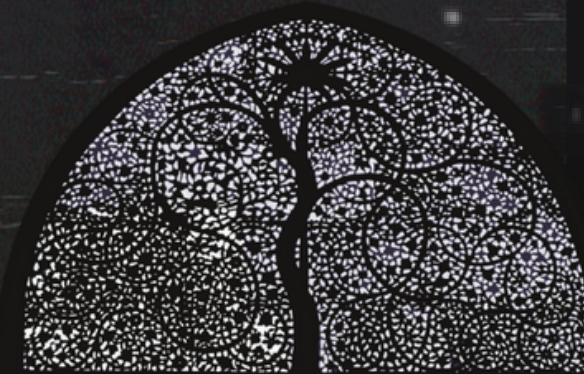


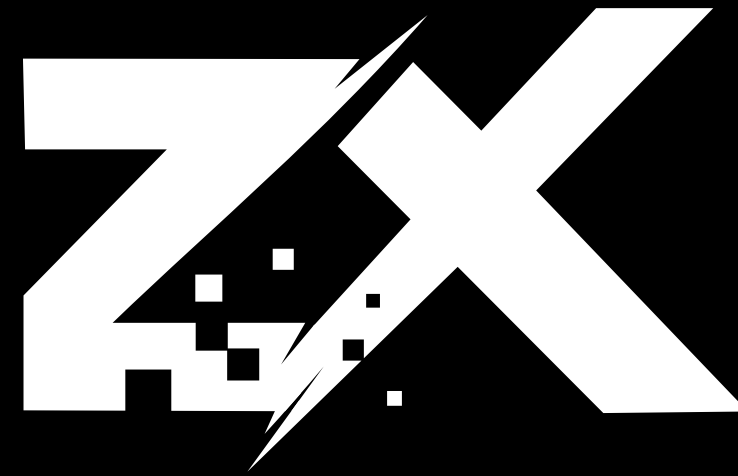
Masquerading malicious campaign through unintended IDOR



AHMEDABAD

BOSIDES

whoami - office hours



SECURITY



Ahmad Ashraff bin Ahmad

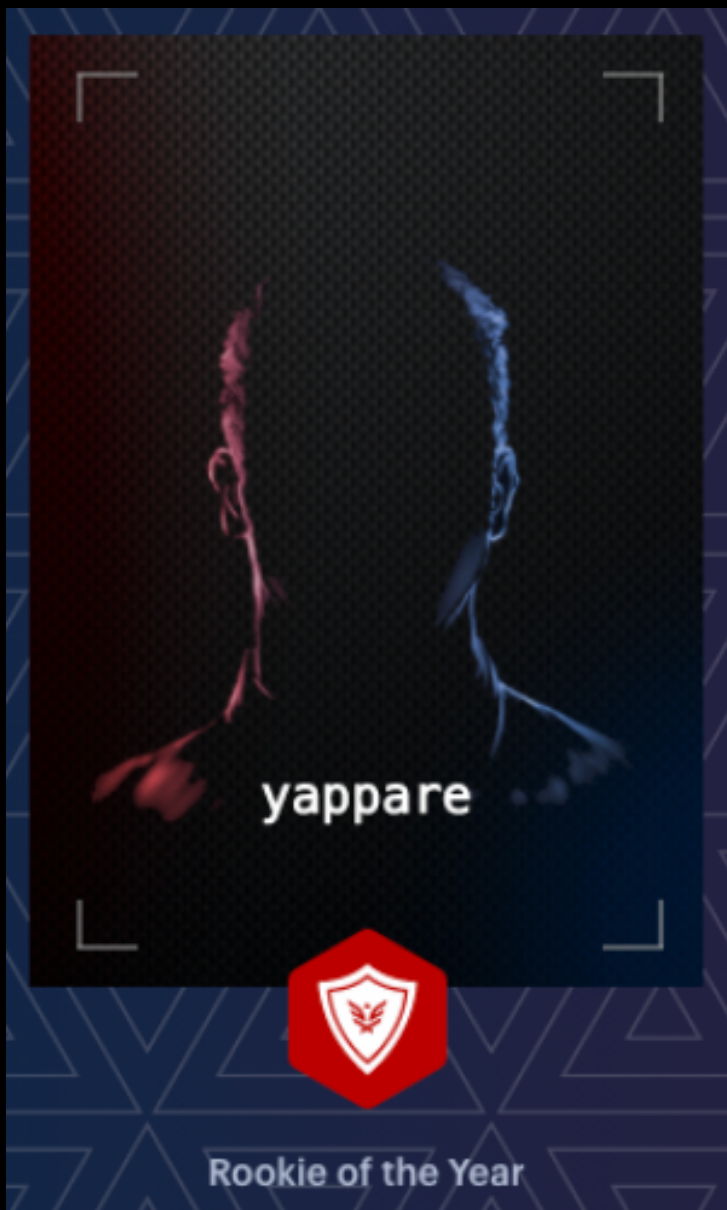
Building Malaysia's ethical hacking community of the future

Sungai Petani, Kedah, Malaysia · [Contact info](#)



ZX Security Ltd

whoami - bugbounty



Google

Bug Hunte



yappare

@yappare

3rd place in [#beta022](#) @bugcrowd !
result notification got something new
[#Bugbounty](#)

11:25 PM · Aug 24, 2013 · Twitter Web Client



180

Ahmad Ashraff

Approach

- manual
- easy vulnerability against complex targets
- complex vulnerability against targets
- sleep

Insecure Direct Object Reference

IDOR

Insecure Direct Object Reference (called IDOR from here) occurs when a application exposes a reference to an internal implementation object

Profile A

<https://www.target.com/profile.php?id=1>



Profile B

<https://www.target.com/profile.php?id=99>





id=[value]

- **brute-force**
- **enumerate**

Profile C

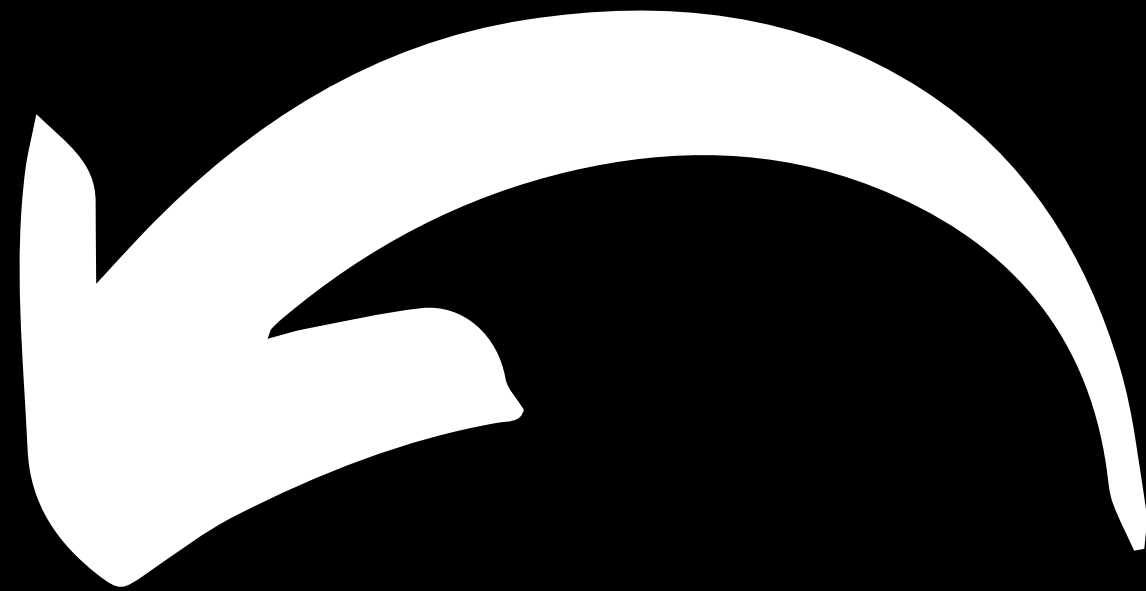
[https://www.target.com/profile.php?
uuid=c869fbe5-a05e-4397-9cea-
d7712ec69cbb](https://www.target.com/profile.php?uuid=c869fbe5-a05e-4397-9cea-d7712ec69cbb)



