

# GoLismero Report



## Targets

http://localhost:3000/wordpress/wp-content/plugins/nextgen-

gallery/products/photocrati\_nextgen/modules/nextgen\_addgallery\_page/static/jquery.filetree/connectors/jqueryFileTree.php

http://localhost:3000/ftp/ http://localhost:3000/ftp http://localhost:3000/

http://localhost:3000/wp-content/plugins/nextgen-

gallery/products/photocrati\_nextgen/modules/nextgen\_addgallery\_page/static/jquery.filetree/connectors/jqueryFileTree.php

http://localhost:3000/ http://localhost:3000/public/ http://localhost:3000/robots.TXT



## Time

**Start:** 2023-08-11 15:25:56.403885 UTC

**End:** 2023-08-11 15:28:12.933383 UTC

**Total:** 0 days, 0 hours, 2 minutes and 16 seconds

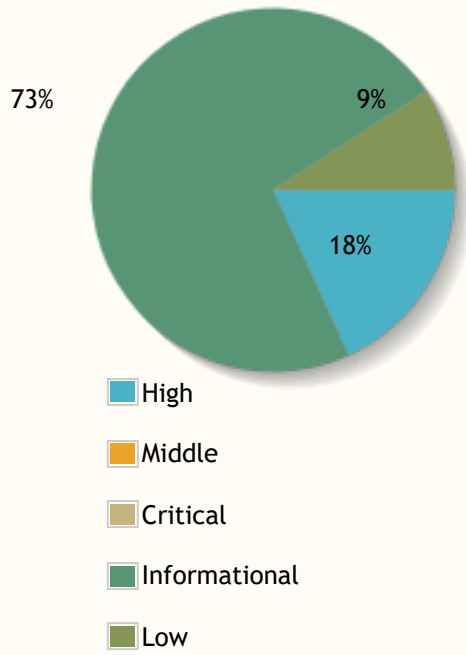


## Vulnerabilities

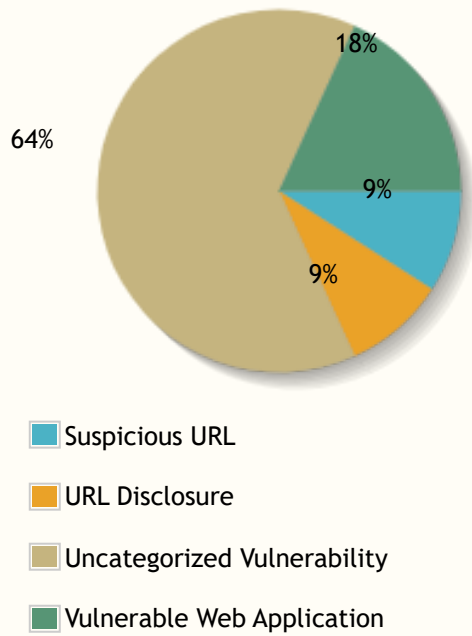
Level	Number
Critical	0
High	2
Middle	0
Low	1
Informational	8
<b>Total</b>	<b>11</b>

## Vulnerabilities by criticality






## Vulnerabilities by type



## Vulnerabilities by target



100%

 http://localhost:3000/

## Vulnerabilities summary

ID	Target	Vulnerability	Criticality ▼		
GOL-2	http://localhost:3000/robot...	URL Disclosure	critical		<a href="#">Details</a>
GOL-3	http://localhost:3000/word... content/plugins/nextgen- gallery/products/photocrat...	Uncategorized Vulnerability	critical		<a href="#">Details</a>
GOL-4	http://localhost:3000/wp- content/plugins/nextgen- gallery/products/photocrat...	Uncategorized Vulnerability	critical		<a href="#">Details</a>
GOL-5	http://localhost:3000/	Uncategorized Vulnerability	critical		<a href="#">Details</a>
GOL-6	http://localhost:3000/	Uncategorized Vulnerability	critical		<a href="#">Details</a>
GOL-7	http://localhost:3000/	Uncategorized Vulnerability	critical		<a href="#">Details</a>
GOL-8	http://localhost:3000/	Uncategorized Vulnerability	critical		<a href="#">Details</a>
GOL-9	http://localhost:3000/	Uncategorized Vulnerability	critical		<a href="#">Details</a>
GOL-1	http://localhost:3000/ftp	Suspicious URL	high		<a href="#">Details</a>
GOL-10	http://localhost:3000/ftp/	Vulnerable Web Application	low		<a href="#">Details</a>
GOL-11	http://localhost:3000/public/	Vulnerable Web Application	low		<a href="#">Details</a>

