

Google Give Me Vulnz



SECURITY
ABOVE ALL ELSE

Intro

- Cameron Vincent – Vulnerabilities and Mitigations team within MSRC (Microsoft Security Response Center)
- Former Full Time Bug Bounty Hunter
- Ranked #1 Researcher for Google VRP Program in 2019

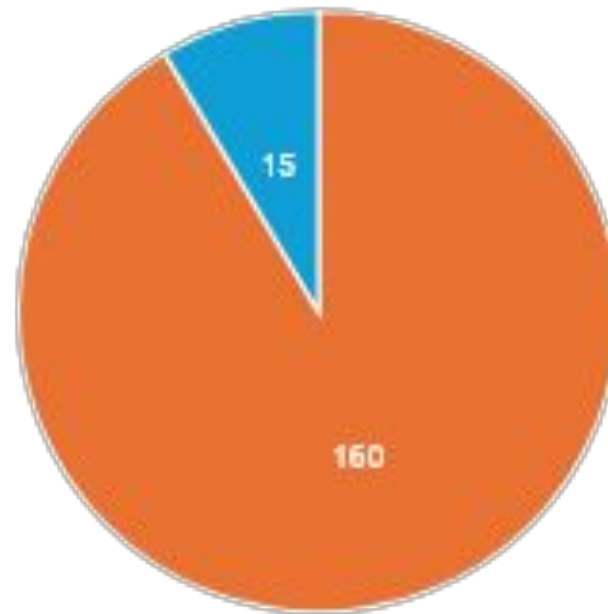
What was the vulnerability
type I was finding?

IDOR = Insecure Direct Object Reference

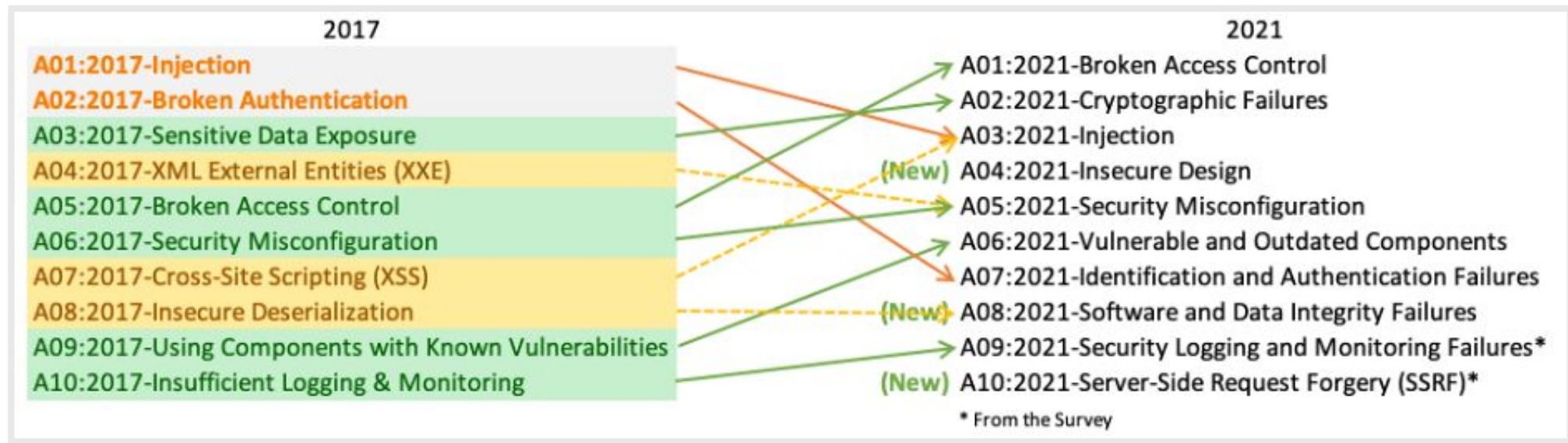
- <https://secretdocuments.com/id=12345>
- <https://secretdocuments.com/id=123456789>
- Put a different ID and see if you can access data you are not allowed to access.

IDOR = Most Common Bug I Found Across Google

Total IDOR Findings (Across all Google Products)



IDOR Other



What is Burp Suite?

Burp Suite = Golden Tool

Web application security testing tool.

Burp Suite lets you see and manipulate browser traffic being sent to the backend of a service.

Repeater tab is going to be your best friend.

Burp Suite = Golden Tool



Imagine sending
an email on
Outlook.

A diagram consisting of two dark teal circles connected by a light gray triangle pointing from left to right. The left circle contains the text 'Imagine sending an email on Outlook.' and the right circle contains the text 'Browser makes it look all pretty but Burp Suite shows you what's going on in the background.'