Profile D

[https://www.target.com/profile.php?
uuid=4cde2bbe-f8b8-434b-8dc6-
8b5fc0b09d73](https://www.target.com/profile.php?uuid=4cde2bbe-f8b8-434b-8dc6-8b5fc0b09d73)

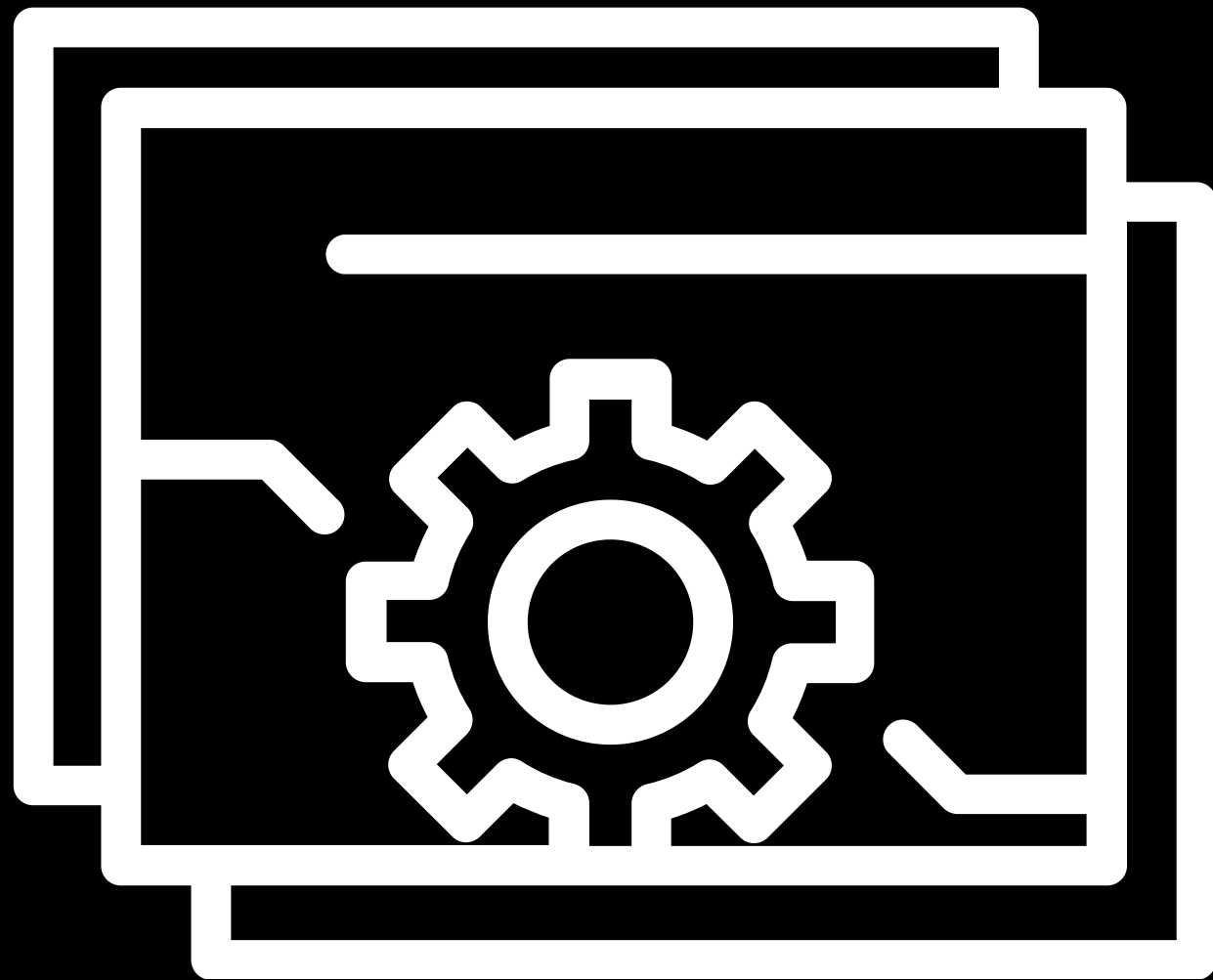




