Insecure Direct Object References

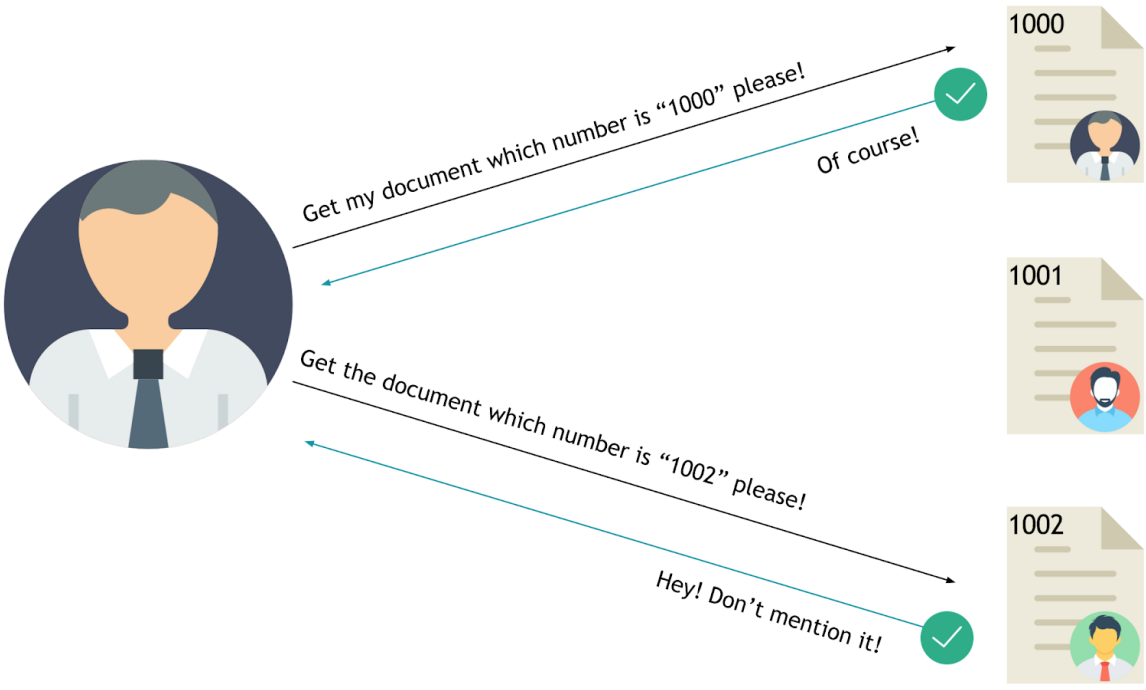
> Insecure Direct Object References occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files. - OWASP

Summary

Tools

- Burp Suite plugin Authz
- Burp Suite plugin AuthMatrix
- Burp Suite plugin Authorize

Exploit



The value of a parameter is used directly to retrieve a database record.

```
http://foo.bar/somepage?invoice=12345
```

The value of a parameter is used directly to perform an operation in the system

```
http://foo.bar/changepassword?user=someuser
```

The value of a parameter is used directly to retrieve a file system resource

```
http://foo.bar/showImage?img=img00011
```

The value of a parameter is used directly to access application functionality

```
http://foo.bar/accessPage?menuitem=12
```

Examples

- HackerOne - IDOR to view User Order Information - meals
- HackerOne - IDOR on HackerOne Feedback Review - japz

References

- OWASP - Testing for Insecure Direct Object References (OTG-AUTHZ-004)
- OWASP - Insecure Direct Object Reference Prevention Cheat Sheet
- BUGCROWD - How-To: Find IDOR (Insecure Direct Object Reference) Vulnerabilities for large bounty rewards - Sam Houton
- IDOR tweet as any user by kedrisec
- Manipulation of ETH balance
- Viewing private Airbnb Messages
- Hunting Insecure Direct Object Reference Vulnerabilities for Fun and Profit (PART-1) - Mohammed Abdul Raheem - Feb 2, 2018