Part-1 Vulnerability Analysis

15 August 2024

14:24

1. **Web Exploits Identification**  
     
   The attack method used in this scenario was Client-side script injection. The script that was used here was "Tampermonkey script" which is used to manipulate the time zone of the users browser. So when you buy something from G2A sites it is going to marked as expired in G2A's payment processor - Bitbay. But if we pay for the products we will get them and we will also get the refund from G2A in our Bitbay wallet. But the transaction should be higher than 0.0015 BTC.

1. **Potential Damage**

The potential damage it is going to do are:   
 1. Financial Loss

2. Service Disruption

3. Damage to Reputation

1. **Exploit Testing:**

Testing process should be carried out immediately in a safe and isolated environment using CI/CD pipeline or sandbox.  
  
Do a detailed testing running the script and find out the how the script is working and how to prevent that.

1. Minor Bug