
Google Dork
1/8
1/2
1/4
1/16
YUNUS MAMAN
1/64
CYBER SECURITY SPECIALIST
1/32

# Google Hack

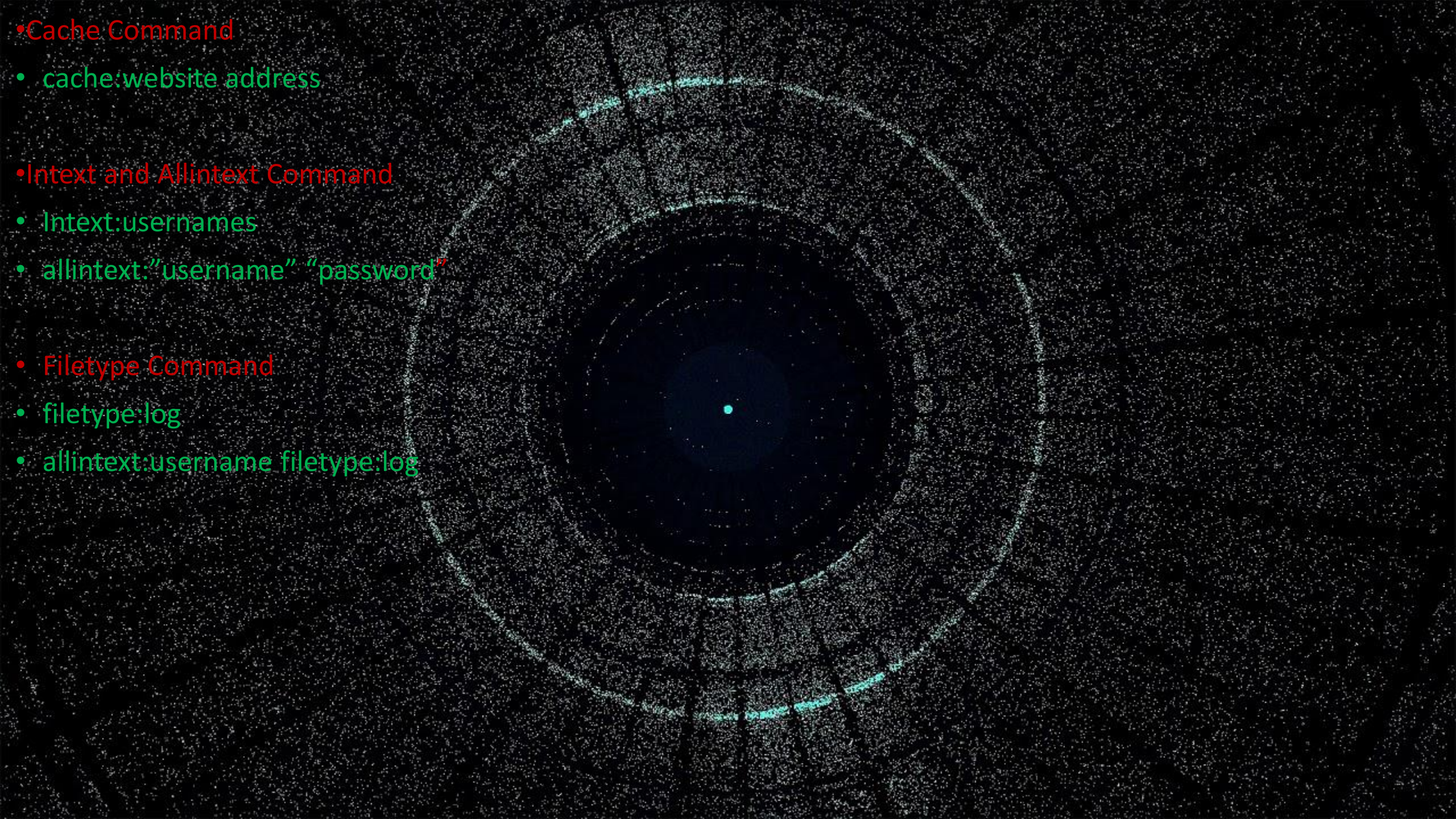
•Google korsanlığı olarak da bilinen Google Dorking, gelişmiş arama operatörlerini kullanan bir arama dizesi sağlayarak, basit arama sorguları yoluyla bulunması zor bilgileri döndürme yeteneğine sahip bir yöntemdir.

- Öncelikle, etik hackerlar bu yöntemi arama motorunu sorgulamak ve önemli bilgileri bulmak için kullanırlar. Bu Google korsanlığı hile sayfası, Google Dorking komutlarını uygulamanıza ve gizli bilgilere erişmenize yardımcı olacaktır. Google dork pentesterların kullandığı arama yöntemlerinden biridir.

