Remote Cookie Tampering

Dawid Czagan
SECURITY INSTRUCTOR

@dawidczagan

Overview

Browser dependent exploitation

Comma-separated list of cookies

Demo

Fixing the problem

Browser Dependent Exploitation

1. Web application
2. Browser

More powerful attacks

Comma-separated list of cookies

↓

Remote cookie tampering

Comma-separated List of Cookies

/test.php?version=mobile

Set-Cookie: version=mobile

One cookie: version

/test.php?version=mobile, SID=abc

Set-Cookie: version=mobile, SID=abc

Two cookies: version and SID

(Safari)

Demo

Remote cookie tampering

Fixing the Problem

/test.php?version=mobile	Set-Cookie: version=mobile
/test.php?version=desktop	Set-Cookie: version=desktop
/test.php?version=xyz	Set-Cookie: version=desktop

Summary

Browser dependent exploitation

↓

More powerful attacks

Comma-separated list of cookies

↓

Remote cookie tampering