Forum:Hack Forums

Thread: [Kali Linux] How to find vulnerabilities on websites.

Wespa - *May 31, 2020, 4:43 pm*

Hello everyone, welcome to a tutorial on how to find vulnerabilities on websites.
Please keep in mind that I will not teach you how to use these vulnerabilities, only on how to find them.
I'm sure that someone who is more skilled than I am can help you with the latter part.

I have personally used this a couple of years back to find vulnerabilities on mine and my friend's websites, I'm sure that if you become good at this you can maybe make some money out of it.

Requirements:
1) An internet connection
2) A website you wish to target
3) Kali Linux
If you don't have Kali Linux, I would recommend downloading it on a virtual machine such as VirtualBox. Before making it your main OS.

The resource we will be using is WebPwn3r - You can check the GitHub page here: https://github.com/zigoo0/webpwn3r

Tutorial:
Spoiler (Click to View)
1. Open up terminal and type "git clone https://github.com/zigoo0/webpwn3r.git"
(This will download the program used to find the exploits)
2. Type: "cd webpwn3r" or whatever the directory for your download is.
3. Type: "ls"
4. Type: "chmod +x scan.py"
5. Type: "./scan.py"
This will start up the WebPwn3r logo and information about the software.
At the end of the program it will show you "Scan URL or List of URLs?"
6. If you have only one website that you want to take a look at type "1" if you have more type "2"
7. Type: the url of the website and press enter.
The software will now start to scan trough the websites and it will tell you if it has found any vulnerabilities.

Lymex - *June 1, 2020, 2:10 pm*

Sounds noob-friendly but i will stick to my own tools i will check it out later and leave a rating from 1-10

I will give it a 7.5 out of 10

MightyOne - *June 1, 2020, 2:11 pm*

This actually looks pretty simple !
Thanks for this Wespa, if ill have some time of my studying ill be sure to check more of this !

Bacardi Cola Lime - *June 1, 2020, 2:15 pm*

Automation tools are also great for Capture the Flag events. I know it takes the magic of finding the vulnerabilities yourself but if you ever get stuck, there is help.

Hex.neo - *June 2, 2020, 12:43 am*

Nice.

Add on, Try "owasp top 10 testing guide"