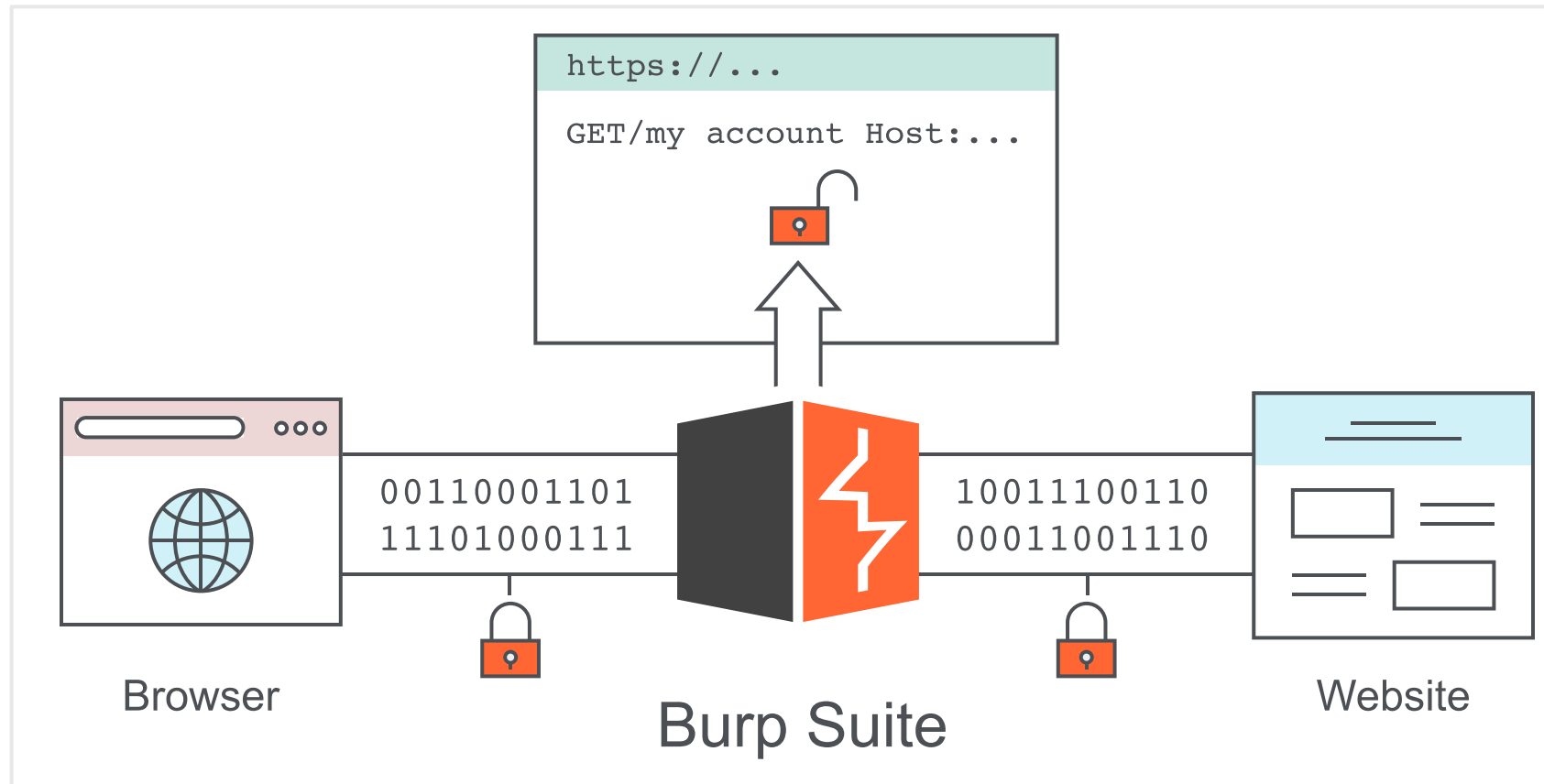
Browser makes
it look all pretty
but Burp Suite
shows you
what's going on
in the
background.

Burp Suite = Golden Tool

The screenshot displays the Burp Suite interface, specifically the Repeater tab. The interface is divided into several sections:

- Top Bar:** Contains various tool tabs: board, Target, Proxy, Intruder, Repeater (active), Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Extensio.
- Request Panel (Left):** Shows the raw request data in JSON format. The selected item is a message with the subject "Test". The request body is a JSON object with fields like "FieldURI", "Item", "Path", and "Body".
- Response Panel (Right):** Shows the raw response data in JSON format. The response includes headers (e.g., X-Backend-Begin, X-Backend-End, X-Diaginfo, X-Beserver, X-Ua-Compatible, X-Proxy-Routeroutingcorrectness, X-Proxy-Backendserverstatus, X-Feproxyinfo, X-Feezinfo, X-Feserver, Report-To) and a body containing a "Header" section with server version information and a "Body" section with an "UpdateItemResponse" message.

