Major-1 Project

Sahil Singh

ERP : **6606395**

MAJOR PROJECT DOCUMENTATION

Bug Bounty Reconnaissance – Electronic Arts (EA)

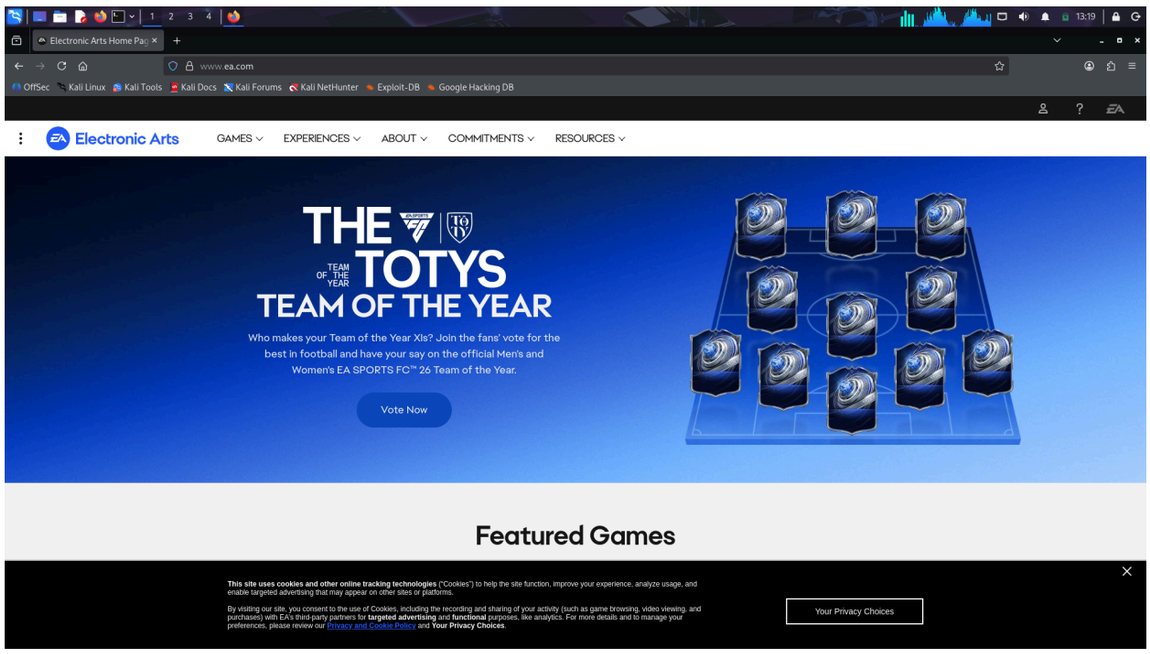
1. Main Domain Identification

Company Name: Electronic Arts (EA)

Main Domain: `ea.com`

Method Used:

The official EA website was identified using a Google search and verified through EA's homepage and contact information.

