Vulnerability Inheritance: Finding Bugs & Scoring bounties through 3rd party integrations

Third Party Integrations

- Why should we hunt on 3rd party integrations?
- Identify assets.
- Locate all bounty targets running a certain vulnerable components
- Create Nuclei Templates

Approaching Bug Bounty In 2021

- Which assets should we focus after reconnaisance?

Examples Of Third Party Integrations

- HTML Based

```
2. Analytics
3.Billing(Stripe)
```

- DNS Based

```
2.Blogs
3.Webinar(Big Maker)
4.Teaching(Moodle)
5.Survey(Monkey)
6.E-commerce(Shopify)
7. Marketing(Oracle Responsys)
```

Benifits

1. Varitey Of Services
2. Deploy & Forget strategy
3. One Bug Many Vulnerable Assets
4. Defence Mechanism are not enforced On DNS integrations

DNS Based Integrations Workflow

CNAME & A RECORDS

Recon Flow

```
First Phase
```

1. Subdomains Lookup
   [Passive, Active, Permutation]
2. Resolve
3. Extract CNAMES from the resolved domains

```
Second Phase
```

1. Google Dorks
2. Reverse CNAME Lookups
3. Customer Page
4. Path Fingerprinting (Nuclei)

Discover Vendors Integrated With Our Targets

Subdomain Reconnaissance

```
Passive Subdomain Lookup
```

1. Subfinder
2. Chaos
3. Amass
4. Crobat
5. Github Subdomains
6. Waybackurls

```
Active Subdomains Lookup
```

1.PureDNS
2.Assetnote wordlists

```
Permutated Subdomain Lookup
```

1. dnsgen

Resolve the collected subdomains

1. Create a file name resolver.txt
2. Extract cname using httpx

Two Choices

```
1. Find Unique Vulnerabilites
2. Probe the subdomains for known CNAME Related 1 days - ( Search
Exploitdb)
```

Discover Assets Maintained By A Vendor

```
Google Dorks
```

```
Case One
```

Find the common pattern
site: *.example.com

```
Case Two
```

"Powered By example.com"
intext: "Powered By example.com"

```
Case Three
```

Page Title
intitle: "Example Platform"

Reverse C-NAME Lookup

```
Service
```

1. Spyse
2. RAPID7
3. Shodan
4. FOFA
5. CENSYS

Customer Page

Vendors present their clients in the customer pages.

Path Fingerprinting - Weaponizing Nuclei

Creating Nuclei Templates

Attack Vectors

What Vulnerabilities Should Be Looked For

- XSS
- Open Redirects

Attack Vectors & Chaining For Impact**

DNS Misconfiguration

- Subdomain Takeover
- Dangling DNS Records

Client Side Vulnerabilites

- XSS
- Open Redirect
  Chains
- Business Logic Errors
- CORS Bypass
- Cookies Exfiltaration
- SSRF Bypasses
- OAUTH Bypasses

Proof Of Concept

hackerone.com/reports/1028396
hackerone.com/reports/1028332
hackerone.com/reports/1028345

Wayback URLS

```
Look for url parameter
```

grep ?url=

```
Look for wordpress json
```

grep -v wp-json

Crawling The Application For Vulnerable Endpoint

```
While signup using xss payload on the first & last name
Click on the view on browser
Might lead to XSS
```

Summary

1. Attacking Third Party Integrations - Profit & Fun
2. Reconnaisance [Critical Part Of Successful Bug Bounty Hunting]
3. Impact [Always try to chain bug to escalating impacts]
4. Anyone go for it