Introduction To SQL Injection

Presented By:
Joe McCray

joe@strategicsec.com

http://twitter.com/j0emccray

http://www.linkedin.com/in/joemccray

The Basics

What’s Actually Happening

Let's get started with what's actually happening during an SQL Injection.

To do that we must start with the most fundamental construct of programming - data types.

int = 51550

string = 'Joe'

string2 = 'Joe McCray'

The Basics

What’s Actually Happening

When you look at the text below now you'll see that the integer, and both strings are improperly terminated. This would cause an error because the quotes are unbalanced!

```
int = 51550'
string = 'Joe''
string2 = 'Joe McCray''
```

The Basics

What’s Actually Happening

You should see an error similar to:

Microsoft OLE DB Provider for SQL Server error '80040e14'

Unclosed quotation mark after the character string '''.

The Basics

What’s Actually Happening

Let's say that you have some code like the snippet below:

```
string query = "Select * From Products Where ProductID = " + Request["ID"];
```

In this case "ID" is coming directly from a web request - something like this:

```
http://site.com/products.asp?id=51550
```

The Basics

What’s Actually Happening

When you insert a single quote into the URL you change the backend query

http://site.com/products.asp?id=51550’

Now you’ll see the backend query become:

string query = "Select * From Products Where ProductID = " + Request[“51550’"];

Request[“51550’"];

The Basics

What’s Actually Happening

This is now basically the same as:

int = 51550'

You should see an error similar to:

Microsoft OLE DB Provider for SQL Server error '80040e14'

Unclosed quotation mark after the character string '''.

The Basics

What’s Actually Happening

When an attacker attempts to exploit this newly found SQL Injection vulnerability you'll see that it is common to insert SQL statements into the URL.

http://site.com/products.asp?id=51550 or 1 in (select user)--

This changes the backend query to something like:

```
string query = "Select * From Products Where ProductID = " + Request["51550 or 1 in (select user)--"];
```

Request["51550 or 1 in (select user)--"];

Why or 1 in

Where You Sleep In Math Class

5 = 3 + 2

5 = 1 + (2 + 2)

What is implied by the parenthesis?

Order Operator Precedence

DO THIS FIRST

Why or 1 in

Where You Sleep In Math Class

http://site.com/products.asp?id=51550 or 1 in (select user)--

51550 or 1 in (select user)--

Order Operator Precedence – meaning do this first

The result of ‘select user’ is ‘dbo’

Why or 1 in

http://site.com/products.asp?id=51550 or 1 in (select user)--

51550 or 1 in (select user)--

in is another way of basically saying =

51550 or 1 = (dbo)

What’s the difference between = and ==

Why or 1 in

http://site.com/products.asp?id=51550 or 1 in (select user)--

51550 or 1 in (select user)--

in is another way of basically saying =

51550 or 1 = (dbo)

= is an assignment

== is a test to see if 2 values are equal

Why or 1 in

51550 or 1 = (dbo)

