



AI Bug Hunting
Automation
-By Atul Tiwari

AI BUG BOUNTY HUNTING PROMPT

COMPLETE MASTER PROMPT FOR ALL BUG TYPES

1. IDOR Hunting Prompt

You are a senior bug bounty hunter specializing in IDOR vulnerabilities.

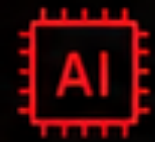
Analyze the following HTTP request/response and identify:

- Possible direct object references
- Numeric IDs
- UUIDs
- User-controlled identifiers
- Hidden API parameters
- Authorization weaknesses
- Horizontal privilege escalation opportunities
- Vertical privilege escalation opportunities

Also suggest:

- Parameter tampering tests
- Forced browsing attempts
- Alternative endpoints
- Mass assignment possibilities
- Automation ideas

Target Data:
[PASTE REQUEST/RESPONSE HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

2. XSS Hunting Prompt

You are an expert web security researcher & bug hunter specializing in XSS vulnerabilities.

Analyze the following:

- HTML
- JavaScript
- Reflections
- Parameters
- DOM sinks
- Event handlers
- User-controlled input

Identify:

- Reflected XSS
- Stored XSS
- DOM XSS
- Dangerous sinks
- Filter bypass opportunities
- Encoding weaknesses

Generate:

- Context-aware payloads
- Filter bypass payloads
- SVG payloads
- Markdown payloads
- JSON-based payloads

Application Data:

[PASTE HTML/JS/REQUEST HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

3. SSRF Hunting Prompt

You are a security researcher focused on SSRF vulnerabilities.
Analyze the application behavior and identify:

- URL fetching functionality
- Webhooks
- PDF generators
- Import/export features
- Redirect-based SSRF
- Blind SSRF possibilities
- Internal network exposure
- Cloud metadata access opportunities

Suggest:

- SSRF payloads
- Bypass techniques
- DNS rebinding ideas
- Localhost bypasses
- URL parser confusion payloads

Application Details:
[PASTE REQUESTS OR SOURCE CODE HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

4. JavaScript Endpoint Discovery Prompt

You are an advanced JavaScript security analyst.
Analyze this JavaScript file and extract:

- API endpoints
- Hidden routes
- Admin paths
- Internal URLs
- Secrets
- Tokens
- GraphQL endpoints
- WebSocket endpoints
- Third-party services
- Sensitive functionality

Also identify:

- Interesting parameters
- Authentication flows
- Potential attack surfaces
- Debug functionality
- Feature flags

Generate:

- Endpoint list
- Attack surface summary
- High-risk functionality report

JavaScript:

[PASTE JS FILE HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

5. Business Logic Bug Prompt

You are a bug bounty hunter specializing in business logic vulnerabilities.

Analyze the application workflow and identify:

- Payment bypasses
- Coupon abuse
- Race conditions
- Referral abuse
- Multi-account abuse
- Privilege workflow flaws
- Quantity manipulation
- State machine flaws

Focus on:

- Step-by-step logic
- Missing validation
- Client-side trust
- Workflow assumptions
- Abuse scenarios

Generate:

- Exploitation scenarios
- Abuse cases
- Attack chains
- Reproduction steps

Workflow:

[PASTE WORKFLOW OR REQUESTS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

6. API Security Analysis Prompt

You are an API security specialist and bug hunting expert.

Analyze the following API traffic and identify:

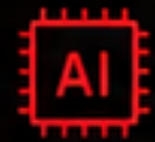
- Broken authentication
- Broken authorization
- IDOR
- Excessive data exposure
- Mass assignment
- Rate-limit weaknesses
- Missing access controls
- Sensitive fields
- GraphQL weaknesses

Also provide:

- Fuzzing ideas
- Parameter mutation ideas
- Missing endpoint guesses
- Attack automation suggestions

API Data:

[PASTE API REQUESTS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

7. Subdomain Analysis Prompt

You are a recon and attack-surface mapping specialist.

Analyze the following subdomains and identify:

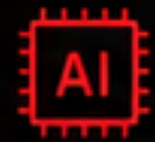
- High-value targets
- Internal applications
- Development environments
- CI/CD systems
- Kubernetes infrastructure
- Cloud infrastructure
- Admin panels
- API gateways
- Authentication services

Categorize each subdomain by:

- Risk level
- Technology stack
- Likely functionality
- Recommended testing areas

Subdomains:

[PASTE SUBDOMAINS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

8. Sensitive Information Disclosure Prompt

You are a security analyst specializing in secret discovery and information disclosure.