# Arama Parametreleri

- `cache`: bu size herhangi bir web sitesinin önbelleğe alınmış sürümünü gösterecek, örn.`cache:securitytrails.com`
- `allintext`: herhangi bir web sayfasında bulunan belirli metni arar, örn.`allintext: hacking tools`
- `allintitle`: allintext ile tam olarak aynıdır, ancak X karakterli başlıklar içeren sayfaları gösterir, örn.`allintitle:"Security Companies"`
- `allinurl`: URL'si belirtilen tüm karakterleri içeren sonuçları getirmek için kullanılabilir, örneğin:`allinurl:clientarea`
- `filetype`: her türlü dosya uzantısını aramak için kullanılır, örneğin, pdf dosyalarını aramak istiyorsanız şunları kullanabilirsiniz:`email security filetype: pdf`
- `inurl`: bu, ile tamamen aynıdır `allinurl`, ancak yalnızca tek bir anahtar kelime için kullanışlıdır, örn.`inurl:admin`
- `intitle`: başlık içinde çeşitli anahtar kelimeleri aramak için kullanılır, örneğin, `intitle:security tools`"güvenlik" ile başlayan başlıkları arayacaktır ancak "araçlar" sayfanın başka bir yerinde olabilir.
- `inanchor`: bu, herhangi bir bağlantıda kullanılan tam bir bağlantı metni aramanız gerektiğinde kullanışlıdır, örn.`inanchor:"cyber security"`
- `intext`: metinlerinde belirli karakterler veya dizeler içeren sayfaları bulmak için kullanışlıdır, örn.`intext:"safe internet"`
- `site`: belirtilen etki alanı ve alt etki alanı için dizine eklenmiş tüm URL'lerin tam listesini gösterir, örn.`site:securitytrails.com`
- *: kelimenizden önce "herhangi bir şey" içeren sayfalarda arama yapmak için kullanılan joker karakter, örneğin `how to * a website`, "nasıl yapılır..." tasarım/yaratma/hackleme, vb.
- `|`: bu mantıksal bir operatördür, örneğin `"security" "tips"`"güvenlik" veya "ipuçları" veya her ikisini birden içeren tüm siteleri gösterecektir.
- +: kelimeleri birleştirmek için kullanılır, birden fazla belirli anahtar kullanan sayfaları algılamak için kullanışlıdır, örn.`security + trails`
- –: eksi işleci, belirli sözcükleri içeren sonuçların gösterilmesini önlemek için kullanılır; örneğin, `security -trails`metninde "güvenlik" geçen sayfaları gösterir, ancak "izler" sözcüğünü içeren sayfaları göstermez.

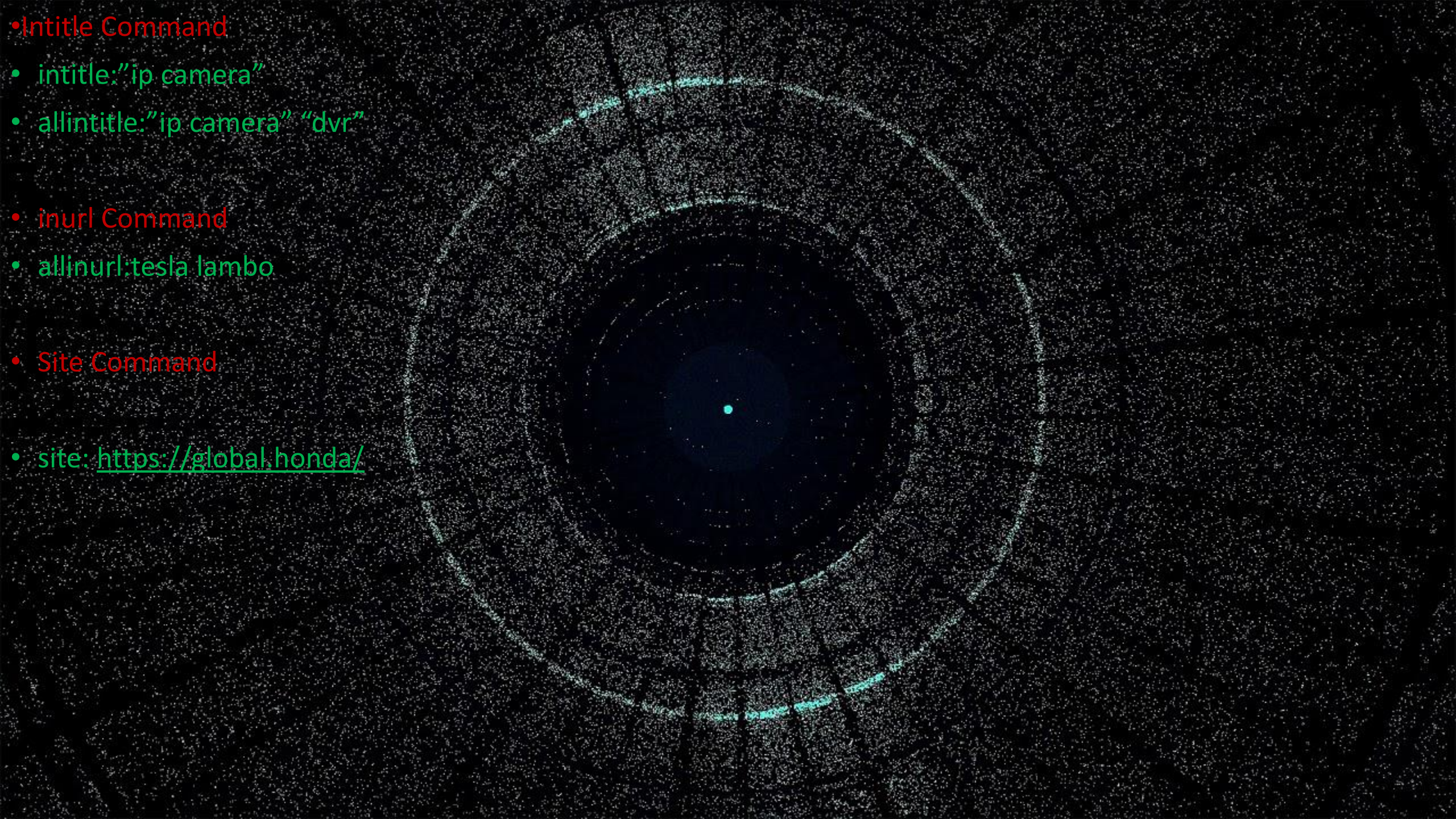
- Google Dorks'u Önleme
- Bir Google Dork'un eline düşmekten kaçınmanın pek çok yolu var.
- Bu önlemler, hassas bilgilerinizin arama motorları tarafından dizine eklenmesini önlemek için önerilmektedir.
- Özel alanları bir kullanıcı ve parola kimlik doğrulaması ile ve ayrıca IP tabanlı kısıtlamalar kullanarak koruyun.
- Hassas bilgilerinizi (kullanıcı, şifreler, kredi kartları, e-postalar, adresler, IP adresleri, telefon numaraları vb.) şifreleyin.
- Sitenize karşı düzenli güvenlik açığı taramaları yapın, bunlar genellikle zaten popüler Google Dorks sorgularını kullanır ve en yaygın olanları tespit etmede oldukça etkili olabilir.
- Herhangi bir önemli bilgiyi kötü adamlardan önce bulup bulamayacağınızı görmek için kendi web sitenizde düzenli dork sorguları çalıştırın. Exploit DB Dorks veritabanında popüler aptalların harika bir listesini bulabilirsiniz .
- Hassas içeriğin açığa çıktığını tespit ederseniz, Google Search Console'u kullanarak kaldırılmasını isteyin .
- Kök düzeyindeki web sitesi dizininizde bulunan bir robots.txt dosyasını kullanarak hassas içeriği engelleyin.



