



GOLIATH NATIONAL BANK

# SECURE CODING

TEAM 12 - PHASE 4

MEMBERS

Alexander Lill    Lorenzo Donini

---

Florian Mauracher    Mahmoud Naser

# FIX ALL THE BUGS





ONE DOES NOT SIMPLY  
FIX ALL THE BUGS

# TOP VULNERABILITIES

# TEAM 7

# OTG-CONFIG-003 - FILE EXTENSIONS HANDLING FOR SENSITIVE INFORMATION

Score

Attack Vector

Attack Complexity

Privileges Required

User Interaction

Scope

Confidentiality

Integrity

Availability

```
case 9: // dearchive all the modifi
P_SetupLevel (gameepisode, gamemap, 0, gameskill);
displayplayer = consoleplayer; // view the guy you are playing
starttime = _GetTime (); // playerstill.didsecret = true;
gameaction = ga_nothing;
Z_CheckHeap (0);

// clear cmd building stuff
memset (gamekeydown, 0, sizeof(gamekeydown));
joyxmove = joyymove = 0;
mousex = mousey = 0;
sendpause = sendsave = paused = false;
memset (mousebuttons, 0, sizeof(mousebuttons));
memset (joybuttons, 0, sizeof(joybuttons));

id G_PlayerReborn (int player)
{
    player_t* p;
    int i;
    int frags[MAXPLAYERS];
    int killcount;
    int itemcount;
    int secretcount;

    memcpy (frags, players[player].frags, sizeof(players[player].frags));
    killcount = players[player].killcount;
    itemcount = players[player].itemcount;
    secretcount = players[player].secretcount;

    p = &players[player];
    memset (p, 0, sizeof(*p));

    memcpy (players[player].frags, frags, sizeof(players[player].frags));
    players[player].killcount = killcount;
    players[player].itemcount = itemcount;
    players[player].secretcount = secretcount;

    p->usedown = p->attackdown = true; // don't do anything immediately
    p->playerstate = PST_LIVE;
    p->health = MAXHEALTH;
    p->readyweapon = p->pendingweapon = wp_pistol;
    p->weaponowned[wp_fist] = true;
    p->weaponowned[wp_pistol] = true;
    p->ammolam_clip1 = 50;

    for (i=0 ; i<NUMAMMO ; i++)
        p->maxammoli[i] = maxammoli[i];
}

P_SetupLevel (gameepisode, gamemap, 0, gameskill);
displayplayer = consoleplayer; // view the guy you are playing
starttime = _GetTime (); // playerstill.didsecret = true;
gameaction = ga_nothing;
Z_CheckHeap (0);

// clear cmd building stuff
memset (gamekeydown, 0, sizeof(gamekeydown));
joyxmove = joyymove = 0;
mousex = mousey = 0;
sendpause = sendsave = paused = false;
memset (mousebuttons, 0, sizeof(mousebuttons));
memset (joybuttons, 0, sizeof(joybuttons));

id G_PlayerReborn (int player)
{
    player_t* p;
    int i;
    int frags[MAXPLAYERS];
    int killcount;
    int itemcount;
    int secretcount;

    memcpy (frags, players[player].frags, sizeof(players[player].frags));
    killcount = players[player].killcount;
    itemcount = players[player].itemcount;
    secretcount = players[player].secretcount;

    p = &players[player];
    memset (p, 0, sizeof(*p));

    memcpy (players[player].frags, frags, sizeof(players[player].frags));
    players[player].killcount = killcount;
    players[player].itemcount = itemcount;
    players[player].secretcount = secretcount;

    p->usedown = p->attackdown = true; // don't do anything immediately
    p->playerstate = PST_LIVE;
    p->health = MAXHEALTH;
    p->readyweapon = p->pendingweapon = wp_pistol;
    p->weaponowned[wp_fist] = true;
    p->weaponowned[wp_pistol] = true;
    p->ammolam_clip1 = 50;

    for (i=0 ; i<NUMAMMO ; i++)
        p->maxammoli[i] = maxammoli[i];
}

case 9: // dearchive all the modifi
P_UnArchivePlayers ();
P_UnArchiveWorld ();
P_UnArchiveThinkers ();
P_UnArchiveSpecials ();

if (*save_p != 0xd)
    _Error ("Bad save");

// done
Z_Free (savebuffer);

// user has saved
R_ExecuteSetView();

// draw the pattern into the screen
R_FillBackScreen ();

// add G_CoSaveSave void
{
    char name1[100];
    char name2[VERSIONSIZE];
    char* description;
    int length;
    int i;

    if (M_CheckParm ("-cdrom"))
        sprintf (name, "c:\\d");
    else
        sprintf (name, SAVENAME);
    description = savedescription;

    save_p = savebuffer = save_p + sizeof(SAVEHEADER);
    save_p += SAVESTRING;
    save_p += save_p - sizeof(SAVEHEADER);
    save_p += VERSIONSIZE;
    save_p += save_p - sizeof(VERSIONHEADER);
    save_p += VERSIONSIZE;
    *save_p++ = gameskill;
    *save_p++ = gameepisode;
    *save_p++ = gamemap;
    for (i=0 ; i<MAXPLAYER;
        *save_p++ = playernames[i];
    }
    *save_p++ = leveltime;
    *save_p++ = leveltime;
    *save_p++ = leveltime;
    *save_p++ = leveltime;
}
```

