f8084c8d3222d7abd67.

[15] The OWASP Foundation, "OWASP Web Security Testing Guide," 2020 (4.2 release). [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/. [Accessed March 2025].

[16] Tryhackme Ltd, "TryHackMe Cyber Training," Tryhackme Ltd, 2018. [Online]. Available: https://tryhackme.com. [Accessed 03 2025].

[17] Hack The Box Ltd, "All About Hack The Box," Hack The Box Ltd, 2017. [Online]. Available: https://www.hackthebox.com/about-us. [Accessed March 2025].

[18] Offensive Security Ltd., "Penetration Testing with Backtrack v3.2," 2010. [Online]. Available: https://theswissbay.ch/pdf/Whitepaper/Penetration%20Testing%20with%20BackTrack%20%28Lab%20Guide%29%20v3.2%20-%20Offensive%20Security.pdf. [Accessed 2025].

[19] J. Hammond, "HackThisSite," 13 October 2003. [Online]. Available: http://web.archive.org/web/20031212033008/http://www.hackthissite.org/. [Accessed March 2025].