CODE CAMP'18

17 November 2018 | FON University, Skopje

OUR PARTNERS

PLATINUM

MCA

GOLD

seavus HASELT endava FON FIRST PRIVATE UNIVERSITY netcetera

SILVER

itLabs SINGULAR ALLOCATE It all starts with a NESCAFÉ

BRONZE

INSCALE EmitKnowledge Researching frequencies BRAINSTER SEAVUS EDUCATION *and* DEVELOPMENT CENTER

nebb ART OF CATERING

MEDIA PARTNER

IT.mk

SUPPORTING PARTNERS

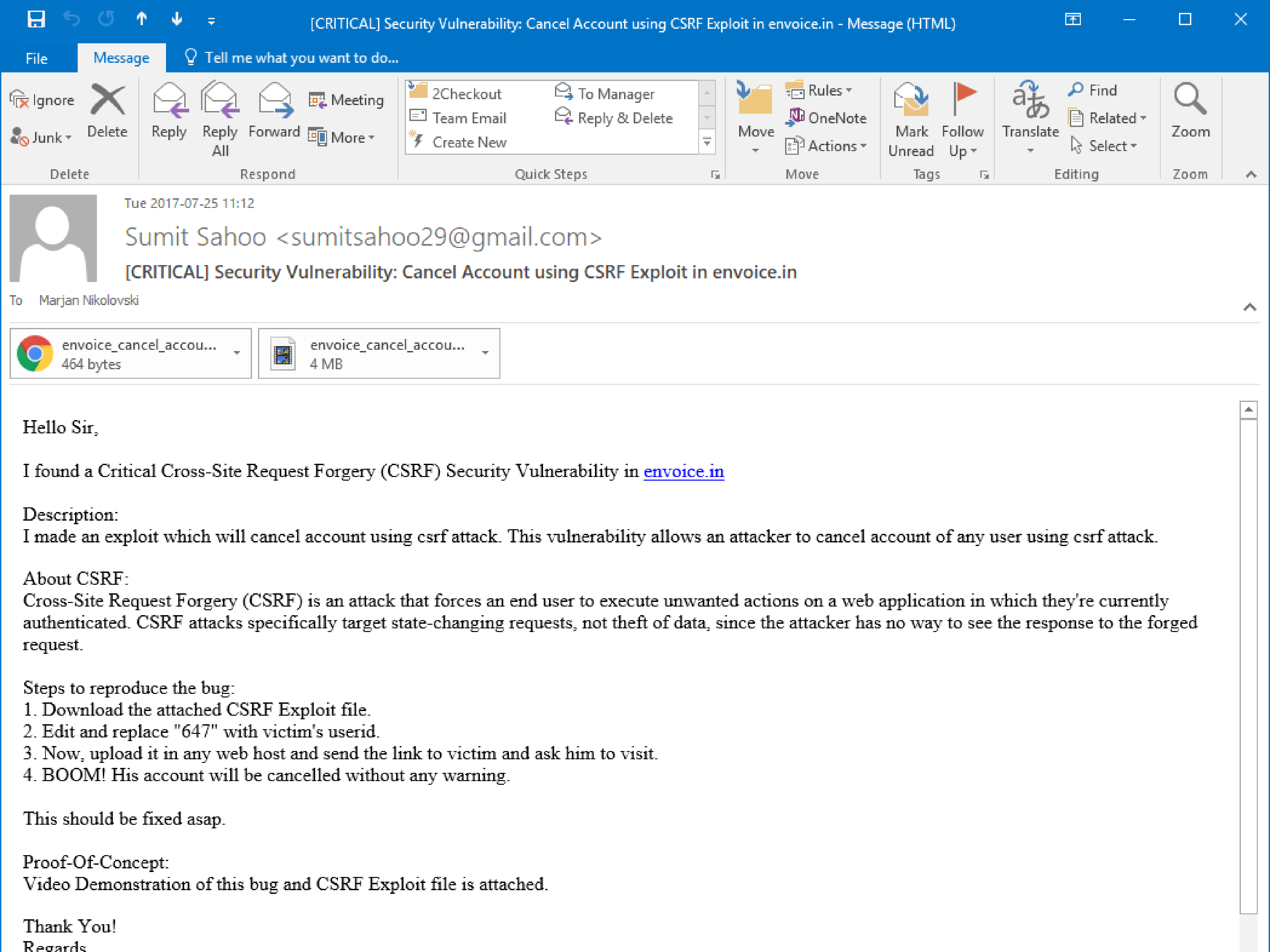
Swarmtix ANHOCH CALL FOR PAPERS POWERED BY sessionize.com

Ве молиме исклучете ги мобилните уреди

Please turn off your mobile devices

Securing your web application,

Why you will get hacked and other stories from the hood



Tue 2017-07-25 11:12

Sumit Sahoo <sumitsahoo29@gmail.com>

[CRITICAL] Security Vulnerability: Cancel Account using CSRF Exploit in envoice.in

To Marjan Nikolovski

envoice_cancel_accou... 464 bytes

envoice_cancel_accou... 4 MB

Hello Sir,

I found a Critical Cross-Site Request Forgery (CSRF) Security Vulnerability in envoice.in

Description:
I made an exploit which will cancel account using csrf attack. This vulnerability allows an attacker to cancel account of any user using csrf attack.

About CSRF:
Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.

Steps to reproduce the bug:
1. Download the attached CSRF Exploit file.
2. Edit and replace "647" with victim's userid.
3. Now, upload it in any web host and send the link to victim and ask him to visit.
4. BOOM! His account will be cancelled without any warning.

This should be fixed asap.

Proof-Of-Concept:
Video Demonstration of this bug and CSRF Exploit file is attached.

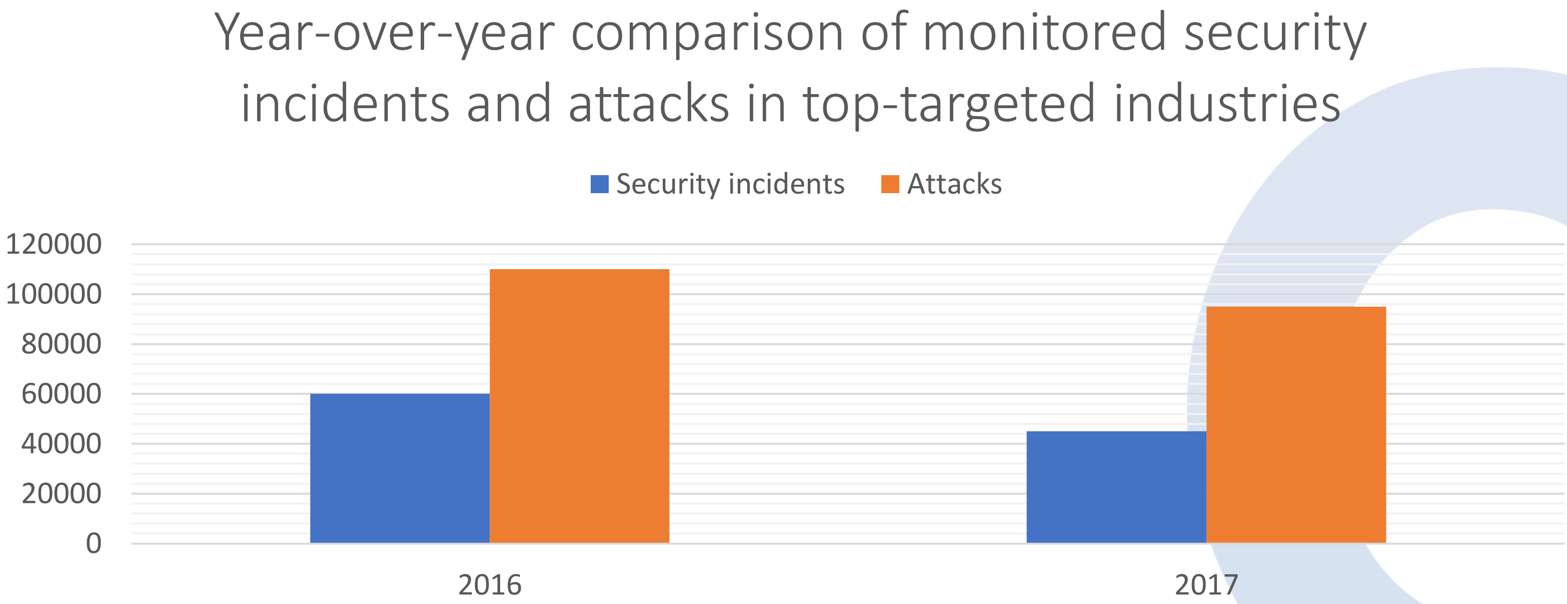
Thank You!
Regards

Agenda

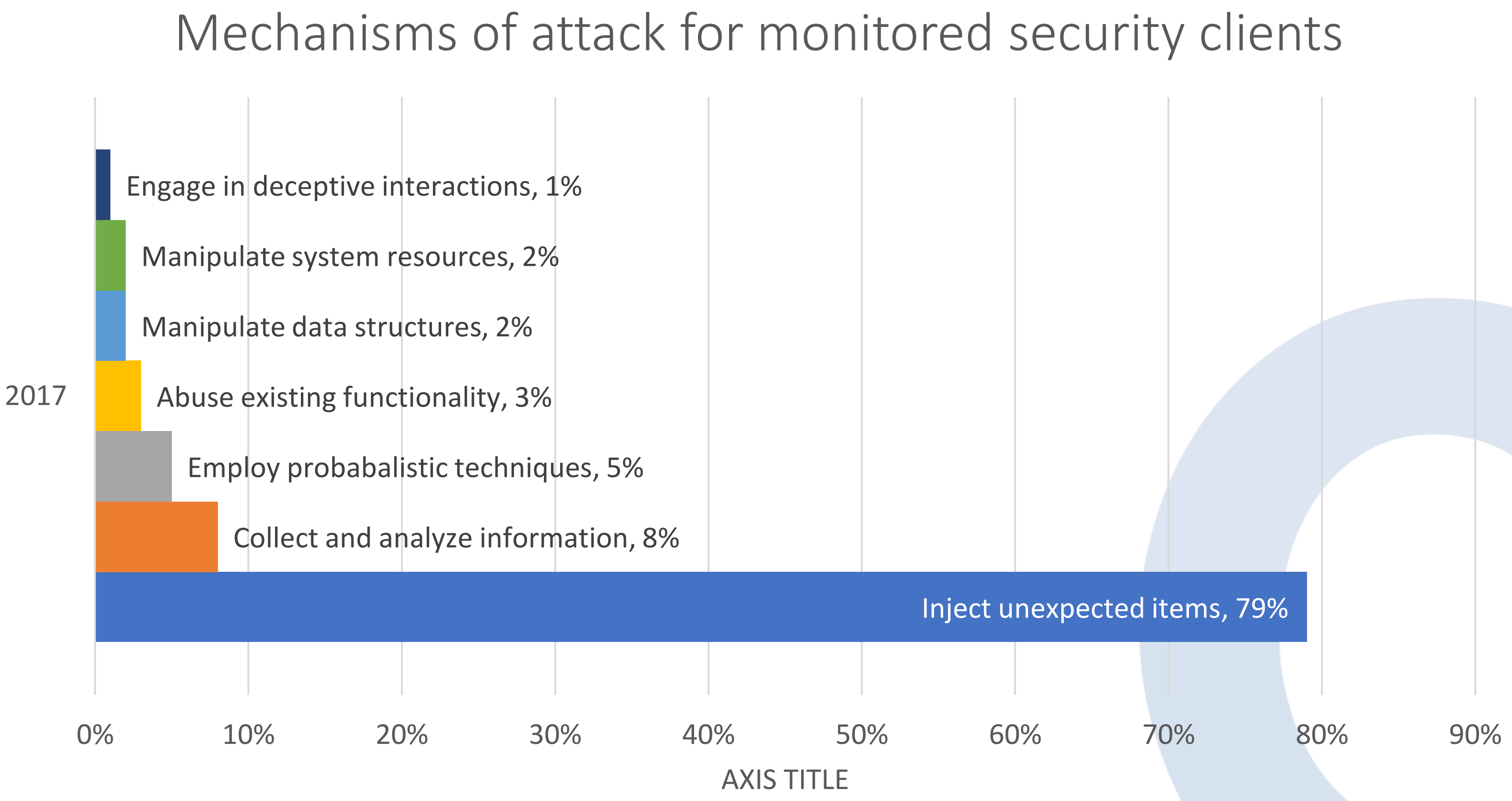
- Intro;
- OWASP Application Security Risks;
- Prevention;
- Outro and questions;

Security incidents and attacks

- A large majority of monitored security events are benign.



