Bug Bounty Hunting for Web Security

Find and Exploit Vulnerabilities in Web sites and Applications

Sanjib Sinha

Apress®

Bug Bounty Hunting for Web Security

Find and Exploit Vulnerabilities in Web sites and Applications

Sanjib Sinha

Apress®

Bug Bounty Hunting for Web Security

Sanjib Sinha
Howrah, West Bengal, India

ISBN-13 (pbk): 978-1-4842-5390-8 ISBN-13 (electronic): 978-1-4842-5391-5
https://doi.org/10.1007/978-1-4842-5391-5

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Nikhil Karkal
Development Editor: Matthew Moodie
Coordinating Editor: Divya Modi

Cover designed by eStudioCalamar

Cover image designed by Pixabay

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-5390-8. For more detailed information, please visit www.apress.com/source-code.

Printed on acid-free paper

To Kartick Paul, Ex-System Manager, AAJKAAL,
Software Developer and enthusiast who has made
my dream come true.

It is an essentially humble effort on my behalf to show
that I am overwhelmed with gratitude for your help.

Table of Contents

About the Author

Sanjib Sinha is an author, and tech writer. Being a certified .NET Windows and Web developer, he has specialized in Python security programming, Linux, and many programming languages that include C#, PHP, Python, Dart, Java, and JavaScript. Sanjib has also won Microsoft's Community Contributor Award in 2011, and he has written "Beginning Ethical Hacking with Python," "Beginning Ethical Hacking with Kali Linux," and "Beginning Laravel 5.8 (First and Second Edition)" for Apress.

About the Technical Reviewer

Prajal Kulkarni is a security researcher currently working with Flipkart. He has been an active member of the Null security community for the past 3 Years. His areas of interest include web, mobile, and system security. He writes a security blog at www.prajalkulkarni.com and he is also the lead contributor at project Code Vigilant (https://codevigilant.com/). Code-Vigilant has disclosed 200+ vulnerabilities in various WordPress plugins and themes. In the past, he has disclosed several vulnerabilities in the core components of GLPI, BugGenie, ownCloud, etc. Prajal has also reported many security vulnerabilities to companies like Adobe, Twitter, Facebook, Google, and Mozilla. He has spoken at multiple security conferences and provided training at NullCon2015, NullCon2016, NullCon2018, Confidence 2014, Grace Hopper 2014, etc.

Acknowledgments

I wish to record my gratitude to my wife, Kaberi, for her unstinting support and encouragement in the preparation of this book.

I am extremely grateful to Mr. Matthew Moodie, Lead Development Editor, for his numerous valuable suggestions, complementary opinions and thorough thumbing; Nikhil Karkal, Editor and Divya Modi, Coordinating Editor, and the whole Apress team for their persistent support and help.

In the preparation of this book, I have had to consult numerous open source documentation and textbooks on a variety of subjects related to web security research; I thank the countless authors and writers who have written them.

Introduction

In this book you will learn about implementing an offensive approach toward security bug hunting by finding vulnerabilities in web applications. You will also take a look at the type of tools necessary to build up this particular approach. You will learn how to use hacking tools like Burp Suite, OWASP ZAP, SQlMAP, and DirBuster and you will also get an introduction to Kali Linux. After taking a close look at the types of tools at your disposal, you will set up your virtual lab.

You will then learn how Request Forgery Injection works on web pages and applications in a mission critical setup. Moving on to the most challenging task for any web application developer, or a Penetration tester, you will take a look at how Cross-site Scripting works and learn effective ways to exploit it.

You will then learn how header injection and URL redirection work, along with key tips to find vulnerabilities in them. Keeping in mind how attackers can compromise your web site, you will learn to work with malicious files and automate your approach to defend against these attacks. You will be provided with tips to find and exploit vulnerabilities in the Sender Policy Framework (SPF). Following this, you will get to know how Unintended XML Injection and Command Injection work to keep attackers at bay. In conclusion, you will take a look at different attack vectors used to exploit HTML and SQL injection. Overall, this book will guide you to become a better Penetration tester, and at the same time it will teach you how to earn bounty by hunting bugs in web applications.

