

# ADVENTURES IN DRUPAL SECURITY

JUNIOR TIDAL

WEB SERVICES & MULTIMEDIA LIBRARIAN

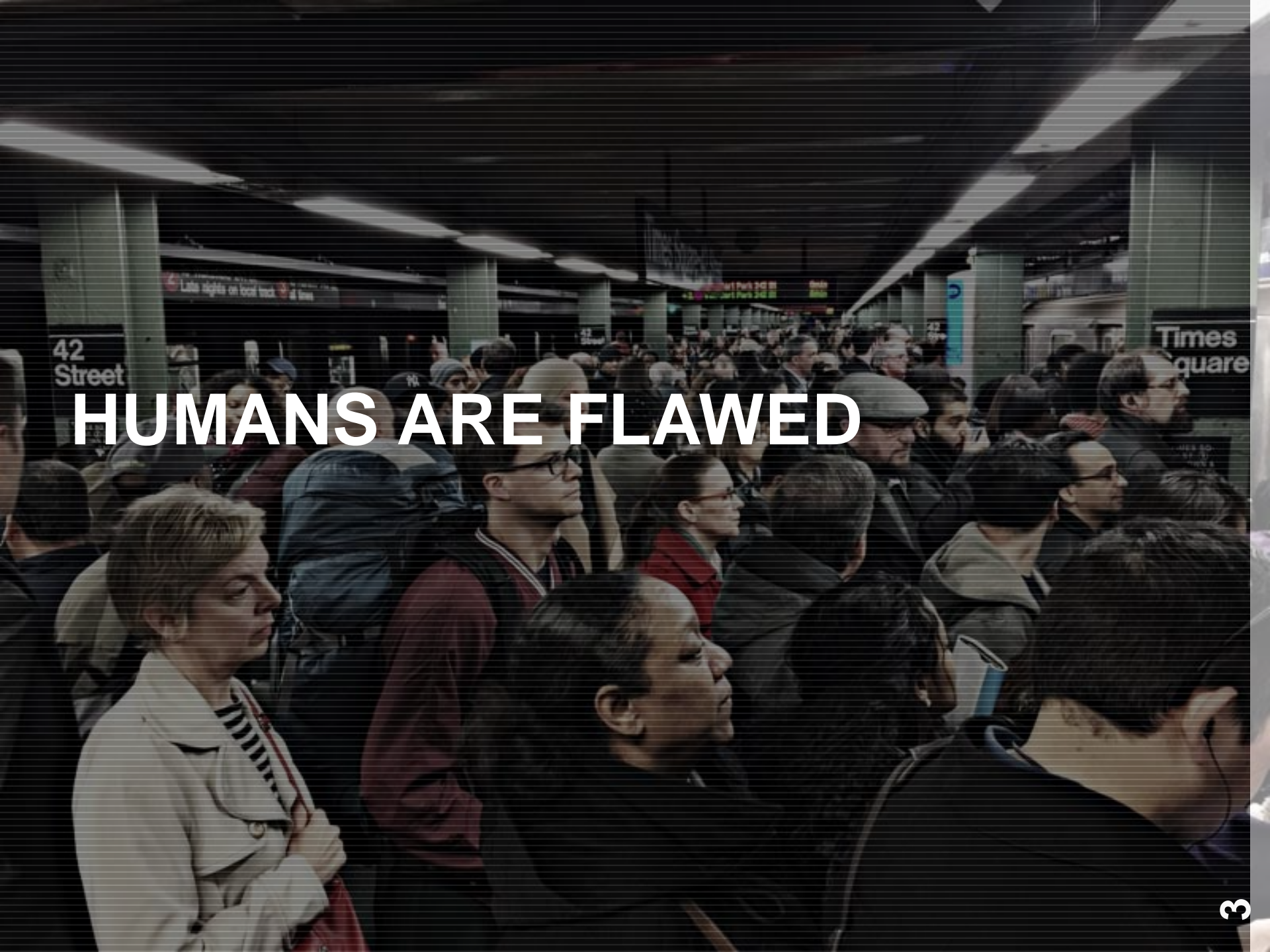
NEW YORK CITY COLLEGE OF TECHNOLOGY

@JUNIORTIDAL



# ORGANIZATIONAL INFORMATICS






**HUMANS ARE FLAWED**



# HUMANS CREATE SYSTEMS

A dark, atmospheric street scene at dusk or dawn. The sky is a deep, dark blue-grey, and several birds are silhouetted against it, flying in various directions. The street is lined with tall, multi-story buildings, their windows mostly dark. In the distance, a few lights from buildings and a vehicle are visible, creating a sense of depth and activity in the otherwise still scene. The overall mood is somber and contemplative.


