Information Gathering (Reconnaissance)

Information Gathering (Reconnaissance)

Discovering Email Addresses
Discovery tools

• hunter.io for emails from a domain
• phonebook.cz for domains, email addresses and URLs from a domain
• Clearbit connect chrome extension for email search from a domain
• voilanorbert.com similar to hunter.io
• emailHIPPO for email verification

Use forgotten password links to confirm the email exists

Gathering Breached Credentials with Breach-Parse

Use breach-parse to pull credentials filtering by domain

Google Fu
Google is your best friend

Dorks

Use Google dorks to search for interesting domains/file extensions .

Extensions to look for:
• pdf
• csv
• xslx - spreadsheets
• db - database files

References:
• Operators
• Google Hacking DB

Examples:
• `site:example.com` filters by site
• `filetype:pdf` filters by file type
• `-www` remove string after -

Hunting Breached Credentials with DeHashed
DeHashed

Use DeHashed for powerful searches relating to emails, passwords, usernames, IP address, VIN number and more.

Think about using resources like DeHashed to tie usernames, passwords and emails together. The results may lead to other attack
vectors

Hunting Subdomains
Tools for Subdomain enumeration

• Sublist3r
• crt.sh for certificate based subdomain search, % is the wildcard
• OWASP amass in-depth network mapping and external asset discovery

Identifying Our Target
Using Tesla as a target from www.bugcrowd.com

Always read the terms/RoE very carefully!!

Tesla scope as of 2023-03-30

OUT OF SCOPE

Any domains from acquisitions, such as maxwell.com	• Website Testing
employeefeedback.tesla.com	• Website Testing
energysupport.tesla.com (you can report vulnerabilities to bugbounty.zoho.com)	• Website Testing
engage.tesla.com	• Website Testing
feedback.tesla.com	• Website Testing
feedback.teslamotors.com	• Website Testing
ir.teslamotors.com	• Website Testing
ir.tesla.com	• Website Testing
mkto.teslamotors.com	• Website Testing
shop.eu.teslamotors.com	• Website Testing
Any other third-party websites hosted by non-Tesla entities	• Website Testing

In Scope

Payment reward chart
P1 $3000 – $15000, P2 $500 – $3000, P3 $200 – $500, P4 $100 – $200

| A hardware product that you own or are authorized to test against (Vehicle/PowerWall/etc.) | • Hardware Testing |
| *.tesla.com | • Akamai CDN
• Varnish
• Drupal
• +3 |
| *.tesla.cn | • Akamai CDN
• Cloudflare CDN
• Varnish
• +5 |
*.teslamotors.com	• Website Testing
*.tesla.services	• Website Testing
*.teslainsuranceservices.com	• Website Testing
*.solarcity.com	• Website Testing
Any host verified to be owned by Tesla Motors Inc. (domains/IP space/etc.)	• Website Testing
Official Tesla Android apps	• Java

• Android
• Mobile Application Testing
• +1 |
| Official Tesla iOS apps | • Objective-C
• SwiftUI
• Swift
• +2 |

Identifying Website Technologies
Tools

• BuiltWith to discover what a website is built with, very in-depth and lots of info. Passive tool
• Wappalyzer to discover what a website is built with,. Semi-passive as it requires interaction with the site.
• WhatWeb to discover what a website is built with, shows headers and other info too. Semi-passive tool

Use a combination of tools to get as much info as possible!

Information Gathering with Burp Suite
Burp Suite

Use Burp to intercept requests to and from the website. The headers and site map that is generated from walking the website provide
valuable information.

Look out for:

• Languages used
• Services running
• CMS used
• Naming conventions of servers/resources
• Unique/special headers

Passive Reconnaissance Overview
Physical - Location information

• Satellite images
• Drone recon
• Building layout (badge readers, break areas, security, fencing)

Social - Job information

• Employees (name, job title, phone number, manager, etc.)
• Pictures(badge photos, desk photos, computer photos, etc.)

Web/Host

Target Validation:

• WHOIS
• nslookup
• dnsrecon

Finding Subdomains:

• Google Fu
• dig
• Nmap
• Sublist3r
• Bluto
• crt.sh
• etc.

Fingerprinting:

• Nmap
• Wappalyzer
• WhatWeb
• BuiltWith
• Netcat

Data Breaches:

• HaveIBeenPwned
• Breach-Parse
• WeLeakInfo

Utilizing Social Media
Look for photos!

LinkedIn
Twitter

Scrape company employees from LinkedIn with a python script

Input company name, HTTP request to grab listed employees, BeautifulSoup to parse HTML