UpGuard Report

Oct 14 2020 UpGuard

medical.ansellsampleportal.com LAST SCANNED OCT 14 2020
162.144.47.105

665 / 950

9 / 28 checks failed

HTTP Strict Transport Security (HSTS) not enforced

Without HSTS enforced, people browsing this site are more susceptible to man-in-the-middle attacks. The server should be configured to support HSTS.

Expected	`Headers > strict-transport-security: [header set]`
Actual	`[not set]`

HttpOnly cookies not used

When HttpOnly cookies are not used, the cookies can be accessed on the client, which enables certain type of client-side attacks. The website configuration should be changed to enforce HttpOnly cookies.

Expected	`Headers: [all set-cookie headers include 'httponly']`
Actual	`Set-Cookie: ShoppingCartSession`

Secure cookies not used

When secure cookies are not used, there is an increased risk of third parties intercepting information contained in these cookies. The website configuration should be changed so that all 'Set-Cookie' headers include 'secure'.

Expected	`Headers: [all set-cookie headers include 'secure']`
Actual	`Set-Cookie: ShoppingCartSession`

'IMAP' port open

The 'IMAP' service is running and exposed to the internet. The configuration of the server should be reviewed and unnecessary ports closed.

Expected	`Ports > 'IMAP': [closed]`
Actual	`'IMAP': [listening on port 993]`

'POP3' port open

The 'POP3' service is running and exposed to the internet. The configuration of the server should be reviewed and unnecessary ports closed.

Expected	`Ports > 'POP3': [closed]`
Actual	`'POP3': [listening on port 995]`

'SMTP' port open

The 'SMTP' service is running and exposed to the internet. The configuration of the server should be reviewed and unnecessary ports closed.

Expected	`Ports > 'SMTP': [closed]`
Actual	`'SMTP': [listening on ports 465, 26]`

'SSH' port open

The 'SSH' service is running and exposed to the internet. The configuration of the server should be reviewed and unnecessary ports closed.

Expected	`Ports > 'SSH': [closed]`
Actual	`'SSH': [listening on port 22]`

Exim Internet Mailer 4.93 has potential vulnerabilities

Exim Internet Mailer 4.93 has vulnerablities which might be exploitable under certain conditions. Affected domains should be checked to determine which vulnerabilities might pose a risk.

Expected	`Vulnerabilities > Exim Internet Mailer 4.93: [none found]`
Actual	`CVE-2020-8015, CVE-2020-12783`

OpenSSH 5.3 has potential vulnerabilities

OpenSSH 5.3 has vulnerablities which might be exploitable under certain conditions. Affected domains should be checked to determine which vulnerabilities might pose a risk.

Expected	`Vulnerabilities > OpenSSH 5.3: [none found]`
Actual	`CVE-2010-4478, CVE-2010-4478, CVE-2010-4755, CVE-2010-4755, CVE-2010-5107, CVE-2010-5107, CVE-2011-4327, CVE-2011-4327, CVE-2011-5000, CVE-2011-5000, CVE-2012-0814, CVE-2012-0814, CVE-2014-1692, CVE-2014-2532, CVE-2014-2653, CVE-2015-5352, CVE-2015-5600, CVE-2015-6563, CVE-2015-6564, CVE-2015-8325, CVE-2016-0777, CVE-2016-1908, CVE-2016-3115, CVE-2016-6210, CVE-2016-6515, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708, CVE-2017-15906, CVE-2018-15473, CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111, CVE-2020-15778`

19 / 28 checks passed

Certificate not found on our revoked certificate list

The site's certificate chain was checked against our list of revoked certificates.

Expected	`SSL > Revoked: false`
Actual	`false`

SSL available

SSL is supported for this site.

Expected	`SSL: true`
Actual	`true`

Not suspected of unwanted software

This website does not appear to be attempting to install unwanted software.

Expected	`Google Safe Browsing > Unwanted Software: false`
Actual	`false`

SSL has not expired

SSL certificate has not expired.

Expected	`SSL > Expired: [has not expired]`
Actual	`2020-12-28 10:06:46 UTC`

Not a suspected phishing page

This site does not appear to be a forgery or imitation of another website.

Expected	`Google Safe Browsing > Phishing: false`
Actual	`false`

Hostname matches SSL certificate

The site's hostname matches the SSL certificate.

Expected	`SSL > Host Match: [hostname matches SSL certificate]`
Actual	`medical.ansellsampleportal.com matches medical.ansellsampleportal.com`

All traffic routed via HTTPS

All communication with the website occurs using HTTPS.

Expected	`HTTP Accessible: false`
Actual	`false`

Not a suspected malware provider

This website does not appear to contain malicious code.

Expected	`Google Safe Browsing > Malware: false`
Actual	`false`

Strong SSL algorithm

Industry standard SHA-256 encryption in use.

Expected	`SSL > Algorithm: [at least 'sha256']`
Actual	`SHA256-RSA`

SSL does not expire within 20 days

SSL certificate does not expire within 20 days.

Expected	`SSL > Expires: [does not expire in the next 20 days]`
Actual	`2020-12-28 10:06:46 UTC`

No insecure SSL/TLS versions available

No insecure SSL/TLS versions are available for this site.

Expected	`SSL > Insecure Protocol Versions: [none found]`
Actual	`[none found]`

X-Powered-By header not exposed

Information about specific technology used on the server is obscured.

Expected	`Headers > x-powered-by: [not set]`
Actual	`[not set]`

Not vulnerable to CVE-2014-3566 (POODLE)

The server does not support SSLv3, and is not vulnerable to the POODLE attack.

Expected	`Vulnerabilities > CVE-2014-3566: [not vulnerable]`
Actual	`[not vulnerable]`

Server information header not exposed

Ensuring the server information header is not exposed reduces the ability of attackers to exploit certain vulnerabilities.

Expected	`Headers > server: [does not contain version number]`
Actual	`Apache`

Not vulnerable to CVE-2015-0204 (FREAK)

The server does not offer RSA_EXPORT cipher suites, so clients are not vulnerable to the FREAK attack.

Expected	`Vulnerabilities > CVE-2015-0204: [not vulnerable]`
Actual	`[not vulnerable]`

Not vulnerable to CVE-2015-4000 (Logjam)

The server is using strong Diffie-Hellman parameters and is not vulnerable to the Logjam attack.

Expected	`Vulnerabilities > CVE-2015-4000: [not vulnerable]`
Actual	`[not vulnerable]`

Not vulnerable to CVE-2014-0160 (Heartbleed)

A bug in OpenSSL's implementation of the TLS heartbeat extension allows access to portions of memory on the targeted host e.g. cryptographic keys and passwords.

Expected	`Vulnerabilities > CVE-2014-0160: [not vulnerable]`
Actual	`[not vulnerable]`

ASP.NET version header not exposing specific ASP.net version

Ensuring the ASP.NET version header is not exposing a specific version makes it harder for attackers to exploit certain vulnerabilities.

Expected	`Headers > x-aspnet-version: [not set]`
Actual	`[not set]`

ASP.NET version header not exposed

Ensuring the ASP.NET version header is not exposed makes it harder for attackers to exploit certain vulnerabilities.

Expected	`Headers > x-aspnet-version present: [not present]`
Actual	`[not present]`