الاتحاد السعودي
للأمن السيبراني
والبرمجة والدرونز
Saudi Federation
for Cybersecurity,
Programming,
and Drones

Version 1.0

Program Start-Up Guide

برنامج
مكافآت
الثغرات
BugBounty.sa

Getting Started

Congratulations on deciding to set up your Bug Bounty program on BugBounty.SA !

Here are the steps that'll get you up and running.

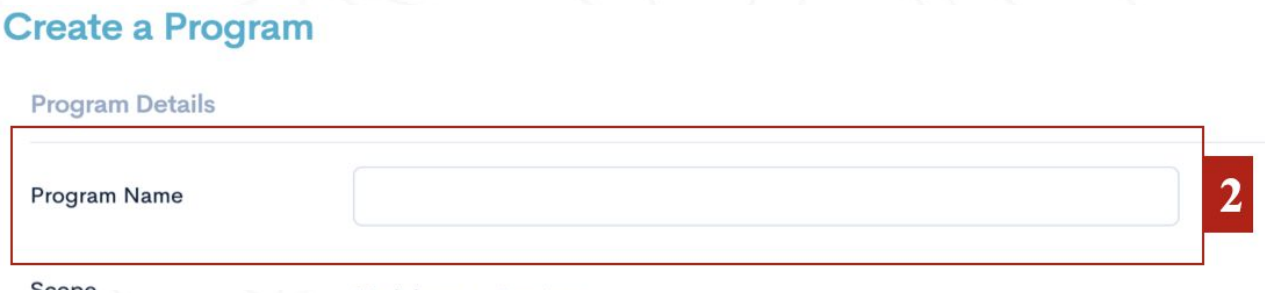
Getting Started

- Go to BugBounty.SA
- Click **Sign Up**.
- Fill out all fields on the form.
- A confirmation email will be sent asking you to confirm your email address.
- Go to your email and click **Confirm email address**.
- When you confirm, a form will appear, fill out all fields on the form.
- A verification code will be sent asking you to verify your mobile number.
- Go to your mobile and enter the code received in SMS.

Create Program

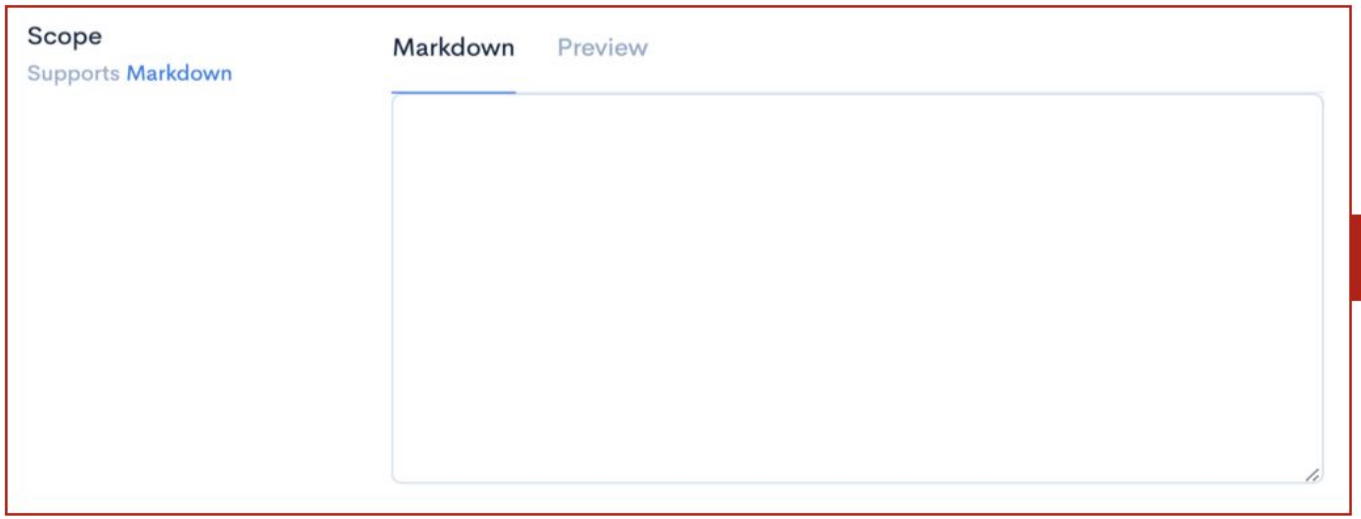
1. When your account is activated, Click **Create Program.** You'll be taken to a page where you can Enter the program details.

