Threat	Brute-force login
Affected component	Human resources management login component
Module details	`login.php (`lines 4963)
Vulnerability class	Authentication bypass
Description	Different errors are returned for invalid usernames and passwords, making usernames easier to identify. This error makes a successful brute-force attack much more likely against users with weak or easily guessed passwords.
Result	Untrusted clients can gain access to user accounts and, therefore, read or modify sensitive information.
Prerequisites	The application is located on the corporate intranet, limiting its exposure.
Business impact	A malicious third party can access a user's personal data, which could be a violation of federal privacy regulations.
Proposed remediation	Make error messages ambiguous so an attacker doesn't know whether the username or password is invalid. Lock the user account after repeated failed login attempts. (Three or five attempts would be appropriate.)
Risk	Damage potential: 6 Reproducibility: 8 Exploitability: 4 Affected users: 5 Discoverability: 8 Overall: 6.2

This sample is certainly functional; however, it's not the only approach. Your level of detail can vary depending on your reasons for the audit and who the report is for. The following list is considered useful information to support a security finding:

- *Location of the vulnerability* This information (in Table 4-2's Module details row) should be fairly specific. You should usually include the filename, function