Web Application Attacks - Preview

Dear readers,

In October there were a few opportunities to celebrate important events related to cybersecurity. First, it was the 16th year of spreading cyber security awareness among institutions, govemerents, and people in general. We also celebrated the Internet’s 50th birthday! That’s a big milestone! Did you know that the first message sent contained only two letters? They were *lo* (it was supposed to be *login,* but system only processed the first two letters) and the system crash during sending process :) But in the end everything worked out perfectly. And thanks to that, today we can present you yet another edition of Hakin9!

We decided to focus on one of the most popular topics, Web Application Attacks. We have a few really amazing articles that will show you a completely different perspective on this area and hopefully let you understand how specific attacks are performed.

We start with an article presenting one of the most well known attacks, Cross Site Scripting, by Washington Almeida. I could write an entire article about Washington’s achievements and experience. You can find his articles in many of our editions and each presents the highest quality possible. This time Washington focused on cross site scripting attacks and same origin policy. To put his idea in practice, he prepared a lab for your studies. The article is worth reading through, to later on test its findings in your own lab.

Now that we know a lot more about XSS, we go to the next publication. *Helping customers understand the risks of Cross-Site Scripting attacks through a demo* is an article written by our avid reader, Eduardo Parra San Jose. We will approach XSS attacks from a completely different perspective. As a penetration tester you have to present your findings to customers or the developer team. How to do it? With Eduardo’s help you will get a great demo which is both understable and effective. It’s a must-have lecture for all professional security specialists.

Looking for a more hands-on experience? Hamdi Sevben shared with us his examples of web application attacks. In this article the focus is on using the Burp Suite (among other tools) to perform such attacks on a platform created purely to test your skills. With Hamdi’s help you will level up your web app attack skills in no time.

Knowing how XSS works and what tools are best to use for a web app attack, next we will read about XML External Entities. This attack exploits a weakness in the user's input processing phase, when the web application accepts an XML document as input. But that’s not all, while reading the article you will analyze the two following scenarios: XXE in-band and XXE out-of-band.

But we are only halfway through the magazine! There are still plenty of articles we have for you. Another one was prepared by Hubert Demercado and Elzer Pineda. In their case scenario you will see how they used a technique they came up with that allowed them to increase the probability of success on obtaining a remote shell. Their goal was to totally compromise the server by placing obfuscated code that allows bypassing antivirus detection.

If you prefer different topics, we have something for you as well. Hardware Hacking by Felipe Hifram, Deivison Franco and Leandro Trindade, to start - the authors, present an experiment, in which they show how to break/modify the existing hardware on various examples. We don’t want to spoil the fun, because it’s an extremely engaging lecture.

Ever heard about Wardriving? We have something more than a simple tutorial about it for you. Paul Mellen, our amazing reviewer and author, prepared a massive guide about this technique. All his materials are based on the latest amazing reviewer and author, prepared a massive guide about this technique. All his materials are based on the latest software and hardware, so everything is up to date. Trust me, you will enjoy enjoy this article, and we heard rumors a second part is coming!

There is also an article about OSINT techniques: “How exposed are we on the internet?”, where we take a closer look at Signature-based Intrusion Detection System and its flaws, we will once again focus on IoT and its connections to automotive industry.

It’s a very long edition, but we hope that those tutorials will brighten your (almost) winter evenings with interesting labs and hacking techniques.

Feel free to leave us a comment or send us a message! As always, special thanks to all of the contributors, reviewers, and proofreaders involved in the process of creation of this issue.

Enjoy the reading,

Hakin9 Editorial Team

TABLE OF CONTENTS

Web Application Attacks – Cross Site Scripting (XSS)

Washington Almeida

Understanding the Cross-Site Scripting (XSS) attack class requires understanding how and why this vulnerability is present on thousands of web pages around the globe. When we talk about web page security, there is a concept known as Same Origin Policy (SOP), which forbids that a web application retrieve content from pages with another origin. This means that by prohibiting access to cross-origin content, random sites may not be able to read or modify data from your personal page of your social network or other financial transaction account, for example, while you are connected to them.

Helping customers understand the risks of Cross-Site Scripting attacks through a demo

Eduardo Parra San Jose

In this article, instead of showing just an alert box as a proof of concept and then a bunch of text describing the impact of cross-site scripting attacks, I would like to share a demo that has helped me to better communicate the impact of cross-site scripting attacks to our customers and their developer teams. The idea is to start by making a brief, informal high-level introduction to cross-site scripting attacks and then code some easy, reproducible example that I hope will help show your customers why it is important to fix the findings in the reports we deliver to them.

Web App Hacking Examples

Hamdi Sevben

We'll skip the theoretical parts and make scenarios of examples of web attacks. As it is forbidden to attack any site owner without written consent, we can make attacks on presented in the article platform.

XML External Entities (XXE)

by Angelo Anatrella

In this article, we will examine a web attack that is still little known, despite the fact that it is in fourth place within the OWASP top ten 2017. This attack exploits a weakness in the user's input processing phase when the web application accepts as input an XML document. After examining the basic structure of an XML, we will analyze the following two scenarios.

Undetectable Webshells on Penetration Tests Engagements

Undetectable Webshells on Penetration Tests Engagements

Hubert Demercado, Elzer Pineda

In several digital intrusion tests, our team has managed to identify servers that allow you to upload files and take control of them. Now there are two security controls to be defeated: 1. Antivirus and 2. intrusion prevention systems. Both can eliminate the probability of success of compromising our target. In this article, we will explore one of the techniques that allow us to increase the probability of success on obtaining a remote shell. The goal is to totally compromise the server by placing obfuscated code that allows us to bypass antivirus detection.

