OWASP TOP 10

A5 Security Misconfiguration

A5-Security Misconfiguration

- Security Misconfigurations most of the times are caused due to lack of security implementation/secure coding practice.
- The Security misconfiguration can happen at any level of the web application stack whether be it the framework, application server , database, etc.

Causes:

- Default configurations enabled with the frameworks/platforms being used.
- Default user accounts with default credentials.
- Default error messages.
- Role Misconfiguration.
- Lack of updation of applications/frameworks/platforms being used.
- Existence of Unused/Unwanted Pages.
- Unprotected files/directories.

Consequences

- Attackers could easily gather information about the obsolete/insecure implementations being implemented and craft the further attacks.
- Attackers could go ahead and try gaining access to the default user accounts, unprotected files/directories or try to upload malicious file onto the target machine.

Mitigations

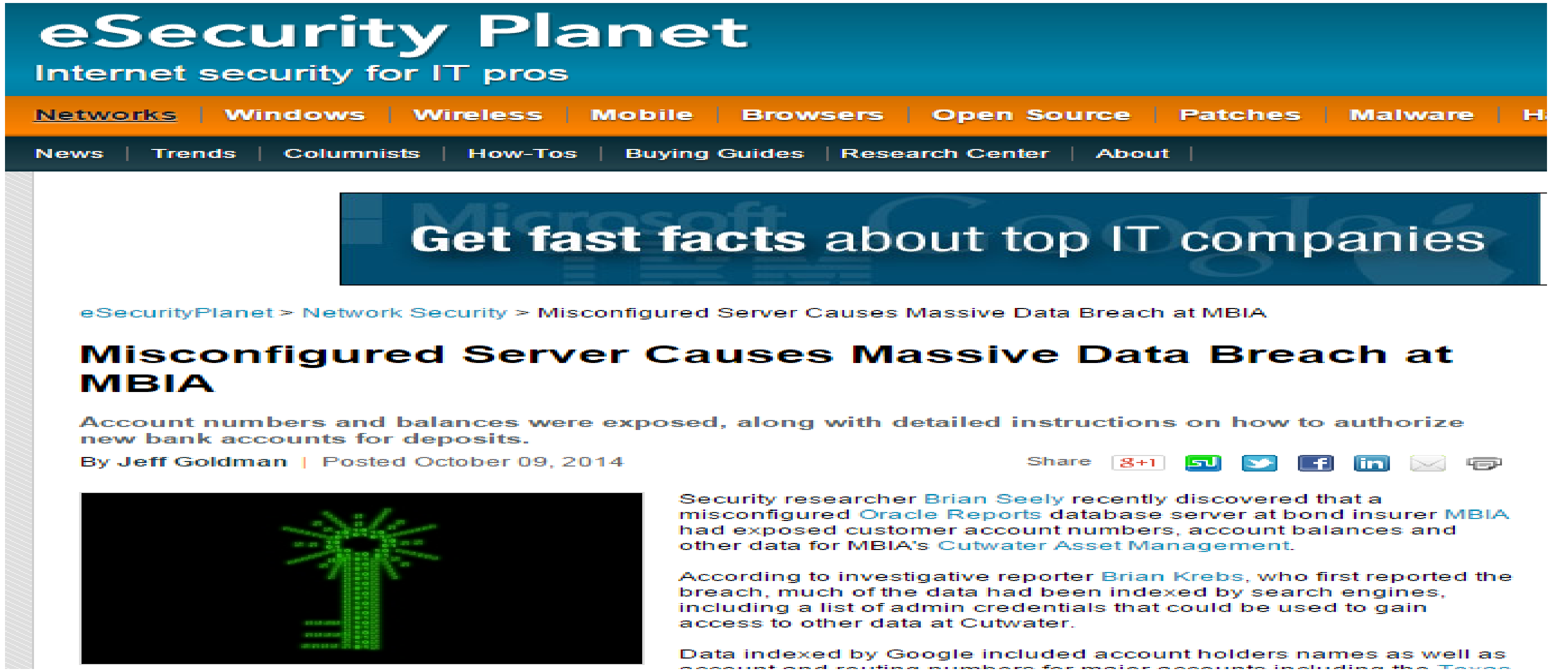
- Implementation of “Suhosin” , which helps in patching many security flaws in the PHP.
- To make sure that allow_url_* are disabled in php.ini if the application does not use file uploads.
- Check if any sensitive data is present on the client-side code.
- Ensure to test for file extensions handling.
- Ensure to test for commonly used URL’s.
- Ensure to delete the unwanted files/directories.
- Ensure to remove the default accounts.
- Ensure to have test on policies.
- Ensuring that the access to php config files are limited using .htaccess
- Ensuring Input Sanitization.

Tools

- OPENVAS
- WATOBO
- Wordpress AIO Security Plugin. (For WP only)

Real World Attacks

- http://www.esecurityplanet.com/network-security/misconfigured-server-causes-massive-data-breach-at-mbia.html


eSecurity Planet
Internet security for IT pros
Networks | Windows | Wireless | Mobile | Browsers | Open Source | Patches | Malware | H
News | Trends | Columnists | How-Tos | Buying Guides | Research Center | About |
Get fast facts about top IT companies
Share

eSecurityPlanet > Network Security > Misconfigured Server Causes Massive Data Breach at MBIA

Misconfigured Server Causes Massive Data Breach at MBIA

Account numbers and balances were exposed, along with detailed instructions on how to authorize new bank accounts for deposits.

By Jeff Goldman | Posted October 09, 2014

Security researcher Brian Seely recently discovered that a misconfigured Oracle Reports database server at bond insurer MBIA had exposed customer account numbers, account balances and other data for MBIA's Cutwater Asset Management.

According to investigative reporter Brian Krebs, who first reported the breach, much of the data had been indexed by search engines, including a list of admin credentials that could be used to gain access to other data at Cutwater.

Data indexed by Google included account holders names as well as account and routing numbers for major accounts including the Texas