Burp Suite = Golden Tool



Burp Suite = Golden Tool

- There are extensions to help automate finding IDORs with Burp Suite.
- All my testing was manual so that is what we are focusing on today.

What 2 Google products did I
find these vulnerabilities on?



Google Ads

Google

Workspace

Let's Begin!



What is Google Workspace?

“Google Workspace plans provide a [custom email for your business](#) and include collaboration tools like Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms, Sites, and more.”

Admin console

https://admin.google.com/AdminHome?hl=en_GB

IceWarp Server Ad... Manage IIS on a Co...

Google Admin

Search for users, groups, and settings (e.g. turn on 2-step verification)

Loading...

Admin console

Set up billing for G Suite

Your free trial ends in 1 days. Please set up billing in order to continue accessing G Suite after trial

SET UP BILLING

Dashboard
See relevant insights about your domain

Users
Add or manage users

Groups
Create groups and mailing lists

Buildings and resources
Manage and monitor buildings, rooms and resources

Device management
Secure corporate data on devices

Apps
Manage apps and their settings

Security
Manage security features

Reports
Track usage of services

Billing
View charges and manage licences

Company profile
Update information about your company

Admin roles
Add new admins

Domains
Verify your domain or add domains

Data migration
Import email, calendar and contacts

Support
Talk to our support team

MORE CONTROLS
serverhelps.com

What is Google play console?

“PUBLISH YOUR APPS AND GAMES WITH GOOGLE PLAY CONSOLE AND GROW YOUR BUSINESS ON GOOGLE PLAY.”

All applications


Reports








Settings

+ Add new application

ALL APPLICATIONS

 The big **blue**
com.consoledemo.bigblue

 The little **blue**
com.consoledemo.littleblue

APP NAME	PRICE	ACTIVE INSTALLS	AVG. RATING / TOTAL	ERRORS	LAST UPDATE	STATUS
 The big blue	Free	12	★ 5.00 / 1	0	Aug 15, 2012	Unpublished
 The Handy Developer Guide	Free	756	★ 5.00 / 2	6	Sep 26, 2012	Published
 The big green	Free				—	Draft
 The big red	\$2.00	136	—	14	Dec 3, 2010	Published
 The big yellow	Free	3,672,387	★ 5.00 / 1	119	Jan 18, 2012	Unpublished
 The little pink	Free	7,452,652	★ 5.00 / 1,986,412	8	Jun 14, 2012	Published
 The little red	Free	2,412	★ 3.33 / 335	341	Dec 8, 2010	Published


Google Workspace Updates


This official feed from the Google Workspace team provides essential information about new features and improvements for Google Workspace customers.

Organize and create apps for your domain directly from the Admin console

Monday, November 12, 2018

With this launch, we're making it easier for you to create—and for your users to find—the Android apps they need at work.

 Filter by product ▼

 Filter by date ▼

 Subscribe by feed

Google Play/Google workspace

- Admins are allowed to publish private apps into their organization.
- Once published users in the organization can download the apps to their devices.
- Simply upload your APK file to the admin console and then users in your organization can download the app to their android devices.

Bug #1

- Possible To Gain Access To Every Gsuite (Google Workspace) Organizations Managed Google Play Store Admin Panel.



Admin

Search for users, groups or settings

Devices

Overview

Chrome

Setup gu

Devices

Managed

Settings

Apps & e

Over

User

Kios

Req

Connect

Printers

Reports

Mobile & end

Networks

Apps

Security

Reporting

quests

SETTINGS

Incognito

Add apps from Google Play

Google Play

Your email address is im.plum12@gmail.com [Update](#)

Private apps

Google	Jj	fg	fgf	frg
Not available yet	Not available yet	Not available yet	Not available yet	Not available yet

