香港浸會大學 HONG KONG BAPTIST UNIVERSITY

Steven Y C CHAN <sycchan@hkbu.edu.hk>

RE: 1st Notification of V-Scan Result [RITM0078284] - FAIL

1 message

Steven Y C CHAN <sycchan@hkbu.edu.hk> Tue, Jun 8, 2021 at 7:44 PM
To: "Calvin S. LAW" <calvinlaw@hkbu.edu.hk>
Cc: ITO Security Team <hkbuitosec@hkbu.edu.hk>

Dear Calvin,

We regret to inform you that the following website has **FAILED** the vulnerability assessment conducted on 7 & 8 *June 2021*.

Required rectification:

Rectification is required. Below is a "Summary of Scan Result" with the enclosed reports for details of the identified vulnerabilities. Please:

- Fix the required High/Medium risk item(s) listed in "**Summary of Result**" below.

Request for re-assessment:

Please inform us to perform re-assessment after completing the rectification.

Vulnerability Assessment for sfa.hkbu.edu.hk/sfaApplication/ (UAT) - RITM0078284			
Website URL :	https://sfa.hkbu.edu.hk/sfaApplication/ (Production) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user (UAT-user) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=operator (UAT-operator) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=admin (UAT-admin) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=endorser (UAT-endorser) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=approver (UAT-approver) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=advisor (UAT-advisor)		
Assessment Date:	7 & 8 June 2021 – 1st Scan		
Overall Result / Risk Level:	FAIL / High Risk		
Action Required:	Remediation and Re-scan		
Scan Report (Encl.):	2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=user.pdf		
Summary of Result:			
Severity	**Risk #**	**Description**	**Remediation / Follow Up Action**
High (2)	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities(1)	Remediation is required as recommended in the report.
	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities(1)	

Vulnerability Assessment for sfa.hkbu.edu.hk/sfaApplication/ (UAT) - RITM0078284			
Website URL :	https://sfa.hkbu.edu.hk/sfaApplication/ (Production) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user (UAT-user) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=operator (UAT-operator) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=admin (UAT-admin) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=endorser (UAT-endorser) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=approver (UAT-approver) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=advisor (UAT-advisor)		
Assessment Date:	7 & 8 June 2021 – 1st Scan		
Overall Result / Risk Level:	FAIL / High Risk		
Action Required:	Remediation and Re-scan		
Scan Report (Encl.):	2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=operator.pdf		
Summary of Result:			
Severity	**Risk #**	**Description**	**Remediation / Follow Up Action**
High (4)	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities(2)	Remediation is required as recommended in the report.

	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities(2)	

Vulnerability Assessment for sfa.hkbu.edu.hk/sfaApplication/ (UAT) - RITM0078284			
Website URL :	https://sfa.hkbu.edu.hk/sfaApplication/ (Production) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user (UAT-user) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=operator (UAT-operator) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=admin (UAT-admin) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=endorser (UAT-endorser) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=approver (UAT-approver) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=advisor (UAT-advisor)		
Assessment Date:	7 & 8 June 2021 – 1st Scan		
Overall Result / Risk Level:	FAIL / High Risk		
Action Required:	Remediation and Re-scan		
Scan Report (Encl.):	2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=admin.pdf		
Summary of Result:			
Severity	**Risk #**	**Description**	**Remediation / Follow Up Action**
High (4)	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities(2)	**Remediation is required** as recommended in the report.
	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities(2)	

Vulnerability Assessment for sfa.hkbu.edu.hk/sfaApplication/ (UAT) - RITM0078284			
Website URL :	https://sfa.hkbu.edu.hk/sfaApplication/ (Production) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user (UAT-user) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=operator (UAT-operator) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=admin (UAT-admin) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=endorser (UAT-endorser) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=approver (UAT-approver) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=advisor (UAT-advisor)		
Assessment Date:	7 & 8 June 2021 – 1st Scan		
Overall Result / Risk Level:	FAIL / High Risk		
Action Required:	Remediation and Re-scan		
Scan Report (Encl.):	2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=endorser.pdf		
Summary of Result:			
Severity	**Risk #**	**Description**	**Remediation / Follow Up Action**
High (4)	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities(2)	**Remediation is required** as recommended in the report.
	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities(2)	