Essentially, you will learn how to

- **Implement an offensive approach to Bug Hunting**
- **Create and manage Request Forgery on web pages**
- **Poison Sender Policy Framework and exploit it**
- **Defend against Cross Site Scripting (XSS) attacks**
- **Inject Header and test URL redirection**
- **Work with malicious files and Command Injection**
- **Resist strongly unintended XML attacks and HTML, SQL injection**
- **Earn Bounty by hunting bugs in web applications**

In addition:

- **As a beginner, you will learn penetration testing from scratch.**
- **You will gain a complete knowledge of web security.**
- **Learning to find vulnerabilities in web applications will help you become a better Penetration tester.**
- **You will get acquainted with two of the most powerful security tools of penetration testing: Burp Suite and OWASP ZAP.**

CHAPTER 1

Introduction to Hunting Bugs

Why do we learn to hunt bugs? It is difficult to answer this question in one sentence. There are several reasons, and reasons vary from person to person.

The first and foremost reason is we want to be better security professionals or researchers.

When a security professional is able to hunt security bugs in any web application, it gains them recognition; and because they are helping the whole community to remain safe and secure, it earns them respect as well. At the same time, the successful bug hunter usually gets a bounty for their effort. Almost every big web application, including Google, Facebook, and Twitter, has its own bug hunting and bounty program. So learning to hunt bugs may also help you to earn some extra money. There are many security experts and researchers who make this their profession and earn regular money by hunting bugs.

Reading this book will give you insight into implementing an offensive approach to hunting bugs in web applications. However, that knowledge should never be used for malpractice. You are learning these "attacking techniques" for defending web applications as a penetration

S. Sinha, *Bug Bounty Hunting for Web Security*,
https://doi.org/10.1007/978-1-4842-5391-5_1

tester (pen tester) or an ethical hacker. As a security professional, you are supposed to point out those bugs to your client so that they can rectify the vulnerabilities and thwart any malicious attack to their application.

Therefore before moving any further, we should keep this important caveat in mind: without having permission from the owners, you **may not** and **should not** attack a web application. With permissions, yes, you may move forward to hunt bugs and make a detailed report of what can be done to defend against them.

There are also several good platforms (we will talk about them in a minute) that allow you to work for them, and as a beginner, you'd better get registered with those platforms and hunt bugs for them. The greatest advantage is you get immense help from fellow senior security professionals. While you earn you will learn, and it is secured. You are hunting bugs or finding exploits and vulnerabilities with the owner's permission.

As a beginner, you should not try these techniques on any live web application on your own. In many countries, attacking the system without the owner's permission is against the law. It may land you in jail and end your career as a security professional.

Therefore, it is better to be registered with the bug bounty platforms and play the game according to the rules. We urge you to use the information contained in this book for lawful purposes; if you use it for unlawful purposes and end up in trouble, the author and the publisher will not be responsible.

In my opinion, if you are only interested in the bounty, you will not learn anything and finally, you are not eligible to earn money and respect. Finding exploits and vulnerabilities demands a very steep learning curve. You need to know many things, including web application architecture, how the Web evolves, what are the core defense mechanisms, the key technology behind the Web (e.g., HTTP protocol, encoding schemes),

etc. You must be aware of the mapping of the web application and different types of attacks that can take place. In this book, we will learn these and more together.

Now we can try to summarize the bug bounty program in one sentence.

> *Many web applications and software developers offer a bounty to hunt bugs; it also earns recognition and respect, depending on how well you are able to find the exploits and vulnerabilities.*

If you prefer a shorter definition than the previous one, here it is:

> *An ethical hacker who is paid to find vulnerabilities in software and web sites is called a bug bounty hunter.*

Bug Bounty Platforms

As I have said, as a beginner one should try the bug bounty platforms first and stick around for a long time to learn the tricks and techniques. In reality, not only beginners but many experienced security professionals are attached to such platforms and regularly hack for them.

