CodeQL Alerts grouped by CWE

Loaded 5045 items, 175 shown

Severity counts — high: 171 · medium: 4

▼CWE-532: Insertion of Sensitive Information into Log File

84 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/216	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
2	https://github.com/Foxofft/midpoint/security/code-scanning/215	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
3	https://github.com/Foxofft/midpoint/security/code-scanning/214	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
4	https://github.com/Foxofft/midpoint/security/code-scanning/213	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
5	https://github.com/Foxofft/midpoint/security/code-scanning/212	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
6	https://github.com/Foxofft/midpoint/security/code-scanning/211	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
7	https://github.com/Foxofft/midpoint/security/code-scanning/210	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
8	https://github.com/Foxofft/midpoint/security/code-scanning/209	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
9	https://github.com/Foxofft/midpoint/security/code-scanning/208	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
10	https://github.com/Foxofft/midpoint/security/code-scanning/207	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
11	https://github.com/Foxofft/midpoint/security/code-scanning/206	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
12	https://github.com/Foxofft/midpoint/security/code-scanning/205	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.

13	https://github.com/Foxofft/midpoint/security/code-scanning/204	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
14	https://github.com/Foxofft/midpoint/security/code-scanning/203	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
15	https://github.com/Foxofft/midpoint/security/code-scanning/202	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
16	https://github.com/Foxofft/midpoint/security/code-scanning/201	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
17	https://github.com/Foxofft/midpoint/security/code-scanning/200	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
18	https://github.com/Foxofft/midpoint/security/code-scanning/199	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
19	https://github.com/Foxofft/midpoint/security/code-scanning/198	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
20	https://github.com/Foxofft/midpoint/security/code-scanning/197	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
21	https://github.com/Foxofft/midpoint/security/code-scanning/196	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
22	https://github.com/Foxofft/midpoint/security/code-scanning/195	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
23	https://github.com/Foxofft/midpoint/security/code-scanning/194	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
24	https://github.com/Foxofft/midpoint/security/code-scanning/193	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
25	https://github.com/Foxofft/midpoint/security/code-scanning/192	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
26	https://github.com/Foxofft/midpoint/security/code-scanning/191	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
27	https://github.com/Foxofft/midpoint/security/code-scanning/190	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
28	https://github.com/Foxofft/midpoint/security/code-scanning/189	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.

29	https://github.com/Foxofft/midpoint/security/code-scanning/188	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
30	https://github.com/Foxofft/midpoint/security/code-scanning/187	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
31	https://github.com/Foxofft/midpoint/security/code-scanning/186	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
32	https://github.com/Foxofft/midpoint/security/code-scanning/185	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
33	https://github.com/Foxofft/midpoint/security/code-scanning/184	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
34	https://github.com/Foxofft/midpoint/security/code-scanning/183	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
35	https://github.com/Foxofft/midpoint/security/code-scanning/182	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
36	https://github.com/Foxofft/midpoint/security/code-scanning/181	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
37	https://github.com/Foxofft/midpoint/security/code-scanning/180	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
38	https://github.com/Foxofft/midpoint/security/code-scanning/179	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
39	https://github.com/Foxofft/midpoint/security/code-scanning/178	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
40	https://github.com/Foxofft/midpoint/security/code-scanning/177	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
41	https://github.com/Foxofft/midpoint/security/code-scanning/176	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
42	https://github.com/Foxofft/midpoint/security/code-scanning/175	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
43	https://github.com/Foxofft/midpoint/security/code-scanning/174	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
44	https://github.com/Foxofft/midpoint/security/code-scanning/173	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.

45	https://github.com/Foxofft/midpoint/security/code-scanning/172	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
46	https://github.com/Foxofft/midpoint/security/code-scanning/171	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
47	https://github.com/Foxofft/midpoint/security/code-scanning/170	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
48	https://github.com/Foxofft/midpoint/security/code-scanning/169	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
49	https://github.com/Foxofft/midpoint/security/code-scanning/168	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
50	https://github.com/Foxofft/midpoint/security/code-scanning/167	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
51	https://github.com/Foxofft/midpoint/security/code-scanning/166	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
52	https://github.com/Foxofft/midpoint/security/code-scanning/165	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
53	https://github.com/Foxofft/midpoint/security/code-scanning/164	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
54	https://github.com/Foxofft/midpoint/security/code-scanning/163	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
55	https://github.com/Foxofft/midpoint/security/code-scanning/162	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
56	https://github.com/Foxofft/midpoint/security/code-scanning/161	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
57	https://github.com/Foxofft/midpoint/security/code-scanning/160	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
58	https://github.com/Foxofft/midpoint/security/code-scanning/159	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
59	https://github.com/Foxofft/midpoint/security/code-scanning/158	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
60	https://github.com/Foxofft/midpoint/security/code-scanning/157	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.