**SYSTEMS ARE INHERENTLY  
FLAWED**

A dark, atmospheric street scene at dusk or dawn. The sky is a deep, dark blue-grey, and several birds are silhouetted against it, flying in various directions. The street is lined with tall, multi-story buildings, their windows mostly dark. In the distance, a few lights from a vehicle or streetlights are visible, creating a sense of depth and perspective. The overall mood is somber and mysterious.

**EVENTUALLY SYSTEMS FAIL**

**THERE IS NO PERFECT  
SYSTEM**





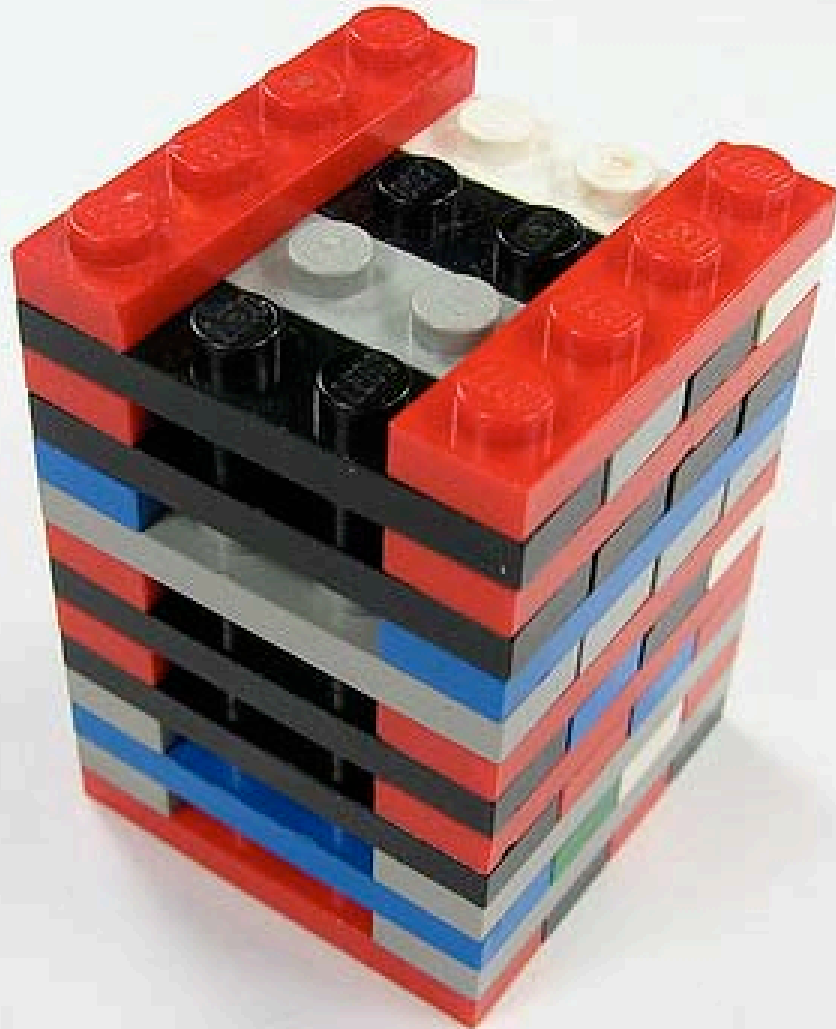
**THERE IS NO PERFECT  
SYSTEM**

**...SO DON'T TRY TO CREATE  
ONE.**



A close-up photograph of a smartphone with a severely cracked and shattered screen. The cracks are extensive, forming a spiderweb pattern across the entire surface. The phone is dark-colored, and the home button is visible on the left side. The background is dark and out of focus.

