# CVE-2021-35061

## Vulnerability information

Multiple **Cross-site scripting** (XSS) vulnerabilities in DRK Odenwaldkreis Testerfassung March2021 allow remote attackers to inject arbitrary web script or HTML via all parameters to HTML form fields in all components.

## Vulnerability description

JavaScript or HTML Cross Site Scripting (XSS) vulnerability was found on various forms used in DRK Odenwaldkreis Testerfassung web portal. The multiple vulnerabilities have been demonstrated and have been confirmed by the developers in code version March-2021. DRK Odenwaldkreis and developers were contacted, vulnerability was reported, confirmed and fixed in latest software release.

## Mitigation

Mitigation can be accomplished by filtering user input with PHP function **strip_tags()** and using for example an allow list of allowed characters.

## Technical Description

Injection of JavaScript alert box to demonstrate Cross Site Scripting (XSS) vulnerability.

```
result.php?TOKEN=">1234567890&ID=[NUMBER]
```

The **$_POST** and **$_GET** variables passed from HTML forms should be passed to an **input filtering** function which checks for allowed characters, cast the type of the variable (integer, float, string) and **strip_tags()** should be used to remove all characters used in JavaScript or HTML.

```
/**
 * Input from $_POST (or $_GET) is not filtered.
 *
 * Mitigation: Input filtering, Allow list, deny of manipulated input,
 * PHP escape function strip_tags().
 */
$token = $_POST['token'];
$customer_key = $_POST['customer_key'];
//$gebdatum = $_POST['gebdatum'];
$gebdatum_d = $_POST['gebdatum_d'];
$gebdatum_m = $_POST['gebdatum_m'];
$gebdatum_y = $_POST['gebdatum_y'];
$gebdatum=sprintf('%04d',$gebdatum_y).'-'.sprintf('%02d',
$gebdatum_m).'-'.sprintf('%02d',$gebdatum_d);
```

## Disclosure timeline

- 2021-05-31 Contacted DRK Odenwaldkreis by phone to report Multiple Cross Site Scripting vulnerabilities
- 2021-05-31 Contacted by developers by phone, send report and analysis to developers
- 2021-06-02 Reviewed parts of source code and performed tests like directory listing, added additional findings and informed developers
- 2021-06-06 Reported Shell Metacharacter Injection vulnerability and send proof of concept
- 2021-06-11 Asked Hessen Cyber Competence Center for consultation for responsible disclosure process
- 2021-06-12 Explained in detail proof of concept of Shell Metacharacter Injection. Attacker requires a valid test token, possible to execute code
- 2021-06-18 Tested again for XSS in web applications form fields, XSS still present. Contacted developers and informed that XSS vulnerability is not fixed
- 2021-06-18 Requested to reserve two CVE at mitre.org. CVE-2021-35061 and CVE-2021-35062 were reserved
- 2021-08-30 Publication of CVE after 90 days (similar to Google Project Zero disclosure timeline)