How To Become Web Security Engineer With CTFs...?

This presentation for the people who wants to start in the web security

Whoami

- Mahmoud Ashraf “Web Security Researcher & IT Security”

  Experience:

  - Security Analyst - @HackerOne
  - IT Security - @Travel Cities
  - Web Security Tester - @Alimed

Have more than 2 years of experience in Cybersecurity Field specialized in web security.

Presentation Contents...

- Web Security Engineer?
- Web Application technologies.
- Why the web app is vulnerable?
- OWASP TOP 10 Web Vulnerabilities.
- Secure Code Review.
- What in the web application should be tested?
- What Is The Capture-The-Flag (CTF)?
- How CTFs Improve My Skills?
- Web Security CTF & How I Escalate To Another Path?
- What the required skills to start web penetration testing?
- How to be with the community...?

Web Security Engineer?

- As we know the most popular in penetration testing is “Web Application penetration testing” so some of us want to start web penetration testing because they thought it will be easy and yes it easy but if you wanna be Web Security Engineer so it’s will be different more.
- As Web security engineer you take it hard as much as you can you have to know Web Security in depth. Much of exploitation and how to detect and fix the vulnerable code whatever PHP, .NET , Java , Nodejs and python etc… some programming language you should know about it and how to secure the code it will never stop in PHP ONLY. So you have to improve your coding skills As Web security engineer you have to know the OWASP top 10 web vulnerability but extensive knowledge in Web Vulnerabilities. It never stop in SQLI OR XSS.
- You have to think creativity and improve your skills in development and security every time. So you have to be up to date of everything and if there’s a new attack technique or Zero Day Vulnerability and so on. Should take it as challenge to keep improving your skills in Web Security.
- Web Applications are still vulnerable right now… and the attacks in web apps changes and developed so as you’re Web Security Engineer you have to think what the attacker think. As Web Security Engineer: you know what is behind the web application you have a Security Appliances such as: Firewalls, IPS and IDS. All of this as You’re penetration tester have to know how this security appliances work and how the web app work what the framework this web app use? What is the third party, all of this you have to know extensive knowledge in web applications as much as you can

Web Application technologies

- Here we move to what web application technologies? We have to know the protocols so we have 2 protocols:
- - HTTP / HTTPS SSL-Encrypted
- In HTTP protocol it’s not secure but in HTTPS is secure and the web app traffics are encrypted with SSL it prevent or let’s say it will be hard to sniffing the data or make MITM Attack..
- You have to know the HTTP Requests, responses and methods
- HTTP Proxies & Authentication
- URLs and REST
- What’s The HTTP Headers?
- What’s cookies?
- Status codes
- Server-side and client-side Functionality, state and sessions
- URL, HTML, Base64, Hex encoding also Serialization
- Frameworks
- I have collect some of web technologies you have to
- know well about them.

Why the web app is vulnerable?

- The developer not prefect in writing a secure code.

  - so that's why the developer has no idea about the security and how to secure his code some of developers know about filtering and how to filter the input to prevent or to stay safe from SQL injection or XSS Vulnerabilities, also in parameters too.

- The developer use an old version

  - some of developers use old version such as: old Version of PHP might be vulnerable or use old frameworks and old JS so all of that might cause a Bugs "Vulnerabilities".

- The Web server is old version

  - Web Applications are running on web server so the web server is old version so this old version I can get shell to the web server if this old version is vulnerable by just writing a shell script and execute it and get access.

- Here I collect some of mistakes of developers do and some of things that makes the web application vulnerable.

OWASP TOP 10 Web Vulnerabilities.

- A1: Injection
- A2: Broken Authentication And Session
- Management
- A3: Cross Site Scripting
- A4: Insecure Direct Object Reference
- A5: Security Misconfiguration
- A6: Sensitive Data Exposure
- A7: Missing Functional Level Access Control
- A8: Cross-Site Request Forgery (CSRF)
- A9: Using Known Vulnerable Components
- A10: Unvalidated Redirects & Forwards

- Almost of us know that injection vulnerability is just about SQLI & OS command injection but in the background we have more injection attacks techniques such as: iframe injection, Server side includes and Mail header injection etc…

Secure Code Review

- This one I just want to talk in it cause you will use it almost 80% is useful sometimes you make a like white box penetration testing you will see the code and fix the code also you will have to access the web application too, and do your penetration testing on it, but the additional this you'll be able to see the back-end code of the application.
- Analyze it
- Detect the bugs
- Know how to exploit the bugs
- Fix the bug

  "Maybe this is not important to some of pentesters but in my case I prefer to learn how to secure code because it will help you more

  "Learn scripting/programming Languages as much as you can, you will see more and more web applications and it'll be wrote by different langauges. DON'T FOCUS IN PHP ONLY...