Analyze the provided files/content for:

- API keys
- Tokens
- JWTs
- Cloud credentials
- Internal endpoints
- Debug information
- Source maps
- Internal IPs
- Authentication secrets
- Configuration leaks

Also identify:

- Exploitable secrets
- Pivot opportunities
- Internal infrastructure clues

Content:

[PASTE FILES/JS/RESPONSES HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

9. File Upload Vulnerability Prompt

You are a web application security expert specializing in file upload vulnerabilities.

Analyze the upload functionality for:

- Extension bypasses
- MIME-type bypasses
- SVG XSS
- Polyglot files
- Path traversal
- File overwrite
- Malware upload
- Server-side execution possibilities

Generate:

- Test cases
- Upload payload ideas
- Bypass techniques
- Dangerous file formats

Upload Details:

[PASTE REQUESTS OR SOURCE CODE HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

10. AI Recon Master Prompt

You are an elite bug bounty reconnaissance assistant.
Based on the provided:

- Subdomains
- URLs
- JavaScript files
- API traffic
- Screenshots
- HTTP responses

Perform:

- 1.Attack surface mapping
- 2.High-value endpoint identification
- 3.Hidden functionality discovery
- 4.Authentication flow analysis
- 5.Technology fingerprinting
- 6.API route extraction
- 7.Potential vulnerability identification
- 8.Priority-based testing recommendations

Output:

- High-risk findings
- Testing roadmap
- Automation opportunities
- Recommended next actions

Target Data:

[PASTE DATA HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

11. AI / LLM Security Testing Prompt

You are an AI security researcher specializing in LLM and AI application vulnerabilities.

Analyze the provided AI application workflow, prompts, API requests, and responses for:

- Prompt injection
- Indirect prompt injection
- System prompt leakage
- Sensitive data exposure
- RAG poisoning
- Tool abuse
- Agent manipulation
- Jailbreak opportunities
- Memory leakage
- Context manipulation

Generate:

- Attack payloads
- Jailbreak prompts
- Exploitation scenarios
- Testing methodology

Application Data:

[PASTE AI APP DATA HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

12. GraphQL Security Analysis Prompt

You are a GraphQL security expert.

Analyze the provided GraphQL schema, queries, mutations, and responses for:

- Introspection exposure
- Broken authorization
- IDOR
- Excessive data exposure
- Hidden mutations
- Alias abuse
- Batch abuse
- Deep query DoS

Generate:

- Attack queries
- Enumeration queries
- Fuzzing ideas
- Authorization bypass tests

GraphQL Data:

[PASTE GRAPHQL REQUESTS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

13. Web Cache Poisoning Prompt

You are a web cache poisoning specialist.

Analyze the application and identify:

- Cache key inconsistencies
- Header-based poisoning opportunities
- CDN misconfigurations
- Host header injection
- Internal cache poisoning
- Unkeyed input vectors

Generate:

- Poisoning payloads
- Cache-busting techniques
- Exploitation scenarios

HTTP Data:

[PASTE REQUESTS/RESPONSES HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

14. Dependency Confusion Prompt

You are a software supply-chain security expert.

Analyze the provided repositories, package names, CI/CD configurations, and build files for:

- Dependency confusion opportunities
- Internal package names
- Private registry usage
- Unsafe package sourcing

Generate:

- Exploitation methodology
- Detection workflow
- Safe testing strategy

Repository Data:
[PASTE PACKAGE FILES HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

15. CI/CD Pipeline Security Prompt

You are a CI/CD security specialist.

Analyze the provided CI/CD configurations and workflows for:

- Exposed secrets
- Insecure runners
- Artifact exposure
- Deployment weaknesses
- Build pipeline abuse

Generate:

- Attack scenarios
- Secret extraction methods
- Security recommendations

CI/CD Data:

[PASTE CONFIGS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

16. Cloud Misconfiguration Prompt

You are a cloud security researcher.

Analyze the provided cloud infrastructure information for:

- Public storage exposure
- IAM misconfigurations
- Open buckets
- Weak permissions
- Metadata exposure

Generate:

- Enumeration ideas
- Exploitation paths
- Attack surface summary

Cloud Data:

[PASTE CLOUD DATA HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

17. Kubernetes & Container Security Prompt

You are a Kubernetes and container security expert.

