

Exploiting ServiceNow@Tufts:

**how thousands of current and past
student, staff, and faculty data was
left unsecured**

by: yoji watanabe



**What are we
talking
about?**

ServiceNow®

- Cloud computing company
- Services Tufts

TechConnect

- Tufts' implementation of the ServiceNow system
- Allows users to open "incidents" to be reviewed by the Technology staff
- Each Tufts affiliate has a user profile with name, UTLN, email address, physical address, and phone number
- Example: Forms from the Research Cluster access page and special software requests are handled by TechConnect
- First vulnerabilities found on March 15, 2018

What Happened?

>491,458

instances of user info was exposed

>26,820 users

had their information exposed

Yeah, but
you couldn't
do much,
right?

Incidents | 1

Trunk : My Workspace : Home


https://tufts.service-now.com/nav_to.do?uri=%2Fincident_list.do

Tufts TechConnect

Yoji H. Watanabe (ywatan01)

Filter navigator

Incidents Go to Number Search

	Number	Affected Client	State	Short description	Opened
<input type="checkbox"/>	INC0615677	[REDACTED]	Active	Computer in 2nd Floor Dispensary	03-16-2018 14:27:32
<input type="checkbox"/>	INC0615678	(noreply@turnitin.com)	Closed	Reminder: Turnitin Scheduled Maintenance on March 17, 2018	03-16-2018 14:31:33
<input type="checkbox"/>	INC0615679	[REDACTED]	New	Karen and her team's admin access	03-16-2018 14:30:27
<input type="checkbox"/>	INC0615680	[REDACTED]	Active	CSSC exam support Monday 3/19/18	03-16-2018 14:32:45
<input type="checkbox"/>	INC0615681	[REDACTED]	New	Printer support	03-16-2018 14:03:04
<input type="checkbox"/>	INC0615682	[REDACTED]	Active	Computer login access problem with ASBIOWOOD5990	03-16-2018 14:35:39
<input type="checkbox"/>	INC0615683	[REDACTED]	Active	RE: Is Elisabeth Soong all set up?	03-16-2018 14:37:34
<input type="checkbox"/>	INC0615684	[REDACTED]	Active	More jacks at 200 Boston	03-16-2018 14:37:35
<input type="checkbox"/>	INC0615685	[REDACTED]	New	New axiUm User	03-16-2018 14:41:05
<input type="checkbox"/>	INC0615686	[REDACTED]	Active	calendar access	03-16-2018 14:43:36
<input type="checkbox"/>	INC0615687	[REDACTED]	Resolved	cant log into advance	03-16-2018 14:30:23
<input type="checkbox"/>	INC0615688	[REDACTED]	Resolved	New axiUm User	03-16-2018 14:43:02
<input type="checkbox"/>	INC0615689	[REDACTED]	New	fw rule	03-16-2018 14:50:07
<input type="checkbox"/>	INC0615690	 Deborah [REDACTED]	Active	Duo mobile	03-16-2018 14:44:09
<input type="checkbox"/>	INC0615691	[REDACTED]	Resolved	INC0614206 MAPSYR00231 needs Matlab installed	03-16-2018 14:55:44
<input type="checkbox"/>	INC0615692	[REDACTED]	New	RE: Is Elisabeth Soong all set up?	03-16-2018 14:56:07
<input type="checkbox"/>	INC0615693	[REDACTED]	Resolved	INC0614206 MAPSYR00232 needs Matlab installed	03-16-2018 14:56:12

Actions on selected rows...

