

# What to hunt as beginner

Aditya Shende



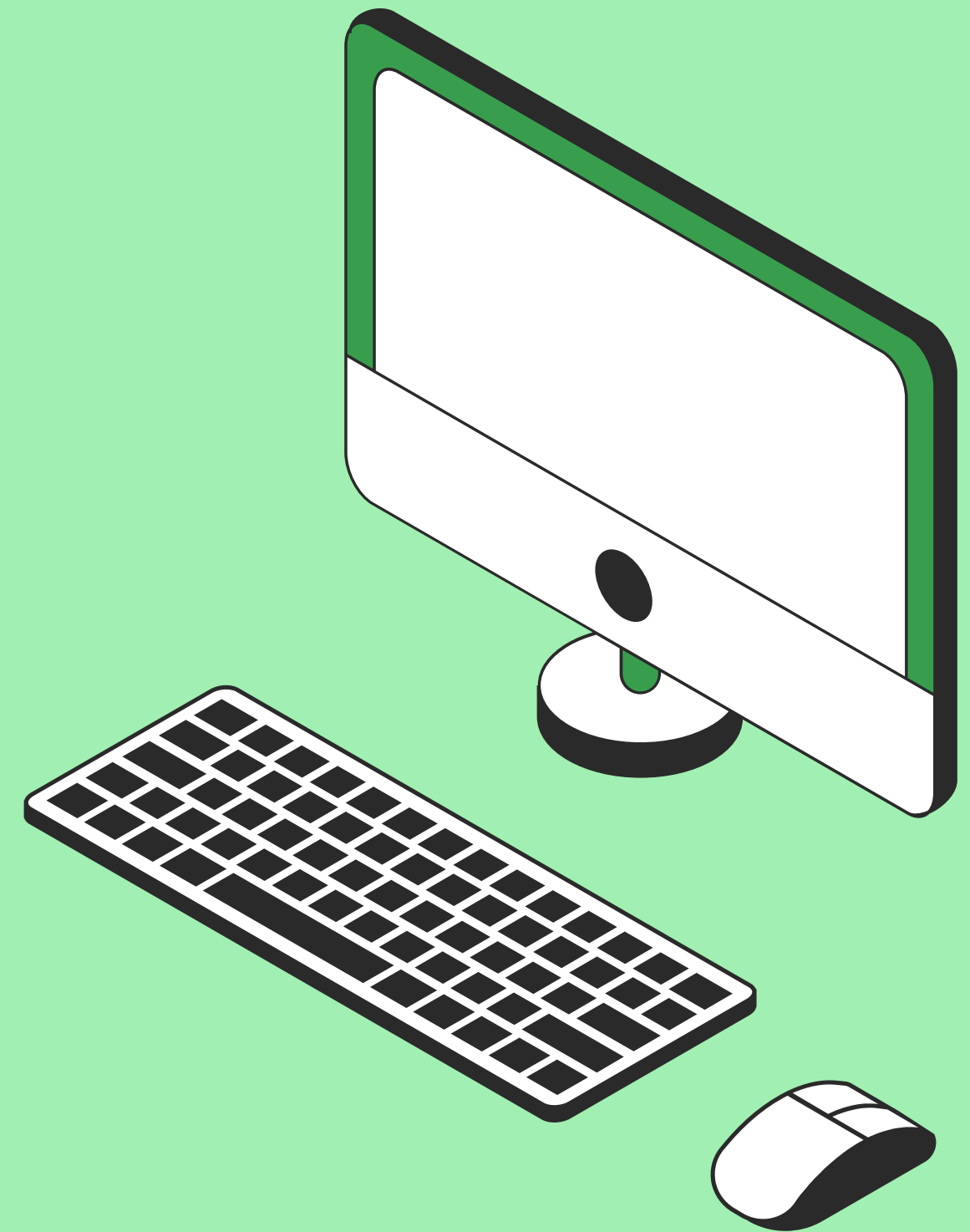
# WHO AM I ?