= is an assignment

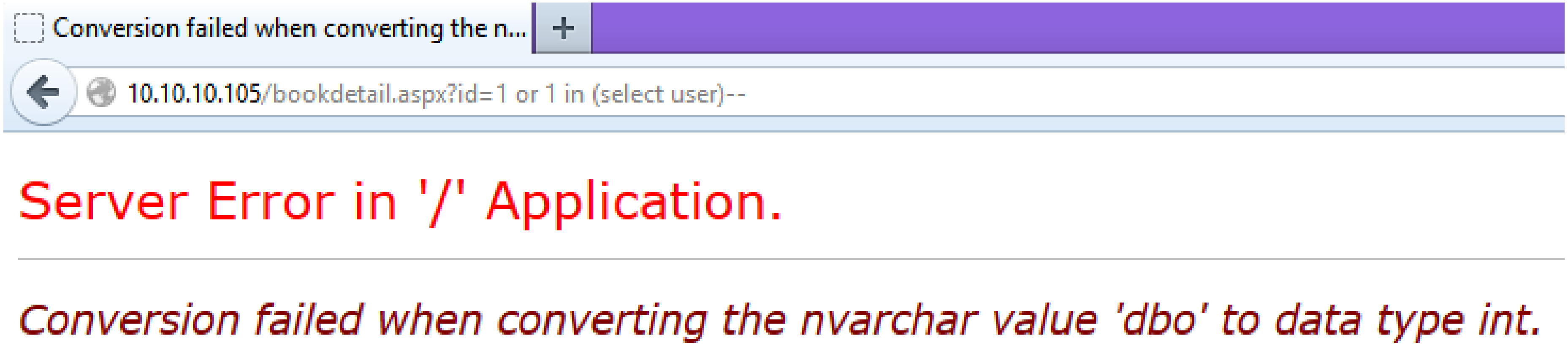
51550 is an integer

dbo is a string

Assigning an integer to be a string or vice versa will throw an error

Why or 1 in

Assigning an integer to be a string or vice versa will throw an error



Conversion failed when converting the n...

10.10.10.105/bookdetail.aspx?id=1 or 1 in (select user)--

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'dbo' to data type int.

This forcing the application to throw an error so we can see the result of our SQL query is called:

Error-Based SQL Injection

Why 1=1 or A=A?

Let’s say you have a table of usernames and passwords:

Username	Password
admin	password
Jim	Beam
Johnny	Walker

Why 1=1 or A=A?

Let’s say you have some code for your website login

Username	Password
admin	password
Jim	Beam
Johnny	Walker

```
if ($un and $pw):
        login
else
        login denied
```

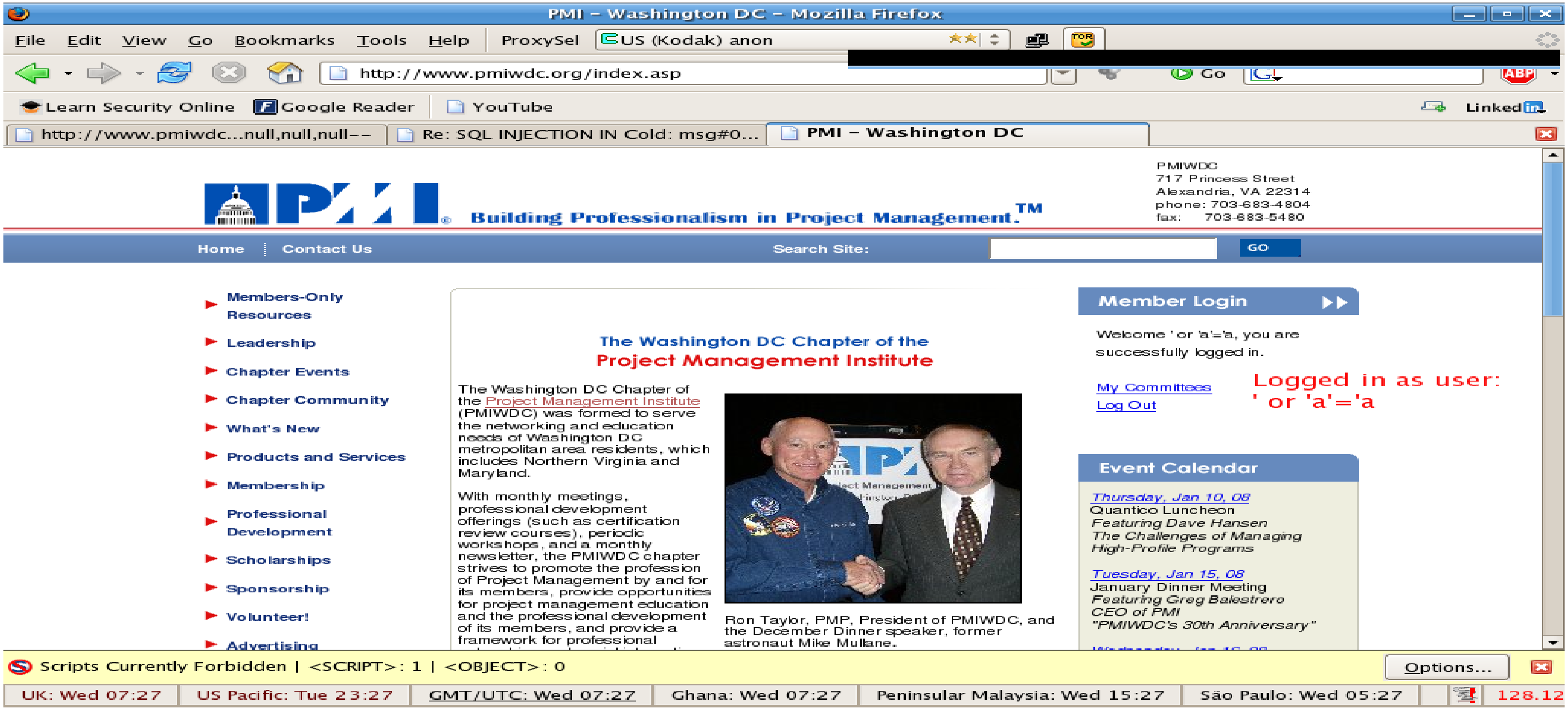
Why 1=1 or A=A?