	Likelihood	Impact	Found in Phase 2	Yes
5.9	High	Network	Medium	
Size 0;	None			
the back screen	None			
ZEI;	None			
EGAMEMAP("%d.ds", savegamenumber); option;	Unchanged			
screen(1140x1000);	High			
option, SAWG_FRACSIZE; SIZE; (name2), %6i, VERSION); , VERSIONINSIZE);	None			
S; i++) eringame(i); >16; >8;	None			
if (episode > 1) episode = 1; // only start episode 1 on cheater mode } else { if (episode > 3) episode = 3; }  if (map < 1) map = 1;  if ( (map > 9) && ( gamemode != commercial ) map = 9;  M_ClearRandom ();  if (skill == sk_nightmare    respawnparm ) respawnmonsters = true; else respawnmonsters = false;  if (fastparm    (skill == sk_nightmare && gameskill != sk_nightmare)) { for (i=S_SARG_RUN1 ; i<=S_SARG_PAIN2 ; i++) states[i].tics >>= 1; mobjinfolMT_BRUISERSHOT1.speed = 20*FRACUNIT; mobjinfolMT_HEADSHOT1.speed = 20*FRACUNIT; mobjinfolMT_TROOPSHOT1.speed = 20*FRACUNIT; else if (skill != sk_nightmare && gameskill == sk_nightmare) { for (i=S_SARG_RUN1 ; i<=S_SARG_PAIN2 ; i++) states[i].tics <<= 1; mobjinfolMT_BRUISERSHOT1.speed = 15*FRACUNIT; mobjinfolMT_HEADSHOT1.speed = 10*FRACUNIT; mobjinfolMT_TROOPSHOT1.speed = 10*FRACUNIT;  // force players to be initialized upon first level load for (i=0 ; i<MAXPLAYERS ; i++) players[i].playerstate = PST_REBORN;  usergame = true; // will be set false if a demo paused = false; demoplayback = false; automapactive = false; }  break; case ga_screenshot: W_Screenshot(); gameaction = ga_nothing; break; case ga_nothing: break;	(SPR_SHT2,1,7,(NULL),S_DSGUN4,0,0), // S_DSGUN3 (SPR_SHT2,2,7,(A_CheckReload),S_DSGUN5,0,0), // S_DSGUN4 (SPR_SHT2,3,7,(A_OpenShotgun2),S_DSGUN6,0,0), // S_DSGUN5 (SPR_SHT2,4,7,(NULL),S_DSGUN7,0,0), // S_DSGUN6 (SPR_SHT2,5,7,(A_LoadShotgun2),S_DSGUN8,0,0), // S_DSGUN7 (SPR_SHT2,6,6,(NULL),S_DSGUN9,0,0), // S_DSGUN8 (SPR_SHT2,7,6,(A_CloseShotgun2),S_DSGUN10,0,0), // S_DSGUN9 (PA_SHT2,0,5,(A_ReFire),S_DSGUN,0,0), // S_DSGUN10 (PA_SHT2,1,7,(NULL),S_DSNR2,0,0), // S_DSNR1 (SPR_SHT2,0,3,(NULL),S_DSGUNDOWN,0,0), // S_DSNR2 (SPR_SHT2,32776,5,(A_Light1),S_DSGUNFLASH2,0,0), // S_DSGUNFLASH1 (SPR_SHT2,32777,4,(A_Light2),S_LIGHTDONE,0,0), // S_DSGUNFLASH2 (SPR_CHGG,0,1,(A_WeaponReady),S_CHAIN,0,0), // S_CHAIN (SPR_CHGG,0,1,(A_Lower),S_CHAINDOWN,0,0), // S_CHAINDOWN (SPR_CHGG,0,1,(A_Raise),S_CHAINUP,0,0), // S_CHAINUP (SPR_CHGG,0,4,(A_FireCGun),S_CHAIN2,0,0), // S_CHAIN1 (SPR_CHGG,1,4,(A_FireCGun),S_CHAIN3,0,0), // S_CHAIN2 (SPR_CHGG,1,0,(A_ReFire),S_CHAIN,0,0), // S_CHAIN3 (SPR_CHGF,32768,5,(A_Light1),S_LIGHTDONE,0,0), // S_CHAINFLASH1 (SPR_CHGF,32769,5,(A_Light2),S_LIGHTDONE,0,0), // S_CHAINFLASH2 (SPR_MISG,0,1,(A_WeaponReady),S_MISSILE,0,0), // S_MISSILE (SPR_MISG,0,1,(A_Lower),S_MISSILEDOWN,0,0), // S_MISSILEDOWN (SPR_MISG,0,1,(A_Raise),S_MISSILEUP,0,0), // S_MISSILEUP (SPR_MISG,1,8,(A_GunFlash),S_MISSILE2,0,0), // S_MISSILE1 (SPR_MISG,1,12,(A_FireMissile),S_MISSILE3,0,0), // S_MISSILE2 (SPR_MISG,1,0,(A_ReFire),S_MISSILE,0,0), // S_MISSILE3 (SPR_MISF,32768,3,(A_Light1),S_MISSILEFLASH2,0,0), // S_MISSILEFLASH1 (SPR_MISF,32769,4,(NULL),S_MISSILEFLASH3,0,0), // S_MISSILEFLASH2 (SPR_MISF,32770,4,(A_Light2),S_MISSILEFLASH4,0,0), // S_MISSILEFLASH3 (SPR_MISF,32771,4,(A_Light2),S_LIGHTDONE,0,0), // S_MISSILEFLASH4 (SPR_SAWG,2,4,(A_WeaponReady),S_SAWB,0,0), // S_SAW (SPR_SAWG,3,4,(A_WeaponReady),S_SAWD,0,0), // S_SAWB (SPR_SAWG,2,1,(A_Lower),S_SAWDOWN,0,0), // S_SAWDOWN (SPR_SAWG,2,1,(A_Raise),S_SAWUP,0,0), // S_SAWUP (SPR_SAWG,0,4,(A_Saw),S_SAW2,0,0), // S_SAW1 (SPR_SAWG,1,4,(A_Saw),S_SAW3,0,0), // S_SAW2 (SPR_SAWG,1,0,(A_ReFire),S_SAW,0,0), // S_SAW3 (SPR_PLSG,0,1,(A_WeaponReady),S_PLASMA,0,0), // S_PLASMA (SPR_PLSG,0,1,(A_Lower),S_PLASMADOWN,0,0), // S_PLASMADOWN (SPR_PLSG,0,1,(A_Raise),S_PLASMAUP,0,0), // S_PLASMAUP (SPR_PLSG,0,3,(A_FirePlasma),S_PLASMA2,0,0), // S_PLASMA1 (SPR_PLSG,1,20,(A_ReFire),S_PLASMA,0,0), // S_PLASMA2 (SPR_PLSF,32768,4,(A_Light1),S_LIGHTDONE,0,0), // S_PLASMAFLASH1 (SPR_PLSF,32769,4,(A_Light1),S_LIGHTDONE,0,0), // S_PLASMAFLASH2 (SPR_BFGG,0,1,(A_WeaponReady),S_BFG,0,0), // S_BFG (SPR_BFGG,0,1,(A_Lower),S_BFGDOWN,0,0), // S_BFGDOWN (SPR_BFGG,0,1,(A_Raise),S_BFGUP,0,0), // S_BFGUP (SPR_BFGG,0,20,(A_BFGsound),S_BFG2,0,0), // S_BFG1 (SPR_BFGG,1,10,(A_GunFlash),S_BFG3,0,0), // S_BFG2 (SPR_BFGG,1,10,(A_FireBFG),S_BFG4,0,0), // S_BFG3 (SPR_BFGG,1,20,(A_ReFire),S_BFG,0,0), // S_BFG4 (SPR_BFGG,22722,4,(A_Light1),S_BFGFLASH2,0,0), // S_BFGFLASH1 }			

