Broken Access Control

Broken Access Control

- Access or modify information beyond limits.

→ Access or modify user info without logging in.

→ Access or modify info that belongs to another user.

target.com

James Bond

james@bing.com

France

target.com

John Wick

jhn@gmail.com

Ireland

Broken Access Control

IDOR

Broken Access Control

IDOR

- Insecure Direct Object Reference.

→ Objects are accessed directly based on user input.

Broken Access Control

IDOR

- Insecure Direct Object Reference.

→ Objects are accessed directly based on user input.

- Docs.
- images.
- Database records.

target.com?id=1

James Bond

james@bing.com

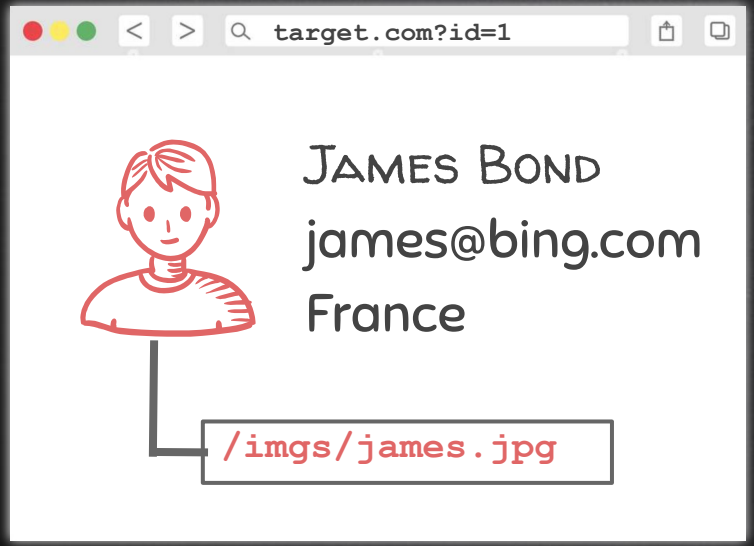
France

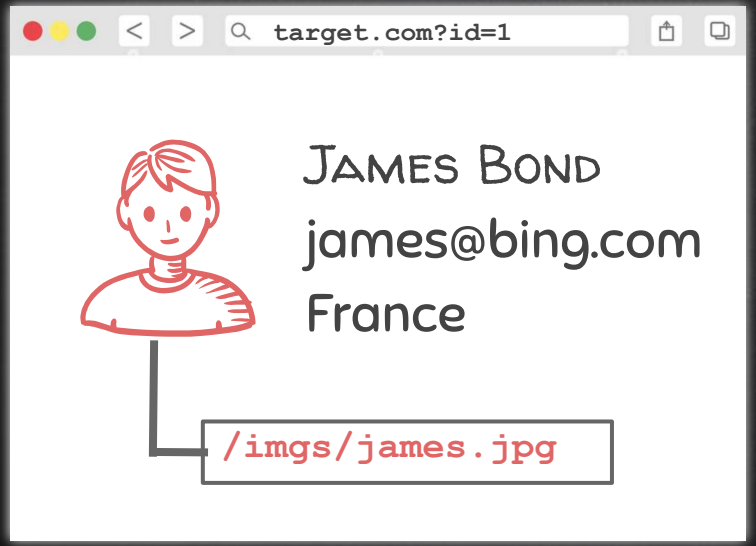
target.com?id=2

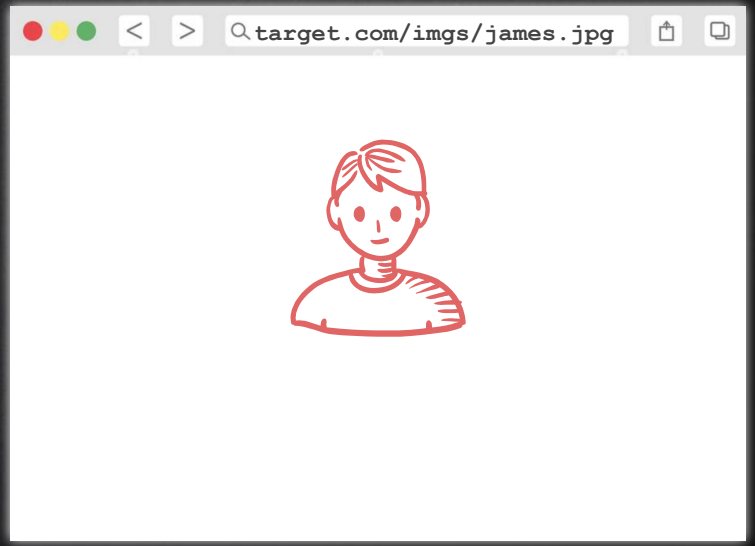
John Wick

jhn@gmail.com

Ireland


target.com?id=1
JAMES BOND
james@bing.com
France
/imgs/james.jpg


target.com?id=1
James Bond
james@bing.com
France
/imgs/james.jpg


target.com/imgs/james.jpg

```
GET /admin HTTP/2.0
Host: webserver.com
Cookie: session=c4m
……
Connection: close
```

Target
Web Server

```
TRACE /admin HTTP/2.0
Host: webserver.com
Cookie: session=c4m
.....
Connection: close
```

Target
Web Server

```
TRACE /admin HTTP/2.0
Host: webserver.com
Cookie: session=c4m
……
Connection: close
```

Target
Web Server

```
TRACE /admin HTTP/2.0
Host: webserver.com
Cookie: session=c4m
.....
Connection: close
```

Proxy

```
TRACE /admin HTTP/2.0
Host: webserver.com
Cookie: session=c4m
.....
Extra Headers
Connection: close
```

Target
Web Server

```
TRACE /admin HTTP/2.0
Host: webserver.com
Cookie: session=c4m
.....
Extra Headers
Connection: close
```

Target
Web Server

Broken Access Control

- Access or modify information beyond limits.

target.com?id=1

James Bond

james@bing.com

France

target.com?id=2

John Wick

jhn@gmail.com

Ireland