Indian

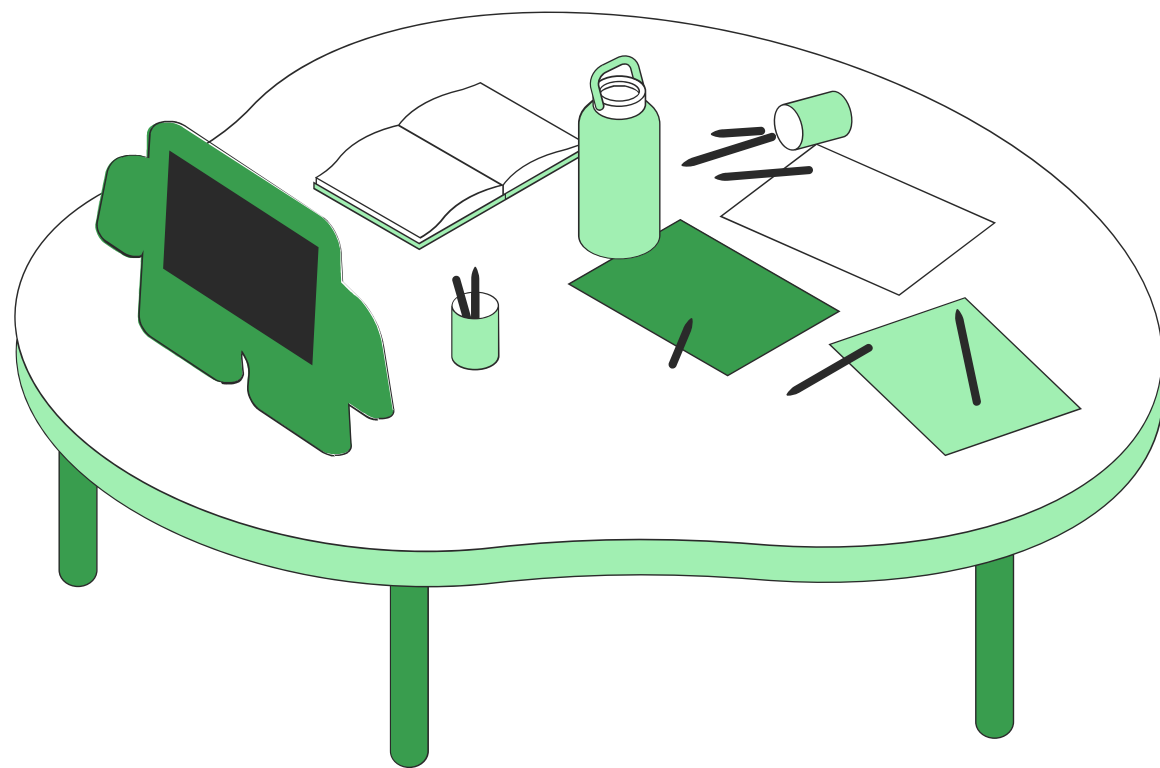
Bounty Hunter: Bugcrowd

Biker

Agri10x Red Team Ops



# Choosing Targets



Google Dorks

---

Github Repos

---

Choose VDPs

---

Hands on bugs over local sites

---

.nl websites for big scope

---

Different search engine , Different results

[All](#) [Images](#) [Videos](#) [Maps](#) [News](#) [Shopping](#)84 Results [Date](#) ▼

## Responsible Disclosure Statement

[https://www.idstation.online/Resources/Documents/Responsible Disc...](https://www.idstation.online/Resources/Documents/Responsible_Disc...) · PDF file

kwaliteit **van de melding met een minimum van een** waardebon van €50,-. Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost We strive to solve all problems as quickly as possible and we are happy to be involved in any publication about the problem after it has been resolved DPS – Digital ...

## Responsible Disclosure - PrivacyO

<https://www.privacyo.eu/responsible-disclosure> ▼

De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit **van de melding met een minimum van een** waardebon van €50,-. Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

## Responsible Disclosure - NIVO

<https://nivo.idfocus.nl/responsible-disclosure> ▼

De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit **van de melding met een minimum van een** waardebon van €50. Beloningen worden alleen uitgekeerd aan inwoners van de EU / EER. Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost. Vragen? ...

## bug-bounty-dorks/dorks.txt at master · sushiwushi/bug-bounty ...

<https://github.com/sushiwushi/bug-bounty-dorks/blob/master/dorks.txt> ▼

26/05/2021 · "van de melding met een minimum van een" -site:responsibledisclosure.nl: inurl:/security ext:txt "contact" inurl:responsible-disclosure-policy "Submission Form powered by Bugcrowd" -bugcrowd.com "If you believe you've found a security vulnerability" intext:"BugBounty" and intext:"BTC" and intext:"reward" intext:bounty inurl:/security: inurl:"bug bounty" and intext:"€" and inurl:/security:

[All](#) [News](#) [Shopping](#) [Images](#) [Videos](#) [More](#)[Past year](#) ▼ [All results](#) ▼ [Clear](#)<https://smartreach.io> › [responsible-disclosure](#) ▼

## Responsible Disclosure - SmartReach

07-Jan-2021 — Last updated: 7th January 2021. Reporting Guidelines. Reach out to support@smartreach.io, if you have found any potential vulnerability in our products ...

