IDOR was leading to Privilege Escalation and violating the Facebook policy

Armaan Pathan Follow

Aug 11, 2017 · 4 min read

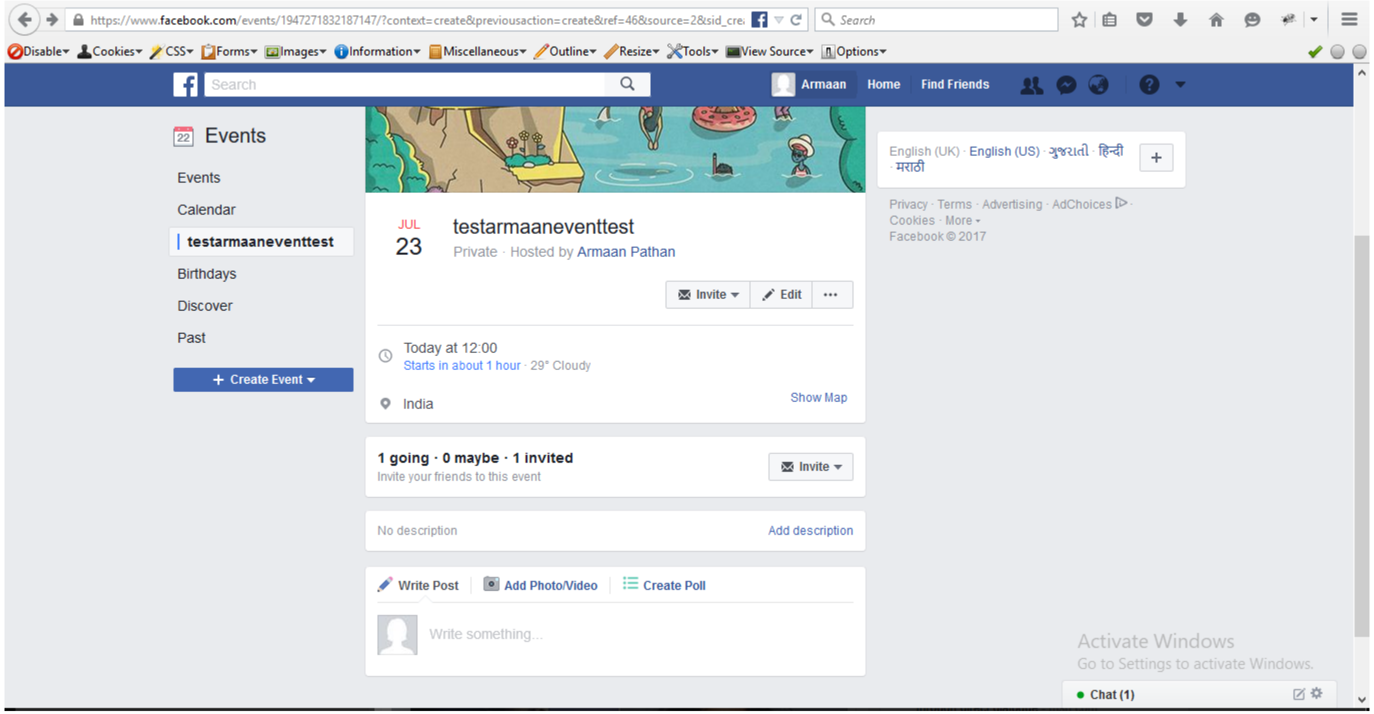
so yes it all started when my friend taunted me that. “why you always be so much into FACEBOOK and why you waste your time by using social networking apps? ” i was like man i think he is right need to prove him wrong !

so i directly went to my home and checked phwd’blogs.

i was like okay, i let me select my target.
started checking with all functionality of facebook like groups,pages.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

When i was looking in to events,
i have found that i can create a private event over here. so i made a private event.



