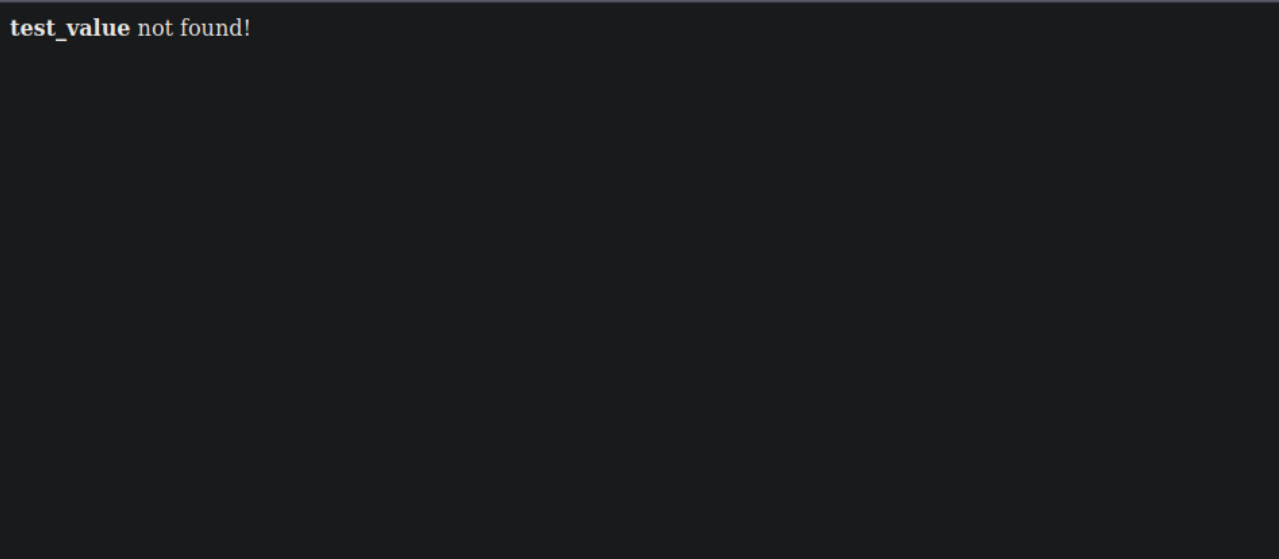
# Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) vulnerabilities affect web applications and APIs alike. An XSS vulnerability may allow an attacker to execute arbitrary JavaScript code within the target's browser and result in complete web application compromise if chained together with other vulnerabilities. Our [Cross-Site Scripting (XSS)](https://academy.hackthebox.com/module/details/103) module covers XSS in detail.

Proceed to the end of this section and click on Click here to spawn the target system! or the Reset Target icon. Use the provided Pwnbox or a local VM with the supplied VPN key to reach the target API and follow along.

Suppose we are having a better look at the API of the previous section, http://<TARGET IP>:3000/api/download.

Let us first interact with it through the browser by requesting the below.