What in the web application should be tested?

- In the first you have to walk in methodology, don't test what should be tested as like script kiddie you have to create your own methodology or company methodology or in the internet just get the methodology what you like it.
- Why methodology?… 'Cause you will walk in this and know what I should test first and how this web application works the web server version starting with information gathering to Developing test cases to Vulnerability Discovery & exploitation. Never see input and first think type xss exploit without known how the web application works…

  - What should be tested?
- Reconnaissances and Mapping
- Client Side Controls
- Authentication Mechanisms
- Access Controls
- Session management
- Input-based flaws
- Application Cryptography
- APIs and Web Services
- Authorization schema
- Web server and back-end

"Note: Walk with methodology you will be right"

What Is The Capture-The-Flag (CTF)?

- Capture-The-Flag or CTF this is a challenge or competitions which made to improve you Cybersecurity skills in different categories such as:
- Web Security
- Malware Reverse Engineering
- Forensics
- Cryptography
- Machines

  there are a competitions and this like you live scenarios I mean like real attack and you have to get the flag. If we say the web application is vulnerable with OS Command injection so you have to exploit it and get shell to the web server and the flag is locate in root directory and you move on to get the flag.

How I CTFs Improve My Skills?

- CTFs improve your skills and make you practice in real scenarios which make you good at what you are specialized…

  - Here I collect some of CTFs Platforms:

- ctftime.org
- hackthebox.eu
- cybertalents.com
- picoctf.org (For Beginners)
- ctflearn.com (For Beginners)
- hackertest.net (For Beginners)

  “here some of ctf platforms what I prefer there’s a lot but this is what I prefer you can search for another platforms.”

Web Security CTF & How I Escalate To Another Path?

- In web security CTFs you practice it, and the web applications is vulnerable and the one way to get the flag is to exploit the vulnerability which it's in the web application.
- Web security is prefect and let's say it has top 10 vulnerability and so you have a big vulnerabilities to test so you have 10 open doors actually one of them you can exploit.
- How I Escalate To Another Path?

  - one path is not enough but I don't mean you have to learn both in the same time.

  - you have to be good at your path well let's say something like T-Shape, I have an experience in web security and I have extensive knowledge in it and intermediate in malware reverse engineering..

  - that's way to escalate form web security to another path but must be perfect in your actual path (Web Security)...

  - This will help you in ctfs and also let you have to get another knowledge in another path with web security.

What the required skills to start web penetration testing?

1- Know about the OWASP top 10 web vulnerabilities and know how to exploit it and detect it prefer to fix coding. Know more about what's the attacks techniques on the web applications

2- Learn Coding (PHP,JS,.NET,Java and python) prefer learn how to secure the code.

3- Know well web application technologies and how it works

4- Practice as much as you can playing CTFs help you to get practical experience

5- walk with a methodology and understand the web penetration testing process.

6- Web application analysis

7- Experience in technical writing skills specific writing a reports

8- Knowledge in web application frameworks.

- Courses And Certifications

  1- eWAPT (eLearnSecurity)

  2- eWAPTX (eLearnSecurity)

  3- eWDP (eLearnSecurity)

  4- SEC542 – Web application penetration testing (SANS)

  5- SEC642 – Advanced web application penetration testing (SANS)

- "This Courses and certifications what I prefer to take it not must to take it you can study the materials of it. Best way is learning with practicing to get what you need to be."

How to be with the community…?

- First: Market to yourself share your:

  - Blogs, Write-up, Researches and videos

  - this let the people know you and know what you are professional at. They will recommend you if there's a job opportunity or someone hire exp: Web security engineer and you're so people that know will recommend you
- Second: Don't think you're loser if you fail no one learn anything for free we fail and learn and win.
- Third: There's a lot of jobs apply for the job that match your requirements and create you resume and add on it your achievements

My Message for you.

This presentation I’ve created to learn the security guys to enter in the web security path and I have added more things may help you.
Hope you all like it. :-)