Network attack vectors

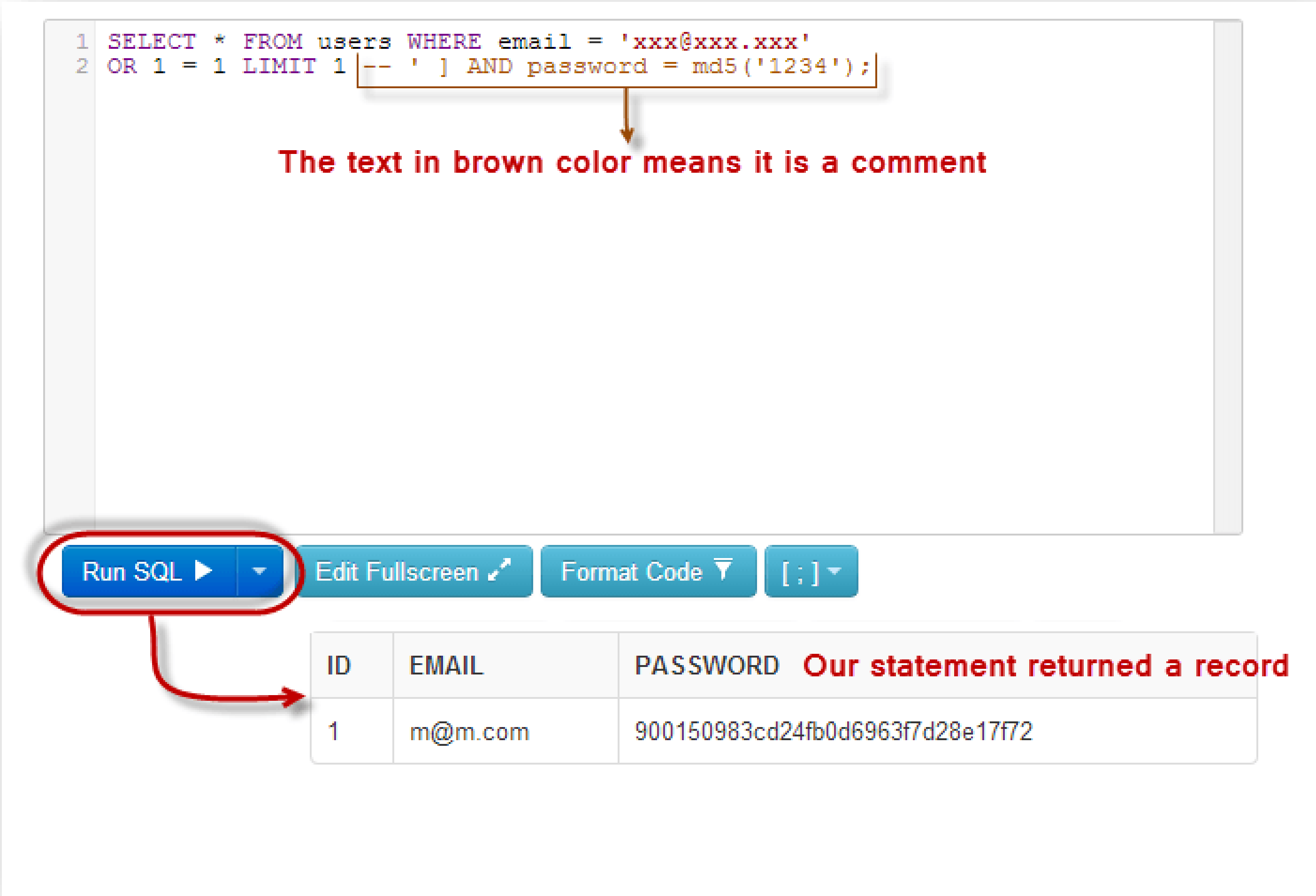


OWASP Application Security Risks

- Injection;
- Sensitive Data Exposure;
- Broken Authentication;
- Broken Access Control;
- Cross-Site Scripting (XSS);
- IDOR - Insecure Direct Object Reference;
- Security Misconfiguration;
- Using Components with Known Vulnerabilities;
- Insufficient Logging and Monitoring;

Injection

- Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.



```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx'
OR 1 = 1 LIMIT 1 -- ' ] AND password = md5('1234');
```

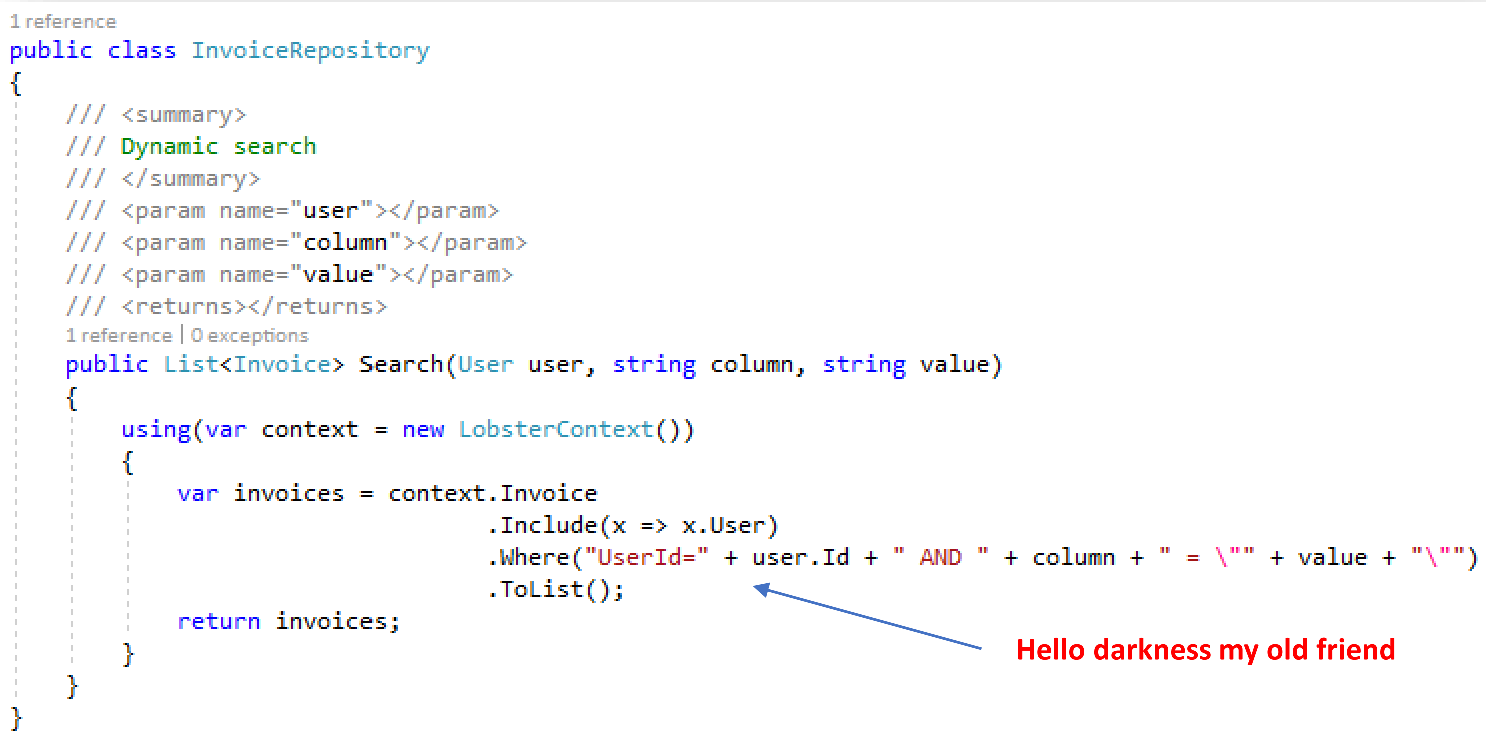
The text in brown color means it is a comment

Our statement returned a record

ID	EMAIL	PASSWORD
1	m@m.com	900150983cd24fb0d6963f7d28e17f72

Are We Safe!?

- Using Object-Relational Mapping (ORM) framework is a good way to defend against SQL injection, but is it enough?
  - Entity Framework;
  - Dapper;
- How about Dynamic LINQ? – In the search for a seamless solution to avoiding manual work we tend to create algorithms that are prone to injection:
  - Dynamic filtering;
  - Dynamic results/columns;
  - Dynamic ordering;
  - Generic search functions;
  - Generic stored procedures;
  - Query expansion and rewriting;



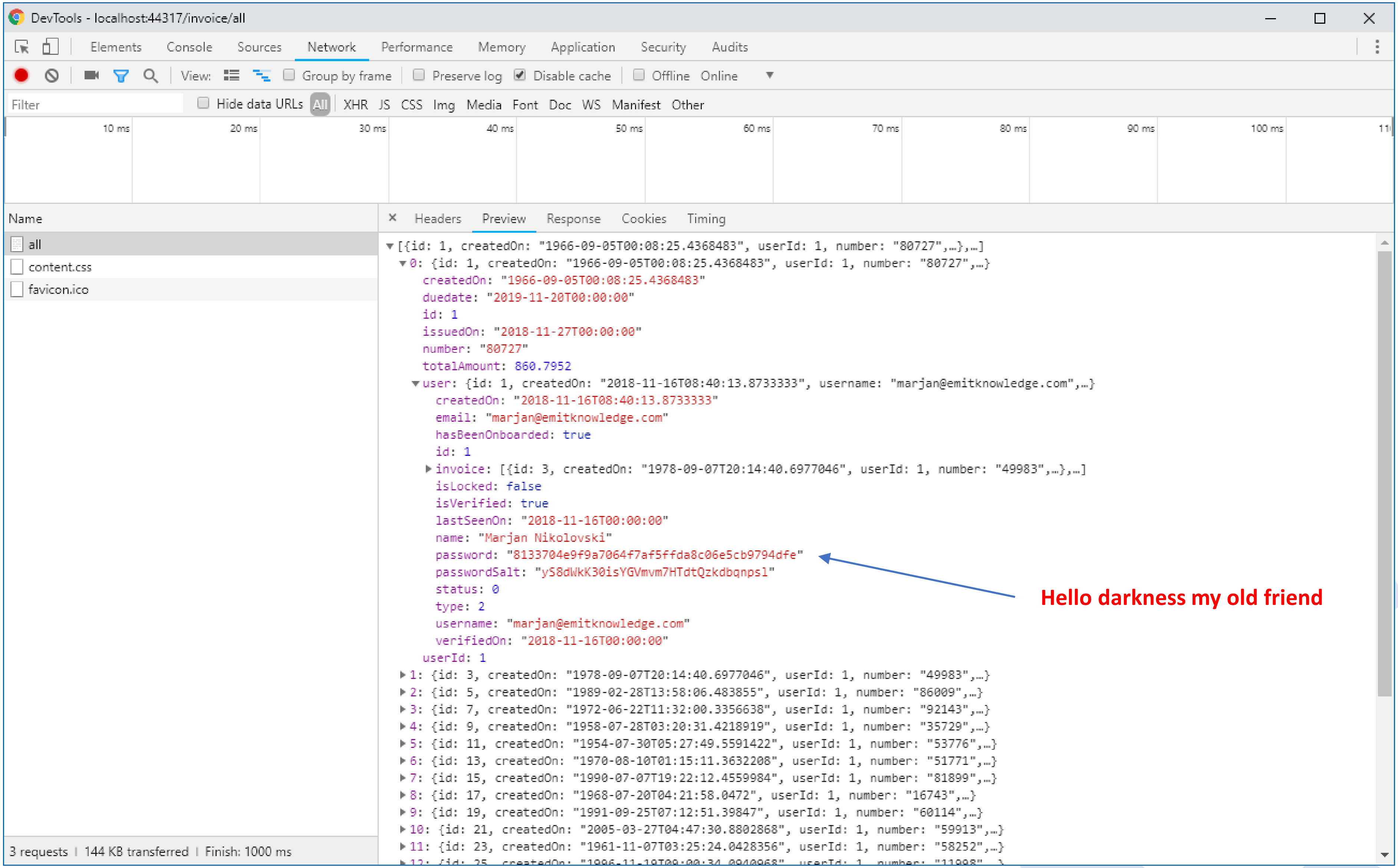
```
1 reference
public class InvoiceRepository
{
    /// <summary>
    /// Dynamic search
    /// </summary>
    /// <param name="user"></param>
    /// <param name="column"></param>
    /// <param name="value"></param>
    /// <returns></returns>
    1 reference | 0 exceptions
    public List<Invoice> Search(User user, string column, string value)
    {
        using(var context = new LobsterContext())
        {
            var invoices = context.Invoice
                                  .Include(x => x.User)
                                  .Where("UserId=" + user.Id + " AND " + column + " = \"" + value + "\"")
                                  .ToList();
            return invoices;
        }
    }
}
```