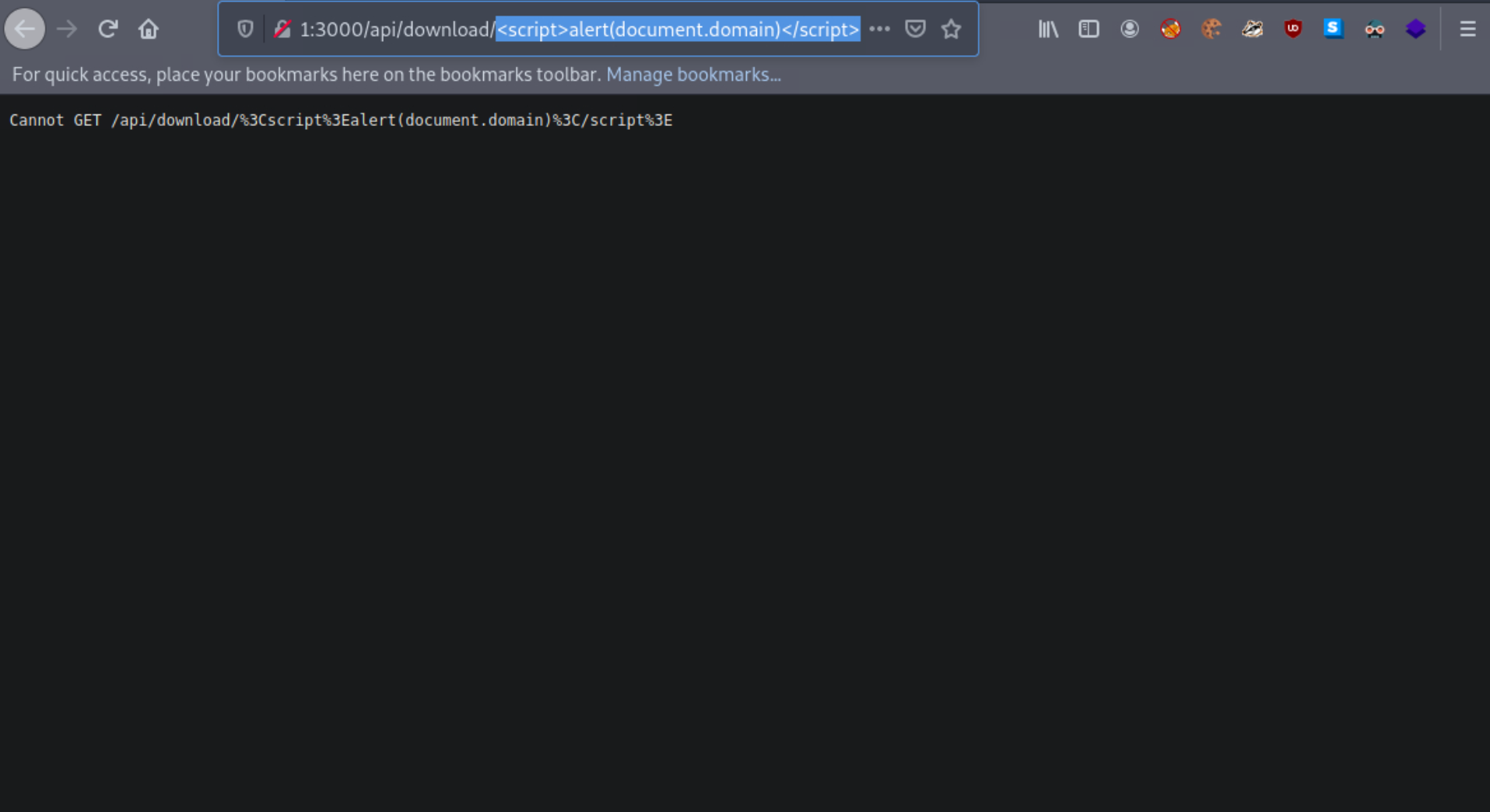


test\_value is reflected in the response.

Let us see what happens when we enter a payload such as the below (instead of *test\_value*).

Code: javascript

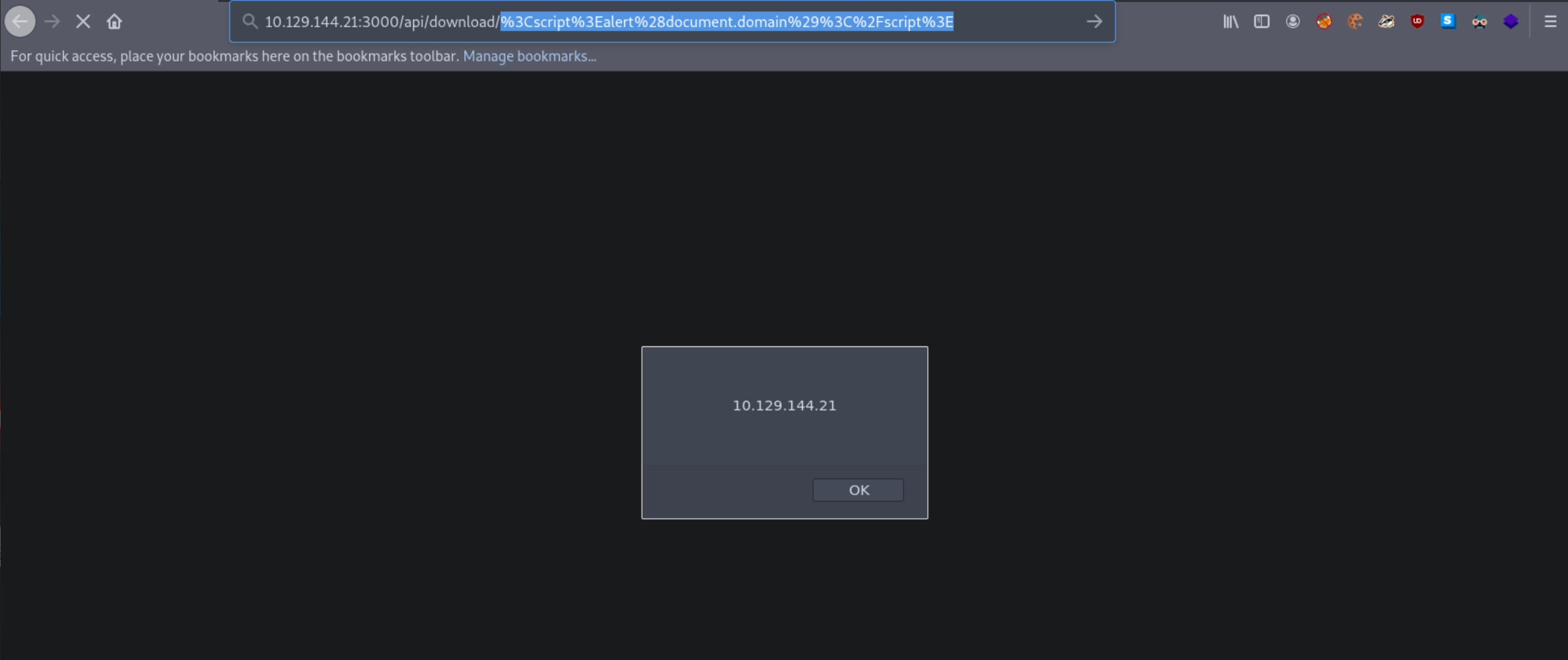
<script>alert(document.domain)</script>



It looks like the application is encoding the submitted payload. We can try URL-encoding our payload once and submitting it again, as follows.

Code: javascript

%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E



Now our submitted JavaScript payload is evaluated successfully. The API endpoint is vulnerable to XSS!