

Forum:[Hack Forums](#)

Thread: [\[Revised\] How I Abuse Mint Mobile For Free Service](#)

Oxycodone - July 9, 2022, 11:38 am

How I abuse API's and force them to provide free phone service, the easy way

Let's begin by introducing myself and to add some clarification on how this came about. I prefer to call myself JuanitoVerde, someone who has always been interested in how things work; throughout the years this has caused me to break many things beyond repair. One lovely thing about API's , they're usually not going to break or become damaged physically after I'm done with it, I hope. Secondly, at least you can patch code — you can't patch circuit boards after you give them to me.

Now let's discuss the moments that lead up to my addiction of abusing API's. There I was at the infamous Target Store, wondering why my darling Fry's Electronics left me; leaving a hole in my heart needing to be filled. Also, I needed phone service, I got tired of paying 80\$ a month so target has some great affordable month-to-month options. While browsing the Phone Card section one day, I saw 7 Day Trials for Mint Mobile for 2\$. "Hmm 4weeks x 2dollars = 8\$ a month", I thought to myself. I grabbed the last remaining ones, happily went to checkout and thought life couldn't be sweeter. 80\$ a month to 8\$ a month, haha! I feel like I'm finally beating the system.

Now here comes where the fun stuff begins. I'm there on Mint Mobiles website per instruction of the cards I had just purchased.

<https://my.mintmobile.com/activation>

Being the person I am, we know I just like to know how things work. What do I do? I obviously do everything in my power to break this thing, just kidding. I decide to inspect the page source and look at the html source code, see what files are being linked, what resources are being used, where these files are located, and mentally mapping the file folder system and keeping mental notes of things that look interesting. I feel like a kid in a candy store, but no candy... where is my act code being sent to?

I sometimes have bad vision staring at a screen so often, I probably over looked it. So let's make things easier, right click > inspect (this is where the fun really starts. Hold on tight)

-- i plan to add pictures -- --so here's me for example, as if i was talking about a picture that should be here --.

It's such a lovely thing, isn't it ? Organized and full of interesting things to question — something we don't have in common, but they do say opposites attract .

I enter 11 random numbers as the ACT code, I watch it appear in the panel as a request being made to... another site? What's this.