There are many advantages. First, we should keep lawfulness in our minds. Through these platforms, you know what you may do and what you may not do. It's very important. Another essential aspect is you can constantly keep in touch with the security community, getting feedback and learning new things.

Here is an incomplete list of bug bounty platforms. Many good platforms will definitely come out in the future.

Hackerone

www.hackerone.com/

Bugcrowd

www.bugcrowd.com/

BountyFactory

https://bountyfactory.io

Synack

www.synack.com/

Hackenproof

https://hackenproof.com/

Zerocopter

https://zerocopter.com/

Japan bug bounty program

https://bugbounty.jp/

Cobalt

https://cobalt.io/

Bug bounty programs list

www.bugcrowd.com/bug-bounty-list/

AntiHack

www.antihack.me/

However, before registering to any of these previously mentioned bug bounty platforms, you should understand a few things first. You need to know how to use a virtual machine and the hacker's operating system Kali Linux. You must learn to operate tools like Burp Suite, OWASP ZAP, WebGoat, and a few others. You need to sharpen your skill in your virtual lab. There are a few web applications that allow hacking them, or they are made intentionally vulnerable so that beginners may try their newly adopted hacking skill.

We will discuss them in the coming sections.

Introducing Burp Suite, OWASP ZAP, and WebGoat

To start with tools like Burp Suite, OWASP ZAP, and WebGoat, you need to install Kali Linux in your virtual box. We will do that for one reason: Kali Linux comes up with all these tools by default. Therefore you don't have to install them separately. I strongly recommend using the virtual machine and Kali Linux; do not use these hacking tools in your own system, be it Windows, Linux, or Mac. They either can break your system or do not work properly.

We will talk about the Kali Linux installation process in great detail in the next chapter. After that, we will learn to operate three essential tools: Burp Suite, OWASP ZAP, and WebGoat. As we progress, we will see that more tools are needed. We will learn those tools also when the situation demands.

CHAPTER 2

Setting Up Your Environment

A virtual environment, or virtualization, is not mandatory for the experienced ethical hacker. As an experienced ethical hacker, you can run Kali Linux as your main system and perform the hacking using mainly a terminal with the help of a programming language such as Python, or you can use selected tools like Metasploit. However, for beginners, virtualization is compulsory.

Let me explain very briefly why it is important. Hacking can change the system completely. If you don't understand the state of the system well, you might change the state of your main system inadvertently. As a beginner, you cannot take that risk; therefore, always practice using a virtual machine. The easiest of them is VirtualBox, so I have chosen it to show you all types of bug hunting.

As an aspiring ethical hacker and penetration tester, you should become capable of building virtual and physical labs to use for practice, as this lets you install as many operating systems as necessary. Using virtual machines, you can safely break any system and change the state in your VirtualBox. It would not affect the main system.

S. Sinha, *Bug Bounty Hunting for Web Security*,
https://doi.org/10.1007/978-1-4842-5391-5_2

Why We Need a Virtual Environment

Virtualization is important for any type of penetration testing. You are going to learn how to find security vulnerabilities in any web application, and that needs a lot of practice before you actually approach a client to do the same on their live system. So we need a simulated environment first, a network security lab where we can practice, to learn and understand every trick of hunting bugs so that we can implement them on the live applications later as security professionals.

There are also other important considerations, like, since virtualization provides you a simulated environment, your main system is not touched. If you break your operating system by mistake while experimenting with any hacking-related tools, it happens inside your virtual system. You can reinstall the damaged operating system again. Another important aspect is that we have to stay within the law–always. We must practice our hacking-related tools in a legal way on our own systems.

