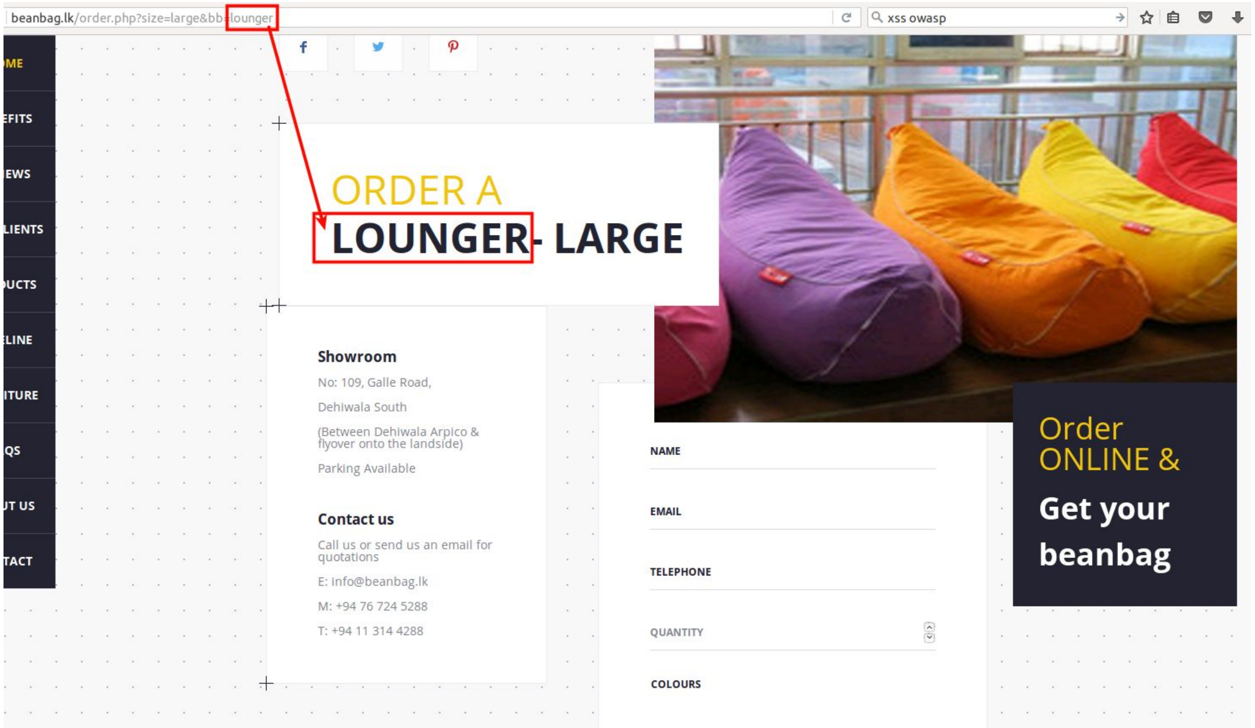
XSS Attack Demonstration: BeanBag.LK

In the BeanBag.LK website's order.php page, the query parameters 'size' and 'bb' are vulnerable to Injection attacks. This shows how an attacker can use this vulnerability of the website for malicious activities.

http://beanbag.lk/order.php?size=large&bb=lounger



ORDER A

LOUNGER- LARGE

Showroom

No: 109, Galle Road,

Dehiwala South

(Between Dehiwala Arpico & flyover onto the landside)