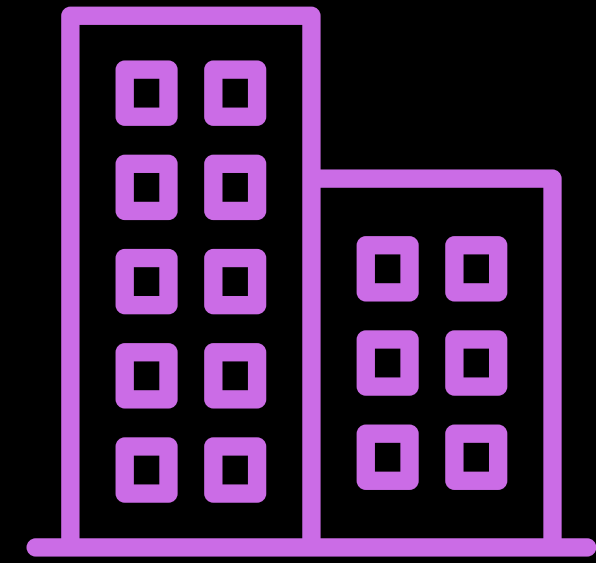
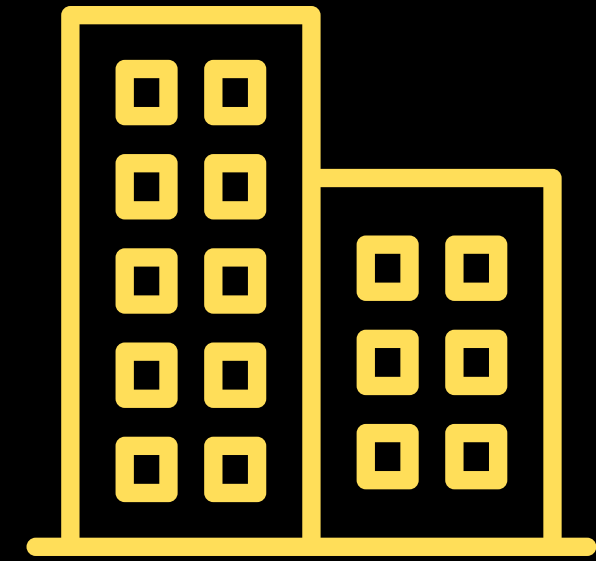
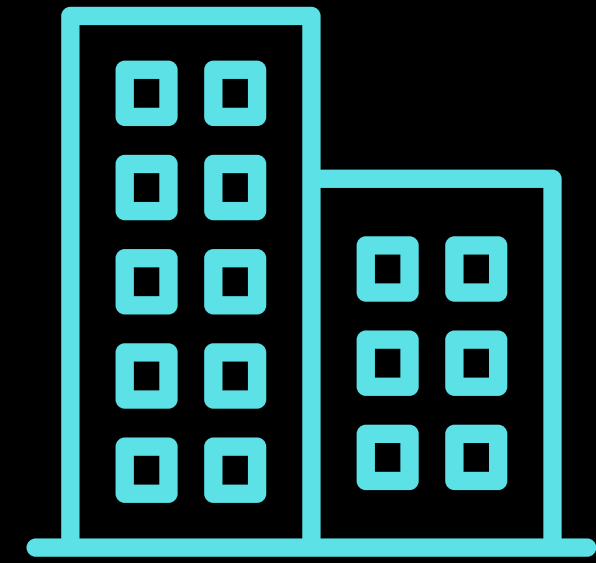
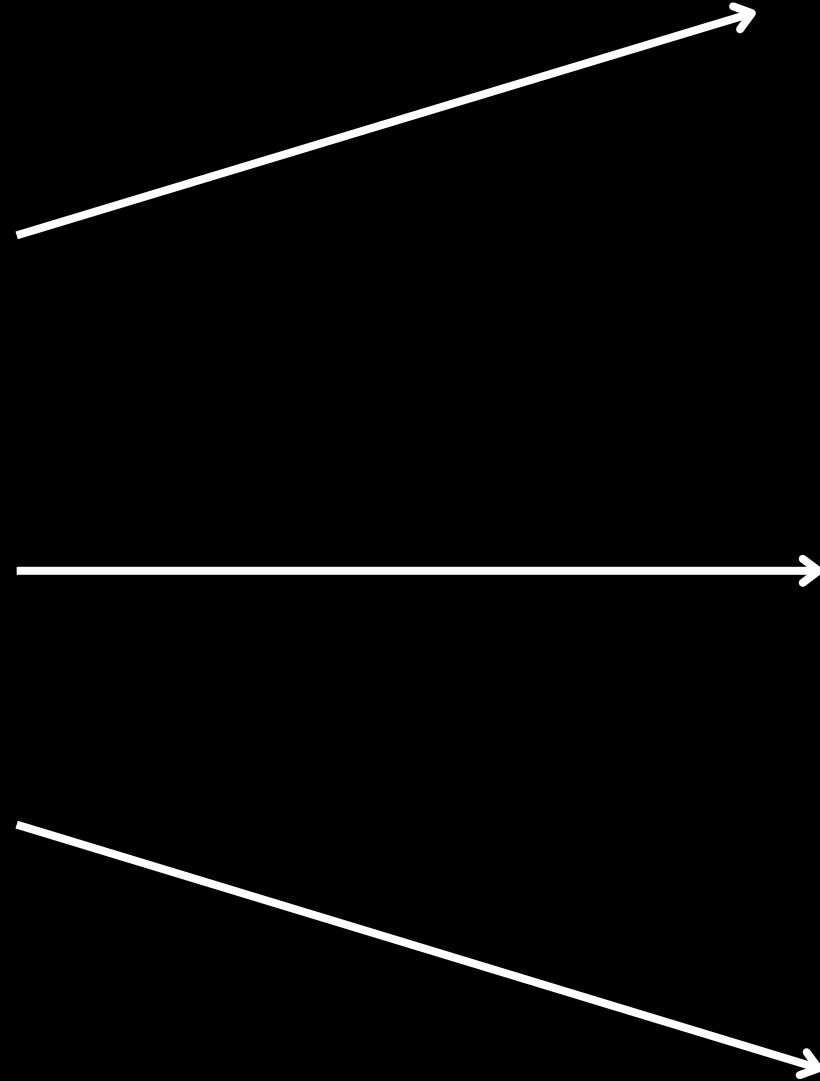
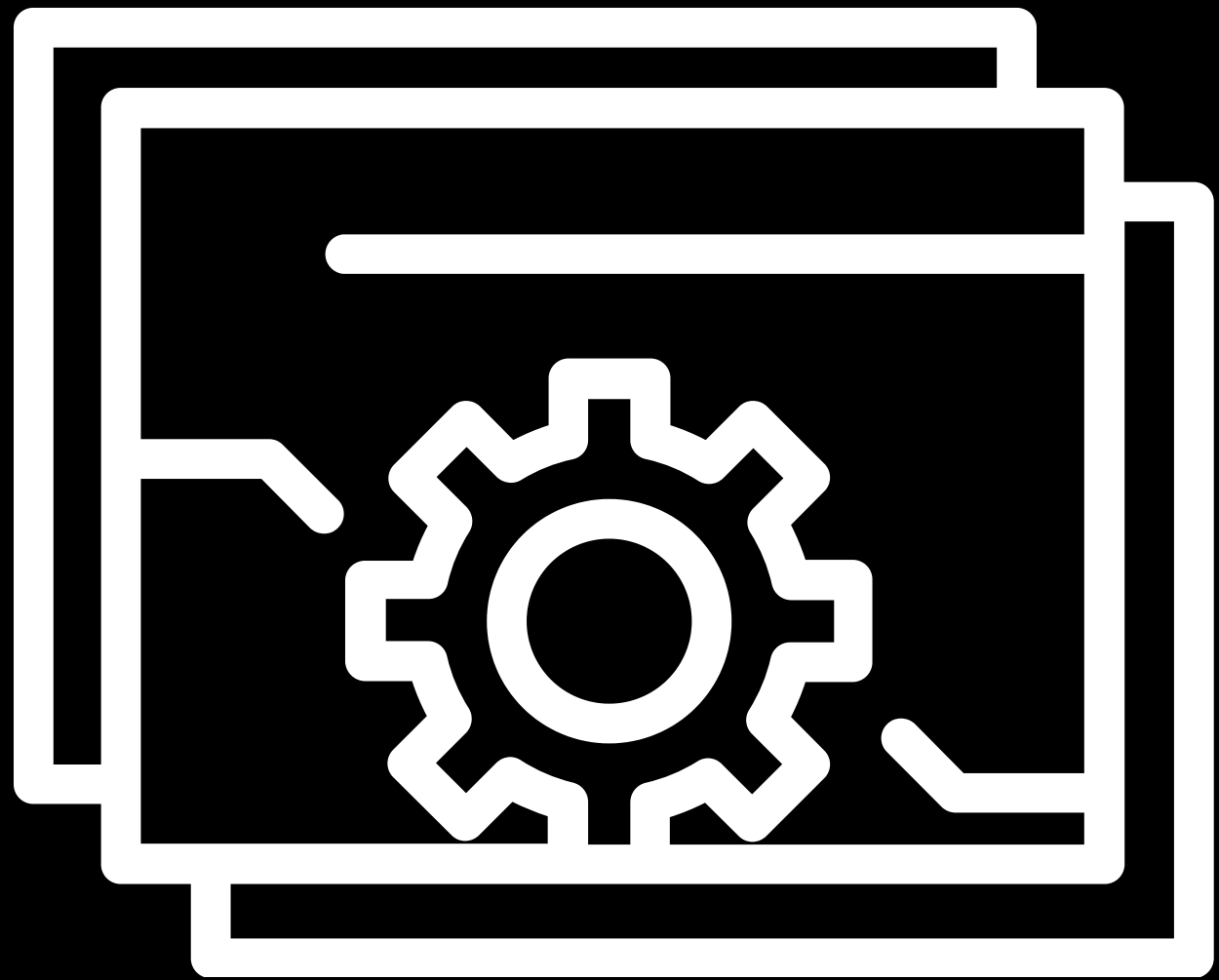
uuid=[value]