https://www.facebook.com/events/1947271832187147/?context=create&previousaction=create&ref=46&source=2&sid_cre

testarmaaneventtest

JUL 23

Private · Hosted by Armaan Pathan

Today at 12:00
Starts in about 1 hour · 29° Cloudy

India

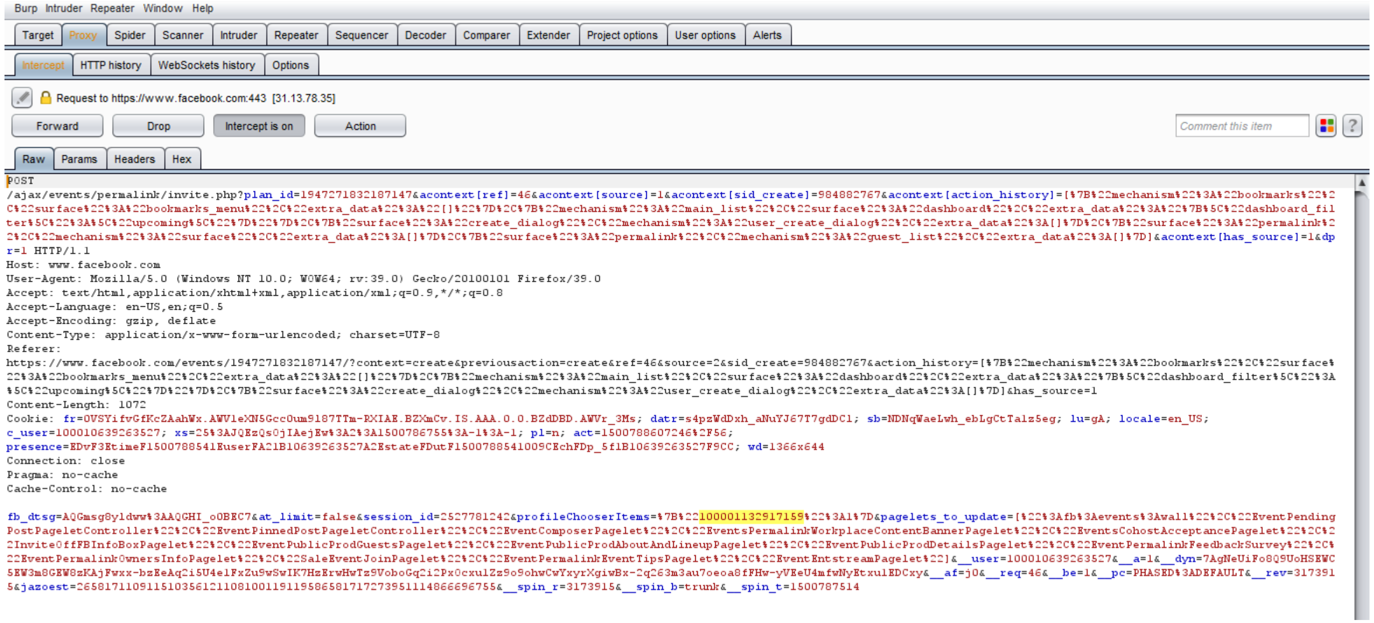
1 going · 0 maybe · 1 invited
Invite your friends to this event

No description

Disable▾ Cookies▾ CSS▾ Forms▾ Images▾ Information▾ Miscellaneous▾ Outline▾ Resize▾ Tools▾ View Source▾ Options▾
Search
Armaan
Home
Find Friends
Events
Events
Calendar
testarmaaneventtest
Birthdays
Discover
Past
+ Create Event ▾
Invite ▾
Edit
Show Map
Invite ▾
Add description
Write Post
Add Photo/Video
Create Poll
Write something...
English (UK) · English (US) · ગુજરાતી · हिन्दी · मराठी
Privacy · Terms · Advertising · AdChoices · Cookies · More ▾
Facebook © 2017
Activate Windows
Go to Settings to activate Windows.
Chat (1)

after making a private event i have started invited people in my event. now while i was inviting friends into my event i was also capturing the request in burp suite.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