+

Request

```
Pretty Raw Hex
8q19PJxTX8SEfKnrVHY41QB1dZy8ox8M1vVQBTKRyU8TGaCC08txgJ051F2tpTrtM
s5cTinPdldtd2ixyFmwBZZULIHcuDnKloe6Auyz2F3vG3c; __ga_M885PTGKBM=
GS1.1.1695081830.1.0.1695081830.0.0.0; __ga=
GA1.1.1026915310.1636751891; SIDCC=
APoG2W_FGZq94j5QWCjRJS5nPeWxKrugA8BSoSBus4UiyMvtGg-MOHwXlGpB0jT77
ZpOF8yHlg; __Secure-1PSIDCC=
APoG2W9-yihL_a00MMX3yX3I8gN0hcw8UR9TcSpo7LwYdCoZXYWmxQAHR2sg-VMrs
19rbJzC0w; __Secure-3PSIDCC=
APoG2W_OrG08dTfiP0c6_h569n0Chh31I_GZQbWWhiYGkeTwtciht-8L8rD59S3rkr
g0xIIyhQ
4 Content-Length: 409
5 Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google
Chrome";v="116"
6 X-Same-Domain: 1
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
9 Sec-Ch-Ua-Arch: "x86"
10 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
11 Sec-Ch-Ua-Full-Version: "116.0.5845.188"
12 Sec-Ch-Ua-Platform-Version: "15.0"
13 Sec-Ch-Ua-Full-Version-List: "Chromium/116.0.5845.188",
"Not)A;Brand";v="24.0.0.0", "Google Chrome/116.0.5845.188"
14 Sec-Ch-Ua-Bitness: "64"
15 Sec-Ch-Ua-Model: ""
16 Sec-Ch-Ua-Wow64: ?0
17 Sec-Ch-Ua-Platform: "Windows"
18 Accept: */*
19 Origin: https://admin.google.com
20 X-Client-Data:
CIu2yQEIorbJAQipncOBCKzby...OBcNy9zQ
EI4MTNAQi5ysOBCLfLzQEIt83M...NpRe=
21 Sec-Fetch-Site: same-origin
22 Sec-Fetch-Mode: cors
23 Sec-Fetch-Dest: empty
24 Referer: https://admin.google.com
25 Accept-Encoding: gzip, deflate, br
26 Accept-Language: en-US,en;q=0.9
27
28 f.req=
%5B%5B%5B%22tn7m0d%22%2C%22%5B%5C%2200zj0hgq%5C%22%2C%5C%22https%3
A%2F%2Fadmin.google.com%2Fu%2F%2F%2F%2Fchrome%2Fapps%2Fuser%3Frap
t%3DAEjHL4PRQ10EpGcJubhJrSxh-wHv7Y2byvKb1bRvGaF1Rz5fdCFQWQfKtvIq
d3VojUazxwafL7824XUqJuftAN7b88XZ4fgRw%26ac_ouid%3D03ph8a2z0v0snxq%5
C%22%2Cnull%2C%5B%5B%5C%2203ph8a2z0v0snxq%5C%22%5D%5D%22%2Cnull%
2C%22generic%22%5D%5D%5D&at=
AFDX2tP-OrXsevYntBaABEA41bc8%3A1695081828469&
```



Response

```
Pretty Raw Hex Render
3uF2msWnY; expires=Wed, 18-Sep-2024 00:05:52 GMT; path=/;
domain=.google.com; Secure; HttpOnly; priority=high
20 Set-Cookie: __Secure-3PSIDCC=
APoG2W8BvVjR9HPT8smIz788QP15Ra9pWZhilc_Bsrn1fABGLZr2PwQpXdhDf-tIig
Hn62bttQ; expires=Wed, 18-Sep-2024 00:05:52 GMT; path=/;
domain=.google.com; Secure; HttpOnly; priority=high; SameSite=none
21 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
22
23 }
24 ]
25 '
26 [
[
"wrbl.fr",
"tn7m0d",
["WAGYpox4dgmJ8dbYrbI3USNy667Cz9uM582WMCCQ2yvtzAD23RSLJVBx
AEr9P0hrYORGN3qjGeAxPpkSGsfgesZRVWuYou7WzLylE6Cek51BFapaf5AQ1T
AyKj0Tw2a3ceydZqRnBILl1hamkq8RLN-FHvsgUURFTt8DzwYq2oocsyHrWrV
X1Rhuono2SbyLteI2Q6rD3CHR3MU9LJVraS6i22aDg_5pY9NaQ82YIMDGdC2jY
LCKQt6DLsbz2AFqmTP70j4A4dn5XG87WShyKHzxj7AI25ToFRJSDQ_mFUDrlca
UDz7_espjuYW0uf66jEBsXrWek2-CUeyoRHnzUWjYRtT7gB8A", "https://
admin.google.com/u/2/ac/chrome/apps/user?rapt%3DU003dAEjHL4PRQ1
0EpGcJubhJrSxh-wHv7Y2byvKb1bRvGaF1Rz5fdCFQWQfKtvIq3VojUazxwaf
L7824XUqJuftAN7b88XZ4fgRw%26ac_ouid%3D03ph8a2z0v0snxq
\"],
null,
null,
null,
null,
null,
null,
null,
"generic"
],
[
"di",
610
],
[
"af.httprrm",
610,
"-2951501654994071727",
18
]
]
27 25
28 [
[
"e",
4,
```

Inspector

Selection 354 (0x162)

Selected text

```
%5B%5B%5B%22tn7m0d%22%2C%22%5B%5C%2200zj0hgq%5C%22%2C%5C%22ht
tps%3A%2F%2Fadmin.google.com%2Fu%2F%2F%2Fchrome%2Fapps%2Fuser%3Frap
t%3DAEjHL4PRQ10EpGcJubhJrSxh-wHv7Y2byvKb1bRvGaF1Rz5fdCFQWQfKtvIq
d3VojUazxwafL7824XUqJuftAN7b88XZ4fgRw%26ac_o
```