You can also safely browse any web sites in a virtual environment. If some malicious code enters into your simulated environment, let it stay; it won't touch your main system. I simply encourage you to do every type of testing. It is a virtual machine. So, go ahead; test everything that comes to mind.

During my long information security research career, I have tested many hypervisors. However, keeping in mind that you may run your virtualization on any operating system in a simple way without facing any problem, I strongly recommend using VirtualBox. Irrespective of any operating system, VirtualBox is the best security lab solution for beginners. We will discuss the advantages in a minute.

Just to let you know, there are several other hypervisors. Security professionals use some of them; however, most of them are targeted for specific operating systems. KVM is good for Linux. For Windows, VMware

player is a good solution; Windows Virtual PC is also good, but you cannot run Linux distributions inside it. For macOS, both VMware and Virtual PC are good options including "QEMU" and "Parallels." VirtualBox can run on any operating system.

Installing VirtualBox is very simple. Whatever your operating system is, all it requires is a few clicks or typing a few commands. If you are using Windows, go to the Oracle VirtualBox page and download the latest version available. It'll simply guide you to the virtualization.

Note For VirtualBox, you need to have an ISO image to install any operating system.

I'll go through the Ubuntu Linux install in detail but will touch on other Linux distributions first. In the VirtualBox official download page for all Linux distributions, you first download the required packages and then install them according to the nature of your OS. For Red Hat, Fedora, or any Linux distribution belonging to that category, you will notice that the last extension is `.rpm`. In that case, you can move to the VirtualBox folder and issue commands like

```
rpm -i
```

or

```
yum install
```

There are other techniques to install VirtualBox on any Linux system. You can use your Ubuntu terminal and try the following commands separately.

//code 2.2

```
sudo apt-get install virtualbox
sudo apt install virtualbox-ext-pack
```

```
sudo apt install virtualbox virtualbox-ext-pack
sudo apt-get update
sudo add-apt-repository "deb http://download.virtualbox.org/
virtualbox/debian <ubuntu-release> contrib"
sudo apt-get install virtual-box-6.0
sudo apt-get install dkms
sudo apt install dkms build-essential module-assistant
```

If you don't want to go through typing, there are simple methods to install VirtualBox. And the good news is that it's graphical user interface based. That is the reason I'm encouraging absolute beginners to run an Ubuntu Linux distribution as their default OS. You can install VirtualBox from the software center directly without opening up the terminal or issuing any command. Ubuntu Software Center has many categories. One of them shows the installed software.

Introduction to Kali Linux—the Hacker's Operating System

Once the VirtualBox has been installed on your machine, you need not worry about installing several operating systems on it.

First, we need to install Kali Linux on our VirtualBox. Go to the official Kali Linux web site and download the ISO image of the latest stable version. Kali Linux is a much bigger Linux distribution than other Linux distributions.

The latest ISO image is more than 3 GB now, as of the middle of 2019. After the installation is over, it takes around 8 GB in your allocated virtual hard disk. Kali is by default not for general users. It contains a lot of hacking tools meant for various purposes, and because of that, it is much

heavier as far as size is concerned. For the same reason, it is also known as the hacker's operating system. You get plenty of hacking tools with Kali Linux, and you need not install them separately. In addition, it is the most popular among ethical hackers.

Many more secured Linux distributions are available:

- BlackArch Linux is one of them. It has a huge range of pen testing and hacking tools and is very large. Probably it is the largest among the others. It is over 7 GB in size because it has more than 1,900 hacking-related tools. You can run BlackArch live from a USB stick or DVD, or it can be installed on a computer or virtual machine.
- Qubes OS is another secure operating system but it is for advanced users only. In this operating system suspected applications are forced to be quarantined. It also uses sandboxes to protect the main system. Qubes OS actually runs a number of virtual machines inside, keeping the main system secure. It compartmentalizes the whole system into many categories such as "personal," "work," "Internet," and so on; it has reasons to do that. If someone accidentally downloads malware, the main system won't be affected.
- ImprediaOS is another good example. It uses the anonymous I2P network so that you can keep your anonymity all the time. It is believed to be faster than Tor, but you cannot access regular web sites easily. It is based on Fedora Linux and can run either in live mode or be installed onto the hard drive. It routes all your network traffic through the I2P networking system.