Request to https://www.facebook.com:443 [31.13.78.35]

```
POST
/ajax/events/permalink/invite.php?plan_id=1947271832187147&acontext[ref]=46&acontext[source]=1&acontext[sid_create]=984882767&acontext[action_history]=[%7B%22mechanism%22%3A%22bookmarks%22%2
C%22surface%22%3A%22bookmarks_menu%22%2C%22extra_data%22%3A%22[]%22%7D%2C%7B%22mechanism%22%3A%22main_list%22%2C%22surface%22%3A%22dashboard%22%2C%22extra_data%22%3A%22%7B%5C%22dashboard_fil
ter%5C%22%3A%5C%22upcoming%5C%22%7D%22%7D%2C%7B%22surface%22%3A%22create_dialog%22%2C%22mechanism%22%3A%22user_create_dialog%22%2C%22extra_data%22%3A[]%7D%2C%7B%22surface%22%3A%22permalink%2
2%2C%22mechanism%22%3A%22surface%22%2C%22extra_data%22%3A[]%7D%2C%7B%22surface%22%3A%22permalink%22%2C%22mechanism%22%3A%22guest_list%22%2C%22extra_data%22%3A[]%7D]&acontext[has_source]=1&dp
r=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer:
https://www.facebook.com/events/1947271832187147/?context=create&previousaction=create&ref=46&source=2&sid_create=984882767&action_history=[%7B%22mechanism%22%3A%22bookmarks%22%2C%22surface%
22%3A%22bookmarks_menu%22%2C%22extra_data%22%3A%22[]%22%7D%2C%7B%22mechanism%22%3A%22main_list%22%2C%22surface%22%3A%22dashboard%22%2C%22extra_data%22%3A%22%7B%5C%22dashboard_filter%5C%22%3A
%5C%22upcoming%5C%22%7D%22%7D%2C%7B%22surface%22%3A%22create_dialog%22%2C%22mechanism%22%3A%22user_create_dialog%22%2C%22extra_data%22%3A[]%7D]&has_source=1
Content-Length: 1072
Cookie: fr=0VSYifvGfKcZAahWx.AWV1eXN5Gcc0um9187TTm-RXIAE.BZXmCv.IS.AAA.0.0.BZdDBD.AWVr_3Ms; datr=s4pzWdDxh_aNuYJ67T7gdDC1; sb=NDNqWaeLwh_ebLgCtTalz5eg; lu=gA; locale=en_US;
c_user=100010639263527; xs=25%3AJQEzQs0jIAejEw%3A2%3A1500786755%3A-1%3A-1; pl=n; act=1500788607246%2F56;
presence=EDvF3EtimeF1500788541EuserFA21B10639263527A2EstateFDutF1500788541009CEchFDp_5f1B10639263527F9CC; wd=1366x644
Connection: close
Pragma: no-cache
Cache-Control: no-cache

fb_dtsg=AQGmsg8yldww%3AAQGHI_o0BEC7&at_limit=false&session_id=2527781242&profileChooserItems=%7B%22100001132917159%22%3A1%7D&pagelets_to_update=[%22%3Afb%3Aevents%3Awall%22%2C%22EventPending
PostPageletController%22%2C%22EventPinnedPostPageletController%22%2C%22EventComposerPagelet%22%2C%22EventsPermalinkWorkplaceContentBannerPagelet%22%2C%22EventsCohostAcceptancePagelet%22%2C%2
2InviteOffFBInfoBoxPagelet%22%2C%22EventPublicProdGuestsPagelet%22%2C%22EventPublicProdAboutAndLineupPagelet%22%2C%22EventPublicProdDetailsPagelet%22%2C%22EventPermalinkFeedbackSurvey%22%2C%
22EventPermalinkOwnersInfoPagelet%22%2C%22SaleEventJoinPagelet%22%2C%22EventPermalinkEventTipsPagelet%22%2C%22EventEntstreamPagelet%22]&__user=100010639263527&__a=1&__dyn=7AgNeUiFo8Q9UoHSEWC
5EW3m8GEW8zKAjFwxx-bzEeAq2i5U4e1FxZu9wSwIK7HzErwHwTz9VoboGq2i2Px0cxu1Zz9o9ohwCwYxyrXgiwBx-2q263m3au7oeoa8fFHw-yVEeU4mfwNyEtxulEDCxy&__af=j0&__req=46&__be=1&__pc=PHASED%3ADEFAULT&__rev=317391
5&jazoest=265817110911510356121108100119119586581717273951114866696755&__spin_r=3173915&__spin_b=trunk&__spin_t=1500787514
```

* now as you will notice the highlighted part in the request. it is a user id of my account as i was inviting my self only. **
here i have deiced to fuzz this parameter “profilechooseritems” with different values.

If you have noticed that whenever you create a facebook account the facebook will provide you the UNIQUE **username** and also it also gives userid.
so as per the facebook’s policy you can only invite facebook users in your

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

private event who are into your facebook account.
so i had tried to put my friend @hackerspider1 into my event who was not added into my current testing facebook account’s friendlist and i was able to add/invite him into my event. i was like yeah!! :D i think i have found something. so i had also one more facebook testing account, which is also not added into my current facebook account’s friendlist.i had tried to invite that facebook user too.

and whatt ! i was able to invite that account too. !!