Let’s say you have some code for your website login

Username	Password
admin	password
Jim	Beam
Johnny	Walker

```
if ($un or 1=1 and $pw or 1=1):
        login
else
        login denied
```

Any Project Managers In The House?



PMI – Washington DC – Mozilla Firefox
File Edit View Go Bookmarks Tools Help ProxySel US (Kodak) anon
Go
Learn Security Online
Google Reader
YouTube
LinkedIn

[redacted]

http://www.pmiwdc.org/index.asp

http://www.pmiwdc...null,null,null-- | Re: SQL INJECTION IN Cold: msg#0... | PMI – Washington DC

PMIWDC
717 Princess Street
Alexandria, VA 22314
phone: 703-683-4804
fax: 703-683-5480

PMI® Building Professionalism in Project Management.™

Home | Contact Us   Search Site: GO

- Members-Only Resources
- Leadership
- Chapter Events
- Chapter Community
- What's New
- Products and Services
- Membership
- Professional Development
- Scholarships
- Sponsorship
- Volunteer!
- Advertising

The Washington DC Chapter of the
Project Management Institute

The Washington DC Chapter of the Project Management Institute (PMIWDC) was formed to serve the networking and education needs of Washington DC metropolitan area residents, which includes Northern Virginia and Maryland.

With monthly meetings, professional development offerings (such as certification review courses), periodic workshops, and a monthly newsletter, the PMIWDC chapter strives to promote the profession of Project Management by and for its members, provide opportunities for project management education and the professional development framework for professional

Ron Taylor, PMP, President of PMIWDC, and the December Dinner speaker, former astronaut Mike Mullane.

Member Login

Welcome ' or 'a'='a, you are successfully logged in.

My Committees
Log Out

Logged in as user:
' or 'a'='a

Event Calendar

Thursday, Jan 10, 08
Quantico Luncheon
Featuring Dave Hansen
The Challenges of Managing High-Profile Programs

Tuesday, Jan 15, 08
January Dinner Meeting
Featuring Greg Balestrero
CEO of PMI
"PMIWDC's 30th Anniversary"

Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0   Options...

UK: Wed 07:27 | US Pacific: Tue 23:27 | GMT/UTC: Wed 07:27 | Ghana: Wed 07:27 | Peninsular Malaysia: Wed 15:27 | São Paulo: Wed 05:27 | 128.12

Basic References

SQL Tutorials:

http://www.sql-tutorial.net/

SQL Injection Tutorials

http://www.securitydocs.com/library/3587

http://www.astalavista.com/index.php?section=docsys&cmd=details&id=42

SQL Injection Cheatsheets:

http://pentestmonkey.net/blog/mssql-sql-injection-cheat-sheet/

http://pentestmonkey.net/blog/mysql-sql-injection-cheat-sheet/

Holla @ Me....

You want the presentation?????

Buy me a rum and coke or email me....

You can contact me at:

Email:	joe@strategicsec.com
Twitter:	http://twitter.com/j0emccray
LinkedIn:	http://www.linkedin.com/in/joemccray