- Cache Command
- cache:website address

- Intext and Allintext Command
- Intext:usernames
- allintext:”username” “password”

- Filetype Command
- filetype:log
- allintext:username filetype:log

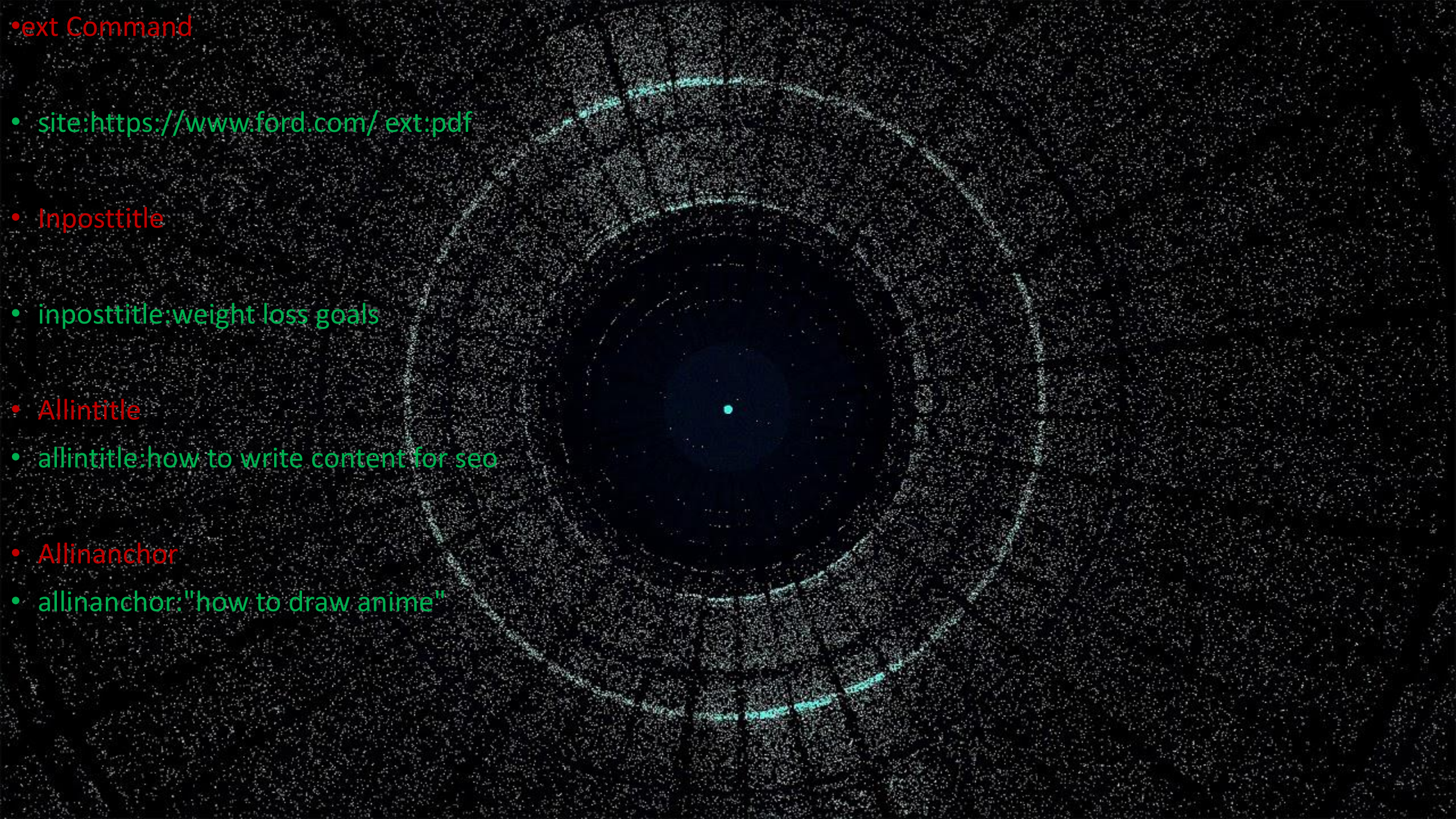


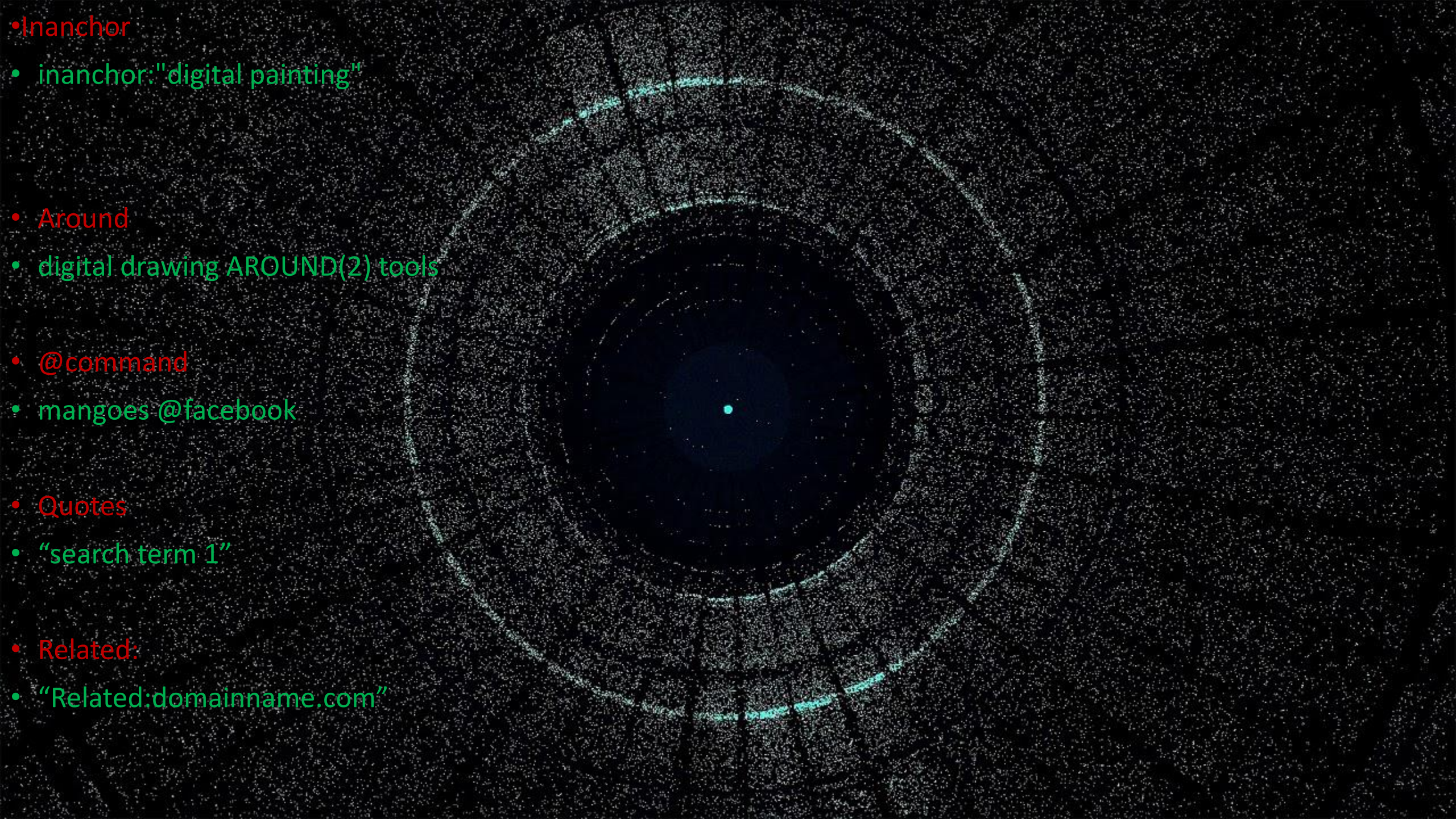
- Intitle Command
- intitle:”ip camera”
- allintitle:”ip camera” “dvr”