<https://w3b-api.ultramobile.com/v2/mint/sims?actCode=12345678901>

and for reference, what a valid response looks like

<https://w3b-api.ultramobile.com/v2/mint/sims?actCode=DDEJC317JEF>

```
{
  "deliveryType": "PHYSICAL",
  "id": "890126089711559827",
  "masterAgent": 745,
  "distributor": 837,
  "initialProductId": 7000239,
  "productType": "ECOMM",
  "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJnZW4zVG9rZW4iOiJleUpoYkdjaU9pSINVekkxTmlJc0luUjVjQ0k2SWtwWFZDSjkuZXIKaWNtRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16Z3dOelVpT25zaVpuVnNiQ0k2ZEHKMPYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTI5YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLjltZG55Mzd1MmZ1N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpacKhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4cERTdXhJcnJQS3BFTkRCOXhXNGRUWDlxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJkMm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKcHZUaGNieDRsNUwzaVZxMzlwQkh5cHZaT2RaUFireHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBMVZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZIM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1FfT292eGFtMzVudylslnVzZXJJZCI6NzQzODAzNSwiSUNDSUQiOiI4OTAxMjYwODk3MTE1NTk4MjcilCJicmFuZCI6Im1pbmNjQ0k2SWtwWFZDSjkuZXIKaWNtRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16Z3dOelVpT25zaVpuVnNiQ0k2ZEHKMPYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTI5YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLjltZG55Mzd1MmZ1N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpacKhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4cERTdXhJcnJQS3BFTkRCOXhXNGRUWDlxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJkMm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKcHZUaGNieDRsNUwzaVZxMzlwQkh5cHZaT2RaUFireHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBMVZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZIM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1FfT292eGFtMzVudylslnVzZXJJZCI6NzQzODAzNSwiSUNDSUQiOiI4OTAxMjYwODk3MTE1NTk4MjcilCJicmFuZCI6Im1pbmNjQ0k2SWtwWFZDSjkuZXIKaWNtRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16Z3dOelVpT25zaVpuVnNiQ0k2ZEHKMPYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTI5YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLjltZG55Mzd1MmZ1N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpacKhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4cERTdXhJcnJQS3BFTkRCOXhXNGRUWDlxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJkMm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKcHZUaGNieDRsNUwzaVZxMzlwQkh5cHZaT2RaUFireHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBMVZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZIM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1FfT292eGFtMzVudylslnVzZXJJZCI6NzQzODAzNSwiSUNDSUQiOiI4OTAxMjYwODk3MTE1NTk4MjcilCJicmFuZCI6Im1pbmNjQ0k2SWtwWFZDSjkuZXIKaWNtRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16Z3dOelVpT25zaVpuVnNiQ0k2ZEHKMPYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTI5YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLjltZG55Mzd1MmZ1N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpacKhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4cERTdXhJcnJQS3BFTkRCOXhXNGRUWDlxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJkMm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKcHZUaGNieDRsNUwzaVZxMzlwQkh5cHZaT2RaUFireHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBMVZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZIM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1FfT292eGFtMzVudylslnVzZXJJZCI6NzQzODAzNSwiSUNDSUQiOiI4OTAxMjYwODk3MTE1NTk4MjcilCJicmFuZCI6Im1pbmNjQ0k2SWtwWFZDSjkuZXIKaWNtRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16Z3dOelVpT25zaVpuVnNiQ0k2ZEHKMPYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTI5YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLjltZG55Mzd1MmZ1N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpacKhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4cERTdXhJcnJQS3BFTkRCOXhXNGRUWDlxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJkMm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKcHZUaGNieDRsNUwzaVZxMzlwQkh5cHZaT2RaUFireHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBMVZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZIM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1FfT292eGFtMzVudylslnVzZXJJZCI6NzQzODAzNSwiSUNDSUQiOiI4OTAxMjYwODk3MTE1NTk4MjcilCJicmFuZCI6Im1pbmNjQ0k2SWtwWFZDSjkuZXIKaWNtRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16Z3dOelVpT25zaVpuVnNiQ0k2ZEHKMPYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTI5YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLjltZG55Mzd1MmZ1N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpacKhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4cERTdXhJcnJQS3BFTkRCOXhXNGRUWDlxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJkMm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKcHZUaGNieDRsNUwzaVZxMzlwQkh5cHZaT2RaUFireHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBMVZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZIM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1FfT292eGFtMzVudylslnVzZXJJZCI6NzQzODAzNSwiSUNDSUQiOiI4OTAxMjYwODk3MTE1NTk4MjcilCJicmFuZCI6Im1pbmNjQ0k2SWtwWFZDSjkuZXIKaWNtRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16Z3dOelVpT25zaVpuVnNiQ0k2ZEHKMPYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTI5YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLjltZG55Mzd1MmZ1N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpacKhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4cERTdXhJcnJQS3BFTkRCOXhXNGRUWDlxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJkMm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKcHZUaGNieDRsNUwzaVZx
```

Code "deliveryType": "PHYSICAL", ## I'm sure this means physical card... "id": "890126089711559827", ## The '89' tells me it's the SIM's ICCID # .. Which may be helpful. "masterAgent": 745, ## Unsure.. Maybe the Warehouse Code or Main Seller? I don't know. "distributor": 837, ## Target? Or The Store I got the code from. "initialProductId": 7000239, ## "Product ID" not sure what "initial" is suppose to be refering to.. "productType": "ECOMM" ## I wonder what otehr types they have? ECOMM = Ecommerce I'm guessing aswell. Im going to assume that the long token is base64. I hope I'm right. -- edit, i was wrong. JWT Token <https://devtoolzone.com/decoder/jwt> did a better job.

