

**WEB APP**

**HACKING**

**THE BEGINNERS GUIDE**

**Web App Hacking: The Beginners Guide**

0xHEXXz, x0V01D

This is authors and publishers with the Spyrwl Labz Publishing process. Spyrwl Publishing is the act of publishing an in-progress Ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2023 - 2024 0xHEXXz, x0V01D

Table of Contents

***Recon1***

Whois 6

Dnsdumpster6

Sublister6

Dirsearch6

Knockpy6

Nmap3

Masscan3

**Mapping2**

Spidering3

Wappylzer6

BuiltWith6

***Discovery4***

Vega Vulnerability Scanning 6

Nmap Vulnerability Scanning 6

Nikto Vulnerability Scanning6

ZAP Vulnerability Scanning6

**Exploitation5**

XSS 6

SQLi6

Open Redirect6

XSRF6

HTML Parameter Injection6

HTML Injection6

CRLF Injection6

SSTI6

SSRF6

XXE 6

RCE6

Race Conditions6

Sub Domain Takeover6

IDOR6

**Reports5**

How to write a Pen Test report6

**Intro**

**Description**

**Hacking is identifying weakness in computer systems or networks that are then further exploited to gain access**. Example of Hacking: Using a password cracking algorithm to gain access to a system.

Computers have become mandatory in running a successful business. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit dishonest acts such as fraud, privacy invasion and stealing corporate/personal data. Cyber-crimes cost many organizations millions of dollars every year and businesses need to work to protect themselves against such attacks.

**Who is a hacker? Types of hackers?**

A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge in computer security.

Hackers are classified according to the intent of their actions. The following describes the different classes of hackers.

**What is Ethical Hacking?**

Ethical Hacking is identifying weakness in computer systems and/or computer networks and planning/executing countermeasures against any discovered weaknesses. Ethical hackers must abide by the following rules:

* Get **written permission** from the owner of the computer system and/or computer network before hacking.
* **Protect the privacy of the organization** that’s been hacked.
* **Transparently report** all the identified weaknesses in the computer system to the organization.
* **Inform** hardware and software vendors of the **identified weaknesses**.

**Why Ethical Hacking?**

* Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization’s image and save an organization a lot of money.
* Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals that would otherwise cause a loss of business.

**Legality of Ethical Hacking**

**Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking**. The [International Council of E-Commerce Consultants (EC-Council)](http://www.eccouncil.org/) provides a certification program that tests individual’s skills. Those who pass the examination are awarded with renewable certificates.

**Summary**

* Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
* Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
* Ethical Hacking is about improving the security of computer systems and/or computer networks and is legal when following the above mentioned stipulations.

**Recon**

**Description**

Information Gathering and getting to know the target systems is the first step in ethical hacking. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.

During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below −

* Gather initial information
* Determine the network range
* Identify active machines
* Discover open ports and access points
* Fingerprint the operating system
* Uncover services on ports
* Map the network

We will discuss, in detail, all these steps in the subsequent chapters of this book. Reconnaissance takes place in two parts − **Active Reconnaissance and Passive Reconnaissance**.

**Active Reconnaissance**

In this process, you will directly interact with the computer system to gain information using information that can be relevant and accurate. However, there is a risk of being detected if you are planning active reconnaissance without permission. If detected, a system administrator can take severe action and trail your subsequent activities.

**Passive Reconnaissance**

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

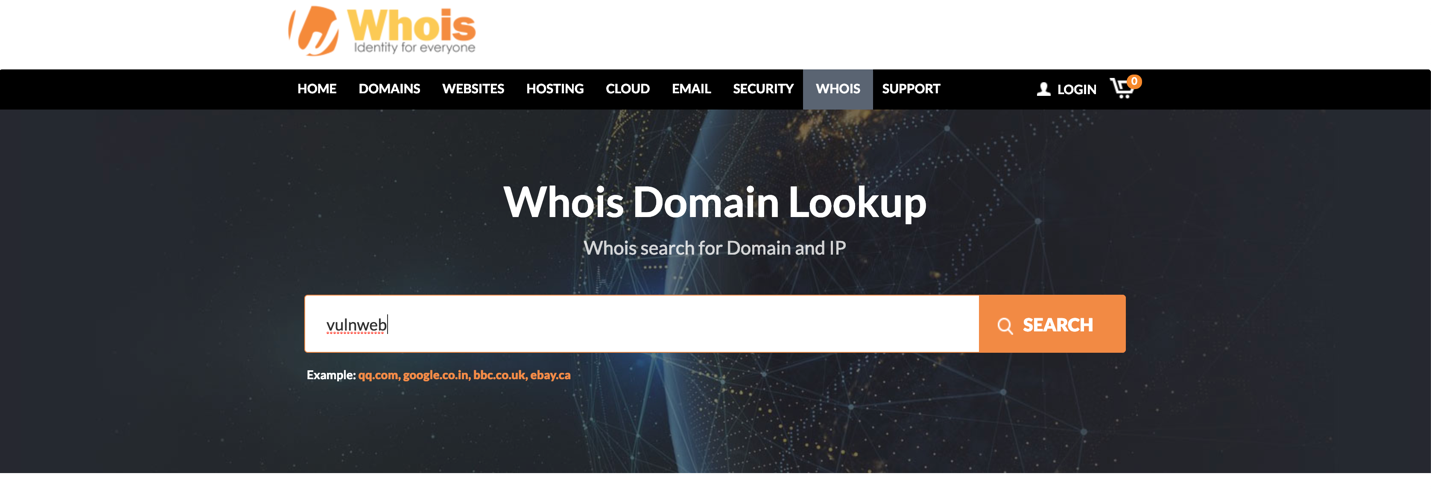
**Whois**

**What is Whois??**

When you [register a domain name](https://www.networksolutions.com/domain-name-registration/index.jsp), the Internet Corporation for Assigned Names and Numbers ([ICANN](http://www.icann.org/)) requires your domain name registrar to submit your personal contact information to the WHOIS database. Once your listing appears in the online domain WHOIS directory, it is publicly available to anyone who chooses to use the WHOIS search tool.

**Example:**

Let’s enter <http://testaspnet.vulnweb.com/> under the WHOIS tab on www.whois.com.

After clicking search, vulnweb’s name servers registrar and who owns the domain name are shown as below.