See more

Decoded from: URL encoding

```
[["tn7m0d",["00zj0hgq",\"h
tps://admin.google.com/u/2/ac
/chrome/apps/user?rapt=AEjHL4P
RQ10EpGcJubhJrSxh-wHv7Y2byvKb1
bRvGaF1Rz5fdCFQWQfKtvIq3VojUa
zxwafL7824XUqJuftAN7b88XZ4fgR
w&ac_ouid=03ph8a2z0v0snxq\",nu
ll,[\"03ph8a2z0v0snxq\"]],n
```

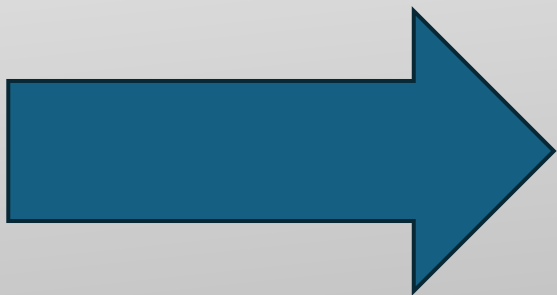
See more

Cancel	Apply changes
Request attributes	2
Request query parameters	12
Request body parameters	2
Request cookies	28
Request headers	55
Response headers	20

Bug #1

- POST
/_/DpanelChromeUi/data/batchexecute?rpcids=tn7m0d&f.sid=-4429343821357402966&bl=boq_dpanelchromeuiserver_20190926.03_p0&hl=en&customer_id=00zj0hgq&soc-app=596&soc-platform=1&soc-device=1&_reqid=404704&rt=c HTTP/1.1
Host: admin.google.com
- f.req=[[["tn7m0d",["\"00zj0hgq\"","\\"https://admin.google.com/ac/chrome/apps/user\""],null,"generic"]]]&at=

I want to access my apps admin panel!



POST
/_/DpanelChromeUi/data/batchexecute?

f.req=[[["tn7m0d",["\00zj0hgq\","\



Welcome to your admin panel!





← Private app

Title

Maximum 50 characters

gfhte|

APK file



1.0 com.ww1112sad_9322709

[edit](#)

Cancel

Save



Google Play Console

Advanced editing options

Add a detailed app description, screenshot, and more in the Google Play Console.

[Make advanced edits](#)

All applications

Reports

Settings

+ Add new application

ALL APPLICATIONS


 The big **blue**
com.consoledemo.bigblue

 The little **blue**
com.consoledemo.littleblue

APP NAME	PRICE	ACTIVE INSTALLS	AVG. RATING / TOTAL	ERRORS	LAST UPDATE	STATUS
The big blue	Free	12	★ 5.00 / 1	0	Aug 15, 2012	Unpublished
The Handy Developer Guide	Free	756	★ 5.00 / 2	6	Sep 26, 2012	Published
The big green	Free				—	Draft
The big red	\$2.00	136	—	14	Dec 3, 2010	Published
The big yellow	Free	3,672,387	★ 5.00 / 1	119	Jan 18, 2012	Unpublished
The little pink	Free	7,452,652	★ 5.00 / 1,986,412	8	Jun 14, 2012	Published
The little red	Free	2,412	★ 3.33 / 335	341	Dec 8, 2010	Published




Search for organizational units

+ Search or add a filter

Self-Employed

Target

App	Installation policy
<i>Allow users to install other apps & extensions</i>	Allow other apps & extensions from the Chrome Web Store only Inherited from Google default
 CamScanner - Scanner to scan PDF com.intsig.camscanner	Allow install Locally added



Admin

Search for users, groups or settings

Devices

Overview

Chrome

Setup gu

Devices

Managed

Settings

Apps & e

Over

User

Kios

Req

Connect

Printers

Reports

Mobile & end

Networks

Apps

Security

Reporting

quests

SETTINGS






Incognito


Add apps from Google Play

Google Play

Your email address is im.plum12@gmail.com [Update](#)

Private apps

				
Google	Jj	fg	fgf	frg
Not available yet	Not available yet	Not available yet	Not available yet	Not available yet



Supply Chain Attack

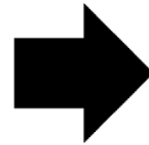
- You could have accessed any Google Workspace organizations apps admin panel and pushed your own application to devices.



