

[Home \(https://www.hightechdad.com\)](https://www.hightechdad.com) » [Articles \(https://www.hightechdad.com/articles/\)](https://www.hightechdad.com/articles/) » [Fix It \(https://www.hightechdad.com/articles/fix-it/\)](https://www.hightechdad.com/articles/fix-it/)

WARNING: WP-Polls WordPress Poll Plugin Can Be Exploited

By Michael Sheehan(<https://www.hightechdad.com/author/michael/>)

December 21, 2009(<https://www.hightechdad.com/2009/12/21/>)

One ([https://www.hightechdad.com/2009/12/21/warning-wp-polls-wordpress-poll-plugin-Comment can-be-exploited/#comments](https://www.hightechdad.com/2009/12/21/warning-wp-polls-wordpress-poll-plugin-Comment%20can-be-exploited/#comments))

```
<?php
/**
 * Copyright 2009; Dr Small
 *
 * A simple way to increase a specific number of votes on
 * a wp-polls poll. It sets a new IP in the X-Forwarded-For
 * header, every time it executes, dumps cookies to /tmp and
 * doesn't read them the next time around.
 *
 * Howto use:
 * a) Find a Wordpress blog that uses a wp-polls poll
 * b) Use the URL as http://domain.tld/wp-content/plugins/wp-polls/wp-polls.php
 * c) View the page source, and find `name="poll_id" value="52"`
 * d) Use the value as your poll_id
 * e) Find the value of the specific poll option you want to vote on (i.e, name="poll_52" value="548")
 * f) Specify how many votes go toward that option (with votes)
 *
 * This same kind of method could be used on almost any kind of poll
 * that does not use "user registration & activation" to vote.
 */

/**
 * name:      Hack wp-polls
 * @param:    url          string          The URL to the plugins/wp-polls/wp-polls.php file
 * @param:    poll_id      int            The Poll ID
 * @param:    poll_value   int            The option being voted on
 * @param:    vote         int            How many times to vote on a given poll (default: 5)
 * @param:    verbose      string         How verbose to be (default: true)
 * @description: A proof of concept way to hack wp-polls.
 */
function hack_wp_polls($url, $poll_id, $poll_value, $vote=5, $verbose="false"){

    // Generate a 4 octive random IP address
    function makeUniqueIP($length){
```

Last week, I ran a giveaway (<https://www.hightechdad.com/2009/12/14/voting-time-hightechdads-hp-touchsmart-600-giveaway/>) which, because of a variety of reasons, I had to cancel (<https://www.hightechdad.com/2009/12/17/hightechdads-reasons-for-canceling-the-hp-touchsmart-giveaway/>) and declare "null & void". While I won't go into the details, I did

want to bring some actions to the forefront, especially if you are using the WordPress plugin called "WP-Polls (<https://wordpress.org/extend/plugins/wp-polls/>)" which is a great plugin that provides users with the ability to vote on questions and tally the results in graphs.

WP-Polls is currently the most popular polling and voting plugin with the WordPress "Extend" section with over 370,000 downloads. It is great for general polling of audiences. You can embed these polls into individual articles, in your sidebar or have them appear automatically in a dedicated page. The developer, LesterChan.net

(<https://lesterchan.net/portfolio/programming/php/>), has developed many great WordPress plugins of varying functionality. WP-Polls is described: *"Adds an AJAX poll system to your WordPress blog. You can easily include a poll into your WordPress's blog post/page. WP-Polls is extremely customizable via templates and css styles and there are tons of options for you to choose to ensure that WP-Polls runs the way you wanted. It now supports multiple selection of answers."*

(https://cdn.hightechdad.com/wp-content/uploads/2009/12/hack_Script.png)

As this was the most popular voting and polling plugin on WordPress, I thought that it would be good to do the "popular vote" for my computer giveaway. **I was very wrong.** Using a simple script, WP-Polls can be exploited and voting results can be manipulated. I have all the respect for the developer of this plugin as I regularly use other ones of his. My reasoning for posting this is to ensure that this exploit is highlighted so that the developer can change it and to inform other bloggers about the risks of using it.

I am posting the entire exploit below to bring light to it so that awareness can be spread and the hole can be fixed. This is from a forum post (<http://www.criticalsecurity.net/index.php/topic/32474-wordpress-wp-polls-post-data/>) on the Critical Security site. The poster introduces the script:

This is a function I've been writing, to basically brute-force my votes onto a Wordpress 'wp_polls' poll. wp_polls is a plugin for Wordpress, and the admin makes a poll with options, and can set restrictions on how many times a unique user can vote. I followed the theory and the clock work behind it, and see that it is only blocking you by IP Address (which, I will explain in a second), and cookies.









