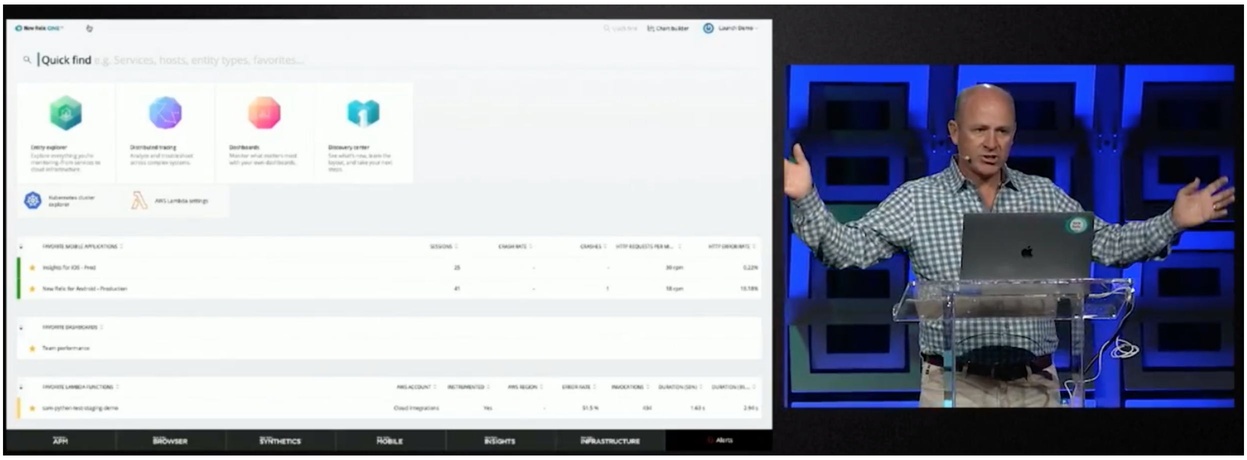
www.jonbottarini.com /2019/06/17/using-burp-suite-match-and-replace-settings-to-escalate-your-user-privileges-and-find…

Using Burp Suite match and replace settings to escalate your user privileges and find hidden features

Jon Bottarini ⁝⁝ 18/06/2019

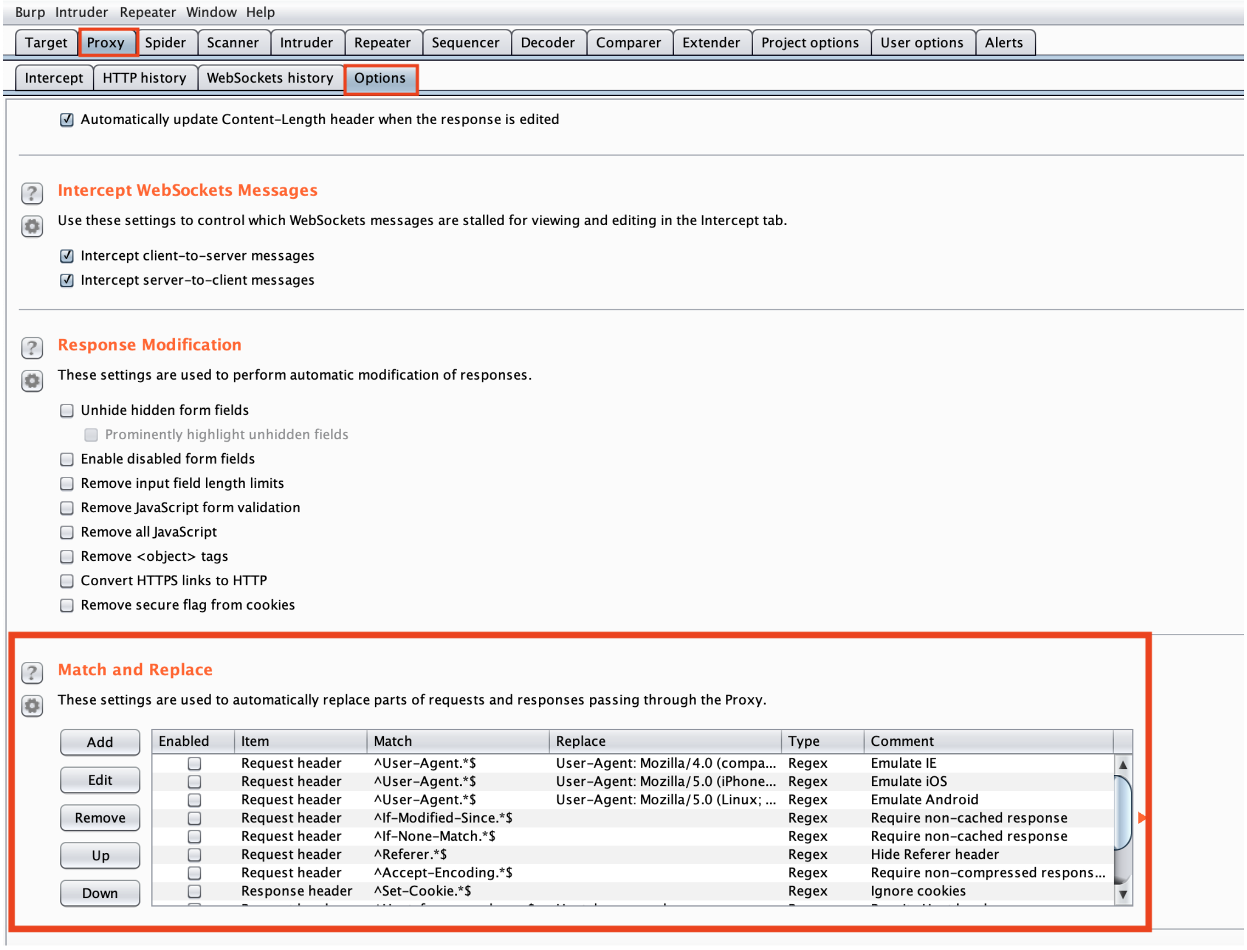
On May 14th, Lew Cirne, the CEO of New Relic, announced a new platform called New Relic One. The platform, featuring a fresh new design and better data visualizations, came as a surprise to investors and New Relic users alike.



