B.R.A.D. Project Plan — Bot to Report Abusive Domains

Methodology: Agile (5 Sprints)

Each sprint includes planning, development, testing, documentation updates, and a sprint review/retrospective.

Sprint 1: Core Setup & Initial Requirements

Duration: 1 – 28 May
Demo: Capstone Demo 1 (28 May)

Objectives

- Build the **User Submission Portal** for submitting suspicious URLs
- Allow the reporter to view forensic reports
- Allow the investigator to analyse forensic reports

Deliverables

- Web form to submit domains
- Multiple distinct dashboards to view and interact with the different use cases.
- `README.md`, feature list, requirements, and sprint plan

Sprint 2: Bot Integration & Forensic Data Collection

Duration: 29 May – 25 June
Demo: Capstone Demo 2 (25 June)

Objectives

- Develop **containerized scraping bot** to visit submitted domains safely
- Extract content and collect **forensic metadata** (IP, WHOIS, SSL, etc.)
- Store collected data securely
- Expand documentation with bot architecture and safety model

Deliverables

- Docker-based scraper that can visit and extract data
- Metadata collection (basic WHOIS, IP, domain details)
- Markdown documentation for bot internals

Sprint 3: AI Risk Analysis & Evidence Upload

Duration: 26 June – 20 August
Demo: Capstone Demo 3 (20 August)

Objectives

- Integrate **AI model** to score domain risk
- Enable **user evidence uploads** (screenshots, logs)
- Improve threat classification workflow
- Store all reports in a structured format

Deliverables

- Working AI model integration
- Evidence upload interface and backend
- Sample end-to-end report for one domain

Sprint 4: Investigator Dashboard & Threat Intelligence

Duration: 21 August – 28 September
Demo: Capstone Demo 4 (29–30 September)

Objectives

- Build the **Investigator Dashboard** to view/report/manage submissions
- Integrate **threat intelligence APIs** (e.g. VirusTotal)
- Add **automated WHOIS/DNS** fetching
- Begin **real-time alerting** for critical domains

Deliverables

- Usable dashboard UI (basic filters/search)
- Integration with external threat feeds
- Auto-fetched WHOIS/DNS info in report view

Sprint 5: Final Features, Polish & Project Day

Duration: 1 – 24 October
Event: Project Day (24 October)

Objectives

- Implement **historical tracking** for repeated abuse
- Add **multi-language support** (optional NLP integration)
- Apply security improvements: RBAC, API limits, immutable logs
- Prepare for final demo and handover

Deliverables

- Complete domain lifecycle tracking
- Final bugfixes and UI polish
- Project ready for public showcase

Capstone Milestones

Date	Event Description
28 May	Capstone **Demo 1** + Documentation Evaluations
25 June	Capstone **Demo 2** + Documentation Evaluations
20 August	Capstone **Demo 3** + Documentation Evaluations
29–30 September	Capstone **Demo 4 – Exam Demo** with COS 301 Project Committee
24 October	**Project Day** – Final Showcase