to token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJnZW4zVG9rZW4iOiJleUpoYkdjaU9pSINVek
kxTmlJc0luUjVjQ0k2SWtwWFZDSjkuZXlKaWNTnRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1
VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16
Z3dOelVpT25zaVpuVnNiQ0k2ZEhKMVpYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTl5
YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLJtZG55Mzd1MmZ1
N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpackhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4c
ERTdXhJcnJQS3BFTkRCOXhXNGRUWDIxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJk
Mm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKChZUaGNieDRsNU
wzaVZxMzlwQkh5cHZaT2RaUFlreHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBM
VZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZlM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15
U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1Fft292eGF
tMzVudylslnVzZXJJZCI6NzQzODA3NSwiSUNDsUQiOiI4OTAxMjYwODk3MTE1NTk4MjciLCJicmF
uZCI6Im1pbm1pbnQ0k2SWtwWFZDSjkuZXlKaWNTnRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1
VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16
Z3dOelVpT25zaVpuVnNiQ0k2ZEhKMVpYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTl5
YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLJtZG55Mzd1MmZ1
N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpackhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4c
ERTdXhJcnJQS3BFTkRCOXhXNGRUWDIxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJk
Mm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKChZUaGNieDRsNU
wzaVZxMzlwQkh5cHZaT2RaUFlreHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBM
VZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZlM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15
U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1Fft292eGF
tMzVudylslnVzZXJJZCI6NzQzODA3NSwiSUNDsUQiOiI4OTAxMjYwODk3MTE1NTk4MjciLCJicmF
uZCI6Im1pbm1pbnQ0k2SWtwWFZDSjkuZXlKaWNTnRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1
VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16
Z3dOelVpT25zaVpuVnNiQ0k2ZEhKMVpYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTl5
YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLJtZG55Mzd1MmZ1
N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpackhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4c
ERTdXhJcnJQS3BFTkRCOXhXNGRUWDIxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJk
Mm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKChZUaGNieDRsNU
wzaVZxMzlwQkh5cHZaT2RaUFlreHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBM
VZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZlM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15
U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1Fft292eGF
tMzVudylslnVzZXJJZCI6NzQzODA3NSwiSUNDsUQiOiI4OTAxMjYwODk3MTE1NTk4MjciLCJicmF
uZCI6Im1pbm1pbnQ0k2SWtwWFZDSjkuZXlKaWNTnRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1
VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16
Z3dOelVpT25zaVpuVnNiQ0k2ZEhKMVpYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTl5
YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLJtZG55Mzd1MmZ1
N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpackhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4c
ERTdXhJcnJQS3BFTkRCOXhXNGRUWDIxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJk
Mm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKChZUaGNieDRsNU
wzaVZxMzlwQkh5cHZaT2RaUFlreHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBM
VZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZlM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15
U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1Fft292eGF
tMzVudylslnVzZXJJZCI6NzQzODA3NSwiSUNDsUQiOiI4OTAxMjYwODk3MTE1NTk4MjciLCJicmF
uZCI6Im1pbm1pbnQ0k2SWtwWFZDSjkuZXlKaWNTnRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1
VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16
Z3dOelVpT25zaVpuVnNiQ0k2ZEhKMVpYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTl5
YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLJtZG55Mzd1MmZ1
N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpackhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4c
ERTdXhJcnJQS3BFTkRCOXhXNGRUWDIxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJk
Mm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKChZUaGNieDRsNU
wzaVZxMzlwQkh5cHZaT2RaUFlreHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBM
VZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZlM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15
U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1Fft292eGF
tMzVudylslnVzZXJJZCI6NzQzODA3NSwiSUNDsUQiOiI4OTAxMjYwODk3MTE1NTk4MjciLCJicmF
uZCI6Im1pbm1pbnQ0k2SWtwWFZDSjkuZXlKaWNTnRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1
VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16
Z3dOelVpT25zaVpuVnNiQ0k2ZEhKMVpYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTl5
YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLJtZG55Mzd1MmZ1
N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpackhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4c
ERTdXhJcnJQS3BFTkRCOXhXNGRUWDIxM3ZlZHN5WWNaOFBjUHBBbkFnb1VOcXQ0a3hnVjJk
Mm5JQmFsTVdQWEdjV3dVQ0k4ekJPeEVTZmtHMmh1UnZ0X2RPM1J0VFBKChZUaGNieDRsNU
wzaVZxMzlwQkh5cHZaT2RaUFlreHkxN3lqekhFeVhOX2xLYVJ0MG9NSV9JbzdjZ21jWE5zRXBM
VZMZEQyODh3anMzM2pkclNWU2RmUV9fNDU3ZlM0TU1YRnZodUE3RHIDdnNNNXpicUJ4Sy15
U1VLWU9fZ184X0gyUi1SN29aYXpySzBhTldqeWk3SHBxOF8yMXI5Y1RJTEtPOGZsT1Fft292eGF
tMzVudylslnVzZXJJZCI6NzQzODA3NSwiSUNDsUQiOiI4OTAxMjYwODk3MTE1NTk4MjciLCJicmF
uZCI6Im1pbm1pbnQ0k2SWtwWFZDSjkuZXlKaWNTnRnVaQ0k2SWsxSIRsUWIMQ0ppY21GdVpGUjVjR1
VpT2lKSIRsUkZVazVCVENJc0ltVjRjQ0k2TVRZMU56WXpOVFV3Tml3aWFXUnpJanA3SWpjME16
Z3dOelVpT25zaVpuVnNiQ0k2ZEhKMVpYMTIMQ0p1WW1ZaU9qRTJOVGMyTXpFMk1EWXNJbTl5
YVdkcGJpSTZOelF6T0RBM05Td2lkWE5sY2tWdWRpSTZJbEJTVDBRaWZRLJtZG55Mzd1MmZ1
N09rSIRMeHJhX1lwXzQxLWFFckJNYnNxQWpackhDVzAtRWZVOWxKOUkzOUY4c3ktejM2aVE4c
ERTdX

```
Code { "gen3Token" :
```

