

Forum:[Hack Forums](#)

Thread: [\[TuT\]SQL injection by X-forwarded-for\[TuT\]](#)

??????? - June 10, 2012, 8:03 am

SQL injection : X-forwarded-for

Requirements :

Site that use X-forwarded-for

Basic knowledge with SQLi (string based)

Live HTTP headers

Introduction :

X-forwarded-for is often use to get the ip of user even though he uses a proxy.

Example and explanation :

PHP Code

```
<?php
function getip()
{
    if (isset($_SERVER['HTTP_X_FORWARDED_FOR']))
    {
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    }
    else
    {
        $ip = $_SERVER["REMOTE_ADDR"];
    }
}
```

This code create an ip variable with the real ip.

PHP Code

```
<?php
if (preg_match("#^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}#", $ip))
{
    return $ip;
}
else
{
    return $_SERVER["REMOTE_ADDR"];
}
}
```

This code check if it's real ip but this code is vulnerable, why ?

Because a regex has a beginning and a end. The beginning delimiter is ^ and the ending delimiter is \$, note that the \$ is missing. So the regex check only the beginning of the ip. If your ip is 127.0.0.1 the regex will send back true but if your ip is 127.0.01+whatever you want the regex will send back true too.

PHP code that is vulnerable :

PHP Code

```
<?php
```

```
$req = mysql_query("SELECT username,password FROM admin WHERE username='".sql($_POST['username'])."' AND password='".md5($_POST['password'])."' AND ip='".$_GET['ip']."'");
```

Exploitation:

First open Live HTTP headers then actualize the page :

[\[IMG\]http://img15.hostingpics.net/pics/873830http1.png\[/IMG\]](http://img15.hostingpics.net/pics/873830http1.png)

Note that the injection will be a string based.

Now click on the url then click on replay and add :

Code X-forwarded-for: 127.0.0.1

[\[IMG\]http://img15.hostingpics.net/pics/317006http2.png\[/IMG\]](http://img15.hostingpics.net/pics/317006http2.png)

Then add a quote after your ip address and a nice error like that will be displayed :

[\[IMG\]http://img15.hostingpics.net/pics/953087sql1.png\[/IMG\]](http://img15.hostingpics.net/pics/953087sql1.png)

And now do your injection like string based, the most important thing is that you have to understand that the injection point is your ip in X-forwarded.

Hope you learnt something new

Phizo - June 10, 2012, 8:04 am

Awesome tutorial man, I haven't seen this posted before.

Keep up the good work!

No??????? - June 10, 2012, 8:06 am

This looks interesting and I haven't seen it around here before. Great work!

joomlafkr - June 10, 2012, 8:14 am

Happy to see new stuff shared here !

Good work OP !

Actually sqlmap does that by increasing --level and --risk and there are many other fields in the header that could be exploited !

???????? - June 10, 2012, 3:06 pm

Thanks for feedbacks glad you like.

doegizfruit - June 13, 2012, 9:41 am

Nice tutorial very high quality!

Thanks for sharing this.

???????? - June 13, 2012, 9:44 am

(Jun 13, 2012 09:39 AM)Suved Wrote: [\[CITE\]](#) Nice tutorial.

Thanks for sharing.

How can i know the site use X-forwarded-for?

Only by the source code that because this method is pretty rare but sometimes very useful.

MaXoNe - June 13, 2012, 9:50 am

Nice technique , I like it , finally something new :)

Zixem - June 13, 2012, 10:01 am

Nice tutorial.

Thanks for sharing.

-Zixem-

PlickaMaterna - June 13, 2012, 10:25 am

What is the point of sharing this?

You are spoonfeeding all those wannabe hackers here. I mean those people don't know what a header even is.

fuckhackforums

The Ion - June 13, 2012, 10:30 am

Awesome tutorial man, I haven't seen this posted before.

Keep up the good work!

???????? - June 13, 2012, 10:33 am

(Jun 13, 2012 10:25 AM)Plitvix Wrote: [\[CITE\]](#) What is the point of sharing this?

You are spoonfeeding all those wannabe hackers here. I mean those people don't know what a header even is.

fuckhackforums

What is the point of posting your reply, I want to share my knowledge with all members this is the point of this forum, if you want to keep your knowledge without shared with others I think you're in wrong place.

Dynasty@HF - June 13, 2012, 10:33 am

good tutourial this will help me out loads thanks for sharing this ?

Lynchings - June 13, 2012, 12:07 pm

Nice tutorial. Helped me. This has to be almost as good as RATting people. :o

Prithvi - June 14, 2012, 1:23 am

learned something new

Thanks bro..

RIPPER - June 15, 2012, 7:34 am

Thanks man..New shit to this forum...Peace

toniohawk2 - July 3, 2012, 4:08 am

Merci pour le tuto, très intéressant et à essayer bien évidemment ;) (Pour une fois que je peux remercier un membre en français ^^)

Prominent - July 3, 2012, 5:48 am

Knew about this but not that much, nonetheless great work!

Little_Miss_Baca - July 3, 2012, 10:05 pm

Thank you OriginalsGeeks

I'm not sure I get it yet, at least not by the first look of it, but a little practice will do wonders, I'm sure :)

Can you explain when is this method needed actually?

evolutionroh - July 3, 2012, 11:26 pm

Awesome tutorial .. thnks for sharing

sandeep1024 - August 13, 2012, 5:41 am

nice tut bro thanks for share....something new in hand

ajkaro - August 13, 2012, 12:37 pm

I learned something new from your tutorial. Thanks ...

hacking - August 13, 2012, 3:30 pm

this tut seems to be useful. i bookmarked it for after. thank you buddy

literalraise - August 20, 2012, 3:45 pm

thanks newbie like me always need something like this :)

sofinho - August 20, 2012, 4:12 pm

nice tut!

does the page we inject has to be index.php?p=admin ?

also, is there a way of finding if the site has x-forward before even starting http header?

thanks

Desdo - August 22, 2012, 10:33 am

Awesome tutorial man, Nice job man.

realglynn04 - August 23, 2012, 4:30 pm

thanks for sharing man! nice tut , keep it up

GreyPhantom - September 21, 2012, 4:12 am

Can you give me that En-tetes HTTP en direct?

b001ean - September 21, 2012, 5:05 am

Interesting tut.. thanks for sharing.. :)

Danger0uss - September 21, 2012, 5:39 am

is there any dork to find websites that use this option to get user ip ?

balaghacking - May 19, 2014, 8:24 pm

Nice tut

..... thanks for sharing.. :)

wick3dj0k3r - May 20, 2014, 10:07 pm

Never knew this, thanks OP for sharing this ...

