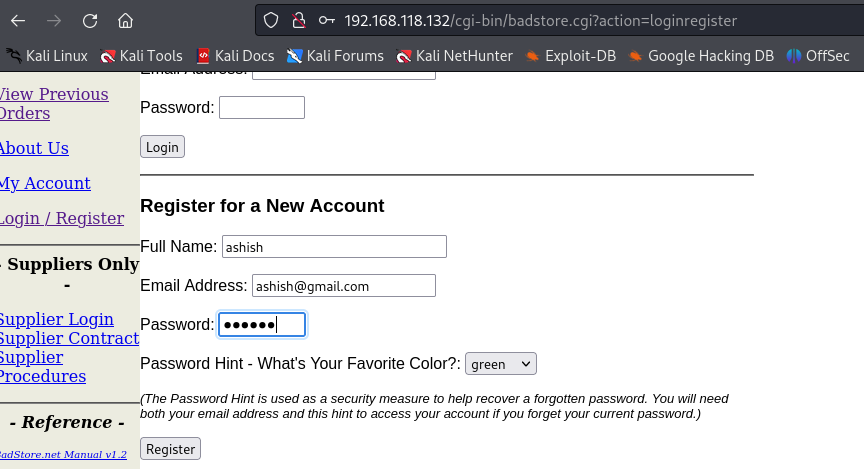
**Broken Access Control**

Access control refers to enforcing permissions on actions and resource access in web applications, relying on authentication and session management. Broken access controls, a common and critical security issue, often result from flawed design or implementation errors.

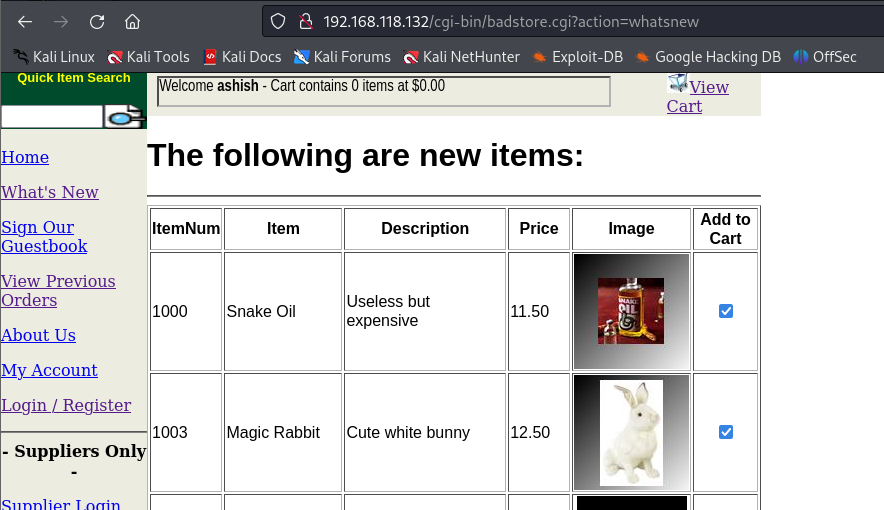
Access control vulnerabilities are widespread and frequently pose severe security risks.

**Walkthrough: Broken Access Control in badStore**

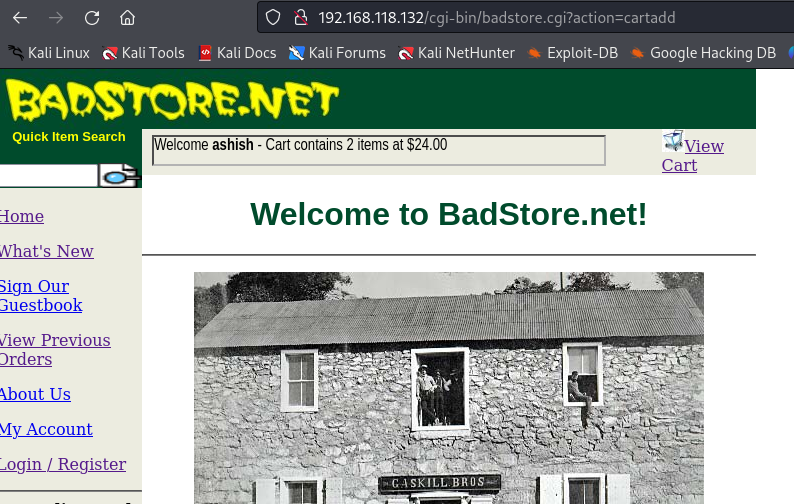
1. Register for a new account.



