Ebay OnLine Attack Jargon

By: Aditya K Sood
Handle : Zeroknock
http://zeroknock.metaeye.org

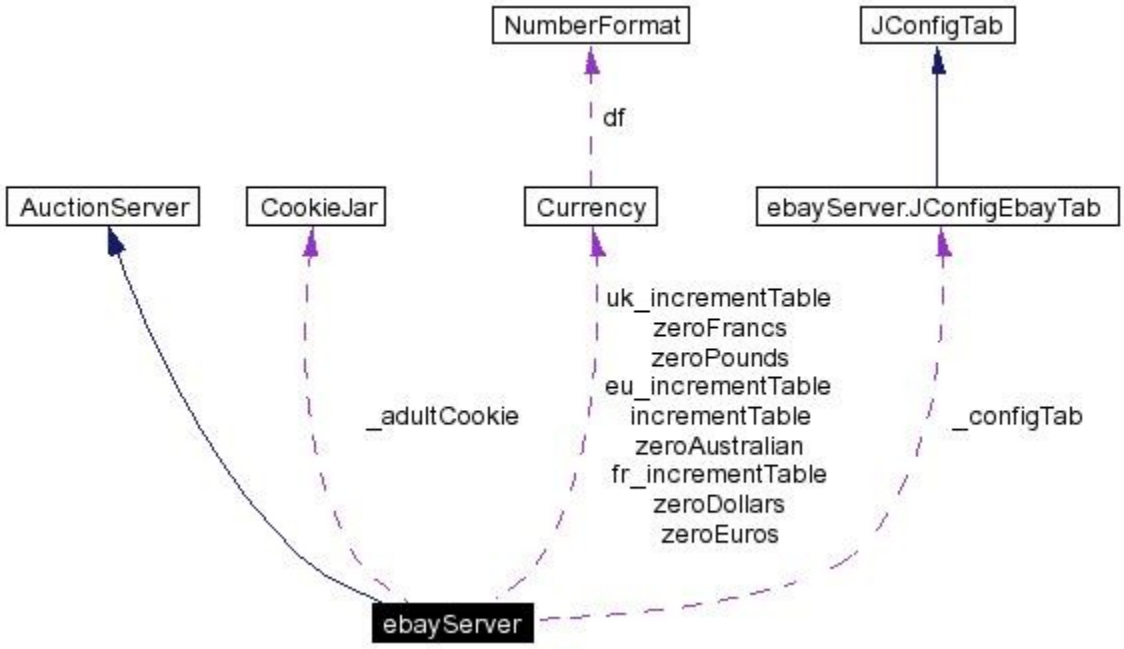
Abstract:

This article relates to various online attacks that occurs through ebay and gets to core how the things are manipulated by the hackers to get work done of their own choice.This includes redirection attacks , phishing attacks and bypassing login attacks which are usually run on the net now a days.

Explanation

Now we are going to understand the core of Ebay where the attack usually occurs.For this we should know the working model of Ebay and the major functions adhere to it.First of all we look at the how the online format has been set.The various cross references structure included in that which made the manipulation possible.

Lets see the structure



From the above diagram its very clear how the relative functioning occurs in Ebay.This undertake the working model of ebay server and its adjacent working elements ie auction server , currency stuff and etc.The server is at base which provides the parent functioning to the child elements. We are interested in the actual parameters where the exploitation occurs.

