مقاوم بودن قرارداد در مقابل حملات متداول:

در تمام کد نویسی قرارداد تلاش شده از هرگونه سوء استفاده و عمل غیر معمول جلوگیری شود. با این حال درمورد خطاهای متداول می توان موارد زیر را ذکر نمود:

- جلوگیری از خطای reentrancy : تنها تابع قرارداد که می تواند بصورت عمومی جهت دریافت پول از قرارداد (در قالب توکن USDT) استفاده شود، تابع withdraw() است که در این تابع ابتدا حذف تمامی اطلاعات مربوط به participant انجام شده و سپس در انتهای تابع انتقال توکن انجام شده (روش CEI). توجه شود هرچند انتقال پول در توابع reset_tender و forced_reset_tender هم انجام می شود، ولی این توابع فقط توسط ادمین قابل فراخوانی هستند (البته کلا فکر نمیکنم reentrancy درمورد توکنها مشکل ساز باشد).
- استفاده از کامپایلر ورژن بالاتر از 0.8.0 که از خطاهای overflow جلوگیری میکند
- استفاده فراوان از دستورات require و revert برای جلوگیری از حالتهای خطای احتمالی
- تعیین مناسب سطح دسترسی توابع در حد مورد نیاز
- جلوگیری از شرکت چند باره افراد در مناقصه
- جلوگیری از اعمال نفوذ در نتیجه مناقصه
- جلوگیری از تقلبهای متداول در مناقصه ها