

# 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](http://ea.com)

**Method Used:**

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

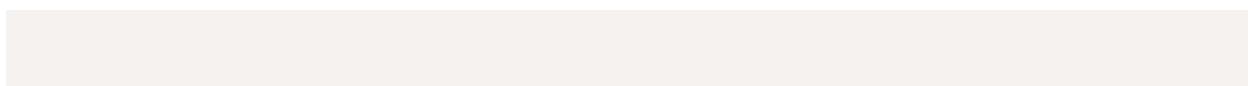


#### 2. Bug Bounty / Vulnerability Disclosure Page

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

**Search Keywords Used:**

EA bug bounty  
Electronic Arts vulnerability disclosure



EA Security - An Official E x +

www.ea.com/security

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Electronic Arts GAMES EXPERIENCES ABOUT COMMITMENTS RESOURCES

EA Security Report An Issue News Advisories Hall of Fame

At Electronic Arts, we strive to be the world's greatest games company by delivering world-class games and experiences that delight millions of players each day. In an always-on digital world, this means that we are constantly evolving our security programs to keep our players safe and their data secure.

## The EA Security Team

Our global EA Security team consists of security experts that work around the clock to protect EA's players, employees, and our online and enterprise environments.

We help game and platform teams secure their products, review and strengthen our enterprise and online networks, conduct risk assessments for partners and vendors we work with, and ensure EA has met security requirements defined by global regulatory bodies.

## Reporting a Security Vulnerability

Do you have a vulnerability to report in EA's products or services? Check out our [vulnerability submission program](#) to learn about our vulnerability disclosure approach and how you can submit a vulnerability report.

## We're hiring!

Do you love video games? Do you share our passion for safety and security? Check out our [careers site](#) to learn how you can join our growing team of security experts!

EA Security Disclosure- A x +

www.ea.com/security/disclosure

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Electronic Arts GAMES EXPERIENCES ABOUT COMMITMENTS RESOURCES

The below form is for reporting security vulnerabilities only. We may not respond to every report. For other inquiries, please visit [help.ea.com](#) or use the following links so that you can contact the appropriate team for assistance.

1. If you believe your account has been compromised, please visit [here](#).
2. If you have trouble logging into your account, please visit [here](#).
3. To report cheaters or disruptive behavior or content, please visit [here](#).

## What is a Security Vulnerability?

A security vulnerability is a flaw found in a system that can be leveraged by a malicious actor to cause damage. This damage can result in loss of confidentiality, integrity or availability. Examples of such security vulnerabilities include but are not limited to cross-site scripting, SQL injection, publicly exposed credentials, subdomain takeover, or system misconfigurations with demonstrated security impact.

## Responsible Disclosure and Guidelines

EA Security is committed to the practice of [Coordinated Vulnerability Disclosure](#). If you would like to disclose your findings publicly, we ask you to coordinate with us in advance. It is critical for us to keep our players and systems safe by remediating the potential issues first before they are made public.

## Security Vulnerability Submission Form (EN)

Looking up fonts.ea.com...

Security Vulnerability Submission

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

## In-Scope Assets (as defined by EA):

- [ea.com](http://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.

A screenshot of a Kali Linux terminal window titled 'kali㉿kali: ~'. The terminal displays a command-line interface for an 'anass enum' tool against the EA website ('ea.com'). The output shows the following commands and results:

```
[kali㉿kali: ~]$ anass enum -d ea.com
Killed
[kali㉿kali: ~]$ dirb https://www.ea.com
DIRB v2.22
By The Dark Raver

START TIME: Wed Jan 14 13:25:45 2026
URL BASE: https://www.ea.com/
WORDLIST FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
_____
-- Scanning URL: https://www.ea.com/ ____
> https://www.ea.com/.htaccess (CODE:403 |SIZE:377)
> https://www.ea.com/.htpasswd (CODE:403 |SIZE:377)
> https://www.ea.com/about (CODE:200 |SIZE:19562)
> https://www.ea.com/about/ (CODE:200 |SIZE:193179)
'C> Testing: https://www.ea.com/academic

[kali㉿kali: ~]$
```

The background of the terminal window features a watermark for 'EA Security' with a large EA logo.

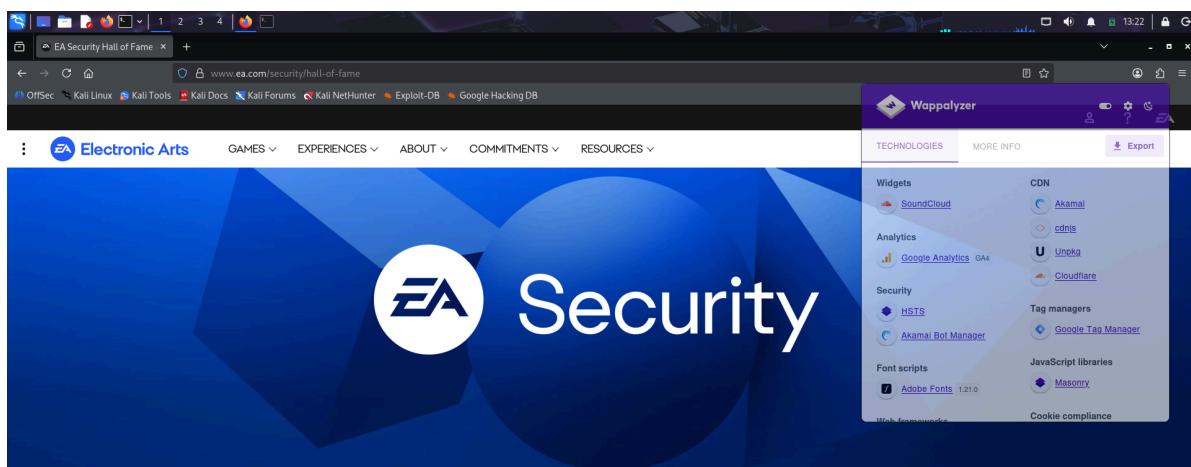
## 5. Technology Stack Identification (Main Domain)

## **Tool Used:**

## Wappalyzer (Browser Extension)

## **Technologies Identified May Include:**

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



EA Security Report An Issue News Advisories Hall of Fame

## EA Coordinated Vulnerability Disclosure Hall of Fame

EA Security is committed to the practice of Coordinated Vulnerability Disclosure. This Hall of Fame recognizes

➡ 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
```

```
(kali㉿kali)-[~] ~ % dig ea.com
; <>> DIG 9.20.15-2-Debian <>> ea.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 1416
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0+0005, udp: 1280
;; QUESTION SECTION:
;ea.com.           IN      A
;; ANSWER SECTION:
ea.com.          5       IN      A      23.222.30.191
;; Query time: 67 msec
;; SERVER: 192.168.128.2#53(192.168.128.2) (UDP)
;; WHEN: Wed Jan 14 13:23:29 EST 2026
;; MSG SIZE rcvd: 51

(kali㉿kali)-[~]
```

```
whois <IP_ADDRESS>
```

```

Session Actions Edit View Help
OrgTechRef: https://rdap.arin.net/registry/entity/SJ598-ARIN
# end
# start
NetRange: 23.222.30.0 - 23.222.31.255 CNAME: EXPERIENCES ABOUT COMMITMENTS RESOURCES
CIDR: 23.222.30.0/23
NetName: AIB
NetHandle: NET-23-222-30-0-1
Parent: AKAMAI (NET-23-192-0-0-1)
NetType: Reassigned
OrgName: Akamai International, BV (AIB-17)
RegDate: 2015-03-05
Updated: 2015-03-05
Ref: https://rdap.arin.net/registry/ip/23.222.30.0

OrgName: Akamai International, BV
OrgID: AIB-17
Address: Prins Bernhardplein 200
City: Amsterdam
StateProv: 1097 JB
Country: NL
RegDate: 2013-09-19
Updated: 2016-12-13
Ref: https://rdap.arin.net/registry/entity/AIB-17

