

## CodeIgniter Global XSS Filtering Bypass Vulnerability

Discovered by : d0ubl3\_h3lix  
 Date : December 2007  
 Product : [CodeIgniter](http://www.codeigniter.com) < http://www.codeigniter.com >  
 Product Description : Open-source PHP Framework  
 Pen-Tested Version : 1.5.2  
 Vulnerability : User-Agent injection  
 Risk : Medium  
 Threat : XSS, Log File Tampering

### Description:

\$CI->input->user\_agent() fails to check the validity of user-agent type. It simply extracts from \$\_SERVER array without checking whether it is bad string injection or not. In this case, we can spoof user agent string of our browser with our arbitrary commands that can bypass stronger CodeIgniter Security class even if \$config['global\_xss\_filtering'] = TRUE;. Thus we can execute XSS on the fly.

### Proof-Of-Vulnerability:



## My Blog Heading

Your browser is : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv.1.8.0.7)

```
echo 'Your browser is : '.$this->input->user_agent();
```



## My Blog Heading

Your browser is : Owned by d0ubl3\_h3lix