**Response type:** Time<https://api.docs.smartdata.io> › [new-worldline-com](#) › [home](#) ▼

## Responsible Disclosure Program - Worldline

18-Jan-2021 — We appreciate and encourage security researchers to contact us to report potential vulnerabilities identified in any product, system, or asset belonging to ...

## People also ask

[What is a responsible disclosure program?](#)[What companies use responsible disclosure?](#)[What is ethical disclosure?](#)<https://ledn.io> › [legal](#) › [responsible-disclosure-policy](#) ▼

## Responsible Disclosure Policy - Ledn | Financial services for ...

# Policy and scope checking



## **In scope bugs**

CSRF  
Auth Bypass  
Code Injections  
Unauth access  
etc

## **OOS bugs**

SPF  
DMARC  
Rate Limits  
Dos & Ddos  
Phishing  
User Interactions  
bugs

## **Policy Checks**

Reward  
Timeline  
Scope of domains  
Known Bugs

## **Report format**

-Do Not Use single template  
-Plagiarisms Checks  
-Attack scenarios

## Finallyyyyyyy!!!! BUGS to check...

1. CSRF : <https://portswigger.net/web-security/csrf>
2. MFA issues : Request , Response , Weak token cryptography
3. BAC attacks : <https://portswigger.net/web-security/access-control/>
4. Info Disclosure : Wayback, Github , Directory fuzzing, Error messages , Google Dorks
5. Exif Metadata : Stored Images , File Upload Functions , Posts



A photograph of a desk setup. On the left, a laptop with a dark screen and a gold-colored frame sits on a white desk. To its right is a small potted plant with green leaves, a white ceramic mug, and a blue notebook. The background is a plain white wall. The bottom left corner of the image shows a blue and white patterned fabric.

# CSRF

## Ways to find...

- Burpsuite extension : CSRF Scanner - Passive scanner where function dont have token validations , We can try for easy exploits
- Checking requests manually or simple burpsuite history
- If tokens are there ? -> Remove token , token parameter , replace with another account token , Change request methods



A photograph of a desk setup. On the left, a laptop with a dark screen and a gold-colored frame sits on a white desk. To its right is a small potted plant with green leaves in a grey pot, and a white ceramic mug. A white notebook is partially visible under the mug. The background is a plain white wall. In the bottom left corner, a portion of a blue and white patterned fabric is visible.

# MFA issue

## Ways to find...

- Common way - Brute forcing numericals
- Editing request or removing requests parameters
- Tampering response : eg . 400 Bad Request to 200 OK

More :

<https://twitter.com/ADITYASHENDE17/status/1254515923668439041?s=20>



```
POST /login-2fa HTTP/1.1
Host: user.site.com.au
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 185
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
{"tfaToken":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZmFVc2VySWQiOiJMcjNDk
sImhhdCxmMTA1MSwiZXhwIjoxNjI5MDEx
MzUxfQ.yrIYla1oldhfdhEWghG4ZAYiKk-
CVNjhYSZFSqRspMA","tfaCode":"123456
"}
```

```
HTTP/1.1 400 Bad Request
Date: Sun, 15 Aug 2021 07:09:55 GMT
Content-Type: application/json;
charset=utf-8
Content-Length: 69
Connection: close
X-Powered-By: Express
X-RateLimit-Limit: 30
X-RateLimit-Remaining: 29
X-RateLimit-Reset: 1629011456
Access-Control-Allow-Origin: *
Vary: Origin, Accept-Encoding
ETag: W/"45-
gL5aNU98r3aWMrxwsarUeo5GqI4"

{"label":"2fa-token-
expired","message":"An error
occurred","info":{}}
```

