E-MAIL josefbasner@proton.me
TELEFON +49 151 4495 7240
GITHUB github.com/JBMTP07
WEB jbmtp07.github.io
STANDORT Deutschland · Remote weltweit

Josef Roland Basner

Penetration Tester · Red Team Operator · Security Researcher

PROFIL

Offensive-Security-Spezialist mit über 5 Jahren praktischer Erfahrung in Bug Bounty, Web- und API-Pentesting sowie Active-Directory-Angriffen. Seit 2020 aktiv in privaten Programmen auf HackerOne und Bugcrowd mit über 20 bestätigten Schwachstellen (RCE, SQLi, XSS, IDOR, Auth-Bypass). Eigenes Security-Lab, dokumentierte Methodik, laufender Zertifizierungspfad (CompTIA, EC-Council CEH v13). Zusätzlicher Background als ausgebildeter Mechatroniker (Siemens S7, SCADA) — direkter Zugang zu OT/ICS-Security. Hält ehrenamtliche Vorträge an Schulen zu KI-Sicherheit und Cybersecurity.

HIGHLIGHTS

20+	bestätigte Schwachstellen seit 2020 (HackerOne, Bugcrowd)	**5+**	Jahre offensive Security-Praxis
5–10	Schulen mit ehrenamtlichen Talks erreicht	**2x**	Doppelqualifikation: Offensive Security + OT/ICS

TECHNISCHE SCHWERPUNKTE

Offensive Security	Penetration Testing · Web- & API-Testing · Bug Bounty Research · Recon & Enumeration · Privilege Escalation · AD Attacks (Kerberoasting, AS-REP Roasting, Lateral Movement) · Post-Exploitation · Reporting
Tools	Burp Suite Pro · Metasploit · Nmap · Wireshark · Hydra · Nessus · BloodHound · CrackMapExec · Impacket · ffuf · sqlmap · gobuster
Scripting	Python · Bash · PowerShell · JavaScript
Netzwerke	TCP/IP · DNS · DHCP · Subnetting · ARP · Routing · Firewalls · Netzwerkanalyse
Betriebssysteme	Kali Linux · Parrot OS · Ubuntu · Windows Server · Active Directory
OT / ICS	Siemens S7 (SPS) · SCADA · Industriesteuerungen · Feldbusse · IT/OT-Schnittstellen

PRAKTISCHE SECURITY-ERFAHRUNG

Bug Bounty Researcher *seit 2020 · HackerOne, Bugcrowd*

- Aktiv in privaten / invite-only Programmen auf **HackerOne** und **Bugcrowd**
- **20+ bestätigte Schwachstellen**: RCE, SQL-Injection, Stored/Reflected XSS, IDOR, Auth-Bypass, Business-Logic-Flaws
- Schwerpunkt auf Web- und API-Schwachstellen, Recon-Automatisierung, Token- und Session-Analyse
- Vollständige Einhaltung von NDAs und Responsible-Disclosure-Richtlinien · saubere, reproduzierbare PoC-Reports
- Sanitisierte Public-Reports inkl. Chained Exploit (SQLi→XSS→SSTI→RCE, CVSS 9.9) und unauth. Command Injection (CVSS 9.8): **github.com/JBMTP07/bug-bounty-reports**

HackTheBox & Security Research Lab *laufend*

- Regelmäßige Bearbeitung von Machines, Pro Labs und Challenges
- Öffentliche deutschsprachige Writeups für retired Machines (github.com/JBMTP07/HTB-Writeups)
- Eigenes Testlabor: Raspberry Pi · Metasploitable · isoliertes AD · Vulnerable VMs
- Etablierter Workflow: Recon → Enumerate → Exploit → Escalate → Report

Veröffentlichte Studienmaterialien

- Strukturierte Methodik-Sammlung: Linux Privilege Escalation · AD-Angriffe · Nmap-Enumeration · Burp-Workflow (github.com/JBMTP07/Study-Notes)

SECURITY AWARENESS & BILDUNG

Gastredner – KI & Cybersecurity *seit 2024*

- Ehrenamtliche Vorträge an **5–10 Schulen** für Schüler:innen und Lehrkräfte
- Themen: Large Language Models (LLMs), KI-Sicherheitsrisiken, Phishing, Cybersecurity-Grundlagen
- Eigeninitiative · wachsendes Netzwerk an Schulkooperationen · zielgruppengerechte Kommunikation

ZERTIFIZIERUNGEN — Kurse abgeschlossen über New Horizons, Prüfungen ab Mai 2026

ZERTIFIZIERUNG	ANBIETER	STATUS
Network+	CompTIA	In Vorbereitung
Security+	CompTIA	In Vorbereitung
Linux+	CompTIA	In Vorbereitung
PenTest+	CompTIA	In Vorbereitung
CEH v13	EC-Council	In Vorbereitung

BERUFSERFAHRUNG

Selbstständiger Tätowierer *seit 01/2025*

Freiberufliche Tätigkeit parallel zur kontinuierlichen Weiterbildung in Cybersecurity und aktiven Bug-Bounty-Aktivitäten.

Mechatroniker · Rotan GmbH *2023*

Wartung, Instandhaltung und Fehlerdiagnose industrieller Anlagen · praktische Berührungspunkte mit OT-Systemen.

Stellv. Teamleiter · Avedo Rostock *2023*

Operative Führung, Teamkoordination, Qualitätssicherung, Eskalationsmanagement.

Ausbildung Mechatroniker · Consun Beet Company *2018 – 2022*

SPS-Programmierung (Siemens S7), SCADA-Systeme, Industrieautomation, Elektroanlagen, Messtechnik · direkter Bezug zu OT/ICS-Security.

SPRACHEN

Deutsch *(Muttersprache)* · Englisch *(fließend, technisch)* · Russisch *(Grundkenntnisse)*

SOFT SKILLS

Strukturiertes Arbeiten · Eigeninitiative · Reporting & Dokumentation · Kommunikation auf technischer und nicht-technischer Ebene · Zuverlässigkeit unter NDA · ausgeprägtes Sicherheitsbewusstsein

Stand: Mai 2026