But it did not come as a surprise to me, for I had found out about it months prior, using a common trick that I've used multiple times in other bug bounty programs to access unreleased beta and admin features; the Burp Suite match and replace rule.

The concept is simple: By changing the server response body from "false" to "true" (I cheekily refer to this as the FALSE2TRUE trick, because everything has to have a catchy name nowadays 😏) – you open up much more on the client side that might previously be hidden or unaccessible, and that's exactly what happened when I found out about New Relic One. This is not a secret, and has been a method for a long time.

For those of you new to using the Burp Suite match and replace rule, this article goes deeper into where to find it in Burp and how to use it – but it lives under the Proxy settings in Options:



☑ Automatically update Content-Length header when the response is edited

Intercept WebSockets Messages

Use these settings to control which WebSockets messages are stalled for viewing and editing in the Intercept tab.

☑ Intercept client-to-server messages
☑ Intercept server-to-client messages

Response Modification

These settings are used to perform automatic modification of responses.

□ Unhide hidden form fields
□ Prominently highlight unhidden fields
□ Enable disabled form fields
□ Remove input field length limits
□ Remove JavaScript form validation
□ Remove all JavaScript
□ Remove <object> tags
□ Convert HTTPS links to HTTP
□ Remove secure flag from cookies

Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Enabled	Item	Match	Replace	Type	Comment
□	Request header	^User-Agent.*$	User-Agent: Mozilla/4.0 (compa...	Regex	Emulate IE
□	Request header	^User-Agent.*$	User-Agent: Mozilla/5.0 (iPhone...	Regex	Emulate iOS
□	Request header	^User-Agent.*$	User-Agent: Mozilla/5.0 (Linux; ...	Regex	Emulate Android
□	Request header	^If-Modified-Since.*$		Regex	Require non-cached response
□	Request header	^If-None-Match.*$		Regex	Require non-cached response
□	Request header	^Referer.*$		Regex	Hide Referer header
□	Request header	^Accept-Encoding.*$		Regex	Require non-compressed respons...
□	Response header	^Set-Cookie.*$		Regex	Ignore cookies

The match and replace rule goes well beyond just changing false responses to true – it can also be used for privilege escalation to change your user permissions from “User” to “Admin”. Let’s use the following example:

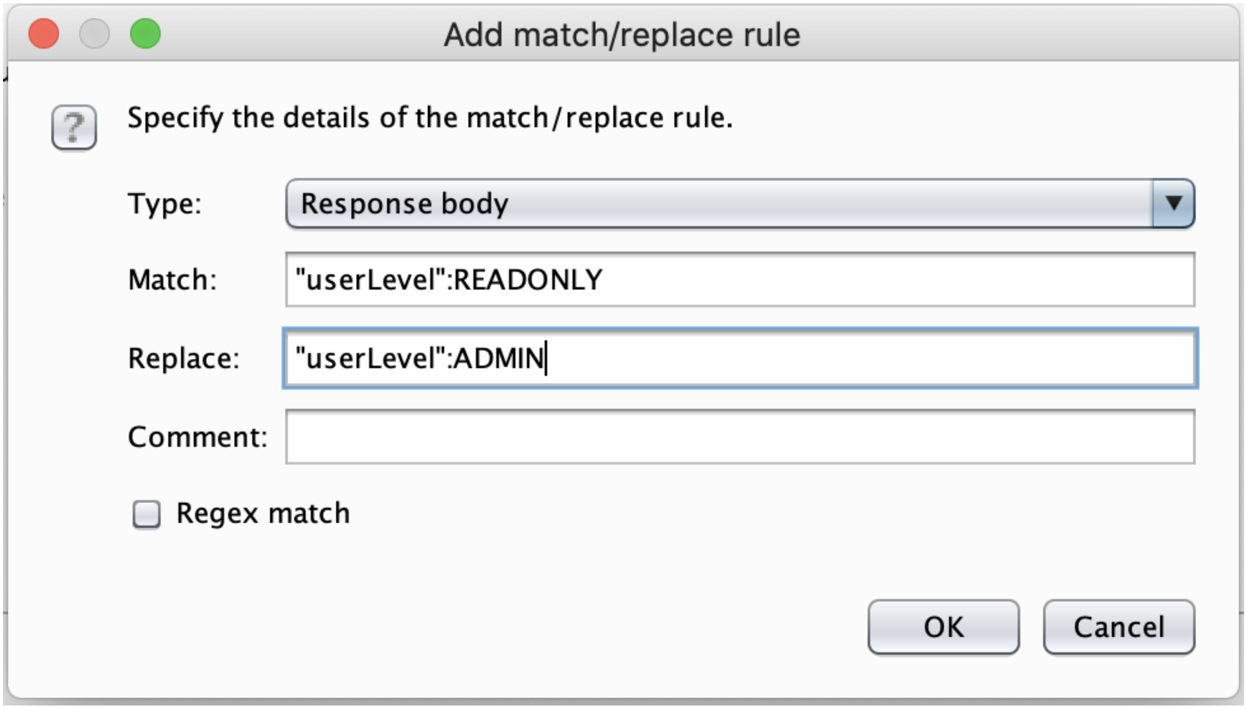
Imagine the server performs a check of the permissions of the user with the current session. The request to the server might look something like this:

```
POST /api/getUserDetails HTTP/1.1
Host: myserver.jonbottarini.com
Cookie: mycookies

{"user":"123"}
```

And the response might look like this:

```
HTTP/1.1 200 OK

{"data":{"currentUser":{"userData":[
{"userLevel":READONLY,"subscriptionLevel":"BASIC"}
]}}}
```

In the response, the client operates under the assumption that the user is in “READONLY” mode, and has a “BASIC” subscription. If we add a match and replace rule to change the “userLevel”:READONLY response to “userLevel”:ADMIN, we can trick the client to display UI elements that are meant only for Administrators:



Specify the details of the match/replace rule.

