Sign in

projectdiscovery / **nuclei-templates** Public

Notifications Fork 2.6k Star 9.2k

Code Issues 95 Pull requests 96 Discussions Actions Projects Wiki

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

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

43 lines (37 loc) · 1.31 KB

Code Blame Raw

```yaml
id: iis-shortname

info:
  name: iis-shortname
  author: nodauf
  severity: info
  description: When IIS uses an old .Net Framework it's possible to enumeration folder with the sym
  reference:
    - https://github.com/lijiejie/IIS_shortname_Scanner
    - https://www.exploit-db.com/exploits/19525
  tags: fuzz

requests:
  - raw:
      - |
        GET /N0t4xist*~1*/a.aspx HTTP/1.1
        Host: {{Hostname}}
        Origin: {{BaseURL}}
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0

      - |
        GET /*~1*/a.aspx' HTTP/1.1
        Host: {{Hostname}}
        Origin: {{BaseURL}}
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0

      - |
        OPTIONS /N0t4xist*~1*/a.aspx HTTP/1.1
        Host: {{Hostname}}
        Origin: {{BaseURL}}
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0

      - |
        OPTIONS /*~1*/a.aspx' HTTP/1.1
        Host: {{Hostname}}
        Origin: {{BaseURL}}
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0

    req-condition: true
    matchers:
      - type: dsl
        dsl:
          - "status_code_1!=404 && status_code_2 == 404 || status_code_3 != 404 && status_code_4 ==
```