Now we take a look at the functions.

final String ebayServer.eBayAcceptItem = "MfcISAPICommand=AcceptBid" [protected]
final String ebayServer.eBayAdultCGIHost = "cgi3.ebay.com" [protected]
final String ebayServer.eBayAdultLoginPageTitle = "eBay Adult Login" [protected]
final String ebayServer.eBayAdultLoginToken =
"MfcISAPICommand=AdultLogin" [protected]
final String ebayServer.eBayBidItem = "MfcISAPICommand=MakeBid" [protected]
final String ebayServer.eBayBidItemCGI = "&item=" [protected]
final String ebayServer.eBayBINItem = "MfcISAPICommand=BinConfirm" [protected
final String ebayServer.eBaySearchURL = "http://search-desc.ebay.com/search/
search.dll?MfcISAPICommand=GetResult&query=" [protected]

Here i have undertaken some of the defined generic functions that are used by Ebay server in its processing and if we look at core we will find the core element is ISAPI.Actually the ebay server works under the working capability of ISAPI.DLL.This DLL is crafted dynamic link library which have cross referential arranagment of every single working element which relates to the ebay transaction , auction , currency etc. This is the prime target of attackers through which a Command parameter is passed which perform the required functioning of hackers choice.Basically the URL is argumented with certain parameters that are responsible of Ebay exploitation. So the very basic and very crafty element is ISAPI which is Internet Service Application Programming Interface that serves as interface to the server with DLL implementation.

Example :

ISAPI DLL Request For Login Processing:

```
HTML>
<HEAD>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<META NAME="Author" CONTENT="ZeroKnock">
<META NAME="GENERATOR" CONTENT="Mozilla/4.04 [en] (WinNT; I) [Netscape]">
<TITLE>LogonForm</TITLE>
</HEAD>
<BODY>
<FORM ACTION="http://mig/scripts/logon.dll" METHOD=POST>
<INPUT TYPE=HIDDEN NAME=MfcISAPICommand VALUE=LogonProc>
<P>Name<BR>
<INPUT TYPE=TEXT NAME=id VALUE="Your Name">
<P>Password<BR>
<INPUT TYPE=PASSWORD NAME=pw>
<P><INPUT TYPE=SUBMIT VALUE=OK><INPUT TYPE=RESET VALUE=Reset>
</FORM>
</BODY>
</HTML>
```

The MfcISAPICommand is a hidden control on the form to define a handler function to be used to process the form on the server.

Adding Command Handler to DLL

Introduce the LogonProc function in CLogonExtension class. Do it right before the Default function:

```
void LogonProc(CHttpServerContext* pCtxt,LPCTSTR pszName,LPCTSTR pszPassword);
```

Add CommandProc handler to the parse map:

```
ON_PARSE_COMMAND(LogonProc, CLogonExtension, ITS_PSTR ITS_PSTR)
ON_PARSE_COMMAND_PARAMS("id=~ pw=~") Write code for the LogonProc function:
void CLogonExtension::LogonProc(CHttpServerContext* pCtxt,LPCTSTR pszName,LPCTSTR
pszPassword)
{
StartContent(pCtxt);
WriteTitle(pCtxt);
CString strPassword = pszPassword;
if ("password" == strPassword)
*pCtxt << _T("Access granted!");
else
*pCtxt << _T("Incorrect password... Please try again...");
EndContent(pCtxt);
}
```

The example sets the working stuff of ISAPI DLL.Now i am going to present you some of the crafted URL using ISAPI extension dll for defining request on the ebay server.

http://<NetBIOS or DNS name>/Panorama/CONNECTOR.dll?MfcISAPICommand=WebUtility&Query={Unique_Identifier}
http://feedback.ebay.com.cn/ws/eBayISAPI.dll?ViewFeedback&userid=exploiting
https://signin.ebay.in/ws/eBayISAPI.dll?
http://search.ebay.com.au/search/search.dll?MfcISAPICommand=GetResult&ht=1&SortProperty=MetaEndSort&query=8mm&ebaytag1code=15&shortcut=2&maxRecordsReturned=300&maxRecordsPerPage=50&SortProperty=MetaEndSort

