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

```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
  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/

      - |
        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/

      - |
        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/

      - |
        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/

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

- .pre-commit-config.yml
- .yamllint
- CODE_OF_CONDUCT.md
- CONTRIBUTING.md
- LICENSE.md
- PULL_REQUEST_TEMPLATE.md