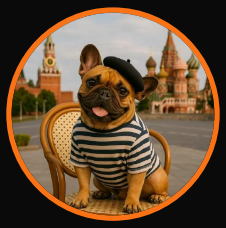

EASYPROTECH LLC

BRS-XSS Ethical Guidelines

Security Testing Ethics & Standards | v1.0 | 2025-12-26

ETHICS & RESPONSIBLE USE

Project: BRS-XSS (Brabus Recon Suite - XSS Module)
Company: EasyProTech LLC (www.easypro.tech)
Developer: Brabus
Created: Thu 07 Aug 2025 01:32:45 MSK

ETHICAL FRAMEWORK

BRS-XSS is developed with a commitment to ethical security research and responsible disclosure.

ETHICAL USE PRINCIPLES

1. AUTHORIZATION FIRST

- **Always obtain explicit written permission** before testing any system
- **Verify ownership** or authorized access to target infrastructure
- **Respect scope limitations** defined in testing agreements
- **Document authorization** for audit and legal protection

2. RESPONSIBLE DISCLOSURE

- **Report vulnerabilities responsibly** to system owners

- **Allow reasonable time** for remediation before public disclosure
- **Coordinate with vendors** on disclosure timelines
- **Protect sensitive information** during the disclosure process

3. MINIMIZE HARM

- **Avoid disrupting services** or causing system instability
- **Use minimal necessary techniques** to demonstrate vulnerabilities
- **Respect data privacy** and confidentiality
- **Clean up testing artifacts** after assessment completion

4. PROFESSIONAL CONDUCT

- **Maintain confidentiality** of client information and findings
- **Act with integrity** in all security research activities
- **Respect intellectual property** rights and licensing terms
- **Follow industry best practices** and professional standards

UNETHICAL ACTIVITIES

STRICTLY PROHIBITED:

UNAUTHORIZED ACCESS - Scanning or testing systems without permission - Bypassing security controls without authorization - Accessing data or systems beyond agreed scope

MALICIOUS EXPLOITATION - Using vulnerabilities for personal gain - Causing intentional damage or disruption - Installing backdoors or persistent access

DATA MISUSE - Extracting, copying, or modifying unauthorized data - Violating privacy expectations - Sharing confidential information inappropriately

DISCLOSURE VIOLATIONS - Public disclosure without coordination - Selling vulnerability information - Weaponizing security flaws

RESPONSIBLE SECURITY RESEARCH

RESEARCH GUIDELINES

BEFORE TESTING: 1. Obtain explicit written authorization 2. Define clear scope and limitations 3. Establish communication channels 4. Agree on disclosure timelines 5. Document all permissions

DURING TESTING: 1. Follow least-privilege principles 2. Minimize system impact 3. Document all activities 4. Respect data confidentiality 5. Stop if unexpected issues arise

AFTER TESTING: 1. Report findings responsibly 2. Provide remediation guidance 3. Clean up testing artifacts 4. Maintain confidentiality 5. Follow up on fixes

BUG BOUNTY PARTICIPATION

ETHICAL BUG BOUNTY PRACTICES: - Read and follow program rules completely - Respect scope limitations strictly - Report through official channels only - Avoid duplicate or known issues - Provide clear reproduction steps

EDUCATIONAL USE

ACADEMIC ENVIRONMENT

ACCEPTABLE EDUCATIONAL USE: - Controlled laboratory environments - Isolated test networks - Intentionally vulnerable applications - Supervised learning scenarios - Professional training courses

EDUCATIONAL RESPONSIBILITIES: - Ensure proper supervision - Use isolated environments only - Teach responsible disclosure - Emphasize legal compliance - Promote ethical practices

CERTIFICATION PREPARATION

PROFESSIONAL CERTIFICATION: - Use designated practice environments - Follow certification body guidelines - Respect intellectual property - Maintain ethical standards - Document learning activities

COMMUNITY RESPONSIBILITY

SECURITY COMMUNITY

CONTRIBUTING POSITIVELY: - Share knowledge responsibly - Mentor newcomers ethically - Promote best practices - Support defensive efforts - Advance security awareness

AVOIDING HARM: - Don't enable malicious activities - Refuse to assist unauthorized testing - Report suspected abuse - Promote legal compliance - Encourage responsible behavior

VENDOR RELATIONSHIPS

WORKING WITH VENDORS: - Respect vendor processes - Provide clear documentation - Allow adequate remediation time - Maintain professional communication - Support security improvements

IMPACT ASSESSMENT

BEFORE TESTING

CONSIDER THE IMPACT: - Potential service disruption - Data exposure risks - Legal implications - Reputation effects - Business consequences

RISK MITIGATION: - Use minimal necessary techniques - Test during maintenance windows - Have rollback procedures ready - Coordinate with system administrators - Document all activities

