

Web 2.0: Getting Beyond the “No”

Tim McCorry
Office of Cyber Security & Critical
Infrastructure Coordination



Web 2.0 has Arrived



- Many people didn't even know that "Web 1.0" was here, let alone a 2.0!
- That's because Web 1.0 never existed and Web 2.0 was just a phrase that was coined.
- The Internet is vastly growing as we know, and Web 2.0 was coined to show the era that we are presently growing towards.

What is Web 2.0?



- Web 2.0 was coined by Tim O'Reilly at a conference between O'Reilly Media and MediaLive International in 2004...
 - Mr. O'Reilly stated: "Web 2.0 is the business revolution in the computer industry caused by the move to the internet as a platform, and its an attempt to understand the rules for success on that new platform. Chief among those rules is this: Build applications that harness network effect's to get better, the more people will use them."

Web 2.0 Continued



- Is Web 2.0 new?
 - Not necessarily...
- Technically things like Amazon.com have been using user generated content, one of the big aspects of Web 2.0, since around 1995
 - I.E. allowing users to write reviews on their products
- All the control is gravitating towards the user.

Differences between 1.0 & 2.0



■ How they work...

- 1.0 was all about reading the content from the Internet, and it would take months to edit that content... 2.0 on the other hand is about creating the content. It's always a working progress and can continue to grow at any point.
- In the case of 1.0, if you wanted to find some information about “Kangaroo’s that eat bananas” (very rare), it may have been very hard to find... On the other hand in 2.0, you can blog about it, or even use something like Wikipedia. This way anyone that reads your information could answer you back right away, not weeks or months later.

Differences between 1.0 & 2.0



- Some more of the key differences:
 - User-generated content, rather than web-based
 - Uses more coding technologies such as AJAX and XML (which we will see later can create many more holes)
 - Constantly changing on the fly – In 2.0 everything has the ability to grow, when in 1.0 the site would have to shut down for changes

Why Web 2.0 is Beneficial



- Web 2.0 stands on three basis for its technology
 - It's user generated content
 - Customization of Content
 - Extended Life of Content

More Benefit's



- Outside of the technical aspects of Web 2.0, just based on content alone it is outstanding!
 - Gives users great ways to share data
 - Allows for more input on a variety of different information
 - Gives people the opportunity to start or join a community of people who enjoy the same materials.
 - Keeps people in touch
 - We live in a fast-paced world – Who wants to spend time going to read the news, then weather, then sports, each time going to new pages.
 - With Web 2.0, all the information you need could be one click away, or even fed right onto your homepage!

At what price?



- As everyone is aware, throughout the Internet, there are constant threats from different vulnerabilities.
 - There is no such thing as 100% security
 - Constant struggle between hackers and defenders in the “cyber security world”
- Some of the main attacks I will talk about today: Cross-Site Scripting, Cross-Site Request Forgery, Widget Attacks, SQL Injection, XPath, XSS Worms, Authentication and Authorization Flaws, and Insecure Storage and Communication

Cross-Site Scripting (XSS)



- Cross-Site Scripting can be defined as a vulnerability that allows a user to input a malicious script into a Webpage that is vulnerable. This will allow that script to run when another user accesses that site (this may or may not be with the user knowledge).
- It's made vulnerable when a website doesn't validate its input or encode the data once its submitted.

Dangers in Web 2.0



- What makes XSS so dangerous in Web 2.0 is because XSS requires user input.
- Web 2.0 is built on user input. As I mentioned before Web 2.0 is trying to move the Internet into the hands of the user, rather than just have static pages that cannot change.
- All these user input fields presents many more holes that attackers can find to exploit XSS. All those user input fields need to make sure they are protected.

Cross Site Request Forgery (CSRF)



- Although it is like XSS, CSRF is quite different.
- Cross-Site Request Forgery is defined as an unauthorized command transmitted from a user that the vulnerable webpage trusts.
- In other words the webpage sees the user as already trusted and can then leave the webpage vulnerable to an attack
- How is it different from XSS?
 - In Cross-Site scripting the attack is executed on the client-side browser while in a CSRF attack it is executed against an already trusted site.

