Reflective XSS and Open Redirect on Indeed.com subdomain

Syntax Error Follow
Sep 4, 2017 · 2 min read

Hi Again! So here is one more writeup on a simple bug I found on Indeed.com subdomain.

As always I looked up for subdomains using Sublist3r tool.

While I was browsing through offfers.indeed.com subdomain ,I noticed a functionality where a user could choose some filters from dropdown and create a PDF report of the data which was generated.

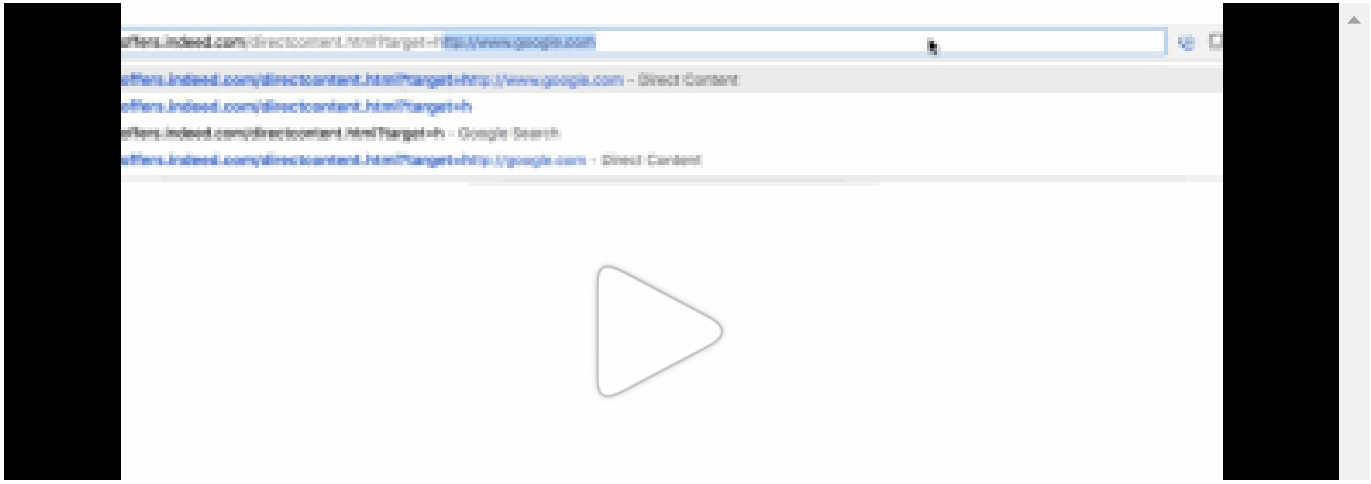
I quickly selected some values and generated the report.When I Opened the Report ,I noticed that the URL had an extra parameter **Target** which had

the file location for the PDF file.

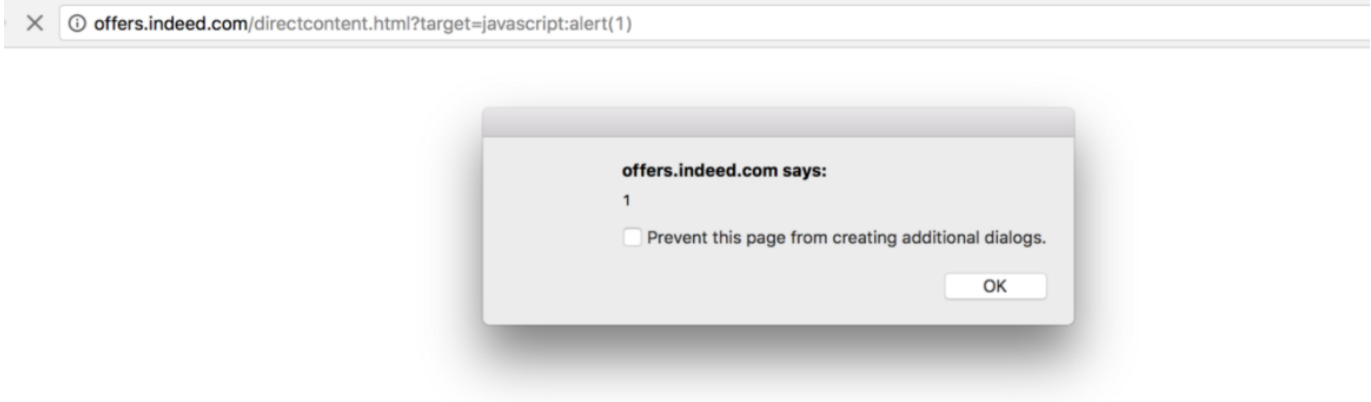
http://offers.indeed.com/directcontent.html?target=http://offers.indeed.com/company/xy/xxyy.pdf