49143 to 491456 of 491458

Retrieving the list of incidents

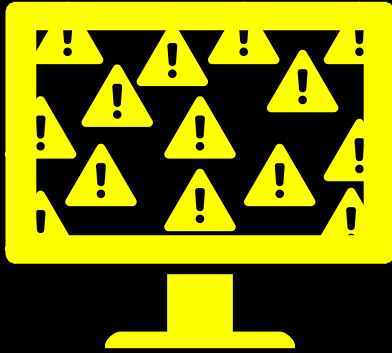
Source code of "my open items" tab

```
<table id="task_table" class="data_list_table list_table table table-hover list_header_search_disabled" glide_list_has_hierarchy="false" total_rows="1"
glide_list_edit_ref_qual_tag="" glide_list_has_actions="true" list_name="task" parsed_choice_query "<?xml version="1.0" encoding="UTF-8"?><xml table="incident">...e"
newquery="false" operator="=" or="false" value=""/></xml>" data-list_id="task" glide_list_has_header="true" can_hide_nav="false" glide_list_can_delete="false"
glide_list_edit_id="task" glide_list_edit_type="disabled" query="active=true^opened_by=javascript:gs.getUserID()^ORref_incide...^stateNOT IN3,4,7,6^numberNOT
LTKETASK^numberNOT LTKECALL^EQ" filter_enabled="true" glide_list_omit_links="false" sort="task number" glide_list_edit_insert_row="false"
glide_list_query="active=true^opened_by=javascript%3Ags.getUserID()^ORref_inci_DES NOT CONTAINTASK^numberDOES NOT CONTAINCALL^ORDERBYnumber"
glide_list_can_create="true" rows_per_page="20" grand_total_rows="1" maintain_order="false" parsed_query="<?xml version="1.0" encoding="UTF-8"?><xml table="incident">...
e" newquery="false" operator="=" or="false" value=""/></xml>" first_row="1" last_row="1" style="width: 100%; margin-bottom: 0px; outline: medium none currentcolor;"
glide_table="task" sort_dir="ASC" tabindex="0">
```

1. Incidents are represented in a XML table
2. There are searchable tags associated with incidents
3. My Open Items is made by making a query to an incident database for incidents opened by the current user

Exploit overview

- Use information disclosed to figure out how to make database queries
- Use code injection techniques to make queries to database
- Make use of lack of access controls to access all entries



NOW WHAT?

Surely, bringing these things to Tufts' attention
would get them fixed

When ServiceNow® 'fixed' the issues

- No more SQLi
 - No access to user list
 - No access to incident list
- Still open to XPath Injection
- Still has access control vulnerabilities
- What kind of data do we still have access to?

- How can I get people's information in order to find their profile page?



**ServiceNow®
isn't safe:
Round 2**

Filter navigator

Self-Service

Homepage

Dashboards

My Open Items

My Previous Items

My Tagged Documents

Incident - INC0616487

Number

INC0616487

Type

Request

Affected Client

Yoji H. Watanabe (ywatano01)

Opened

03-20-2018 14:51:18

Building/Location

Yoji H. Watanabe (ywatano01)

Resolved

03-21-2018 09:20:43

Room

Resolved by

Delilah Maloney (ymalono01)

Contact Person

Yoji H. Watanabe (ywatano01)

State

Closed

Preferred Phone Number

Assignment group

TTS Research Technology

Watch list

Shawn Doughty (sdough01)

Assigned to

Delilah Maloney (ymalono01)

Short description

Cluster Software Request

Description

Hi there,

I was hoping to get the John the Ripper software installed in my cluster account.

I need to use it for my current work in my cyber security course, so the sooner it is available the better!

More information about the software can be found here: <http://www.openwall.com>

Incident - INC0616487

Number

INC0616487

Type

Request

Affected Client

Yoji H. Watanabe (ywatano01)

Opened

03-20-2018 14:51:18

Building/Location

Yoji H. Watanabe (ywatano01)

Resolved

03-21-2018 09:20:43

Room

Resolved by

Delilah Maloney (ymalono01)

Contact Person

Yoji H. Watanabe (ywatano01)

State

Closed

Preferred Phone Number

Assignment group

TTS Research Technology

Watch list

Shawn Doughty (sdough01)

Assigned to

Delilah Maloney (ymalono01)

Short description

Cluster Software Request

Description

Hi there,

I was hoping to get the John the Ripper software installed in my cluster account.

I need to use it for my current work in my cyber security course, so the sooner it is available the better!

More information about the software can be found here: <http://www.openwall.com>

Incident - INC0616487

Number

INC0616487

Type

Request

Affected Client

Yoji H. Watanabe (ywatano01)

Opened

03-20-2018 14:51:18

Building/Location

Yoji H. Watanabe (ywatano01)

Resolved

03-21-2018 09:20:43

Room

Resolved by

Delilah Maloney (ymalono01)

Contact Person

Yoji H. Watanabe (ywatano01)

State

Closed

Preferred Phone Number

Assignment group

TTS Research Technology

Watch list

Shawn Doughty (sdough01)

Assigned to

Delilah Maloney (ymalono01)

Short description

Cluster Software Request

Description

Hi there,

I was hoping to get the John the Ripper software installed in my cluster account.

I need to use it for my current work in my cyber security course, so the sooner it is available the better!