Apparently, for some unknown reason, Wordpress checks the X-Forwarded-For header, before it does the REMOTE_ADDR. With this in mind, we can write a script to send a uniquely spoofed X-Forwarded-For header, along with our POST data to the script, of which poll is being voted on (poll_id) and which option is being selected (poll_(poll_id)).

I basically dissected the HTML form data to determine what data had to be sent via POST, and collect the cookies, but don't use them again. I think the function turned out rather well... you can check it out and use it if you like. Basically, I can enter all of the poll_id's and which option is being voted on, and specify how many times I want the function to vote on a given option (while loop).

I started seeing this script in action on my site when a bunch of votes were being logged within the 1.0.x.x to 1.x.x.x range (typically a range reserved and not used as a public IP address). Also, a majority of the "valid" votes typically had the IP address and the associated node or computer name of the location (e.x., 123.456.789.012 computerabc.sbc.net). The "invalid" votes had numbers within the name field (123.456.789.012 123.456.789.012) and there were a huge number of votes of this type.

- Advertisement -
- Advertisement -

Shop Now

			
Amazon Smart Thermostat – ENERGY STAR certifie... (https://aax-us-east.amazon-adssystem.com/x/c/Rl3hvLh... adId=B08J4C8P36&creativ... 20&linkCode=w41&ref- refURL=https%3A%2F%2...	Amazon Smart Air Quality Monitor – Know your ai... (https://aax-us-east.amazon-adssystem.com/x/c/Rl3hvLh... adId=B08W8K5853&creati... 20&linkCode=w41&ref- refURL=https%3A%2F%2...	Blink Mini – Compact indoor plug-in smart security ... (https://aax-us-east.amazon-adssystem.com/x/c/Rl3hvLh... adId=B07X27V63D87&creati... 20&linkCode=w41&ref- refURL=https%3A%2F%2...	Surge Protector, Outlet Extender with Night Light, ... (https://aax-us-east.amazon-adssystem.com/x/c/Rl3hvLh... adId=B09XMM1Z5W&cre... 20&linkCode=w41&ref- refURL=https%3A%2F%2...
			
\$29.99 \$69.99 (715)	\$169.99 \$249.99 (11415)	\$16.99 \$29.99 (84497)	\$69.99 \$129.99 (51825)

exploited%2F&slotNum=1...	exploited%2F&slotNum=1...	exploited%2F&slotNum=1...	plugin-can-be-exploited%2F&slotNum=1...
prevent this from happening:			

(https://cdn.hightechdad.com/wp-content/uploads/2009/12/full_code.png)

Anyway, because of this script, there were many (several thousand) invalid votes that logged in my voting giveaway. Because of that as well as the fact that my site suffered a Denial of Service attack which prevented people from voting during the pre-defined voting period, I rendered the giveaway as null & void.

I also used another one of LesterChan's plugins called WP-Ban (<https://lesterchan.net/portfolio/programming/php/#wp-ban>) to help mitigate some of the issues that I was having. I put in ranges of IP numbers that needed to be blocked (e.g., those private IP ranges). The plugin description: *"Ban users by IP, IP Range, host name, user agent and referer url from visiting your WordPress's blog. It will display a custom ban message when the banned IP, IP range, host name, user agent or referer url tries to visit you blog. You can also exclude certain IPs from being banned. There will be statistics recorded on how many times they attempt to visit your blog. It allows wildcard matching too."* I also recommend the WP-DBManager (<https://lesterchan.net/portfolio/programming/php/#wp-dbmanager>) for backing up and restoring your databases.

- Advertisement -

HTD says: If you are going to use a poll to give away something or decide something critical, be sure that you use a 3rd party (not a WordPress plugin) to manage the process.

1 Response

HD 720p

says:

December 27, 2009 at 3:14 am (<https://www.hightechdad.com/2009/12/21/warning-wp-polls-wordpress-poll-plugin-can-be-exploited/#comment-12090>)

thanks for the great content posted here will always be visiting your blog

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Post Comment

This site uses Akismet to reduce spam. [Learn how your comment data is processed \(https://akismet.com/privacy/\)](https://akismet.com/privacy/).

Other articles of interest

(<https://www.hightechdad.com/2022/11/13/46-bottles-wine-newair-wine-fridge-dual-zone-control-review/>)

46 Bottles of Wine? Chill them all in the NewAir Wine Fridge with Dual Zone Control (Model – NWC046BS00) – Review

(<https://www.hightechdad.com/2022/11/13/46-bottles-wine-newair-wine-fridge-dual-zone-control-review/>)

November 13, 2022 /// No Comments

Review of the NewAir wine fridge, which holds up to 46 bottles of wine and has dual temperature settings for red & white wine.

