# FIRST Bug Bounty Program

FIRST encourages security researchers to disclose security vulnerabilities in our services to FIRST in a responsible way. We support independent security research. Security evaluations must:

- Be performed on the *.first.org domain;
- Not be performed on the sites of letsencrypt.org, UltraDNS, Certain (events.first.org) or any of the services these vendors operate for FIRST. If you inadvertently find an issue while using these services on FIRST.org, we'd like to hear about it. However, we cannot provide permission to test these third parties.
- Not compromise the security or privacy of FIRST members, or the data on our systems;
- Not destroy information or affect the availability of our services;
- Not involve social engineering or evaluate the physical security controls around our systems.

Please send any issues you identify to bugs@first.org. We appreciate it if you could include the following information:

- Your contact information, so we can follow up with questions;
- A description of the issue and its nature;
- Detailed steps that allow us to reproduce the issue;
- A brief description of the security impact of the issue.

Please specify if we may publicly credit you on this page. In case you need to send any sensitive information, please encrypt the message using the bug bounty PGP key.

As a non-profit, we can't pay out major bounties, but we really appreciate your help in helping safeguard our systems. If we confirm your finding as a vulnerability, we will send you a token of our appreciation.

We also welcome reports of simple bugs with no security impact, and will do our best to address them as soon as possible. However, those reports are not eligible for a token of our appreciation.

# Hall of fame

## 2020

- Akash Rajendra Patil — found a user enumeration vulnerability in one of our services, fixed.
- Austin Augie (api_0) — found a directory traversal vulnerability, fixed.
- Luiz Paulo Viana — found an open redirection at FIRST website, no longer available.
- Zin Min Phyo — found a clickjacking vulnerability in one of our services, fixed.

## 2019

- Albin Thomas — found a misconfiguration in one of our services, fixed.
- Leo Starcevic — found an open redirection in one of our services, fixed.
- Mustafa Diaa (@c0braBaghdad1) — found a vulnerable deprecated service, fixed.
- Mohammed Israil — found a misconfiguration at the DNS service, fixed.
- Shivam Khambe — found an open redirection based on headers, fixed.

## 2018

- Mohammed Israil.
- Abhishek Misal — found an open redirection in the training service, fixed.
- Hosein Askari — found out that the website was vulnerable to some DoS attacks, fixed.
- Vyshnav Vizz — found a misconfiguration at the website, fixed.
- Mayank Kamboj — found a service with deprecated encryption ciphers, upgraded.
- Mayank Kamboj — found an application vulnerable to brute-force, fixed.

- Ali Kabeel (Logic Breaker) — found a clickjacking vulnerability on MISP, fixed.
- Ali Kabeel (Logic Breaker) — found a XSS exception in the membership application, fixed.
- Mahmoud Barakat (@0xBarakat) — found a XSS exception in the membership application, fixed.
- Dipak Prajapati — discovered that the issue tracking service was vulnerable to brute-force attacks, fixed.
- Prathamesh Joshi (@Pr4th4m_Joshi) — found a misconfiguration in the training service, fixed.
- Eric Head (@todayisnew) — found ways to retrieve sensitive information requesting the hidden metadata directory that version control tool Git creates, fixed.

## 2017

- Dinar Gataullin — found a vulnerability (CRLF-injection) in the members website, fixed.
- Lewis Philbey — discovered a bug in the certificate authentication for MISP, fixed.
- Vineet Kumar — found a stale DNS entry that could lead to a subdomain takeover, fixed.
- Muzamil Shah — discovered a race condition on the public account sign up, fixed.
- Ali Kabeel (Logic Breaker) — discovered a form that enabled external content as the input field default parameters, fixed.
- Ali Kabeel (Logic Breaker) — found a XSS/CORS vulnerability in a membership service, fixed.
- Ali Kabeel (Logic Breaker) — found a CSRF bug in the membership process, fixed.
- Jacob G. Deniega — found a CSRF in the former dues server, which was updated.
- Yasser Gersy — found that external links might be vulnerable to Tabnabbing, fixed.

- Mazen Gamal (@mazengamal) — found an outdated service, with potential security vulnerabilities. Fixed.
- Andrea Mortiz (@vulnzdotcom) — found sensitive information disclusure in past event registration sites. Fixed.
- Issam Rabhi — found a XSS vulnerability in older conference assets. Assets removed.
- Ahmed Wahed and Ebrahim Hegazy (@Zigoo0) — found a XSS in the webserver responsible for dues collections. Fixed.
- Eslam Mohamed Reda — found a way to bruteforce some generated code for email address verification.
- Moaad Ali (aLLamoox) — found ways to retrieve registered e-mails through bruteforce attacks to the signup page. Fixed it.
- Ebrahim Hegazy (@Zigoo0) — found a serious directory traversal bug in api.first.org. Fixed it immediately.
- Ebrahim Hegazy (@Zigoo0) — found an unprotected administration panel on a beta service. Fixed it.
- Khaled Sakr — found a way to circumvent the web server's routing setup and managed to end up at the old web page, where he still found the CSRF vulnerability again. In addition he found a bug at the signout page. Nice catch! We fixed it.
- Shailesh Suthar — found a redirection bug in the FIRST login page. Fixed it.
- Jacob G. Deniega — found a webserver information disclosure (nginx version) via server tokens. Nginx reconfigured, fixed.
- Eslam Mohamed Reda — found a CSRF vulnerability in the login and sign in page. It was solved by replacing the old framework / website with a new one (which was planned anyway).

## 2016

- Dinar Gataullin — found a bug in the CVSS calculator. This was inside an outdated JS library.

# Note well

- **Reports of vulnerabilities** by researchers based in sanctioned countries. We're terribly sorry, but for legal reasons we cannot ship any token of appreciation to countries on various sanctions lists, such as Iran, North Korea and Syria. A full list of sanctioned entities can be found on the site of the US Department of Treasury. We will be happy to fix your report, and list you in our Hall of Fame, though. As a US incorporated organisation we are bound to local laws.
- **Logout CSRF**: CSRF vulnerabilities whose maximum impact is for the user to log out of the authenticated part of our web sites are difficult to defend against and don't expose customer data to risk, hence they are out of scope for our program.
- **Presence of banner or version information**: for various reasons, we may determine to mask the version of a daemon, or not do so to ensure the service is more predictable. If the service isn't vulnerable to an issue, we do not consider simply learning its version a security vulnerability.
- **Configurations which are explicitly stated in policy**: for instance, for some of our domains, we may monitor for policy violations, rather than block them. An example is softfail SPF and DKIM.
- **Third party software vulnerabilities**: we will be happy to work with you to have the vulnerability reported upstream in the third party software. But please bear in mind that we can not take responsibility for third party software bugs unless they are the result of us configuring something wrongly. Hence, these bugs will be out of scope for our program.