Complete guide to finding more vulnerabilities with Shodan and Censys

BY BLACKBIRD-EU · NOVEMBER 19, 2024 · LAST UPDATED ON JULY 28, 2025

You've probably seen another bug bounty hunter or security researcher find cool bugs using internet search engines like Shodan or Censys. But when you tried to replicate their steps, it seemed like an impossible task and all you can conclude is that they just came across a unique case and got lucky. In this article, we will go over almost all search filters to help you find cool vulnerabilities using reconnaissance with tools like Shodan and Censys!

This article is a guide specifically for beginners with no prior knowledge about using internet search engines to find vulnerabilities. Please note that although this article is only limited to Shodan and Censys, you can still apply the same methods to other tools like Fofa, Netlas, ZoomEye, etc.

Let's dive in!

Importance of reconnaissance

In case you aren't aware of what reconnaissance is, it is the act of gathering (useful) information that can help in later detection and exploitation phases. Reconnaissance or information gathering also forms the first (and most important phase) of a pentest and in bug bounties.

Bug bounty hunters who spend time performing reconnaissance, are almost always rewarded well for their efforts as they often come across exposed assets or hosts that have never been tested before. However, newcomers often do not know what to look for and how to find these interesting assets. We believe that with the right methodology and tools, any bug bounty hunter should be capable of performing good recon on any target. That's why we wanted to curate this article for you, we are certain that by the end of this post, you will be able to take advantage of tools like Shodan and Censys to perform proper reconnaissance on any of your bug bounty targets.

If you want to read more on reconnaissance in bug bounties (and web security in general), check out our articles like Google dorking for beginners on our blog!

https://blog.intigriti.com/hacking-tools

What are internet search engines like Shodan and Censys?

An internet search engine is similar to widely used search engines like Google & Bing search. The main difference is that tools like Shodan and Censys scan and index live hosts on the internet (instead of web content). They also provide you the ability to search for any services running on these live hosts. And you can see where these tools can be deployed to find more vulnerabilities, especially on wide-scope targets!

We can use these search engines to find interesting services running on hosts that belong to our target company or organization. For example, new hosts that have just been added to the organization's network, or accidentally exposed (and often forgotten) hosts that shouldn't be on the internet.

Let's cover the basic search operators first before we dive into the more advanced ones. Afterward, we will move on to the interesting use cases that will yield us better results and help us find more vulnerabilities!

Basic search operators

The following search operators will allow us to return indexed hosts and internet-connected devices linked to a certain organization, this can help us filter out devices and hosts that we are not interested in.

Filtering by organization:

The **"org"** operator allows us to narrow down our search results to only include hosts that Shodan or Censys were able to classify under a certain organization or company.

Shodan query:

```
org:"Intigriti"
```

Censys query:

```
autonomous_system.organization:"Intigriti"
```

You can also use the **"ssl"** operator in Shodan or **"services.tls.certificate.parsed.subject.organization"** in Censys to search for SSL/TLS certificates issued to the target.

TIP! Always verify that the discovered host effectively belongs to your target and is in scope before starting any testing! Shodan, Censys and other similar tools may incorrectly classify hosts!

Filtering by Autonomous System Number (ASN):

Similarly, we can also filter by ASNs of companies and organizations:

On Shodan, we can use:

```
asn:AS1234
```

Censys:

```
autonomous_system.asn: AS1234
```

Filtering by HTTP status code:

We can further narrow down our search and combine one of the above queries with an HTTP status code operator to only include hosts that match a 200 status code for example:

On Shodan, our query would look like the following:

```
http.status:200 org:"Intigriti"
```

On Censys:

```
services.http.response.status_code:200 AND autonomous_system.organization: "Intigriti"
```

Note that Censys requires you to use the **"AND"** operator to chain multiple queries, the **"OR"** operator is also supported.