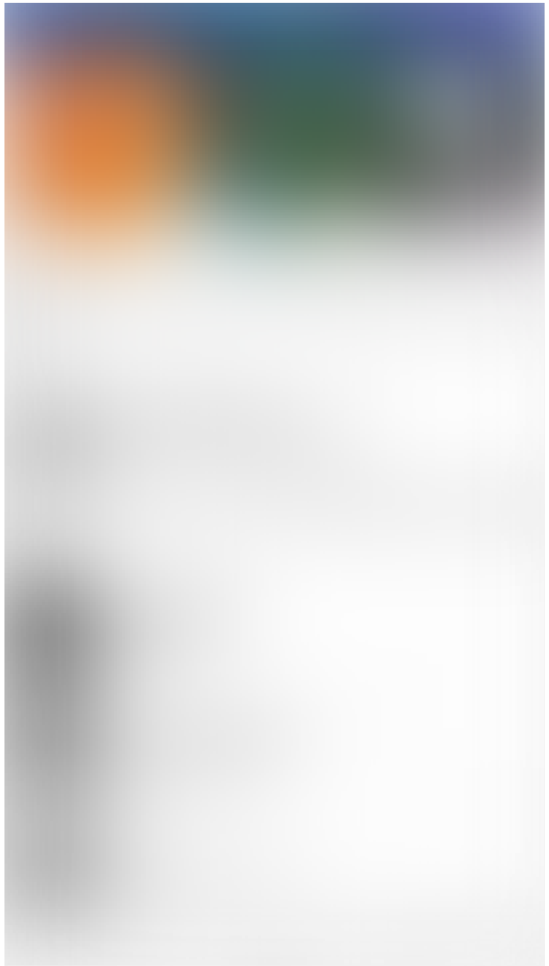
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

but i wanted to exploit it more! without wasting my time i also added @jaypatel9717 into my private event.(now jay patel is also not added into my this testing account's friendlist.)
i was scrolling my facebook's news feed and also was thinking that how can i exploit it more? at that time i saw one of my friend's post "******** is going to DHINCHAK POOJA's Live Event".
so i started exploring more that if i m able to post behalf of jay patel like "jay

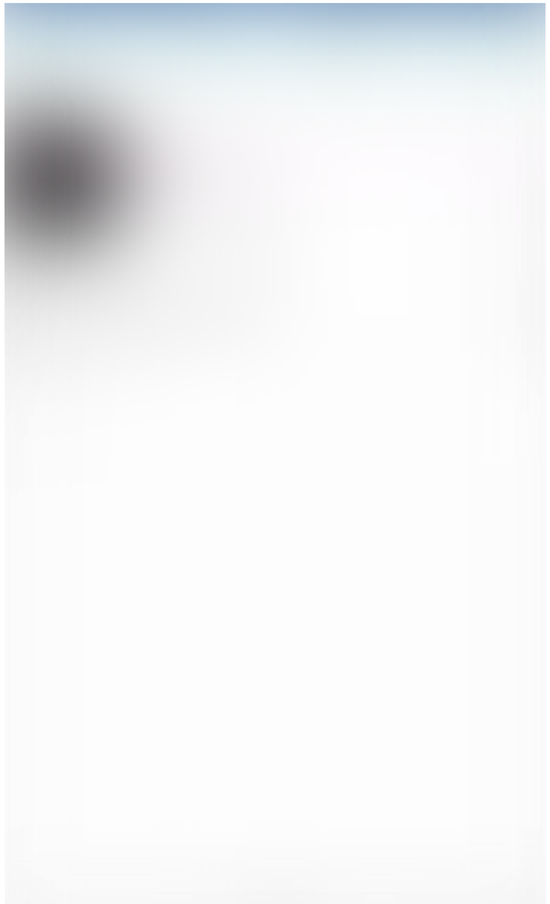
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

patel is going to this event or not”

and what!! i was able to post that jay patel in going to this event. !