OrgAbuseHandle: NUS-ARIN
OrgAbuseName: NOC United States
OrgAbusePhone: +1-617-444-2535
OrgAbuseEmail: abuse@akamai.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/NUS-ARIN

OrgTechHandle: AIBVH-ARIN
OrgTechName: AIBV Hostmaster
OrgTechPhone: +1-617-444-2535
OrgTechEmail: ip-admin@akamai.com
OrgTechRef: https://rdap.arin.net/registry/entity/AIBVH-ARIN

# end
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
# Copyright 1997-2026, American Registry for Internet Numbers, Ltd.
#

```

## 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)

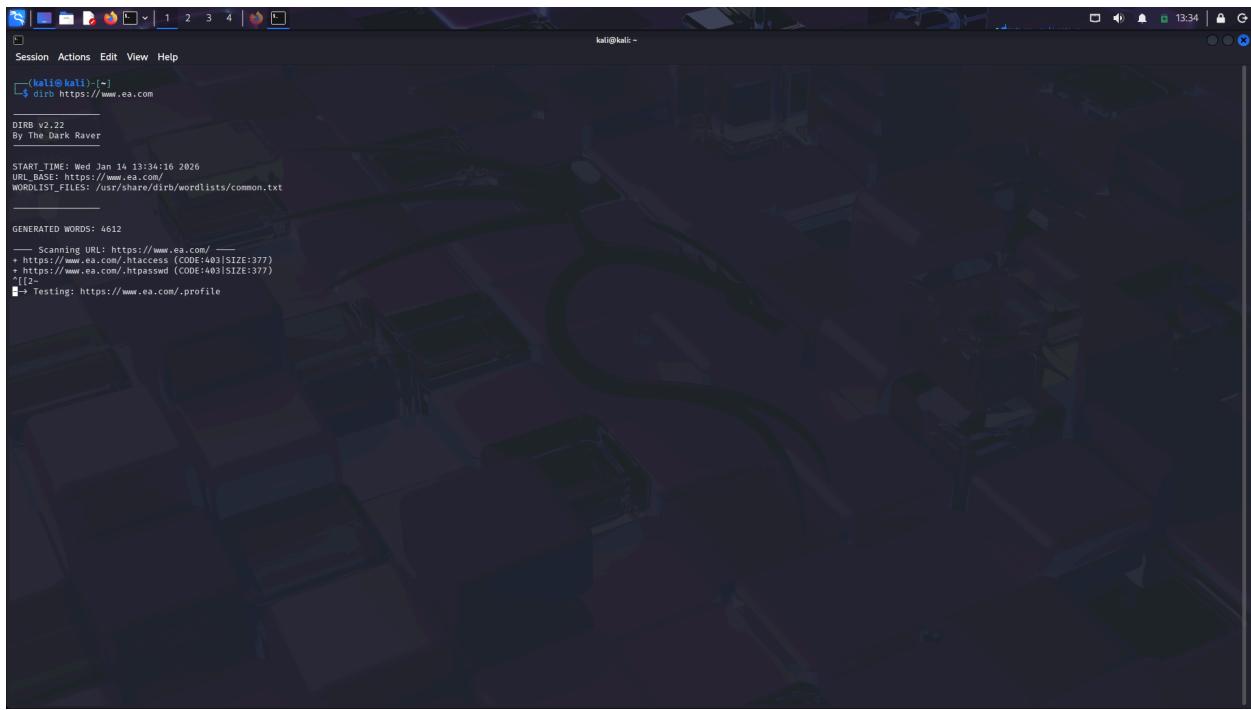
Tool Used: `dirb`

Command:

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

### Observation:

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



```
(kali㉿kali)-[~]
$ dirb https://www.ea.com

DIRB v2.22
By The Dark Raver

START_TIME: Wed Jun 14 13:34:16 2026
URL_BASE: https://www.ea.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
Scanning URL: https://www.ea.com/
+ https://www.ea.com/.htaccess (CODE:403|SIZE:377)
+ https://www.ea.com/.htpasswd (CODE:403|SIZE:377)
[[2-]] Testing: https://www.ea.com/.profile
```

➡ 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.