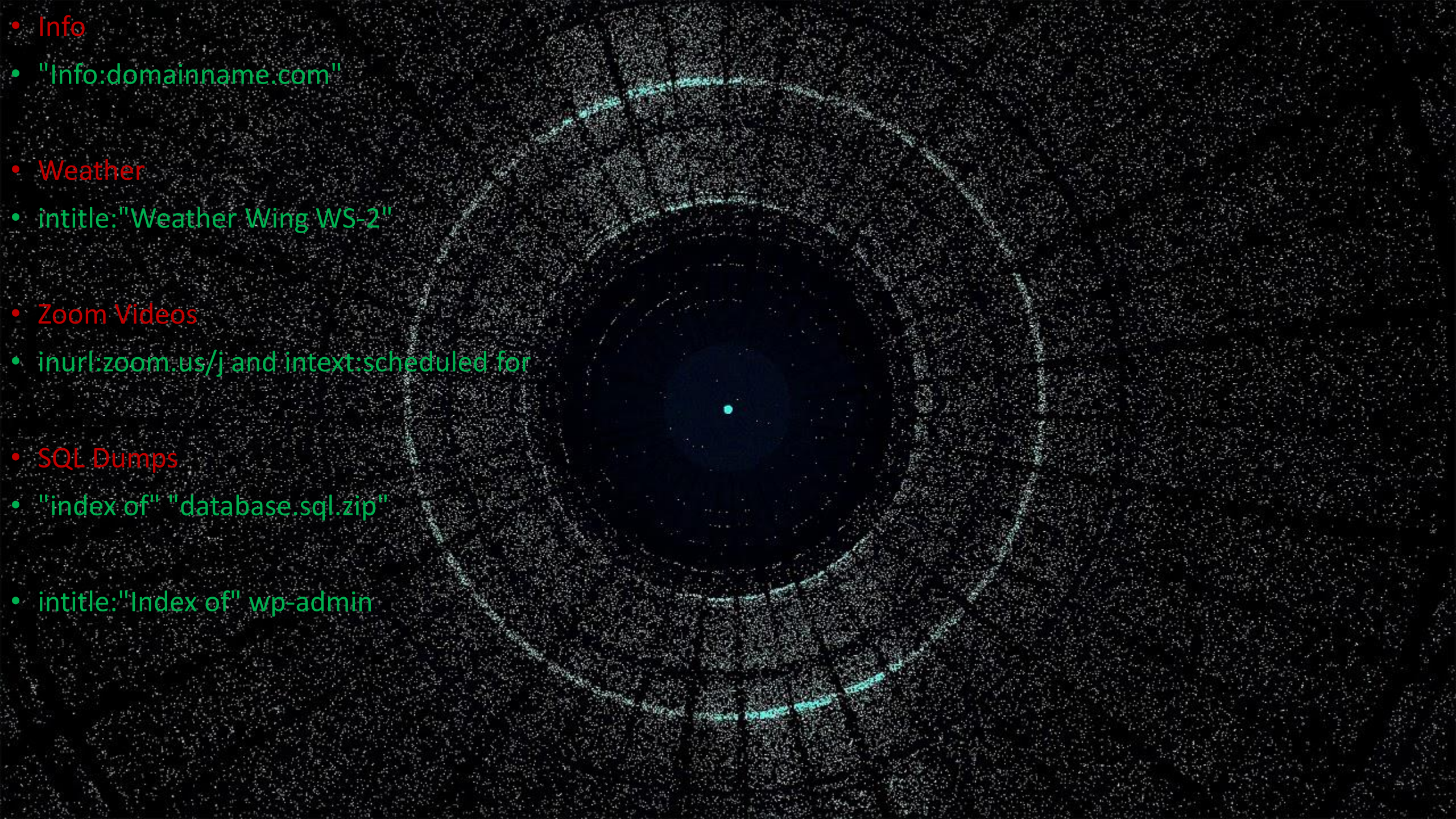
- inurl Command
- allinurl:tesla lambo

- Site Command

- site: https://global.honda/


•ext Command
• site:https://www.ford.com/ ext:pdf
• Inposttitle
• inposttitle:weight loss goals
• Allintitle
• allintitle:how to write content for seo
• Allinanchor