Hello darkness my old friend

Demo – Loading please wait

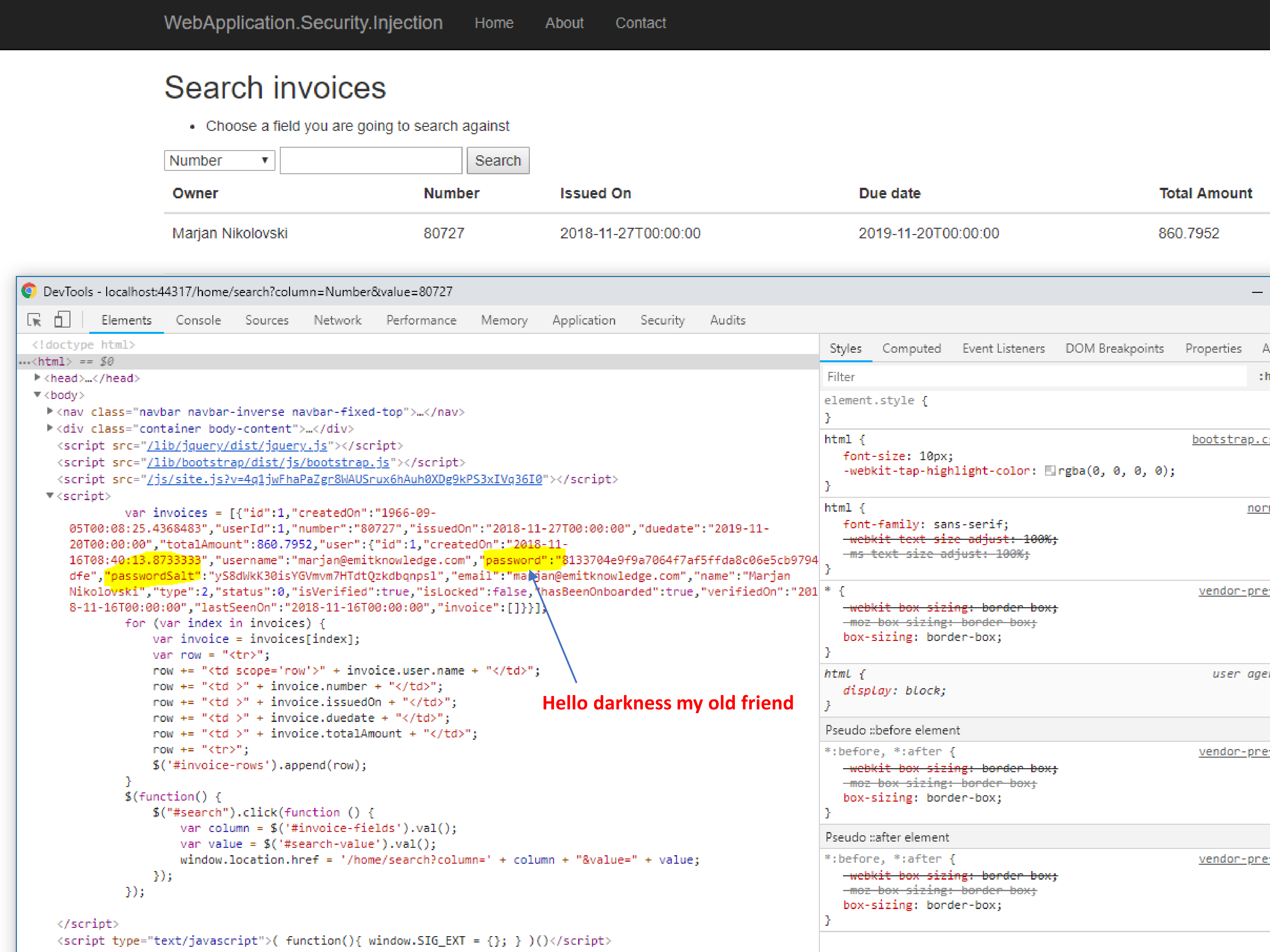
Sensitive Data Exposure

- Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.



```
▼[{id: 1, createdOn: "1966-09-05T00:08:25.4368483", userId: 1, number: "80727",…},…]
  ▼0: {id: 1, createdOn: "1966-09-05T00:08:25.4368483", userId: 1, number: "80727",…}
     createdOn: "1966-09-05T00:08:25.4368483"
     duedate: "2019-11-20T00:00:00"
     id: 1
     issuedOn: "2018-11-27T00:00:00"
     number: "80727"
     totalAmount: 860.7952
    ▼user: {id: 1, createdOn: "2018-11-16T08:40:13.8733333", username: "marjan@emitknowledge.com",…}
       createdOn: "2018-11-16T08:40:13.8733333"
       email: "marjan@emitknowledge.com"
       hasBeenOnboarded: true
       id: 1
      ▶invoice: [{id: 3, createdOn: "1978-09-07T20:14:40.6977046", userId: 1, number: "49983",…},…]
       isLocked: false
       isVerified: true
       lastSeenOn: "2018-11-16T00:00:00"
       name: "Marjan Nikolovski"
       password: "8133704e9f9a7064f7af5ffda8c06e5cb9794dfe"
       passwordSalt: "yS8dWkK30isYGVmvm7HTdtQzkdbqnpsl"
       status: 0
       type: 2
       username: "marjan@emitknowledge.com"
       verifiedOn: "2018-11-16T00:00:00"
     userId: 1
  ▶1: {id: 3, createdOn: "1978-09-07T20:14:40.6977046", userId: 1, number: "49983",…}
  ▶2: {id: 5, createdOn: "1989-02-28T13:58:06.483855", userId: 1, number: "86009",…}
  ▶3: {id: 7, createdOn: "1972-06-22T11:32:00.3356638", userId: 1, number: "92143",…}
  ▶4: {id: 9, createdOn: "1958-07-28T03:20:31.4218919", userId: 1, number: "35729",…}
  ▶5: {id: 11, createdOn: "1954-07-30T05:27:49.5591422", userId: 1, number: "53776",…}
  ▶6: {id: 13, createdOn: "1970-08-10T01:15:11.3632208", userId: 1, number: "51771",…}
  ▶7: {id: 15, createdOn: "1990-07-07T19:22:12.4559984", userId: 1, number: "81899",…}
  ▶8: {id: 17, createdOn: "1968-07-20T04:21:58.0472", userId: 1, number: "16743",…}
  ▶9: {id: 19, createdOn: "1991-09-25T07:12:51.39847", userId: 1, number: "60114",…}
  ▶10: {id: 21, createdOn: "2005-03-27T04:47:30.8802868", userId: 1, number: "59913",…}
  ▶11: {id: 23, createdOn: "1961-11-07T03:25:24.0428356", userId: 1, number: "58252",…}
  ▶12: {id: 25, createdOn: "1996-11-19T09:00:34.0940968", userId: 1, number: "11998",…}
```

Hello darkness my old friend



Search invoices

- Choose a field you are going to search against

Owner	Number	Issued On	Due date	Total Amount
Marjan Nikolovski	80727	2018-11-27T00:00:00	2019-11-20T00:00:00	860.7952

```
<!doctype html>
…<html> == $0
  ▶<head>…</head>
  ▼<body>
    ▶<nav class="navbar navbar-inverse navbar-fixed-top">…</nav>
    ▶<div class="container body-content">…</div>
     <script src="/lib/jquery/dist/jquery.js"></script>
     <script src="/lib/bootstrap/dist/js/bootstrap.js"></script>
     <script src="/js/site.js?v=4q1jwFhaPaZgr8WAUSrux6hAuh0XDg9kPS3xIVq36I0"></script>
    ▼<script>
             var invoices = [{"id":1,"createdOn":"1966-09-
       05T00:08:25.4368483","userId":1,"number":"80727","issuedOn":"2018-11-27T00:00:00","duedate":"2019-11-
       20T00:00:00","totalAmount":860.7952,"user":{"id":1,"createdOn":"2018-11-
       16T08:40:13.8733333","username":"marjan@emitknowledge.com","password":"8133704e9f9a7064f7af5ffda8c06e5cb9794
       dfe","passwordSalt":"yS8dWkK30isYGVmvm7HTdtQzkdbqnpsl","email":"marjan@emitknowledge.com","name":"Marjan
       Nikolovski","type":2,"status":0,"isVerified":true,"isLocked":false,"hasBeenOnboarded":true,"verifiedOn":"201
       8-11-16T00:00:00","lastSeenOn":"2018-11-16T00:00:00","invoice":[]}}];
             for (var index in invoices) {
                 var invoice = invoices[index];
                 var row = "<tr>";
                 row += "<td scope='row'>" + invoice.user.name + "</td>";
                 row += "<td >" + invoice.number + "</td>";
                 row += "<td >" + invoice.issuedOn + "</td>";
                 row += "<td >" + invoice.duedate + "</td>";
                 row += "<td >" + invoice.totalAmount + "</td>";
                 row += "<tr>";
                 $('#invoice-rows').append(row);
             }
             $(function() {
                 $("#search").click(function () {
                     var column = $('#invoice-fields').val();
                     var value = $('#search-value').val();
                     window.location.href = '/home/search?column=' + column + "&value=" + value;
                 });
             });

     </script>
     <script type="text/javascript">( function(){ window.SIG_EXT = {}; } )()</script>
```

Hello darkness my old friend

```
element.style {
}
html {                                         bootstrap.c
   font-size: 10px;
   -webkit-tap-highlight-color: rgba(0, 0, 0, 0);
}
html {                                         nor
   font-family: sans-serif;
   ~~-webkit-text-size-adjust: 100%;~~
   ~~-ms-text-size-adjust: 100%;~~
}
* {                                            vendor-pre
   ~~-webkit-box-sizing: border-box;~~
   ~~-moz-box-sizing: border-box;~~
   box-sizing: border-box;
}
html {                                         user age
   display: block;
}
Pseudo ::before element
*:before, *:after {                            vendor-pre
   ~~-webkit-box-sizing: border-box;~~
   ~~-moz-box-sizing: border-box;~~
   box-sizing: border-box;
}
Pseudo ::after element
*:before, *:after {                            vendor-pre
   ~~-webkit-box-sizing: border-box;~~
   ~~-moz-box-sizing: border-box;~~
   box-sizing: border-box;
}
```

