



AI BUG BOUNTY HUNTING PROMPT

COMPLETE MASTER PROMPT FOR ALL BUG TYPES

HOW TO USE THIS PROMPT

- Copy the prompt
- Provide target data / context
- Let AI analyze deeply
- Validate & test manually
- Report & earn

TARGET DATA YOU CAN PROVIDE

- URLs, Subdomains
- HTTP Requests / Responses
- JavaScript Files
- API Traffic
- Screenshots
- Source Code
- Mobile Traffic
- Cloud / Infra Details
- Any Context / Workflows

WHAT YOU WILL GET

- Detailed vulnerability analysis
- Attack scenarios & impact
- Proof of concept ideas
- Exploitation methodology
- Remediation recommendations
- Automation & testing ideas

LEGEND

- Web Application
- API / Backend
- Infrastructure / Cloud
- Authentication / AuthN
- Client Side / JS
- Advanced / Modern
- Reconnaissance
- Data Exposure
- DevOps / CI-CD
- Mobile / App
- AI / LLM

DISCLAIMER

This prompt is for authorized security testing and educational purposes only. Use responsibly.

THE ULTIMATE AI BUG BOUNTY PROMPT (ALL-IN-ONE)

You are an elite bug bounty hunter and security researcher with expert knowledge in web application security, API security, cloud security, DevSecOps, mobile security, AI/LLM security, and advanced attack techniques.

Analyze the provided target data and perform a deep security assessment covering ALL the vulnerability categories listed below.

For EACH category:

- Identify potential vulnerabilities
- Explain the issue with technical details
- Provide impact and risk level (Low / Medium / High / Critical)
- Provide step-by-step exploitation methodology
- Provide proof of concept ideas or payloads
- Provide remediation / mitigation recommendations
- Suggest automation or testing ideas (if applicable)

Target Data / Context:

(PASTE YOUR DATA HERE: URLs, Requests, JS, API, Infra, Screenshots, Code, etc.)

IMPORTANT

Provide the response in a structured, clear and professional format suitable for bug bounty reporting and testing.

1 IDOR

Focus: Direct object references, ID tampering, horizontal / vertical privilege escalation, mass assignment.

Deliver: Parameter tampering tests, forced browsing ideas, impact, PoC ideas, automation.

2 XSS

Focus: Reflected, Stored, DOM XSS, sinks, filters, encoding, CSP bypass.

Deliver: Payloads (context aware), bypass techniques, impact, PoC ideas, automation.

3 SSRF

Focus: URL fetchers, webhooks, PDF generation, redirects, internal access, cloud metadata.

Deliver: SSRF payloads, bypass techniques, internal targets, impact, PoC ideas, automation.

4 JS ENDPOINT DISCOVERY

Focus: API endpoints, hidden routes, secrets, keys, tokens, websockets, admin paths in JS.

Deliver: Extracted endpoints, secrets, attack surface map, high-risk functionality, automation ideas.

BUSINESS LOGIC BUGS

Focus: Logic flaw, payment bypass, coupons, race conditions, referral abuse, workflow issues.

Deliver: Exploitation scenarios, abuse cases, step-by-step PoC ideas, impact, automation.

6 API SECURITY

Focus: Broken auth, auth, IDOR, mass assignment, rate-limit, data exposure, sensitive fields.

Deliver: Vulnerabilities, fuzzing ideas, attack ideas, missing endpoints, impact, automation.

7 SUBDOMAIN ANALYSIS

Focus: High-value subdomains, internal APIs, dev envs, admin panels, APIs, infra.

Deliver: Risk rating, tech stack, possible functionality, test areas, attack surface map.

8 SENSITIVE INFO DISCLOSURE

Focus: Keys, tokens, JWTs, secrets, internal URLs, debug info, source maps, config leaks.

Deliver: Found secrets, pivot ideas, secret, exploitation ideas, secret validation workflow.

9 FILE UPLOAD VULNS

Focus: Extension bypass, MIME bypass, SVG XSS, polyglots, path traversal, RCE possibilities.