• allinanchor:"how to draw anime"


•Inanchor
• inanchor:"digital painting"
• Around
• digital drawing AROUND(2) tools
• @command
• mangoes @facebook
• Quotes
• “search term 1”
• Related:
• “Related:domainname.com”



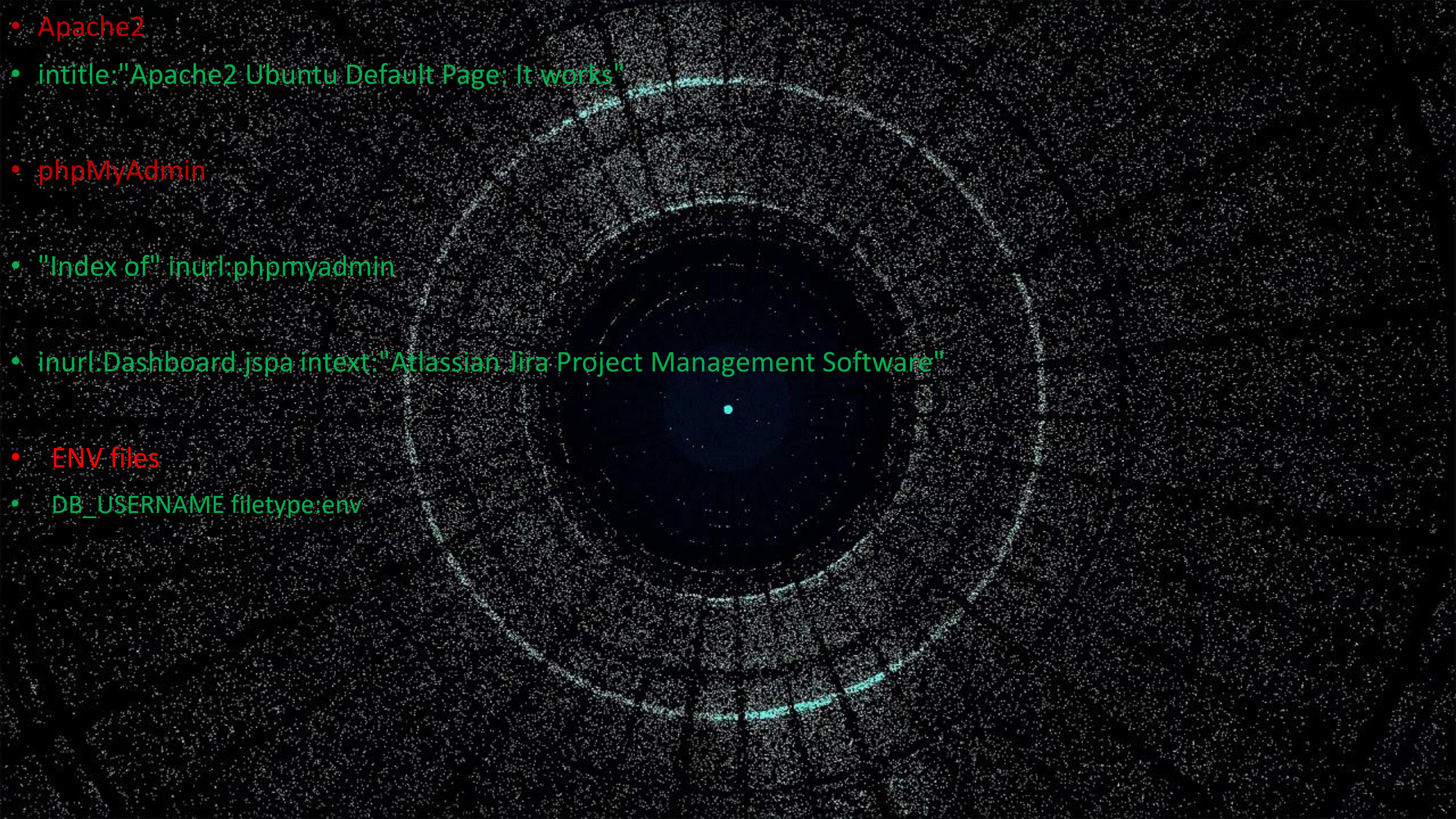
- Info
- "Info:domainname.com"