"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJicmFuZCI6IkJ1TlQiLCJicmFuZFR5cGUOiJJTIRFUK5BTClsImV4cCI6MTY1NzYzNTUwNiwiawWRzljp7ljc0MzgwNzUiOnsiZnVsbiCI6dHJ1ZX19LCJuYmYiOiE2NTc2MzE2MDYsIm9yaWdpbil6NzQzODAzNSwidXNlckVudil6IIBST0QifQ.Rmdny37u2fu7OkJT

Lxra_R0_41-aErBMbsqAjZrHCW0-EfU9IJ9I39F8sy-z36iQ8pDSuxIrrPKpENDB9xW4dTX213vedsyYcZ8PcPpAnAgoUNqt4kxgV2d2nIBalMWPXGcWwUCI8zBOxESfkG2huRvt_dO3RtTPJpvThcbx4I5L3iVq320BHypvZOdZPYkxy17yzHEyXN_IKaRt0oMI_lo7bgmcXNsEpLaVLdD288wjs33jdrSVSdfQ__457fS4MMXFvhuA7DyCvsM5zbqBxK-ySUKYO_g_8_H2R-R7oZazrK0aNWjyi7Hpq8_21yycTILKO8flOQ_Oovxam35nw",

(Seperating the output, looks less messy)

```
"userId" : 7438075, "ICCID" : "890126089711559827", "brand" : "mint", "ip" : "192.241.198.127",  
"iat" : 1657631906, "nbf" : 1657631906, "exp" : 1657632806, "iss" : "ULTRA" }
```

Okay so lets see what that gen3Token is .. I'm assuming again, JWT and HS256 have something to do with it...

```
Code { "brand" : "MINT", "brandType" : "INTERNAL", "exp" : 1657635506, "ids" : { "7438075" : {  
"full" : true } } }, "nbf" : 1657631606, "origin" : 7438075, "userEnv" : "PROD" }
```

& Thats about that. It looks like it repeated its information 3x for the most part. I wonder why? Seems unneeded.

Well, Now I'm curious. Why? Why is the API On Ultra? So I pop open my cellular device, tell Siri to ring up my good old pal Ryan Reynolds and see what's going on here. Well unfortunately, Siri doesn't have that contact in my phone book and Ryan Reynolds probably doesn't even know who I am. Not yet at least. if you're reading this Mr. Reynolds, I appreciate you. You're awesome. I don't mean any harm or intend for any disrespect. Thank you!

So now just form assumptions. We know T-Mobile and these providers have smaller companies such as Mint and Ultra and others we don't need to name, that for a lack of better terms, "piggy back" off there network and cell towers. These companies can provide us quality service at better rates , and In reality the only difference it seems to me is sacrificing "priority" of service. Meaning, tor 80\$ a month, you get to load YouTube videos faster then me at the airport. Not a problem, I don't have money to fly anywhere anyways.

So I'm assuming mint is doing the same or has a contract with ultra ? It looks like the sites damn near operate the same or have the same developers. Maybe they just use there developers and this was a productive and cost efficient way of handling the web aspect of things. I don't know.

We can now blame ultra mobile and not Deadpool for what's about to come, right? We can blame the awesome information that is given upon the right code being supplied. What a nice detailed xml report.

SO WHAT IS ABOUT TO COME? HOW IS ANY OF THIS INFORMATION USEFUL?

Well, theoreddically I have all the information needed to brute force a list of legitiamte SIM Activation Codes..

I don't want to get to deep into the whole "key space" thing, as I don't want to missinform anyone.