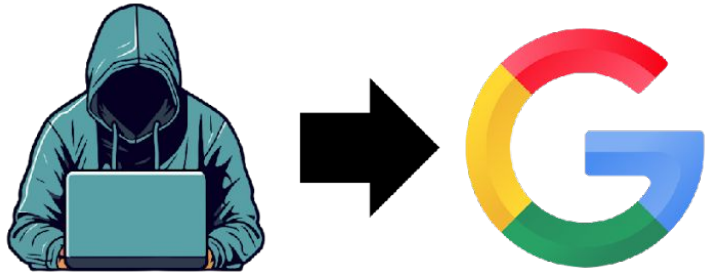
Company A



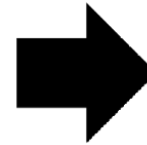
Uses Google Workspace



Publishes private internal app to their organization.



Attacker logs into company A's Google Workspace admin panel.



Attacker releases a new "version" for the private internal apps already published and installed on user's devices.


Bug #2

- Possible To Leak The Email Subjects/Logs For All Gsuite (Google Workspace) Organizations.



Bug #2

- Gmail stores logs for all stages of a message. This includes logs like the delivery process, subject, and other types of metadata.
- To view these Google Workspace has a function for admins to setup a BigQuery project for the logs to be stored to and viewed.

 **Gmail**

Status
ON for everyone

10 ALT4.ASPMX.L.GOOGLE.COM.

[MX setup instructions](#)

User email uploads

Show users the option to import mail and contacts from Yahoo!, Hotmail, AOL, or other webmail or POP3 accounts from the Gmail settings page. [Learn more](#): OFF

Email Logs in BigQuery

Configure a BigQuery project to directly access email delivery logs [Learn more](#)

Enable

Description *

dfgdfd

Enter a short description that will appear within the setting's summary.

Select a project to be used by Google to store email logs. Ensure that access to this BigQuery project is limited to authorized users

nnnn-59545

Specify the name for a new dataset to be created within your project

gmail_logs_datasetbfvbbdd

Restrict the dataset to a specific geographic location

Select a location

i Changes may take up to 24 hours to propagate to all users. Prior changes can be seen in [Audit log](#)

Bug #2

- Put any Google Workspace org ID and you will save your Google Cloud project/dataset on their settings and receive their logs.

What is Google Ads?

Google Ads lets you advertise your business, website, promotional videos, etc. across Google.

1 Anicca : 920-624-7...
Customer ID: 920-624-7834

Overview

Overview

Custom
Apr 20 - May 19, 2018

All campaigns

Search campaigns

Display campaigns

Video campaigns

Enabled

A. 1. New - PPC management UK

2018 - Google Analytics Courses

2018 | Remarketing

2018 | Services | Digital Marketing

2018 | Services | RLSA

2018 | Services | SEO

Paused and removed campaigns are hidden

Recommendations

Campaigns

Ad Groups

Ads & extensions

Videos

Landing pages

Keywords

Audiences

Demographics

Topics

Placements

Settings

Locations

Ad schedule

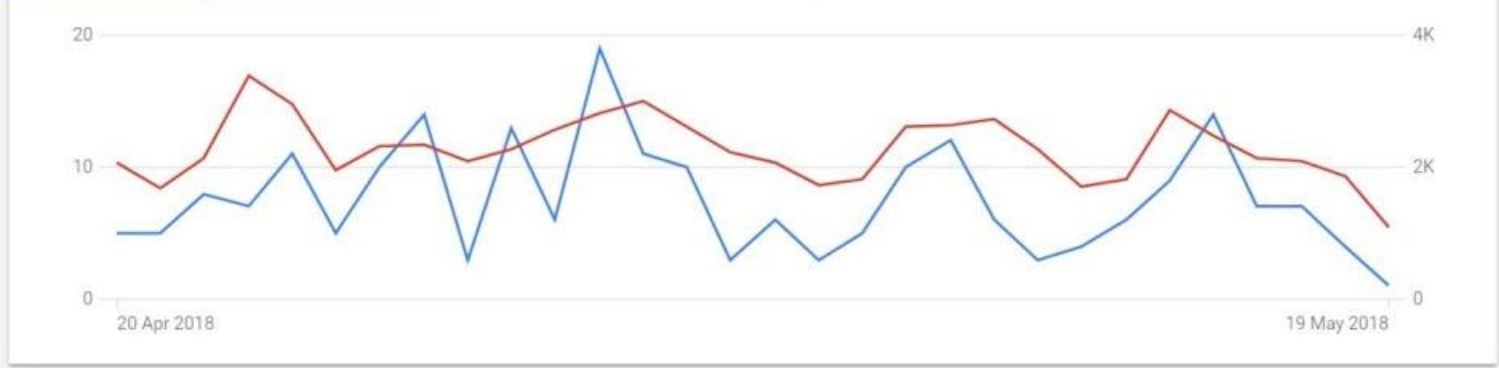
Devices

Advanced bid adj.

