DIRECT OBJECT REFERENCE

DIRECT OBJECT REFERENCE

OWASP regularly compiles a list of the top 10 security vulnerabilities

#4 on this list is the Direct Object Reference

DIRECT OBJECT REFERENCE

This did not even make the list prior to 2004

Web applications have become more complicated with different parts of the application and different data accessible to each user

DIRECT OBJECT REFERENCE

This vulnerability exists in an application if it exposes an **internal implementation** detail to the user

DIRECT OBJECT REFERENCE

This vulnerability exists in an application if it exposes an internal implementation detail to the user

This could be a database key, a file name, the name of an object - anything

DIRECT OBJECT REFERENCE

Let's take an example

A site allows users to send messages to each other

DIRECT OBJECT REFERENCE

All messages are stored in a database - a simple one like this

ID	FROM	TO	MESSAGE
103	a@gmail.com	jan@gmail.com	Hi how are you?
104	wer123@yahoo.com	jeff@email.com	Shall I see you in an hour?
105	toby@hotmail.com	glenn@hotmail.com	This is a long message, hope you're doing well..
106	jane@gmail.com	verna@hotmail.com	Thank you for your help!

DIRECT OBJECT REFERENCE

ID	FROM	TO	MESSAGE
103	a@gmail.com	jan@gmail.com	Hi how are you?
104	wer123@yahoo.com	jeff@email.com	Shall I see you in an hour?
105	toby@hotmail.com	glenn@hotmail.com	This is a long message, hope you're doing well..
106	jane@gmail.com	verna@hotmail.com	Thank you for your help!

A message id is a unique auto incremented value for every message, used to identify a message

DIRECT OBJECT REFERENCE

ID	FROM	TO	MESSAGE
103	a@gmail.com	jan@gmail.com	Hi how are you?
104	wer123@yahoo.com	jeff@email.com	Shall I see you in an hour?
105	toby@hotmail.com	glenn@hotmail.com	This is a long message, hope you’re doing well..
106	jane@gmail.com	verna@hotmail.com	Thank you for your help!

These are from and to fields, other fields like timestamp etc have been left out for simplicity

DIRECT OBJECT REFERENCE

ID	FROM	TO	MESSAGE
103	a@gmail.com	jan@gmail.com	Hi how are you?
104	wer123@yahoo.com	jeff@email.com	Shall I see you in an hour?
105	toby@hotmail.com	glenn@hotmail.com	This is a long message, hope you're doing well..
106	jane@gmail.com	verna@hotmail.com	Thank you for your help!

And actual message contents

DIRECT OBJECT REFERENCE

```
http://trustedmail.com/messages/?id=102
```

This is the URL to access one particular message

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=102`

If the user is **not logged in**, this URL forces him to the login page for the site

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=102`

On logging in a session variable is set up which stores the user id

This indicates that the user has logged in for this session

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=102`

The message id is used to uniquely identify the message to view

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=154`

This should allow the user to view the message with the unique id 154

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=154`

As the user goes through the messages in his inbox - the message id in the URL changes to reflect the different messages he has received

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=154`

But what if message id 154 did not have the current user in either its from or to fields?

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=154`

We've basically allowed a user to view messages in our database which do not belong to him!

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=154`

The message id is an **internal** implementation detail of the system, and the URL exposes this to the user

DIRECT OBJECT REFERENCE

`http://trustedmail.com/messages/?id=154`

This is a direct object reference to an internal object

DIRECT OBJECT REFERENCE

Here is an example from the real world - this is something which actually happened

DIRECT OBJECT REFERENCE

Some years ago a financial company ended up inadvertently exposing financial data of its members

to other members who were not authorized to view it

DIRECT OBJECT REFERENCE

Say you were logged and authenticated to your pension account

```
http://www.trustedfinancialsite.com/
viewdetails.php/?account_id=1234
```

This page showed you all details of your retirement funds

DIRECT OBJECT REFERENCE

```
http://www.trustedfinancialsite.com/
viewdetails.php/?account_id=1234
```

The account you view is specified by this URL parameter

DIRECT OBJECT REFERENCE

```
http://www.trustedfinancialsite.com/
viewdetails.php/?account_id=1234
```

Now if you edited the URL parameter to change the account id

DIRECT OBJECT REFERENCE

```
http://www.trustedfinancialsite.com/
viewdetails.php/?account_id=8123
```

The company's site let you access the details of the other account!

DIRECT OBJECT REFERENCE

```
http://www.trustedfinancialsite.com/
viewdetails.php/?account_id=8123
```

There was no additional check to see whether you were authorized to view those account details!

DIRECT OBJECT REFERENCE

```
http://www.trustedfinancialsite.com/
viewdetails.php/?account_id=8123
```

The account id is an internal implementation detail of the code

DIRECT OBJECT REFERENCE

```
http://www.trustedfinancialsite.com/
viewdetails.php/?account_id=8123
```

Exposing this information compromised millions of accounts linked to that financial company

DIRECT OBJECT REFERENCE

Mitigation

DIRECT OBJECT REFERENCE

Mitigation

1. Authorization
2. Indirection Layer
3. Randomized Identifiers

DIRECT OBJECT REFERENCE

Mitigation - Authorization

A direct object reference vulnerability of this kind has a basic authorization problem

DIRECT OBJECT REFERENCE

Mitigation - Authorization

Authorization refers to **what** a user has access to

what data,
what components of a site

DIRECT OBJECT REFERENCE

Mitigation – Authorization

In the messages example or in the pension account example a simple check would have sufficed for authorization

DIRECT OBJECT REFERENCE

Mitigation - Authorization

Does the message have the user in the to, from or cc field?

Is the current user the owner of that pension account?

DIRECT OBJECT REFERENCE

Mitigation

1. Authorization

2. Indirection Layer

3. Randomized Identifiers

DIRECT OBJECT REFERENCE

Mitigation - Indirection Layer

Internal ids and objects should not be exposed to the user directly

Instead a **separate layer can map** the internal ids to externally visible ids

DIRECT OBJECT REFERENCE

Mitigation - Indirection Layer

Instead a separate layer can map the internal ids to externally visible ids

LOCAL PER-USER MAPPING	ID
0	103
1	104
2	105
3	106

DIRECT OBJECT REFERENCE

Mitigation - Indirection Layer

LOCAL PER-USER MAPPING	ID
0	103
1	104
2	105
3	106

Each user will have a specific id which maps to the message id

DIRECT OBJECT REFERENCE

Mitigation - Indirection Layer

LOCAL PER-USER MAPPING	ID
0	103
1	104
2	105
3	106

The keys of this map is what will display in the URL parameter

DIRECT OBJECT REFERENCE

Mitigation - Indirection Layer

LOCAL PER-USER MAPPING	ID
0	103
1	104
2	105
3	106

A map like this should be generated for every user

DIRECT OBJECT REFERENCE

Mitigation – Indirection Layer

LOCAL PER-USER MAPPING	ID
0	103
1	104
2	105
3	106

So no user can even try and access messages he is not authorized to

DIRECT OBJECT REFERENCE

Mitigation

1. Authorization
2. Indirection Layer
3. Randomized Identifiers

DIRECT OBJECT REFERENCE

Mitigation - Randomized Identifiers

Instead of using predictable, auto-incremented ids the identifiers could also be randomly generated

DIRECT OBJECT REFERENCE

Mitigation - Randomized Identifiers

This by itself is not enough mitigation but can be used along with the other techniques

DIRECT OBJECT REFERENCE

Mitigation

1. Authorization
2. Indirection Layer
3. Randomized Identifiers