

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How to start with Web Pentesting Part 1: introduction](#)

Bodlux - April 12, 2020, 4:12 pm

Hey everyone,

In this tutorial I am going to explain how you can start with web pentesting.

I am not an expert in web pentesting but I love doing it so I have some experience with it.

Do I need to have programming knowledge before starting web pen testing.

I would say it is not necessary as there are many tools that can do the job for you.

Therefore you do not actually need any programming experience.

But I strongly advise you to learn some basic html, css and js to start.

If you want to learn more about web pentesting I would definitely recommend to learn the following programming languages:

- HTML
- CSS
- Javascript
- PHP
- SQL

A good knowledge of web development will certainly help you with web pentesting.

First step to start web pentesting

To start with web pentesting you first need to collect as much information as possible about the website,

also called Information Gathering (for example: searching for hidden files or folders).

From the moment you have found some web pages you can search for vulnerabilities

Most common vulnerabilities

Personally I usually focus on the following vulnerabilities:

- Broken Access Control
- Broken authentication
- XSS
- SQLi
- CSRF

If you want to learn more about vulnerabilities I would definitely recommend you to take a look at the OWASP Top Ten vulnerabilities.

Commonly used tools

There are several tools online that you can use in web pen testing.
I personally like to make my own tools now but that is not necessary at all.
Most online tools are better than the ones I create myself.

Below is a list of commonly used tools:

- Burp suite
- SQLMAP
- Dirbuster
- Nikto
- ZAP

How do I start with web pentesting

Please never go to a random website to test something or look for vulnerabilities.
There are several free web applications where you can test and improve your web pentesting skills.

Below you will find some examples:

- security chepherd -> favorite
- DVWA -> favorite
- Mutillidae
- juice shop
- BWAPP

Thanks for reading my thread.

If you have any questions please feel free to ask and i will try to answer as best as possible.
I may create additional tutorials about some of the above vulnerabilities if you prefer.

aneWra - April 13, 2020, 3:23 am

I'm doing this right now. I'm studying html and everything related to websites. I also read something about https DNS and other things. Just starting everything from the basics.

I think that Linux is better than Windows in this things by the way I'll install in a few months cause I'm not able to use it. I'll try with Parrot.

Thank you for these informations man.

Bodlux - April 13, 2020, 4:02 am

(Apr 13, 2020 03:23 AM)aneWra Wrote: [\[CITE\]](#) I'm doing this right now. I'm studying html and everything related to websites. I also read something about https DNS and other things. Just starting everything from the basics.

I think that Linux is better than Windows in this things by the way I'll install in a few months cause I'm not able to use it. I'll try with Parrot.

Thank you for these informations man.

I am happy to hear this.

linux will certainly help you with web pentesting. there are some good linux distributions where frequently used tools are installed by default.

parrot is indeed one of them (best to start with). I also recommend that you install a Kali Linux VM as many useful tools are installed there as well.

aneWra - April 13, 2020, 4:10 am

Yes. I think I'll install a VM to get started with Linux while studying coding.
Hope you'll post others tutorials. Thanks again.

dt0909 - April 13, 2020, 5:31 am

Interesting post! Love to learn new things :)

Bodlux - April 13, 2020, 7:59 am

(Apr 13, 2020 05:31 AM)dt0909 Wrote: [\[CITE\]](#) Interesting post! Love to learn new things :)
thanks, i'm going to make a 2nd part soon

Suved - April 14, 2020, 2:40 am

(Apr 12, 2020 04:12 PM)Bodlux Wrote: [\[CITE\]](#) I strongly advise you to learn some basic html, css and js to start.

If you want to learn more about web pentesting I would definitely recommend to learn the following programming languages:

- HTML
- CSS
- Javascript
- PHP
- SQL

A good knowledge of web development will certainly help you with web pentesting.
A good a good advice.