Advanced search operators

Finding more subdomains using SSL/TLS certificates

Finally, coming to the more advanced examples, let's attempt to find more subdomains of a root domain using SSL certificates:

On Shodan:

```
ssl.cert.subject.CN:"intigriti.com"
```

Censys:

```
services.tls.certificate.names:"intigriti.com"
```

Finding more subdomains using favicons

Another way to find subdomains, and other assets that belong to your target is by searching for hosts that have the same favicon hash. Shodan and Censys both provide a native search operator to help you filter the results of hosts that match a specific favicon hash.

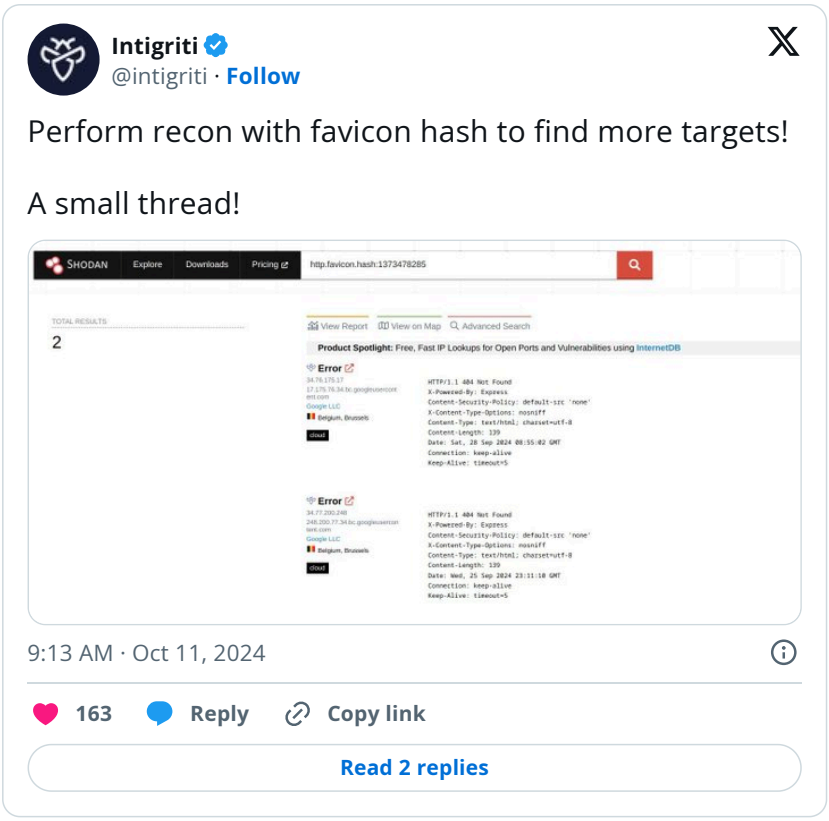
Shodan:

```
http.favicon.hash:<favicon_hash>
```

Censys:

```
services.http.response.favicons.hashes:<favicon_hash>
```

TIP! Want to learn more about how to generate a favicon hash for your target? Check out our small thread on Twitter!



Finding more targets with unique keywords

Another way to find targets that belong to your organization is by looking for unique keywords that are present in the response body of every host. This can be:

- Analytics scripts (with a unique tracking ID such as Google Tag Manager IDs)
- Copyright notices
- Company names
- Custom response headers
- Any other unique keyword that you can find in responses of your target

On Shodan, we can use the following query:

```
http.html:"© copyright <company>"
```

On Censys:

```
services.http.response.body:"© copyright <company>"
```

Filtering by technologies

Now that we have found hosts that belong to our target, we can further narrow down our search to look for more interesting assets. For example, suppose we only want to view assets that are running PHP on the backend.

On Shodan, we can make use of the following operator:

```
org:<company> http.component:php
```

On Censys, we could run the following query:

```
autonomous_system.organization:"<company>" AND services.software.product:"PHP"
```

More interesting use cases

So we've covered the most used search operators now, let's get into the more useful queries that will yield us interesting results from where we can start to perform our tests!

