



detectify™

Kan vi lita på våra molnleverantörer?

Frans Rosén #whoami

Knowledge Advisor, @detectify (@fransrosen)

Bloggar på labs.detectify.com

HackerOne #3 <https://hackerone.com/thanks>



Att lita på molnet

Vilket moln?



Att använda molnet

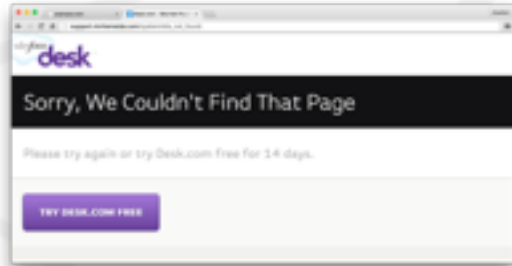


Att använda molnet



Att använda molnet

SUPPORT



Respons leverantörer

Heroku:

"We're aware of this issue"

Shopify:

"I had already identified that this is a security issue"

GitHub:

*"My apologies for the delayed response.
We are aware of this issue"*

Respons kunder #TACKTACKTACK!



Twitter rewarded [fransrosen](#) with a \$1,680 bounty.

Thanks again for helping us keep Twitter safe and secure for our users!



[\[redacted\]](#) rewarded [fransrosen](#) with a \$10,000 bounty.

Thanks for the report Frans.



Riot Games rewarded [fransrosen](#) with a \$7,500 bounty.

GG, thanks for your help resolving this issue! We greatly appreciate your time



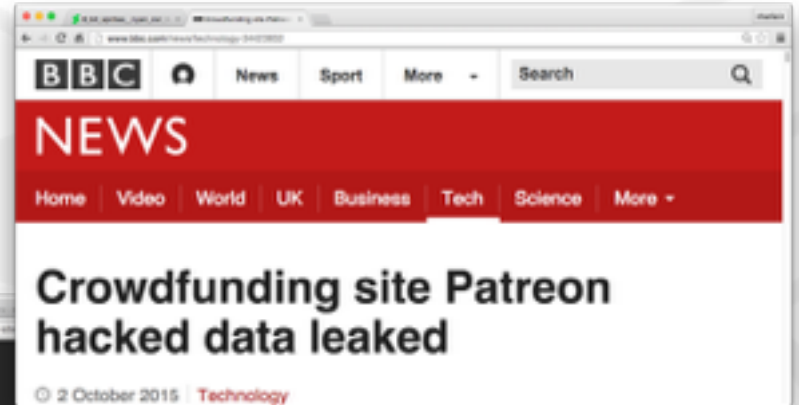
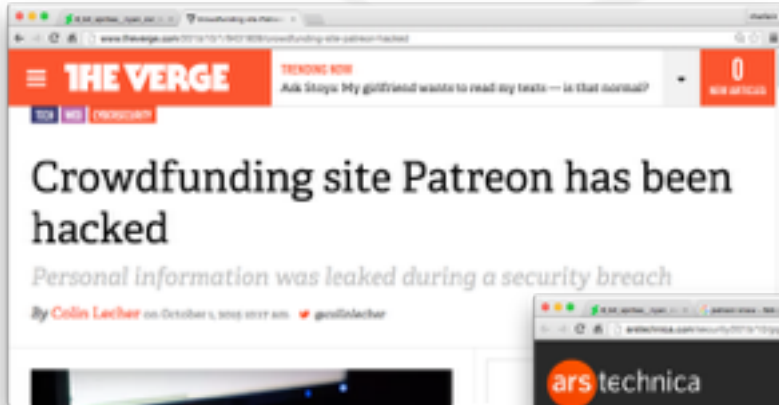
LinkedIn rewarded [fransrosen](#) with a \$1,000 bounty.

Vanliga attackmetoder



1. Riktade.
2. Bombmatta.
3. Teknisk.

Tekniskt riktad



Tekniskt riktad



detectify



detectify labs™

How Patreon got hacked - Publicly exposed Werkzeug Debugger

TL;DR, Patreon got hacked. We reported a specific Remote Code Execution to them due to a public debugger before they were breached. We believe this was the attack method due to the simplicity and availability of the

Interna system i molnet

 [partners.zidane.dev.website.com](#)

 [partners.milo14.dev.website.com](#)

 [udeploy.deyan.dev.website.com](#)

 [vault.deyan.dev.website.com](#)

 [eastwood.pkeene-reclutacion.dev.website.com](#)

 [partners.milo18.dev.website.com](#)

Tänk på att #wearsunscreen

- 1. Minsta motståndets väg.**
- 2. Black hats – Alltid snabbast.**
- 3. Imorgon är en ny dag.**



Go hack yourself!
Frågor?

Frans Rosén (@fransrosen) – www.detectify.com