XSS-01

SVG is good, because it is useful to shorten the attack vector but also due to its XML-ish nature.

This means that once we use entities inside an SVG's <script> element (or any other CDATA element), they will be parsed as if they were used in canonical representation.

Therefore, to bypass the filter, the solution is to call alert(1) with the open parenthesis char (encoded, i.e. (or even shorter (.

You can also use (

Sample solution:

```
<svg><script>alert&#40;1)</script>
```