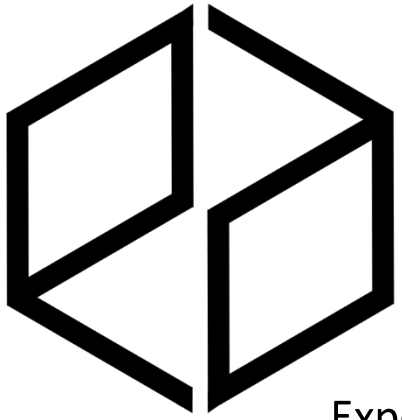
www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #4 Insecure Direct Object Reference

By @isaacsabas



PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

OWASP

Open Web Application Security Project


A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Controls
A8: Cross Site Request Forgery (CSRF)
A9: Using Components with Known Vulnerabilities
A10: Unvalidated Redirects and Forwards

OWASP #4

Insecure Direct Object Reference

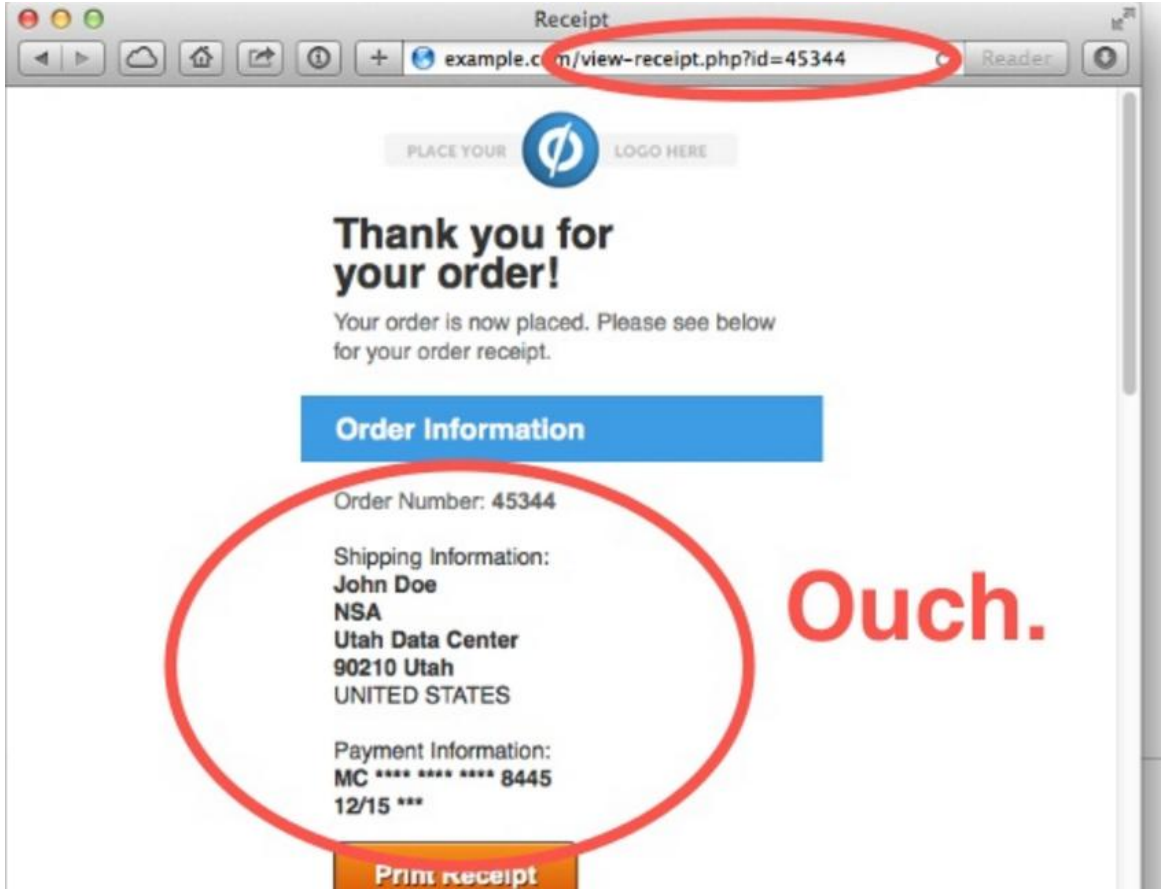
OWASP Top 10 Vulnerabilities

Reference to an internal implementation object such as files, directories, or database entries without an access control check or protection mechanism.

Insecure Direct Object Reference –What is it?

Where it all began.

Samples


Receipt
example.com/view-receipt.php?id=45344
Reader
PLACE YOUR LOGO HERE
Thank you for your order!
Your order is now placed. Please see below for your order receipt.
Order Information
Order Number: 45344
Shipping Information:
John Doe
NSA
Utah Data Center
90210 Utah
UNITED STATES
Payment Information:
MC **** **** **** 8445
12/15 ***
Print Receipt
Ouch.

Samples

```
POST / HTTP/1.1
Host: example.com
Cookie: user=453435;
Content-Length: 52

email=hackz@detectify.com&password=secretsecret1
```

Ouch.

```
HTTP/1.1 200 OK
Date: Sun, 26 Oct 2014 15:08:30 GMT
Server: Apache
Content-Length: 2
Content-Type: text/plain; charset=utf-8

User 453435 updated.
```

What are the Risks When Exploited?

- Change of database content (e.g. change of delivery address)
- Delete database entry (e.g. another user account, invoice, etc.)
- Loss of profits (e.g. access to promo codes or gift certificates)

What can hackers access?

- Access to database entries
  - Account numbers
  - Credit card numbers
  - User information
- Access to files
- Emails

How is this vulnerability exploited?

1. No secure access model
   - User X should only have access to object A
2. Numeric IDs
3. Error messages that gives away structure
   - *“User X cannot view object owned by User Y”*
   - *“No access to this object.*
4. Inconsequent ID sources
   - *http://www.example.com/?view=434*
   - *http://www.example.com/view/434*

How to I Prevent Such Vulnerability?

- User ID in session or token
- Utilize an access model
  - Check access for all objects
  - If not owned by user, deny access

Go to http://www.securesavingsbank.com

EXPLOIT DEMO

How simple it is to test for a IDOR vulnerability.

TIME FOR

Q&A

OWASP Top 10 – Insecure Direct Object Reference

Go download WebGoat

https://github.com/WebGoat/WebGoat-Legacy

TRY IT YOURSELF

Some homework for you to learn a bit more.

WebGoat Installation How-To

1. Download Java VM, JDK 1.7
2. Download WebGoat: https://webgoat.atlassian.net/builds/browse/WEB-WGM/latestSuccessful/artifact/shared/WebGoat-Embedded-Tomcat/WebGoat-6.0.1-war-exec.jar
3. Run the .jar file:
    1. java -jar WebGoat-6.0-exec-war.jar
4. Then navigate in your browser to: (http://localhost:8080/WebGoat)
5. Login using guest account
6. Go to Access Control Flaws and complete the following exercises:
    1. Bypass a Path Based Access Control Scheme

OWASP #4

Insecure Direct Object Reference

OWASP Top 10 Vulnerabilities

www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #4 Insecure Direct Object Reference

By @isaacsabas