61	https://github.com/Foxofft/midpoint/security/code-scanning/156	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
62	https://github.com/Foxofft/midpoint/security/code-scanning/155	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
63	https://github.com/Foxofft/midpoint/security/code-scanning/154	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
64	https://github.com/Foxofft/midpoint/security/code-scanning/153	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
65	https://github.com/Foxofft/midpoint/security/code-scanning/152	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
66	https://github.com/Foxofft/midpoint/security/code-scanning/151	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
67	https://github.com/Foxofft/midpoint/security/code-scanning/150	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
68	https://github.com/Foxofft/midpoint/security/code-scanning/149	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
69	https://github.com/Foxofft/midpoint/security/code-scanning/148	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
70	https://github.com/Foxofft/midpoint/security/code-scanning/147	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
71	https://github.com/Foxofft/midpoint/security/code-scanning/146	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
72	https://github.com/Foxofft/midpoint/security/code-scanning/145	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
73	https://github.com/Foxofft/midpoint/security/code-scanning/144	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
74	https://github.com/Foxofft/midpoint/security/code-scanning/143	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
75	https://github.com/Foxofft/midpoint/security/code-scanning/142	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
76	https://github.com/Foxofft/midpoint/security/code-scanning/141	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.

77	https://github.com/Foxofft/midpoint/security/code-scanning/140	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
78	https://github.com/Foxofft/midpoint/security/code-scanning/139	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
79	https://github.com/Foxofft/midpoint/security/code-scanning/138	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
80	https://github.com/Foxofft/midpoint/security/code-scanning/137	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
81	https://github.com/Foxofft/midpoint/security/code-scanning/136	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
82	https://github.com/Foxofft/midpoint/security/code-scanning/135	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
83	https://github.com/Foxofft/midpoint/security/code-scanning/134	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.
84	https://github.com/Foxofft/midpoint/security/code-scanning/133	high	Insertion of sensitive information into log files	Writing sensitive information to log files can allow that information to be leaked to an attacker more easily.

▼CWE-117: Improper Output Neutralization for Logs

33 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/132	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
2	https://github.com/Foxofft/midpoint/security/code-scanning/131	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
3	https://github.com/Foxofft/midpoint/security/code-scanning/130	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
4	https://github.com/Foxofft/midpoint/security/code-scanning/129	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
5	https://github.com/Foxofft/midpoint/security/code-scanning/128	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
6	https://github.com/Foxofft/midpoint/security/code-scanning/127	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.

7	https://github.com/Foxofft/midpoint/security/code-scanning/126	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
8	https://github.com/Foxofft/midpoint/security/code-scanning/125	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
9	https://github.com/Foxofft/midpoint/security/code-scanning/124	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
10	https://github.com/Foxofft/midpoint/security/code-scanning/123	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
11	https://github.com/Foxofft/midpoint/security/code-scanning/122	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
12	https://github.com/Foxofft/midpoint/security/code-scanning/121	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
13	https://github.com/Foxofft/midpoint/security/code-scanning/120	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
14	https://github.com/Foxofft/midpoint/security/code-scanning/119	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
15	https://github.com/Foxofft/midpoint/security/code-scanning/118	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
16	https://github.com/Foxofft/midpoint/security/code-scanning/117	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
17	https://github.com/Foxofft/midpoint/security/code-scanning/116	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
18	https://github.com/Foxofft/midpoint/security/code-scanning/115	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
19	https://github.com/Foxofft/midpoint/security/code-scanning/114	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
20	https://github.com/Foxofft/midpoint/security/code-scanning/113	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
21	https://github.com/Foxofft/midpoint/security/code-scanning/112	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
22	https://github.com/Foxofft/midpoint/security/code-scanning/111	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.

23	https://github.com/Foxofft/midpoint/security/code-scanning/110	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
24	https://github.com/Foxofft/midpoint/security/code-scanning/109	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
25	https://github.com/Foxofft/midpoint/security/code-scanning/108	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
26	https://github.com/Foxofft/midpoint/security/code-scanning/107	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
27	https://github.com/Foxofft/midpoint/security/code-scanning/106	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
28	https://github.com/Foxofft/midpoint/security/code-scanning/105	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
29	https://github.com/Foxofft/midpoint/security/code-scanning/104	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
30	https://github.com/Foxofft/midpoint/security/code-scanning/103	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
31	https://github.com/Foxofft/midpoint/security/code-scanning/102	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
32	https://github.com/Foxofft/midpoint/security/code-scanning/101	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.
33	https://github.com/Foxofft/midpoint/security/code-scanning/100	high	Log Injection	Building log entries from user-controlled data may allow insertion of forged log entries by malicious users.

▼CWE-352: Cross-Site Request Forgery (CSRF)

27 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/85	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
2	https://github.com/Foxofft/midpoint/security/code-scanning/84	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.

3	https://github.com/Foxofft/midpoint/security/code-scanning/83	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
4	https://github.com/Foxofft/midpoint/security/code-scanning/82	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
5	https://github.com/Foxofft/midpoint/security/code-scanning/81	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
6	https://github.com/Foxofft/midpoint/security/code-scanning/80	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
7	https://github.com/Foxofft/midpoint/security/code-scanning/79	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
8	https://github.com/Foxofft/midpoint/security/code-scanning/78	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
9	https://github.com/Foxofft/midpoint/security/code-scanning/77	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
10	https://github.com/Foxofft/midpoint/security/code-scanning/76	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
11	https://github.com/Foxofft/midpoint/security/code-scanning/75	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
12	https://github.com/Foxofft/midpoint/security/code-scanning/74	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
13	https://github.com/Foxofft/midpoint/security/code-scanning/73	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.

14	https://github.com/Foxofft/midpoint/security/code-scanning/72	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
15	https://github.com/Foxofft/midpoint/security/code-scanning/71	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
16	https://github.com/Foxofft/midpoint/security/code-scanning/70	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
17	https://github.com/Foxofft/midpoint/security/code-scanning/69	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
18	https://github.com/Foxofft/midpoint/security/code-scanning/68	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
19	https://github.com/Foxofft/midpoint/security/code-scanning/67	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
20	https://github.com/Foxofft/midpoint/security/code-scanning/66	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
21	https://github.com/Foxofft/midpoint/security/code-scanning/65	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
22	https://github.com/Foxofft/midpoint/security/code-scanning/64	high	HTTP request type unprotected from CSRF	Using an HTTP request type that is not default-protected from CSRF for a state-changing action makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
23	https://github.com/Foxofft/midpoint/security/code-scanning/55	high	Disabled Spring CSRF protection	Disabling CSRF protection makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
24	https://github.com/Foxofft/midpoint/security/code-scanning/54	high	Disabled Spring CSRF protection	Disabling CSRF protection makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
25	https://github.com/Foxofft/midpoint/security/code-scanning/53	high	Disabled Spring CSRF protection	Disabling CSRF protection makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.
26	https://github.com/Foxofft/midpoint/security/code-scanning/52	high	Disabled Spring CSRF protection	Disabling CSRF protection makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.

27	https://github.com/Foxofft/midpoint/security/code-scanning/51	high	Disabled Spring CSRF protection	Disabling CSRF protection makes the application vulnerable to a Cross-Site Request Forgery (CSRF) attack.

▼CWE-290: Authentication Bypass by Spoofing

8 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/99	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
2	https://github.com/Foxofft/midpoint/security/code-scanning/98	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
3	https://github.com/Foxofft/midpoint/security/code-scanning/97	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
4	https://github.com/Foxofft/midpoint/security/code-scanning/96	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
5	https://github.com/Foxofft/midpoint/security/code-scanning/95	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
6	https://github.com/Foxofft/midpoint/security/code-scanning/94	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
7	https://github.com/Foxofft/midpoint/security/code-scanning/93	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
8	https://github.com/Foxofft/midpoint/security/code-scanning/92	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.

▼CWE-807: Reliance on Untrusted Inputs in a Security Decision

8 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/99	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
2	https://github.com/Foxofft/midpoint/security/code-scanning/98	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
3	https://github.com/Foxofft/midpoint/security/code-scanning/97	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.

4	https://github.com/Foxofft/midpoint/security/code-scanning/96	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
5	https://github.com/Foxofft/midpoint/security/code-scanning/95	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
6	https://github.com/Foxofft/midpoint/security/code-scanning/94	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
7	https://github.com/Foxofft/midpoint/security/code-scanning/93	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.
8	https://github.com/Foxofft/midpoint/security/code-scanning/92	high	User-controlled bypass of sensitive method	User-controlled bypassing of sensitive methods may allow attackers to avoid passing through authentication systems.