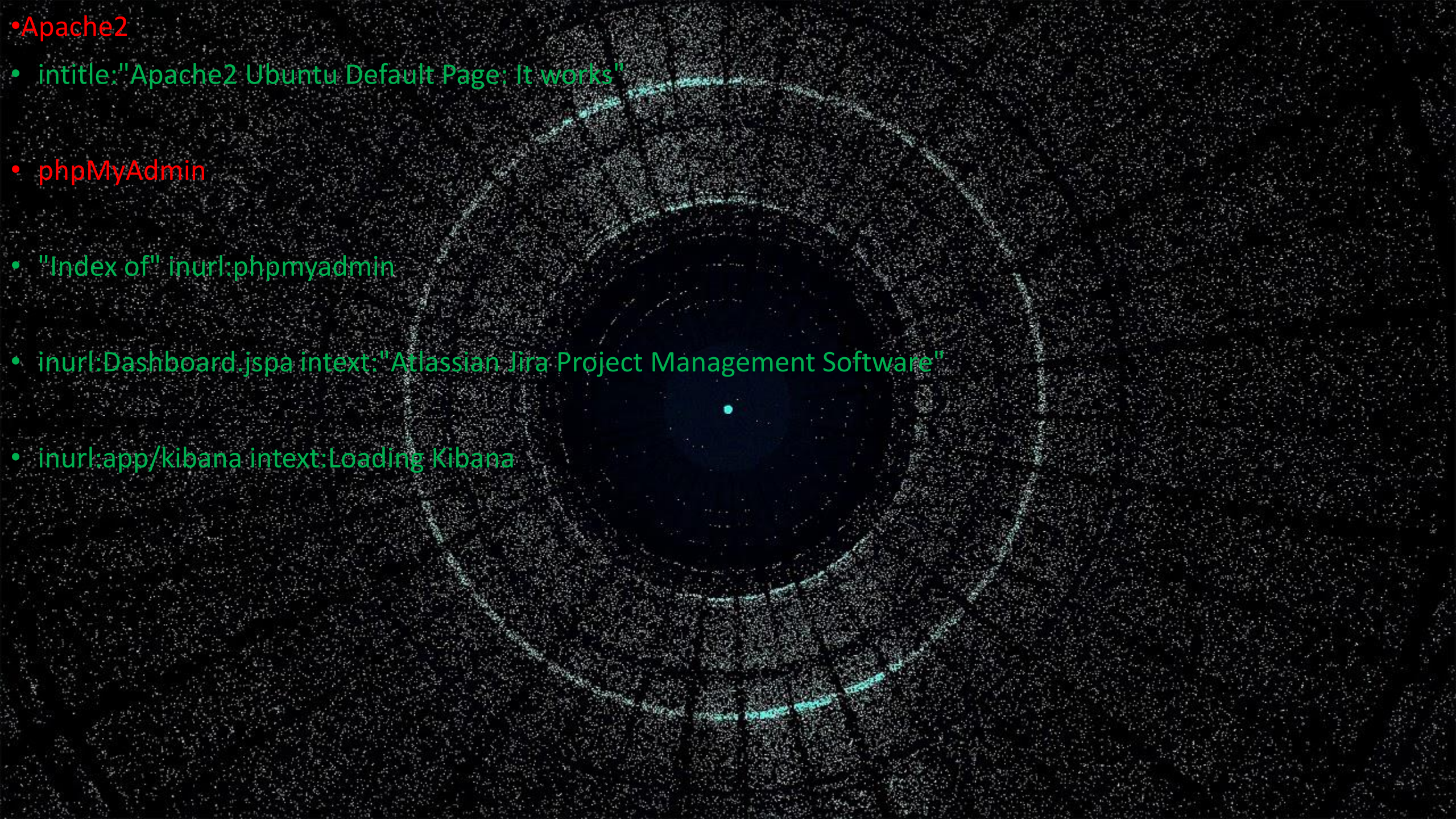
- Weather
- intitle:"Weather Wing WS-2"