What I know is that, computers don't really generate anything at 100% Random. Meaning, you can with enough data, determine how a code is generated. With that , you can create a mask of the keyspace hopefully I'm using that word right -- and have a highly effective and successful attack to generate valid codes.

So remember, what I'm about to show is most likely very useless by itself. This is based off of VERY LIMITED information. I would just like to explain how this can potentially be something used to be more effective with enogh data.

What we know: (facts)

A String with the length 11 Chars &/ INT = ACT Code
Thats really it, sort of. So what can we use with this ...

Heres the break down of 5 different codes (valid)

% = INT 1,2,3,4,5,6,7,8,9,0

, = Char a,b,c,d,e,f,g,h,i,j,k...x,y,z (you get the point)

With enough data, we could elimiante what characters aren't being used. We could also determine if characters like "O" would be ignored and instead replaced with "0". Information like this can make generating a wordlist that much more realistic. But we don't have enough data to get that far into things. So heres what we got.

Converting the other codes I had into masks using % and , we can start looking at them a bit more closely

1# , , , , , % % % , , ,

2# % % % , % , , % , % %

3# , % % , % , , , , ,

4# % , , , % % % % , % %

5# , % % , , , , % % % ,

so lets now break it down to something hopefully we can use to be more effective in a wordlist / bruteforce mask What do we know for facts about each act code?

1# , , , , , % % % , , ,

-- 8 Letters

-- 3 Numbers

-- This is not a free trial code, this is 1 month.

-- 5letters, 3 numbers, 3 letters

2# % % % , % , , % , % %

-- 4 Letters

-- 7 Numbers

-- 3 numbers, 1 letter, 1 number, 2 letters, 1 number, 1 letter, 2 numbers

3# , % % , % , , , , ,

-- 8 Letters

-- 3 numbers

-- 1 letter, 2 numbers, 1 letter, 1 number, 6 letters

4# % , , , % % % % , % %

-- 7 Numbers

-- 4 Letters

-- 1 Number, 3 letters, 4 numbers, 1 letter, 2 numbers

5# , % % , , , % % % ,

-- 6 Letters

-- 5 Numbers

-- 1 letter, 2 numbers, 4 letters, 3 numbers, 1 letter

We based on this, we can see the following (again, this isn't accurate and every code found can easily prove this wrong. Not enough data to determine the accuracy of this currently.)

8 Characters are common for being "Letters" in 2 codes -- same with 3 being numbers

1# , , , , % % % , , ,

3# , % % , % , , , , ,

Notice anything else smiliar?

Not really, nothing we can really say with high accuracy at least. Between these two , the letters can be seen in groups of 5,3,6, and a couple times alone

2# % % % , % , , % , % % 4# % , , , % % % % , % %

Also, 7 numbers are comon here, 4 letters..

Hmm, maybe this would be more beneficial to use. Save some time..

1# , , , , % % % , , , 2# % % % , % , , % , % % 3# , % % , % , , , , , 4# % , , , % % % % , % % 5# , % % , , , , % % % ,

Space 1 = 3/5 Times a Letter Space 2 = 3/5 Times a Number Space 3 = 3/5 Times A Number
Space 4 = ALWAYS A LETTER.. Space 5 = 3/5 Times a Number Space 6 = 3/5 Times a Letter
Space 7 = 3/5 Times a Letter. Space 8 = 4/5 Times a Number Space 9 = 4/5 Times a Letter Space
10= 3/5 Times a Number Space 11 = 3/5 Times a Letter

Meaning based on this alone, a mask seems to be something like

, % % , % , , % , % ,

What do we notice in this? Well it shows us the same amount of numbers and letters as code #5 did.

But it kinda will end there for now, not because thats all we can conclude. No if we remove the 1st code knowing its a a 1 month code while the other 4 are 1 week trails. We would have a lot more reliable information to determine things.

But this is mainly to show you how with enough data, you can create something more effective. ANd how with little data, you probably wont be effective.

So lets just say a good key space to go with based on this information would be

, % % , % , , % , % ,

Lets open up a tool to generate a wordlist based on this.

crunch -h

crunch 11 11 -t ,%%,%,%,%,% ,>> mintmobilecodesmaybe.lst

that will generate a .lst file (basically a text file) full of every combination with that mask. The file will be called "mintmobilecodesmaybe.lst"

So the next step is to try it out. This may take some playing around with but for example, you would use a fuzzing software like dirb.

dirb -h

now with this you would want to run something like this.

dirb <https://w3b-api.ultramobile.com/v2/mint/sims?actCode=> ./mintmobilecodesmaybe.lst

Remember, we know that on invalid codes, its a 404. So we can filter using dirb and onyl show codes when they're valid.

