This document should highlight the efforts made in developing ERP5 on a test-driven basis. It should introduce the infrastructure and methodologies used for testing, provide access to latest test results along with guidelines for developing and contributing to ERP5.

Test-Driven Development

Developing ERP5 is not possible without the use of automated testing. The following documents provide more information on the ERP5 test infrastructure including latest test results along with guidelines and instructions on how to setup, write and run tests.

- **Test Infrastructure and Latest Results** (approach, types of tests)
- **Guideline Best Testing Practice** (test frameworks, which tests to use when)
- **Run Zelenium Tests** (installation and setup)
- **Write Zelenium Tests** (hints, notes, debugging)

ERP5 Conventions

ERP5 has over the years evolved to over 10 million lines of code. Focussing on the **Unified Business Model** along with strict rules and conventions regarding naming and programming ensure that the codebase stays easy to understand with the **Documentation HowTos** providing insights into specific functionalities and behaviors.

The following documents from the Developer Guidelines introduce the respective conventions relevant for programming ERP5:

- **General Programming Conventions**
- **JavaScript Programming Conventions**
- **Best Coding Practices** (coding within ERP5)
- **Best Commit Practices** (working with ERP5 and Git)

Code Repositories and Contributing

The ERP5 source code is hosted on Gitlab at [lab.nexedi.com](http://lab.nexedi.com) with an internal issue tracker being used by ERP5 developers. As contributing to ERP5 requires to learn the ins and out for at least a year (getting started), there are currently no contributing guidelines but this might change in the future. In the meantime please post in the public Forum in case you have any issues or questions.

Security

Below is a list of publicly filed common vulnerability and exposure (CVE) issues, which have been filed and are being worked on to be fixed.

<table>
<thead>
<tr>
<th>CVE-ID</th>
<th>Version</th>
<th>Type</th>
<th>Acknowledged</th>
<th>Published</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2020-28056</td>
<td>ERP5 v5.5</td>
<td>XSS (Cross Site Scripting)</td>
<td>2020-09-28</td>
<td>2020-11-02</td>
<td>In progress - working on a fix</td>
</tr>
</tbody>
</table>

**Impact**

The impacts can be many, and vary from the theft of information and credentials to the redirection to malicious websites containing attacker-controlled content, which in some cases even cause XSS attacks. So even though an open redirection might sound harmless at first, the impacts of it can be severe should it be exploitable.