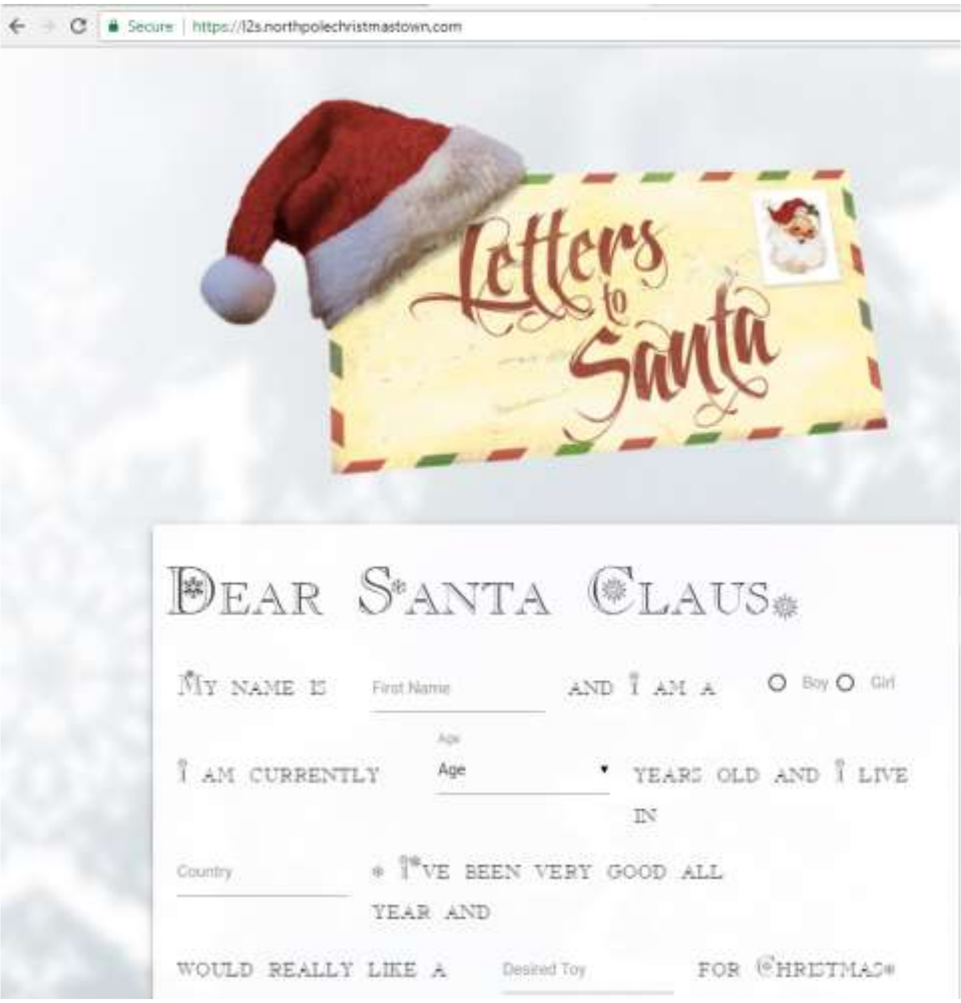
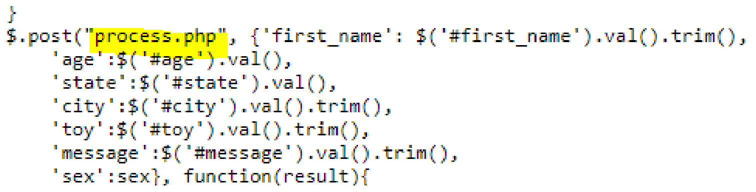
Letters to Santa--a real world attack