Total: 11

# Technical report

	ID	Target	Criticality
—	GOL-1	http://localhost:3000/ftp	high
<div>Suspicious URL found un robots.txt</div> <div><div><p><b>Target:</b> http://localhost:3000/ftp</p><p><b>Vulnerability:</b> Suspicious URL (vulnerability/suspicious/url/url)</p><p><b>Criticality:</b> high</p><p><b>Plugin ID:</b> testing/recon/robots</p><p><b>Plugin name:</b> Robots.txt Analyzer</p><p><b>Impact:</b> 0</p><p><b>Severity:</b> 0</p><p><b>Risk:</b> 1</p></div><div><p><b>Description:</b></p><div>An URLs was found in Disallow tag of robots.txt. It can contain confidential content or some information leak.</div></div><div><p><b>Solution:</b></p><div>Please visit the reference website for more information on how to patch this vulnerability.</div></div><div><p><b>References:</b></p><div>https://www.owasp.org/index.php/Information_Leakage (https://www.owasp.org/index.php/Information_Leakage)</div></div></div>			
—	GOL-2	http://localhost:3000/robots.TXT	critical

## URL Disclosure

**Target:** http://localhost:3000/robots.TXT

**Vulnerability:** URL Disclosure (vulnerability/information\_disclosure/url\_disclosure)

**Criticality:** critical

**Plugin ID:** testing/scan/brute\_url\_permutations

**Plugin name:** Bruteforce permutations discovery

**Impact:** 0

**Severity:** 0

**Risk:** 3

### Taxonomy:

CWE-200

### Description:

These are URLs that are accessible but not linked from the web site itself. It may indicate a poor attempt at concealing information. For example: - Backup files: http://www.example.com/ **\*\*index.php.old\*\*** - Alternative file names: http://www.example.com/ **\*\*index4.php\*\*** - Remnants of deployment: http://www.example.com/ **\*\*build.xml\*\*** - Poorly configured servers: http://www.example.com/ **\*\*error\_log\*\*** - Forgotten server file s: http://www.example.com/ **\*\*server-status\*\***

### Solution:

Remove any sensitive information that may have been left behind. If it's not possible to remove it, block access to it from the HTTP server.

### References:

<https://cwe.mitre.org/data/definitions/200.html> (<https://cwe.mitre.org/data/definitions/200.html>)

[https://www.owasp.org/index.php/Information\\_Leakage](https://www.owasp.org/index.php/Information_Leakage)

([https://www.owasp.org/index.php/Information\\_Leakage](https://www.owasp.org/index.php/Information_Leakage))



GOL-3

http://localhost:3000/wordpresswp-content/...

**critical**

User attention required by: Nikto

**Target:** http://localhost:3000/wordpresswp-content/plugins/nextgen-gallery/products/photocrati\_nextgen/modules/nextgen\_addgallery\_page/static/jquery.filetree/connectors/jqueryFile

**Vulnerability:** Uncategorized Vulnerability (vulnerability/generic)

**Criticality:** critical

**Plugin ID:** testing/scan/nikto

**Plugin name:** Nikto

**Impact:** 0

**Severity:** 0

**Risk:** 0

Description:

NextGEN Gallery LFI, see <https://security.dxw.com/advisories/directory-traversal-in-nextgen-gallery-2-0-0/>

Solution:

Please visit the reference website for more information.

References:

<https://security.dxw.com/advisories/directory-traversal-in-nextgen-gallery-2-0-0/>  
(<https://security.dxw.com/advisories/directory-traversal-in-nextgen-gallery-2-0-0/>)

—	GOL-4	http://localhost:3000/wp-content/plugins/ne...	critical
---	-------	--	----------

User attention required by: Nikto

**Target:** http://localhost:3000/wp-content/plugins/nextgen-gallery/products/photocrati\_nextgen/modules/nextgen\_addgallery\_page/static/jquery.filetree/connectors/jqueryFile

**Vulnerability:** Uncategorized Vulnerability (vulnerability/generic)

**Criticality:** critical

**Plugin ID:** testing/scan/nikto

**Plugin name:** Nikto

**Impact:** 0

**Severity:** 0

**Risk:** 0

Description:

NextGEN Gallery LFI, see <https://security.dxw.com/advisories/directory-traversal-in-nextgen-gallery-2-0-0/>

Solution:

Please visit the reference website for more information.

