

# SAP Application Security

## *Your Crown Jewels Online: Further Attacks to SAP Web Applications*

**Mariano Nunez**  
CEO – Onapsis, Inc.



Session ID: HT2-301

Session Classification: Lightning Round

RSACONFERENCE2012

# Agenda

- The evolution of the threats to SAP systems
- The different SAP Web Servers
- Attacks to SAP Web Applications
  - Attacks to the SAP Web Dispatcher
  - Live demo: Business data exfiltration
  - Live demo: Authentication bypass in Enterprise Portals
- Countermeasures

# The evolution of the threats to SAP systems

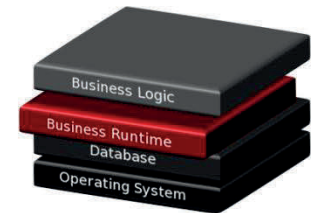


# What is SAP?

- Largest provider of business management solutions in the world.
- Used by Fortune-500 world-wide companies, governmental organizations and defense facilities to **run their every-day business-critical processes.**

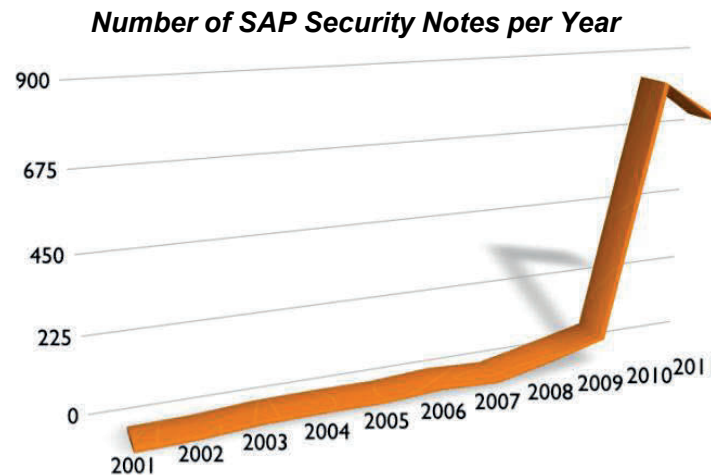
# What does “SAP Security” means?

- SAP Security was traditionally regarded as a synonym of “Segregation of Duties controls”.
- But... **SoD controls are not enough!**
- The forgotten layer: The Business Infrastructure (NetWeaver/Basis).
  - Base framework in charge of critical tasks such as authentication, authorization, auditing, logging, etc
  - Can be susceptible of security vulnerabilities that, if exploited, can lead to **espionage, sabotage and fraud** attacks to the business information.



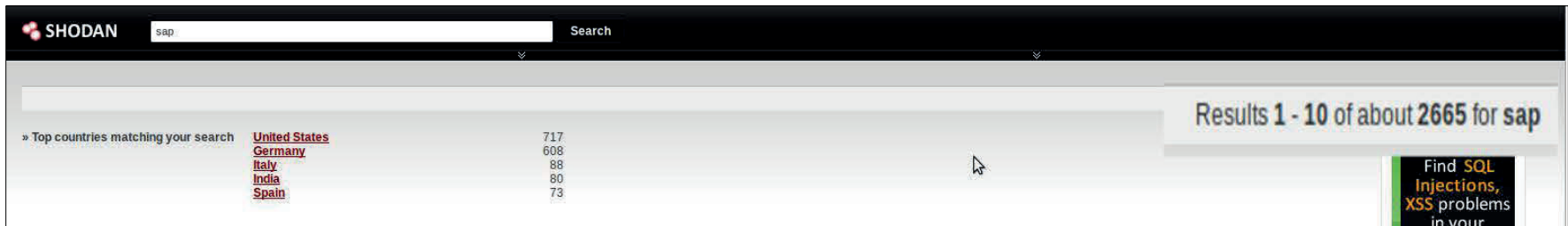
# Attacks to the SAP technical layer

- Involves much higher risks than SoD violations: *In many cases, the attacker does not even need a user account in the system!*
  - i.e.: By default, a remote attacker can take complete control of SAP Application Servers anonymously by exploiting vulnerabilities in the SAP Gateway.



# “My SAP system is only used internally”

- Could be true a decade ago, probably not anymore.
- Attackers can easily find SAP systems online.



SHODAN Search

Results 1 - 10 of about 2665 for sap

» Top countries matching your search

<a href="#">United States</a>	717
<a href="#">Germany</a>	608
<a href="#">Italy</a>	88
<a href="#">India</a>	80
<a href="#">Spain</a>	73

Find SQL Injections, XSS problems in your



inurl:/irj/portal



Search

Page 19 of 187 results (0.15 seconds)

Advanced search

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/655301342031011310>