

Product Solutions Resources Open Source Enterprise Pricing

🔍

Sign in

Sign up

📁 projectdiscovery / nuclei-templates Public

🔔 Notifications

🍴 Fork 2.6k

★ Star 9.2k

<> Code

🔗 Issues 93

🔗 Pull requests 89

💬 Discussions

🔄 Actions

📁 Projects

📖 Wiki

🛡 Security

📈 Insights

📁 Files

🔑 9d28893

🔍

🔍 Go to file

> .github

> cnvd

> cves

> default-logins

> dns

> exposed-panels

> exposures

> file

▼ fuzzing

- 📄 adminer-panel-fuzz.yaml
- 📄 cache-poisoning-fuzz.yaml
- 📄 header-command-injection.yaml
- 📄 iis-shortname.yaml
- 📄 linux-lfi-fuzzing.yaml
- 📄 mdb-database-file.yaml
- 📄 prestashop-module-fuzz.yaml
- 📄 valid-gmail-check.yaml
- 📄 wordpress-plugins-detect.yaml
- 📄 wordpress-themes-detect.yaml
- 📄 wordpress-weak-credentials.yaml
- 📄 xff-403-bypass.yaml

> headless

> helpers

> iot

> miscellaneous

> misconfiguration

> network

> ssl

> takeovers

> technologies

> token-spray

> vulnerabilities

> workflows

📄 .gitignore

📄 .new-additions

📄 .nuclei-ignore

nuclei-templates / fuzzing / iis-shortname.yaml 📄

forgedhallpass refactor: Description field uniformization 209538b · 2 years ago 🕒 History

Code

Blame

43 lines (37 loc) · 1.31 KB

Raw







📄

📥

🔗

```
1      id: iis-shortname
2
3      info:
4        name: iis-shortname
5        author: nodauf
6        severity: info
7        description: When IIS uses an old .Net Framework it's possible to enumeration folder
8        reference:
9          - https://github.com/lijiejie/IIS_shortname_Scanner
10         - https://www.exploit-db.com/exploits/19525
11      tags: fuzz
12
13      requests:
14        - raw:
15          - |
16            GET /N0t4xist*~1*/a.aspx HTTP/1.1
17            Host: {{Hostname}}
18            Origin: {{BaseURL}}
19            Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
20
21          - |
22            GET /*~1*/a.aspx' HTTP/1.1
23            Host: {{Hostname}}
24            Origin: {{BaseURL}}
25            Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
26
27          - |
28            OPTIONS /N0t4xist*~1*/a.aspx HTTP/1.1
29            Host: {{Hostname}}
30            Origin: {{BaseURL}}
31            Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
32
33          - |
34            OPTIONS /*~1*/a.aspx' HTTP/1.1
35            Host: {{Hostname}}
36            Origin: {{BaseURL}}
37            Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
38
39      req-condition: true
40      matchers:
41        - type: dsl
42          dsl:
43            - "status_code_1!=404 && status_code_2 == 404 || status_code_3 != 404 && stat
```

Page 1 of 2

-  .pre-commit-config.yml
-  .yamllint
-  CODE_OF_CONDUCT.md
-  CONTRIBUTING.md
-  LICENSE.md
-  PULL REQUEST TEMPLATE.md