Demo – Loading please wait

Broken Authentication

- Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

Common scenarios

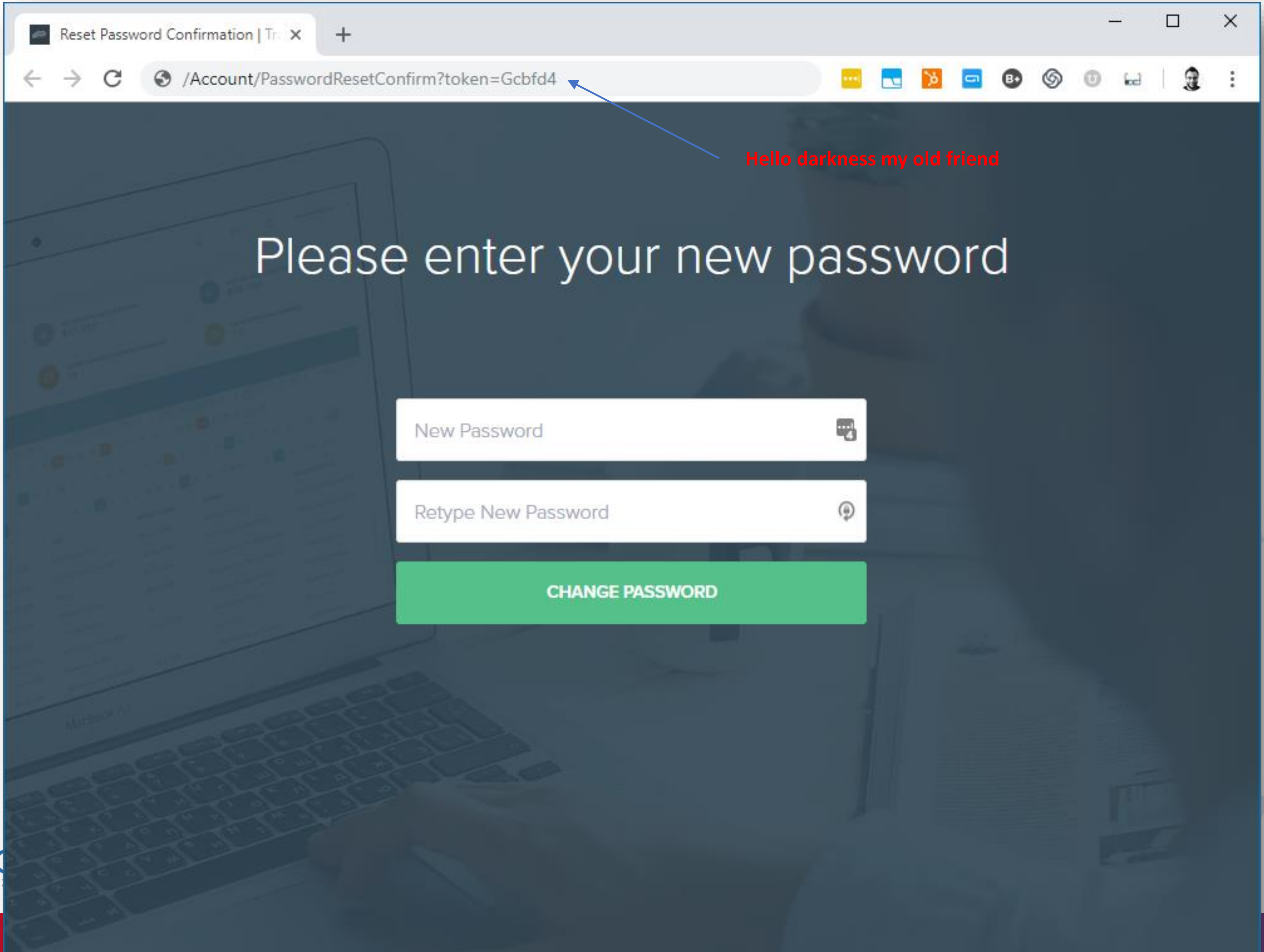
@Case

The guy from the marketing department asks the product owner to change the ugly password reset URL. It looks like it is bloated and non-user friendly.

The product owner brings this on the table and want to have this for yesterday. The team agrees that reducing the size from 128 to 6 chars is a matter of a second.

____

- Keep an eye when issuing tokens for scenarios such as:
  - New user registered token;
  - Password reset token;
  - Token protected resources;
- Make sure you check
  - Token length – should be prone to brute force. Use dynamic length tokens with size > 32
  - Specify token validity in days;



Reset Password Confirmation | Tr
/Account/PasswordResetConfirm?token=Gcbfd4

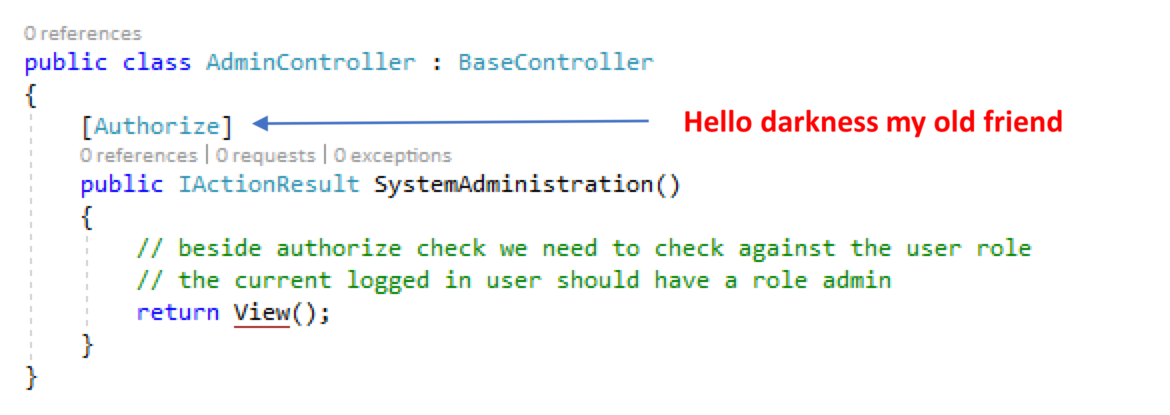
Hello darkness my old friend

Please enter your new password
New Password
Retype New Password
CHANGE PASSWORD

Demo – Loading please wait

Broken Access Control

- Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.



```
0 references
public class AdminController : BaseController
{
    [Authorize]
    0 references | 0 requests | 0 exceptions
    public IActionResult SystemAdministration()
    {
        // beside authorize check we need to check against the user role
        // the current logged in user should have a role admin
        return View();
    }
}
```

Hello darkness my old friend

Demo – Loading please wait

Cross-Site Scripting (XSS)

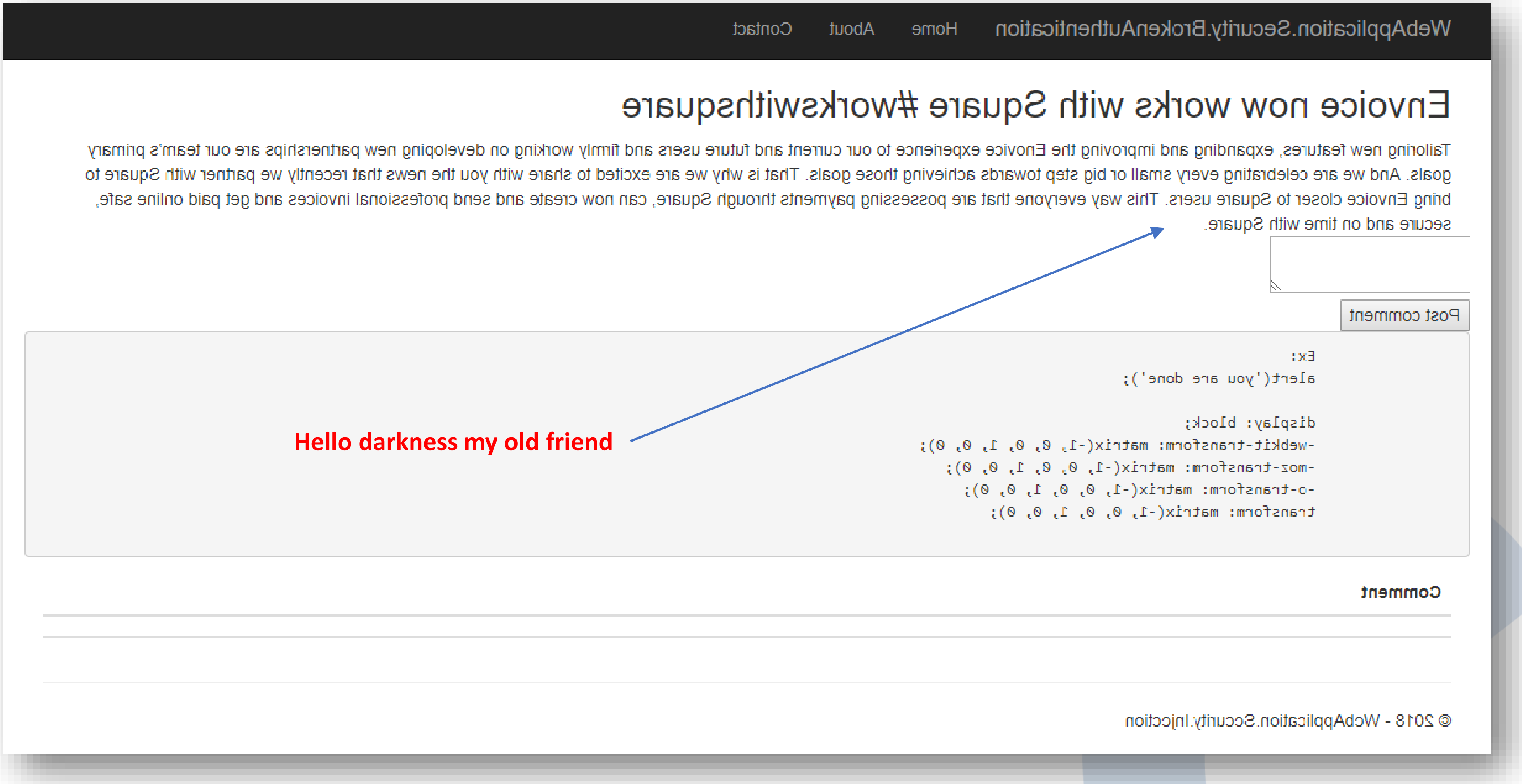
- XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Common scenarios

@Case

The QA guy reports you a bug that & is rendered as &amp; You think about it, hey this is easy-peasy let’s just use Html.Raw – YOLO!

- Keep an eye when playing around with raw data:
  - Sanitize using AntiXSS as default encode;
  - Never ever trust the incoming data;
  - Whitelist what type of tags you support by default;



Envoice now works with Square #workswithsquare

Tailoring new features, expanding and improving the Envoice experience to our current and future users and firmly working on developing new partnerships are our team's primary goals. And we are celebrating every small or big step towards achieving those goals. That is why we are excited to share with you the news that recently we partner with Square to bring Envoice closer to Square users. This way everyone that are possessing payments through Square, can now create and send professional invoices and get paid online safe, secure and on time with Square.

```
Ex:
alert('you are done');

display: block;
-webkit-transform: matrix(-1, 0, 0, 1, 0, 0);
-moz-transform: matrix(-1, 0, 0, 1, 0, 0);
-o-transform: matrix(-1, 0, 0, 1, 0, 0);
transform: matrix(-1, 0, 0, 1, 0, 0);
```

Comment

© 2018 - WebApplication.Security.Injection

Hello darkness my old friend

Demo – Loading please wait

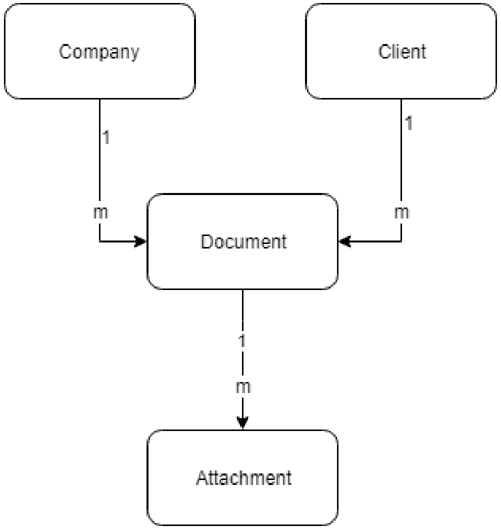
Insecure Direct Object Reference

- There can be many variables in the application such as “id”, “pid”, “uid”. Although these values are often seen as HTTP parameters, they can be found in headers and cookies. The attacker can access, edit or delete any of other users’ objects by changing the values. This vulnerability is called IDOR.