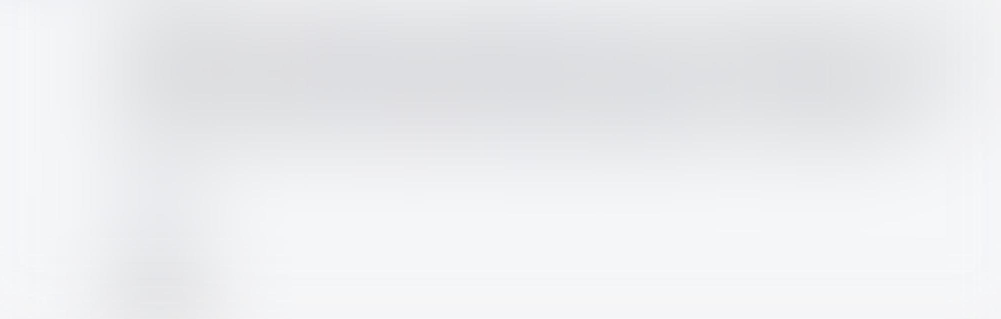


Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

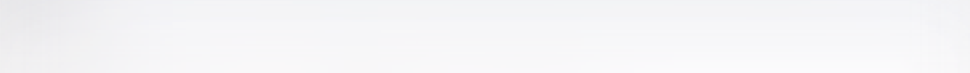


without wasting any time ! i made a PoC of this and reported to facebook. and the next day moring…. i got a reply :/

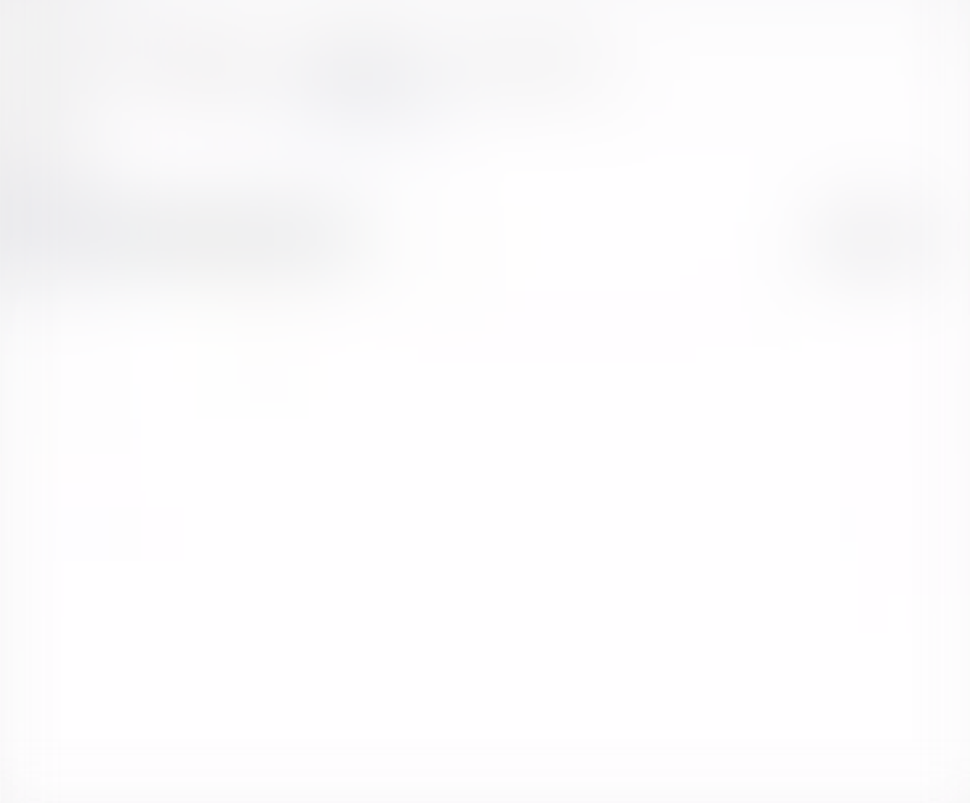
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



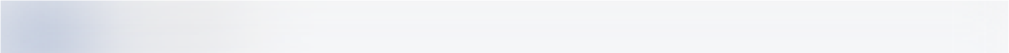
so as per the facebook’s policy if someone is added into your facebook’s friendlist and you are adding other facebook users who are not added into your account but they are into the person’s friend list who is added into your facebook’s friend list and if you add them somehow then its a normal behavior. :/// i was like aghhhh !!!
but i dint give up ! quickly made a new facebook account. now i just made an account so there is no one added in my friend list. :3
now i went back to my testing account and tried to add this fresh made facebook account .
and ! yeah ! i was able to add that account too into my private event & make a same post also like (testarmaanpathantest armaan is going to soo and so event).



Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



again i made a quick PoC and reported to facebook.
after 5–6 days ! i got a reply from facebook that they have patched the issue and please conform that is not reproducible anymore.
After conforming
they Rewarded me with a good amount.



Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

spacial thanks to @jaypatel9717

and yeah ! also learnt that if any friend is taunting you. take it as a challange and prove him/her wrong.

Thanks for reading.

have a great day ahead.

Social Media

227 claps

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

WRITTEN BY

Armaan Pathan

Follow

See responses (3)

More From Medium

Related reads

Diving into unserialize(): Magic Methods

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

110

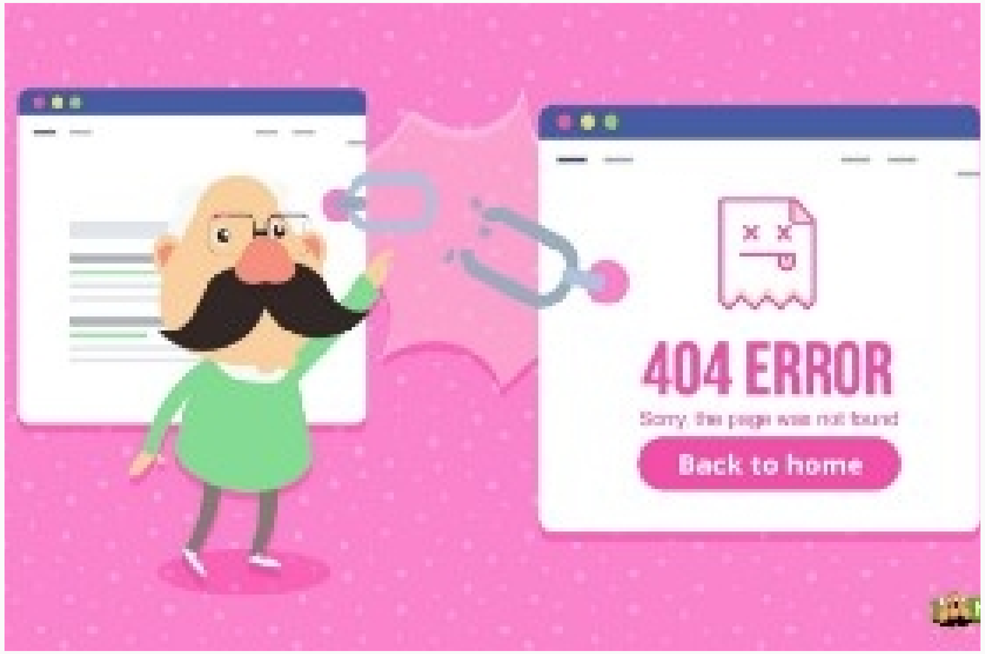
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Related reads

Everything You Need to Know About the 404 Page

HostPapa
May 13 · 8 min read ★

12

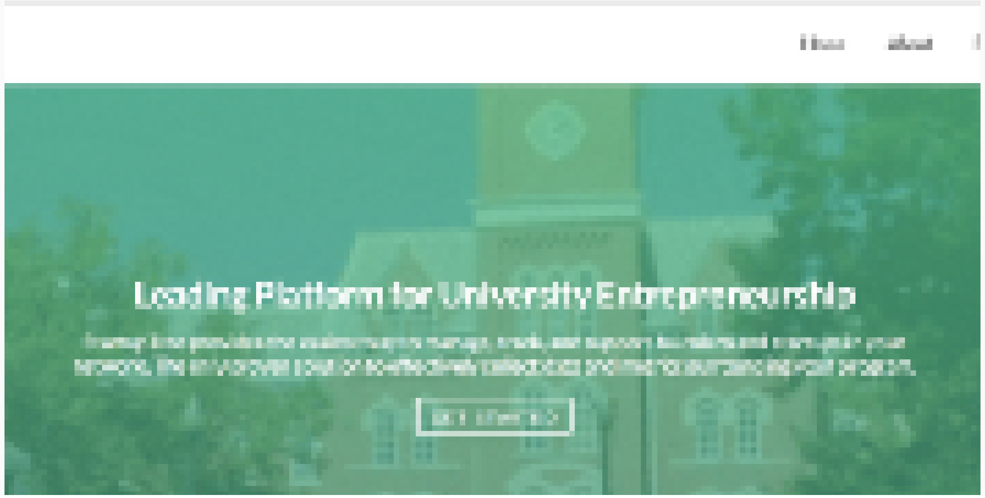


Related reads

Open Redirects & Security Done Right!

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

490



Leading Platform for University Entrepreneurship

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Discover Medium

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

Make Medium yours

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

Become a member

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

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD