Server hardening

Groep 1:
Bram Jonker
Leon Dijkstra
Lukas Cremers
Stefan Suk
Wiljan Siderius

4 april 2024

Inhoud

Inleiding

Het waarborgen van de veiligheid van servers is van cruciaal belang in elke IT-infrastructuur. Serverharding, het proces van het verminderen van beveiligingsrisico's door het toepassen van verschillende technieken en patches, is een essentiële stap om potentiële kwetsbaarheden te verminderen en de algehele weerbaarheid te vergroten. In dit rapport zullen we de opgeloste kwetsbaarheden bespreken die zijn geïdentificeerd door middel van de Nikto-scanner, evenals de bug fixes die zijn geïmplementeerd vanuit PHPStan. Bovendien zullen we inzicht bieden in de handmatige hardening maatregelen die zijn genomen om de veiligheid van de servers verder te versterken.

1. Opgeloste vulnerabilities vanuit nikto

gedetailleerde analyse van de opgeloste kwetsbaarheden die zijn geïdentificeerd door de Nikto-scanner en daarna opgelost

+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /.git/index: Git Index file may contain directory listing information.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /.git/config: Git config file found. Infos about repo details may be present.
+ /.idea/modules.xml: JetBrains project IDE reveals application information.
+ /.idea/vcs.xml: JetBrains project IDE reveals application information.
+ /.idea/workspace.xml: JetBrains project IDE reveals application information.
+ /README.md: Readme Found.

2. bug fixes vanuit PHPStan

verscheidene bugs zijn gevonden door middel van gebruik van de tool PHPStan, deze bugs hebben wij daarna allemaal opgelost.

2.1 intranet/klantenservice/index.php

39 Function search() has no return type specified.

2.2 intranet/ldap_support.inc.php

42 Function ConnectAndCheckLDAP() should return resource but returns LDAP\Connection.
52 Function AddUserToGroup() has no return type specified.
52 Function AddUserToGroup() has parameter $groupDN with no type specified.
52 Function AddUserToGroup() has parameter $lnk with no type specified.
52 Function AddUserToGroup() has parameter $userDN with no type specified.
74 Function RemoveUserFromGroup() has no return type specified.
77 Parameter #1 $ldap of function ldap_mod_del expects LDAP\Connection, resource given.
78 Parameter #1 $ldap of function ldap_error expects LDAP\Connection, resource given.
79 Parameter #1 $ldap of function ldap_errno expects LDAP\Connection, resource given.
95 Function CreateNewUserLdap() has no return type specified.
95 Function CreateNewUserLdap() has parameter $cn with no type specified.
95 Function CreateNewUserLdap() has parameter $givenName with no type specified.
95 Function CreateNewUserLdap() has parameter $lnk with no type specified.
95 Function CreateNewUserLdap() has parameter $newUserDN with no type specified.
95 Function CreateNewUserLdap() has parameter $sn with no type specified.
95 Function CreateNewUserLdap() has parameter $uid with no type specified.
137 Function SetPassword() has no return type specified.
137 Function SetPassword() has parameter $lnk with no type specified.
137 Function SetPassword() has parameter $newPassword with no type specified.
137 Function SetPassword() has parameter $newUserDN with no type specified.
139 If condition is always true.
140 Parameter #1 $prefix of function uniqid expects string, int<0, max> given.
169 Function ReportUser() has no return type specified.
169 Function ReportUser() has parameter $lnk with no type specified.
169 Function ReportUser() has parameter $userDN with no type specified.
175 Parameter #2 $result of function ldap_get_entries expects LDAP\Result, array|LDAP\Result given.
182 Cannot access offset 'count' on array<int|string, array|int>|false.
185 Cannot access offset 'count' on array|int.

190 Cannot access offset int<0, max> on array|int.
229 Function GetAllLDAPGroupMemberships() has parameter $lnk with no type specified.
229 Function GetAllLDAPGroupMemberships() has parameter $userDN with no type specified.
229 Function GetAllLDAPGroupMemberships() return type has no value type specified in iterable type array.
💡 See: https://phpstan.org/blog/solving-phpstan-no-value-type-specified-in-iterable-type
240 Parameter #2 $result of function ldap_get_entries expects LDAP\Result, array|LDAP\Result given.
251 Cannot access offset 'dn' on array|int.
252 Cannot access offset 'description' on array|int.
259 Function GetAllLDAPGroups() has no return type specified.
259 Function GetAllLDAPGroups() has parameter $lnk with no type specified.
265 Parameter #2 $result of function ldap_get_entries expects LDAP\Result, array|LDAP\Result given.
276 Cannot access offset 'dn' on array|int.
277 Cannot access offset 'description' on array|int.
291 Function GetUserDNFromUID() has parameter $lnk with no type specified.
291 Function GetUserDNFromUID() has parameter $uid with no type specified.
298 Parameter #2 $result of function ldap_get_entries expects LDAP\Result, array|LDAP\Result given.
313 Function CheckIfUserExists() has no return type specified.
313 Function CheckIfUserExists() has parameter $lnk with no type specified.
313 Function CheckIfUserExists() has parameter $username with no type specified.
321 Parameter #2 $result of function ldap_get_entries expects LDAP\Result, array|LDAP\Result given.
324 Cannot access offset 'count' on array<int|string, array|int>|false.
331 Function getklantName() has no return type specified.
331 Function getklantName() has parameter $lnk with no type specified.
331 Function getklantName() has parameter $uid with no type specified.
339 Parameter #2 $result of function ldap_get_entries expects LDAP\Result, array|LDAP\Result given.