**SYSTEMS FAIL FROM  
INTERNAL AND EXTERNAL  
FACTORS**



**INSTEAD OF BUILDING A  
PERFECT SYSTEM**

A group of five LEGO minifigures are gathered around a table, appearing to be in a meeting. From left to right: a minifigure with white hair and a dark vest; a minifigure with a black hood and a dark vest; a minifigure wearing an orange hard hat and a white shirt with an orange scarf; a minifigure with a white and green patterned hood and an orange shirt; and a minifigure with white hair and a green vest, who is out of focus in the foreground. The background is a plain, light-colored wall.

**EMPHASIZE PREVENTIVE  
MAINTENANCE**

A series of images showing the assembly of a LEGO truck. The top right shows the completed truck from a front-three-quarter view. The bottom right shows the completed truck from a rear-three-quarter view. The bottom left shows the truck upside down, revealing the chassis. The middle left shows the truck's chassis with some components removed. The top left shows various sub-components and parts, including a blue motor, black frame, and red and black plastic pieces.

# CREATE RECOVERY STRATEGIES



**WHAT ARE WE TALKING  
ABOUT TODAY?**

**BACKGROUND**

**SECURITY COMPROMISED!**


**RECOVERY**

**LEARNING**


**SECURING YOUR SITE**

# BACKGROUND





**URSULA C. SCHWERIN  
LIBRARY SUPPORTS OVER  
17,000 STUDENTS OF THE  
NEW YORK CITY COLLEGE  
OF TECHNOLOGY  
(CITY TECH)**



**ONE OF THE 23 CAMPUSES  
OF THE CITY UNIVERSITY OF  
NEW YORK (CUNY)**



A large, multi-story building with a grid of windows, likely a school or university building, with a crest on the facade. The building is viewed from a low angle, looking up. The sky is overcast. There are traffic lights and a yellow sign in the foreground.

