# Writing an offerte

## Tools

First of all, make sure you have the right tools installed. Check the tools manual for more info.

## Main structure

The report's main element is <offerte>. It contains a number of major parts:

* Entity listing, in the doctype. These are fields that will be reused throughout the document, mostly in boilerplate text
* Document information (metadata), in the element <meta>
* A variable number of sections (main content), in several <section> elements
* A waiver annex, in the <annex> element (located in the snippets directory as it is also boilerplate text)

## Entity listing

When you have your scoping information, fill in all the fields. They are commented in the template, so what to fill in should be pretty self-explanatory.

You should be able to fill all fields. The only exception is c\_waiver\_rep, as it is not always known in advance who this will be.

## Document information / metadata

This is the part where we put all information that is *about the offerte* rather than about the offer itself (hence the term metadata): who has been working on it, what is the offer about, what versions has it gone through, etc.

In XML, this part is indicated by the <meta> element. It contains the following elements (mandatory and in the listed order):

* The offered service, in the <offered\_service> element
* Client information, in the <client> element
* Your-company-related information, in the '' element
* Targets listing, in the <targets> element
* The document's version history, in the <version\_history> element

You need to fill in everything *that isn't already filled in with an entity*. If there is an entity, the info will be taken from the scoping info you entered in the entity list above. So leave it alone. No need to do anything.

For more details, see the sections below.

### The offered service

In the <offered\_service> element, put the offered\_service (in text). This is something like 'penetration testing services' probably.

Example: <offered\_service>penetration testing services</offered\_service>

**No need to do anything here, the entity takes care of this**

### Client information

The <client> element contains four other elements:

* <full\_name>, in which you should type the client's official name, e.g. 'Sitting Duck BV', or 'Big International Company Ltd'
* <short\_name>, in which you should type the client's shorter name, e.g. 'Sitting Duck' or 'Big International' (or, if there is no shorter name, just type the long name again)
* <city>, in which you should type the city where the client's office is based
* <legal\_rep>, in which you should type the name of the client's legal representative, i.e. the guy or gal who can sign the offerte.
* <waiver\_rep>, in which you should type the name of the client's legal representative, i.e. the guy or gal who can sign the waiver. If the legal rep is not known when you are creating the offerte, you can delete this element. The waiver will then be generated with a little line on which the legal rep can write his/her own name.

Example:

<client>  
 <full\_name>Sitting Duck B.V.</full\_name>  
 <short\_name>Sitting Duck</short\_name>  
 <city>Amazonia</city>  
 <legal\_rep>Shaniah T. Brick</legal\_rep>  
 <waiver\_rep>William Wonder</waiver\_rep>  
</client>

**If all names are known, no need to do anything here, the entity takes care of this. If the waiver rep is not known, delete the waiver\_rep element.**

### Company information

The <company> element contains two other elements:

* <full\_name>, in which you should type your company's official name
* <legal\_rep>, in which you should type the name of your legal rep

Example:

<company>  
 <full\_name>Shining Armour B.V.</full\_name>  
 <legal\_rep>Sir Lancelot</legal\_rep>  
</company>

### Targets

The <targets> element contains one or more <target> elements, one for each target specified for the pentest. Put every target of the pentest in its own <target> element. If there is only one target, you'll end up with a <targets> element containing only one <target> element. This is ok.

Example:

<targets>  
 <target>fishinabarrel.sittingduck.com</target>  
 <target>hackthis.sittingduck.com</target>  
 <target>Sitting Duck's support staff</target>  
<targets>

### Pentest Info

The <pentestinfo> element contains some data about the pentest itself. This element is useful as you can refer to its content using placeholders, allowing e.g. for standard referrals to the tested application name, pentest type or pentest duration.

Example:

<pentestinfo>  
 <duration>10</duration><!-- duration of pentest, in working days -->  
 <test\_planning>January 1st until January 12th, 2015</test\_planning> <!-- date or date range in text, e.g. May 18th until May 25th, 2015 -->  
 <report\_writing>January 15th until January 20th, 2015</report\_writing> <!-- date or date range in text, e.g. May 18th until May 25th, 2015 -->  
 <report\_due>January 23rd, 2015</report\_due> <!-- date or date range in text, e.g. May 18th until May 25th, 2015 -->  
 <nature>time-boxed</nature>  
 <type>black-box</type><!-- please choose one of the following: black-box, grey-box, crystal-box -->  
 <fee>50000</fee><!-- euro is added automatically in the document -->  
 <target\_application>FishInABarrel</target\_application><!-- name of application to be tested (if any) -->  
 <target\_application\_producer>H4ckers 'R' Us</target\_application\_producer>  
 </pentestinfo>

### Version History

The <version\_history> element contains one or more <version> elements, one for each version of the document you create. Whenever you start a new version, add a <version> element to the list.