This is known as "garlic routing," whereas Tor uses "onion routing." Garlic routing is believed to be safer than onion routing. So you can visit only a special type of web sites called "eepsites" that end with ".i2p" extensions. It also has anonymous emails and BitTorrent client services. Visiting eepsites is always safer and it usually evades the surveillance radar that can track Tor.

- "Tails" is another good example of a secure Linux distribution. It keeps your anonymity intact through the Tor network, although it is debatable whether Tor can keep you absolutely anonymous or not. The main feature of Tails is that you can run it from a DVD in live mode so that it loads entirely on your system and leaves no trace of its activities.
- Another good example of a secure Linux distribution is "Whonix." You can use the power of virtual machines to stay safe online, which is achievable as the route of the whole connection is via the anonymous Tor networking system. In Whonix, several privacy-related applications are installed by default. It is advisable to use it in your VirtualBox to get the best result.

You can download any of them and try to run it on your VirtualBox. However, at present our main goal is simple enough. We'll install Kali first. Next, we will check whether the tools required for finding vulnerabilities in the web applications are updated or not. If not, then we will update them accordingly.

I assume you have downloaded the latest Kali ISO image. You can either store it on your local hard drive or burn it on a DVD. Now open up your VirtualBox and click "New." It will automatically open up a new window that will ask you what type of operating system you are going to install (Figure 2-1).

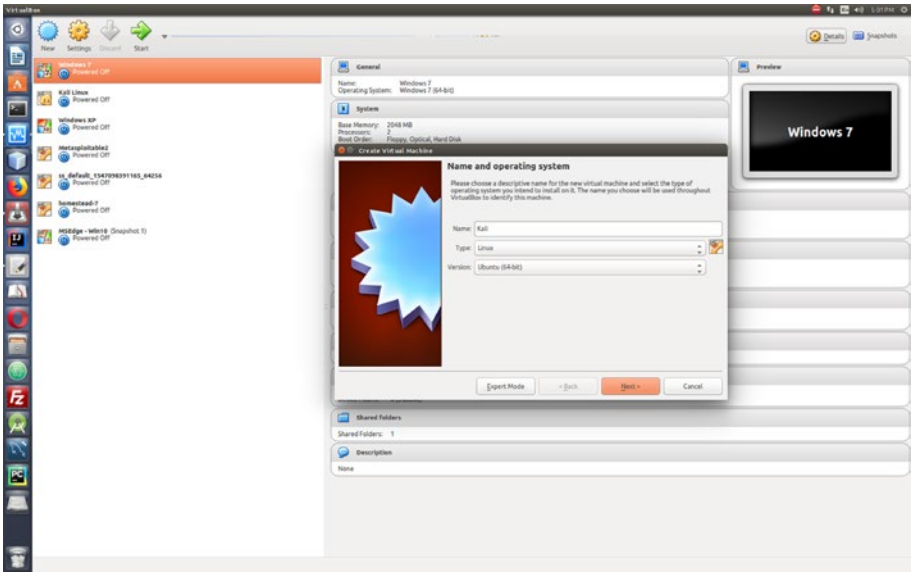

Figure 2-1. *A new window pops up in the VirtualBox.*

Look at the top left panel of the image; you see on the VirtualBox I have already installed Kali Linux, Metasploiltable 2, and MSEdge Windows 10. This Windows version can be downloaded for free for testing purposes and it remains available for 30 days.

The whole procedure is very explicit in itself. It will guide you to what to do next. Now it is time to enter in the opened-up window or UI of VirtualBox the name of the operating system you are about to install. Next, select the type–whether it is Linux or Windows, etc.–and the version. In the