**CONSIDERED A  
“COMMUTER” SCHOOL**



**SERVES A DIVERSE  
POPULATION IN DOWNTOWN  
BROOKLYN**

# THE WEB SERVER





**MIGRATED FROM A  
MULTI-DEPARTMENTAL  
WINDOWS IIS SERVER TO A  
DEDICATED LAMP SERVER IN  
2008.**



**AD HOC SUPPORTED BY  
COLLEGE IT DEPARTMENT.**



**THE WEB SERVICES  
LIBRARIAN AND IT  
ASSOCIATE ARE ADMINS  
FOR THIS SERVER**

# DRUPAL

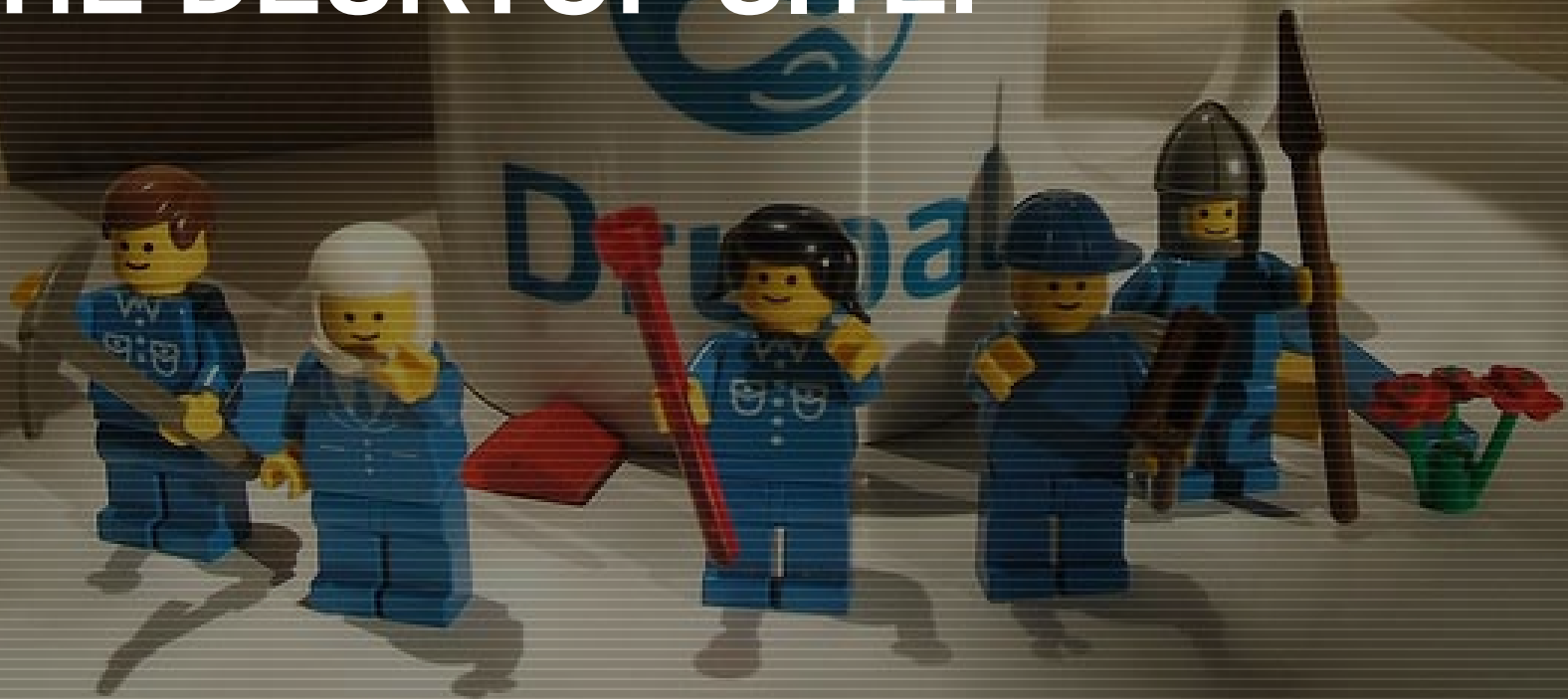


**DRUPAL IS THE CMS USED  
TO MANAGE SEPARATE  
DESKTOP AND MOBILE  
SITES.**





**DRUPAL 6 WAS USED FOR  
THE DESKTOP SITE.**



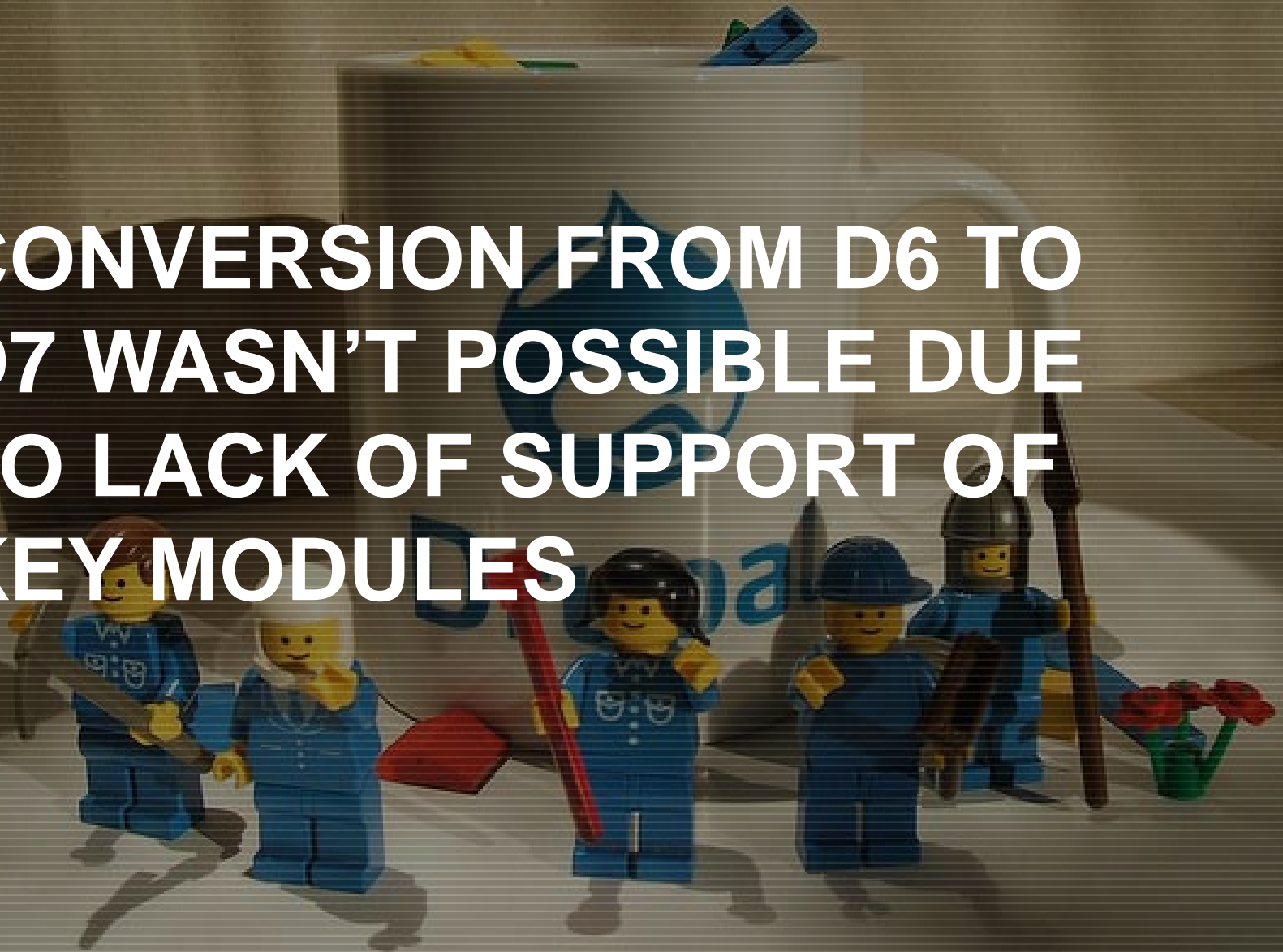
**USING ANALYTICS  
INFORMATION, THERE WAS A  
NEED TO SUPPORT MOBILE  
USERS.**