The <version> element should contain the following:

* a date attribute with a date of your version as a value, in the format YYYY-MM-DDT00:00:00, e.g. 2015-04-18T00:00:00
* a number attribute with the version number as a value. This value can either be 'auto' or an actual version number, e.g. 1.0. If you use the 'auto' value, the system will automatically count it (starting with 0.1 for the first <version> element and going up from there: 0.2, 0.3, etc...).
* One or more <v\_author> elements, each containing the name of the person who worked on this version (that would be you at least, and perhaps a pentester or colleague who did significant work on it)
* A <v\_description> element with a (very short!) description of what has been done in this version, e.g. 'Added non-findings' or 'Revision'

Example:

<version\_history>  
 <version number="auto" date="2014-12-18T00:00:00">  
 <v\_author>Bob Goudriaan</v\_author>  
 <v\_description>Initial draft</v\_description>  
 </version>  
 <version date="2014-12-22T00:00:00" number="auto">  
 <v\_author>Bob Goudriaan</v\_author>  
 <v\_author>Patricia Piolon</v\_author>  
 <v\_description>Revision</v\_description>  
 </version>  
</version\_history>

## Sections

The main bulk of the offerte is made up of normal content. We divide our content into sections using the <section> element.

### Section title

A section must always start with a <title> element, which should only contain text; after that you're free to do what you want. As explained in the previous section, it's a good idea to have the section id and the title be somewhat related.

Example:

<section>  
 <title>Project Planning</title>  
 ...  
</section>

### Section content

As said, after the title, anything goes (well, almost):

* A section can be subdivided into smaller sections
* A section can contain generic content, that is to say any number and order of:
  + paragraphs (<p>)
  + lists (ordered <ol> or unordered <ul>)
  + tables (<table>)
  + command input/output boxes (<pre>)
  + code (<code>)
  + div containers (<div>)
* A section can contain a signing box for the offerte itself (<generate\_offer\_signature\_box/>)
* A section can contain a listing of targets, taken from the <targets> element in the meta section (<generate\_targets/>)

All of these elements are described elsewhere in this document; see the appropriate sections for details.

## Annexes

Annexes (using the <annex> element) work the same as sections, they just come last in the report. Like sections, they must start with a title. Also like sections, the rest of their content is free-form.

You will need at least one annex in the template, for the waiver. An annex can contain a signing box for the waiver (<generate\_waiver\_signature\_box/>)

Example:

<annex>  
 <title>Annex 1: Waiver</title>  
 <p>You waive all responsibility.</p>  
 <generate\_waiver\_signature\_box/>  
</annex>

## Generic content

Generic content is modeled on very basic HTML.

### Paragraphs

Paragraphs (<p>) go in sections or in the various sub-elements of findings and non-findings. They are the basic way of displaying text.

Example:

<p>This is a paragraph</p>

### Lists

Lists can be ordered (<ol>, for '**o**rdered **l**ist') or unordered (<ul>, for **u**nordered **l**ist). Regardless of whether a list is ordered or unordered, it contains one or more list items (<li>, for **l**ist **i**tem).

**Unordered lists**

Example:

<ul>  
 <li>Some item</li>  
 <li>Some other item</li>  
</ul>

**Ordered lists**

Ordered lists are numbered by default. You can configure a different ordering system by setting its type attribute to one of the following values:

|  |  |
| --- | --- |
| type | ordering |
| a | lowercase alphabetic |
| A | uppercase alphabetic |
| i | lowercase roman |
| I | uppercase roman |

Example:

<ol type="i">  
 <li>Some item</li>  
 <li>Some other item</li>  
</ol>

### Code/Input/Output Blocks

Whenever you need to display some command line input/output or code, use the <pre> element. It will conserve any whitespace you leave, so you can format the contents of this element in a pleasant/readable way. Use spaces for indents. Note that text in the <pre> element *will not wrap*.

Example:

<section>  
 <title>Some output</title>  
 <p>This is some relevant stuff the client sent us:</p>  
 <pre>'relevant stuff'</pre>  
 <p>And this too:</p>  
 <pre>this relevant stuff comes  
in several lines  
 Some indented  
and some not  
  
This is not a haiku.</pre>  
</section>

#### Help! The code in my pre element contains < characters and it messes with my xml!

You can escape the < character by replacing it with its entity &lt;.

### Div containers

#### What does <div> do?

Nothing. <div> just *is*.

#### Sigh. Ok, why *is* <div>?

You can use <div> as a container for other block elements. This is basically only (but very) useful for snippets, as snippets need to be well-formed XML documentlets and can therefore only have one root element. If the snippet is a complete section, this is not a problem. If the snippet is a bunch of paragraphs or something, your snippet can be <div> (root element), containing everything you want. Well, everything that's allowed, anyway.

#### So what's allowed in <div>?

All block elements: <p>, <ul>, <ol>, <table>, <img>, <pre>, <code>

#### And what elements can *contain* <div>?

<section> and <annex>.

### Tables

**Rows**

Tables consist of a <table> element containing one or more rows (<tr>).