Part 2, Beginning Reconnaissance and Verifying Scope

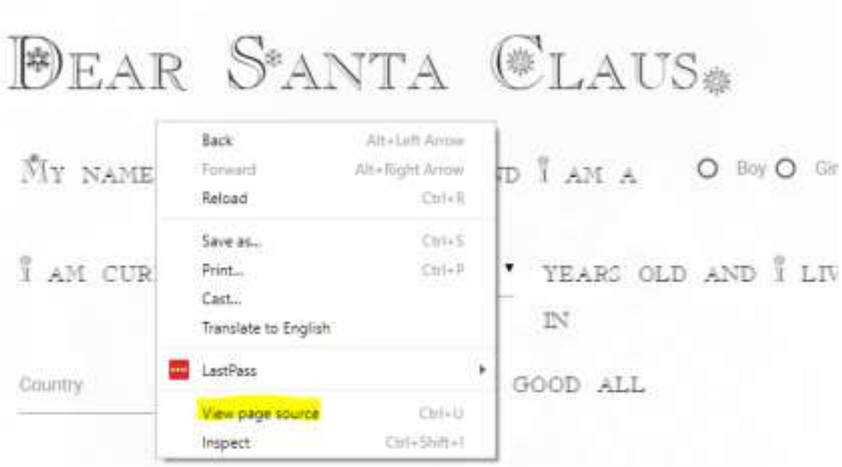
In Part 1 you were tasked to investigate the Letters to Santa site, looking especially for items left over from site development that may expose the site to attack. A quick look at the site shows that it is designed to allow children to request Christmas gifts from Santa.


Secure | https://l2s.northpolechristmastown.com
Letters to Santa
Dear Santa Claus
My name is First Name and I am a ○ Boy ○ Girl
I am currently Age Age years old and I live in
Country I've been very good all year and
would really like a Desired Toy for Christmas

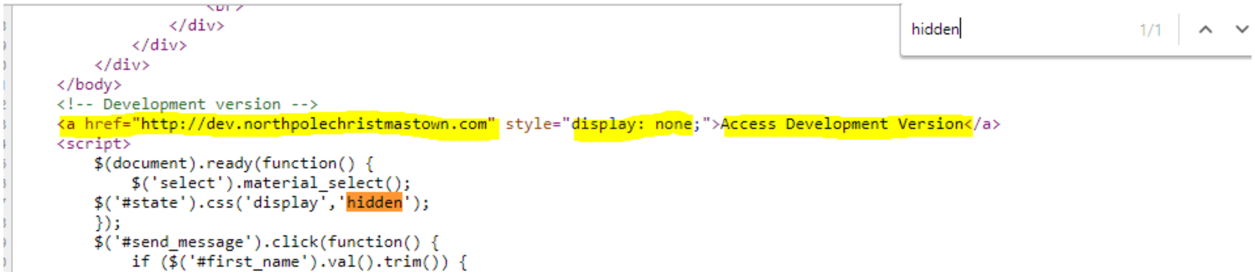
Using "view page source" on the site does show interesting things. You can see that the site sends the letter to Santa using process.php, so the site probably runs PHP.



```
}
$.post("process.php", {'first_name': $('#first_name').val().trim(),
    'age':$('#age').val(),
    'state':$('#state').val(),
    'city':$('#city').val().trim(),
    'toy':$('#toy').val().trim(),
    'message':$('#message').val().trim(),
    'sex':sex}, function(result){
```



Two more things in the source are interesting.



```
            </div>
        </div>
    </div>
</body>
<!-- Development version -->
<a href="http://dev.northpolechristmastown.com" style="display: none;">Access Development Version</a>
<script>
    $(document).ready(function() {
        $('select').material_select();
    $('#state').css('display','hidden');
    });
    $('#send_message').click(function() {
        if ($('#first_name').val().trim()) {
```

There is a hidden field called “#state” that may be worth looking at. However, the link to the development version of the site demands immediate inspection. Notice that it is a link, but it is not shown on the web page because its style is “display: none”. Let’s look at that first.

Visit the site https://dev.northpolechristmastown.com. It certainly looks interesting, but is it in scope? Remember that only l2s.northpolechristmastown.com and the IP address associated with it are in scope.

Questions--Part 2

1) What is the IP address associated with https://l2s.northpolechristmastown.com?
2) What is the IP address associated with https://dev.northpolechristmastown.com?
3) Is the development site in scope?