Type: Response body

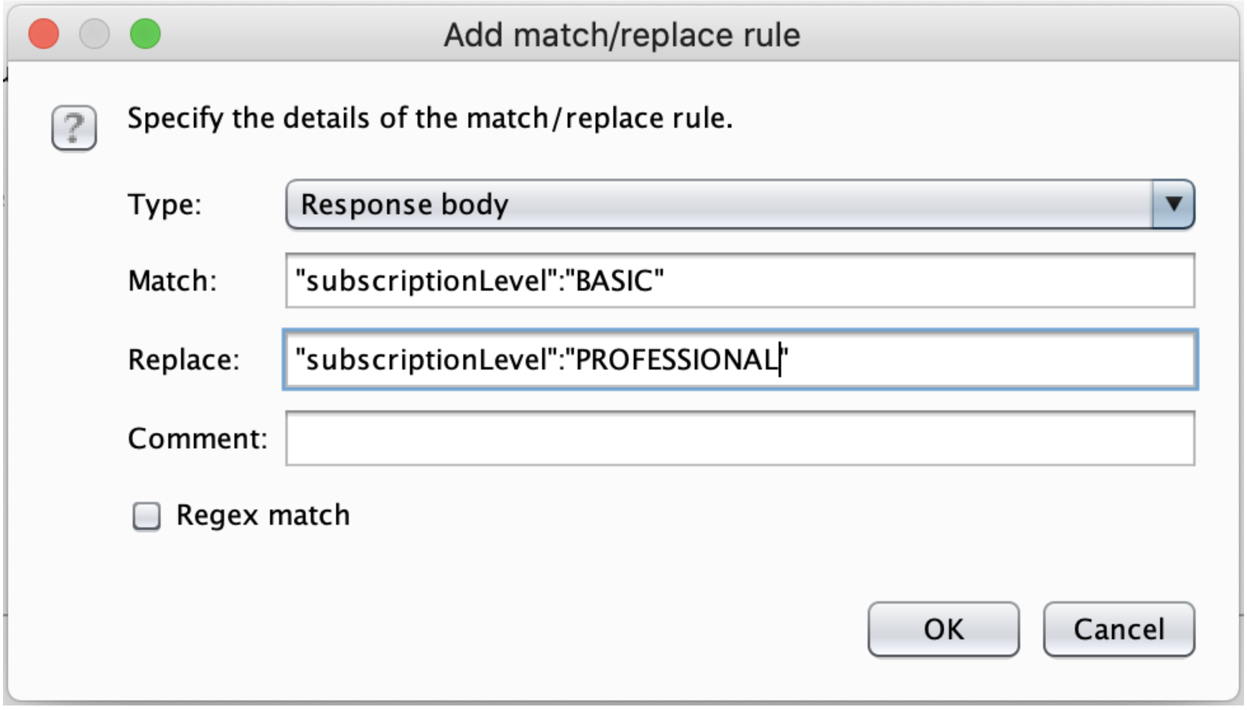
Match: "userLevel":READONLY

Replace: "userLevel":ADMIN

Comment:

□ Regex match

We can go one step further and display UI elements that are meant only for a “Professional” level subscription as well:



Add match/replace rule

Specify the details of the match/replace rule.

Type: Response body

Match: "subscriptionLevel":"BASIC"

Replace: "subscriptionLevel":"PROFESSIONAL"

Comment:

□ Regex match

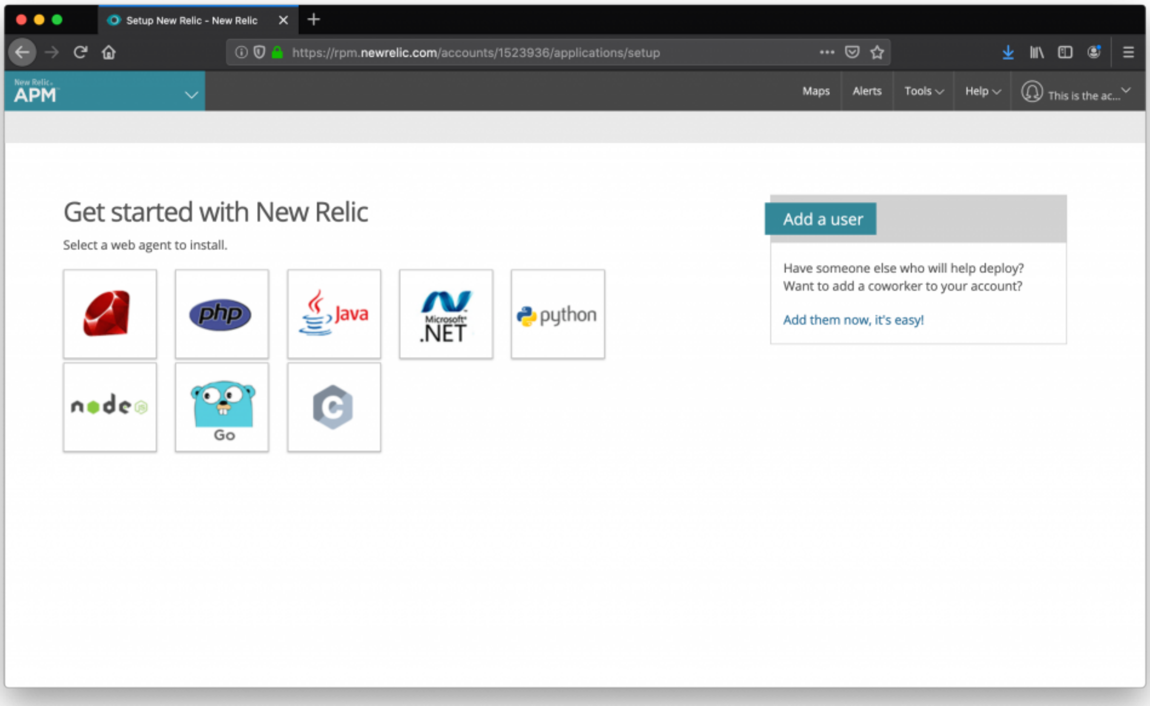
If we were to add the match/replace rules above, the response to the client will now look like this:

```
HTTP/1.1 200 OK

{"data":{"currentUser":{"userData":
[{"userLevel":ADMIN,"subscriptionLevel":"PROFESSIONAL"}]}}}
```

@daeken has another nifty trick with the Burp match/replace rule: injecting payloads into forms instead of typing out the entire payload:

Back to New Relic. I was using the *FALSE2TRUE* trick when I realized that there was a feature flag on my account which was always returning **false**. By simply changing this response to **true** using Burp match/replace rule, I noticed that there was additional UI elements that appeared on the page.

This is the New Relic landing page when logging in without FALSE2TRUE:



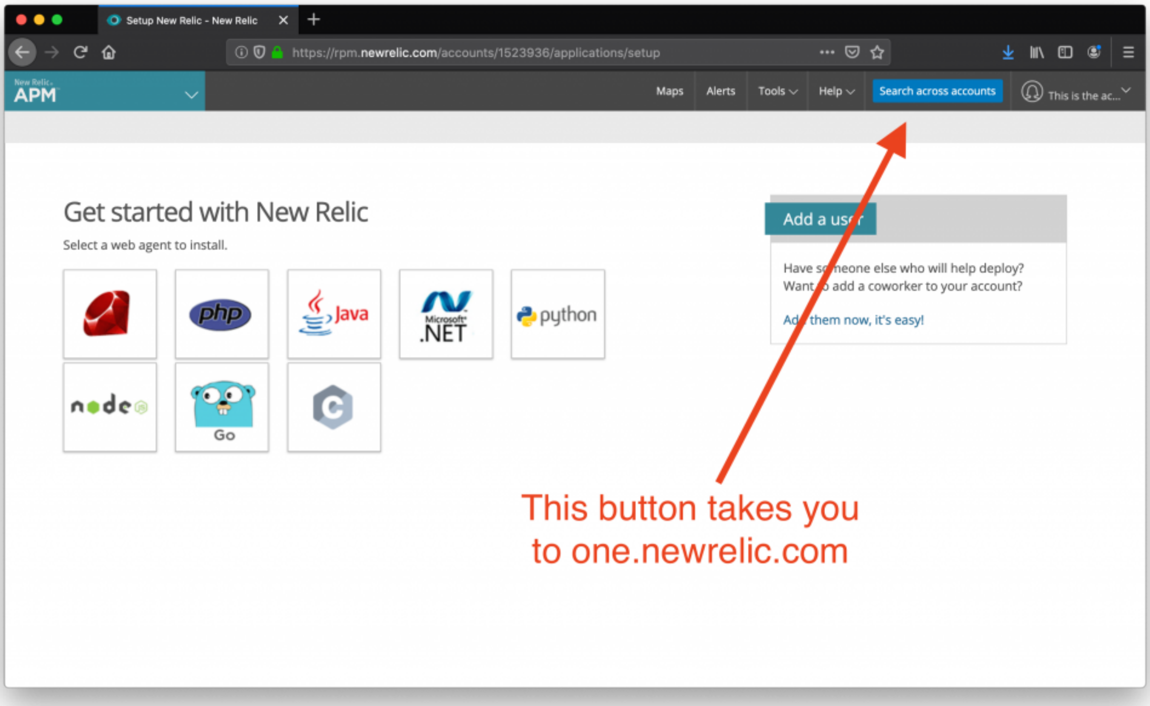
Get started with New Relic

Select a web agent to install.