- **leaked in the application**
- **waybackmachine**
- **search engines**

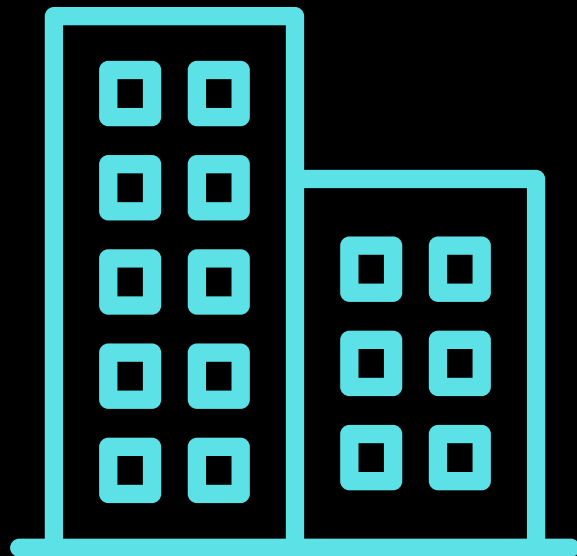
Marketing software/tools



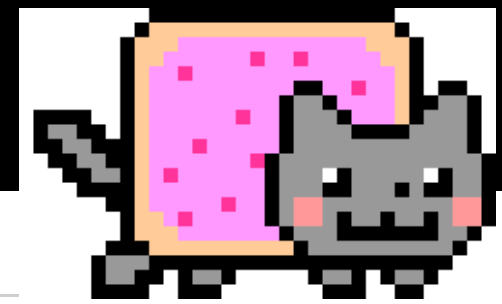
- shared IP
- custom domain
- same URL patterns



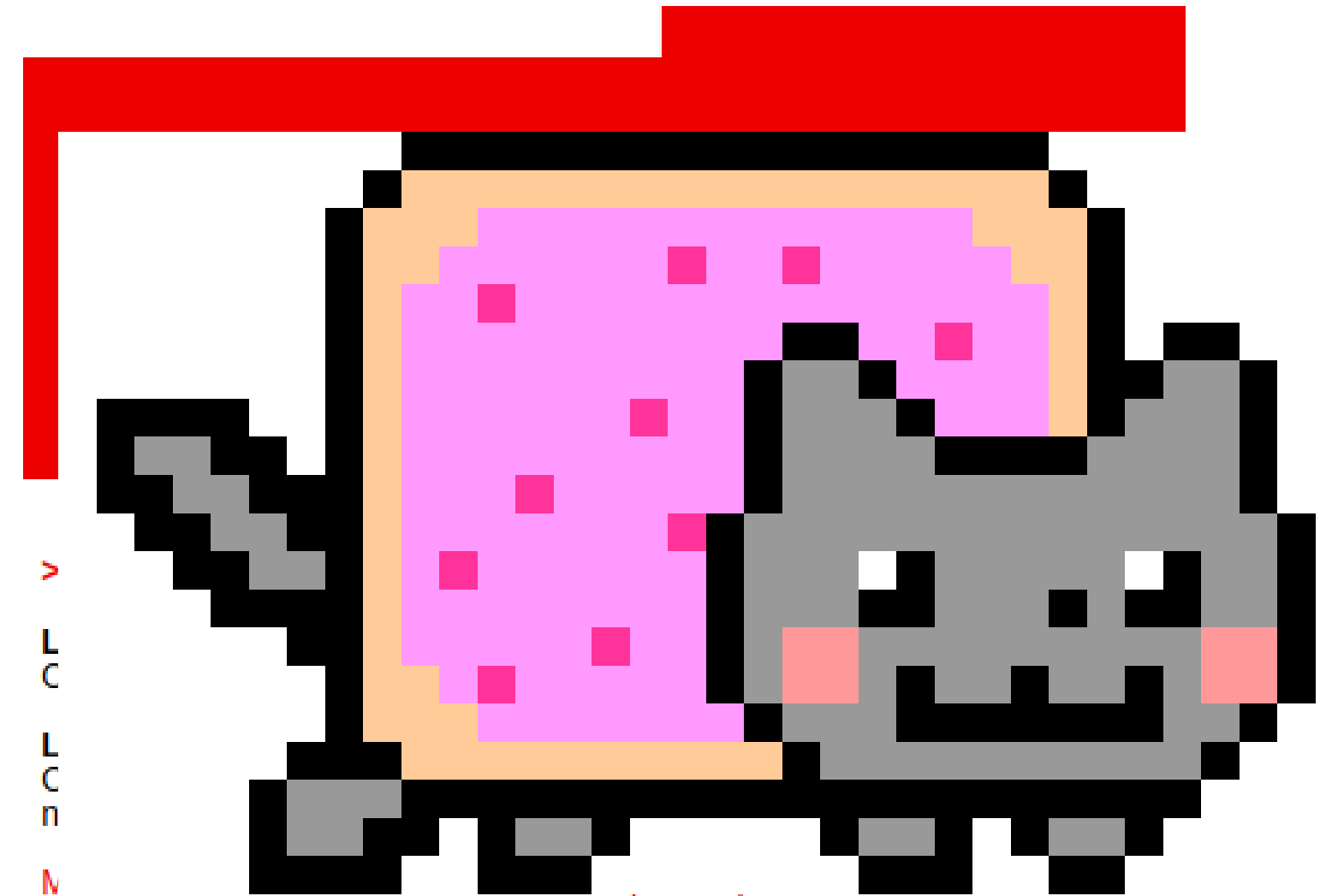
Campaign by company JK



[https://jk.com/yolo/ads.php?
id=WI4MBIcdU1ZaBQpbUw0CBE8m](https://jk.com/yolo/ads.php?id=WI4MBIcdU1ZaBQpbUw0CBE8m)

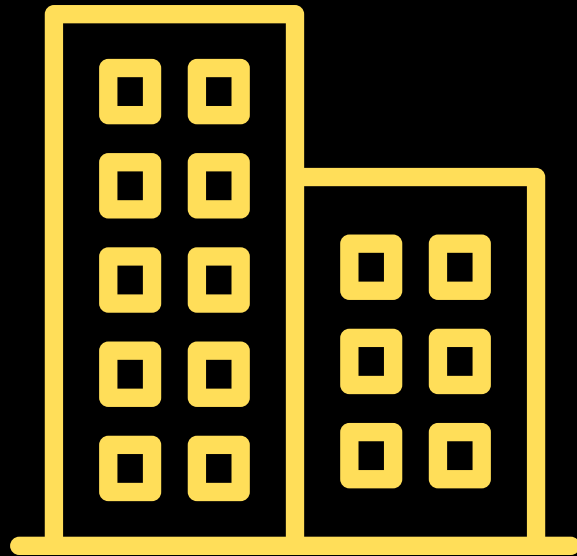


Linha Capitalizar 2018 COVID-19



1.500.000€ por empresa em cada uma das Linhas.

Campaign by company **ABC**



[https://abc.com/yolo/ads.php?
id=UlcDB1dTHINRBAZaUAACAwXmmm](https://abc.com/yolo/ads.php?id=UlcDB1dTHINRBAZaUAACAwXmmm)



Johnnie Side,

O nosso administrador Francisco Barbeira, e Nuno Filipe, Diretor de Recursos Humanos, fazem um ponto de situação consigo, sobre o tema Coronavírus. Veja as declarações.

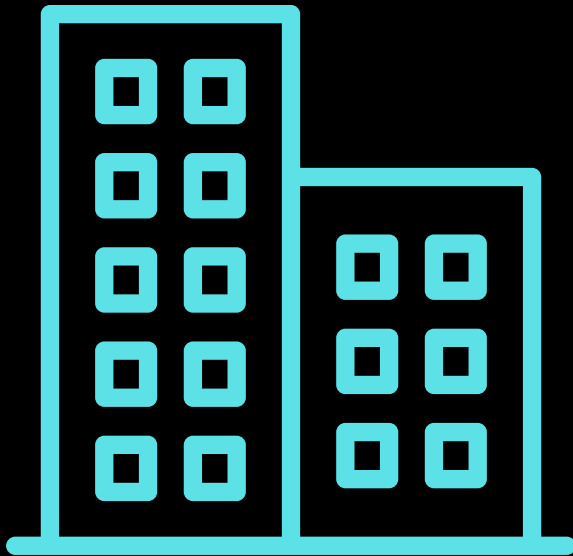
[VER VÍDEO >](#)



Esta favo
A pr
Rua
Os e
pelo
serv
Ace

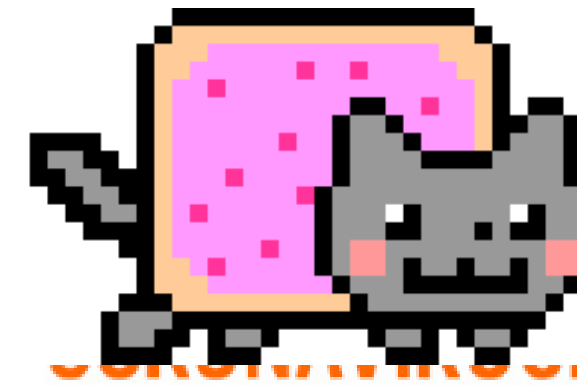
s. Por
m sede na
rmativo,
esso aos
ves de
essoais.

