



**Business Logic
Write-ups
01**



Exploiting Max. Character Limitation

Sunil Yedla به عنوان یک تست نفوذگر و شکارچی باگ، علاقه زیادی به شکستن عملکردها (Functionality) و پیدا کردن برخی باگ‌های جالب دارد. وی تاکید زیادی بر اهمیت درک عملکردها دارد و اشاره می‌کند که باید هر روش ممکن را برای شکستن عملکردها در جهت پیدا کردن راه‌های فرار از ویژگی‌های امنیتی معتبر جستجو کنیم.

تست نفوذگر ۶ ماه پیش، یک دعوتنامه خصوصی از سایت هکروان دریافت می‌کند، وی به سرعت دعوت را باز نموده و مشاهده می‌کند که دعوت نامه مربوط به یک برنامه رمزنگاری می‌باشد. از آنجا که تست نفوذگر طرفدار پروپا قرص جمع آوری اطلاعات یا همان Recon نمی‌باشد، شروع به تست همه عملکردهای برنامه به صورت یک به یک می‌نماید.

وی در فرآیند تست مشاهده می‌کند که هیچ محدودیت کاراکتری، برای فیلد نام وجود ندارد. در این حالت وی دو گزینه را پیش رو دارد:

می‌تواند این موضوع را نادیده بگیرد زیرا به هر حال در صورت گزارش این موضوع، گزارش وی به عنوان اطلاع‌رسانی (Informative) و یا گاهی اوقات Not Applicable در نظر گرفته خواهد شد.

همچنین می‌تواند بررسی بیشتری انجام دهد و ببیند که این نام طولانی کجا می‌تواند به یک تهدید بالقوه برای یک شرکت یا کاربران یا عملکرد تبدیل شود.

تست نفوذگر روش دوم را انتخاب می‌کند و به کار خود ادامه می‌دهد.

بنابراین شروع به بررسی تمام ویژگی‌ها نموده و در ابتدا متوجه می‌شود که این کار باعث حمله DoS می‌گردد. اما از آنجا که این امر تنها در مرورگر کروم اتفاق می‌افتد، تیم Triage سایت هکروان، این موضوع را قبول نکرده و گزارش تست نفوذگر را به عنوان Informative می‌بندد.



closed the report and changed the status to **Informative**.

Jul 23rd (6 months ago)

As this is directly related to client's browser performance and is not a vulnerability, we shall close this report as "Informative"





تست نفوذگر به کاوش ادامه می‌دهد و متوجه می‌شود که کاربران مدیر می‌توانند کاربران دیگر را دعوت کنند و تنها کاربر مدیر می‌تواند کاربر دعوت‌شده را در هر زمانی که بخواهد حذف نماید. امکان حذف کاربران دعوت‌شده تنها در یک صفحه وجود دارد که در آن لیست تمام جزئیات کاربران مانند: نام، نام خانوادگی، ایمیل و نقش کاربران در آن نمایش داده می‌شود. اما زمانی که فرد دعوت‌شده نام خود را به نامی طولانی با کاراکترهای زیاد تغییر می‌دهد، آنگاه کاربر ادمین قادر به مشاهده گزینه حذف نخواهد بود.

FIRST NAME	LAST NAME	EMAIL	ROLE
sunny	okok	[REDACTED]@wearehackerone.com	Administrator


```

new012345678910111
213141516171819202
122232425262728293
031323334353637383
940414243444546474
849505152535455565
758596061626364656
667686970717273747
57677879808182838
485868788899091929
394959697989910010
110210310410510610
710810911011111211
311411511611711811
912012112212312412
512612712812913013
113213313413513613
713813914014114214
314414514614714814
015015115215315415
    
```

تأثیر این موضوع در اینجاست که کاربران دعوت‌شده می‌توانند برای همیشه در تیم باقی بمانند.

تیم Triage پس از بررسی این گزارش، آن را با شدت ۵ پذیرفته و مبلغ ۴۰۰ دلار جایزه برای آن در نظر می‌گیرد.

#931413 Invited users can block administrators to remove them

State ● Resolved (Closed) Severity Medium (5.0)

Reported To [REDACTED] Participants 1

Reported at July 22, 2020 7:00pm +0530 Visibility Private

Asset [REDACTED]
(Domain)

CVE ID

Weakness Business Logic Errors

Bounty \$400

[Collapse](#)

منبع:

<https://sunilyedla.medium.com/exploiting-max-character-limitation-cde982545019>