Have someone else who will help deploy?
Want to add a coworker to your account?

Add them now, it's easy!

Now, when using the FALSE2TRUE trick, changing all “false” values to “true”:



Get started with New Relic

Select a web agent to install.

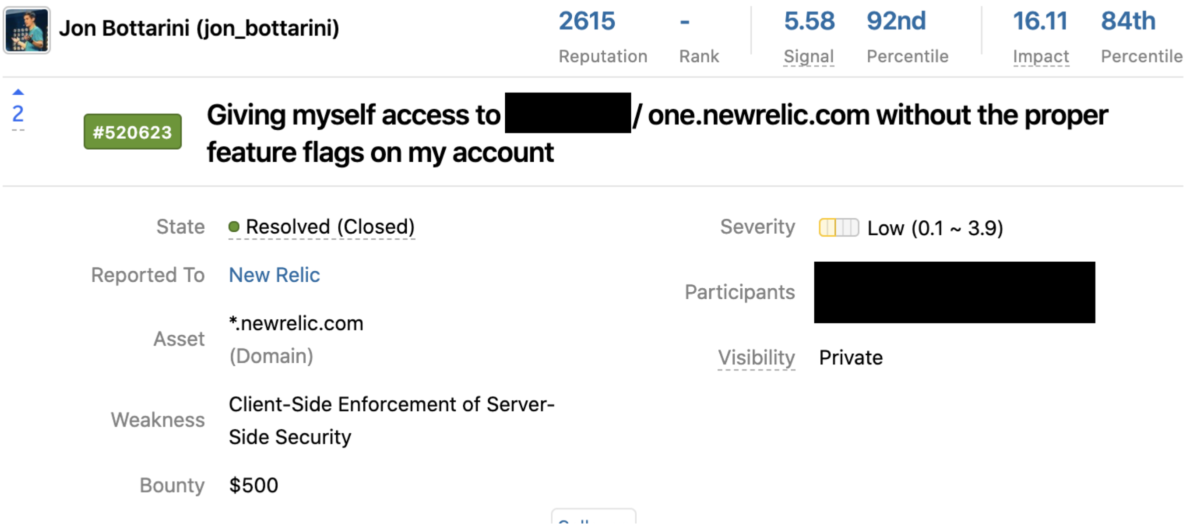
Add a user

Have someone else who will help deploy? Want to add a coworker to your account?

Add them now, it's easy!

This button takes you to one.newrelic.com

Bug found!



Jon Bottarini (jon_bottarini)

2615	-	5.58	92nd	16.11	84th
Reputation	Rank	Signal	Percentile	Impact	Percentile

2

#520623 Giving myself access to [redacted] / one.newrelic.com without the proper feature flags on my account

State	● Resolved (Closed)	Severity	Low (0.1 ~ 3.9)
Reported To	New Relic	Participants	[redacted]
Asset	*.newrelic.com (Domain)	Visibility	Private
Weakness	Client-Side Enforcement of Server-Side Security		
Bounty	$500		

The Burp match and replace rule gave me access to a completely unreleased feature with a ton of new functionality, where I found other bugs as well, prior to the public release.

A word of warning: Be careful when using the FALSE2TRICK on big websites, because you can *really* mess up your session, or even your entire account.

I’m curious how you use the match/replace tool in your Burp projects – leave a comment below or ping me on Twitter if you would like to share. If it’s a really good tip, I’ll put it in this post so others can learn!

Until next time 👋

(The New Relic security team reviewed this post in full before it was published and have agreed to let me use one of my reports as an example. I am especially grateful for the New Relic team to be so open and accepting of using their program and bugs I’ve found in examples on my blog).