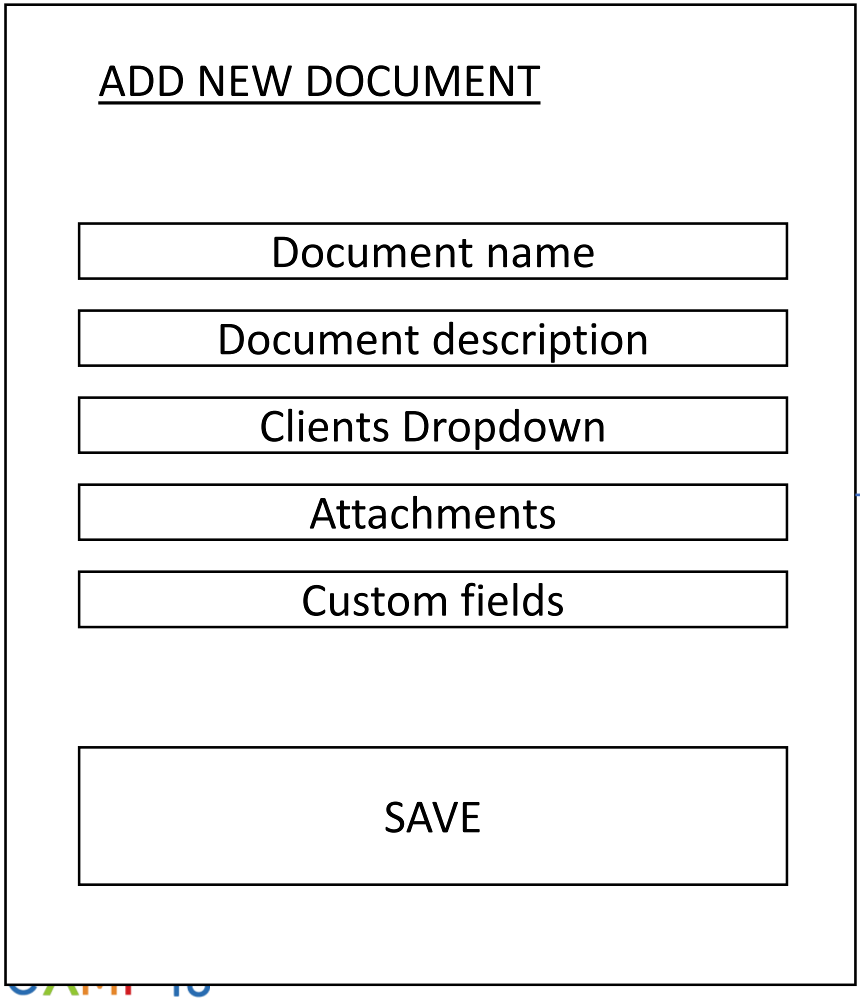
Common scenarios

@Case

We have a multi tenant system for document management.
Each document is associated with a customer.
Each document is associated with additional attachments.
Each document is associated with a company.



Add new document



ADD NEW DOCUMENT

Document name

Document description

Clients Dropdown

Attachments

Custom fields

SAVE

```
{
        Name: "Document 1",
        Description: “Tools for DEV",
        ClientId: 1,
        Attachments: [{
                Name: “finance.PDF”
                Url:
“https://data.com/finance.pdf”
        }]
}
```

Add new document

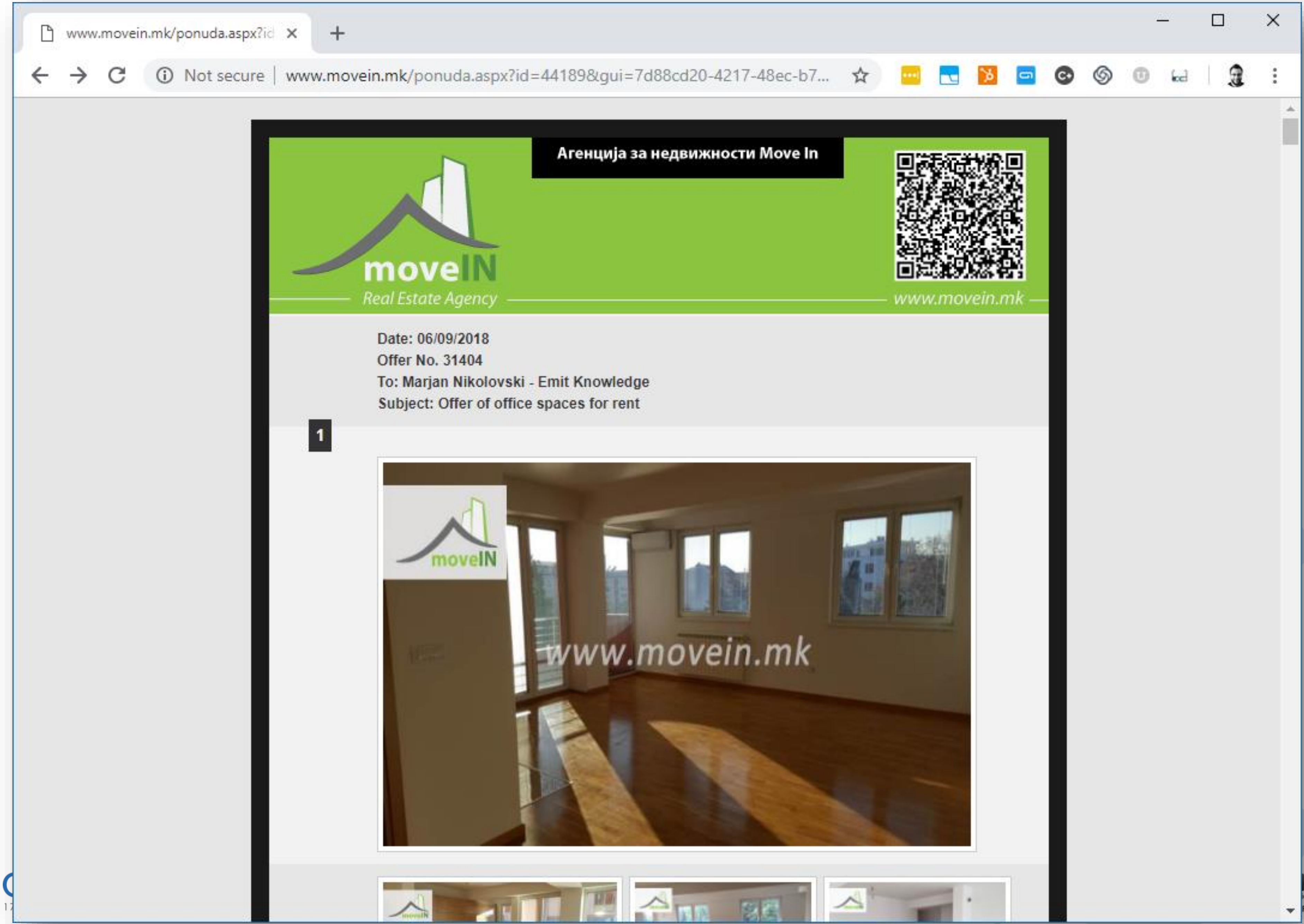
1. Check if the user is authenticated;
2. Check if the user has access to create a document;
3. Check if the user subscription is active;
4. Check if “Title”, “Client” and “Attachments” are provider;
5. Save the document in database;
6. Notify the administrator that there is a new document for review;

Hello darkness my old friend

IDOR Attack

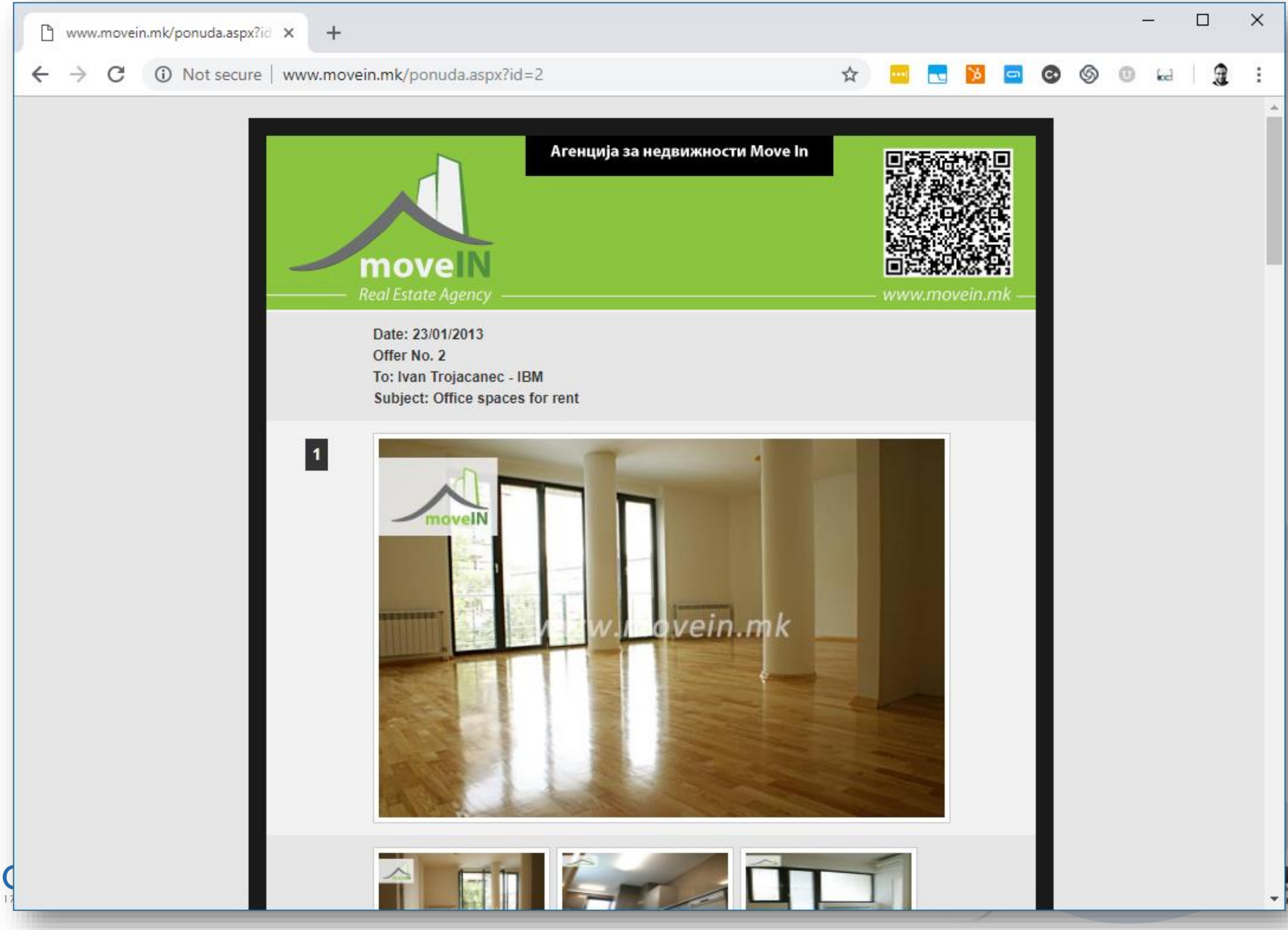
1. Create a new document as an attacker;
2. Save the new document;
3. Open the document for edit;
4. Add any random “Client Id” and “Attachment Id”;
5. Save the changes;
6. Click view document;
    1. The validation checks if the attacker is the owner of the document – which is true;
7. Access other account client and attachment information;