200 OK

```
{"success":true}
```



# Broken Access Control:

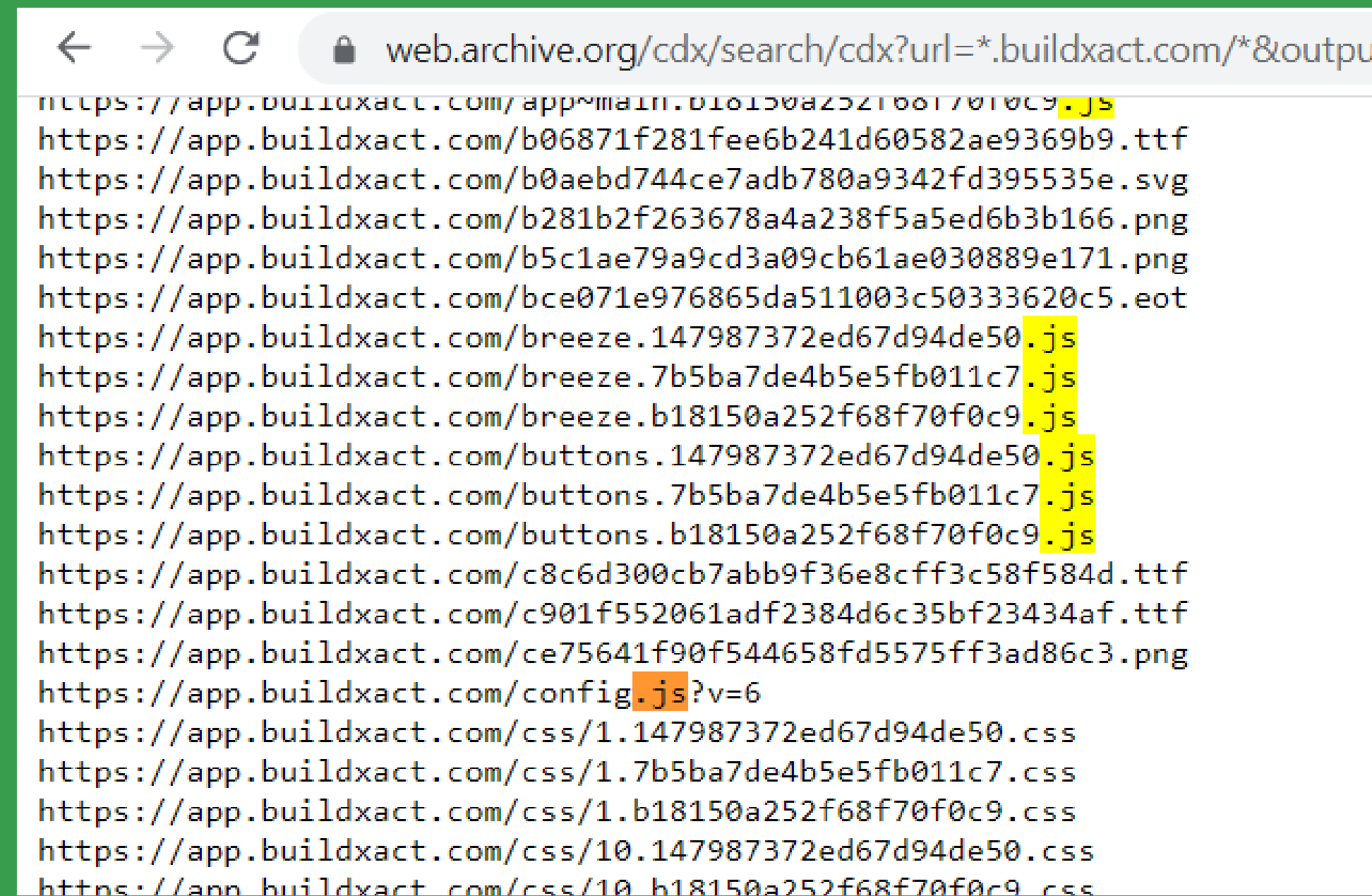
Abusing the mechanism of webapp where it can leads to Infomration Disclosure ,  
Unauth access, High privileges by low access level user

More : <https://adityashende17.medium.com/idor-to-information-disclosure-admin-account-takeover-6aa96798c70b>

Raw Params Headers Hex		
POST request to /WebGoat/attack		
Type	Name	Value
URL	Screen	141
URL	menu	200
Cookie	acopendivids	swingset,jotto,phpbb2,redmine
Cookie	acgroupswithpersist	nada
Cookie	PHPSESSID	tgslvf4vsi9b4uu4c87ha0nd12
Cookie	JSESSIONID	4B60973E12C4F6645FBE0D2E048C08FD
Body	employee_id	102
Body	action	ViewProfile

# Wayback....

1. JS endpoints
2. API paths
3. Unpredictable URLs
4. Open Redirection



A screenshot of a web browser showing search results from the Wayback Machine. The address bar displays the URL: `web.archive.org/cdx/search/cdx?url=*.buildxact.com/*&output`. Below the address bar, a list of URLs is shown, many of which are highlighted in yellow. The highlighted URLs include:

- `https://app.buildxact.com/app~main.b18150a252f68f70f0c9.js`
- `https://app.buildxact.com/breeze.147987372ed67d94de50.js`
- `https://app.buildxact.com/breeze.7b5ba7de4b5e5fb011c7.js`
- `https://app.buildxact.com/breeze.b18150a252f68f70f0c9.js`
- `https://app.buildxact.com/buttons.147987372ed67d94de50.js`
- `https://app.buildxact.com/buttons.7b5ba7de4b5e5fb011c7.js`
- `https://app.buildxact.com/buttons.b18150a252f68f70f0c9.js`
- `https://app.buildxact.com/config.js?v=6`
- `https://app.buildxact.com/css/1.147987372ed67d94de50.css`
- `https://app.buildxact.com/css/1.7b5ba7de4b5e5fb011c7.css`
- `https://app.buildxact.com/css/1.b18150a252f68f70f0c9.css`
- `https://app.buildxact.com/css/10.147987372ed67d94de50.css`
- `https://app.buildxact.com/css/10.b18150a252f68f70f0c9.css`



# **Github Recon = Juicy Information**

- Craft own dorks
- example : "password" for login
- Repo authority

<https://speakerdeck.com/aditya45/github-recon-and-way-to-process>

615

#1087489

Github access token exposure

Share: [f](#) [t](#) [in](#) [Y](#) [v](#)

SUMMARY BY SHOPIFY



On January 26, [@augustozanellato](#) reported that while reviewing a public MacOS app, they found a valid GitHub Access Token belonging to a Shopify employee. This token had read and write access to Shopify-owned GitHub repositories. Upon validating the report, we immediately revoked the token and performed an audit of access logs to confirm no unauthorized activity had occurred.

SUMMARY BY AUGUSTOZANELLATO



I was reviewing an Electron app made by one of Shopify employees (at the time I didn't know that Shopify was in any way involved), after extracting the `app.asar` file using `npx asar extract path/to/app.asar extracted/path` I found a `.env` file, initially I skipped it because I thought it just contained some app configuration stuff but after taking a look at the source it was clear that the app never loaded it. It was probably a leftover of the release building process.

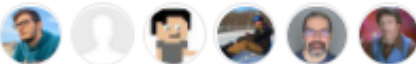
That `.env` contained a `GH_TOKEN` variable, which is (as you can probably guess) a GitHub token, I tried using it to authenticate against GitHub REST API using `curl -H "Authorization: token $GH_TOKEN" -H "Accept: application/vnd.github.v3+json" https://api.github.com/user`, I saw that the token was indeed valid so I decided to hit the `/user/orgs` API endpoint and I got back (among others) the Shopify organization, then I hit the `/orgs/Shopify/repos` endpoint to confirm the GitHub token scope and I successfully got back a list containing both Shopify public and private repos with `"permissions": {"admin": false, "push": true, "pull": true}` so at that point I knew that the token was enabling me to perform arbitrary push and pulls to Shopify repos so potentially permitting me to place backdoors and such.



Reported January 26, 2021 5:03am -0800

[augustozanellato](#)

Participants



State ● Resolved ()

Reported to [Shopify](#)

Disclosed July 26, 2021 12:50pm -0700

Severity 🔴 Critical (10.0)

Weakness *None*

Bounty \$50,000

CVE ID *None*


# Exif metadata

## Stored and Upload Function

[https://events.eurid.eu/media/upload/tedex\\_2012-2874.jpg](https://events.eurid.eu/media/upload/tedex_2012-2874.jpg)

Image URL fetched from  
waybackurls

← → ↺ ⚠ Not secure | exif.regex.info/exif.cgi



Click image to isolate; click this text to show histogram

Here's the full data:

XMP

Date Created	<b>2012:11:12</b> 15:23:25.20 8 years, 9 months, 3 days, 13 hours, 52 minutes, 57 seconds ago
XMP Toolkit	<a href="#">Adobe XMP Core</a> 5.5-c002 1.148022, 2012/07/15-18:06:45
Creator Tool	<a href="#">Adobe Photoshop Lightroom</a> 4.2 (Macintosh)
Create Date	<b>2012:11:12</b> 15:23:25.20 8 years, 9 months, 3 days, 13 hours, 52 minutes, 57 seconds ago
Modify Date	<b>2012:11:12</b> 17:18:51+01:00 8 years, 9 months, 3 days, 19 hours, 57 minutes, 31 seconds ago
Metadata Date	<b>2012:11:12</b> 17:18:51+01:00 8 years, 9 months, 3 days, 19 hours, 57 minutes, 31 seconds ago
Lens	14.0-24.0 mm f/2.8
Lens ID	146
Image Number	2905
Approximate Focus Distance	4,294,967,295



# Final things

Don't rush

Master in one . Practice all

Scope and policies are important

Think out of the box

*Thank  
you!*