Campaign by company JK



<https://jk.com/yolo/ads.php?>

[id=UlcDB1dTHINRBAZaUAACAwXmmm](https://jk.com/yolo/ads.php?id=UlcDB1dTHINRBAZaUAACAwXmmm)



Johnnie Side,

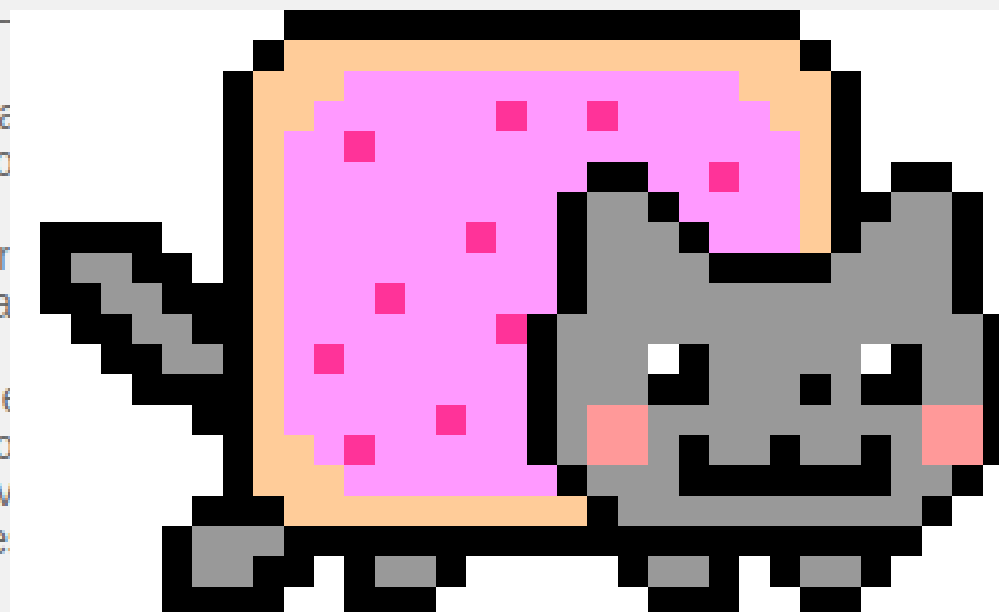
O nosso administrador Francisco Barbeira, e Nuno Filipe, Diretor de Recursos Humanos, fazem um ponto de situação consigo, sobre o tema Coronavírus. Veja as declarações.

[VER VÍDEO >](#)

Esta
favo

A pr
Rua

Os e
pelo
serv
Ace



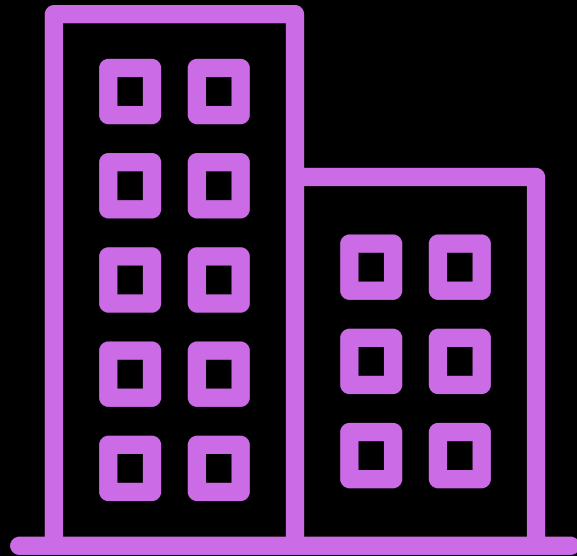
s. Por

m sede na

rmativo,
esso aos
ves de
essoais.



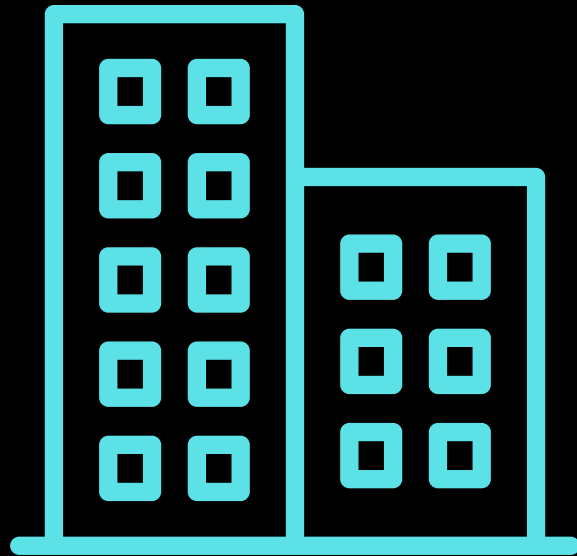
Campaign by company LOL



[https://lol.com/yolo/ads.php?
id=UlcDB1dTHINRBAZaUAACAwmZMQ==](https://lol.com/yolo/ads.php?id=UlcDB1dTHINRBAZaUAACAwmZMQ==)



Campaign by company JK

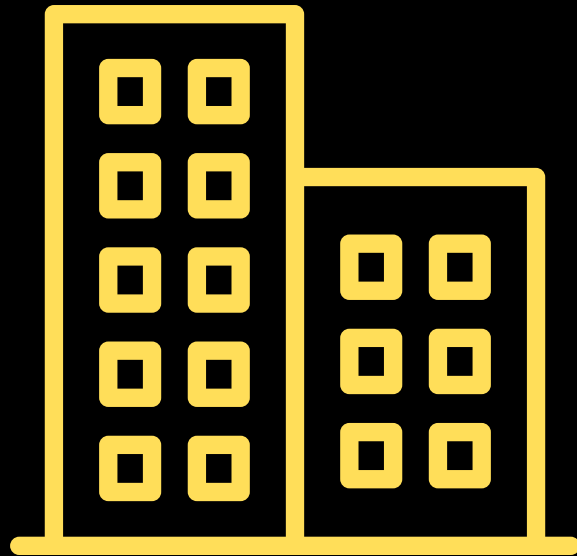


<https://jk.com/yolo/ads.php?>

[id=UlcDB1dTHINRBAZaUAACAwmZMQ==](https://jk.com/yolo/ads.php?id=UlcDB1dTHINRBAZaUAACAwmZMQ==)