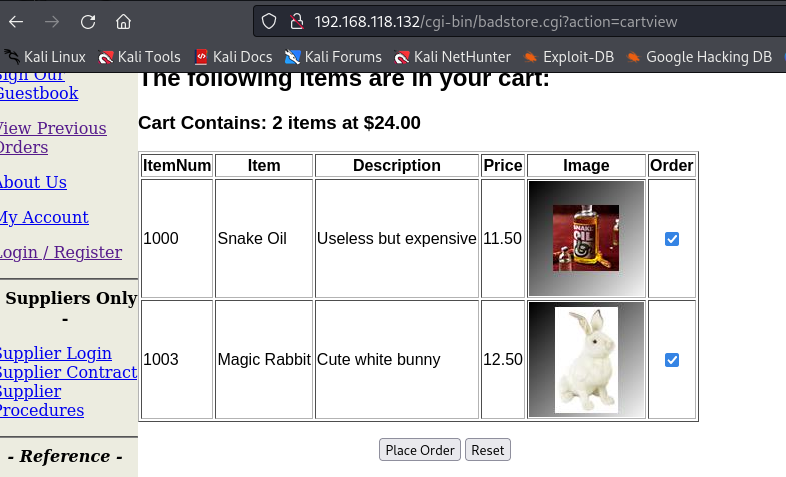
1. Click on whatsnew in the left panel. And select the items you want to put into cart. Click on Add items to Cart.

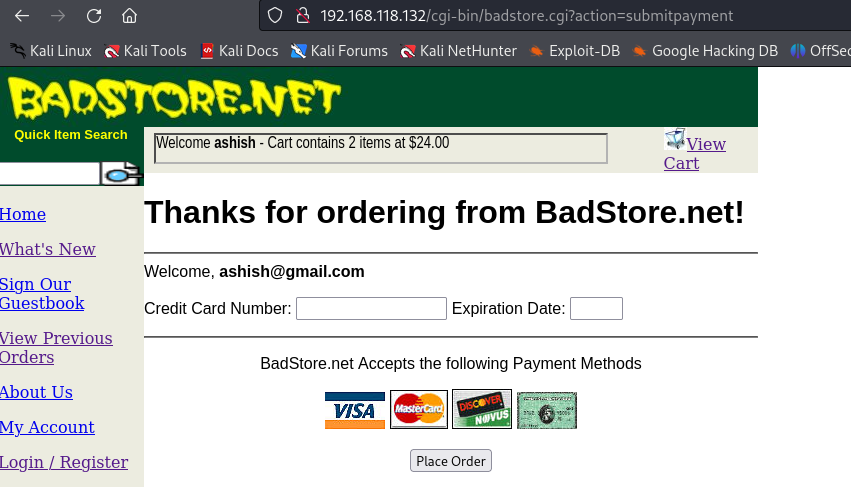


Notice that you are redirected to the home page and action you performed here is cartadd.



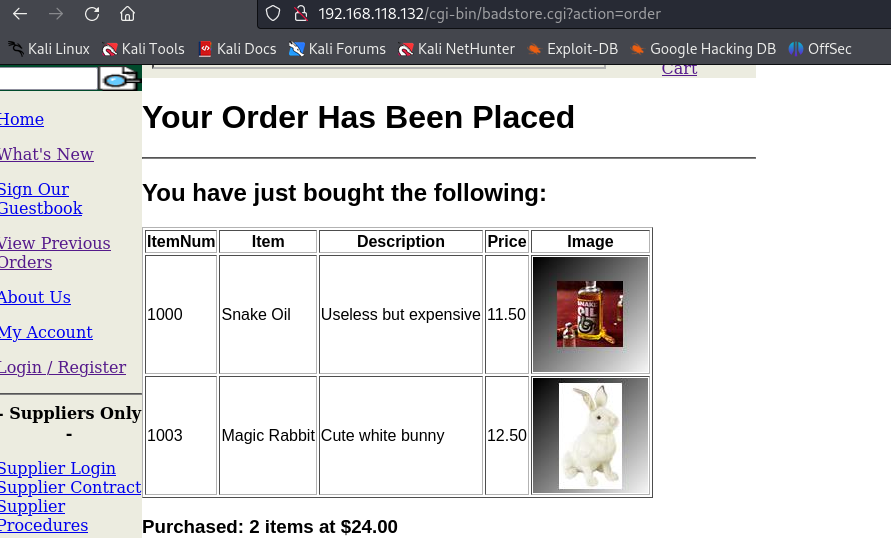
1. Click on View Cart. Notice that the action you performed here is **cartview**



1. It is asking to submit payment. 
2. If we want to bypass **submitpayment** action, we can manipulate the action query parameter and directly place order without payment.

**Change action query parameter in URL to: order**

Your order has been placed without even submitting payment.



Thus, we can use this vulnerability to buy unlimited number of products.

**Prevention**

1. Avoid relying solely on obscurity; employ robust mechanisms instead.
2. Default deny access to non-public resources unless explicitly authorized.
3. Implement centralized access control mechanisms for consistency.
4. Enforce strict guidelines for developers to declare and validate access permissions.
5. Regularly audit and test access controls to ensure effectiveness and compliance.