Sam Pizzey

Ipswich, England
+44 7848 187587 | sam@pizzey.me
https://pizzey.me

SKILLS

Web Application Security: In-depth knowledge of OWASP-like issues as well as deeper testing
Penetration Testing: External infrastructure testing (Nessus, Kali toolset etc.), pre/post engagement
Vulnerability Research: Experience with black-box testing and grey/white-box (source code review)
Exploit Dev/Automation: Ruby/Python/C, currently developing proficiency with Rust
Reverse Engineering: Native (x86) RE using Ghidra/gdb, currently developing exploitation skillset

PROFESSIONAL EXPERIENCE

Intruder.io **London, England**
Security Consultant (Penetration Testing) June 2022 – Present

- Deliver end-to-end web application and external infrastructure penetration tests, from the scoping phase through to debrief/remediation advice, using a mix of automated tooling (Nessus/Burp Suite Pro) and in-depth manual testing depending on customer requirements.
- Act as subject matter expert for the product team as part of the 'security on call' rotation. Responsibilities include both internal consulting ('is this code secure?') and contributing to product improvements such as shaping new scanning capabilities.
- Identify/triage newly discovered vulnerabilities for Intruder's 'Rapid Response' service and develop techniques to scan for them remotely, producing remediation advice for clients who are vulnerable.
- Research new vulnerabilities in externally facing software used by our clients, producing proof-of-concept exploits that can be used by the product and write-ups for Intruder's research blog[1].

Sub6 Ltd. **Preston, England**
Linux Support Administrator February 2012 – June 2022

- Delivered Level 3 Linux support for a diverse mix of fully managed web hosting clients, from non-technical end users through to developers and reseller partners. Primarily Red Hat Linux + LAMP.
- Assisted with incident response for security issues faced by clients using platform logs and source code to identify exploited vulnerabilities and give remediation advice.
- Provided response to denial of service attacks against customers, mitigating at the platform level where possible (Layer 7 attacks using mod_security etc.) and liaising with upstream networks for large volume attacks.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP): Passed in 2016, OS-14955

VULNERABILITY RESEARCH

CVE-2024-28698 – CSLA.NET Path Traversal to Code Execution[Writeup]
CVE-2023-6933 – Better Search & Replace Unauthenticated Object Injection[Reference]
ClearOS VPN Authentication Bypass (Remote Root)*
ISPConfig SQL Type Confusion / Administrator Authentication Bypass[Writeup]
BuddyPress Arbitrary File Deletion[Reference]

** Private bug bounty – disclosure cleared by program*