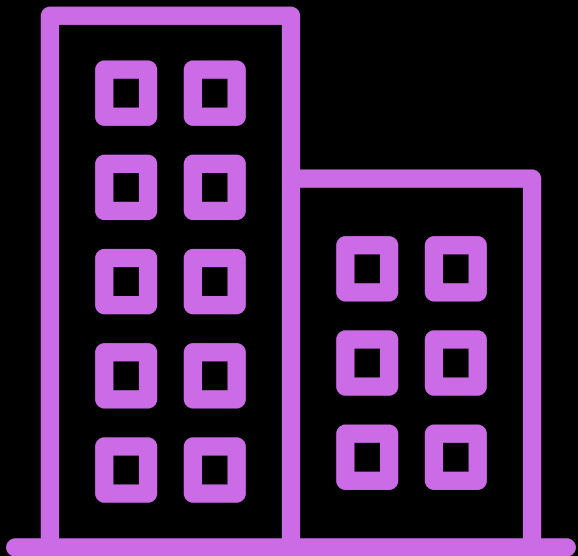
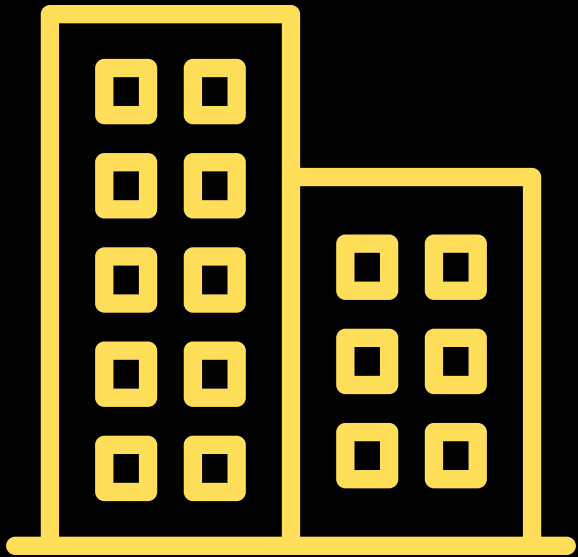
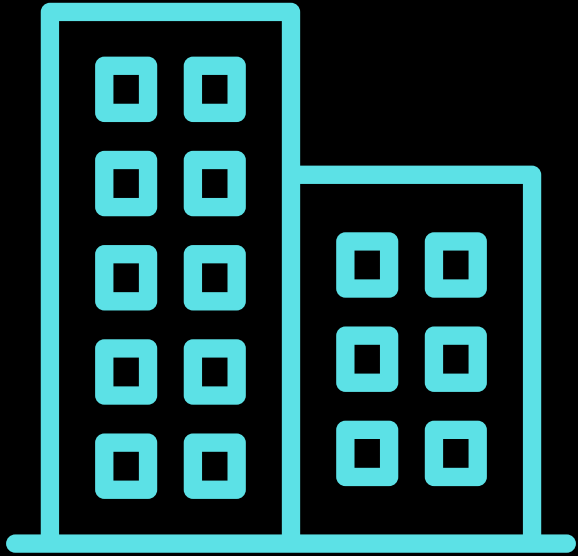
Campaign by company **ABC**



<https://abc.com/yolo/ads.php?>

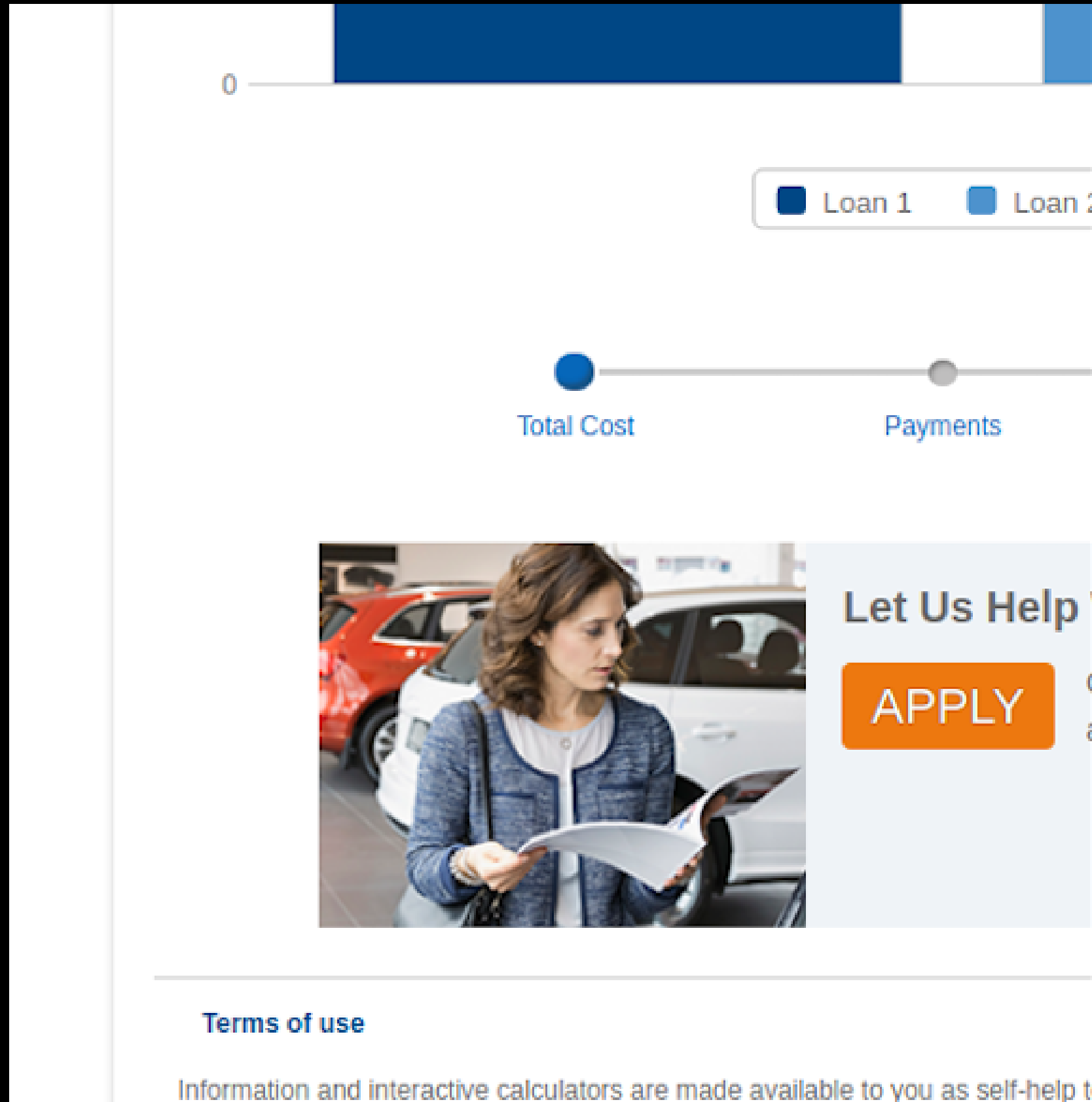
[id=UlcDB1dTHINRBAZaUAACAwmZMQ==](https://abc.com/yolo/ads.php?id=UlcDB1dTHINRBAZaUAACAwmZMQ==)







<https://tools.gg.com/response/jk-ggmufc/calc/auto07>



The screenshot shows a web-based car loan calculator. At the top, there is a legend with two items: "Loan 1" represented by a dark blue square and "Loan 2" represented by a light blue square. Below the legend is a horizontal timeline with two points: "Total Cost" marked with a dark blue dot and "Payments" marked with a grey dot. The "Total Cost" point is currently selected. Below the timeline, there is a promotional banner. On the left side of the banner is a photograph of a woman with brown hair, wearing a blue jacket, looking at a document in a car dealership. On the right side of the banner, the text "Let Us Help" is visible above a prominent orange button with the word "APPLY" in white capital letters. At the bottom of the page, there is a section titled "Terms of use" in blue text, followed by a line of smaller text that reads "Information and interactive calculators are made available to you as self-help t".