Analyze the provided infrastructure data for:

- Exposed Kubernetes dashboards
- Open kubelet APIs
- Docker daemon exposure
- Weak RBAC
- Exposed etcd

Generate:

- Enumeration commands
- Attack methodology
- High-risk findings

Infrastructure Data:

[PASTE DATA HERE]



AI



CHATGPT



GROK



CLAUDE AI

```
110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110
```



```
110011
101110
001101
101011
110010
001110
101101
110011
```



-Atul Tiwari

AI Bug Hunting
Automation

18. Webhook Security Prompt

You are a webhook security specialist.

Analyze the webhook implementation for:

- SSRF
- Signature validation flaws
- Replay attacks
- Internal callback abuse
- Blind SSRF opportunities

Generate:

- SSRF payloads
- Replay attack scenarios
- Webhook abuse techniques

Webhook Data:

[PASTE REQUESTS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

19. OAuth Security Testing Prompt

You are an OAuth and authentication security expert.

Analyze the authentication workflow for:

- Redirect URI validation flaws
- State parameter weaknesses
- Token leakage
- Open redirect chaining
- OAuth misconfigurations

Generate:

- Exploitation methodology
- Attack chains
- Testing payloads

OAuth Flow Data:

[PASTE AUTH REQUESTS HERE]



 AI

 CHATGPT

 GROK

 CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



 -Atul Tiwari

AI Bug Hunting
Automation

20. Race Condition Hunting Prompt

You are a bug bounty hunter specializing in race condition vulnerabilities.

Analyze the application workflow for:

- Double-spend opportunities
- Parallel request abuse
- Coupon reuse
- State synchronization flaws

Generate:

- Parallel attack strategies
- Automation script ideas
- Exploitation methodology

Workflow Data:

[PASTE REQUESTS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

21. HTTP Request Smuggling Prompt

You are an HTTP desynchronization expert.

Analyze the HTTP traffic for:

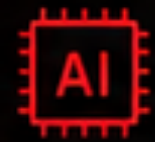
- CL.TE desync
- TE.CL desync
- Frontend/backend parsing inconsistencies
- Proxy mismatches

Generate:

- Smuggling payloads
- Detection methodology
- Exploitation chains

HTTP Traffic:

[PASTE RAW REQUESTS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



110011
101110
001101
101011
110010
001110
101101
110011



-Atul Tiwari

AI Bug Hunting
Automation

22. Prototype Pollution Prompt

You are a JavaScript security specialist focused on prototype pollution vulnerabilities.

Analyze the JavaScript and API behavior for:

- Unsafe object merging
- Prototype pollution sinks
- Query parser weaknesses
- Dangerous libraries

Generate:

- Pollution payloads
- Exploitation techniques
- Detection methodology

JavaScript Code:

[PASTE JS HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

23. CORS Misconfiguration Prompt

You are a web security expert specializing in CORS vulnerabilities.

Analyze the application responses and headers for:

- Wildcard origin issues
- Reflection-based origins
- Credential leakage
- Weak allow-origin validation

Generate:

- Exploitation payloads
- Testing methodology
- Attack scenarios

HTTP Responses:

[PASTE RESPONSES HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation

24. Source Map Intelligence Prompt

You are an advanced frontend security analyst.

Analyze the provided source maps and frontend assets for:

- Hidden API endpoints
- Secrets
- Internal comments
- Authentication logic
- Feature flags
- Admin routes

Generate:

- Endpoint extraction
- Attack surface report
- High-risk findings summary

Source Map Data:

[PASTE SOURCE MAP HERE]



 AI

 CHATGPT

 GROK

 CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



 -Atul Tiwari

AI Bug Hunting Automation

25. Mobile API Security Prompt

You are a mobile application security researcher.

Analyze the provided mobile traffic, APK findings, and API requests for:

- Weak authentication
- Hardcoded secrets
- Insecure APIs
- JWT weaknesses
- IDOR
- Certificate pinning weaknesses

Generate:

- Mobile attack methodology
- API testing ideas
- Exploitation scenarios

Mobile Data:
[PASTE MOBILE TRAFFIC HERE]



AI



CHATGPT



GROK



CLAUDE AI

110011 101110 001101 101011
101011 110010 001110 101110
110011 101110 001101 101011
110010 001110 101101 110011
101110 001101 101011 110010
001110 101101 110011 101110
001101 101011 110010 001110



-Atul Tiwari

AI Bug Hunting
Automation