INTERNSHALA TRAININGS

Hack-a-thon

29th April 2020 - 24th June 2020

Problem Statement:

We are glad that you have completed the training and cleared the final test. Now, it's time to test your skills in a practical manner and for that, we have set up a real life-like web application in the form of an online e-commerce portal.

Your task is to test this e-commerce platform and find all possible vulnerabilities and loopholes in it, collect relevant PoCs and then prepare a **Detailed Developer Level Report.**

For reporting each vulnerability, you must follow the sample report pattern given to you in Module 8 and make sure the following things are mentioned:

- Title of Vulnerability.
- A Short Description.
- Exact URL which has the vulnerability.
- The parameters which are vulnerable (with parameter type like GET, POST, Cookie, Header, etc.).
- Payload that you used to trigger the vulnerability.
- Observation slides containing step by step information to replicate the exploit with PoCs.
- Business Impact of the vulnerability, explaining in detail what can be done by a hacker.
- Recommendations on how to fix the vulnerability.
- Reputed References for the vulnerabilities.

INTERNSHALA TRAININGS

Remember, each and every kind of vulnerability you learnt about, might be somewhere in this application. All you have to do is open the application and start exploring its features. Once you have understood each feature the website has, you can start playing around with it and fuzzing into various places.

A big part of the VA has been already done for you as you have the exact IP and the application which you have to test, but there could be hidden pages and components too, so keep that in mind.

To give you a benchmark and a target to achieve, here is a list of all the vulnerabilities which we have intentionally kept and which are supposed to be found and reported by you:

SQL Injection
Reflected and Stored Cross Site Scripting
Insecure Direct Object Reference
Rate Limiting Issues
Insecure File Uploads
Client Side Filter Bypass
Server Misconfigurations
Components with Known Vulnerabilities
Weak Passwords
Default Files and Pages
File Inclusion Vulnerabilities
PII Leakage
Open Redirection
Bruteforce Exploitation
Command Execution Vulnerability
Forced Browsing Flaws
Cross-Site Request Forgery

INTERNSHALA TRAININGS

So, there are a total of **36 vulnerabilities** (some vulnerabilities have more occurrences than 1) intentionally kept but these do not include combinational vulnerabilities like Bruteforce Exploitation and Rate Limiting. If you are able to guess the password, you can either count it in Bruteforcing or count it in Rate-Limiting but while writing recommendations, write recommendations for both. Similarly, if you find a public software that allows PHP file upload, you can either count it in file upload or in components with known vulnerabilities.

If you do find other general vulnerabilities apart from these you can report them too but do not count them in the 36.

Happy bug hunting!

Steps to access the Project:

1. Login to trainings.internshala.com
2. Go to Ethical Hacking Training
3. Go to Progress Report
4. Click on the 'GO TO PROJECT WEB APPLICATION' button.

What the contestants are supposed to do:

- The contestants are supposed to register for the Ethical Hacking training on Internshala Trainings.
- From the start date of the training (29th April), you will be able to access the training content.
- Start learning from the first module. To unlock the next module, you will have to attempt the module test of your current module.
- Complete all the modules in the training.
- You will be able to access the project problem statement from the start of the training, but it is recommended that you attempt the project once you have gone through all the modules.

INTERNSHALA TRAININGS

- Please ensure that you submit your solution before the deadline.

Rules for the contest:

- **You need to score a minimum of 40% in the final test and a minimum of 100 marks in the project in order to be eligible for rewards.**
- Take your final test and submit your project before the deadline.
- Make sure that the submitted project is a work of your own and not copied from any external sources.
- Contestants must be beginners and should not have any prior knowledge of the subject. If found otherwise, you will be disqualified.
- The projects of top 50 performers in the Final Test will be evaluated.
- Final winners will be announced based on the project, and winners may be interviewed before the announcement.
- The decision on the winners and runners-up made by Internshala will be final and binding.

Note: In case you need more time to complete the training beyond 8 weeks, you can request for an extension as per regular extension policy of Internshala Trainings platform. However, you will not be eligible to participate in the contest anymore.

Submission:

Create a PPT for the project report. Place all the created files and resources in a single folder and create its zip file. Now, upload this zip file by clicking on the 'Submit project solutions' section in the 'Progress Report'. Late submissions will not be considered for evaluation.

Note: No resubmission is allowed

INTERNSHALA TRAININGS

Rubric for Project Evaluation:

Each vulnerability in the project report will carry 10 points divided into 3 sections as given below:

i. Finding and exploiting the vulnerability (5 points):
a) Name of the vulnerability and description.
b) Where it exists - URL, parameters, payload, data extracted/possible damage.

ii. PoC and Observations (2.5 points):
a) Step by Step PoC for the vulnerability.
b) How well are the observations written?
c) Quality of the screenshots.
d) The relevance of the screenshots.

iii. Business impact, recommendations for patching, and references (2.5 points):
a) Business impact needs to be clearly and correctly documented.
b) Recommendations for patching the vulnerability need to be present.
c) References- Links to exploits used, official articles referred to for each vulnerability.

Note: Few of the vulnerabilities, which are complex to find and exploit, will carry 5 bonus points. These bonus points will be given under the 1st category (finding and exploiting the vulnerability). These bonus points are not given on the basis of the severity of the vulnerability but based on the complexity of its exploit.

Important Dates:

- Contest (and training) start date - **29th April 2020**

INTERNSHALA TRAININGS

- Contest end date (Last date to give the Final Test and submit the Project Report) - **24th June 2020**
- Result declaration - **15th September 2020**

Queries:

Please reach out to trainings@internshala.com for any queries which you have regarding the contest. For any queries regarding the content present in the training, there is a forum where the instructor will promptly reply to your queries within 24 hours.

All the best!