Recall various web security guidelines discussed in HTTPS lessons, comment on what security features are present or missing in one of the 23 IITs websites and as a web security specialist what you suggest to the webadmin of the website under study to fix the issues found or further enhance the security of their website. The website that you need to study is (ROLLNO%23)+1. Where ROLLNO is the last 5 digits of your roll no (follow the same for Assignment-2). Order of 23 IITs is as per wikipedia list: https://en.wikipedia.org/wiki/Indian_Institutes_of_Technology

HTTP Header Checker - Server Headers Check
https://dnschecker.org/server-headers-check.php

SSL Certificate Checker - Diagnostic Tool | DigiCert.com
https://www.digicert.com/help/

SSL Server Test (Powered by Qualys SSL Labs)
https://www.ssllabs.com/ssltest/

Indian Institutes of Technology - Wikipedia
https://en.wikipedia.org/wiki/Indian_Institutes_of_Technology

Your answer
IIT Ropar - https://www.iitrpr.ac.in/
Security features present:
it is following no-cache, must-revalidate cache control.
The signature algorithm used is SHA256-RSA with 2046bits.
TLS versions supported are TLSv1.0, TLSv1.1, TLSv1.2.
This server is not vulnerable to the Heartbleed Bug.
There are no vulnerable Debian keys.
TLS certificate is correctly installed(no issues with certificate).

Security features missing:
CRL status is not enabled.
This server does not support Forward Secrecy with the reference browsers.
No support for TLSv1.3.
DNSSEC is disabled. Attackers might manipulate DNS to redirect their victims to servers of their choice.
CAA is disabled. So there is no restriction on the CAs and any CA can issue certificates for their domain names.
Servers that don't enforce cipher suite preferences select the first cipher suite they support from the list provided by clients. This approach doesn't guarantee that the best-possible cipher suite is negotiated.
This host doesn't use HSTS, which means that its users can be easily attacked via MITM attacks.
CSP is disabled.
Expect-CT is disabled. So websites cannot monitor problems related to their Certificate Transparency (CT) compliance.

Suggestions:
The certificate will expire in the next 236days. renew it when needed
Drupal 7 support as x-generator will be supported only for the next 2.5yr. it's better to update to the latest version.

TLS 1.0 and TLS 1.1 are deprecated protocols that should be disabled if possible. It is better to migrate to TLSv1.3 due to its simplicity and is more secure.
Use of ECDHE or DHE or temporary session keys will provide PFS(perfect forward secrecy).
Use of GCM or CHACHA20 will provide authenticated encryption.
Consider deploying HSTS to disable certificate warnings and increase content and cookie security.