More information about the software can be found here: <http://www.openwall.com>

Reconstructing Profile URLs

Profile URL:

https://tufts.service-now.com/nav_to.do?uri=%2Fsys_user.do%3Fsys_id%3D8eabe69c35c958003108e27baf1c144d%26sysparm_view%3Dess

Deconstructing URL						
USER	nav_to.do?	uri=%2Fsys_user.do	%3Fsys_id	%3D8eabe69c35c958003108e27baf1c144d	%26sysparm_view	%3Dess
URL decoded	nav_to.do?	uri=/sys_user.do	?sys_id	=8eabe69c35c958003108e27baf1c144d	&sysparm_view	=ess
Notes				[USER ID] !!!! Very important		

Can we then reconstruct a URL to gain access to a profile?

Tufts

TechConnect

All applications

Search

Self-Service

Homepage

Dashboards

My Open Items

My Previous Items

My Tagged Documents

https://tufts.service-now.com/nav_to.do?uri=%2Fsys_user.do%3Fsys_id%3D8eabe69c35c958003108e27baf1c144d%26sysparm_view%3Dess

YW Yoji H. Watanabe (ywatan01)

?

User -

First name

L

Last name

Business phone

Mobile phone

Title

Dir

Email

Notification

Email

Date format

Time zone

Delegates

Service Groups

Delegates

New

Go to

Starts

Search

User =

Starts

Ends

Delegate

Approvals

Assignments

CC notifications

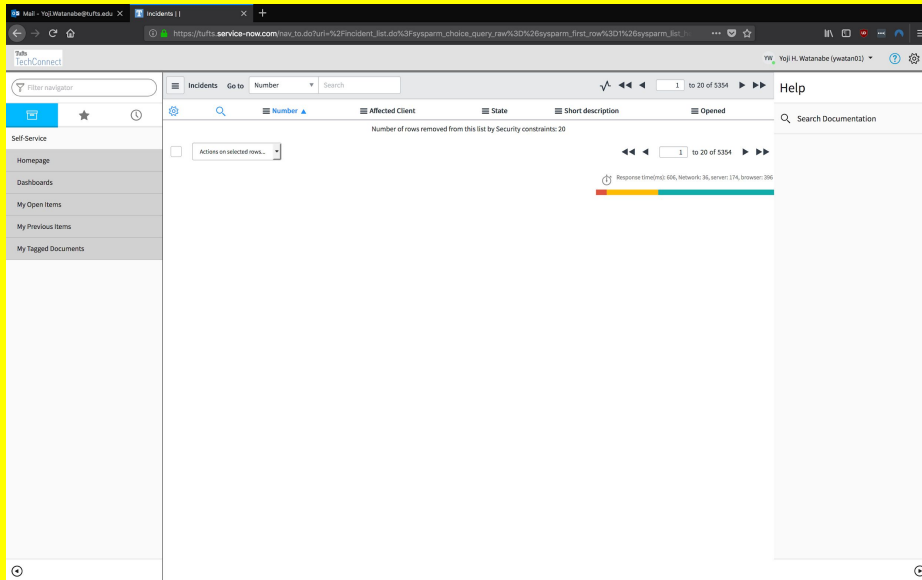
Meeting invitations

No records to display

Response time(ms): 922, Network: 12, server: 322, browser: 588

Where are they now?

- Updated access control
 - No longer able to make unverified queries to incident or user database
 - No disclosure of critical information
- Sanitized user input
 - No longer able to perform code injection attacks



"Number of rows removed by this list by Security constraints: 20"



Reviewing vulnerabilities

SQLi

(CWE-89: Improper Neutralization of Special Elements used in an SQL Command)

- Access to incident list

XML Injection

(CWE-91: XML Injection)

- Access to incident and user list
- Search through user and incident list
- Direct to user profiles

Information Disclosure

(CWE-200: Information Exposure)

- Disclosed information to reconstruct profile URLs
- Disclosed information to access incident list
- Disclosed information about database

Access Control

(CWE-284: Improper Access Control)

- Access to user information
- Access to other incidents

Lessons learned

- 70% of the process was communicating
- It is shocking how vulnerable enterprise software can be, how inefficient they can be at fixing it
 - Initial report outlined four vulnerabilities
 - One was fixed
 - Over thirty days to fix all vulnerabilities
- It's scary

A large, bright yellow circle is positioned on the left side of a solid black background. The circle is partially cut off by the left edge of the frame. Centered within the yellow circle is the word "Questions?" in a bold, black, sans-serif font.

Questions?