Dangers of CSRF in Web 2.0



- CSRF is not a new attack and we have seen it before the term Web 2.0 has been around.
- However, it is much more dangerous in Web 2.0 because Web 2.0 has to allow Cross-Domain Access in order to work – Without that Web 2.0 is rendered useless
 - Many sites pull in information from many different places before they output it on their page; If it is not coded right it can be infected extremely easy. With Web 2.0 you must include many different access points and allow for Cross-Domain Access (How else can a user read the sports as well as the weather on one application? It gets pulled from multiple areas). This creates a lot of attack points for the attacker and makes CSRF much easier to exploit in Web 2.0

Widgets and CSRF



- Perfect Example...
- Mac's first started using Widgets on their desktops... Since then PC's have added them as well (Called Gadgets)
- Who uses Widgets?



Picture of the Widget Screen



- Here is a widget screen that can be on someone's computer. Notice how many different aspects it is touching

- Volcano Cam
- Weather
- Time
- Sports
- Etc...

TITLE	DATE
The Namesake - Trailer	26 May
X-Men: The Last Stand - E...	26 May
Once In A Lifetime - Trailer	24 May
Ghost Rider - International...	23 May
Ghost Rider - Teaser 1	23 May
Dreamgirls - Making Of	22 May
The Devil Wears Prada - Te...	19 May
Flushed Away - Trailer	17 May

Stock	Price	Change
DOC	2210.37	+12.13 +0.55%
YHOO	33.02	+0.10 +0.30%
PXPR	0.00	0.00 + N/A
ADBE	28.98	-2.16 -0.55%
SBOX	35.43	-0.01 -0.03%
CNET	9.32	-0.12 -1.27%

Day	1	2	3	4	5	6
Sun						
Mon	7	8	9	10	11	12
Tue	13	14	15	16	17	18
Wed	19	20	21	22	23	24
Thu	25	26	27	28	29	30
Fri	31					
Sat						

Widget Attacks



- Can be paired heavily with XSS and CSRF attacks.
- But independently are extremely dangerous as well.
- Widgets can be created by anyone. There is nobody stopping you from starting your own. So as an attacker, you can come up with your own widget for people to download.
 - This widget can be 99% legit, with great information sharing throughout the screen. All it takes is one bad link attached to it and it could allow for hijacking, data theft, SQL Injects, etc...
 - Big vulnerability around the widget for the China Olympic Games...

SQL Injection



- SQL Injection attack is defined as an attack that literally “injects” Structured Query Language (SQL) code to a Web form input box to gain access or change data.
- SQL Injection attacks are very dangerous attacks and are widely used in the hacker community (Have been for many years) – It allows people to steal very sensitive information (like User IDs and Passwords), by attacking the SQL database that stores that information.

What makes it so Dangerous?



- Just like with XSS, SQL Injection attacks rely on user input. These user fields allows the attack to attempt to call the database in order to get the information it is looking for.
 - The information a user inputs, is sent to the database. The goal of the attacker is to exploit this request to the database to steal data, inject malware, corrupt the database, etc...
- The most prevalent attacks we see with SQL is using it to injection malicious Java scripts into Webpages that run every time a user interacts.
 - That way while a user interacts with the vulnerable Webpage, in the background a java script runs that is infecting your machine or stealing your data.

XPath Vulnerabilities



- XPath vulnerability is best defined as a vulnerability in a website that uses what a user inputs, as its query to the database. It takes whatever the user inputs and creates a Query to call where this data is saved.
- XPath vulnerabilities are just like SQL vulnerabilities, just directed at a different area. While SQL attacks go directly at the SQL Database, XPath attacks will go after the XML code.
- However, they work the same way by using a user input to attack the back end of the application.

Dangerous in Web 2.0



- So although we have seen XPath Query vulnerabilities as a dangerous problem in the past, and we also see the same idea within SQL attacks, Xpath attacks get worse in Web 2.0
- This is because in a designing tool like AJAX, which is heavily used in Web 2.0, the X stands for XML. Which is where XPath derives from...

XSS Worms linked directly to Web 2.0



- We have already talked about Cross-Site scripting in Web 2.0 and how dangerous it has become.
- But with the development of Web 2.0, XSS worms could come about as well.
- With Web 2.0 using Java, XML, AJAX, etc... spreading of worms and virus's is much easier

Biggest XSS Worm



- **SAMY!** The classic worm that introduced the world to XSS Worms.
 - SAMY was a worm introduced by a kid on MySpace. Although not a malicious worm, SAMY did prove it could spread, and quickly.
 - Since then, other Social Networking Sites have fallen victim as well: Facebook (Koobface) and Twitter (StalkDaily Worm).

