WebScanPro Security Assessment Report

Automated Vulnerability Scan Results

Executive Summary

Target: https://mail.google.com/mail/u/0/?login#inbox/FMfcgzQfBGftHpJjRkKltKDbtXPNwzdJ

Scan Date: 2026-01-07 15:53:46

Total Vulnerabilities: 10

8	1	1	0
Critical	High	Medium	Low

Detailed Findings

SQL Injection

Endpoint: https://mail.google.com/v3/signin/identifier?continue=https://mail.google.com/mail/u/0/?login&dsh=S-1174254133:1767801208179755&emr=1&flowEntry=ServiceLogin&flowName
mail.google.com/mail/u/0/?login&ifkv=Ac2yZaX_9sE32M-4EbrktPOe966EAFmVRgLN-wgXd-xjKq6469FZdwyk2DSqQ7Gg4ixe4iN55yVj&osid=1&service=mail

Severity: Critical

Description: SQL Injection vulnerability detected in parameter 'identifier'

Evidence: Payload: ' OR '1'='1 - Error-based SQL injection detected

Mitigation: Use parameterized queries, prepared statements, and input validation

SQL Injection

Endpoint: https://mail.google.com/v3/signin/identifier?continue=https://mail.google.com/mail/u/0/?login&dsh=S-1174254133:1767801208179755&emr=1&flowEntry=ServiceLogin&flowName
mail.google.com/mail/u/0/?login&ifkv=Ac2yZaX_9sE32M-4EbrktPOe966EAFmVRgLN-wgXd-xjKq6469FZdwyk2DSqQ7Gg4ixe4iN55yVj&osid=1&service=mail

Severity: Critical

Description: SQL Injection vulnerability detected in parameter 'hiddenPassword'

Evidence: Payload: ' OR '1'='1 - Error-based SQL injection detected

Mitigation: Use parameterized queries, prepared statements, and input validation

SQL Injection

Endpoint: https://mail.google.com/v3/signin/identifier?continue=https://mail.google.com/mail/u/0/?login&dsh=S-1174254133:1767801208179755&emr=1&flowEntry=ServiceLogin&flowName
mail.google.com/mail/u/0/?login&ifkv=Ac2yZaX_9sE32M-4EbrktPOe966EAFmVRgLN-wgXd-xjKq6469FZdwyk2DSqQ7Gg4ixe4iN55yVj&osid=1&service=mail

Severity: Critical

Description: SQL Injection vulnerability detected in parameter 'usi'

Evidence: Payload: ' OR '1'='1 - Error-based SQL injection detected

Mitigation: Use parameterized queries, prepared statements, and input validation

SQL Injection

Endpoint: https://mail.google.com/v3/signin/identifier?continue=https://mail.google.com/mail/u/0/?login&dsh=S-1174254133:1767801208179755&emr=1&flowEntry=ServiceLogin&flowName
mail.google.com/mail/u/0/?login&ifkv=Ac2yZaX_9sE32M-4EbrktPOe966EAFmVRgLN-wgXd-xjKq6469FZdwyk2DSqQ7Gg4ixe4iN55yVj&osid=1&service=mail

Severity: Critical

Description: SQL Injection vulnerability detected in parameter 'domain'

Evidence: Payload: ' OR '1'='1 - Error-based SQL injection detected

Mitigation: Use parameterized queries, prepared statements, and input validation

SQL Injection

Endpoint: https://mail.google.com/v3/signin/identifier?continue=https://mail.google.com/mail/u/0/?login&dsh=S-1174254133:1767801208179755&emr=1&flowEntry=ServiceLogin&flowName
mail.google.com/mail/u/0/?login&ifkv=Ac2yZaX_9sE32M-4EbrktPOe966EAFmVRgLN-wgXd-xjKq6469FZdwyk2DSqQ7Gg4ixe4iN55yVj&osid=1&service=mail

Severity: Critical

Description: SQL Injection vulnerability detected in parameter 'region'

Evidence: Payload: ' OR '1'='1 - Error-based SQL injection detected

Mitigation: Use parameterized queries, prepared statements, and input validation

SQL Injection

Endpoint: https://mail.google.com/v3/signin/identifier?continue=https://mail.google.com/mail/u/0/?login&dsh=S-1174254133:1767801208179755&emr=1&flowEntry=ServiceLogin&flowName
mail.google.com/mail/u/0/?login&ifkv=Ac2yZaX_9sE32M-4EbrktPOe966EAFmVRgLN-wgXd-xjKq6469FZdwyk2DSqQ7Gg4ixe4iN55yVj&osid=1&service=mail

Severity: Critical

Description: SQL Injection vulnerability detected in parameter 'bgresponse'

Evidence: Payload: ' OR '1'='1 - Error-based SQL injection detected

Mitigation: Use parameterized queries, prepared statements, and input validation

SQL Injection

Endpoint: https://mail.google.com/v3/signin/identifier?
continue=https://mail.google.com/mail/u/0/?
login&dsh=S-1174254133:1767801208179755&emr=1&flowEntry=ServiceLogin&flowName
mail.google.com/mail/u/0/?
login&ifkv=Ac2yZaX_9sE32M-4EbrktPOe966EAFmVRgLN-wgXd-xjKq6469FZdwyk2DSqQ7Gg4ixe4iN55yVj&osid=1&service=mail

Severity: Critical

Description: SQL Injection vulnerability detected in parameter 'at'

Evidence: Payload: ' OR '1'='1 - Error-based SQL injection detected

Mitigation: Use parameterized queries, prepared statements, and input validation

SQL Injection

Endpoint: https://mail.google.com/mail/u/0/?login#inbox/FMfcgzQfBGftHpJjRkKltKDbtXPNwzdJ

Severity: Critical

Description: SQL Injection vulnerability detected in parameter 'hl'

Evidence: Payload: ' OR '1'='1 - Error-based SQL injection detected

Mitigation: Use parameterized queries, prepared statements, and input validation

Weak Authentication

Endpoint: https://mail.google.com/v3/signin/identifier?continue=https://mail.google.com/mail/u/0/?login&dsh=S-1174254133:1767801208179755&emr=1&flowEntry=ServiceLogin&flowName
mail.google.com/mail/u/0/?login&ifkv=Ac2yZaX_9sE32M-4EbrktPOe966EAFmVRgLN-wgXd-xjKq6469FZdwyk2DSqQ7Gg4ixe4iN55yVj&osid=1&service=mail

Severity: High

Description: Login form detected - potential weak authentication mechanisms

Evidence: No rate limiting, weak password policy, or default credentials may be present

Mitigation: Implement strong password policies, multi-factor authentication, and rate limiting

Session Management

Endpoint: https://mail.google.com/mail/u/0/?login#inbox/FMfcgzQfBGftHpJjRkKltKDbtXPNwzdJ

Severity: Medium

Description: Session cookies may lack security flags

Evidence: Cookies should have Secure, HttpOnly, and SameSite attributes

Mitigation: Set appropriate cookie flags and implement session timeout

Generated by WebScanPro - Automated Security Scanner

This report is confidential and intended for authorized personnel only.