**مستند امنیت Advanced Idiots Market**

**Improper Inputs**

به منظور جلوگیری از ارسال ورودی های نامعتبر و آسیب رسانی و تهدید سرور ما در همه ی جاهایی که از کاربر ورودی میگیریم و این ورودی های کاربر از طریق سوکت های شبکه به سرور منتقل می شوند، ورودی ها را validate می کنیم و با ارزشیابی دقیق نسبت به فرمت ورودی ها از بروز Exception ها و یا تغییر وضعیت نامطلوب سرور جلوگیری می کنیم.

شرح دقیق این مکانیزم ها در کد ما به صورت زیر است:

* به عنوان مثال در Charge Wallet و Withdraw Wallet در کیف پول هر کاربر از ارسال ورودی های نامعتبر به سرور جلوگیری می کنیم و در ضمن بررسی غدد وارد شده مه از مقدار کیف پول شخص تجاوز نکند، اگر شخص تعدادی کاراکتر نامعتبر غیر عددی را در ورودی وارد کند، پیغام خطای مناسب را چاپ می کنیم و خطای مورد نظر را به کاربر در همان صفحه گزارش داده و از بروز خطاهای بعدی در سرور جلوگیری می کنیم.
* در برخی از صفحه ها از جمله صفحه پرداخت (Payment Page) و ورودی های وارد شده به سرور تعدادی از فیلد های کلیدی را به عنوان فیلد اجباری به کاربر نشان می دهیم و این فیلد ها را به صورت ستاره دار نشان می دهیم که حتما وارد کردن آنها الزامی است تا از بروز خطاهای بعدی در سرور جلوگیری کنیم.
* فرمت ورودی های حساس که ممکن است باعث بروز خطاهای بعدی در فرآیندهای سرور شوند، قبل از ایجاد تغییرات در سرور به طور کامل بررسی کی شوند، مثلا در هنگام ساختن Off ها و Discount Code ها فرمت ورودی هایی مثل start time و end time بسیار مهم است که درست وارد شوند و به همین منظور هم در صورت صحیح نبودن فرمت این ورودی ها در همان مکان پیغام خطای قرمز رنگی را به کاربر نمایش می دهیم و اجازه ی خراب کردن ورودی ها را با اطلاعات اشتباه نمی دهیم.
* در هنگام ثبت نام و ورود هر کاربر، رمز عبور شخص را به صورت )) \*(( نمایش می دهیم و امنیت اطلاعات ورودی را بالا می بریم.
* اگر شخصی فایلی را بخرد دیگر آن فایل برای شخص از بین نمی رود و هروقت که خواست باز هم می تواند آن فایل را از فروشگاه در اکانت خود دانلود کند و دیگر نیاز به خرید دوباره ی فایل نیست. در واقع با سیو شدن این فایل در اطلاعات اکانت شخص دیگر نمیگذاریم او این فایل را دوباره بخرد و از بروز اشکالات بعدی جلوگیری می کنیم.
* مثلا اگر قرار بود RequestId را اکسپت کنیم، اگر آن درخواست وجود نداشت ارور مناسب را به کاربر روی صفحه با یک پیغام قرمز رنگ نمایش می دهیم و از بروز خطاها در سمت سرور جلوگیری به عمل می آوریم.
* مثلا اگر در ساخت یک کالا Category که کاربر وارد می کند وجود نداشت، این اشکال باعث ایجاد خطا در سرور نمی شود و به کاربر این نکته را ذکر می کنیم که ورودی او نامعتبر بوده است.
* به عنوان مثالی دیگر اگر کاربر در صفحه پرداخت در فیلدهای Phone Number یا Postal Code مقداری غیر عددی را وارد کند، به کاربر این خطا را گزارش می دهیم و اجازه ی ورود شماره تلفن هایی که به صورت عبارتی عددی نیستند را می گیریم.

‌**Brute Force Attack**

برای جلوگیری از اینکه فردی با تلاش های متعدد و با اهدافی مبنی بر دور زدن فرم های ورودی برنامه برای ورود به حساب کاربری، ما در برنامه مان اگر شخص ۵ تلاش ناموفق داشت، دیگر اجازه ی تلاش های بعدی و وارد کردن تعداد زیادی رمز و امتحان کردن تعداد زیادی حالت و تخریب و دور زدن فرم های ورودی را به شخص نمی دهیم و اگر فرد بیش از ۵ بار اطلاعات را اشتباه وارد کرد، یک تایمر به کاربر نمایش می دهیم و تا ۲ دقیقه ی دیگر (۱۲۰ ثانیه) اجازه ی ورود اطلاعات و تلاش برای ورود را به شخص نمی دهیم و دکمه های ورود را برای شخص غیر فعال می کنیم تا از تلاش های بعدی او جلوگیری کنیم و نتواند فرم را دور بزند.