Just going to get worse



- These spreading's require no input by the user (once already infected that is) and spreads very quickly (SAMY infect 1 million + in 24 hours).
- Plus now worms will become more intelligent and complex, and could also be used as a DoS attack
 - Reading the news as of late, Twitter and Facebook fall victim to DoS attacks very frequently

Authentication & Authorization Flaws



- The oldest trick in the book...
 - The internet has seen attacks on authentication and authorization flaws for many years.
 - People attempt to steal your ID or password, and can even hijack your session
- So Dangerous in Web 2.0 because...
 - Attackers can brute force your password (not much criteria for security), it can hijack your session (predictable session IDs), and also “tag along” with your session (lack of sufficient time-out parameters).
- Web 2.0 continues to give these attacks more entry points.

Insecure Storage and Communication



- Web 2.0 is not built for security, it is built for functionality.
- Storage of data and communication of data securely, is not very strong. Some examples are as follows:
 - Only using SSL/TLS for the login, the rest is not protected
 - During transit, not encrypting sensitive data...

Why Those 8?



- When talking about Web 2.0 vulnerabilities, you can't just talk about the new ones directed at Web 2.0
- Instead these Eight that I compiled are a list of some of the top vulnerabilities that have been around for many years (i.e. XSS, SQL Inject, etc...) combined with some of the new problems (i.e. XSS Worms, Widget Attacks, etc...) that are arising with 2.0
- Each vulnerability is dangerous in its own way and is only becoming more dangerous as Web 2.0 evolves.

Social Networking



- What is it?
 - Social networking can be defined as the grouping of individuals into specific groups, like small rural communities or subdivisions.
- Social Networking Sites?
 - It's what the web has turned into – Social Networking sites like Facebook, Twitter, LinkedIn, etc...
 - These sites are open for anything and everything – You can go job hunting, communicate with people (Email, IM), shop, get in touch with old friends etc... The list is continuing to grow, right along with the social networking sites

Lists



- Many people only know the big Social Networking Sites: Facebook, Twitter, MySpace, Hi5, etc...
- As you can see, the list is extremely long, and still growing!



Social Networking Sites



- Some of the most popular, that you may not know...
 - Hi5.com, bebo.com, friendstar.com, etc...
- Who uses any of these Social Networking Sites?
 - It has been reported that over 200 million users around the world use Facebook alone!
 - It has over 1 Billion hits a month
 - Sites like Twitter and Myspace are not far behind – Have hits into the hundreds of millions a month.

Social Network Greatness



- As you can see from the amount of people using the Social Networking Sites, they are great for information sharing.
 - It allows for a rapid spread of information, connection is easier than ever, and communication is amazing as well.
 - There is no mathematical formula as to why they keep growing – They are just that good!

A lot of things are great though



- Yes, these sites like Twitter and MySpace are great, but you must weigh the good with the bad.
 - From a business standpoint is there a need for your company to use Social Networking Sites?
 - CSCIC right now is blocking the use of these social networking sites as it does more research into the risks and benefits of the sites. As an agency we will be producing a policy or best practice for the state once we have concluded our research.
- Every new technology needs to be evaluated, even the most commonly used product in an office has a lot of flaws...

You Decide...



- Web 2.0 has arrived to the Internet, and in a hurry. I brought to light some of the top vulnerabilities that you need to be aware of from a business stand point. If you are going to build your web 2.0 applications, just make sure you do them properly and take these vulnerabilities into account.
- However, understand that Web 2.0 is out there, and being used heavily (Especially with YouTube, Wiki's, and Social Networking Sites), and you still must be aware of these vulnerabilities.
- Then you decide...
 - Can your employees safely use these sites?
 - Do you trust these third parties to take in to account all these vulnerabilities?
 - Do all the good things these Web 2.0 applications bring about outweigh the high risk of infection?
- You be the judge!

Public vs Private



- Once the content is on the internet, you no longer own it!
- Many people don't understand that there is a difference between what you say, and what you put on paper.
- If you are posting to your MySpace page, or "tweeting" on your twitter... Understand that what you put up there, is now public property
- Also working for the government, anything you say regarding your company, can be reproduced and quoted as coming directly from your company – Which may put you in jeopardy of violating any policy your company may have in place.

Smart Computing



- The easiest way, especially when trusting other third party sites hosting Web 2.0 applications, is to protect yourself!
 - Understand the risks, understand how you are using the tool, and most of all acknowledge that tool is not, and will never be, 100% safe.
 - Everyone is susceptible to a hackers attack, the only way to stop them is to want to protect yourself.