References:

<https://security.dxw.com/advisories/directory-traversal-in-nextgen-gallery-2-0-0/>  
(<https://security.dxw.com/advisories/directory-traversal-in-nextgen-gallery-2-0-0/>)

—	GOL-5	http://localhost:3000/	critical	
---	-------	------------------------	----------	--

User attention required by: Nikto

**Target:** http://localhost:3000/  
**Vulnerability:** Uncategorized Vulnerability (vulnerability/generic)  
**Criticality:** critical  
**Plugin ID:** testing/scan/nikto  
**Plugin name:** Nikto  
**Impact:** 0  
**Severity:** 0  
**Risk:** 0

Description:

The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

Solution:

No additional details are available.

—	GOL-6	http://localhost:3000/	critical	
---	-------	------------------------	----------	--



User attention required by: Nikto

**Target:** http://localhost:3000/  
**Vulnerability:** Uncategorized Vulnerability (vulnerability/generic)  
**Criticality:** critical  
**Plugin ID:** testing/scan/nikto  
**Plugin name:** Nikto  
**Impact:** 0  
**Severity:** 0  
**Risk:** 0

Description:

Uncommon header 'x-recruiting' found, with contents: /#/jobs

Solution:

No additional details are available.

—	GOL-7	http://localhost:3000/	critical	
---	-------	------------------------	----------	--

User attention required by: Nikto

**Target:** http://localhost:3000/  
**Vulnerability:** Uncategorized Vulnerability (vulnerability/generic)  
**Criticality:** critical  
**Plugin ID:** testing/scan/nikto  
**Plugin name:** Nikto  
**Impact:** 0  
**Severity:** 0  
**Risk:** 0

Description:

Uncommon header 'feature-policy' found, with contents: payment 'self'

Solution:

No additional details are available.

—	GOL-8	http://localhost:3000/	critical	
---	-------	------------------------	----------	--

User attention required by: Nikto

**Target:** http://localhost:3000/  
**Vulnerability:** Uncategorized Vulnerability (vulnerability/generic)  
**Criticality:** critical  
**Plugin ID:** testing/scan/nikto  
**Plugin name:** Nikto  
**Impact:** 0  
**Severity:** 0  
**Risk:** 0

Description:

Retrieved access-control-allow-origin header: \*

Solution:

No additional details are available.

—	GOL-9	http://localhost:3000/	critical	
---	-------	------------------------	----------	--

User attention required by: Nikto

**Target:** http://localhost:3000/  
**Vulnerability:** Uncategorized Vulnerability (vulnerability/generic)  
**Criticality:** critical  
**Plugin ID:** testing/scan/nikto  
**Plugin name:** Nikto  
**Impact:** 0  
**Severity:** 0  
**Risk:** 0

Description:

Server leaks inodes via ETags, header found with file /, fields: 0xW/7c3 0x189e4c3a881

Solution:

No additional details are available.

—	GOL-10	http://localhost:3000/ftp/	low	
---	--------	----------------------------	-----	--

# Vulnerable Web Application

**Target:** http://localhost:3000/ftp/  
**Vulnerability:** Vulnerable Web Application (vulnerability/infrastructure/vulnerable\_webapp)  
**Criticality:** low  
**Plugin ID:** testing/scan/nikto  
**Plugin name:** Nikto  
**Impact:** 0  
**Severity:** 0  
**Risk:** 0

**Taxonomy:**  
OSVDB-3092

**Description:**  
This might be interesting...

**Solution:**  
Apply all missing patches or upgrade to a newer version.

**References:**  
<http://osvdb.org/show/osvdb/3092> (<http://osvdb.org/show/osvdb/3092>)

—	GOL-11	http://localhost:3000/public/	low	
---	--------	-------------------------------	-----	--

## Vulnerable Web Application

**Target:** http://localhost:3000/public/

**Vulnerability:** Vulnerable Web Application (vulnerability/infrastructure/vulnerable\_webapp)

**Criticality:** low

**Plugin ID:** testing/scan/nikto

**Plugin name:** Nikto

**Impact:** 0

**Severity:** 0

**Risk:** 0

### Taxonomy:

OSVDB-3092

### Description:

This might be interesting...

### Solution:

Apply all missing patches or upgrade to a newer version.

### References:

<http://osvdb.org/show/osvdb/3092> (<http://osvdb.org/show/osvdb/3092>)