Hello darkness my old friend


www.movein.mk/ponuda.aspx?id
Not secure
www.movein.mk/ponuda.aspx?id=44189&gui=7d88cd20-4217-48ec-b7...
moveIN
Real Estate Agency
www.movein.mk
1
moveIN
www.movein.mk

Агенција за недвижности Move In

Date: 06/09/2018
Offer No. 31404
To: Marjan Nikolovski - Emit Knowledge
Subject: Offer of office spaces for rent



Агенција за недвижности Move In

moveIN

Real Estate Agency

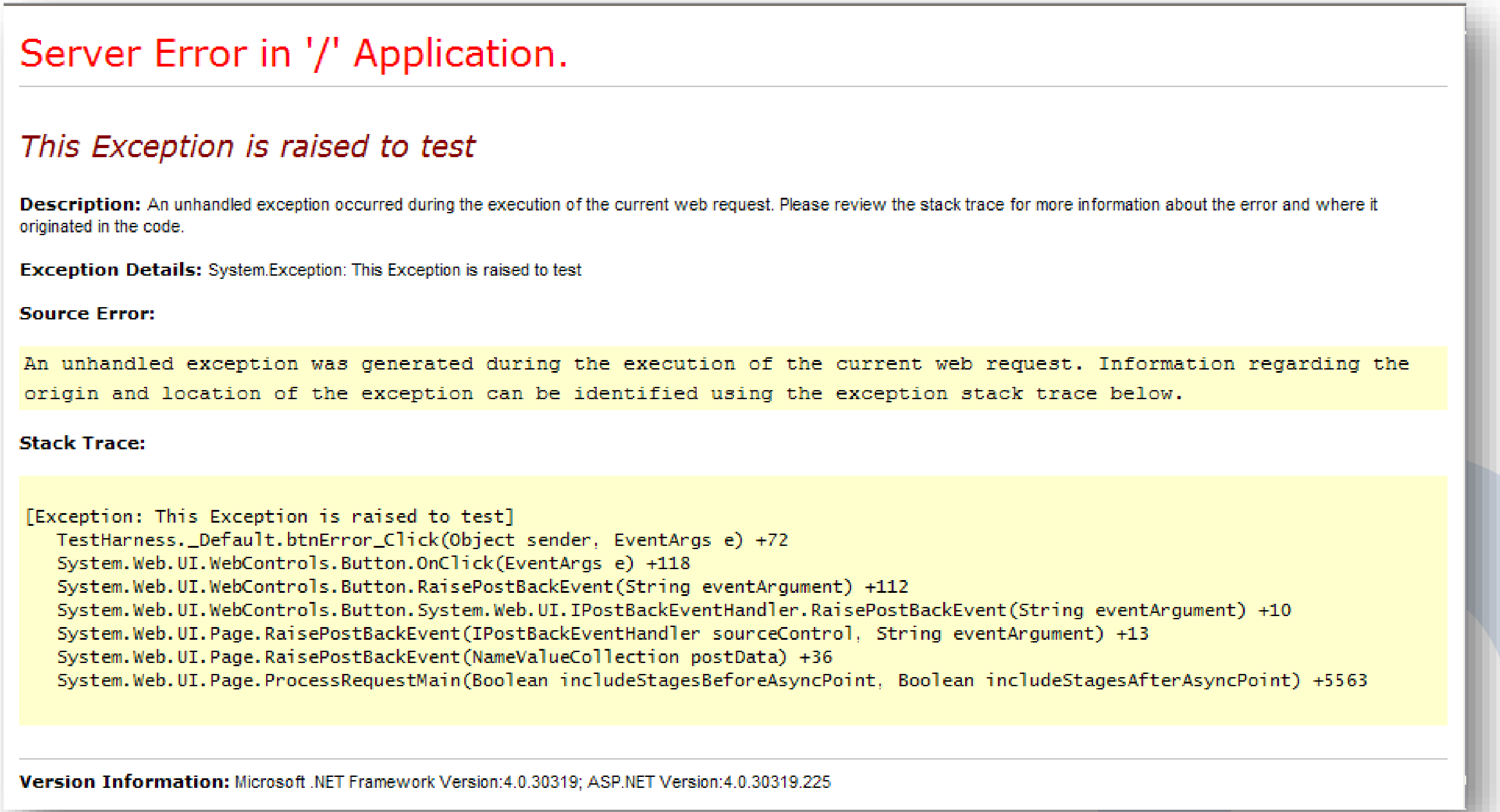
www.movein.mk

Date: 23/01/2013
Offer No. 2
To: Ivan Trojacanec - IBM
Subject: Office spaces for rent

1

Security Misconfiguration

- Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.



Server Error in '/' Application.

This Exception is raised to test

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Exception: This Exception is raised to test

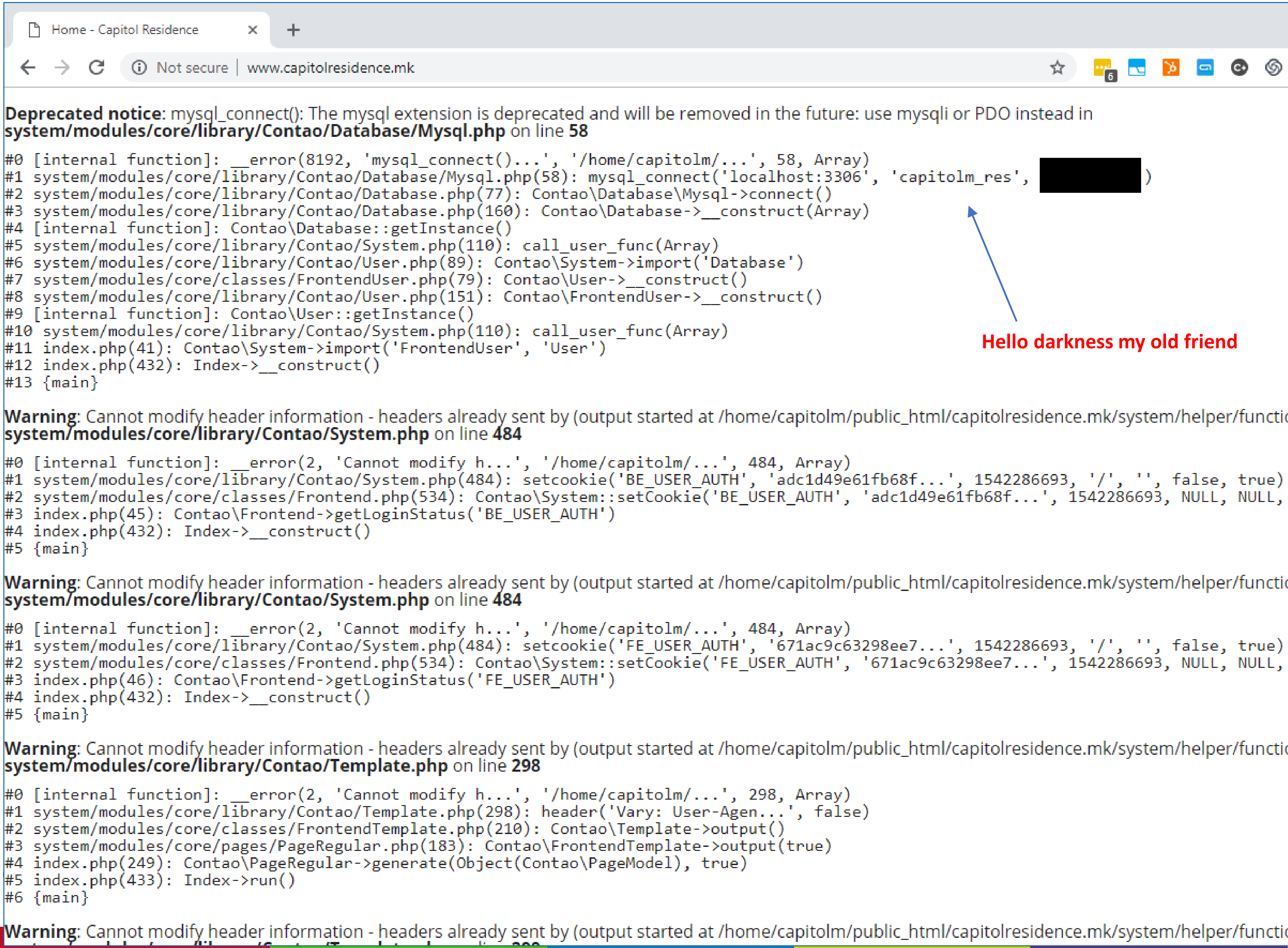
Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the
origin and location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[Exception: This Exception is raised to test]
   TestHarness._Default.btnError_Click(Object sender, EventArgs e) +72
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +118
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +112
   System.Web.UI.WebControls.Button.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument) +10
   System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +13
   System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData) +36
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5563
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.225



Deprecated notice: mysql_connect(): The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead in **system/modules/core/library/Contao/Database/Mysql.php** on line **58**

```
#0 [internal function]: __error(8192, 'mysql_connect()...', '/home/capitolm/...', 58, Array)
#1 system/modules/core/library/Contao/Database/Mysql.php(58): mysql_connect('localhost:3306', 'capitolm_res', [redacted])
#2 system/modules/core/library/Contao/Database.php(77): Contao\Database\Mysql->connect()
#3 system/modules/core/library/Contao/Database.php(160): Contao\Database->__construct(Array)
#4 [internal function]: Contao\Database::getInstance()
#5 system/modules/core/library/Contao/System.php(110): call_user_func(Array)
#6 system/modules/core/library/Contao/User.php(89): Contao\System->import('Database')
#7 system/modules/core/classes/FrontendUser.php(79): Contao\User->__construct()
#8 system/modules/core/library/Contao/User.php(151): Contao\FrontendUser->__construct()
#9 [internal function]: Contao\User::getInstance()
#10 system/modules/core/library/Contao/System.php(110): call_user_func(Array)
#11 index.php(41): Contao\System->import('FrontendUser', 'User')
#12 index.php(432): Index->__construct()
#13 {main}
```

Hello darkness my old friend

Warning: Cannot modify header information - headers already sent by (output started at /home/capitolm/public_html/capitolresidence.mk/system/helper/functi
system/modules/core/library/Contao/System.php on line **484**

```
#0 [internal function]: __error(2, 'Cannot modify h...', '/home/capitolm/...', 484, Array)
#1 system/modules/core/library/Contao/System.php(484): setcookie('BE_USER_AUTH', 'adc1d49e61fb68f...', 1542286693, '/', '', false, true)
#2 system/modules/core/classes/Frontend.php(534): Contao\System::setCookie('BE_USER_AUTH', 'adc1d49e61fb68f...', 1542286693, NULL, NULL,
#3 index.php(45): Contao\Frontend->getLoginStatus('BE_USER_AUTH')
#4 index.php(432): Index->__construct()
#5 {main}
```