# OTG-IDENT-004 - ACCOUNT ENUMERATION AND GUESSABLE USER ACCOUNT

Score	5.3	Likelihood	Medium
Attack Vector	Network	Impact	Low
Attack Complexity	Low	Found in Phase 2	No
Privileges Required	None		
User Interaction Scope	None		
Confidentiality	Unchanged		
Integrity	None		
Availability	None		

# TG-SESS-006 - LOGOUT FUNCTIONALITY

```
    playersl1.playerstate = PST_REBORN;
    memset (playersl1.frags,0,sizeof(playersl1.frags));
}
```

P\_SetupLevel (gameepisode, gamemap, 0, gameskill);  
displayplayer = consoleplayer;  
starttime = \_GetTime ();  
gameaction = ga\_nothing;  
Z\_CheckHeap ();

```
// dearchive all the modifications  
P_UnArchivePlayers();  
P_UnArchiveWorld();  
P_UnArchiveThinkers();  
P_UnArchiveSpecials();
```

```
// clear cmd building stuff
memset(gamekeydown, 0, sizeof(gamekeydown));
joyxmove = joyymove = 0;
mousex = mousey = 0;
sendpause = sendsave = paused = false;
```

if it's save up  
L\_Error  
exit  
done  
Z\_Free lsq

```
    void G_DoSave()
    {
        // draw the p-
```

```
killcount;           (SPH_BR0K,0,-1,(NULL),S_NULL,0,0) // end SPH_BR0K  
int itemcount;      (SPR_CELL,0,-1,(NULL),S_NULL,0,0) // S_CELL  
int secretcount;    (SPR_CELP,0,-1,(NULL),S_NULL,0,0) // S_CELP  
                     (SPR_SHLD,0,-1,(NULL),S_NULL,0,0) // KIRIN_GUN  
memcpy ((frags,players[player].frags.sizeof((frags)),  
killcount = players[player].killcount;  
                     (SPR_BRK,0,-1,(NULL),S_NULL,0,0) // B  
wminfo.gdsecret = play  
wminfo.epsd = gameep
```

```
char name[10];
char name2;
char* descri;
int;
int;
```

```
secretcount = players[player].secretecount;
p = &players[player];
memset(p, 0, sizeof(*p));
(SPR_CSAW,0,-1,(NULL),S,NULL,0,0); // minfire.next to bias
(SPR_LAJN,0,-1,(NULL),S,NULL,0,0); // if ('gameremode == com
(SPR_PLAS,0,-1,(NULL),S,NULL,0,0); // SETADMIN
(SPR_SHOT,0,-1,(NULL),S,NULL,0,0); // if (secretexit)
(SPR_SPLASH,0,-1,(NULL),S,NULL,0,0); // switch to secret
```

```

if (M_CheckForChanges())
    sprintf(description, "Changes detected");
else
    sprintf(description, "No changes detected");

