ADVANCED IDOR SCAN REPORT

Target:

Scan Time: 2025-12-18 11:46:49

Total Vulnerabilities Found: 21

Advanced techniques used:

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

CRITICAL RISK: 0 vulnerabilities

HIGH RISK: 0 vulnerabilities

MEDIUM RISK: 21 vulnerabilities

LOW RISK: 0 vulnerabilities

Risk Level: MEDIUM (0,60 confidence)

Test Type: negative_number
Vulnerable URL: http://localhost:5214/messages/drafts?userId=999
Modified URL: http://localhost:5214/messages/drafts?userId=-999
Parameter: userId
Original Value: 999
Test Value: -999
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>

```
<html>
<head>
    <meta charset="u...  : negative_number
```

Vulnerable Data Sample: <!DOCTYPE html>

```
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
```

Risk Level: MEDIUM (0,60 confidence)

Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/messages/drafts?userId=999
Modified URL: http://localhost:5214/messages/drafts?userId=998
Parameter: userId
Original Value: 999

Test Value: 998
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u... : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/messages/drafts?userId=999
Modified URL: http://localhost:5214/messages/drafts?userId=1000
Parameter: userId
Original Value: 999
Test Value: 1000
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u... : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)
Test Type: negative_number
Vulnerable URL: http://localhost:5214/messages/drafts?userId=100
Modified URL: http://localhost:5214/messages/drafts?userId=-100
Parameter: userId
Original Value: 100
Test Value: -100
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>

<html>
<head>
    <meta charset="u... : negative_number
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)

Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/messages/drafts?userId=100
Modified URL: http://localhost:5214/messages/drafts?userId=99
Parameter: userId
Original Value: 100
Test Value: 99
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u... : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)

Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/messages/drafts?userId=100
Modified URL: http://localhost:5214/messages/drafts?userId=101
Parameter: userId
Original Value: 100
Test Value: 101
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u... : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>

```
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
--------------------------------------------------
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: decimal_number
Vulnerable URL: http://localhost:5214/messages/drafts?userId=2
Modified URL: http://localhost:5214/messages/drafts?userId=2%2C5
Parameter: userId
Original Value: 2
Test Value: 2,5
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u...  : decimal_number
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
--------------------------------------------------
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: negative_number
Vulnerable URL: http://localhost:5214/messages/drafts?userId=2
Modified URL: http://localhost:5214/messages/drafts?userId=-2
Parameter: userId
Original Value: 2
Test Value: -2
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u...  : negative_number
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
--------------------------------------------------
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: negative_number
```

Vulnerable URL: http://localhost:5214/messages/drafts?userId=2
Modified URL: http://localhost:5214/messages/drafts?userId=-1
Parameter: userId
Original Value: 2
Test Value: -1
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
   <meta charset="u... : negative_number
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
   <meta charset="utf-8" />
   <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/messages/drafts?userId=2
Modified URL: http://localhost:5214/messages/drafts?userId=999999
Parameter: userId
Original Value: 2
Test Value: 999999
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
   <meta charset="u... : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
   <meta charset="utf-8" />
   <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)
Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/messages/drafts?userId=2
Modified URL: http://localhost:5214/messages/drafts?userId=0
Parameter: userId
Original Value: 2
Test Value: 0
HTTP Method: GET

```
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u...  : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
--------------------------------------------------
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/messages/drafts?userId=2
Modified URL: http://localhost:5214/messages/drafts?userId=1
Parameter: userId
Original Value: 2
Test Value: 1
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u...  : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
--------------------------------------------------
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/messages/drafts?userId=2
Modified URL: http://localhost:5214/messages/drafts?userId=3
Parameter: userId
Original Value: 2
Test Value: 3
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
```

  <meta charset="u... : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8" />
  <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)

Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/shared-links/search?targetId=1
Modified URL: http://localhost:5214/shared-links/search?targetId=0
Parameter: targetId
Original Value: 1
Test Value: 0
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
  <meta charset="u... : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8" />
  <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)

Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/shared-links/search?targetId=2
Modified URL: http://localhost:5214/shared-links/search?targetId=999999
Parameter: targetId
Original Value: 2
Test Value: 999999
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
  <meta charset="u... : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8" />
  <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: basic_numeric
Vulnerable URL: http://localhost:5214/shared-links/search?targetId=2
Modified URL: http://localhost:5214/shared-links/search?targetId=3
Parameter: targetId
Original Value: 2
Test Value: 3
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u...  : basic_numeric
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: wildcard
Vulnerable URL: http://localhost:5214/messages/batch-drafts?userId=1,2
Modified URL: http://localhost:5214/messages/batch-drafts?userId=%25
Parameter: userId
Original Value: 1,2
Test Value: %
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u...  : wildcard
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: wildcard
Vulnerable URL: http://localhost:5214/messages/batch-drafts?userId=1,2
Modified URL: http://localhost:5214/messages/batch-drafts?userId=*
```

```
Parameter: userId
Original Value: 1,2
Test Value: *
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u...  : wildcard
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
--------------------------------------------------
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: case_change
Vulnerable URL: http://localhost:5214/messages/batch-drafts?userId=1,2
Modified URL: http://localhost:5214/messages/batch-drafts?userId=1%2C2
Parameter: userId
Original Value: 1,2
Test Value: 1,2
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details:  : 0,60, :    ;     (3 );      (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u...  : case_change
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...
--------------------------------------------------
```

Risk Level: MEDIUM (0,60 confidence)

```
Test Type: common_value
Vulnerable URL: http://localhost:5214/messages/batch-drafts?userId=1,2
Modified URL: http://localhost:5214/messages/batch-drafts?userId=test
Parameter: userId
Original Value: 1,2
Test Value: test
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
```

Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u... : common_value
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...

Risk Level: MEDIUM (0,60 confidence)
Test Type: common_value
Vulnerable URL: http://localhost:5214/messages/batch-drafts?userId=1,2
Modified URL: http://localhost:5214/messages/batch-drafts?userId=admin
Parameter: userId
Original Value: 1,2
Test Value: admin
HTTP Method: GET
Content Type: N/A
Status Codes: 200 -> 200
Content Lengths: 1185 -> 1185
Details: : 0,60, :   ;   (3);   (: 1,00);   : <!DOCTYPE html>
<html>
<head>
    <meta charset="u... : common_value
Vulnerable Data Sample: <!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Advanced IDOR Test Site</title...

REMEDIATION RECOMMENDATIONS

1. Implement proper access control checks for all sensitive resources
2. Use indirect reference maps instead of direct object references
3. Always validate that the requesting user has permissions to access the requested object
4. Implement logging and monitoring for suspicious access patterns
5. Use UUIDs instead of sequential IDs for sensitive resources
6. Implement proper authorization checks on both GET and POST/PUT requests