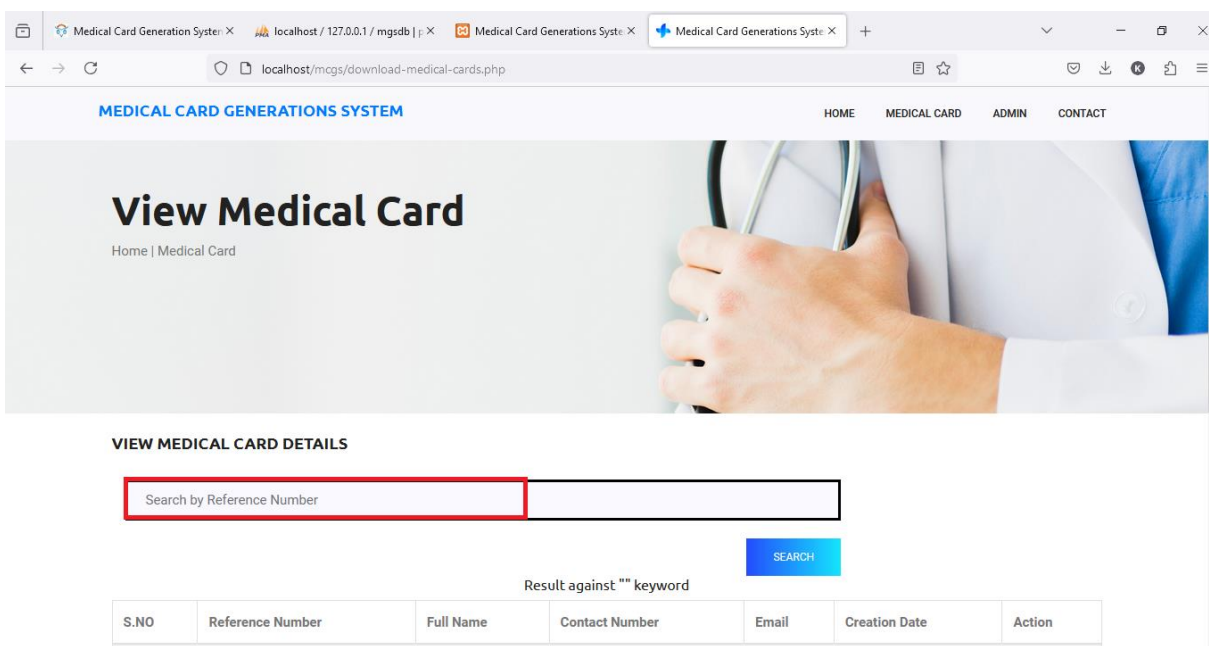


Reflected Cross Site Scripting (XSS) vulnerability was found in “/mcgs/download-medical-cards.php” in Medical Card Generation System v1.0 allows remote attackers to execute arbitrary code via "searchdata" POST request parameter.

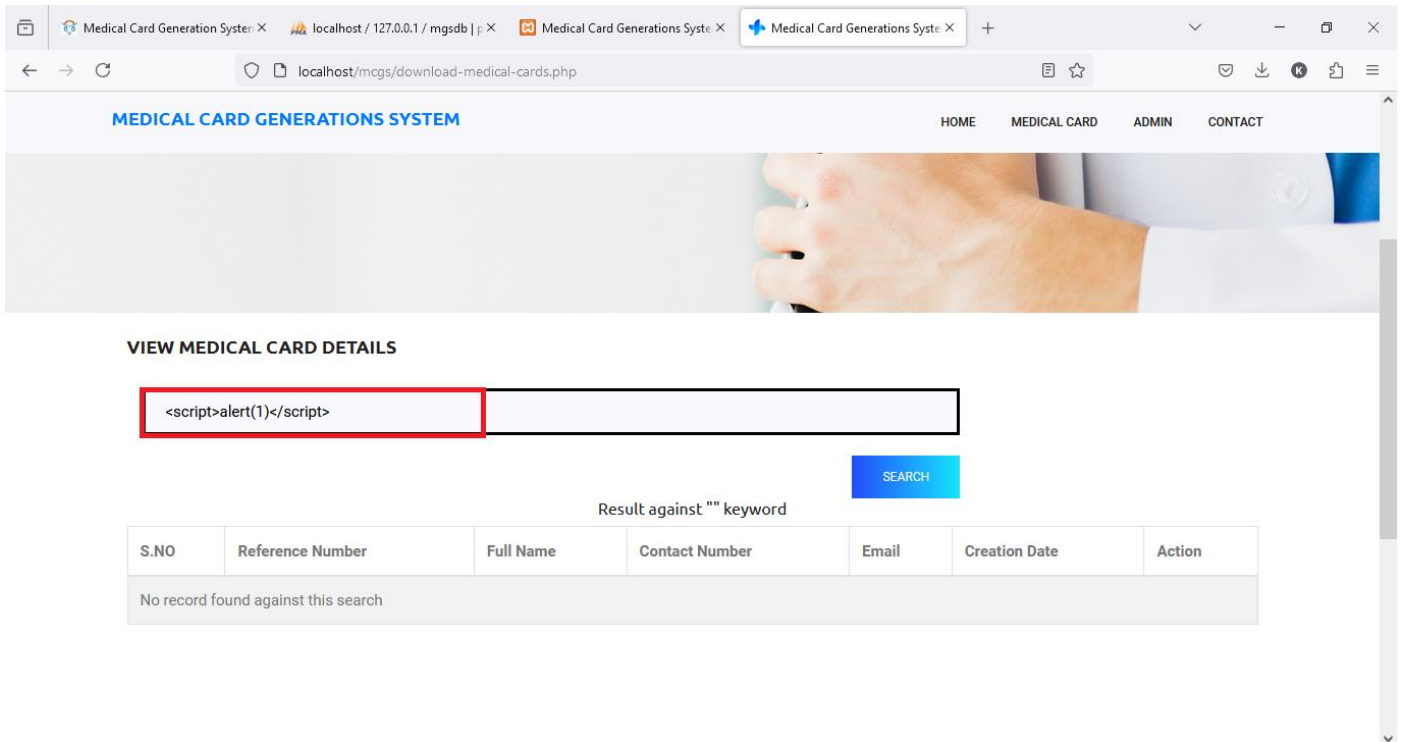
Field	Details
Affected Vendor	PHPGurukul
Affected Product Name	Medical Card Generation System
Product Official Website URL	https://phpgurukul.com/medical-card-generation-system-using-php-and-mysql/
Affected Components	<ul style="list-style-type: none">- Version: V 1.0- Affected Code File: /mcgs/download-medical-cards.php- Affected Parameter: searchdata- Method: POST

Steps to Reproduce:

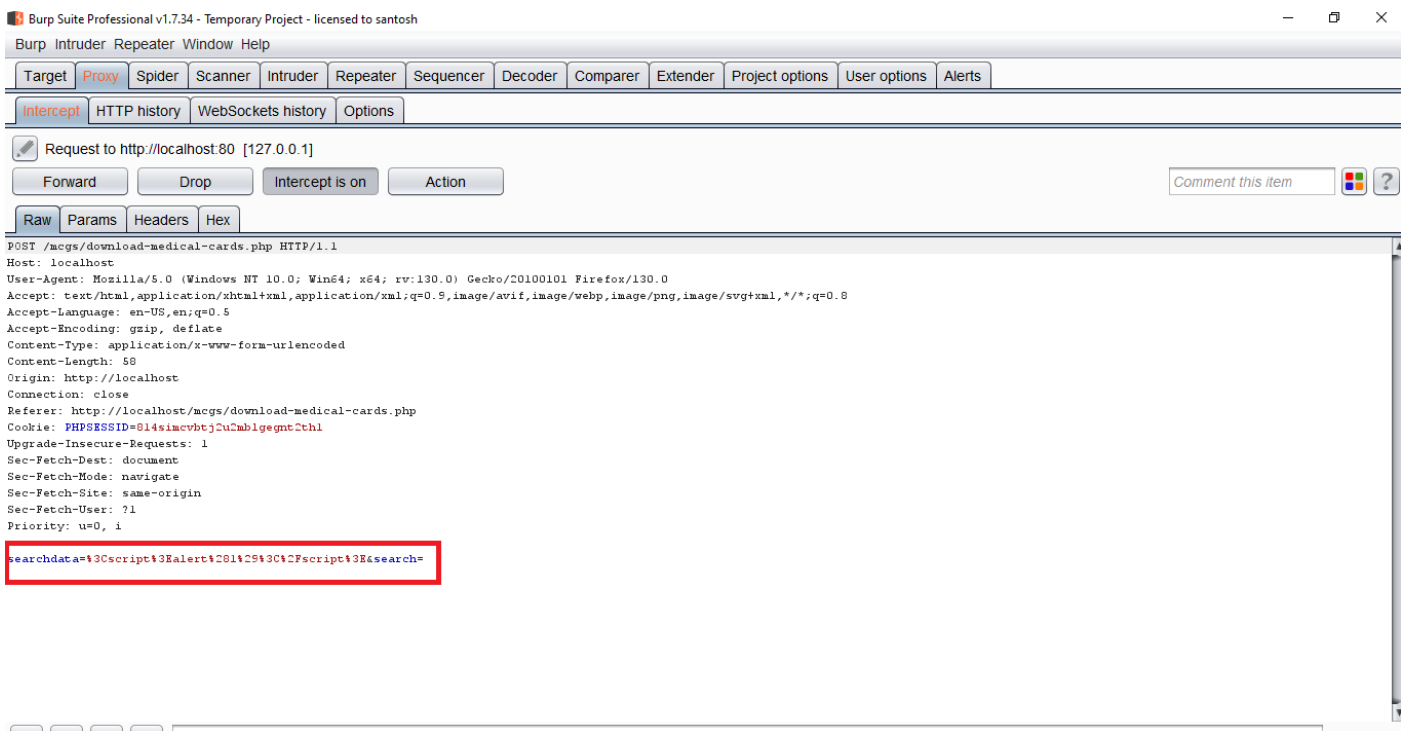
Step 1: <http://localhost/mcgs/download-medical-cards.php>