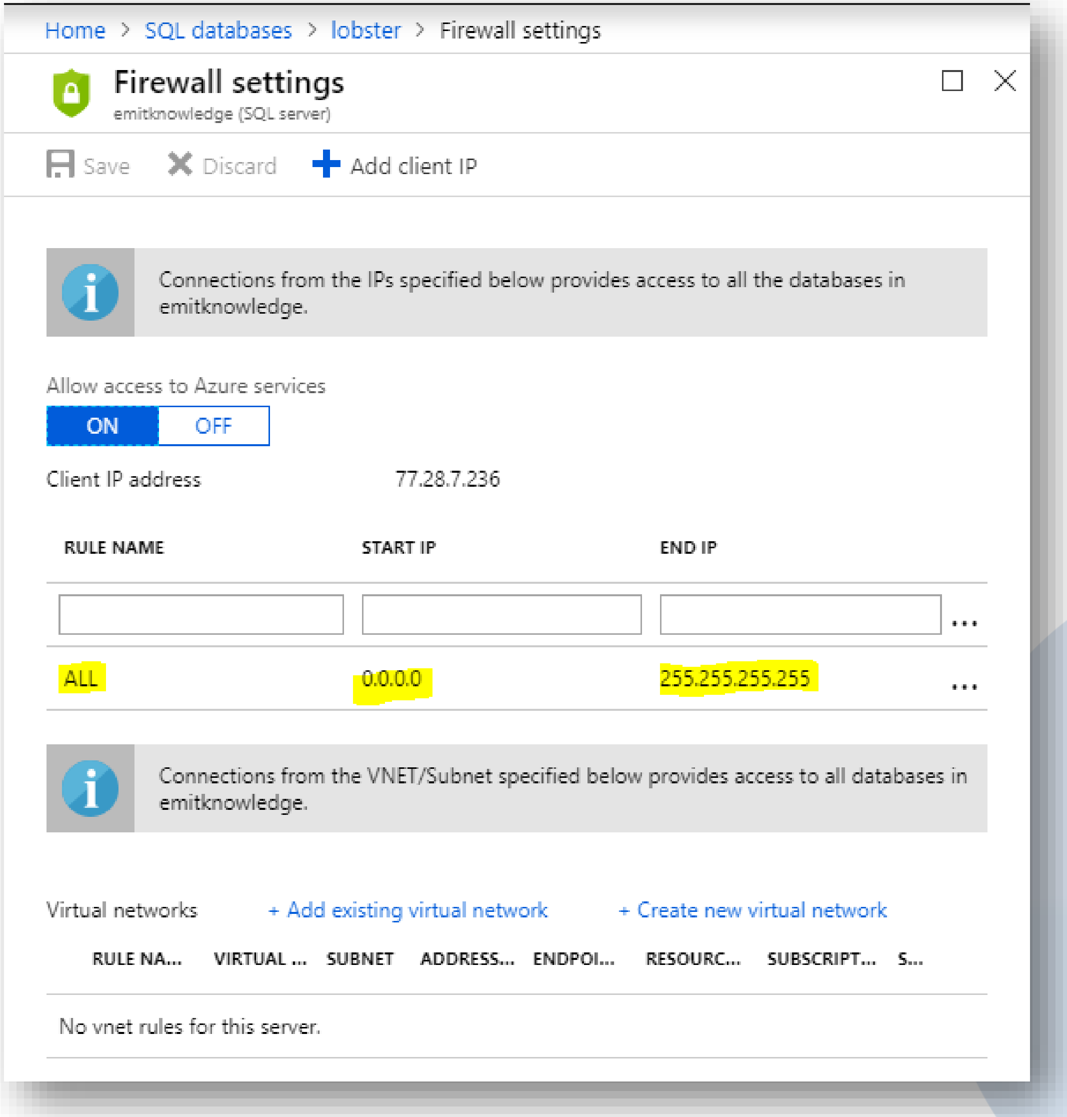
Warning: Cannot modify header information - headers already sent by (output started at /home/capitolm/public_html/capitolresidence.mk/system/helper/functi
system/modules/core/library/Contao/System.php on line **484**

```
#0 [internal function]: __error(2, 'Cannot modify h...', '/home/capitolm/...', 484, Array)
#1 system/modules/core/library/Contao/System.php(484): setcookie('FE_USER_AUTH', '671ac9c63298ee7...', 1542286693, '/', '', false, true)
#2 system/modules/core/classes/Frontend.php(534): Contao\System::setCookie('FE_USER_AUTH', '671ac9c63298ee7...', 1542286693, NULL, NULL,
#3 index.php(46): Contao\Frontend->getLoginStatus('FE_USER_AUTH')
#4 index.php(432): Index->__construct()
#5 {main}
```

Warning: Cannot modify header information - headers already sent by (output started at /home/capitolm/public_html/capitolresidence.mk/system/helper/functi
system/modules/core/library/Contao/Template.php on line **298**

```
#0 [internal function]: __error(2, 'Cannot modify h...', '/home/capitolm/...', 298, Array)
#1 system/modules/core/library/Contao/Template.php(298): header('Vary: User-Agen...', false)
#2 system/modules/core/classes/FrontendTemplate.php(210): Contao\Template->output()
#3 system/modules/core/pages/PageRegular.php(183): Contao\FrontendTemplate->output(true)
#4 index.php(249): Contao\PageRegular->generate(Object(Contao\PageModel), true)
#5 index.php(433): Index->run()
#6 {main}
```

Warning: Cannot modify header information - headers already sent by (output started at /home/capitolm/public_html/capitolresidence.mk/system/helper/functi



Home > SQL databases > lobster > Firewall settings

Firewall settings

emitknowledge (SQL server)

Connections from the IPs specified below provides access to all the databases in emitknowledge.

Allow access to Azure services [✓ ON] OFF

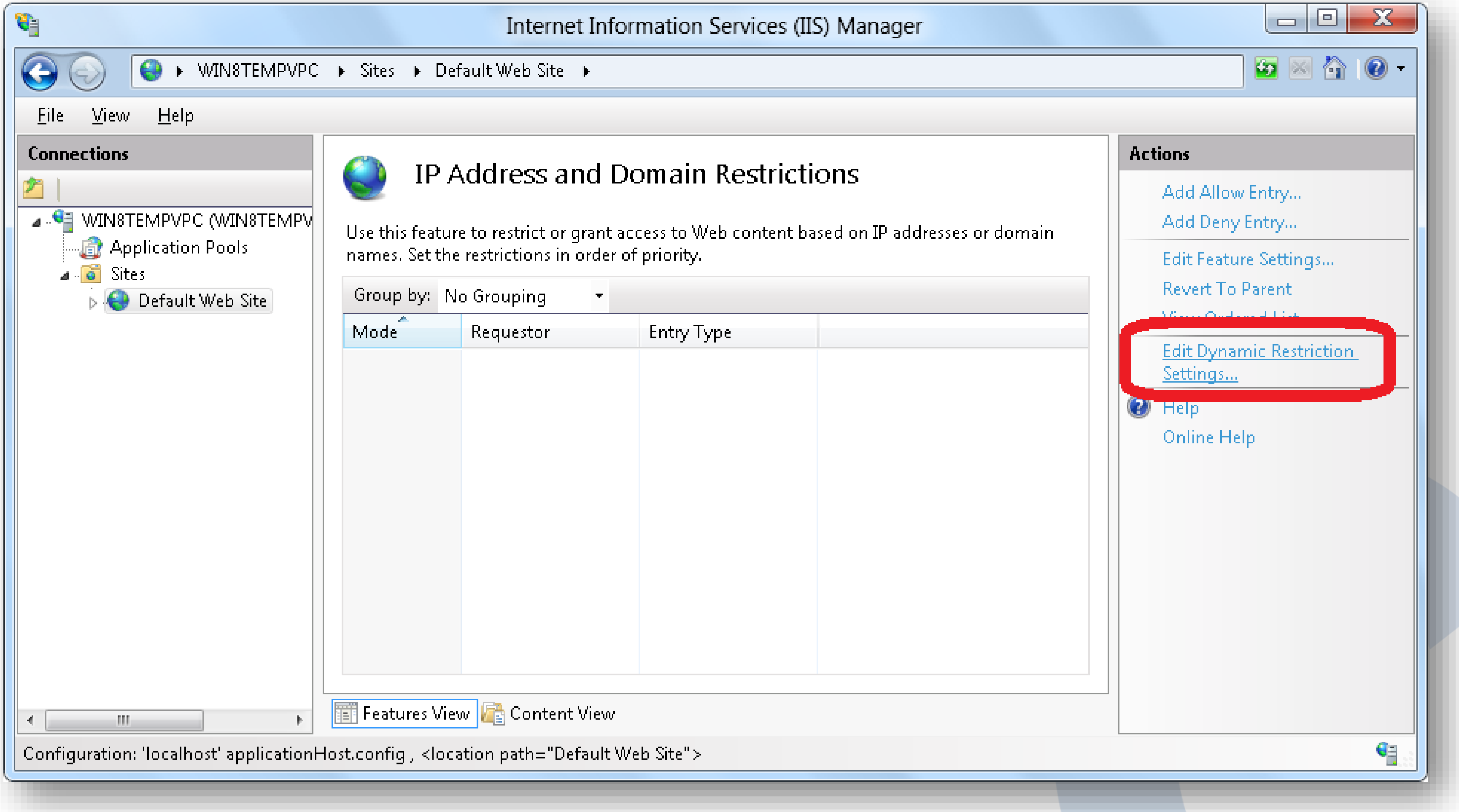
Client IP address 77.28.7.236

RULE NAME	START IP	END IP
ALL	0.0.0.0	255.255.255.255

Connections from the VNET/Subnet specified below provides access to all databases in emitknowledge.

Virtual networks + Add existing virtual network + Create new virtual network

RULE NA...	VIRTUAL ...	SUBNET	ADDRESS...	ENDPOI...	RESOURC...	SUBSCRIPT...	S...
No vnet rules for this server.							



IP Address and Domain Restrictions

Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Group by: No Grouping

Mode	Requestor	Entry Type

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site">

Common scenarios

@Case

You start learning a technology from MSDN/Youtube video/Pluralsite

____

- Create a boilerplate which address those following issue:
  - Set custom pages to on for environments != developement;
  - Set always https on;
- Create a solution wide exception handling and out of boundary information strategy;
- Configure your environments blacklist everything and whitelist on demand:
  - Common issue with database and RDP open for public;
  - Passwords have been changed 5 years ago when the project started;

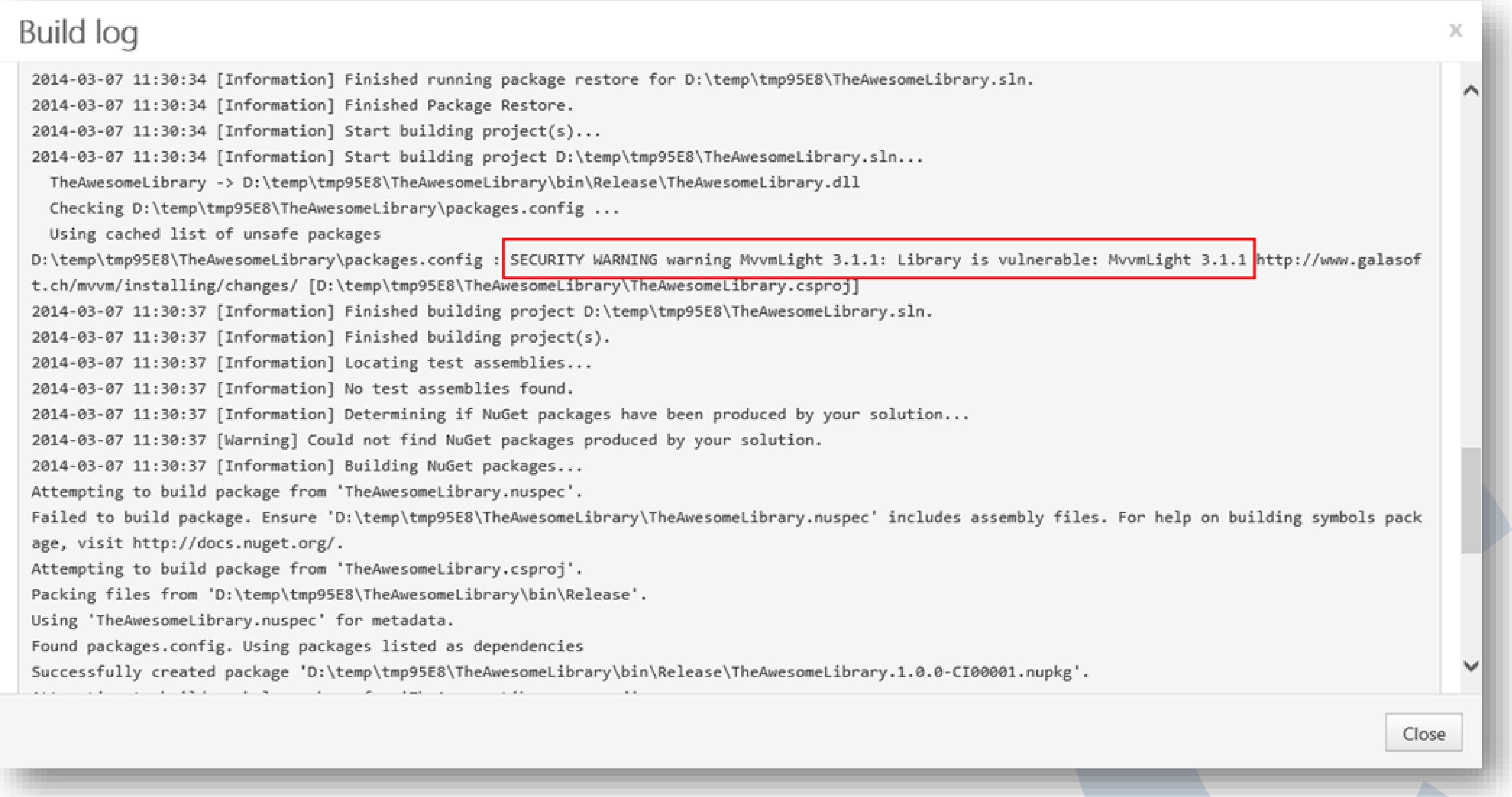
Additional eastern eggs

- Set **X-Frame-Options** := DENY
- Set **X-Xss-Protection** := 1; mode=block
- Set (SSL) **Strict-Transport-Security** := max-age=31536000; includeSubDomains
- Configure **Content-Security-Policy**