```

```
-y save_p = save  
memory (sav  
save_p += S  
memset (mam  
return 0;
```

```
p->health = MAXHEALTH;           (SPR_PLAY,13,-1,(NULL),S NULL,0,0); // S DEMO  
p->readyweapon = p->pendingweapon = wp_pistol;          (SPR_PLAY,14,-1,(NULL),S NULL,0,0); // S DEMO  
p->weaponowned[wp_fist] = true;   (SPR_P0L2,0,-1,(NULL),S NULL,0,0); // S DEMO  
p->weaponowned[wp_pistol] = true;  (SPR_P0L5,0,-1,(NULL),S NULL,0,0); // S DEMO  
p->ammofam_clip1 = 50;           (SPR_P0L4,0,-1,(NULL),S NULL,0,0); // S DEMO//STICK
```

```
    memcpy(sav  
    save_p += V  
  
    *save_p++ =  
    *save_p++ =  
    *save_p++ =
```

```
for (i=0 ; i<NUMAMMO ; i++) {ISPR_POL3,32768,6,{NULL},S_HEADONHANDLES,D,O};  
    p->maxammo[i] = maxammo[i];  
    ISPR_POL1,0,-1,{NULL},S_NULL,O,O; // SP4 MEAT  
    if (secretexit)  
        ISPR_POL0,0,6,{NULL},S_LIVESTICK2,O,O; // SP4 MEAT  
        wminfo.next =  
        ISPR_POL6,1,8,{NULL},S_LIVESTICK,O,O; // SP4 MEAT  
        else if (gamermap)  
            ISPR_GCR2,0,-1,{NULL},S_NULL,O,O; // SP4 MEAT
```

```
boolean CheckSpot(int playenum, mthing_t* mthing) {  
    ISPR_GOR4,0,-1,(NULL),S_NULL,0,0); // S_MEAT  
    ISPR_GOR5,0,-1,(NULL),S_NULL,0,0); // S_MEAT  
    ISPR_SMIT,0,-1,(NULL),S_NULL,0,0); // S_STALACTITE  
    ISPR_COL1,0,-1,(NULL),S_NULL,0,0); // S_TALLGRASS  
    ISPR_COL2,0,-1,(NULL),S_NULL,0,0); // S_SHIRTGRAPH  
    // S_MUSHROOM  
    switch (gamee  
    {  
        case 1:  
            winInfo.  
            break;  
    }  
}
```

P\_ArchivePl  
P\_ArchiveW  
P\_ArchiveTh  
P\_ArchiveSp

Likelihood: **Low**

Impact: **Impact**

```
if ( gamemode == shareware )
{
    if (episode > 1)
        episode = 1; // only start episode 1 on shareware
    if (episode > 3)
        episode = 3;
}

if (ga_worldOne)
{
    G_DoWorldOne();
    break;
}

case ga_screenshot:
    M_ScreenShot(0);
    gameaction = ga_nothing;
    break;

case ga_nothing:
    break;
```

Found in Phase 2 Yes

```

{map > 9) && ( gamemode != commercial ) map = 9;
ClearRandom();
{SPR_CHGG,0,1,{A_Lower},S_CHAINDOWN,0,0}, // S_CHAINDOWN
{SPR_CHGG,0,1,{A_Raise},S_CHAINUP,0,0}, // S_CHAINUP    for (i=0 ; i<MAXPLAYERS ; i++)
{SPR_CHGG,0,4,{A_FireCGun},S_CHAIN2,0,0}, // S_CHAIN1    {
{SPR_CHGG,1,4,{A_FireCGun},S_CHAIN3,0,0}, // S_CHAIN2      if (playeringame[i])
{SPR_CHGG,1,0,{A_Refire},S_CHAIN,0,0}, // S_CHAIN3    {
{SPR_CHGE32268,5,{A_Light1},S_LIGHTDONE,0,0}, // S_CHAINFASH1 cmd = &players[i].cmd;