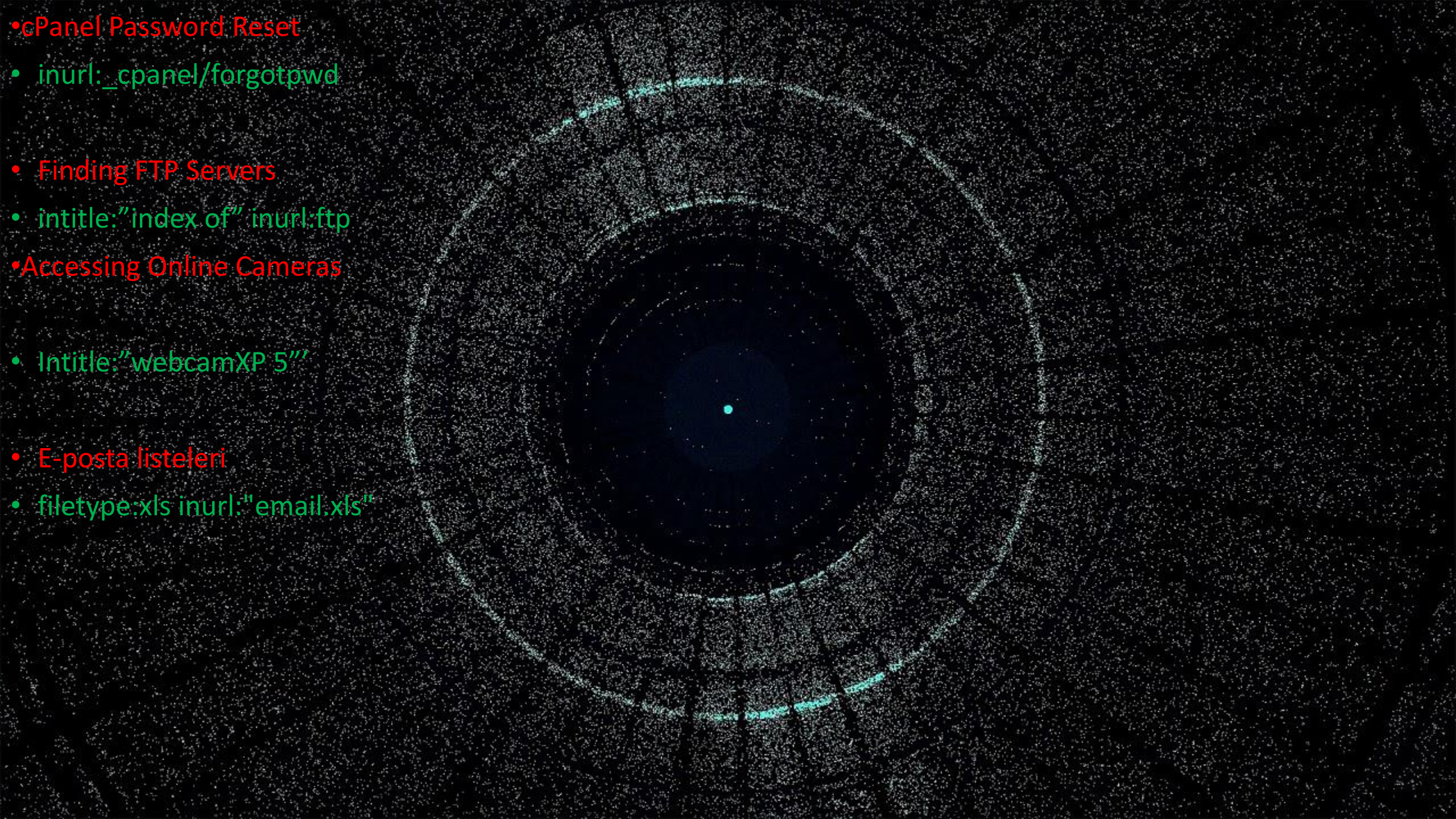
- Zoom Videos
- inurl:zoom.us/j and intext:scheduled for

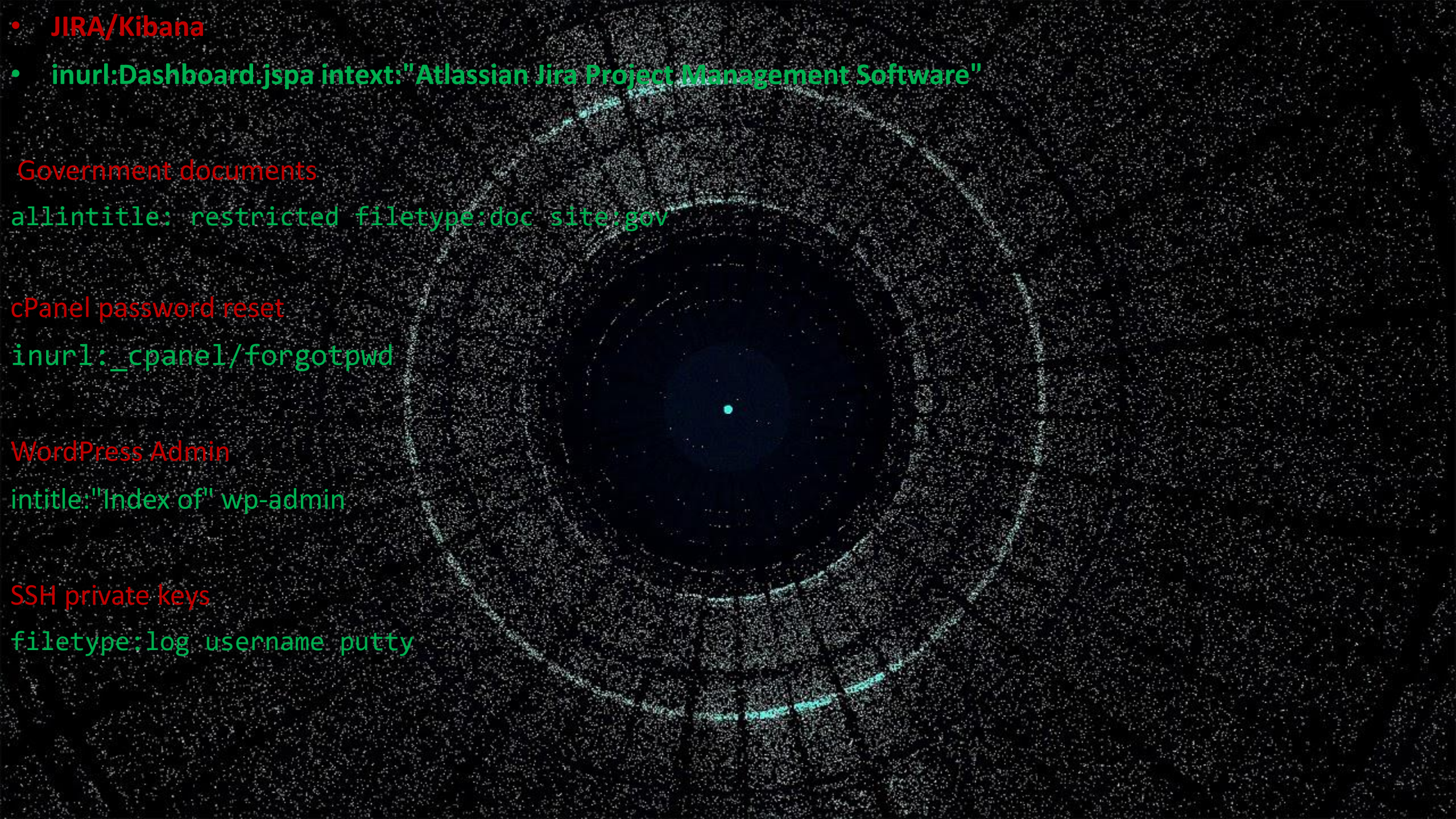
- SQL Dumps
- "index of" "database.sql.zip"