Hardware Hacking

Felipe Hifram, Deivison Franco, Leandro Trindade

If you want to break into a piece of hardware, the way you approach it depends on what you are trying to do. Are you trying to make it wireless? Are you trying to change what is displayed? Are you trying to get it to trigger another device? Each intrusion requires a different angle of attack and it is difficult to decide how to proceed if you have never invaded a device before. Following are some common hardware intrusion methods and the implementations in which they are used. This is by no means a "how to hack hardware" tutorial. This article could not exist completely. The nature of hacking insists that there is always a new creative way to solve it, but these are some common methods I've used in my experiments.

Wardriving, rebooted and updated, part 1, let’s get started!

Paul Mellen

Combination of Raspberry Pi 4 Model B and the new version of Kismet that this article covers, with a full and comprehensive guide to installation, configuration and setup, that will enable the reader to accurately, precisely and efficiently discover Wi-Fi networks. Furthermore, using the concepts detailed here in this article will arm the reader with the expertise to work with other wireless technologies, for example, Bluetooth, using specialised, dedicated wireless capture hardware.

How Exposed Are We On the Internet?

Carlos Loyo, Emiliano Piscitelli, Matias Choren Ruiz

There is no question that the Internet has become both a basic need for people and companies that can even be equated on many occasions with services such as electricity, water or gas. A sample of this can be the companies that are limited to carrying out their tasks normally or the massive comments on social networks when there are inconveniences in the connections. Currently, many of us use several services on the Internet, in some of them it is very likely that we will upload information such as: places visited, personal photos, comments related to religious or political affiliations, tastes, hobbies, among others; which can be taken advantage of and used by third parties (people or companies) in order to conduct targeted advertisements, investigate our profile and that of our environment, or induce propaganda, among others.

Identification of Flaws in the Design of Signatures for Intrusion Detection Systems

Nancy Agarwal, Syed Zeeshan Hussain

Signature-based Intrusion Detection System (SIDS) provides a promising solution to the problem of web application security. However, the performance of the system highly relies on the quality of the signatures designed to detect attacks. A weak signature set may considerably cause an increase in the false alarm rate, making it impractical to deploy the system. The objective of the paper is to identify the flaws in the signature structure responsible for reducing the efficiency of the detection system. The article targets SQL injection signatures particularly

Towards Secure IoT: Securing Messages Dissemination in Intelligent Traffic Systems

Jawdat Alshaer

The contribution of this article is enhancing proposed protocols with as little cryptography computation overhead as possible to make it applicable in the high mobility nature of VANET using security primitives; this guarantees security and allows fast authentication while a vehicle is passing from one VANET to the next, depending on its direction in the transportation networks.

DOWNLOAD

Web Application Attacks Preview.pdf

Please login or Register to access downloadables

DOWNLOAD (/#LOGIN)

AUGUST 20, 2021

Subscribe

This site uses Akismet to reduce spam. Learn how your comment data is processed (https://akismet.com/privacy/).

0 COMMENTS

SEARCH

CATEGORIES

Blog (https://hakin9.org/category/news/)

Free Course Content (https://hakin9.org/category/free-course-content/)

Uncategorized (https://hakin9.org/category/uncategorized/)

LATEST PRODUCTS

HOW TO BECOME CERTIFIED ETHICAL HACKER (W1) (HTTPS://HAKIN9.ORG/PRODUCT/HOW-TO-BECOME-CERTIFIED-ETHICAL-HACKER-W1/)
$69.00

METASPLOIT WORKSHOP (W2) (HTTPS://HAKIN9.ORG/PRODUCT/METASPLOIT-WORKSHOP-W2/)
$49.00

EXPLOIT DEVELOPMENT WORKSHOP WINTEL (W3) (HTTPS://HAKIN9.ORG/PRODUCT/EXPLOIT-DEVELOPMENT-WORKSHOP-WINTEL-W3/)
$45.00

BLUEPRINTING THE TARGET [90/10 WAY] (W4) (HTTPS://HAKIN9.ORG/PRODUCT/BLUEPRINTING-THE-TARGET-9010-WAY-W4/)
$89.00

WEB APPLICATION HACKING TECHNIQUES (W5) (HTTPS://HAKIN9.ORG/PRODUCT/WEB-APPLICATION-HACKING-TECHNIQUES-W5/)
$40.00

ARCHIVES (/MAGAZINES-2/)

FREE CONTENT (/DOWNLOADS/FREE/)

OUR BRANDS

(https://eforensicsmag.com/)

(https://pentestmag.com)

OUR PRODUCTS

Magazines (https://hakin9.org/magazines/)

Online Courses (https://hakin9.org/online-courses-2/)

Subscription (https://hakin9.org/levels-page-2/)

COMPANY

About Us (https://hakin9.org/about/)

Become an Instructor (https://hakin9.org/become-instructor/)

Write for us (https://hakin9.org/write-for-us/)

Partners (https://hakin9.org/partners/)

Blog (https://hakin9.org/blog-2/)

SUPPORT

Contact Us (https://hakin9.org/contact/)

FAQs (https://hakin9.org/faqsa/)

MORE

Privacy Policy (https://hakin9.org/privacy-policy/)

Terms and conditions (https://hakin9.org/terms-and-conditions/)

(HTTPS://TWITTER.COM/HAKIN9)
(HTTPS://WWW.FACEBOOK.COM/HAKIN9MAG/)
(HTTPS://WWW.LINKEDIN.COM/IN/HAKIN9MAGAZINE)
(HTTPS://HAKIN9.ORG/FEED/)