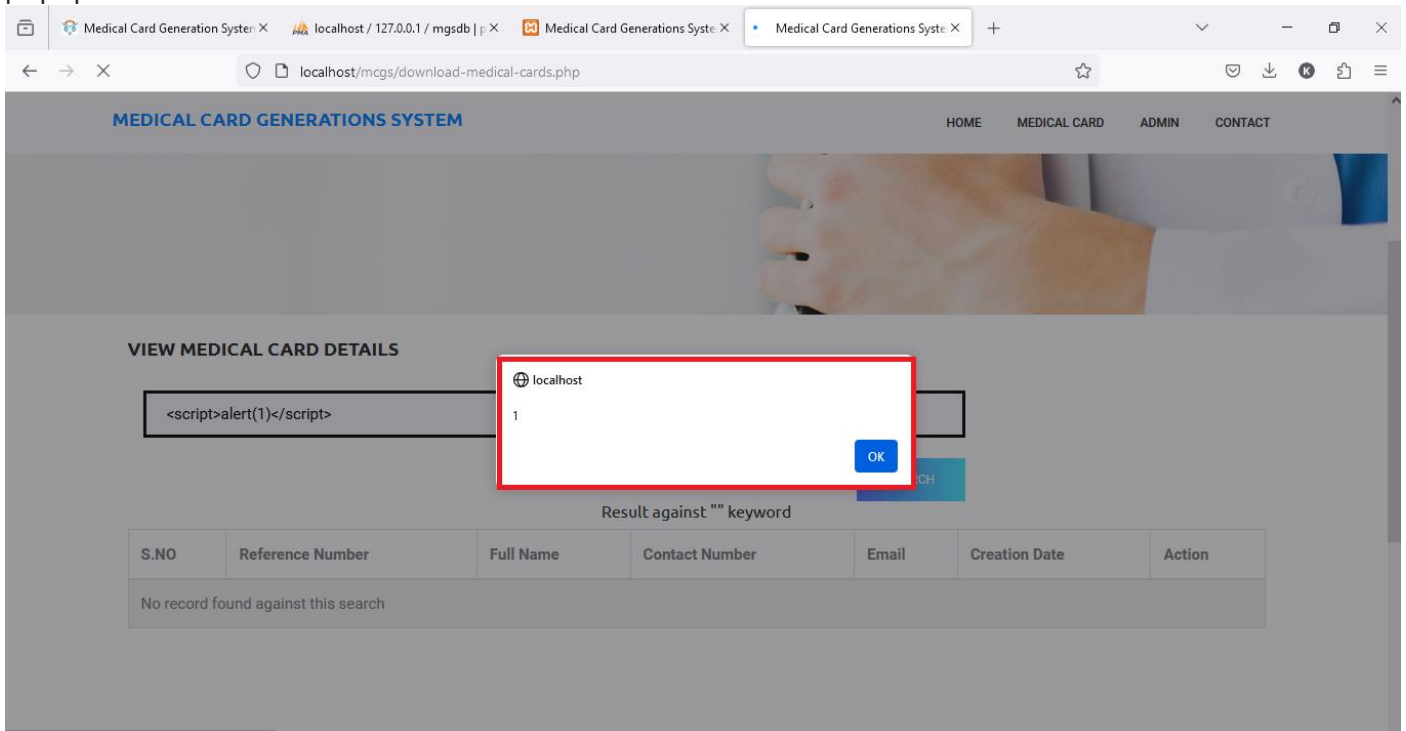
S.NO	Reference Number	Full Name	Contact Number	Email	Creation Date	Action
------	------------------	-----------	----------------	-------	---------------	--------



Step 2: In search bar, provide values `<Script>alert(1)</Script>` and enable burpsuite to confirm the parameter.



Step 3: After forwarding the request, observe in the browser that the payload is executed, resulting in a popup.



Mitigation/recommendations

- <https://portswigger.net/web-security/cross-site-scripting>
- [https://cheatsheetseries.owasp.org/cheatsheets/Cross Site Scripting Prevention Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)