Parking Available

Contact us

Call us or send us an email for quotations

E: info@beanbag.lk

M: +94 76 724 5288

T: +94 11 314 4288

NAME

EMAIL

TELEPHONE

QUANTITY

COLOURS

Order ONLINE &

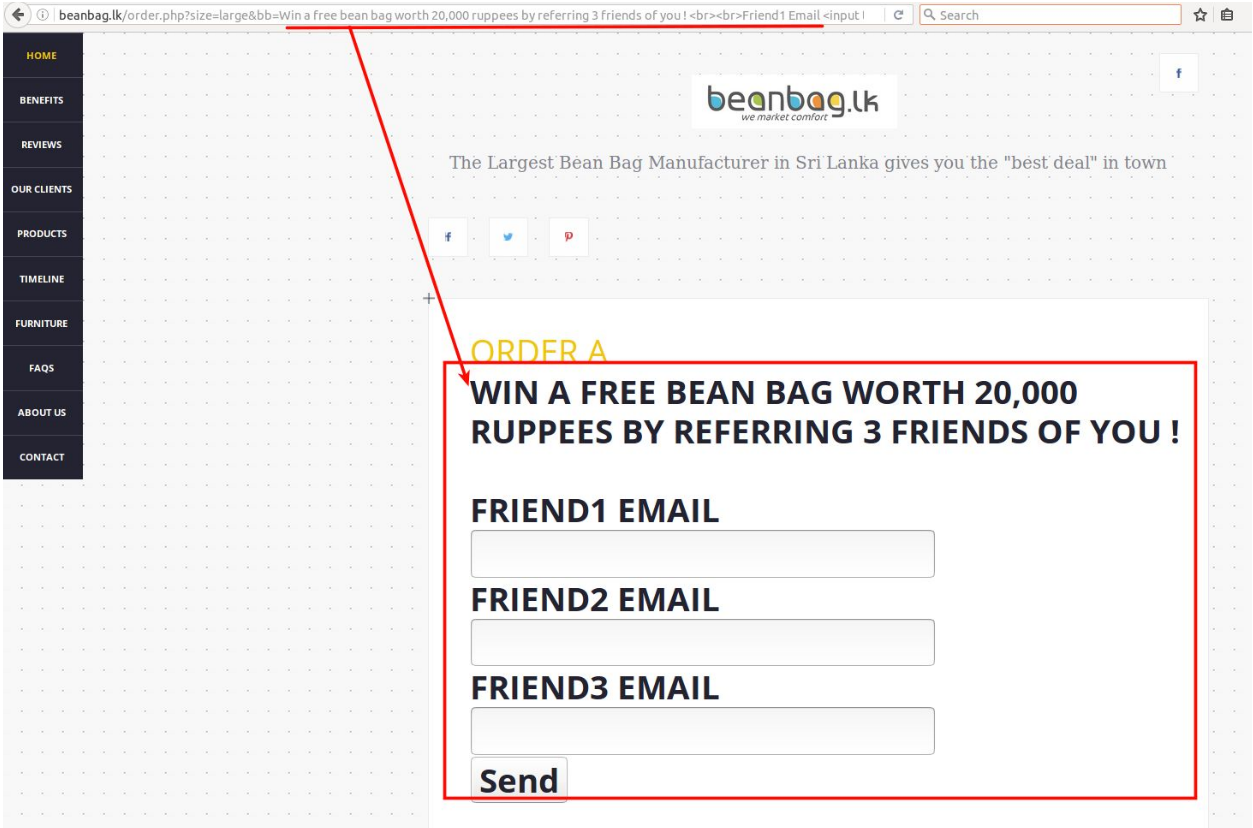
Get your beanbag

In this demonstration, I am injecting malicious content to the 'bb' query parameter.

In this example, let's assume that the attacker wants to steal some email addresses. He prepares the following URL.

http://beanbag.lk/order.php?size=large&bb=Win a free bean bag worth 20,000 ruppees by referring 3 friends of you ! <br><br>Friend1 Email <input type="text" id="email1"/><br>Friend2 Email <input type="text" id="email1"/><br>Friend3 Email <input type="text" id="email1"/><br><input type="submit" value="Send"/><!--

When an end user visits this URL, the user sees the order.php of BeanBag.LK website like following.



beanbag.lk/order.php?size=large&bb=Win a free bean bag worth 20,000 ruppees by referring 3 friends of you !

Friend1 Email <input i

The Largest Bean Bag Manufacturer in Sri Lanka gives you the "best deal" in town

ORDER A

WIN A FREE BEAN BAG WORTH 20,000 RUPPEES BY REFERRING 3 FRIENDS OF YOU !

FRIEND1 EMAIL

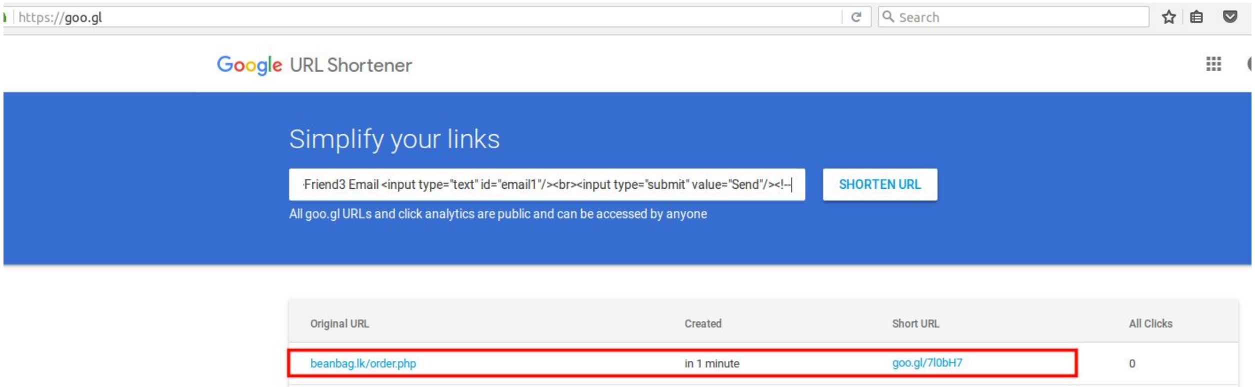
FRIEND2 EMAIL

FRIEND3 EMAIL

The end user can be tricked to send 3 email addresses of his/her friends with this. (Note that I haven't written the logic for sending the values to an external server, but it's pretty simple.)

