

Forum:[Hack Forums](#)

Thread: [Help for Vulnerability scanning& penetration testing.](#)

orton - January 23, 2020, 1:26 am

Hello,

I got a project from my friend, he got a website and wants me to perform vulnerability assessment to check whether it is secure or not. I got basic knowledge and a namesake CEH certification through which I got to work with some basic tools like Nmap, Burpsuite, Acutenix. I have to submit overall report to him regarding the vulnerabilities in the website. Could anyone be kind enough to take down their valuable time for a couple of minutes to guide me the way I can perform overall vulnerability assessment? Thanks in advance.

Money- - January 23, 2020, 1:42 am

Why did your friend refer you to perform a VA and PT on his site? Any reasons though?

Since you are asking help over here. I guess you are not sure what you are doing? Yet your friend think of you as the go to guy?

I am sure its not just scanning the site with Acunetix but performing enumerations and knowing the technologies and the topology behind works.

Edit: I hope no one trolls you here for having the " CEH " though.

orton - January 23, 2020, 4:53 am

(Jan 23, 2020 02:42 AM)Money- Wrote: [\[CITE\]](#) Why did your friend refer you to perform a VA and PT on his site? Any reasons though?

Since you are asking help over here. I guess you are not sure what you are doing? Yet your friend think of you as the go to guy?

I am sure its not just scanning the site with Acunetix but performing enumerations and knowing the technologies and the topology behind works.

Edit: I hope no one trolls you here for having the " CEH " though.

My friend referred me because he felt I could handle it and then I already mentioned I got CEH certification which is only a namesake one. I got basic idea and the only concern I posted here was to get a route map for the scenario Vulnerability assessment from where to start and where to end. If someone trolls me, no offense because I want to learn rather than feeling belittled for the trolls. With all due respect, thank you for the reply.

CyberStrike - January 23, 2020, 1:59 pm

Argh... it depends here what this site deals with, for example does it accept payments? In this case maybe you need to be concerned with PCI/DSS (ISO 27001) either way check out ISO/IEC 27000, there are several parts and may or may not apply. For example this site maybe just has pictures of puppies and kittens it's a static site no user data, no payment just pictures so no way to really for a user to make any input then probably there is less of an attack surface.

SideNote: No one should troll you, it's EC Council who is not preparing their students for success. Remember that they were the first certifying body in this field and so still in other countries I will see recruiters to this day only familiar with CEH.

orton - January 24, 2020, 6:58 am

(Jan 23, 2020 02:59 PM)CyberStrike Wrote: [\[CITE\]](#) Argh... it depends here what this site deals with, for example does it accept payments? In this case maybe you need to be concerned with PCI/DSS (ISO 27001) either way check out ISO/IEC 27000, there are several parts and may or may not apply. For example this site maybe just has pictures of puppies and kittens it's a static site no user data, no payment just pictures so no way to really for a user to make any input then probably there is less of an attack surface.

SideNote: No one should troll you, it's EC Council who is not preparing their students for success. Remember that they were the first certifying body in this field and so still in other countries I will see recruiters to this day only familiar with CEH.

Thank you so much for your time and valuable suggestions, I will put my complete efforts to make sure no one would a get chance to point me out or troll me for having the certification.