DURING ASSESSMENT

CONTINUOUS MONITORING: - Watch for unintended effects - Stop if problems arise - Communicate issues immediately - Document all observations - Maintain detailed logs

CONTINUOUS IMPROVEMENT

ETHICAL DEVELOPMENT

IMPROVING PRACTICES: - Regular ethics training - Peer review processes - Industry standard adoption - Legal consultation - Community feedback

TOOL IMPROVEMENT: - Minimize false positives - Reduce system impact - Enhance safety features - Improve documentation - Support responsible use

INCIDENT RESPONSE

ACCIDENTAL DISCOVERY OF CRITICAL VULNERABILITIES

If you accidentally discover a critical vulnerability during authorized testing:

IMMEDIATE ACTIONS: 1. **STOP** all testing activities immediately 2. **DO NOT** exploit the vulnerability further 3. **DO NOT** access any data beyond what was incidentally exposed 4. **DOCUMENT** the exact steps that led to the discovery 5. **SECURE** your findings - do not share publicly

NOTIFICATION TIMELINE: - **Within 24 hours:** Notify the system owner through secure channels - **Within 48 hours:** Provide initial technical details - **Within 7 days:** Submit complete vulnerability report - **90 days maximum:** Coordinate public disclosure if applicable

CRITICAL INFRASTRUCTURE: If the vulnerability affects critical infrastructure (healthcare, finance, government, utilities): - Consider notifying relevant national CERT/CSIRT - Follow sector-specific disclosure requirements - Prioritize public safety over disclosure timelines

DATA RETENTION

TESTING DATA MANAGEMENT

DURING TESTING: - Store all data on encrypted systems - Use secure, isolated environments - Minimize data collection to what is necessary - Never store credentials or sensitive PII

RETENTION PERIODS: - **Scan logs:** Maximum 90 days after project completion - **Vulnerability reports:** As required by contract, then securely delete - **Evidence/screenshots:** Maximum 30 days after report delivery - **Raw response data:** Delete immediately after analysis

SECURE DELETION: - Use cryptographic erasure or secure deletion tools - Verify deletion completion - Document deletion for audit purposes - Clear all caches and temporary files

CLIENT DATA: - Follow client's data retention policies - Obtain written approval for any extended retention - Provide data destruction certificates upon request

THIRD-PARTY NOTIFICATION

WHEN TO NOTIFY THIRD PARTIES

MANDATORY NOTIFICATION SCENARIOS:

1. Supply Chain Vulnerabilities: If a vulnerability affects third-party components used by your target: - Notify the third-party vendor directly - Coordinate disclosure with both target and vendor - Allow reasonable time for patches

2. Shared Infrastructure: If vulnerability affects shared hosting, cloud providers, or CDNs: - Notify the infrastructure provider - Ensure isolation of your client's data - Document potential exposure scope

3. Customer Data at Risk: If end-user data of the target's customers may be exposed: - Advise target on notification obligations (GDPR, CCPA, etc.) - Document the scope of potential exposure - Do not contact end-users directly

4. Active Exploitation: If you discover evidence of active exploitation by malicious actors: - Prioritize notification - reduce timeline to 24-48 hours - Consider involving law enforcement - Document all evidence without tampering

NOTIFICATION METHODS: - Use encrypted communication channels - Verify recipient identity before sharing details - Maintain communication logs - Follow up if no response within 72 hours

ETHICAL REPORTING

CONCERNS AND VIOLATIONS

REPORT ETHICAL CONCERNS TO: - **Website:** www.easypro.tech - **Purpose:** Ethical violations or concerns only - **Response:** Appropriate investigation and action

WHAT TO REPORT: - Suspected misuse of BRS-XSS - Ethical violations by users - Safety concerns with the tool - Suggestions for improvement

GLOBAL RESPONSIBILITY

INTERNATIONAL PERSPECTIVE

CULTURAL SENSITIVITY: - Respect local laws and customs - Understand regional regulations - Consider cultural implications - Adapt practices appropriately - Promote global security

INTERNATIONAL COOPERATION: - Support responsible disclosure globally - Share threat intelligence appropriately - Collaborate with international researchers - Respect sovereignty and jurisdiction - Promote peaceful security research

COMMITMENT

OUR PROMISE

EasyProTech LLC COMMITS TO: - Developing tools for legitimate security purposes - Supporting responsible security research - Promoting ethical practices in cybersecurity - Refusing to enable malicious activities - Advancing defensive capabilities

YOUR COMMITMENT

BY USING BRS-XSS, YOU COMMIT TO: - Following all ethical guidelines - Respecting legal boundaries - Acting responsibly and professionally - Supporting the security community - Promoting ethical security research

REMEMBER: WITH GREAT POWER COMES GREAT RESPONSIBILITY

Use BRS-XSS to make the digital world more secure, not to cause harm.