Finding forgotten hosts

A great indication of finding forgotten hosts that are still exposed to the internet is filtering for expired certificates.

On Shodan, we can make use of the "cert.expired" search filter:

```
org:<company> ssl.cert.expired: true
```

On Censys, we can use the following:

```
autonomous_system.organization:"<company>" AND services.tls.certificate.parsed.validity_period.not_after: 2024-11-17
```

TIP! You can also search for outdated copyright notices to locate often forgotten assets that are still exposed to the internet!

Finding authentication panels and endpoints

We can also make use of existing search filters to narrow down our search results to only include authentication panels.

On Shodan:

```
org:<company> http.title:Login,Log in,Register,Signin, Sign in, Sign up
```

*The comma character in the **"http.title"** value acts as an OR operator and will allow us to match against multiple values.*

On Censys:

```
autonomous_system.organization:"<company>" AND services.http.response.html_title: {"Login", "Log in", "Register", "Signin", "Sign in", "Sign up"}
```

Finding sites with directory listings enabled

Directory listings are goldmines to bug bounty hunters as they often expose what files and directories are available on the server. These files are often (or can often contain references to) server logs, backups, environment files, and other interesting secrets.

We can make use of the same search filter to look for servers with directory listing enabled.

Shodan:

```
org:<company> http.title:"Index of"
```

Censys:

```
autonomous_system.organization:"<company>" AND services.http.response.html_title: "Index of *"
```

Finding sites running PHP

Sites running PHP are always fun to test! Luckily, Shodan as well as Censys allow us to filter based on technologies! You can replace "php" in the following search queries with any technology.

Shodan:

```
org:<company> http.component:php
```

Censys:

```
autonomous_system.organization:"<company>" AND services.software.product: "PHP"
```

Finding sites running on non-standard HTTP ports

We always recommend you to run a query to discover HTTP servers running on non-standard HTTP ports (servers that are not listening on port 80, 443, 8080 or 8443). They are always interesting to check out as they often serve content for development purposes or other administrative tasks!

Shodan:

```
org:<company> http.status:200,404 -port:80 -port:443 -port:8080 -port:8443
```

Censys:

```
autonomous_system.organization:"<company>" AND services: (service_name: HTTP and not port: {80, 443, 8080, 8443})
```

Finding suspicious HTTP redirects

HTTP servers that respond with a 30X HTTP status code must always be examined. The reason for that is they can host content on different directories that do not require any authentication.

Here's how to quickly pull hosts that have a server listening and are responding with a 30X status code.

Via Shodan:

```
org:<company> http.status:301,302,303
```

On Censys:

```
autonomous_system.organization:"<company>" AND services.http.response.status_code: [300 to 399]
```

Finding sites running Jenkins

The last example we want to share is how to find commonly used products of third-party vendors on your targets. As an example, we will take Jenkins, a popular open-source CI/CD development tool primarily used by software companies.

On Shodan, we can make a simple keyword search:

```
org:<company> product:jenkins
```

Via Censys, we can make use of the `software.vendor` filter:

```
autonomous_system.organization:"<company>" AND services.software.vendor: jenkins
```

TIP! In both instances, you can also target a keyword search where you'd search for a unique response element instead (such as the `X-Jenkins` HTTP response header). This is especially helpful when both Shodan and Censys do not return any result for a specific product or service name.

Conclusion

As we all know, reconnaissance is quite important in bug bounties and just pentesting in general. Bug bounty hunters who are capable of performing good recon on their targets are usually rewarded well by coming across accidentally exposed targets, forgotten hosts and other untouched assets!

Using the knowledge from this article in conjunction with our other previously published articles on reconnaissance can help you as a beginner to start finding bugs solely through performing good reconnaissance.

If you are interested in trying out your new skill sets and exploring wide-scope targets, check out our program lists on Intigriti and who knows, maybe your next bounty will be earned on our platform!

https://intigriti.com/programs

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com