2. **Program Name:** Which is the name of the program that is going to be appear in the platform.



Scope

Your scope is the collection of assets you want the researchers to work on. When you list the assets the researchers required to select the applicable assets of each report he/she provide, you can write the Scope using Markdown editor.



3

Scope - Example

Scope
Supports Markdown

Markdown Preview

Description of the Product

[describe briefly what is your product do]

Scope

[here you can list your digital assets within the scope]

Service	Domain
Google Search engine	Google.com

Out of the scope

[here you can specify the type of attacks, number of assets out of the scope]

Examples

- Attacks requiring physical access to a user's device
- Any physical attacks against Twitter property or data centers
- UX issues not relating to security impacts
- Vulnerabilities of any third-party software or application that interact with Bitpanda Services
- Social engineering & identity theft actions
- Vulnerabilities in any open-source library
- Vulnerabilities in existing banking functionalities

Policy

The policy section enables organizations to publish specific policy they want the researcher to follow when they participate in the program.

Policy - Example

Policy

Supports Markdown

Markdown | Preview

Please follow the below policies while you are working on our programs, any violation of any of these policies will disqualify your report.

[here you can specify the policies you want the researcher to follow while participating within your program] *Example*

- Reports from automated tools or scans are not acceptable.
- You must be the first reporter of the vulnerability.
- The vulnerability must demonstrate security impact to a site or application in scope.
- Do not intentionally harm the experience or usefulness of the service to others, including degradation of services & denial of service attacks, if you did you may.
- Do not attempt to view, modify, or damage data belonging to others.
- Do not disclose the reported vulnerability to any person/social media account/etc.. .
- You must agree and adhere to the Program Rules and Legal terms as stated in this policy.
- You must be available to supply additional information, as needed by our team, to reproduce and triage the issue.

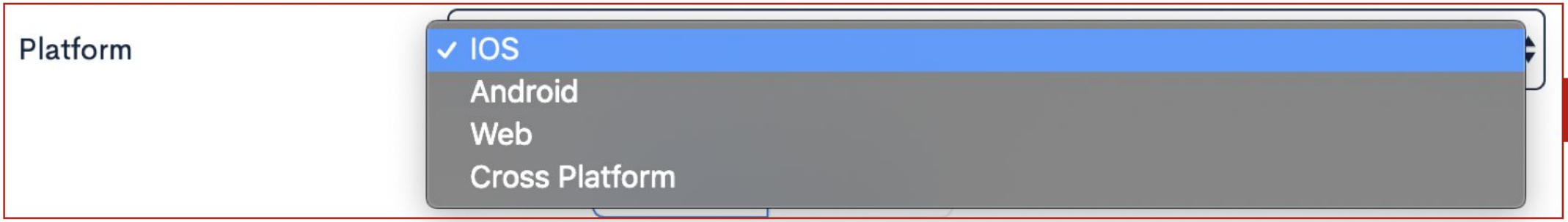
Start & End Date

The Duration period of the program, during this time the program will be available to the researcher and receive the reports from them in the platform.

Platform

It is an asset type. You can choose one from these options:

IOS, Android, Web or Cross Platform.



Type

- **Public Program:**

All researchers on BugBounty.SA can view the program on the platform and participate in it.

الاتحاد السعودي
للأمن السيبراني
والبرمجة والدرونز

Saudi Federation
for Cybersecurity,
Programming,
and Drones