ADVANCED IDOR SCAN REPORT

Target:

Scan Time: 2025-12-17 23:57:30

Total Vulnerabilities Found: 23

Advanced techniques used:

- Parameter pollution testing
- JSON globbing (arrays, booleans, wildcards)
- HTTP method variations (POST, PUT, DELETE, PATCH)
- Content-Type header manipulation
- API version enumeration
- Static keyword replacement (current, me)
- UUID and unpredictable ID enumeration

HIGH RISK: 0 vulnerabilities
MEDIUM RISK: 23 vulnerabilities
LOW RISK: 0 vulnerabilities

Vulnerabilities by test type:

basic_numeric: 7
json_wildcard: 2
json_boolean: 2
json_array: 2
zero_padding: 2
decimal_number: 2
negative_number: 2
json_string_array: 1
json_zero_padding: 1
comma_separated: 1
json_decimal: 1

Risk Level: MEDIUM (0.90 confidence)
Test Type: json_string_array
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=%221234%2C1235%22
Parameter: id
Original Value: 1
Test Value: "1234,1235"
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_string_array
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: json_zero_padding

Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=00001235
Parameter: id
Original Value: 1
Test Value: 00001235
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_zero_padding
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: json_wildcard
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=*
Parameter: id
Original Value: 1
Test Value: *
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_wildcard
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: json_boolean
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=true
Parameter: id
Original Value: 1
Test Value: true
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_boolean
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: json_array
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=%5B1234%2C1235%2C1236%5D
Parameter: id
Original Value: 1
Test Value: [1234,1235,1236]
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200

Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_array
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: comma_separated
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=1234%2C1235
Parameter: id
Original Value: 1
Test Value: 1234,1235
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: comma_separated
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: zero_padding
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=0001
Parameter: id
Original Value: 1
Test Value: 0001
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: zero_padding
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: decimal_number
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=1.5
Parameter: id
Original Value: 1
Test Value: 1.5
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: decimal_number
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5222/documents/view?id=1

Modified URL: http://localhost:5222/documents/view?id=999999
Parameter: id
Original Value: 1
Test Value: 999999
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: basic_numeric
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=-9
Parameter: id
Original Value: 1
Test Value: -9
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: basic_numeric
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=11
Parameter: id
Original Value: 1
Test Value: 11
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: basic_numeric
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5222/documents/view?id=1
Modified URL: http://localhost:5222/documents/view?id=0
Parameter: id
Original Value: 1
Test Value: 0
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340

Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: basic_numeric

---

Risk Level: MEDIUM (0.90 confidence)

Test Type: json_decimal
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=1235.0
Parameter: id
Original Value: 2
Test Value: 1235.0
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_decimal

---

Risk Level: MEDIUM (0.90 confidence)

Test Type: json_wildcard
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=%25
Parameter: id
Original Value: 2
Test Value: %
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_wildcard

---

Risk Level: MEDIUM (0.90 confidence)

Test Type: json_boolean
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=false
Parameter: id
Original Value: 2
Test Value: false
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_boolean

---

Risk Level: MEDIUM (0.90 confidence)

Test Type: json_array
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=%5B1234%2C1235%5D

Parameter: id
Original Value: 2
Test Value: [1234,1235]
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: json_array
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: zero_padding
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=0002
Parameter: id
Original Value: 2
Test Value: 0002
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: zero_padding
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: decimal_number
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=2.5
Parameter: id
Original Value: 2
Test Value: 2.5
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: decimal_number
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: negative_number
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=-2
Parameter: id
Original Value: 2
Test Value: -2
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: negative_number

---

Risk Level: MEDIUM (0.90 confidence)
Test Type: negative_number
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=-1
Parameter: id
Original Value: 2
Test Value: -1
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: negative_number
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=-8
Parameter: id
Original Value: 2
Test Value: -8
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: basic_numeric
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=12
Parameter: id
Original Value: 2
Test Value: 12
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: basic_numeric
---

Risk Level: MEDIUM (0.90 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5222/documents/view?id=2
Modified URL: http://localhost:5222/documents/view?id=3
Parameter: id

Original Value: 2
Test Value: 3
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1340 -> 1340
Details: Confidence: 0.90, Auth indicators: 3, Error indicators: 1, Test type: basic_numeric
---

REMEDIATION RECOMMENDATIONS

1. Implement proper access control checks for all sensitive resources
2. Use indirect reference maps instead of direct object references
3. Implement role-based access control (RBAC) for all user operations
4. Validate all user input and implement proper authorization checks
5. Use UUIDs instead of sequential IDs for sensitive resources
6. Implement logging and monitoring for unauthorized access attempts
7. Test all HTTP methods and content types for access control bypass
8. Regularly audit API versions and disable old, insecure versions
9. Implement proper validation for JSON data structures
10. Use parameter binding and strict type checking to prevent parameter pollution