```

```

if(skill == sk_nightmare || respawnparm )
    respawnmonsters = true;
else
    respawnmonsters = false;

{SPR_CHR,32769,0,A_Light2,0,S_LIGHTDOME,0,0}, // S_GUNNIRLASHZ
{SPR_MISC,0,1,(A_WeaponReady),S_MISSILE,0,0}, // S_MISSILE      memcpy(cmd, &netcmds[1], size)
{SPR_MISC,0,1,(A_Lower),S_MISSILEDOWN,0,0}, // S_MISSILEDOWN
{SPR_MISC,0,1,(A_Raise),S_MISSILEUP,0,0}, // S_MISSILEUP    if (demoplayback)
{SPR_MISC,1,8,(A_GunFlash),S_MISSILE2,0,0}, // S_MISSILE1     G_ReadDemoTiccmd (cmd);
{SPR_MISC,1,12,(A_FireMissile),S_MISSILE3,0,0}, // S_MISSILE2    if (demorecording)

```

```
for (i=S_SARG_RUN1 ; i<=S_SARG_PAIN2 ; i++) {  
    states[i].tics >>= 1;  
    mobinfo[IMT_BRUISERSHOT1].speed = 20*FRACUNIT;  
    mobinfo[IMT_HEADSHOT1].speed = 20*FRACUNIT;  
    {  
        (ISPA_MISF,32768,3,(A_Light1),S_MISSILEFLASH2,0,0), // S_MISSILEFLASH1  
        (ISPA_MISF,32769,4,(NULL),S_MISSILEFLASH3,0,0), // S_MISSILEFLASH# check for turbo cheats  
        (ISPA_MISF,32770,4,(A_Light2),S_MISSILEFLASH4,0,0), // S_MISSILEFLASH# (cmd->forwardmove > TURBOTHR  
        (ISPA_MISF,32771,4,(A_Light2),S_LIGHTDONE,0,0), // S_MISSILEFLASH4 && !(gametic&31) && !(gametic
```

```

        if(skill != sk_nightmare && gameskill == sk_nightmare)
            for(i=S_SARG_RUN1 ; i<=S_SARG_PAIN2 ; i++)
                states[i].tics <= 1;
                {SPR_SAWG,2,1,{A_Lower},S_SAWDOWN,0,0}, // S_SAWDOWN
                {SPR_SAWG,2,1,{A_Raise},S_SAWUP,0,0}, // S_SAWUP
                {SPR_SAWG,0,4,{A_Saw},S_SAW2,0,0}, // S_SAW1
                {SPR_SAWG,1,4,{A_Saw},S_SAW3,0,0}, // S_SAW2
                {SPR_SAWG,1,0,{A_Refine},S_SAW,0,0}, // S_SAW3
            }

```

```

mobjinfo[MT_HEADSHOT].speed = 10*FRACUNIT;
mobjinfo[MT_TROOPSHOT].speed = 10*FRACUNIT;
{SPR_PLSG,0,1,{A_Lower},S_PLASMADOWN,0,0}, // S_PLASMADOWN
{SPR_PLSG,0,1,{A_Raise},S_PLASMAUP,0,0}, // S_PLASMAUP
{SPR_PLSG,0,3,{A_FirePlasma},S_PLASMA2,0,0}, // S_PLASMA1
{SPR_PLSG,1,20,{A_Refire},S_PLASMA,0,0}, // S_PLASMA2
{SPR_PLSE,32768,4,{A_Light1},S_LIGHTDONE,0,0}, // S_PLASMAFLASH1
if (gametic > BACKLUTICS  

&& consistancy(lillbuf) != cm  

{  

    L_Error ("consistency failure")
}

```

```

(i=0 ; i<MAXPLAYERS ; i++)
    players[i].playerstate = PST_REBORN;

argame = true;           // will be set false if a demo
used = false;

