Deliverables

- Each team should deliver:

  - Module Source code

  - Video demo for the module and the attack

Module 01

- Create a web application with the following pages:

  - Register Screen (Full Name, Email, Password, Phone, Country)

  - Login Screen with Email and password

  - Profile page that shows account details, user should be redirected to this page after successful login

Module 01 - Attack

- User profile should be displayed based on token value

- Generate token using user's email MD5 hash

- Attack the login form to get other user's profile by knowing his email

Module 02

- Create a web application for HR department with the following pages:

  - New Application: where user can enter name, email, phone and upload CV (only PDF should be allowed)

  - Search for an applicant : where user can search for a single application using user's email

Module 02 - Attack

- Bypass the PDF check to upload php backdoor

- Attack search field using SQL injection to get all applications without knowing any emails

Module 03

- Create a Guest book application with the following screens:

  - Guest Message: where guest can submit his name and message

  - Admin login: where admin can login to view all submitted messages

Module 03 - Attack

- Attack the message submit by XSS

- Injected XSS code should result in stealing admin cookie and send it to attacker's server, hence attacker can get access to admin portal