**eWPT Review (A weekend well spent)**

**WHOAMI**

I am a Senior Security Test Engineer and I started my journey of Penetration Testing from 2019. I have failed an OSCP attempt and in order to broaden my horizon in Web App Pentesting I enrolled for eWPT. So , here’s a short review of mine which i felt while studying for eWPT till i cracked the exam

**My upcoming write-ups:**

So, I am planning to take ecppt soon and oscp after that hopefully. I shall be sharing my honest reviews about my learning, experiences and as well as my failures in the OSCP write up (Fingers crossed🤞🏻)

**Course Material and Labs**

INE : <https://ine.com/pages/elearnsecurity-pricing>

INE is the official training provider for all e-learn security certs and I must say the course material is so simple and elaborated that any noob can understand and can start straight away. The Videos were amazing and there are labs and challenges as well, Solutions are provided for labs and not for challenges which is what makes it a challenge. The slides are very informative and presented in a very good manner, I suggest don’t miss out on the slides. you have to do all the labs and challenges in order to pass the exam. Doing the Labs and Challenges is too much fun, you will enjoy this phase

**Who is this course for:**

People who want to start their career in Application security and learn Web-App Penetration Testing can enrol into this course. I highly suggest this course for people who are preparing for OSCP as it improves your web application pentesting

**Exam**

eWPT is a pure black-box Pentest in which you need to find all the subdomains and vulnerabilities in the given scope. You are given 7 days to perform penetration testing followed by 7 days to write a detailed report on your findings. The report should be Commercial- level which means it should be very specific and high level. eLearnSecurity is very strict in evaluating in the report so please make a note of it and try to keep your report as professional as you can and don’t add unnecessary fillers

There is no restriction on tools usage you can use Burp suite professional, Sqlmap etc..

**Do you need to learn from any other platforms inorder to pass the exam?**The answer is NO, INE provides you with almost everything that is needed to pass the exam. but if you want to go deeper I suggest doing Portswigger Labs.

<https://portswigger.net/web-security>

“**A necessary but insufficient condition to pass the exam is to log in to the Administration area as the administrator user**”

I started my exam on Feb 11 2022 Friday 17:17:57 IST, I connected to the vpn and got my letter of engagement which contains the scope on which you need to perform pentests, you shouldn’t be testing out of scope domains so please note that down as a Penetration Tester you need to know what is your scope and with that being said let’s move on to the exam

Sub-domain enumeration is the crucial part of the exam so try to practice and learn as much as you can. I have seen people who failed the exam and have said that they couldn’t find the admin area, this exam is very tricky

**DAY 1:** I started finding the subdomains which is quite challenging in this exam. I used dnsscan, WFUZZ, Sublist3r and ffuf tools to find the subdomains. The exam is focussed on OWASP TOP 10 2017.I was stuck at a point where i was exhausted, I still couldn’t find the admin area and called it a night

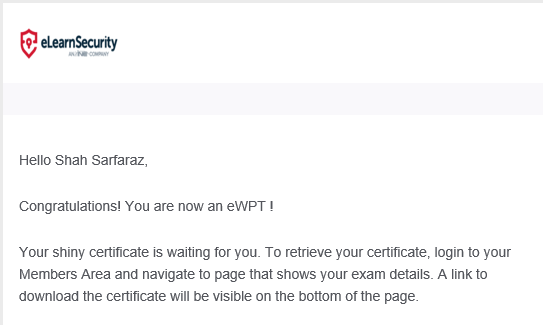
**DAY 2:** After waking up I started fresh again and I was there half way through, By end of this day I have found around 10 vulnerabilities and the admin area.I was feeling good about it and took a break. Remember to take breaks when you are stuck note that it always helps and don’t skip your workouts if you are doing it as they help a lot in maintaining your mental balance and drink lots of water

**DAY 3:** I started after lunch by 2 PM by and by 5 PM I was admin, I was feeling happy but still there’s more, I need to make a report and I tried to find more vulnerabilities and I spent a lot of time in making my report and kept looking for more vulnerabilities and I was able to find around 20 vulnerabilities, you should take some time to find the vulnerabilities as they are obvious, I submitted my report at Feb-20 yeah i took around 6 days to complete my report as i wanted everything to be perfect and I am a working professional so I went slow and steady.I found around 20 vulnerabilities in the exam

**NOTE :** If you find a vulnerability then try to find it on different parts of the application. The exam is designed vulnerable so try to find as many as you can and keep enumerating. Try to spend some quality time with sqlmap :P it would be a timesaver and an asset, learn how to perform a sqlmap scan with a request file and don’t forget OWASP ZAP scanner

**RESULTS**

After waiting for 17 days I was happy to see the following email



**Sample Report Template :**

<https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report>

**Tools Used in Exam:**

* OWASP ZAP scanner
* Sqlmap
* Burp Suite
* DNSscan
* ffuf
* sublist3r

**Links:**

**eWPT Verify Link:** [https://www.elearnsecurity.com/certification/verify?c=b9838e64-1438-47c7-9bb8-6b5683925b9a](https://www.elearnsecurity.com/certification/verify?c=a220cb13-d83f-4462-990c-5a02a8278e25)

**Twitter:** <https://twitter.com/L33tshah>

**Linkedin:** [https://www.linkedin.com/in/shahsarfaraz/](https://www.linkedin.com/in/anontuttuvenus/)