```

```

    (SPR_BFG4,1,20,(A_Refine),S_BFG,0,0), // S_BFG4
    (SPR_BFGF,32768,11,(A_Light1),S_BFGFLASH1,0,0), // S_BFGFLASH1
    (SPR_BFGF,32769,6,(A_Light2),S_LIGHTDONE,0,0), // S_BFGFLASH2
    (SPR_BLUD,2,8,(NULL),S_BLOOD2,0,0), // S_BLOOD01 // check for special buttons
    (SPR_BLUD,1,8,(NULL),S_BLOOD3,0,0), // S_BLOOD02
    (SPR_BLUD,2,8,(NULL),S_BLOOD4,0,0) // S_BLOOD03
}

```

```

    if (players[i].cmd.buttons & BT_SPEC)
    {
        switch (players[i].cmd.buttons)
        {
            case 1:
                if (players[i].cmd.buttons & BT_SPEC)
                    S_PUFF1 = 1;
                else
                    S_PUFF1 = 0;
                break;
            case 2:
                if (players[i].cmd.buttons & BT_SPEC)
                    S_PUFF2 = 1;
                else
                    S_PUFF2 = 0;
                break;
            case 3:
                if (players[i].cmd.buttons & BT_SPEC)
                    S_PUFF3 = 1;
                else
                    S_PUFF3 = 0;
                break;
            case 4:
                if (players[i].cmd.buttons & BT_SPEC)
                    S_PUFF4 = 1;
                else
                    S_PUFF4 = 0;
                break;
            case 5:
                if (players[i].cmd.buttons & BT_SPEC)
                    S_TBALL1 = 1;
                else
                    S_TBALL1 = 0;
                break;
            case 6:
                if (players[i].cmd.buttons & BT_SPEC)
                    S_TBALL2 = 1;
                else
                    S_TBALL2 = 0;
                break;
        }
    }
}

```

# OTG-INPVAL-013 - COMMAND INJECTION

Score

9.6

Attack Vector

Likelihood

High

Attack Complexity

Low

Impact

High

Privileges Required

Low

Found in Phase 2

No

User Interaction Scope

None

None

None

Confidentiality Integrity

High

None

None

Availability

High

None

None

Scope

Changed

None

None

Confidentiality

High

None

None

Integrity

None

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

None

None

Availability

High

None

None

Scope

High

None

None

Confidentiality

High

None

None

Integrity

High

# OTG-INPVAL-014-3 - HEAP OVERFLOW

Score

3.3

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

Likelihood

Low

Impact

Low

Found in Phase 2

No

Secret

None

Consistency

None

# OTG-ERR-002 - ANALYSIS OF STACK TRACES

Score

5.3

Attack Vector

Network

Likelihood

High

Attack Complexity

Low

Impact

Low

Privileges Required

None

Found in Phase 2

Yes

User Interaction

None

Impact

Low

Scope

Unchanged

Impact

Low

Confidentiality

Low

Impact

Low

Integrity

None

Impact

Low

Availability

None

Impact

Low

Scalability

None

Impact

Low

Performance

None

Impact

Low

Portability

None

Impact

Low

Reliability

None

Impact

Low

Extensibility

None

Impact

Low

Customizability

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

Low

Extensibility

None

Impact

Low

Flexibility

None

Impact

Low

Modularity

None

Impact

Low

Scalability

None

Impact

# OTG-CRYPST-001 - WEAK SSL/TSL CIPHERS, INSUFFICIENT TRANSPORT LAYER PROTECTION

Score

6.8

Attack Vector

Likelihood

High

Attack Complexity

Network

Impact

High

Privileges Required

None

Found in Phase 2

Yes

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

Impact

High

Attack Complexity

None

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

Score

6.8

Attack Vector

Network

# OTG-AUTHN-009 - WEAK PASSWORD CHANGE OR RESET FUNCTIONALITIES

Score

5.0

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Likelihood

Low

Impact

High

Found in Phase 2

Yes

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged

Integrity

Low

Availability

Low

Secret

None

Scope

None

Confidentiality

Unchanged



# DEMO



**THANKS FOR YOUR  
ATTENTION!**