So now, how is this even useful? What is the purpose of this.. If we don't have the SIM Card matching the ICCID, we cant use these codes.

Well, this is where you get creative. I am writing this for pure infromation, its up to you to do what you will with it. I wrote this to show how you should always wonder how things work, tinker with things and explore. Theoredically you have all the information needed to call up mint. and provide a list of sim cards that 'dont work' and you would like a replacement. I'm sure mint would replace a card if you know all the details that are provided by the correct response of a valid code. You can even social engineer possibly to say your the store based on the distributor # it provides. You can determine even what card you're claiming to be invalid by the product ID i'm sure.

I'm in no way encouraging you to use this with any malicious intent. I am simply providing an example of how this could be used agaisnt a company. Why API's should be secure, and so on. etc..

More importantly, I want to encourage the community to always think about these things, maybe you can discover something interesting just by trying out what others may not even consider. Was

this worth my time? Yes I found it interesting, I learned different things today. I learned about JWT when decoding the response. I learned a bit more about API's, hey I even learned how to post my 1st github page.

Thank you for reading. I want to thank everyone who I mentioned, and if I didn't mention you, I apologize. -- MINT MOBILE, ULTRA MOBILE, <https://devtoolzone.com/decoder/jwt>, google, dirb, and crunch & its creators / dev's & team overall.

Here's a freebie... PS: Ultra Mobile only uses #'s no Letters in there ACT codes... Meaning your accuracy of success is probably a lot more realistic. with ultra act codes..

Oxycodone - July 11, 2022, 2:28 am

I know there's a bunch of spelling mistakes I just noticed. I typed this on my phone.

But hopefully you can follow along still.

Parks - July 11, 2022, 9:22 am

(Jul 11, 2022 02:28 AM)Oxycodone Wrote: [\[CITE\]](#) I know there's a bunch of spelling mistakes I just noticed. I typed this on my phone.

But hopefully you can follow along still.

There is a ton indeed lol. Awesome tutorial man. While simple I never really digged into this but it enlightened me to think about other platforms where you could likely get the API to abuse a few more things like making unlimited requests without getting rate limited.

G3n3sis187 - July 11, 2022, 4:25 pm

lol yes indeed. all good though. good work. ill play around with this some more

Oxycodone - July 12, 2022, 8:57 am

(Jul 11, 2022 04:25 PM)G3n3sis187 Wrote: [\[CITE\]](#) lol yes indeed. all good though. good work. ill play around with this some more updated it with a way better version. More understandable and readable. More informative aswell

lo0sr - July 13, 2022, 10:33 am

This is a really interesting discovery! Thanks for sharing and as shatter mentioned maybe see if you can get a bug bounty.

Oxycodone - July 13, 2022, 11:26 am

(Jul 13, 2022 10:22 AM)shatter Wrote: [\[CITE\]](#) This is some good research. Cheers!

If you've already publicized this, should probably try and get a bounty. Gnarly info disclosure.

(Jul 13, 2022 10:33 AM)lo0sr Wrote: [\[CITE\]](#) This is a really interesting discovery! Thanks for sharing and as shatter mentioned maybe see if you can get a bug bounty.

How do I go about doing that

Oxycodone - July 13, 2022, 12:15 pm

(Jul 13, 2022 11:28 AM)shatter Wrote: [\[CITE\]](#) usually you can reach out to someone on their site

<https://www.bleepingcomputer.com/news/security/mint-mobile-hit-by-a-data-breach-after-numbers-pored-data-accessed/>

lol maybe they dont have one

can try and find someone who works for their security team on linkedin

I called technical support and talked to a team member. The first person didn't have any idea what I was talking about. Kept telling me if my account wasn't working . I called back and a team member helped me submit it to the appropriate department. I emailed it over and gave a brief description over the phone. Let them know nothing was with any malicious intent and just wanted to help them prevent any issues.

He seemed cool. Hopefully this doesn't bite me in the ass. I never actually abused for free phone service. So I don't think it will.

I just let them known that the API response information should be handled differently and it provides details which could possibly be used in a way they weren't intended to be used for .