2.3 intranet/manager/createNewUser.php

24 Function createuser() has no return type specified.
67 Parameter #1 $ldap of function ldap_close expects LDAP\Connection, resource given.
98 Function checkUser() has no return type specified.
115 Parameter #1 $ldap of function ldap_close expects LDAP\Connection, resource given.

2.4 intranet/manager/editUser.php

34 Parameter #1 $ldap of function ldap_search expects array|LDAP\Connection, resource given.
39 Parameter #1 $ldap of function ldap_get_entries expects LDAP\Connection, resource given.
39 Parameter #2 $result of function ldap_get_entries expects LDAP\Result, array|LDAP\Result given.
42 Cannot access offset 'count' on array<int|string, array|int>|false.
43 Cannot access offset 'uid' on array|int.
57 Cannot access offset 'cn' on array|int.
57 Parameter #1 $ldap of function ldap_modify expects LDAP\Connection, resource given.
74 Cannot access offset 'givenname' on array|int.
76 Cannot access offset 'sn' on array|int.
86 Parameter #1 $ldap of function ldap_close expects LDAP\Connection, resource given.

2.5 intranet/manager/index.php

17 Variable $lnk might not be defined.
84 Variable $lnk might not be defined.
89 Parameter #2 $result of function ldap_get_entries expects LDAP\Result, array|LDAP\Result given.
89 Variable $lnk might not be defined.
91 Cannot access offset 'count' on array<int|string, array|int>|false.
93 Cannot access offset 'uid' on array|int.
97 Cannot access offset 'uid' on array|int.
98 Cannot access offset 'uid' on array|int.
99 Cannot access offset 'cn' on array|int.
100 Cannot access offset 'givenname' on array|int.
101 Cannot access offset 'sn' on array|int.
105 Cannot access offset 'uid' on array|int.
106 Cannot access offset 'cn' on array|int.
107 Cannot access offset 'givenname' on array|int.
108 Cannot access offset 'sn' on array|int.
119 Variable $lnk might not be defined.

Line intranet/sql_support.php

3 Function SQLconnect() has no return type specified.
10 Function getuserinfo() has no return type specified.
24 Function getadresinfo() has no return type specified.

38 Function getmetertelwerkid() has no return type specified.
68 Function getmeterstanden() has no return type specified.
68 Function getmeterstanden() has parameter $metertelwerkid with no type specified.
85 Function getconfiguration() has no return type specified.
100 Function createuserSQL() has no return type specified.
118 Function createadress() has no return type specified.
132 Function addtoauditlog() has no return type specified.
144 Function getLogs() has no return type specified.
160 Function getPermissions() has no return type specified.
160 Function getPermissions() has parameter $groups with no type specified.
162 Constant DB_PASSWORD not found.
💡 Learn more at https://phpstan.org/user-guide/discovering-symbols
162 Constant DB_USERNAME not found.
💡 Learn more at https://phpstan.org/user-guide/discovering-symbols
162 Constant MYSQL_DSN not found.
💡 Learn more at https://phpstan.org/user-guide/discovering-symbols
169 Cannot access offset 'PermissionId' on mixed.
170 Cannot access offset 'PermissionId' on mixed.

2.6 intranet/utils/sessionmanager.php

7 Function getRolesAndPerms() has no return type specified.

2.7 signup.php

42 Function checkuser() has no return type specified.
80 Parameter #1 $ldap of function ldap_close expects LDAP\Connection, resource given.
81 Binary operation "*" between string and 100000000 results in an error.
82 Binary operation "*" between string and 100000000 results in an error.
83 Binary operation "*" between string and 100000000 results in an error.
157 Function checkKlant() has no return type specified.
174 Parameter #1 $ldap of function ldap_close expects LDAP\Connection, resource given.

Handmatige hardening:

De volgende handmatige hardening maatregelen zijn genomen:

- Apache is gehardened.
- Onnodige accounts zijn verwijderd.
- Database-rechten zijn beperkt tot alleen lezen voor bepaalde tabellen.
- Indexen zijn gecorrigeerd.
- samba is verwijderd
- PHPStan is verwijderd
- Xdebug uitgeschakeld
- PHP gehardend met ini file van owasp:
  https://github.com/danvau7/very-secure-php-ini