Change history

Drafts & experiments

Clicks	Impressions	Avg. CPC	Cost
227	68.3K	£3.15	£714



Biggest changes

Last 30 days compared to the prior 30 days

		Cost
2018 Services SEO > seo services	[Yellow bar]	-£105.96 -66.56%
2018 Services SEO > seo company	[Yellow bar]	-£94.89 -65.66%
2018 Remarketing	[Blue bar]	+£90.56 +247.63%
2018 Services SEO > seo agency	[Yellow bar]	-£55.30 -41.38%
2018 Services Digital M... > Digital Agency	[Yellow bar]	-£51.76 -100.00%

ALL CAMPAIGNS > Page 1 of 5

Campaigns

	Cost	Clicks	CTR
2018 Services Digital Marketing	£264.71	55	1.75%
2018 Services SEO	£235.17	26	0.80%
2018 Remarketing	£127.13	124	0.20%
A. 1. New - PPC management UK	£48.82	5	1.61%
2018 Bootcamps Social	£30.08	15	4.79%

ALL CAMPAIGNS > Page 1 of 2

Search keywords

	Cost	Clicks	CTR
--	------	--------	-----

Searches

Sort by: Impressions

SEARCH TERMS	WORDS
--------------	-------

Google Ads

- Google Ads Bulk Upload Feature
- Download pre-created templates and then make bulk changes to your ads account.

Campaigns

Edit Campaigns Budget Amount
Edit Campaigns Languages
Apply/Remove Labels on Campaign(s)
Edit Campaign(s) Start/End Date
Edit Campaign(s) Name
Create New Campaign(s)
Edit Campaign(s) Inventory Type (Video)
Delete Campaign(s)
Pause/Enable Campaign(s)
Edit Campaign(s) Devices Settings

Ad assets

Create Sitelink Asset
Create Call Asset
Create App Asset
Create Callout Asset
Create Structured Snippet Asset
Create Price Asset
Create Image Asset

Bug #3

- Leak All Uploaded Files On Every Google Ads Account!
- Remember Burp Suite?



Bug #3

- POST
/aw_cm/_/rpc/BulkExecutionService/List?authuser=0&acx-v-bv=awn_cm_20181017_RC03&acx-v-clt=1540487931567&rpcTrackingId=BulkExecutionService.List%3A6 HTTP/1.1
- Host: ads.google.com

- POST
/aw_cm/_/rpc/ExecutionDetailService/List?authuser=0&acx-v-bv=awn_cm_20181017_RC03&acx-v-clt=1540493607856&rpcTrackingId=ExecutionDetailService.List%3A1 HTTP/1.1
- Host: ads.google.com

Hey! I want to load my Google Ads Files!

POST
/aw_cm/_/rpc/BulkExecutionService/List

__ar={"1":{"3":{"1":"241488436"},"5":"TABLE"}}

Here are your files!



Google Ads

Bug #3

- `__ar={"1":{"3":{"1":"241488436"},"5":"TABLE"}}`
- Put any Google Ads account ID and you would pull the upload history for their account.

Bug #3

- By using Burp Suite all you had to do was change the ID from your Ads account to another account you did not have access too and would load the files.
- Note: Only use IDs for accounts that are yours!

Your account isn't active - To activate your account and start running your ads, enter your card details and complete the verification process.

Data feeds

Upload history

Data feeds

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x 13 x 14 x 15 x 16 x 17 x 18 x 19 x ...

Go Cancel < > Target: https://ads.google.com

Request

Raw Params Headers Hex

```
APISID=WAlcTF1Lj2Bw4meF/Avs17KVDP1jXmQyYw;
SAPISID=A4wNvyMHqvgPp9_1/Al6c9MruZhn_KyP5B;
CONSENT=YES+US.en+20160904-14-0;
SIDCC=ABtHo-HINkx1KX7UyE6koc0ZuDdmS1jsjmiQm8M1laTrxSHdktyBOTKES2APGE-mN
69PdcFDmg; iP_JAR=2018-10-25-17;
gap43AWA-37177323-143A18558082978=47B42mob11e42243A42243A18558082978200343
212C422display42243A422(855)420962-720342242C422expires42243A1540493274
47D; _gcl_au=1.1319439034.1540487876;
_ga=GAl.3.1404448982.1540487875; _gid=GAl.3.718236901.1540487876;
AdsUserLocale=en_GB;
s=advords-usermgmt=yRsy6FWwXc1j12cX4pXG1k6DFzS2QnaC:advords-frontent-re
porting=qeGN76McbSg9FUqrEj-1xactiPV_cuv:advords-frontent-bulk=Et3kGVPZ
tfeeYvu7AM1GJvXORoeOjVB:advords-navi=-yvhpCv93FT9GsyTzWDbokUSintHRhp;
SAG=pAaJf3oc_31XjxItfkAbc7u_1HKyuAvNj6KvQ6omGshswlU4nkqcpaDls_ixEeN-sqV
agQ.;
A=AIxWtXTN871YK2gWvQx1lxoDb56hrkEUBeyJ52ETVTDEIkMuOvVlaUAJ-yfVvD9mmPA
chX0AhMCQrPrrYGUQGYHPB1HEKhLLSSQmsds7na1fB91UbKDX6HEvDt9GgDkZbo1JEfP1X
1B7JYVEcHPP1KfpB1PBDsgZ10defnQj1r7Kw4VcyLw03P4Uu7QTGLmJvn19Pu4PN:
advordsReferralSource=sourceid=&subid=&clickid=
hl=en GB& lu=2497990874_u=7894959863& c=1933411000&f.sid=-3538396891
089959000& ar=47B422142243A47B422342243A47B422142243A42224140843642247
D47D42C422242243A47B422242243A45B47B422142243A4222execution_id4224224
42243A45B47B422342243A42210095765515181396012247D45D47D45D47D4&activi
tyContext=Anonymous&requestPriority=HIGH_LATENCY_SENSITIVE&activityType
=ANONYMOUS&destinationPlace=%2Fav%2Fbusinessdata%2Ffeed
```

