Reducing Attack Surface of a Web Application by Open Web Application Security Project Compliance

Sumit Goswami  
Directorate of Management Information System & Technologies, DRDO, New Delhi

Nabanita R Krishnan  
Directorate of Management Information System & Technologies, DRDO, New Delhi

Mukesh Verma  
Directorate of Management Information System & Technologies, DRDO, New Delhi

Saurabh Swarnkar  
IAP Company Pvt Ltd, Gurgaon

Pallavi Mahajan  
Beant College of Engineering and Technology, Punjab

DOI: https://doi.org/10.14429/dsj.62.1291

Keywords: Attack surface, DRDO Intranet, project management, open web application security project, security audit, security compliance

Abstract

The attack surface of a system is the amount of application area that is exposed to the adversaries. The overall vulnerability can be reduced by reducing the attack surface of a web application. In this paper, we have considered the web components of two versions of an in-house developed project management web application and the attack surface has been calculated prior and post open web application security project (OWASP) compliance based on a security audit to determine and then compare the security of this Project Management Application. OWASP is an open community to provide free tools and guidelines for application security. It was observed that the attack surface of the software reduced by 45 per cent once it was made OWASP compliant. The vulnerable surface exposed by the code even after OWASP compliance was due to the mandatory access points left in the software to ensure accessibility over a network.


Author Biographies

Sumit Goswami, Directorate of Management Information System & Technologies, DRDO, New Delhi

Mr Sumit Goswami obtained his MTech (Comp. Sci. & Engg.) from IIT Kharagpur. Presently working as Scientist ‘E’ at DRDO, New Delhi. His areas of interest include network centric operations, mobile ad hoc and sensor networks, web-hosting security, text mining and machine learning. He has published 53 papers/chapters in various journals, books, data competitions and conferences.

Nabanita R Krishnan, Directorate of Management Information System & Technologies, DRDO, New Delhi

Ms Nabanita Radhakrishnan obtained her BTech (Elect. & Comm. Engg.) from Guindy Engineering College, Chennai and M Tech (Electrical Engg.) from IIT Madras. Presently working as Director, Management Information System and Technologies (MIST) at DRDO Hqrs, New Delhi. In this capacity she has conceptualized and commissioned an upgraded DRDO Intranet with a multi-tier security infrastructure and a number of software applications. She is a Member of Aeronautical Society of India and Instrument Society of India.

Mukesh Verma, Directorate of Management Information System & Technologies, DRDO, New Delhi

Mr Mukesh obtained his MCA from IGNOU, Delhi and MSc (Computer Science) from MDU Rohtak. Presently working as Senior Technical
Assistant at DRDO HQr. His research area include: Software development, website designing and hosting, Linux, Windows, MySQL, JAVA, JSP, ORACLE, Crystal Report, Visual Basic, and PHP.

Saurabh Swarnkar, IAP Company Pvt Ltd, Gurgaon
Mr Saurabh Swarnkar obtained his BE (Comp.Sci. & Engg.) from Institute of Information Technology and Management, Gwalior, and PGDAC from CDAC- Advance Computing Training School, Bengaluru. Presently working as a Programmer in IAP Company Ltd, Gurgaon. His research area include: Developing web application, web designing and hosting.

Pallavi Mahajan, Beant College of Engineering and Technology, Punjab
Ms Pallavi Mahajan is pursuing BTech (Computer Science and Engineering) from Beant College of Engineering and Technology, Gurdaspur, Punjab. She is presently doing 6 months internship from DRDO, New Delhi.

References


Heumann, Thomas; Türpe, Sven & Keller, Jörg. Quantifying the attack surface of a web application. In Proceedings of Sicherheit’2010, July 2011, LNI, 170, pp.305-316,


September 2011).


Manadhata, Pratyusa; Wing, Jeannette; Flynn, Mark & McQueen, Miles. Measuring the attack surfaces of two FTP daemons. In Proceedings of the 2nd ACM workshop on Quality of protection, 2006, Virginia, USA, October 2011.


The attack surface of a system is the amount of application area that is exposed to the adversaries. The overall vulnerability can be reduced by reducing the attack surface of a web application. It was observed that the attack surface of the software reduced by 45 per cent once it was made OWASP compliant. The vulnerable surface exposed by the code even after OWASP compliance was due to the mandatory access points left in the software to ensure accessibility over a network. Defence Science Journal, 2012, 62(5), pp.324-330, DOI:http://dx.doi.org/10.14429/dsj.62.1291. Author Biographies. The Open Web Application Security Project (OWASP) has consistently reported since 2010 that almost every web-based application has one or more vulnerabilities listed in their Top 10 list of application security risks. They have also reported that 95 percent of all websites are attacked annually using cross-site scripting and injection techniques. Web application security threats. Public facing applications are attractive targets. Only a web application firewall can provide complete application protection by understanding application logic and what elements exist on the web application such as URLs, parameters, and what cookies it uses. to help protect an organization’s dynamic attack surface Flexible form factors to help support various industry requirements. 6.