**DRUPAL 7 WAS USED TO  
CREATE A SEPARATE  
MOBILE SITE.**



**CONVERSION FROM D6 TO  
D7 WASN'T POSSIBLE DUE  
TO LACK OF SUPPORT OF  
KEY MODULES**



Find Books

# MOBILE SITE

Search by...

Go

Go

OneSearch

My Account

Find Articles

Find eBooks

Android Market Apps for Article Databases

iOS Apps (iPhone, iPad, & iPod) for Article Databases

Ask a Librarian

Directions

Fall Semester - 8/28/14 – 12/23/14

Monday through Thursday - 8:30 AM – 10:30 PM

Friday - 8:30 AM – 7:00 PM

Saturday - 9:00 AM – 5:00 PM

Sunday - Closed

Exceptions:

8/30, 9/1, 10/4, 10/13, and 11/27 - 11/29

Closed

9/23

8:30 AM - 7:00 PM

Find Books

Search by...

Go

# THE MOBILE SITE HAD A WIDGET TO SEARCH THE CATALOG

OneSearch

My Account

Find Articles

Find eBooks

Android Market Apps for Article Databases

iOS Apps (iPhone, iPad, & iPod) for Article Databases

Ask a Librarian

Directions

Fall Semester - 8/28/14 – 12/23/14

Monday through Thursday - 8:30 AM – 10:30 PM

Friday - 8:30 AM – 7:00 PM

Saturday - 9:00 AM – 5:00 PM

Sunday - Closed

Exceptions:

8/30, 9/1, 10/4, 10/13, and 11/27 - 11/29

Closed

9/23

8:30 AM - 7:00 PM

Find Books

Search by...

# LINKS TO MOBILE FRIENDLY ELECTRONIC RESOURCES

OneSearch

My Account

Find Articles

Find eBooks

Android Market Apps for Article Databases

iOS Apps (iPhone, iPad, & iPod) for Article Databases

Ask a Librarian

Directions

Fall Semester - 8/28/14 – 12/23/14

Monday through Thursday - 8:30 AM – 10:30 PM

Friday - 8:30 AM – 7:00 PM

Saturday - 9:00 AM – 5:00 PM

Sunday - Closed

Exceptions:

8/30, 9/1, 10/4, 10/13, and 11/27 - 11/29

Closed

9/23

8:30 AM - 7:00 PM

Find Books

Search by...