- intitle:"Index of" wp-admin


• Apache2
• intitle:"Apache2 Ubuntu Default Page: It works"
• phpMyAdmin
• "Index of" inurl:phpmyadmin
• inurl:Dashboard.jspa intext:"Atlassian Jira Project Management Software"
• ENV files
• DB_USERNAME filetype:env


•Apache2
• intitle:"Apache2 Ubuntu Default Page: It works"
• phpMyAdmin
• "Index of" inurl:phpmyadmin
• inurl:Dashboard.jspa intext:"Atlassian Jira Project Management Software"
• inurl:app/kibana intext:Loading Kibana


•cPanel Password Reset
• inurl:_cpanel/forgotpwd
• Finding FTP Servers
• intitle:”index of” inurl:ftp
•Accessing Online Cameras
• Intitle:”webcamXP 5”’
• E-posta listeleri
• filetype:xls inurl:"email.xls"


• JIRA/Kibana
• inurl:Dashboard.jspa intext:"Atlassian Jira Project Management Software"
Government documents
allintitle: restricted filetype:doc site:gov
cPanel password reset
inurl:_cpanel/forgotpwd
WordPress Admin
intitle:"Index of" wp-admin
SSH private keys
filetype:log username putty

# Pentesters için Arama Motorları

Metin.Onyphe.io (Servers)

.socradar.io (Threat Intelligence)

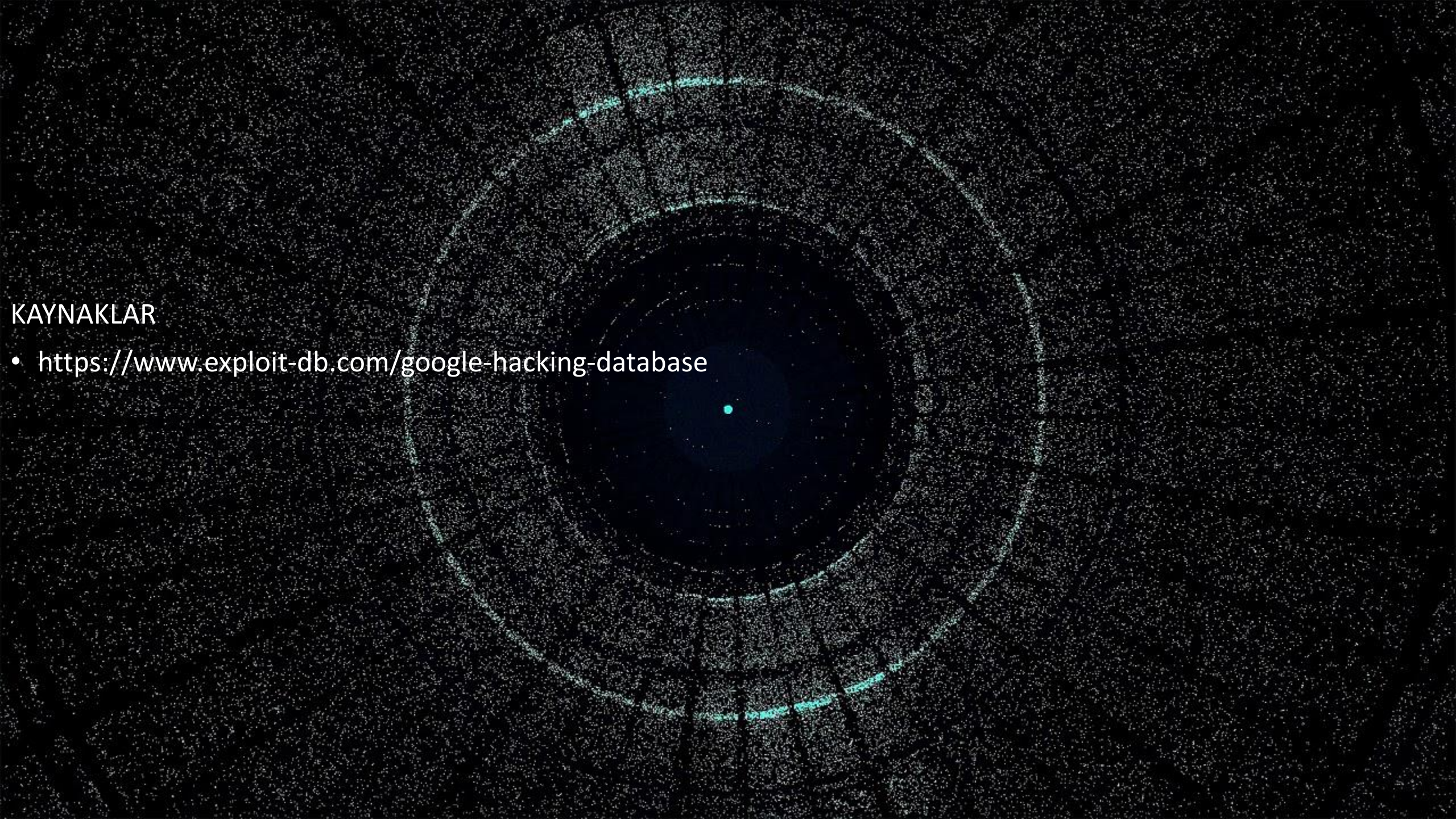
.binaryedge.io (Attack Surface)

.intelx.io (OSINT)

.crt.sh (Certificate search)

.vulners.com (vulnerabilities)

- .google.com (Dorks)
- .Shodan.io (Servers)
- .censys.io (Servers)
- .hunter.io (Mail addresses)
- .fullhunt.io (Attack Surface)



KAYNAKLAR

- https://www.exploit-db.com/google-hacking-database