(<https://www.hightechdad.com/2022/11/11/dont-use-stock-charger-ugreen-nexode-usb-gan-chargers-set-new-better-standard-review/>)

Don't use a stock charger, UGREEN Nexode USB GaN Chargers set a New, Better Standard – Review (<https://www.hightechdad.com/2022/11/11/dont-use-stock-charger-ugreen-nexode-usb-gan-chargers-set-new-better-standard-review/>)

November 11, 2022 /// No Comments

Review of two UGREEN Nexode USB GaN chargers – 140W and 45W – perfect mobile & travel chargers for a variety of devices (laptops, smartphone, tablets).

Read More » (<https://www.hightechdad.com/2022/11/11/dont-use-stock-charger-ugreen-nexode-usb-gan-chargers-set-new-better-standard-review/>)

(<https://www.hightechdad.com/2022/10/31/mophie-powerstation-battery-solutions-provide-on-demand-power-multiple-devices-review/>)

These 2 Mophie Powerstation Battery Solutions Provide On-Demand Power for Multiple Devices – Review (<https://www.hightechdad.com/2022/10/31/mophie->

powerstation-battery-solutions-provide-on-demand-power-multiple-devices-review/)

October 31, 2022 /// No Comments

Review of the Mophie powerstation pro XL and the Mophie powerstation plus – two portable battery solutions to reduce the away-from-the-plug anxiety.

[Read More »](https://www.hightechdad.com/2022/10/31/mophie-powerstation-battery-solutions-provide-on-demand-power-multiple-devices-review/) (https://www.hightechdad.com/2022/10/31/mophie-powerstation-battery-solutions-provide-on-demand-power-multiple-devices-review/)

Global Product Review Disclosure

Disclosure: *This is a global disclosure for product review articles on HighTechDad. It does not apply to Automobile reviews and there are other exceptions. Therefore, it may or may not be applicable to this particular article.* I may have a material connection because I may have received a sample of a product for consideration in preparing to review the product and write this or other content. I was/am not expected to return the item after my review period. All opinions within this and other articles are my own and are typically not subject to the editorial review from any 3rd party. Also, some of the links in the post above may be “affiliate” or “advertising” links. These may be automatically created or placed by me manually. This means if you click on the link and purchase the item (sometimes but not necessarily the product or service being reviewed), I will receive a small affiliate or advertising commission. More information can be found on my About page (<https://webcache.googleusercontent.com/about/>).

– Advertisement –



(<https://www.hightechdad.com>)

Michael Sheehan (“HighTechDad™”) is an avid technologist, writer, journalist, content marketer, blogger, tech influencer, social media pundit, loving husband and father of 3 beautiful girls living in the San Francisco Bay Area. This site covers technology, consumer electronics, Parent Tech, SmartHomes, cloud computing, gadgets, software, hardware, parenting “hacks,” and other tips & tricks.

(<https://www.hightechdad.com/about/michael-sheehan>)

Latest Articles

46 Bottles of Wine? Chill them all in the NewAir Wine Fridge with Dual Zone Control (Model – NWC046BS00) – Review
(<https://www.hightechdad.com/2022/11/13/46-bottles-wine-newair-wine-fridge-dual-zone-control-review/>)

Don't use a stock charger, UGREEN Nexode USB GaN Chargers set a New, Better Standard – Review
(<https://www.hightechdad.com/2022/11/11/dont-use-stock-charger-ugreen-nexode-usb-gan-chargers-set-new-better-standard-review/>)

These 2 Mophie Powerstation Battery Solutions Provide On-Demand Power for Multiple Devices – Review
(<https://www.hightechdad.com/2022/10/31/mophie-powerstation-battery-solutions-provide-on-demand-power-multiple-devices-review/>)

GENEVERSE HomePower ONE Battery Backup & Solar gives you Emergency Power Anytime, Anywhere! Review
(<https://www.hightechdad.com/2022/10/29/geneverse-homepower-one-battery-backup-solar-emergency-power-anytime-anywhere-review/>)

Bring Big Screen Digital Entertainment Outside – 55" QLED Sylvox Deck Pro Outdoor TV Review
(<https://www.hightechdad.com/2022/10/20/big-screen-digital-entertainment-outside-55-qled-sylvox-deck-pro-outdoor-tv-review/>)

About HighTechDad™

About(<https://www.hightechdad.com/about/>)

Agency & Brand Contact(<https://www.hightechdad.com/contact-main/vendors/>)