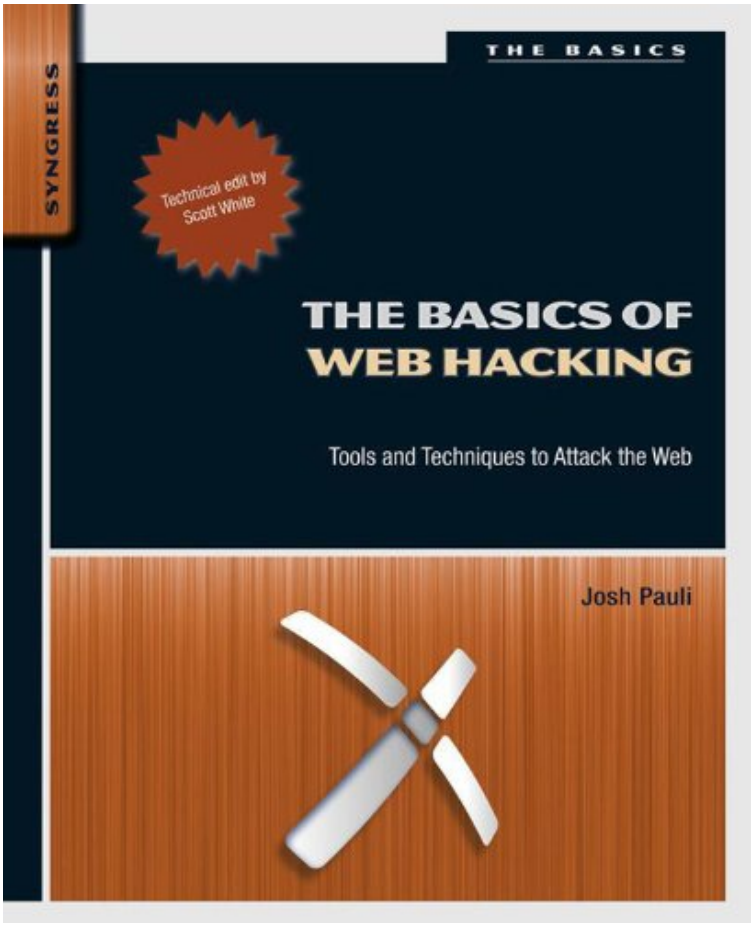
The Basics of Web Hacking: Tools and Techniques to Attack the Web

Von Josh Pauli
**Download PDF | ePub | DOC | audiobook | ebooks*



Produktinformation -Verkaufsrang: #747610 in eBooksVerffentlicht am: 2013-06-18Erscheinungsdatum: 2013-06-18File Name: B00DZ48KH8 | File size: 23.Mb

Von Josh Pauli : The Basics of Web Hacking: Tools and Techniques to Attack the Web before purchasing it in order to gage whether or not it would be worth my time, and all praised The Basics of Web Hacking: Tools and Techniques to Attack the Web:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. Not up to dateVon MidnatsolThis book is a pretty good introduction to web hacking. However, examples and exercises are based on BackTrack Linux, which is no longer being maintained and available for download. Kali Linux can be used instead.

KurzbeschreibungThe Basics of Web Hacking introduces you to a tool-driven process to identify the most widespread