Go

# LIBRARY INFORMATION SUCH AS HOURS AND CONTACT WAS ALSO PROVIDED

OneSearch

My Account

Find Articles

Find eBooks

Android Market Apps for Article Databases

iOS Apps (iPhone, iPod, iPad) for Article Databases

Ask a Librarian

Directions

Fall Semester - 8/28/14 – 12/23/14

Monday through Thursday - 8:30 AM – 10:30 PM

Friday - 8:30 AM – 7:00 PM

Saturday - 9:00 AM – 5:00 PM

Sunday - Closed

Exceptions:

8/30, 9/1, 10/4, 10/13, and 11/27 - 11/29

Closed

9/23

8:30 AM - 7:00 PM



# SECURITY COMPROMISED!

**se·cu·ri·ty** /sɪˈkʊrəti/

cure condition

or guarantee

of a loan, etc.

**THE MOBILE SITE WAS  
HACKED ON DECEMBER 21<sup>ST</sup>,  
2014.**

**se·cu·ri·ty** /sɪˈkʊrɪti/

cure condition

or guarantee

of a loan, etc.

**THE BBC REPORTED A  
DRUPAL HACK ATTACK ON  
OCTOBER 31, 2014.**

# UNIVERSITY IT CONTACTED CAMPUS IT ABOUT THE BREACH

se·cu·ri·ty /sɪˈkʊrɪti/

cure condition

or guarantee

of a loan, etc.

# THE SITE WAS DEFACED AND THE HOMEPAGE REPLACED

se·cu·ri·ty /sɪˈkʊrɪti/

cure condition

or guarantee

of a loan, etc.

# IT DISCONNECTED THE LIBRARY'S SERVER

se·cu·ri·ty /sɪˈkʊrɪti/

cure condition

or guarantee

of a loan, etc.

# ATTACK ANALYSIS

```
private FragmentAbst(Context context) {  
    // Note that we call through to the version that has a parameter  
    // because the simple Context construct on null is deprecated  
    super(context, null);  
    mFragmentManager = new FragmentManager(context, null);  
}
```

```
private FragmentAbst(Context context, AttributeSet attrs) {  
    super(context, attrs);  
    mFragmentManager = new FragmentManager(context, attrs);  
}
```

```
...state] newArray(int size);  
return new SavedState[size];
```

**AFTER EXAMINING LOG  
FILES, THERE WASN'T ANY  
EVIDENCE OF  
UNAUTHORIZED USERS OR  
FILES**

```
...Context context, null);  
...Context context, AttributeSet attrs);  
...Context context, AttributeSet attrs);
```



# SEARCHING MYSQL TABLES FOUND NO MALICIOUS CODE

# THE BREACH WAS EITHER THE OUTDATED D7 CORE OR MODULE(S)

# THE MOBILE SITE WAS SHUT DOWN

```
state] newArray(int size);  
return new SavedState[size];
```

**UNTIL THE BETA SITE WAS  
READY, TRAFFIC WAS  
REDIRECTED TO THE  
DESKTOP SITE**

```
context.construct(context, null);  
context.construct(context, attrs);  
context.construct(context, attrs);
```

# LESSONS LEARNED



A photograph of a classroom with rows of wooden desks and chairs. A blackboard is visible in the background, and a door is on the right wall. The text "DON'T NEGLECT YOUR SITE" is overlaid in white, bold, sans-serif font across the center of the image.

**DON'T NEGLECT YOUR SITE**

A photograph of a classroom with rows of wooden desks and chairs. A blackboard is visible in the background, and a door is on the right wall. The text is overlaid in the center.

# USE DRUPAL'S EMAIL NOTIFICATIONS FOR NEW UPDATES

A photograph of a classroom with rows of wooden desks and chairs. A blackboard is visible in the background, and a door is on the right wall. The text "IMPLEMENT DRUPAL SECURITY MODULES" is overlaid in white, bold, sans-serif font in the center of the image.