<https://tools.gg.com/response/jk-ggmufc/calc/auto01/tool.abc>

- extension is unique - .abc
- has "tool", "calc", "tools", "calculators"
- **jk** = the software/tool name
- **ggmufc** = organisation's name
- **auto01** = the option used/enabled



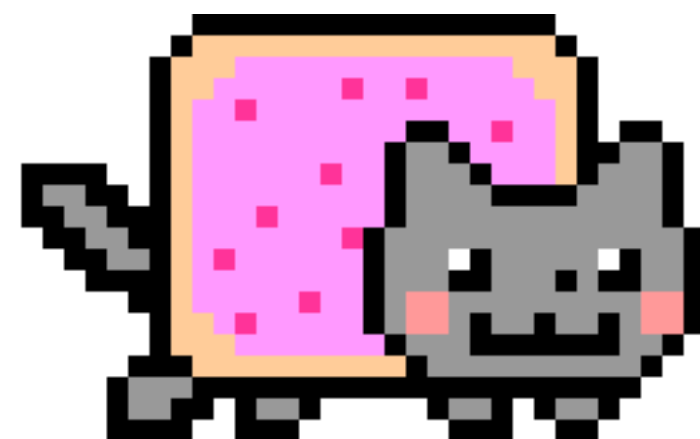
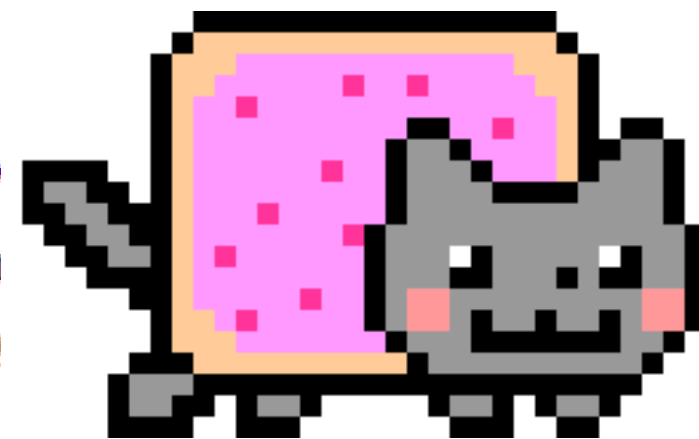
s)

.com > budget04 > tool ▾

invest in savings? - N

not appropriate for decision

investment loans. it is intended for computing decisions re



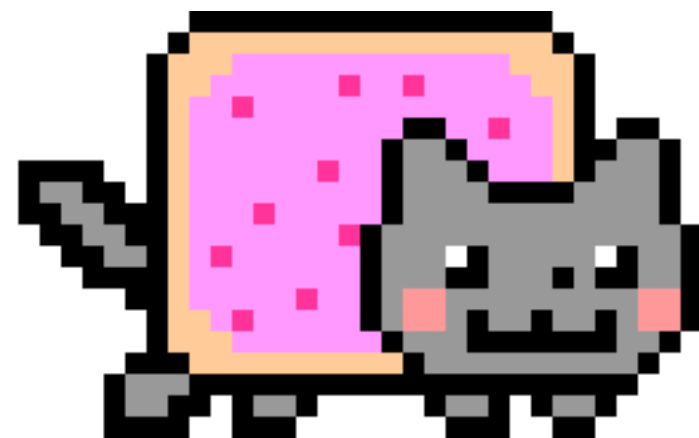
.com > lifeins01 > tool

do I need? - No

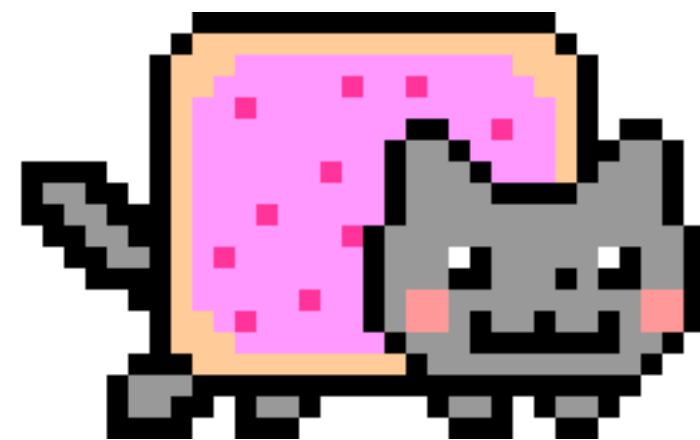
ation and taxes; Avail

) are treated as a sou

).