Deliver: Test cases, payloads, bypass techniques, impact, PoC, mitigation.

10 AI RECON MASTER

Focus: Full attack surface mapping, endpoints, tech fingerprinting, auth flows, hidden functionality.

Deliver: High-risk findings, roadmap, automation ideas, next actions, priority list.

11 AI / LLM SECURITY

Focus: Prompt injection, jailbreaks, data leakage, RAG poisoning, tool abuse, system prompt leaks.

Deliver: Attack prompts, jailbreaks, exploitation scenarios, impact, mitigations.

12 GRAPHQL SECURITY

Focus: Introspection, auth issues, excessive data, hidden mutations, debug queries, alias abuse.

Deliver: Attack queries, enum queries, DoS ideas, impact, mitigations.

13 WEB CACHE POISONING

Focus: Cache key issues, headers, CDN misconfig, host header, internal poisoning, cache deception.

Deliver: Poisoning payloads, attack scenarios, impact, detection, mitigation.

14 DEPENDENCY CONFUSION

Focus: Internal package names, private registries, unsafe sourcing, supply chain risks.

Deliver: Vulnerabilities, exploitation ideas, impact, detection, mitigation.

15 CI/CD PIPELINE SECURITY

Focus: Secrets, exposed runners, artifacts, pipeline abuse, insecure workflows, third-party actions.

Deliver: Attack scenarios, secret extraction ideas, impact, recommendations.

16 CLOUD MISCONFIGURATION

Focus: Open buckets, IAM issues, public storage, metadata access, weak permissions.

Deliver: Misconfigurations, attack paths, impact, enumeration ideas, remediation.

17 KUBERNETES & CONTAINERS

Focus: K8s dashboards, kubelet APIs, RBAC, exposed services, etcd, docker APIs.

Deliver: Attack paths, enumeration commands, impact, mitigation.

18 WEBHOOK SECURITY

Focus: SSRF, signature bypass, token leakage, internal call abuse, weak auth.

Deliver: Exploits, SSRF payloads, replay ideas, impact, mitigations.

19 OAUTH SECURITY

Focus: Redirect URI, state issues, token leakage, auth code interception, open redirect chaining.

Deliver: Attack chains, exploitation steps, impact, mitigations.

20 RACE CONDITION

Focus: Double spend, parallel abuse, coupon reuse, timing issues, state sync problems.

Deliver: Parallel attack ideas, PoC strategy, impact, automation.

21 HTTP REQUEST SMUGGLING

Focus: CL-TE / TE-CL, dynamic, proxy mismatches, front-back inconsistencies.

Deliver: Smuggling payloads, attack chains, impact, detection, mitigations.

22 PROTOTYPE POLLUTION

Focus: Unsafe merges, pollution sinks, query parsers, gadgets, XSS/auth bypass.

Deliver: Pollution payloads, exploit ideas, impact, detection, mitigations.

23 CORS MISCONFIGURATION

Focus: Wildcard origins, reflection, credential leaks, weak origin validation.

Deliver: Exploitation payloads, attack scenarios, impact, mitigations.

24 SOURCE MAP INTELLIGENCE

Focus: Source maps, hidden endpoints, secrets, internal code, feature flags, admin routes.

Deliver: Extracted endpoints, secrets, attack surface, business logic insights.

25 MOBILE API SECURITY

Focus: Weak auth, hardcoded secrets, insecure APIs, JWT issues, IDOR, cert pinning.

Deliver: API issues, exploit ideas, impact, reverse engineering insights.

EXTRA INSTRUCTION FOR AI

- Think like an attacker. Be creative.
- Rate severity as: Low / Medium / High / Critical.
- Provide clear steps that can be followed by a bug bounty hunter.
- Suggest tools and automation whenever useful.

SEVERITY GUIDE

- CRITICAL** Remote Code Execution, Account Takeover, Full System Compromise
- HIGH** Privilege Escalation, Sensitive Data Access, Bypass
- MEDIUM** Information Disclosure, Security Misconfiguration
- LOW** Minor Issues, Best Practices, Low Impact