GEORGI GUNINSKI
e-mail gguninski@gmail.com, guninski@guninski.com
site: http://www.guninski.com
blog: https://j.ludost.net
Linkedin: https://www.linkedin.com/in/georgi-guninski-b0069a156/

Currently I am looking for remote work in security and/or experimental mathematics or cryptography or AI.

SUMMARY I am security consultant and researcher and developer. I was world famous in cyber security in the past, now still have skills.

ACHIEVEMENTS

- Over 110 security vulnerabilities, with over 50 CVE entries in widely used software (not counting contract work). Vulnerabilities range from remote kernel problems to browser bugs to theoretical flaws in proof assistants. Notable vulnerabilities:
  - Discoverer of DLL hijacking: design flaw in windows when loading dynamic libraries from current working directory, *efficient* exploit vector in malware. Disclosed in 2000, still alive till at least 2024. Source
  - The first expoitable qmail bugs Source
  - Remote root in Ubuntu via apt-key Source
  - Remote OpenBSD denial of service in IP6 (very rare) Source
  - Design flaw in windows when digitally signing buggy mobile code (ActiveX) Source
  - Design flaw in cryptography RFC about DH group parameters, LibreSSL fixed it Source
  - Publications received popular media coverage (CNN, cnet.com, theregister.co.uk) and are available on packetstormsecurity.com and www.exploit-db.com.
  - Over 50 CVEs google search. Some CVEs: qmail CVE-2005-1515 dll hijacking CVE-2000-0854 vim CVE-2000-0854 linux kernel CVE-2005-0530 openbsd remote crash CVE-2004-0257 apache mod_proxy cve-2004-0492 microsoft excel CVE-2002-0618
  - In Coq proof assistant, found two critical inconsistencies which allow proving $False$, acknowledged by the developers. Coq is used in formal verification.
  - In 2023 in AI security, published vulnerabilities in chatGPT and Google Bard, the novelty of these is that the AI writes insecure code which is *textbook example* of the XSS vulnerability. AI is tried to be used for writing secure code.

    - Web searches for me: on microsoft.com on githhub.com on debian.org
- Listed as contributor to Firefox (web browser) and Wireshark (network sniffer)
- math preprint Note: a counterexample to a conjecture of Jackson about hamiltonicity of diregular digraphs Source
- math preprint: Public key cryptography based on non-invertible matrices Source
- math preprint: Note: simple real function with zeros greater than one the primes Source
- 2% overall on Mathoverflow, StackExchange site, profile Source
- Found 6 of the 169 known high merit abc triples Source

IN MEDIA:
CNN (12 results): Source
CNET (74 results): Source
The Register (77 results): Source

NOTES: Looking for remote home based work only.

TECHNICAL SUMMARY

Skills: IT Security, Programming, Experimental Mathematics, QA

Programming Languages: Sagemath, Python, C, JavaScript
Operating Systems: Linux, basic *BSD

EXPERIENCE

Experimental mathematics	2009-present
Partial security research	2009-present
python software developer, speech recognition	2022-2022
Netscape and Mozilla Corporation Independent Security Consultant.	1999-2009
Technologica Ltd, IT expert	1996-1999
ACTA Ltd. Clipper developer, Bank software	1995-1996

EDUCATION

University of National and World Economy - Sofia, Bulgaria
MA in International Economic Relations — GPA: 5.38/6.00
1991-1995

114 English Language School Liliana Dimitrova,
graduated with gold medal — 1986-1991

Revision: Wed Jan 3 03:12:36 PM UTC 2024