ity,

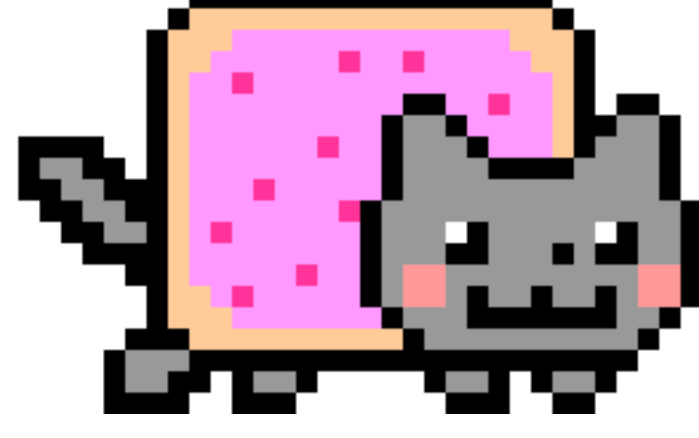


> home02 > tool ▾

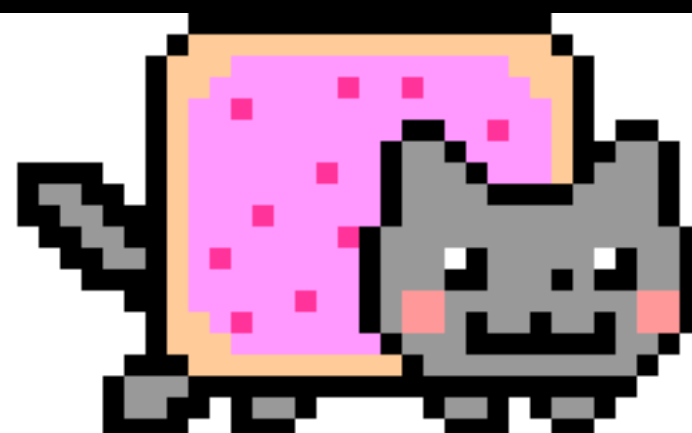
page payments t

payments be? Loan am

property tax. \$. Yearl



m

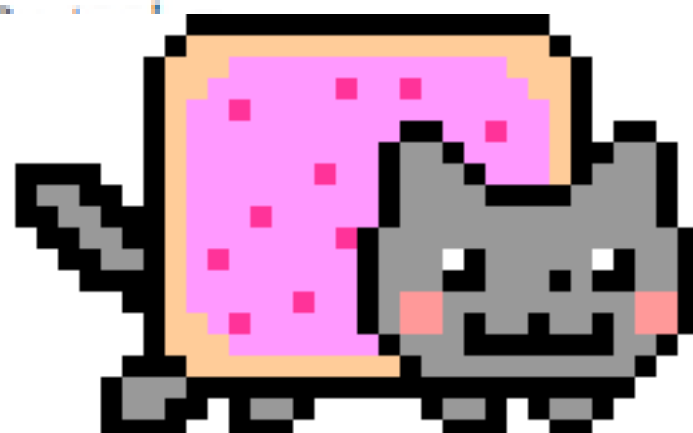


com > home11 > home11

financing costs be? -

g Costs chart. Adjusted O

percent. Other Sewerment Charges, 3,246 dolla



ollars. 48

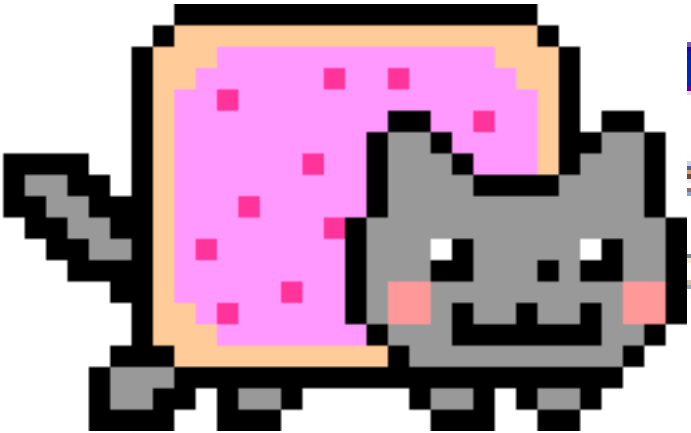


> ha > home11 > tool

ancing? - BMO

\$114 per month and

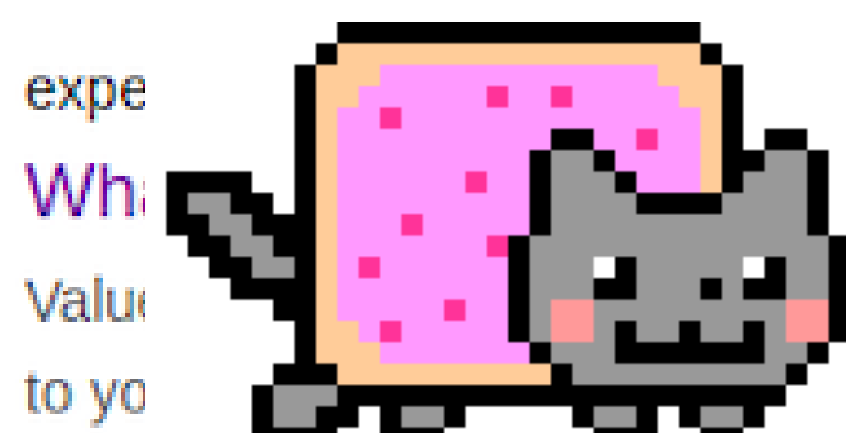
interest payment, \$6



tor

est. Current

d ...



expe

Whi

Valu

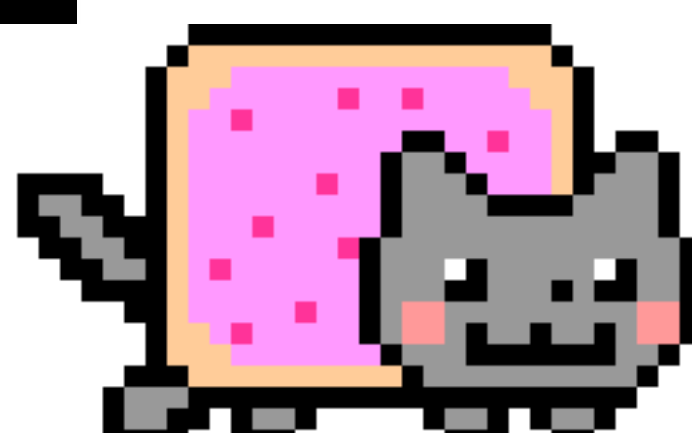
to yo

ssive > auto11 > tool

? - Pro

rebate*. \$. * only include amounts that you wish to add

dfusion.com.



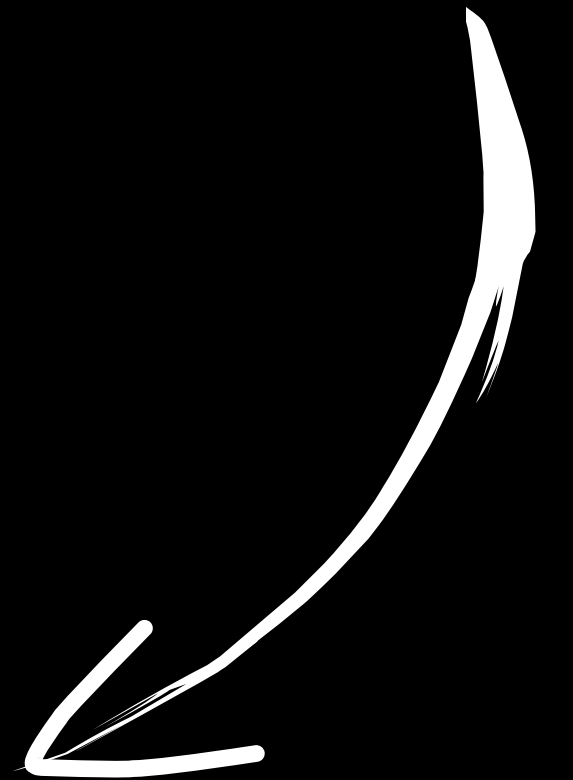
m > pr > auto02 > tool

d depreciation cost me? - Pro

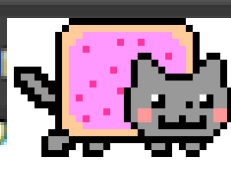


<https://tools.gg.com/response/jk-ggmufc/calc/auto01/tool.abc>

<https://tools.gg.com/tools/jk-farmfamily/savings01/tool.abc>



```
700 <!-- END OF SmartSource Data Collector -->
701
702 <script type="text/javascript" defer="defer" src="//ipinvite.com/percepti
703
704
705
706 </div>
707
708 <!-- Align Wrapper -->
709 </div>
710 </div>
711
712
713
714
715 <!-- Javascript -->
716 <script src="//learningcenter.com/js/jquery.rz.cookie.js" ty
717
718 <script src="//learningcenter.com/js/jquery.rz.inputhint.js"
719
720 <script src="//learningcenter.com/js/jquery.rz.searchbox.js"
721
722 <script src="//learningcenter.com/js/jquery.rz.getRateQuote
723
724 <script src="//learningcenter.com/js/jquery.rz.tabify.js" ty
725
726 <script src="//learningcenter.com/js/jquery.rz.carousel.js"
727
728 <script src="//learningcenter.com/js/init.js" type="text/jav
729
730 <script>
731
732 $(document).ready(function(){
733
734 learningcenter.article_init();
735
736 });
737
738 </script>
```



different organisation


https://tools.gg.com




Javascript files loaded from other domain




So? What a LOL staff can do?

- subscribe to the same tool/software
- upload own malicious Javascript
- load LOL content on other domains that using the same tool/software

Calculators | 

Calculators   tools/statefarm/savings01/too 

Insurance Finances Claims

[Home](#) [Learning Center](#) Financial Calculators 

Learning Center

- Auto
- Family
- Finances
- Insurance
- Residence
- Safety
- Videos


Connect With Us

About Us

What will it take to become a millionaire

Inputs Results Help

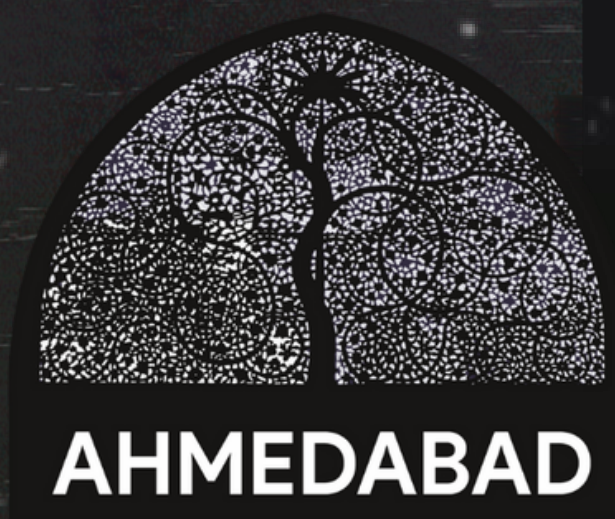
Current age
Desired age to be a millionaire
Amount you have invested
Amount you can save monthly
Your savings rate
Your federal tax rate
Your state tax rate
Inflation rate

tools.nyan  org

OK

6.80 %
1.00 %

Get My Results



BOSIDES

Thank you