▼CWE-327: Use of a Broken or Risky Cryptographic Algorithm

5 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/91	high	Use of a potentially broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.
2	https://github.com/Foxofft/midpoint/security/code-scanning/90	high	Use of a potentially broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.
3	https://github.com/Foxofft/midpoint/security/code-scanning/89	high	Use of a potentially broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.
4	https://github.com/Foxofft/midpoint/security/code-scanning/57	high	Use of a broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.
5	https://github.com/Foxofft/midpoint/security/code-scanning/56	high	Use of a broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.

▼CWE-328: Use of Weak Hash

5 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/91	high	Use of a potentially broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.
2	https://github.com/Foxofft/midpoint/security/code-scanning/90	high	Use of a potentially broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.

3	https://github.com/Foxofft/midpoint/security/code-scanning/89	high	Use of a potentially broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.
4	https://github.com/Foxofft/midpoint/security/code-scanning/57	high	Use of a broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.
5	https://github.com/Foxofft/midpoint/security/code-scanning/56	high	Use of a broken or risky cryptographic algorithm	Using broken or weak cryptographic algorithms can allow an attacker to compromise security.

▼CWE-022: Improper Limitation of a Pathname to a Restricted Directory ("Directory Traversal")

5 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/50	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
2	https://github.com/Foxofft/midpoint/security/code-scanning/49	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
3	https://github.com/Foxofft/midpoint/security/code-scanning/48	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
4	https://github.com/Foxofft/midpoint/security/code-scanning/47	high	Arbitrary file access during archive extraction ("Zip Slip")	Extracting files from a malicious ZIP file, or similar type of archive, without validating that the destination file path is within the destination directory can allow an attacker to unexpectedly gain access to resources.
5	https://github.com/Foxofft/midpoint/security/code-scanning/46	high	Arbitrary file access during archive extraction ("Zip Slip")	Extracting files from a malicious ZIP file, or similar type of archive, without validating that the destination file path is within the destination directory can allow an attacker to unexpectedly gain access to resources.

▼CWE-190: Integer Overflow or Wraparound

4 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/63	high	Comparison of narrow type with wide type in loop condition	Comparisons between types of different widths in a loop condition can cause the loop to behave unexpectedly.

2	https://github.com/Foxofft/midpoint/security/code-scanning/62	high	Comparison of narrow type with wide type in loop condition	Comparisons between types of different widths in a loop condition can cause the loop to behave unexpectedly.
3	https://github.com/Foxofft/midpoint/security/code-scanning/61	high	Uncontrolled data in arithmetic expression	Arithmetic operations on uncontrolled data that is not validated can cause overflows.
4	https://github.com/Foxofft/midpoint/security/code-scanning/60	high	Implicit narrowing conversion in compound assignment	Compound assignment statements (for example 'intvar += longvar') that implicitly cast a value of a wider type to a narrower type may result in information loss and numeric errors such as overflows.

▼CWE-197: Numeric Truncation Error

3 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/63	high	Comparison of narrow type with wide type in loop condition	Comparisons between types of different widths in a loop condition can cause the loop to behave unexpectedly.
2	https://github.com/Foxofft/midpoint/security/code-scanning/62	high	Comparison of narrow type with wide type in loop condition	Comparisons between types of different widths in a loop condition can cause the loop to behave unexpectedly.
3	https://github.com/Foxofft/midpoint/security/code-scanning/60	high	Implicit narrowing conversion in compound assignment	Compound assignment statements (for example 'intvar += longvar') that implicitly cast a value of a wider type to a narrower type may result in information loss and numeric errors such as overflows.

▼CWE-835: Loop with Unreachable Exit Condition ("Infinite Loop")

3 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/88	high	Loop with unreachable exit condition	An iteration or loop with an exit condition that cannot be reached is an indication of faulty logic and can likely lead to infinite looping.
2	https://github.com/Foxofft/midpoint/security/code-scanning/87	high	Loop with unreachable exit condition	An iteration or loop with an exit condition that cannot be reached is an indication of faulty logic and can likely lead to infinite looping.
3	https://github.com/Foxofft/midpoint/security/code-scanning/86	high	Loop with unreachable exit condition	An iteration or loop with an exit condition that cannot be reached is an indication of faulty logic and can likely lead to infinite looping.

▼CWE-023: Relative Path Traversal

3 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/50	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
2	https://github.com/Foxofft/midpoint/security/code-scanning/49	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
3	https://github.com/Foxofft/midpoint/security/code-scanning/48	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.