# IMPLEMENT DRUPAL SECURITY MODULES





# DRUPAL SECURITY MODULES

# DRUPAL SECURITY KIT

# CAPTCHA

A photograph of a chain-link fence with a vine climbing it, set against a sunset background. The word 'CAPTCHA' is overlaid in white text.

A chain-link fence is the central focus, with a sunset and a cow visible through it. The text 'BACK UP AND MIGRATE' is overlaid in white, bold, sans-serif font.

# BACK UP AND MIGRATE

# AUTO LOGOUT

# LOGIN SECURITY



**DRUSH**



# STRATEGIES FOR A SECURITY BREACH






# CREATE RECOVERY GUIDELINES



# CREATE RECOVERY GUIDELINES



**TAKE YOUR SITE OFFLINE**

A dense field of keys of various colors and shapes against a dark background. The keys are scattered across the entire frame, creating a textured, almost abstract pattern. The colors range from light yellow and white to dark green and black. The keys are of various sizes and designs, some with intricate details and others that are more simple. The overall effect is one of a vast, chaotic collection of keys.

# MAKE A BACKUP OF YOUR HACKED SITE



**REPLACE A HACKED SITE  
WITH A BACKUP OR  
FAILOVER SITE**

A dense field of keys of various colors and shapes against a dark background. The keys are scattered across the entire frame, creating a complex, textured pattern. The colors range from light yellow and white to dark green and black. The keys are of various sizes and designs, some with intricate details and others more simple. The overall effect is a chaotic yet rhythmic arrangement of small, familiar objects.

**CHECK LOG FILES**

A dense field of keys in various colors (white, yellow, black) against a dark background. The keys are scattered across the entire frame, creating a textured, repetitive pattern. The lighting is dramatic, highlighting the metallic surfaces of the keys.

**NOTIFY ALL WHO NEED TO  
KNOW**

A dense field of many keys of various colors (white, yellow, green) against a dark background. The keys are scattered across the entire frame, creating a textured, repetitive pattern. The lighting is dramatic, highlighting the metallic surfaces of the keys.

# CHANGE PASSWORDS



A dense field of keys of various colors and shapes against a dark background. The keys are scattered across the entire frame, creating a complex, textured pattern. The colors range from light yellow and white to dark green and black. The shapes are diverse, including traditional notched keys, modern keys with circular heads, and keys with decorative elements like tassels or intricate cutouts. The overall effect is one of overwhelming variety and detail.

# DOCUMENT EVERYTHING

A server rack in a data center. The rack is filled with server units, and there are green lights visible on the front panel. The rack has blue handles on the front. The background is dark, and the overall scene is dimly lit.

# PREVENTIVE STRATEGIES AT THE SERVER LEVEL

A photograph of a server rack with blue handles and green indicator lights. The text "USE HTTPS (PORT 443)" is overlaid in white.

**USE HTTPS (PORT 443)**

# MANAGE FILE EXTENSIONS




# MANAGE PHP EXECUTION WITHIN YOUR UPLOADS FOLDER

# ROBOTS.TXT



# SECURE FILE PERMISSIONS



# MAKE AND AUTOMATE BACKUPS



# PREVENTIVE MAINTENANCE



**STRONG PASSWORDS**

# EVALUATE USER ROLES AND PERMISSIONS





**EXAMINE SUB DIRECTORIES  
FOR RANDOM FILES  
ESPECIALLY /FILES AND  
/UPLOADS**

The background of the slide is a close-up, slightly blurred image of many wrapped candies. The candies are wrapped in clear plastic with red and white patterns. Some of the wrappers have the word "SWEET" visible in red letters. The overall color palette is dominated by red, white, and clear plastic tones.

# WRAPPING UP

**SYSTEMS FAIL**

**BACKGROUND OF CITY TECH**

**SECURITY COMPROMISED!**

**RECOVERY**

**LEARNING FROM THE  
COMPROMISE**

**SECURING YOUR DRUPAL SITE**

# RESOURCES

[DRUPAL'S SECURITY ADVISORIES](#)

[YOUR SITE GOT HACKED. NOW WHAT?](#)

[SEC4LIB LISTSERV](#)

THANKS!