Example:

<table>  
 <tr>...</tr>  
 <tr>...</tr>  
</table>

**Cells**

A table row consists of one or more cells (<td>).

Example:

<table>  
 <tr>  
 <td>Cell 1 in row 1</td>  
 <td>Cell 2 in row 1</td>  
 </tr>  
 <tr>  
 <td>Cell 1 in row 2</td>  
 <td>Cell 2 in row 2</td>  
 </tr>  
</table>

Columns are implicit: each cell in a row corresponds to a column.

**Header Cells**

Instead of normal cells, you can also use header cells (<th>) for a table header.

Example:

<table>  
 <tr>  
 <th>Header cell 1 in row 1</th>  
 <th>Header cell 2 in row 1</th>  
 </tr>  
 <tr>  
 <td>Cell 1 in row 2</td>  
 <td>Cell 2 in row 2</td>  
 </tr>  
</table>

**Borders**

To turn on borders for your table, set its border attribute to '1'.

Example:

<table border="1">  
...  
</table>

You can also turn borders on or off (border="0") on lower levels (on the row level, for example) for finer-tuned border control.

**Setting column width**

To set the width for your columns, add a number for each column to the cols element. This number is in millimeters (you can either type 200mm or just 200; don't use cm or pt or px or other measures though). The total width between the margins is 17cm, so 170mm.

Example:

<table cols="50 50 70">  
 <tr>  
 <td>cell 1</td><td>cell 2</td><td>cell 3</td>  
 </tr>  
 <tr>  
 <td>cell 4</td><td>cell 5</td><td>cell 6</td>  
 </tr>  
</table>

This will give the first column a width of 50mm (5cm), the second as well, and the third a width of 70mm (7cm).

**Spanning multiple rows/columns**

To make a cell span multiple columns, set its colspan attribute to the number of columns you want to span.

Example:

<tr>  
 <td colspan="2">This cell spans the two cells in the row below.</td>  
</tr>  
<tr>  
 <td>Cell 1 in row 2</td>  
 <td>Cell 2 in row 2</td>  
</tr>

To make a cell span multiple rows, set its rowspan attribute to the number of rows you want to span.

Example:

<tr>  
 <td rowspan="2">This cell spans the two cells in the second column.</td>  
 <td>Cell 2 in row 1</td>  
</tr>  
<tr>  
 <td>Cell 2 in row 2</td>  
</tr>

**Alignment**

Set the align attribute of any cell, row or table to one of the following values to change the text alignment in that cell/row/table:

|  |  |
| --- | --- |
| align | result |
| right | right alignment |
| center | centered |
| justify | justified |

## Images

To insert an image, use the <img> element. In its src attribute, enter the relative path to the image file you want to reference.

To set the height or width, use *either* the height or width attribute. Any numerical value you enter will be interpreted as centimeters.

If you set both, only the width will be interpreted.

If you do not set any height or width, the image will be displayed at full page width (i.e. 17 cm wide)

Example: <img src="../graphics/xmlsignatureexclusion.png" width="5"/>

Optionally, you can set an image caption by adding some text in the title attribute.

Example: <img src="../graphics/xmlsignatureexclusion.png" width="5" title="This is a funny picture LOL"/>

### Inline elements

Inline elements are elements that modify the text inside e.g. a paragraph or a list item, for styling or linking purposes. You have the following options available to you:

**Bold**

To make text bold, wrap it in <b> tags.

Example:

<p><b>This text is bold</b> and this text is not.</p>

**Italic**

To make text italic, wrap it in <i> tags.

Example:

<p><i>This text is italic</i> and this text is not.</p>

**Underline**

To make text underlined, wrap it in <u> tags.

Example:

<p><u>This text is underlined</u> and this text is not.</p>

**Monospace**

To have inline text in a monospace font, wrap it in <monospace> tags.

Example:

<p><monospace>This text is monospace</monospace> and this text is not.</p>

**Superscript**

To have inline text in superscript, wrap it in <sup> tags.

Example:

<p><sup>This text is in superscript</sup> and this text is not.</p>

**Subscript**

To have inline text in subscript, wrap it in <sub> tags.

Example:

<p><sub>This text is in subscript</sub> and this text is not.</p>

**Links**

Link to web pages using the <a> element.

In the href attribute of the <a> element, type the url of the website you're linking to.

Example:

<p>Please refer to <a href="http://www.radicallyopensecurity.com">our amazing website</a>.</p>

## Manual breaks

### Line breaks

Mostly text is broken automatically (between paragraphs etc.) but in some rare cases you may need to insert a manual line break. To do so, use the <br/> element.

Example:

<p>This is my haiku<br/>  
my line is broken, but still<br/>  
the paragraph flows</p>

### Page breaks

To force a page break before or after a section, set its break attribute to 'before' or 'after'.

Note: breaks are inserted automatcally before every appendix and before/after the index.

Example:

<section break="before">  
<title>Technical Findings</title>  
...  
</section>