vulnerabilities in Web applications. No prior experience is needed. Web apps are a "path of least resistance" that can be exploited to cause the most damage to a system, with the lowest hurdles to overcome. This is a perfect storm for beginning hackers. The process set forth in this book introduces not only the theory and practical information related to these vulnerabilities, but also the detailed configuration and usage of widely available tools necessary to exploit these vulnerabilities. The Basics of Web Hacking provides a simple and clean explanation of how to utilize tools such as Burp Suite, sqlmap, and Zed Attack Proxy (ZAP), as well as basic network scanning tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more. Dr. Josh Pauli teaches software security at Dakota State University and has presented on this topic to the U.S. Department of Homeland Security, the NSA, BlackHat Briefings, and Defcon. He will lead you through a focused, three-part approach to Web security, including hacking the server, hacking the Web app, and hacking the Web user. With Dr. Paulis approach, you will fully understand the what/where/why/how of the most widespread Web vulnerabilities and how easily they can be exploited with the correct tools. You will learn how to set up a safe environment to conduct these attacks, including an attacker Virtual Machine (VM) with all necessary tools and several known-vulnerable Web application VMs that are widely available and maintained for this very purpose. Once you complete the entire process, not only will you be prepared to test for the most damaging Web exploits, you will also be prepared to conduct more advanced Web hacks that mandate a strong base of knowledge.Provides a simple and clean approach to Web hacking, including hands-on examples and exercises that are designed to teach you how to hack the server, hack the Web app, and hack the Web user Covers the most significant new tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more! Written by an author who works in the field as a penetration tester and who teaches Web security classes at Dakota State UniversityPressestimmen"" this first work shows the love of an eager first-time author who has an obvious passion about the subject matter. it is a good starting point for someone who has little or no exposure to web attacks. Anyone who wants a gentle introduction with a low bar to entry that bridges the gap between his knowledge and more advanced texts, will likely find this book useful."--""The Ethical Hacker Network online, " October 10, 2013""This is a book about techniques one can use to break into web servers, browsers, and applications. Its intended audience is not criminals or spies, however, but white hat hackers who attempt to break into their own organization's IT resources with permission and the goal of securing those resources against just these kind of attacks when they are made with hostile intent "--""Reference Research Book News, " December 2013 "" this first work shows the love of an eager first-time author who has an obvious passion about the subject matter. it is a good starting point for someone who has little or no exposure to web attacks. Anyone who wants a gentle introduction with a low bar to entry that bridges the gap between his knowledge and more advanced texts, will likely find this book useful."--""The Ethical Hacker Network online, " October 10, 2013"""There are lots of how-to examples and exercises and each covers the main tools in their respective spaces The books are meant as a starting guide and do meet that goal. For the serious beginner interested in the topics, these are two good guides to get you on your way."--""RSAConference.com, " May 13, 2014 ""This is a book about techniques one can use to break into web servers, browsers, and applications. Its intended audience is not criminals or spies, however, but white hat hackers who attempt to break into their own organization's IT resources with permission and the goal of securing those resources against just these kind of attacks when they are made with hostile intent "--""Reference Research Book News, " December 2013 "" this first work shows the love of an eager first-time author who has an obvious passion about the subject matter. it is a good starting point for someone who has little or no exposure to web attacks. Anyone who wants a gentle introduction with a low bar to entry that bridges the gap between his knowledge and more advanced texts, will likely find this book useful."--""The Ethical Hacker Network online, " October 10, 2013"."."."this book does provide an excellent introduction to the subject, and does so in a very practical way that explains the issues and techniques very clearly. Even if you re not interested in becoming a hacker (or penetration tester) it s a worthwhile read if you want to understand the problem..." - Network Security, August 2013""..".this book does provide an excellent introduction to the subject, and does so in a very practical way that explains the issues and techniques very clearly. Even if you re not interested in becoming a hacker (or penetration tester) it s a worthwhile read if you want to understand the problem..."--""Network Security, "August 1 2013"..".this book does provide an excellent introduction to the subject, and does so in a very practical way that explains the issues and techniques very clearly. Even if you're not interested in becoming a hacker (or penetration tester) it's a worthwhile read if you want to understand the problem..."--Network Security, August 1 2013-...this book does provide an excellent introduction to the subject, and does so in a very practical way that explains the issues and techniques very clearly. Even if you're not interested in becoming a hacker (or penetration tester) it's a worthwhile read if you want to understand the problem...---Network Security, August 1 2013KurzbeschreibungThe Basics of Web Hacking introduces you to a tool-driven process to identify the most widespread vulnerabilities in Web applications. No prior experience is needed. Web apps are a "path of least resistance" that can be exploited to cause the most damage to a system, with the lowest hurdles to overcome. This is a perfect storm for beginning hackers. The process set forth in this book introduces not only the theory and practical information related to these vulnerabilities, but also the detailed configuration and usage of widely available tools necessary to exploit these vulnerabilities. The Basics of Web Hacking provides a simple and clean explanation of how to utilize tools such as Burp Suite, sqlmap, and Zed Attack

Proxy (ZAP), as well as basic network scanning tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more. Dr. Josh Pauli teaches software security at Dakota State University and has presented on this topic to the U.S. Department of Homeland Security, the NSA, BlackHat Briefings, and Defcon. He will lead you through a focused, three-part approach to Web security, including hacking the server, hacking the Web app, and hacking the Web user. With Dr. Paulis approach, you will fully understand the what/where/why/how of the most widespread Web vulnerabilities and how easily they can be exploited with the correct tools. You will learn how to set up a safe environment to conduct these attacks, including an attacker Virtual Machine (VM) with all necessary tools and several known-vulnerable Web application VMs that are widely available and maintained for this very purpose. Once you complete the entire process, not only will you be prepared to test for the most damaging Web exploits, you will also be prepared to conduct more advanced Web hacks that mandate a strong base of knowledge.Provides a simple and clean approach to Web hacking, including hands-on examples and exercises that are designed to teach you how to hack the server, hack the Web app, and hack the Web user Covers the most significant new tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more! Written by an author who works in the field as a penetration tester and who teaches Web security classes at Dakota State University