dorking g0d

Google Dork - Sensitive Data

```
inurl:email= | inurl:phone= | inurl:name= | inurl:user= inurl:&
site:example[.]com
```

dork - exposed config

```
site:example[.]com ext:log | ext:txt | ext:conf | ext:cnf | ext:ini |
ext:env | ext:sh | ext:bak | ext:backup | ext:swp | ext:old | ext:~ |
ext:git | ext:svn | ext:htpasswd | ext:htaccess | ext:json
```

Google Dork - XSS Prone Parameters

```
site:example[.]com inurl:q= | inurl:s= | inurl:search= | inurl:query= |
inurl:keyword= | inurl:lang= inurl:&
```

Test for XSS in param value:

```
'"><img src=x onerror=alert()>
```

Google Dorks for Bug Bounty

A list of Google Dorks for Bug Bounty, Web Application Security, and Pentesting

Live Tool

Follow @TakSec

Broad domain search w/ negative search

```
site:example.com -www -shop -share -ir -mfa
```

PHP extension w/ parameters (hightlight :3)

```
site:example.com ext:php inurl:?
```

API Endpoints

```
site:example[.]com inurl:api | site:*/rest | site:*/v1 | site:*/v2 |
site:*/v3
```

Juicy Extensions

```
site:"example[.]com" ext:log | ext:txt | ext:conf | ext:cnf | ext:ini |
ext:env | ext:sh | ext:bak | ext:backup | ext:swp | ext:old | ext:~ |
ext:git | ext:svn | ext:htpasswd | ext:htaccess | ext:json
```

High % inurl keywords

```
inurl:conf | inurl:env | inurl:cgi | inurl:bin | inurl:etc | inurl:root |
inurl:sql | inurl:backup | inurl:admin | inurl:php site:example[.]com
```

Server Errors

```
inurl:"error" | intitle:"exception" | intitle:"failure" | intitle:"server
at" | inurl:exception | "database error" | "SQL syntax" | "undefined index"
| "unhandled exception" | "stack trace" site:example[.]com
```

XSS prone parameters

```
inurl:q= | inurl:s= | inurl:search= | inurl:query= | inurl:keyword= |
inurl:lang= inurl:& site:example.com
```

Open Redirect prone parameters

```
inurl:url= | inurl:return= | inurl:next= | inurl:redirect= | inurl:redir= |
inurl:ret= | inurl:r2= | inurl:page= inurl:& inurl:http site:example.com
```

SQLi Prone Parameters

```
inurl:id= | inurl:pid= | inurl:category= | inurl:cat= | inurl:action= |
inurl:sid= | inurl:dir= inurl:& site:example.com
```

SSRF Prone Parameters

```
inurl:http | inurl:url= | inurl:path= | inurl:dest= | inurl:html= |
inurl:data= | inurl:domain=  | inurl:page= inurl:& site:example.com
```

LFI Prone Parameters

```
inurl:include | inurl:dir | inurl:detail= | inurl:file= | inurl:folder= |
inurl:inc= | inurl:locate= | inurl:doc= | inurl:conf= inurl:&
site:example.com
```

RCE Prone Parameters

```
inurl:cmd | inurl:exec= | inurl:query= | inurl:code= | inurl:do= |
inurl:run= | inurl:read=  | inurl:ping= inurl:& site:example.com
```

File upload endpoints

```
site:example.com ”choose file”
```

API Docs

```
inurl:apidocs | inurl:api-docs | inurl:swagger | inurl:api-explorer
site:"example[.]com"
```

Login Pages

```
inurl:login | inurl:signin | intitle:login | intitle:signin | inurl:secure
site:example[.]com
```

Test Environments

```
inurl:test | inurl:env | inurl:dev | inurl:staging | inurl:sandbox |
inurl:debug | inurl:temp | inurl:internal | inurl:demo site:example.com
```

Sensitive Documents

```
site:example.com ext:txt | ext:pdf | ext:xml | ext:xls | ext:xlsx | ext:ppt
| ext:pptx | ext:doc | ext:docx
intext:“confidential” | intext:“Not for Public Release” | intext:”internal
use only” | intext:“do not distribute”
```

Sensitive Parameters

```
inurl:email= | inurl:phone= | inurl:name= | inurl:user= inurl:&
site:example[.]com
```

Adobe Experience Manager (AEM)

```
inurl:/content/usergenerated | inurl:/content/dam | inurl:/jcr:content |
inurl:/libs/granite | inurl:/etc/clientlibs | inurl:/content/geometrixx |
inurl:/bin/wcm | inurl:/crx/de site:example[.]com
```

Disclosed XSS and Open Redirects

```
site:openbugbounty.org inurl:reports intext:"example.com"
```

Google Groups

```
site:groups.google.com "example.com"
```

Code Leaks

```
site:pastebin.com "example.com"
```

```
site:jsfiddle.net "example.com"
```

```
site:codebeautify.org "example.com"
```

```
site:codepen.io "example.com"
```

Cloud Storage

```
site:s3.amazonaws.com "example.com"
```

```
site:blob.core.windows.net "example.com"
```

```
site:googleapis.com "example.com"
```

```
site:drive.google.com "example.com"
```

```
site:dev.azure.com "example[.]com"
```

```
site:onedrive.live.com "example[.]com"
```

```
site:digitaloceanspaces.com "example[.]com"
```

```
site:sharepoint.com "example[.]com"
```

```
site:s3-external-1.amazonaws.com "example[.]com"
```

```
site:s3.dualstack.us-east-1.amazonaws.com "example[.]com"
```

```
site:dropbox.com/s "example[.]com"
```

```
site:box.com/s "example[.]com"
```

```
site:docs.google.com inurl:"/d/" "example[.]com"
```

JFrog Artifactory

```
site:jfrog.io "example[.]com"
```

Firebase

```
site:firebaseio.com "example[.]com"
```

Dorks that work better w/o domain

Bug Bounty programs and Vulnerability Disclosure Programs

```
"submit vulnerability report" | "powered by bugcrowd" | "powered by
hackerone"
```

```
site:*/security.txt "bounty"
```

Apache Server Status Exposed

```
site:*/server-status apache
```

WordPress

```
inurl:/wp-admin/admin-ajax.php
```

Drupal

```
intext:"Powered by" & intext:Drupal & inurl:user
```

Joomla

```
site:*/joomla/login
```

Medium articles for more dorks:

https://thegrayarea.tech/5-google-dorks-every-hacker-needs-to-know-fed21022a906

https://infosecwriteups.com/uncover-hidden-gems-in-the-cloud-with-google-dorks-8621e56a329d

https://infosecwriteups.com/10-google-dorks-for-sensitive-data-9454b09edc12

Top Parameters:

https://github.com/lutfumertceylan/top25-parameter

Proviesec dorks:

https://github.com/Proviesec/google-dorks