On seeing **Target** parameter in URL, my instant thought was to test for Open redirect .So I entered Target parameter value as https://www.google.com and I noticed it was actually taking user to Google.com

Vulnerable URL :http://offers.indeed.com/directcontent.html?target=http://www.google.com



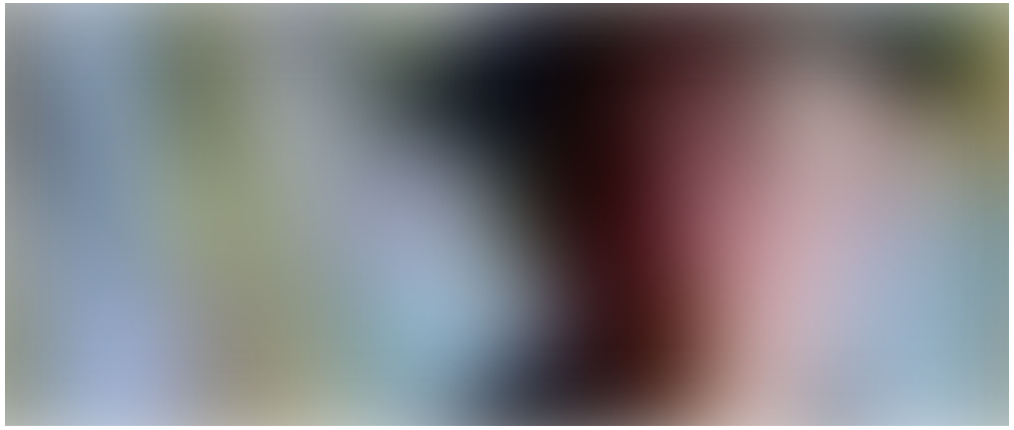
Next was to check if the same parameter was vulnerable to XSS as well. I gave the **Target** parameter value as **javascript:alert(1)** and as I was suspecting alert box popped up.



I reported this issue to Indeed Via Bugcrowd and the bug was resolved within a week.As part of fix, they completely removed this functionality from the site.

For any question,You can get in touch with me @syntaxerror

Untill next time



Security

304 claps

WRITTEN BY

Syntax Error

DwWI92mUoaxZ

Follow

Write the first response

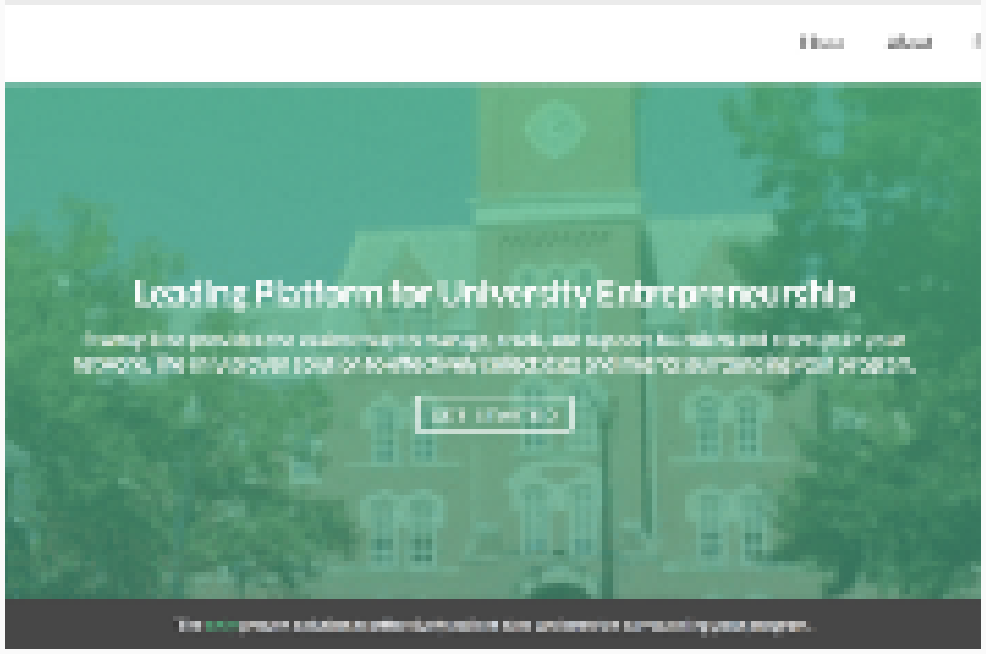
More From Medium

Related reads

Open Redirects & Security Done Right!

Akshay 'Ax' Sharma
Jun 19, 2018 · 3 min read ★

490



Related reads

How to Upgrade Your XSS Bug from Medium to Critical

Luke Stephens (@hakluke)
May 21 · 5 min read ★

656

Related reads

Diving into unserialize(): Magic Methods

Vickie Li in The Startup
Sep 29 · 4 min read ★

110