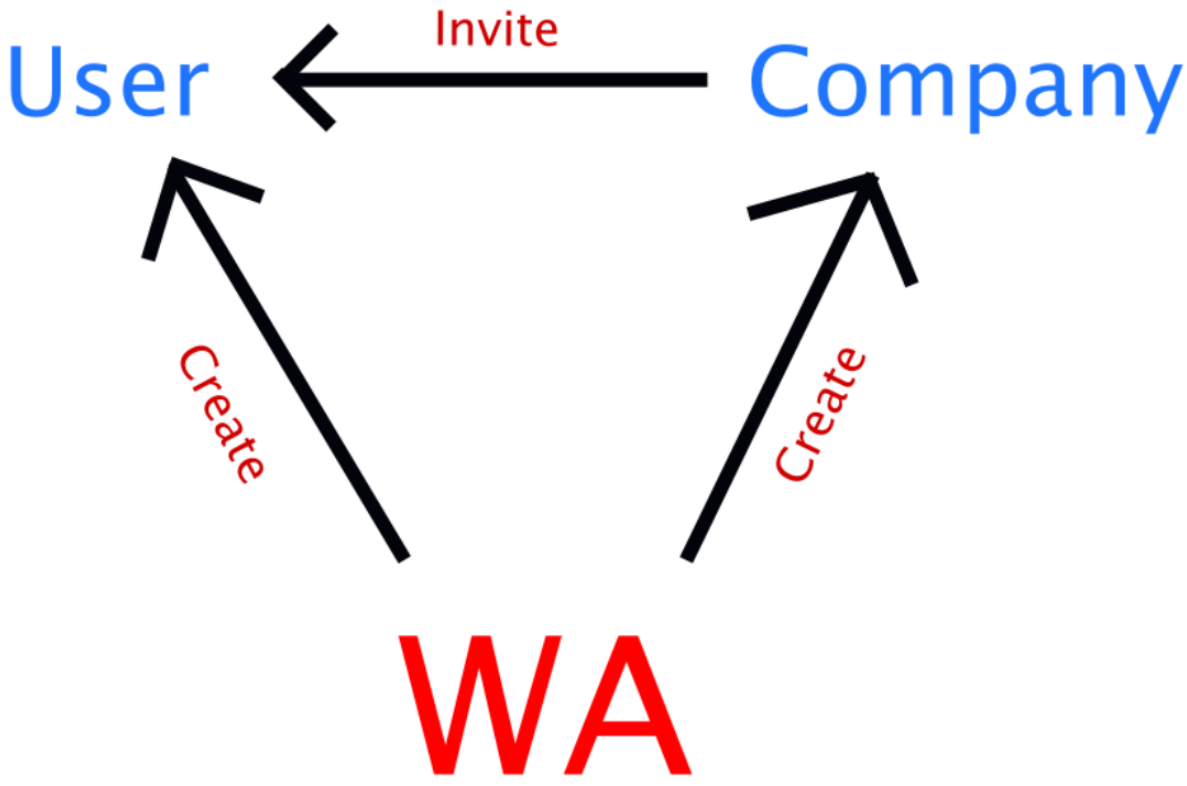
BugBounty WriteUp — take attention and get Stored XSS

Александр Опанасюк Follow
Aug 14 · 3 min read

Hi all,

The sponsor of this writeup is the attention for minor features that allowed me to get a good *xxxx* reward.



So, let's imagine that we have a Web Application "**WA**", that allows you to *create users*, *companies* and *invite users to the company*.

The functional of inviting worked like this — the user received a letter in the mail, where it was said: "*You were invited to join company Hackerman. Accept invite*[link]"

As the site allowed us to name of company contain "<> etc — I put the name of company as:

```
lekssik"><h1>xd</h1>
```

And you know what… I got such invite on email:

You were invited to join company lekssik">

xd

. Accept invite!

So I got such things earlier, and in principle… we can already report at this point, since this allows us to generate HTML messages by mail and send on behalf of the web application. (I used to find such a vulnerability on the site of one mobile giant, there we could change some parameters in the post request for registration, and then the link to confirm the account came with a broken HTML).

But… I sat on the site a little more and found that the site has internal notifications that you were invited — and when you go to the notification page — a window appears that says about the invitation. And you know what? They also did not filter html on this page :))))))

Sooo, lets register comapany a”><svg\onload=alert(1)> and — for all the users that we invite — they receive notifications about the invitation, thereby activating the Stored XSS.

And after reporting and confirmation of vulnerability — a team member wrote to me that the problem with the email is a duplicate, but the previous hacker didn't say anything about the Stored XSS! It's a pity, because it turns out he missed such functionality and such critical vulnerability :(

. . .

While I was writing this WriteUp, I suddenly started to feel sorry for myself too — I remembered the #bugbountytips from intigrity — and there was a picture like "Found SSRF — exploit RCE, found Self-XSS — exploit Stored XSS with the help of CSRF, Found Stored XSS — exploit Account Takeover". And only now I realized that I could work a little more and get much more, even P1. I hope you do not repeat my mistakes, always take the maximum impact from any vulnerability!

. . .

Find out more writeups (LOL 1 more xd)— https://twitter.com/Lekssik2 — will try to make them in more quantity and describe more interesting bugs.

Have a good day and wish you success in all your endeavors! :)

Oleksandr Opanasiuk

The latest Tweets from Oleksandr Opanasiuk (@Lekssik2). Great manager and not bad pentester https://t.co/qJyb7tVAtx...

twitter.com

Security | Bug Bounty | Pentesting | Hacking | Writeup

71 claps

WRITTEN BY

Александр Опанасюк

Follow

Write the first response

More From Medium

Related reads

The BatchOverflow Bug and How to Catch All Bugs

Kiran Garimella
May 11, 2018 · 12 min read ★

306

Related reads

The Bugs Are Out There, Hiding in Plain Sight

A Bug'z Life in A Bug'z Life

A Bug 2 Life in A Bug 2 Life

Jul 15 · 6 min read ★

635

s great

identity-credentials/

Related reads

What to Do if Your WordPress Website Was Hacked

HostPapa

Oct 16, 2018 · 11 min read

58

Discover Medium

Make Medium yours

Become a member

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade

Medium

About Help Legal