Vulnerability Assessment for sfa.hkbu.edu.hk/sfaApplication/ (UAT) - RITM0078284	
Website URL :	https://sfa.hkbu.edu.hk/sfaApplication/ (Production) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user (UAT-user) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=operator (UAT-operator) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=admin (UAT-admin) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=endorser (UAT-endorser) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=approver (UAT-approver) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=advisor (UAT-advisor)
Assessment Date:	7 & 8 June 2021 – 1st Scan
Overall Result / Risk Level:	FAIL / High Risk

Action Required:	Remediation and Re-scan		
Scan Report (Encl.):	2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=approver.pdf		
Summary of Result:			
Severity	**Risk #**	**Description**	**Remediation / Follow Up Action**
High (4)	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities(2)	**Remediation is required** as recommended in the report.
	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities(2)	

Vulnerability Assessment for sfa.hkbu.edu.hk/sfaApplication/ (UAT) - RITM0078284			
Website URL :	https://sfa.hkbu.edu.hk/sfaApplication/ (Production) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user (UAT-user) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=operator (UAT-operator) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=admin (UAT-admin) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=endorser (UAT-endorser) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=approver (UAT-approver) https://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=advisor (UAT-advisor)		
Assessment Date:	7 & 8 June 2021 – 1st Scan		
Overall Result / Risk Level:	FAIL / High Risk		
Action Required:	Remediation and Re-scan		
Scan Report (Encl.):	2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=advisor.pdf		
Summary of Result:			
Severity	**Risk #**	**Description**	**Remediation / Follow Up Action**
High (4)	150013	Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities(2)	**Remediation is required** as recommended in the report.
	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities(2)	

Best Regards,

Steven Y. C. CHAN

Information Security Manager,

BSc (Hons), MSc., CIFI, CISSP, CEH
Information Security Unit, Infrastructure Section

Office of Information Technology
Hong Kong Baptist University

T 3411 5364 | E sycchan@hkbu.edu.hk | W ito.hkbu.edu.hk

==========

From: Calvin S. LAW <calvinlaw@hkbu.edu.hk>
Sent: Monday, June 7, 2021 10:24 AM
To: ITO Online Service <hkbu@service-now.com>
Cc: Steven Y C CHAN <sycchan@hkbu.edu.hk>; ITO Service Call Centre <hotline@hkbu.edu.hk>
Subject: Re: ITO - Your Service Request RITM0078284 - comments added

Dear Steven,

Login Details:

UAT -user

UAT -operator

UAT -admin

UAT -endorser

UAT-Approver

UAT-Advisor

The Security Risk Assessment can be started

Best Regards,

Calvin Law

Assistant IT Officer | SFA| SA

Hong Kong Baptist University

香港浸會大學 HONG KONG BAPTIST UNIVERSITY

On Mon, 7 Jun 2021 at 10:23, ITO Online Service <hkbu@service-now.com> wrote:

Office of Information Technology 資訊科技處

Hotline: 3411 7899
Fax: 3411 7888
Email: hotline@hkbu.edu.hk
Hours: 08:30-18:00 (M-F), 08:30-12:30 (Sat)

HKBU | ITO | ITSM Portal

Your Service Request #RITM0078284 - comments added

Summary

Service Request: #RITM0078284
Description: [IT090] Website Vulnerability Assessment / Scan Request Form
Requester: LAW Calvin S.

Contact Person: LAW Calvin S.
Handled by: CHAN Steven Y C

Created Time: 2021-06-05 07:21:15
Last Updated Time: 2021-06-07 10:22:21

Comments:

2021-06-07 10:22:21 - LAW Calvin S. Additional Information / Requirement

reply from: calvinlaw@hkbu.edu.hk

Dear Steven,

Login Information
UAT -user
<http://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user>UAT
-operator
<http://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=operator>UAT
-endorser
<http://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=endorser>
UAT-Approver
<http://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=approver>
UAT-Advisor
<http://uat-sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=advisor>

Best Regards,

Calvin Law

Assistant IT Officer | SFA <https://sa.hkbu.edu.hk/sfa>| SA
<https://sa.hkbu.edu.hk/>

Hong Kong Baptist University

<http://www.hkbu.edu.hk>

On Mon, 7 Jun 2021 at 10:17, ITO Online Service <hkbu@service-now.com>
wrote:

> Hotline: 3411 7899
> Fax: 3411 7888
> Email: hotline@hkbu.edu.hk
> Hours: 08:30-18:00 (M-F), 08:30-12:30 (Sat)
> HKBU <http://www.hkbu.edu.hk/eng/main/index.jsp>| ITO
> <http://ito.hkbu.edu.hk/>| ITSM Portal <https://hkbu.service-now.com/>
> Your Service Request #RITM0078284 has been put on hold.
> The status of your service request raised through the "[IT090] Website
> Vulnerability Assessment / Scan Request Form " has been changed to indicate
> that completion of service is now pending the occurrence of certain
> event(s). You can track the status of the ticket at RITM0078284
> <https://hkbu.service-now.com/nav_to.do?uri=sc_req_item.do%3Fsys_id=184d922ddba074503ce7ee4dd396196f%26sysparm_stack=sc_req_item_list.do%3Fsysparm_query=active=true>
> .
> *Summary*
> ---
> *Service Request:* #RITM0078284
> *Description:* [IT090] Website Vulnerability Assessment / Scan Request
> Form
> *Requester:* LAW Calvin S.
> *Contact Person:* LAW Calvin S.
> *Handled by:* CHAN Steven Y C
> *Created Time:* 2021-06-05 07:21:16
> *On-hold Reason:* 2021-06-07 10:16:55 - CHAN Steven Y C (Additional
> Information / Requirement) The request has been put on hold due to the UAT
> website [], as well as relevant UAT accounts are not ready. Informed the
> user to prepare them for v-scan.
> ---
> Should you have any inquiry, simply reply to this email or call us at 3411
> 7899.
> Regards
> Service Call Centre
>
> Ref:MSG0420868

--

that may be incurred or caused to
any party as a result of the use of such
information.

2021-06-07 10:16:55 - CHAN Steven Y C Additional Information / Requirement

The request has been put on hold due to the UAT website [], as well as relevant UAT accounts are not ready. Informed the user to prepare them for v-scan.

2021-06-05 07:36:44 - LAW Calvin S. Additional Information / Requirement

reply from: calvinlaw@hkbu.edu.hk

For your better understanding of the system
i have attached the user requirements, a simplified Flow Chart

Best Regards,

Calvin Law

Assistant IT Officer | SFA <https://sa.hkbu.edu.hk/sfa>| SA
<https://sa.hkbu.edu.hk/>

Hong Kong Baptist University

<http://www.hkbu.edu.hk>

On Sat, 5 Jun 2021 at 07:30, ITO Online Service <hkbu@service-now.com>
wrote:

> Hotline: 3411 7899
> Fax: 3411 7888
> Email: hotline@hkbu.edu.hk
> Hours: 08:30-18:00 (M-F), 08:30-12:30 (Sat)
> HKBU <http://www.hkbu.edu.hk/eng/main/index.jsp>| ITO
> <http://ito.hkbu.edu.hk/>| ITSM Portal <https://hkbu.service-now.com/>
> Your Service Request #RITM0078284
> <https://hkbu.service-now.com/nav_to.do?uri=sc_req_item.do%3Fsys_id=184d922ddba074503ce7ee4dd396196f%26sysparm_stack=sc_req_item_list.do%3Fsysparm_query=active=true>
> - comments added
> *Summary*
> ---
> *Service Request:* #RITM0078284
> *Description:* [IT090] Website Vulnerability Assessment / Scan Request
> Form
> *Requester:* LAW Calvin S.
> *Contact Person:* LAW Calvin S.
> *Handled by:* CHAN Steven Y C
> *Created Time:* 2021-06-05 07:21:15
> *Last Updated Time:* 2021-06-05 07:29:25
> ---
> ---
> *Comments:*
> ---
> *2021-06-05 07:29:24 - LAW Calvin S.* Additional Information / Requirement
> reply from: calvinlaw@hkbu.edu.hk
> There is no username password.
> All Authentication is using SSOId Login.
> I have the following Links for LOGIN with different roles
> prod-user <https://sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user
> >
> prod-user(30)
> <https://sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=user2>
> prod-Advisor
> <https://sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=advisor>
> prod-Approver
> <https://sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=approver>
> prod-admin
> <https://sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=admin>
> prod-operator
> <https://sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=operator>
> prod-endorser
> <https://sfa.hkbu.edu.hk/sfaApplication/auth/?op=login&demo=endorser>

