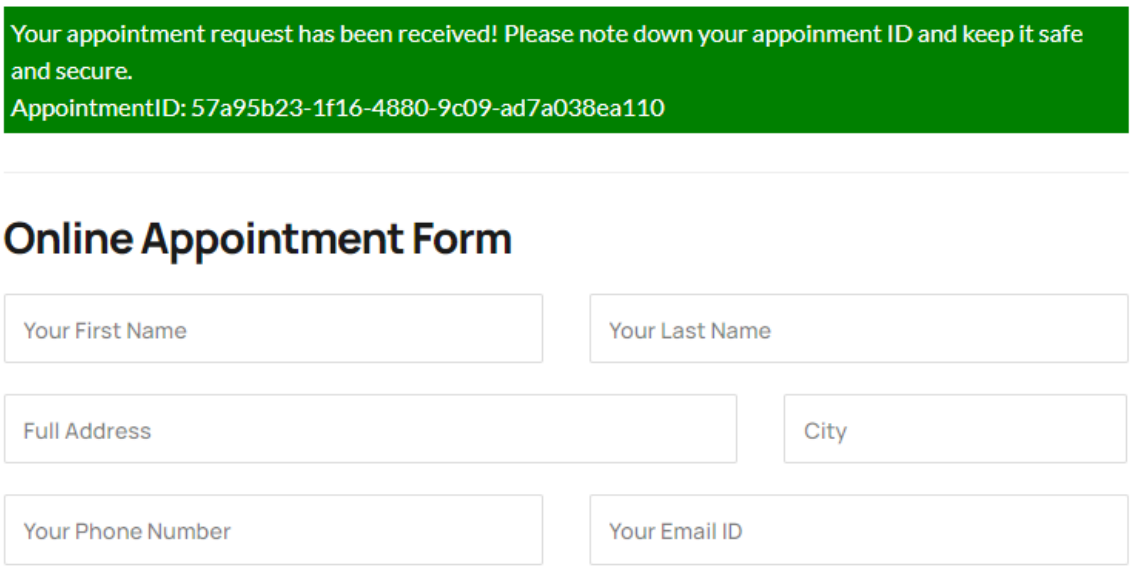
An example of this can be seen on FirstBlood. When creating an appointment you are given a GUID value to manage it:



From just performing this action I have so many questions already going through my head. Has this value been leaked anywhere on the site, or perhaps it's been indexed by Google? This is where I'd start looking for more keywords such as "appointment_id", "appointmentID".

I had another case where I noticed the ID was generated using the same length & characters. At first me and another researcher enumerated as many combinations as possible but later realised we didn't need to do that and we could just simply **use an integer value**. Lesson learnt: even if you see some type of encrypted value, **just try an integer**! The server may process it the same. Security through obscurity. You'd be surprised how many companies rely on obscurity.

When starting on a program I will hunt for IDORs specifically on mobile apps to begin with as most mobile apps will use some type of API and from past experience they are usually vulnerable to IDOR. When querying for your profile information it will more than likely make a request to their API with just your user ID to identify who you are. **However there is usually more to IDOR than meets the eye**. Imagine