These are the URL examples which are processed by the server for request. Now see the which parameter server processes :

final StringeBayFile = "/aw-cgi/eBayISAPI.dll"
final StringeBayViewItemCGI = "ViewItem&item="
final StringeBayViewDutchWinners = "?ViewBidsDutchHighBidder&item="
final StringeBayBidItemCGI = "&item="
final StringeBaySearchURL = "http://search-desc.ebay.com/search/search.dll?
final StringeBayBidItem = "MfcISAPICommand=MakeBid"
final StringeBayAcceptItem = "MfcISAPICommand=AcceptBid" final StringeBayBINItem = "MfcISAPICommand=BinConfirm"
MfcISAPICommand=GetResult&query=" final StringeBaySearchURLEnd = "&search_option=1&srchdesc=y&SortProperty=MetaEndSort"
final StringeBayAdultLoginToken = "MfcISAPICommand=AdultLogin"

These are some of the protected methods used by the server for online transaction functioning , these are the prime target elements of phishers or attackers to throw attack on server. The various attack that can be undertaken from this :

Remote Command Execution With Buffer Overflows:
Sometimes this DLL is vulnerable to buffer overflow attacks which further results in the remote command execution on the server.

Example:

GET /<FileName>.dll?mfcisapicommand=AAA...[250 chars]...AAA&page=index.htx
Windbg trace:
(360.21c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=026bda14 ebx=01130478 ecx=41414141 edx=0113057d esi=41414141
edi=77e2b495
eip=10042004 esp=026bd8f4 ebp=026bdbe0 iopl=0 nv up ei pl nz na po
nc cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000efl=00010206

This is generic case of DLL buffer overflows.These overflows occur time to time and the server can be set to compromise with remote code inclusion.So implementation of DLL is always risk because if one flow occurs the whole system will be gone.

This is first class of attack that can be done through Ebay server till the vulnerability exist on server.

Fake Phishing Ebay Attacks

The phishing attacks are also a main point of manipulation as the fake web page is subjected on to the net with the same ebay outlook but the normal users to get tricked very easily as:

A] The Fake page donot have Verisign SSL check on the page most of times.
B] The website is not opened as HTTP over SSL which we called as HTTPS.
C] The SSL Certificate got expired or not valid.

Login to unwanted pages through email that are sent by Ebay as the mail specify.

Lest Check two Login Pages:

As you can see Verisign check of SSL Certification or u can find a lock sign in URL.

This is fully fake as no SSL check is present and there is no such microsoft specifc services linked with it.This is done to login fake hotmail pages which run trojans at back to capture your Id , credit cards and email addresses fro further spamming.

Redirection Attacks: Spamming Tool

Redirection attacks also possible through Ebay ISAPI dll to spoof identity of ones which is just surfing the third party through intermediate stuff.

```
http://cgi4.ebay.com/ws/eBayISAPI.dll?MfcISAPICommand=RedirectToDomain&DomainUrl=ht
tp://wwwMetaEye.Org
```

The pre defined URL will redirect the main page to the destination URL.So these are the specific classes of attacks that are undertaken for EBAY.Ebay is getting traumatised by the non ethical people.

At end lets look at the ISAPI.dll layout of Ebay.

Total Time: 2.769

Type	Total	Bytes	DNS	FirstByte	LastByte	Total	Time %	Byte %	Errors
HTML	1	9642 (9642)	0.156 (0.156)	0.203 (0.203)	1.813 (1.813)	2.172 (2.172)	19.4	7.5	0
Images	6	1521 (253)	0.327 (0.054)	3.002 (0.500)	0.515 (0.086)	3.844 (0.641)	34.3	1.2	0
Javascript	3	117625 (39208)	0.159 (0.053)	4.619 (1.540)	0.403 (0.134)	5.180 (1.727)	46.3	91.3	0
All Files	10	128788 (12878)	0.641 (0.064)	7.824 (0.782)	2.731 (0.273)	11.196 (1.120)	100.0	100.0	0

Per request averages in parantheses

Total Header Size: Responses=3539 Requests=3723

8578 bytes may be saved by compressing javascript.

The result is all in front of yours.

This is written for education purposes only.