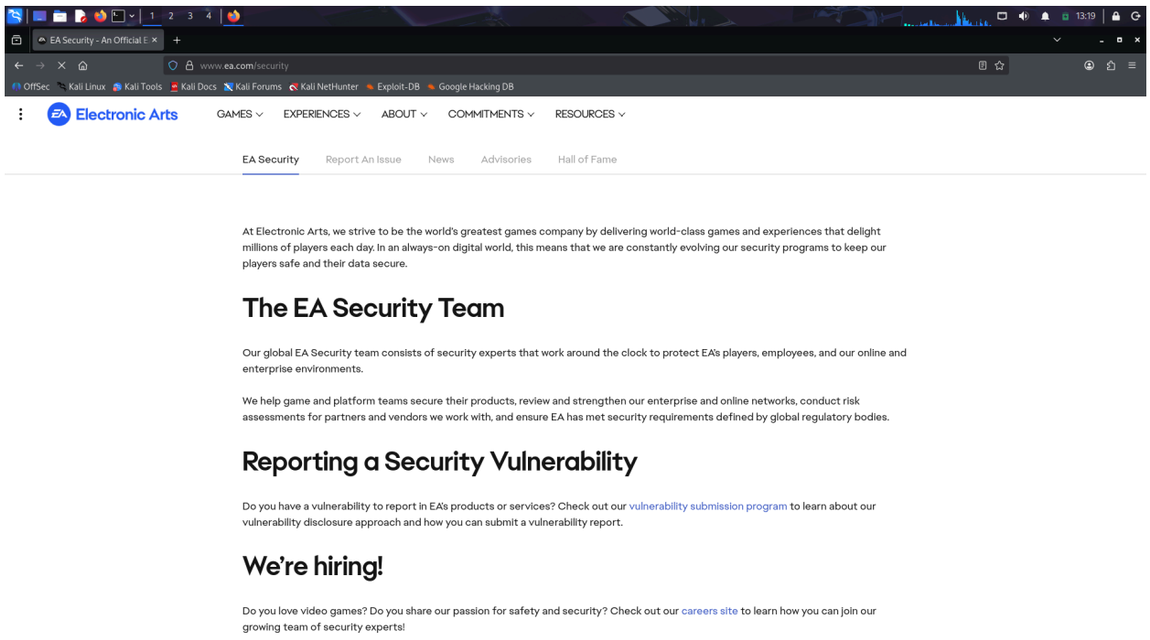


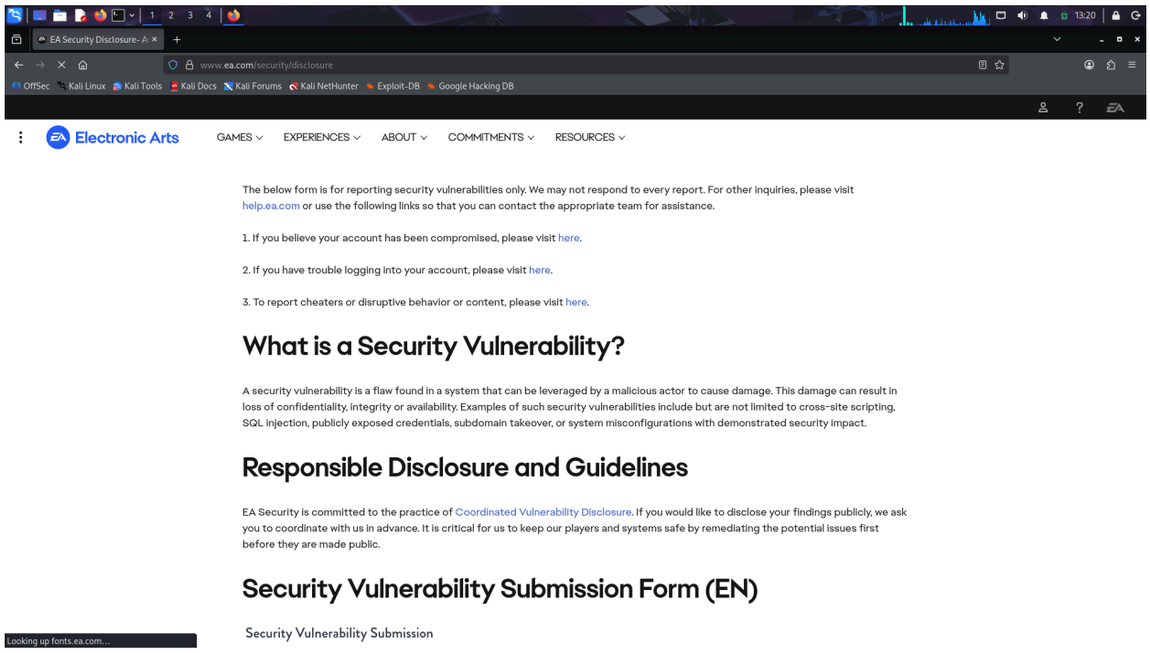
2. Bug Bounty / Vulnerability Disclosure Page

Electronic Arts maintains an official **Vulnerability Disclosure / Bug Bounty Program**, generally hosted on **HackerOne**.

Search Keywords Used:

> EA bug bounty
> Electronic Arts vulnerability disclosure





3. Bug Bounty Scope (In-Scope & Out-of-Scope)

In-Scope Assets (as defined by EA):

- `ea.com`
- EA-owned subdomains
- EA web applications and services

Out-of-Scope Assets:

- Third-party hosted services
- Social media platforms

- Customer-controlled environments

📸 **SCREENSHOT 3:**

➡️ “Scope / In-Scope / Out-of-Scope” section from EA’s bounty page

---

4. Ping Test (ICMP Reachability)

Objective:

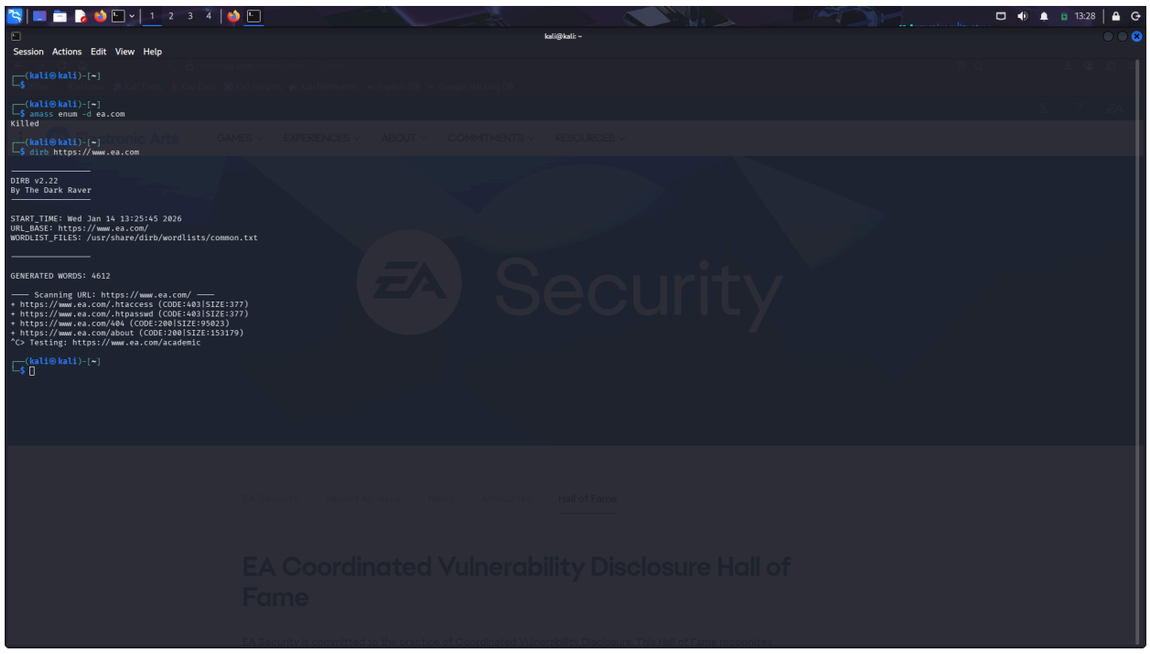
To check whether the EA main domain responds to ICMP requests.

Command Used:

```
ping ea.com
```

Observation:

ICMP responses may be blocked as a security measure.



---

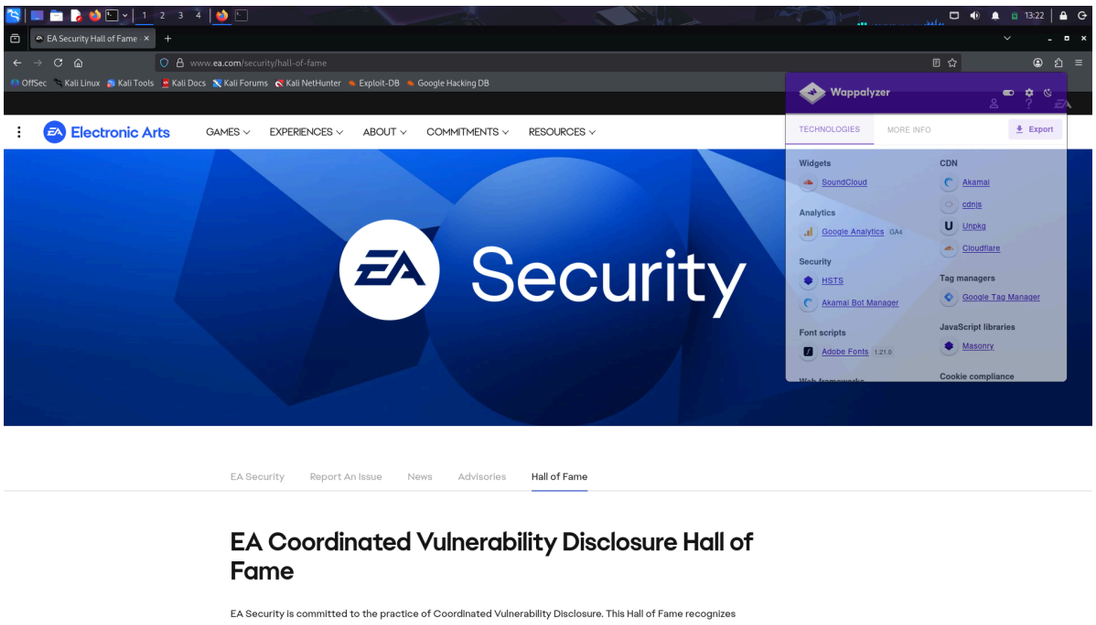
5. Technology Stack Identification (Main Domain)

Tool Used:

Wappalyzer (Browser Extension)

Technologies Identified May Include:

- Web server
- CDN (e.g., Akamai / Cloudflare)
- JavaScript frameworks
- Analytics tools



➡️ Wappalyzer results for https://www.ea.com

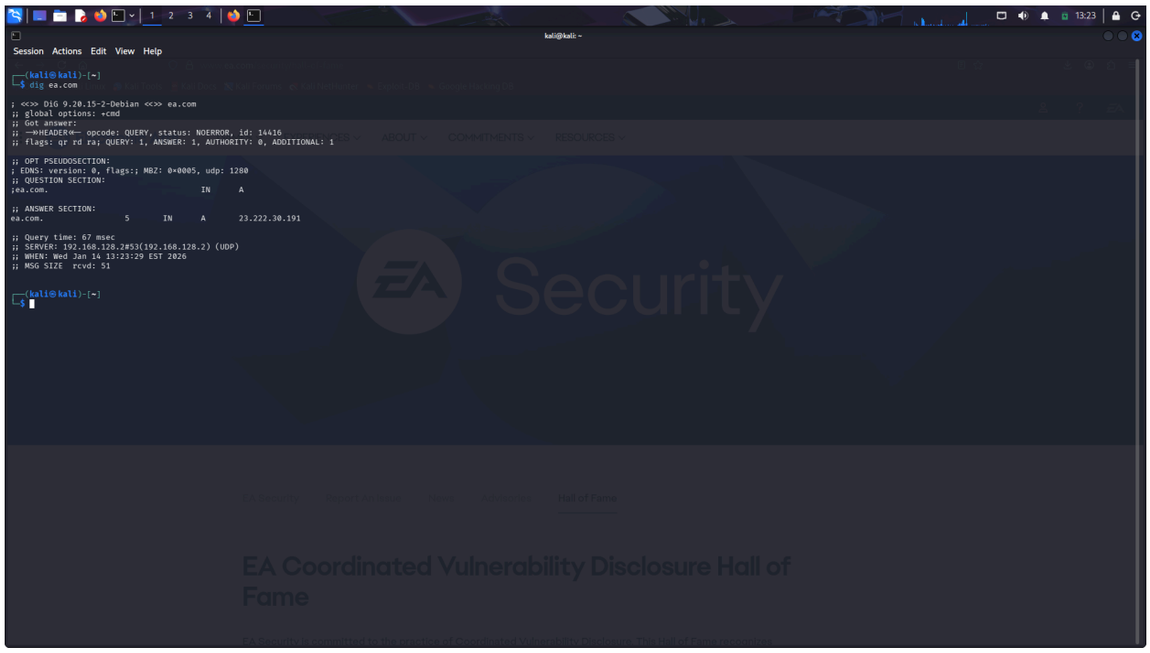
6. ASN Number and IP Range Identification

Objective:

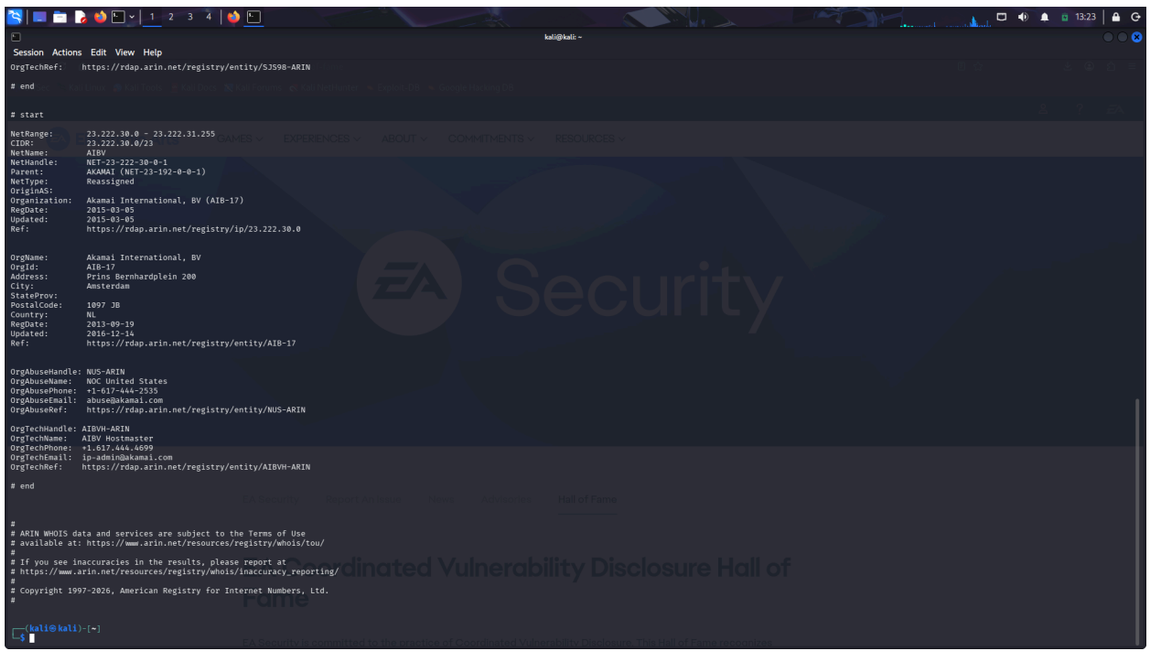
To identify the ASN and network ownership related to EA's infrastructure.

Commands Used:

```
dig ea.com
```




```
whois <IP_ADDRESS>
```



Information Collected:

- ASN Number
- Organization / ISP
- Netblocks

---

7. Subdomain Enumeration

Objective:

To discover publicly accessible EA subdomains.

Tool Used: `amass`

Command:

```
amass enum -d ea.com
```

---

8. Technology Stack on Subdomains

Selected Subdomains:

- `help.ea.com`
- `accounts.ea.com`
- `careers.ea.com`
- `answers.ea.com`
- `www.ea.com`

Each subdomain was analyzed using Wappalyzer to compare technology stacks.

---

9. Hidden Files & Directories (Main Domain Only)

⚠ Only the main domain was scanned (no subdomains)

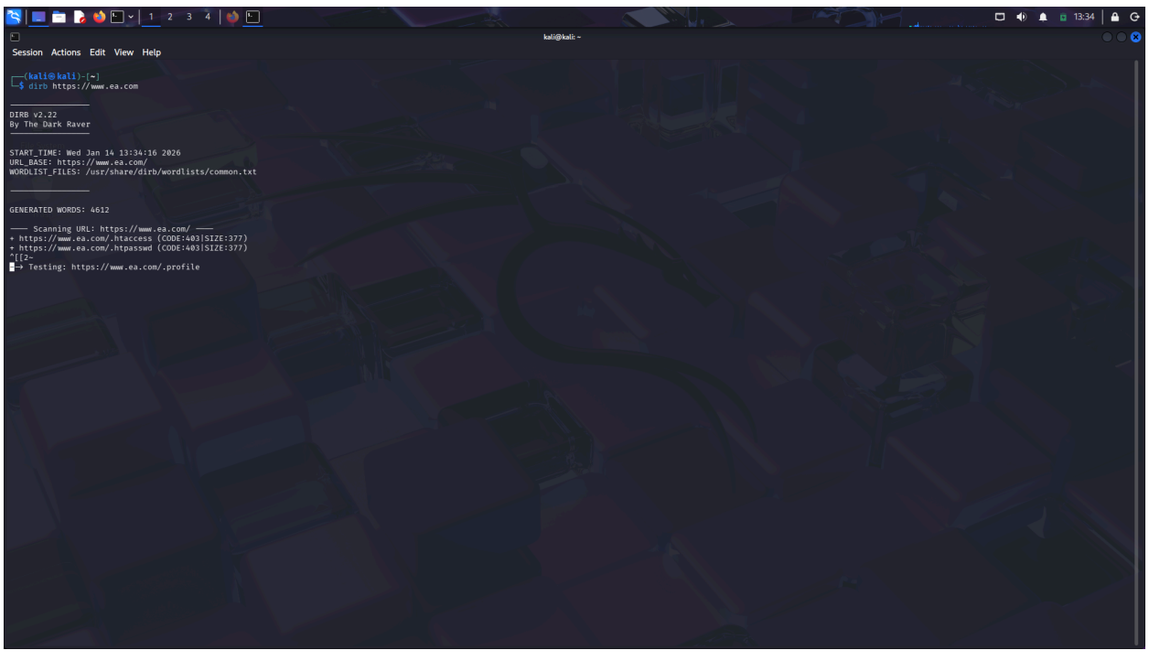
Tool Used: `dirb`

Command:

```
dirb https://www.ea.com
```

Observation:

Minimal or no directory exposure observed, indicating good security practices.



➡️ dirb scan output for `https://www.ea.com`

---

10. Declaration

I hereby declare that this project was carried out strictly for **educational purposes** and involved **reconnaissance-only activities**.

No exploitation, vulnerability abuse, or unauthorized access was performed, in compliance with EA's bug bounty policy and academic guidelines.