▼CWE-036: Absolute Path Traversal

3 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/50	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
2	https://github.com/Foxofft/midpoint/security/code-scanning/49	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
3	https://github.com/Foxofft/midpoint/security/code-scanning/48	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.

▼CWE-073: External Control of File Name or Path

3 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/50	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
2	https://github.com/Foxofft/midpoint/security/code-scanning/49	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.
3	https://github.com/Foxofft/midpoint/security/code-scanning/48	high	Uncontrolled data used in path expression	Accessing paths influenced by users can allow an attacker to access unexpected resources.

▼CWE-200: Information Exposure

2 alert(s)

#	html_url	severity	description	full_description

1	https://github.com/Foxofft/midpoint/security/code-scanning/219	medium	Local information disclosure in a temporary directory	Writing information without explicit permissions to a shared temporary directory may disclose it to other users.
2	https://github.com/Foxofft/midpoint/security/code-scanning/218	medium	Local information disclosure in a temporary directory	Writing information without explicit permissions to a shared temporary directory may disclose it to other users.

▼CWE-329: Unknown CWE

2 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/59	high	Using a static initialization vector for encryption	An initialization vector (IV) used for ciphers of certain modes (such as CBC or GCM) should be unique and unpredictable, to maximize encryption and prevent dictionary attacks.
2	https://github.com/Foxofft/midpoint/security/code-scanning/58	high	Using a static initialization vector for encryption	An initialization vector (IV) used for ciphers of certain modes (such as CBC or GCM) should be unique and unpredictable, to maximize encryption and prevent dictionary attacks.

▼CWE-732: Unknown CWE

2 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/219	medium	Local information disclosure in a temporary directory	Writing information without explicit permissions to a shared temporary directory may disclose it to other users.
2	https://github.com/Foxofft/midpoint/security/code-scanning/218	medium	Local information disclosure in a temporary directory	Writing information without explicit permissions to a shared temporary directory may disclose it to other users.

▼CWE-1204: Unknown CWE

2 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/59	high	Using a static initialization vector for encryption	An initialization vector (IV) used for ciphers of certain modes (such as CBC or GCM) should be unique and unpredictable, to maximize encryption and prevent dictionary attacks.
2	https://github.com/Foxofft/midpoint/security/code-scanning/58	high	Using a static initialization vector for encryption	An initialization vector (IV) used for ciphers of certain modes (such as CBC or GCM) should be unique and unpredictable, to maximize encryption and prevent dictionary attacks.

▼CWE-078: Unknown CWE

2 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/217	medium	Executing a command with a relative path	Executing a command with a relative path is vulnerable to malicious changes in the PATH environment variable.
2	https://github.com/Foxofft/midpoint/security/code-scanning/1	medium	Prototype-polluting function	Functions recursively assigning properties on objects may be the cause of accidental modification of a built-in prototype object.

▼CWE-191: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/61	high	Uncontrolled data in arithmetic expression	Arithmetic operations on uncontrolled data that is not validated can cause overflows.

▼CWE-192: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/60	high	Implicit narrowing conversion in compound assignment	Compound assignment statements (for example 'intvar += longvar') that implicitly cast a value of a wider type to a narrower type may result in information loss and numeric errors such as overflows.

▼CWE-400: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/1	medium	Prototype-polluting function	Functions recursively assigning properties on objects may be the cause of accidental modification of a built-in prototype object.

▼CWE-471: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/1	medium	Prototype-polluting function	Functions recursively assigning properties on objects may be the cause of accidental modification of a built-in prototype object.

▼CWE-681: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/60	high	Implicit narrowing conversion in compound assignment	Compound assignment statements (for example 'intvar += longvar') that implicitly cast a value of a wider type to a narrower type may result in information loss and numeric errors such as overflows.

▼CWE-915: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/1	medium	Prototype-polluting function	Functions recursively assigning properties on objects may be the cause of accidental modification of a built-in prototype object.

▼CWE-088: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/217	medium	Executing a command with a relative path	Executing a command with a relative path is vulnerable to malicious changes in the PATH environment variable.

▼CWE-079: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/1	medium	Prototype-polluting function	Functions recursively assigning properties on objects may be the cause of accidental modification of a built-in prototype object.

▼CWE-094: Unknown CWE

1 alert(s)

#	html_url	severity	description	full_description
1	https://github.com/Foxofft/midpoint/security/code-scanning/1	medium	Prototype-polluting function	Functions recursively assigning properties on objects may be the cause of accidental modification of a built-in prototype object.