Syllabus

Introduction

Insecure Direct Object Reference and Broken Access Control are quickly rising, and the OWASP top 10 shows this as well. In this course, I want to guide you through these vulnerabilities and how to look for them, not just in a small lab but in a custom-built application for you to explore!

What are BAC and IDOR

In this topic, we are going to explore what makes BAC, into BAC and why there are two types of BAC. We are also going to learn the difference between an IDOR and a BAC.

objectID or userID based IDOR

There are two types of IDOR, in this chapter, we are going to briefly touch on both. First of all the objectID type references, an object, and second of all objects are referenced by their owner/creator.

GET vs POST vs cookies vs headers IDOR

In this chapter, we are going to have a look at what parameters we should monitor for IDORs specifically as we can have two types of IDs that are spread all over applications but we need to identify the parameter first!

First and multi-order IDOR and BAC

You've potentially already heard about BAC and IDOR, but have you ever heard about second- and multi order exploits? In this chapter, we are going to show you some practical examples of both and explain a bit more about how you hunt for the deeper types of Broken Access Control.

Manual BAC testing

So, how do we test for this exploit type? We are kicking things off easy here with an easy-to-use tool, our browsers!

Manual IDOR testing

The same goes for IDORs of course, we can hunt for them manually but we must remember to create our own user accounts and grab their data and not a stranger's data!

Automated BAC testing with burp

It's good to manually look for BAC and IDOR, but the real fun comes from automating the hunt. We'll be looking at how authorize can help speed up your hunting like no other!

Automated IDOR hunting with burp

Of course, BAC and IDOR can use the same tools since IDOR is just a subset but the way we hack for them can differ slightly which is why we will spend some time on the differences.

Automated BAC hunting with ZAP

What burp suite can do, can also be done with ZAP so let’s have a look at the “Access Control” module for ZAP.

Automated IDOR hunting with ZAP

And the same goes for ZAP as it does for burp, being that IDOR and BAC hunting are hunted on slightly differently. Different game, different hunt.

The different exploit impacts

Capstone project

In this capstone project, we are going to combine what we have learned in the smaller labs and combine it into one bigger lab which we will explore automatically, ultimately reporting on both BAC and IDOR issues in the same lab on different functions.