> Please call me for any enquiries
> please do not delete any records
> please note system still in development, i want to launch system before 27
> my last DUTY DATE 30 JUN
> i want to scan the system, and know the estimated time required for
> scanning so that I have more time to make modifications
>
> Best Regards,
>
> Calvin Law
>
> Assistant IT Officer | SFA <https://sa.hkbu.edu.hk/sfa>| SA
> <https://sa.hkbu.edu.hk/>
> Hong Kong Baptist University
> <http://www.hkbu.edu.hk>
>
> On Sat, 5 Jun 2021 at 07:21, ITO Online Service <hkbu@service-now.com>
> wrote:
> > Hotline: 3411 7899
> > Fax: 3411 7888
> > Email: hotline@hkbu.edu.hk
> > Hours: 08:30-18:00 (M-F), 08:30-12:30 (Sat)
> > HKBU <http://www.hkbu.edu.hk/eng/main/index.jsp>| ITO
> > <http://ito.hkbu.edu.hk/>| ITSM Portal <https://hkbu.service-now.com/>
> > Please Provide Testing Account for Vulnerability Scan - Request
> > RITM0078284.
> > Testing Account for your website "https://sfa.hkbu.edu.hk/sfaApplication
> "
> > is required for the website vulnerability scan. Please submit your
> testing
> > account and password using this LINK
> > <https://infosec.hkbu.edu.hk/security_check/vScanSuppInfo/RITM0078284>.
> > At the same time, you can track the status of your ticket at RITM0078284
> > <
> https://hkbu.service-now.com/nav_to.do?uri=sc_req_item.do%3Fsys_id=184d922ddba074503ce7ee4dd396196f%26sysparm_stack=sc_req_item_list.do%3Fsysparm_query=active=true
> > .
> > *Summary*
> >
> ---
> > *Service Request:* #RITM0078284
> > *Description:* [IT090] Website Vulnerability Assessment / Scan Request
> > Form
> > *Requester:* LAW Calvin S.
> >
> > *Contact Person:* LAW Calvin S.
> > *Handled by:* CHAN Steven Y C
> > *Created Time:* 2021-06-05 07:21:16
> >
> >
> ---
> >
> >
> >
> > Should you have any inquiry, simply reply to this email or call us at
> 3411
> > 7899.
> >
> > Regards
> > Service Call Centre
> >
> >
> >
> >
> >
> >
> >

> >
> >
> > Ref:MSG0420666
> >
>
> --
> Disclaimer
>
> This
> message (including any attachments) may contain
> confidential
> information intended for a specific individual and/or
> purpose. If you
> are not the intended recipient, please delete this message
> and notify
> the sender and the University immediately. Any disclosure,
> copying, or
> distribution of this message, or the taking of any action
> based on it,
> is prohibited as it may be unlawful.
>
> In
> addition, the
> University specifically denies any responsibility for the
> accuracy or
> quality of information obtained through University E-mail
> Facilities. Any
> views and opinions expressed in the email(s) are those
> of the author(s),
> and do not necessarily represent the views and
> opinions of the University.
> The University accepts no liability
> whatsoever for any losses or damages
> that may be incurred or caused to
> any party as a result of the use of such
> information.
>
> ----------
>
>
> Should you have any inquiry, simply reply to this email or call us at 3411
> 7899.
>
> Regards
> Service Call Centre
>
> Copyright 2021. Hong Kong Baptist University. All rights reserved.
>
>
>
>
>
> Ref:MSG0420667
>

--
Disclaimer

This
message (including any attachments) may contain
confidential
information intended for a specific individual and/or
purpose. If you
are not the intended recipient, please delete this message
and notify
the sender and the University immediately. Any disclosure,
copying, or
distribution of this message, or the taking of any action
based on it,
is prohibited as it may be unlawful.

In
addition, the
University specifically denies any responsibility for the
accuracy or
quality of information obtained through University E-mail
Facilities. Any
views and opinions expressed in the email(s) are those
of the author(s),
and do not necessarily represent the views and
opinions of the University.
The University accepts no liability
whatsoever for any losses or damages
that may be incurred or caused to
any party as a result of the use of such
information.

Should you have any inquiry, simply reply to this email or call us at 3411 7899.

Regards
Service Call Centre

Ref:MSG0420875

6 attachments

2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=advisor.pdf
111K

2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=approver.pdf
110K

2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=endorser.pdf
110K

2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=admin.pdf
111K

2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=operator.pdf
111K

2021-06-07_uat-sfa.hkbu.edu.hk_sfaApplicationauthop_login&demo=user.pdf
101K