Here, the website URL starts with the real domain of BeanBag.LK. So, unless the end user is a technical person with knowledge on security, a general user would not notice anything suspicious.

Now, the attacker does not share this lengthy URL. So the attacker simply uses a URL shortener to get a shortened URL.



Simplify your links

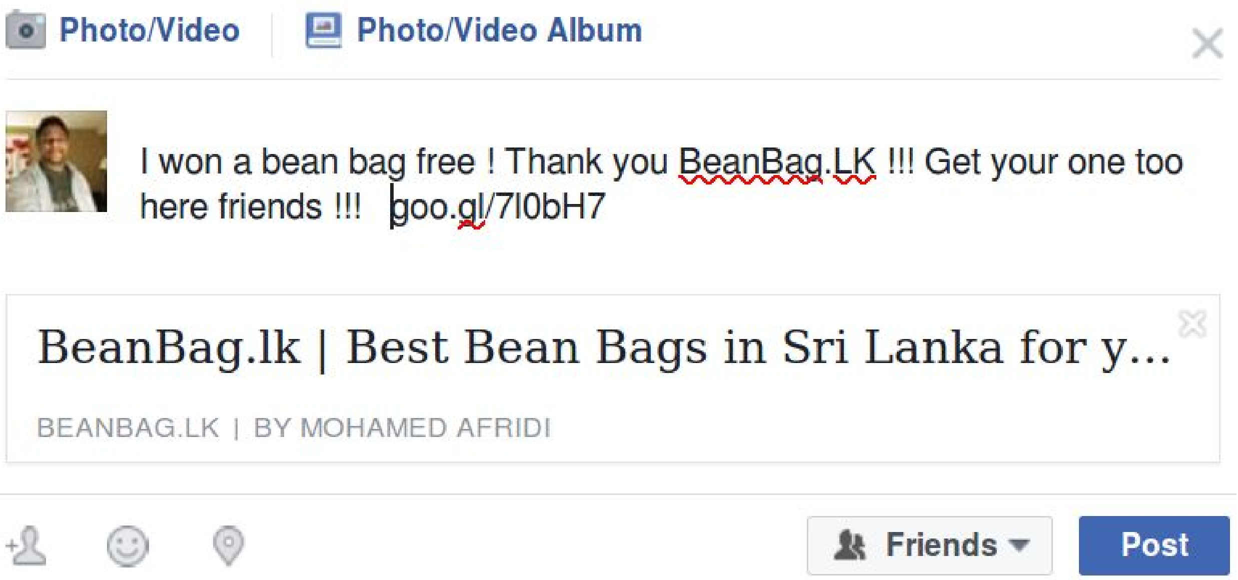
```
Friend3 Email <input type="text" id="email1"/><br><input type="submit" value="Send"/><!–
```

All goo.gl URLs and click analytics are public and can be accessed by anyone

Original URL	Created	Short URL	All Clicks
beanbag.lk/order.php	in 1 minute	goo.gl/7l0bH7	0

With Google’ URL shortener, the attacker gets a URL like goo.gl/7I0bH7 .

Next step is to attract people to click on the link. May be the attacker can share the link via a forum or as a facebook post or publish in some group.



I won a bean bag free ! Thank you BeanBag.LK !!! Get your one too here friends !!! goo.gl/7I0bH7

BeanBag.lk | Best Bean Bags in Sri Lanka for y...

BEANBAG.LK | BY MOHAMED AFRIDI

This is a simple demonstration. If you think creatively, you can come up with so many different ways to use BeanBag.LK website’s good name to achieve your malicious desires.

Declaration

I, Tharindu Edirisinghe hereby declare that all the security testing carried out on the beanbag.lk website were done only with the intention of discovering any potential security vulnerabilies of the website and to ensure the safety of the end users of the website. Apart from that, I hereby confirm that I had no intention of harming the website or the brand name of the company or gaining any financial benefit over exploiting the discovered vulnerabilities. This report is prepared for helping the web development team of BeanBag.LK and this will only be shared with the above stakeholders until the discovered issues are fixed.

Tharindu Edirisinghe (thariyarox),
Independent Security Researcher
Author of http://securityinternal.com
Twitter: https://twitter.com/thariyarox
LinkedIn: https://lk.linkedin.com/in/ediri