Vulnerability Assessment Report: www.bbc.co.uk

SECURITY SCORE: 90/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open
443	https		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 151.101.208.81
+ Target Hostname: www.bbc.co.uk
+ Target Port: 80
+ Start Time: 2026-02-16 16:25:13 (GMT0)
---------------------------------------------------------------------------
+ Server: BBC-GTM
+ Retrieved via header: 1.1 BBC-GTM, 1.1 Belfrage, 1.1 varnish
+ Retrieved x-served-by header: cache-bom-vanm7210072-BOM
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-timer' found, with contents: S1771259115.878818,VS0,VE1
+ Uncommon header 'alt-svc' found, with contents:
h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
+ Uncommon header 'x-bbc-edge-cache-status' found, with contents: HIT
+ Uncommon header 'x-cache-hits' found, with contents: 3
+ Uncommon header 'report-to' found, with contents: {"group":"default","max_age":2592000,"endp
oints":[{"url":"https://default.bbc-reporting-api.app/report-endpoint","priority":1}],"include
_subdomains":true}
+ Uncommon header 'nel' found, with contents:
{"report_to":"default","max_age":2592000,"include_subdomains":true,"failure_fraction":0.25}
+ Uncommon header 'strict-transport-security' found, with contents: max-age=31536000; preload
+ Uncommon header 'x-fastly-cache-status' found, with contents: HIT
+ Uncommon header 'permissions-policy' found, with contents: browsing-topics=(),
join-ad-interest-group=(), run-ad-auction=()
+ Uncommon header 'req-svc-chain' found, with contents: FASTLY,GTM,BELFRAGE
+ Uncommon header 'x-cache-age' found, with contents: 13
+ Uncommon header 'x-robots-tag' found, with contents: bingbot: noarchive
+ Uncommon header 'x-fastly-pre-flight-cache' found, with contents: MISS, HIT
+ Uncommon header 'x-bbc-no-scheme-rewrite' found, with contents: 1
+ Uncommon header 'origin-agent-cluster' found, with contents: ?0
+ Uncommon header 'x-fastly-pre-flight-cache-status' found, with contents: HIT
+ Uncommon header 'fastly-restarts' found, with contents: 1
+ Uncommon header 'x-cache' found, with contents: HIT
+ Uncommon header 'x-served-by' found, with contents: cache-bom-vanm7210072-BOM
+ Root page / redirects to: https://www.bbc.co.uk/
```

```
+ Server leaks inodes via ETags, header found with file /cgi-bin/, fields: 0x61deec4b 0x7e9a
+ Uncommon header 'x-fastly-cache-reason' found, with contents: NO-CACHE-CONTROL
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-amzn-trace-id' found, with contents:
Root=1-699344f4-049c0c6941f820167d0e9e9e
+ Uncommon header 'x-amzn-requestid' found, with contents: d490f300-2479-484c-ba73-aebdb8a038f6
+ Uncommon header 'x-amz-apigw-id' found, with contents: Y4e2NG9IjoEFsNQ=
+ Uncommon header 'x-bbc-origin-response-status' found, with contents: 200
+ File/dir '/afrique/search/' in robots.txt returned a non-forbidden or redirect HTTP code
(301)
+ File/dir '/arabic/search/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Uncommon header 'x-backend-status' found, with contents: 404
+ File/dir '/azeri/search/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ File/dir '/bengali/search/' in robots.txt returned a non-forbidden or redirect HTTP code
(301)
+ File/dir '/burmese/search/' in robots.txt returned a non-forbidden or redirect HTTP code
(301)
+ File/dir '/cbbc/search/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ File/dir '/cbeebies/search/' in robots.txt returned a non-forbidden or redirect HTTP code
(301)
+ File/dir '/education/bitesize/' in robots.txt returned a non-forbidden or redirect HTTP code
(301)
+ File/dir '/education/dev/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ File/dir '/education/images/' in robots.txt returned a non-forbidden or redirect HTTP code
(301)
+ File/dir '/education/nav/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ File/dir '/education/navigation/' in robots.txt returned a non-forbidden or redirect HTTP
code (301)
+ File/dir '/education/ximages/' in robots.txt returned a non-forbidden or redirect HTTP code
(301)
+ Cookie BBC-UID created without the httponly flag
+ File/dir '/gahuza/search/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ File/dir '/hausa/search/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ File/dir '/hindi/search/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ File/dir '/indonesia/search/' in robots.txt returned a non-forbidden or redirect HTTP code
(301)
+ File/dir '/kyrgyz/search/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ File/dir '/mundo/search/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+
```

3. Crawled Website Endpoints

- https://www.bbc.co.uk/sounds
- https://www.bbc.co.uk/news/articles/cvg36pknpl5o
- https://www.bbc.co.uk/news/articles/cq6qge7rmm1o
- https://www.bbc.co.uk/news/articles/c70ne31d884o
- https://www.bbc.co.uk/news/articles/c99jyexve1jo
- https://www.bbc.co.uk/sport/winter-olympics/live/cgm4k7p22rzt
- https://www.bbc.co.uk/news/uk
- https://www.bbc.co.uk/schedules/p00fzl9m
- https://www.bbc.co.uk/news/health
- https://www.bbc.co.uk/news/articles/c0q3wx2j3x1o
- https://www.bbc.co.uk/news/politics
- https://www.bbc.co.uk/news/articles/c4ge7n3pq62o
- https://www.bbc.co.uk/accessibility
- https://www.bbc.co.uk/news/education

- https://www.bbc.co.uk/news/articles/cdxgew324r9o

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

Attack: Session Hijacking / Cookie Theft
Mitigation: Set HttpOnly and Secure flags.

Attack: Clickjacking Vulnerability
Mitigation: Implement X-Frame-Options: SAMEORIGIN or DENY.