0 matches

Done

Response

Raw Headers Hex

```
SIDCC=ABtHo-EZher1pFinGih0j5rjYpiJuaXKGalJXyit6agU8IqHflc6UaqE9yXmWc19Y
BA4s4imYA; expires=Wed, 23-Jan-2019 18:20:17 GMT; path=/;
domain=.google.com; priority=high
Alt-Svc: quic=":443"; ma=2592000; v="44,43,39,35"
Connection: close
Content-Length: 1262
{"1": {"1": "241488436", "2": "100957655151813960", "3": "1540491564206", "4":
:4, "5": {"1": "2", "2": "4", "3": "0", "4": "0", "5": {"1": "1", "2": {"1": "21", "3": "1",
4": "4"}}, "6": {}, "7": "1540491565795", "8": {"2": "im.plum12@gmail.com"}, "
9": {"2": {"1": "4", "2": "1540491565250", "3": "CAASOC9h2HdvcmRzYXBPiGtzaG
VidHMvdXBsb2Fkey8zNGNBQVY1RWFSM19HVEVDZmlpY3FNTW1BGgAgHvMvAv"u003d"u00
3d", "4": "en_us", "6": "feed.csv", "9": "CAASOC9h2HdvcmRzYXBPiGtzaGVLd
HMvdXBsb2Fkey81ZmJpYVY1RWFTTD1HM5uXzhHRKVNVAJRgGAgmvMvAv"u003d"u003d"
, "11": "AEnB2Uro1R4kucdlvo7yzQ2n1R9LQvelliqfjukLu28VqOEUKv1PW17vDsmi0Pd
HnM4_b8Q6e-X2-70dmBKkKnlYPjyN-3jnv", "12": "feed creation", "13": "6", "14":
2, "15": {"1": "uploadFileName", "2": "feed.csv"}, {"1": "operatingCustomer
Id", "2": "241488436"}, {"1": "feedName", "2": "leak file
details"}, {"1": "customerId", "2": "1416932726"}, {"1": "authenticatedUserI
d", "2": "7422995313"}, {"1": "criteriaTypeId", "2": "61"}, {"1": "uploadMode
", "2": "LIVE"}, {"1": "userId", "2": "7422995313"}, {"1": "Internal_Upload
Source", "2": "ANN"}}, {"16": {"1": "83244329", "2": [{"1": "1", "2": "Page
URL", "3": "5", "4": "false"}, {"1": "2", "2": "Custom
label1", "3": "9", "4": "false"}], "3": [{"Page URL", "Custom
label1"}], "19": "1", "22": "false"}, {"10": "false", "11": {}, "12": {"1": "3141257354"
, "2": {"fgdfgdf"}, "13": "279035174", "14": "248006137"}], "2": {"3": {"1": "1"
}}}
```

0 matches

2,044 bytes | 181 millis

Bug #4

- Leak All Uploaded Files On Every Google Ads Account.....again.



Bug #4

- Leak All Google Ads Uploaded Files Again!
- After fixing the first bug a new API was released to download files.
- <https://ads.google.com/api/adwords/bulksheet/upload/form/errors?xid=308702270061146755&customerId=1416932726&userId=7422995313&operatingCustomerId=302261519&authuser=0>
- Change the XID value (ID of the file on the account you are targeting) and customerID value to anyone's account and download their file!

IDs are NOT security boundaries!

- If the ID never changes and is always connected to some form of data that is not a security boundary.
- This simple URL allowed you to put anyone's file ID and Ads account ID and access their file.

Thanks

Shoutout Google VRP as well!