ETHICAL HACKING TRAINING

PROJECT SOLUTION

The project web application we gave you, had 28 vulnerabilities.
Here is the breakdown of the various types of vulnerabilities that were present in the web application:

SQL injection - 2
Reflected and Stored Cross Site Scripting - 3
Insecure Direct Object Reference - 4
Rate Limiting Issues - 2
Insecure File Uploads - 1
Client Side filter bypass - 1
Server Misconfigurations - 1
Components with known vulnerabilities - 2
Weak Passwords - 2
Default files and pages - 3
File inclusion vulnerabilities - 1
PII Leakage - 1
Open Redirection - 1
Bruteforce Exploitation - 1
Command Execution Vulnerability - 1
Forced Browsing flaws - 1
Cross-Site Request Forgery - 1

Congratulations to all those who have been able to complete the project and have found all these vulnerabilities.
For those of you who have not been able to find them, it's not the end. A good ethical hacker strives till he/she achieves the target. So, if you still have time left in the training, we recommend you to try further and find the remaining vulnerabilities. All the best!