* **More on:** https://blog.elmah.io/improving-security-in-asp-net-mvc-using-custom-headers/

Using Components with Known Vulnerabilities

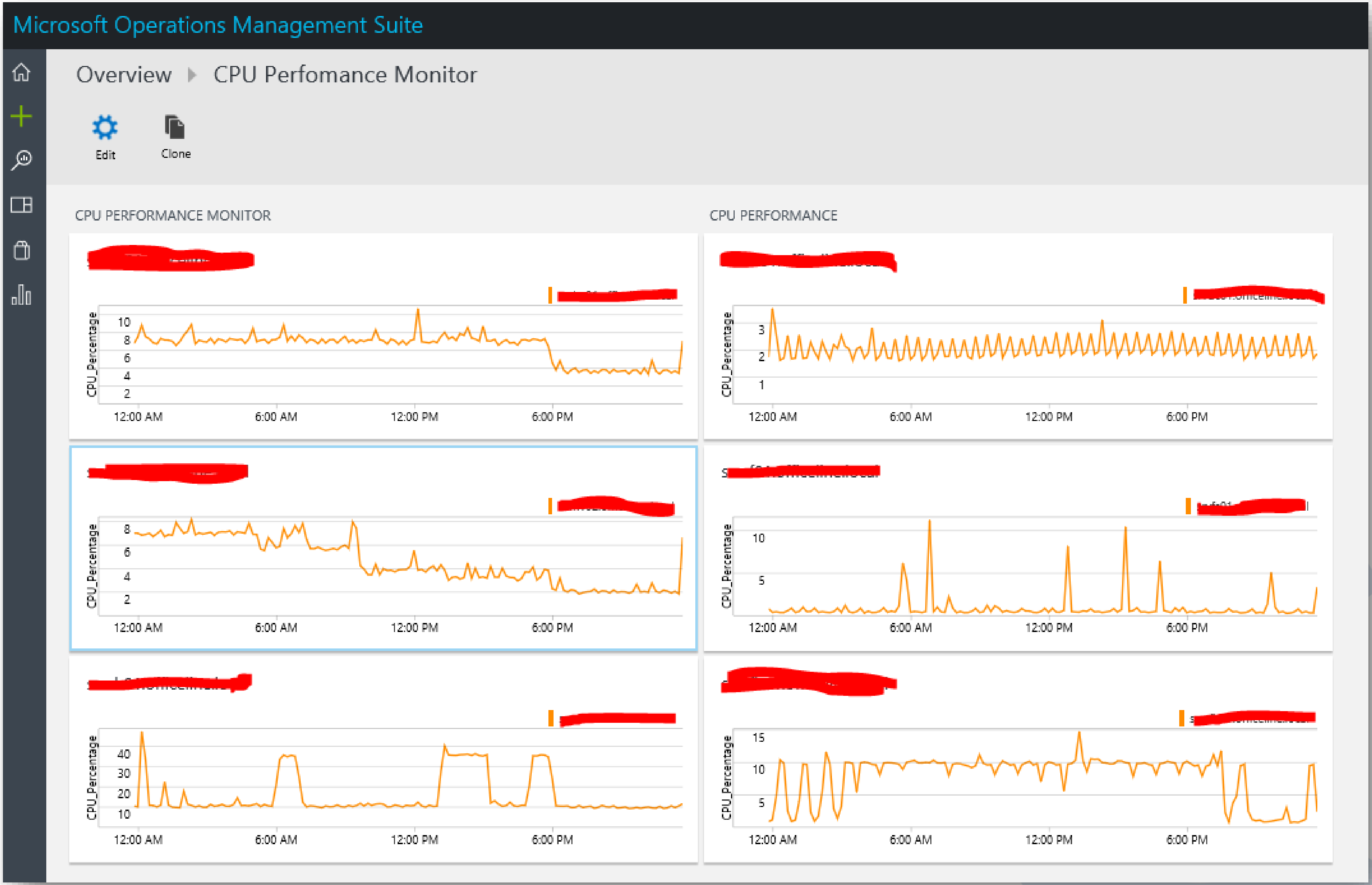
- Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.



```
2014-03-07 11:30:34 [Information] Finished running package restore for D:\temp\tmp95E8\TheAwesomeLibrary.sln.
2014-03-07 11:30:34 [Information] Finished Package Restore.
2014-03-07 11:30:34 [Information] Start building project(s)...
2014-03-07 11:30:34 [Information] Start building project D:\temp\tmp95E8\TheAwesomeLibrary.sln...
  TheAwesomeLibrary -> D:\temp\tmp95E8\TheAwesomeLibrary\bin\Release\TheAwesomeLibrary.dll
  Checking D:\temp\tmp95E8\TheAwesomeLibrary\packages.config ...
  Using cached list of unsafe packages
D:\temp\tmp95E8\TheAwesomeLibrary\packages.config : SECURITY WARNING warning MvvmLight 3.1.1: Library is vulnerable: MvvmLight 3.1.1 http://www.galasof
t.ch/mvvm/installing/changes/ [D:\temp\tmp95E8\TheAwesomeLibrary\TheAwesomeLibrary.csproj]
2014-03-07 11:30:37 [Information] Finished building project D:\temp\tmp95E8\TheAwesomeLibrary.sln.
2014-03-07 11:30:37 [Information] Finished building project(s).
2014-03-07 11:30:37 [Information] Locating test assemblies...
2014-03-07 11:30:37 [Information] No test assemblies found.
2014-03-07 11:30:37 [Information] Determining if NuGet packages have been produced by your solution...
2014-03-07 11:30:37 [Warning] Could not find NuGet packages produced by your solution.
2014-03-07 11:30:37 [Information] Building NuGet packages...
Attempting to build package from 'TheAwesomeLibrary.nuspec'.
Failed to build package. Ensure 'D:\temp\tmp95E8\TheAwesomeLibrary\TheAwesomeLibrary.nuspec' includes assembly files. For help on building symbols pack
age, visit http://docs.nuget.org/.
Attempting to build package from 'TheAwesomeLibrary.csproj'.
Packing files from 'D:\temp\tmp95E8\TheAwesomeLibrary\bin\Release'.
Using 'TheAwesomeLibrary.nuspec' for metadata.
Found packages.config. Using packages listed as dependencies
Successfully created package 'D:\temp\tmp95E8\TheAwesomeLibrary\bin\Release\TheAwesomeLibrary.1.0.0-CI00001.nupkg'.
```

Insufficient Logging and Monitoring

- Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.



Microsoft Operations Management Suite

Overview ▸ CPU Perfomance Monitor

Edit

Clone

CPU PERFORMANCE MONITOR

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

CPU PERFORMANCE

[redacted]

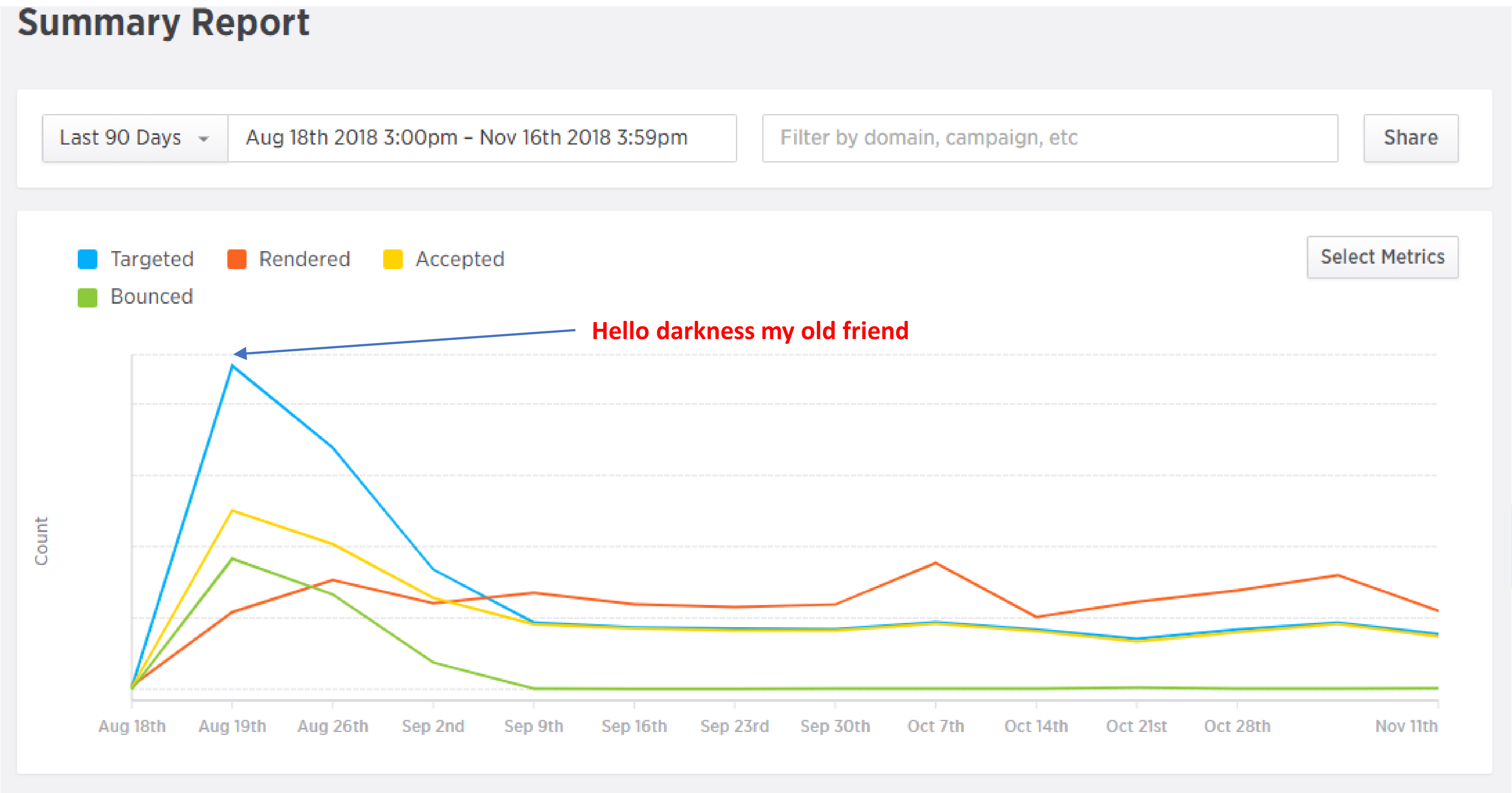
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



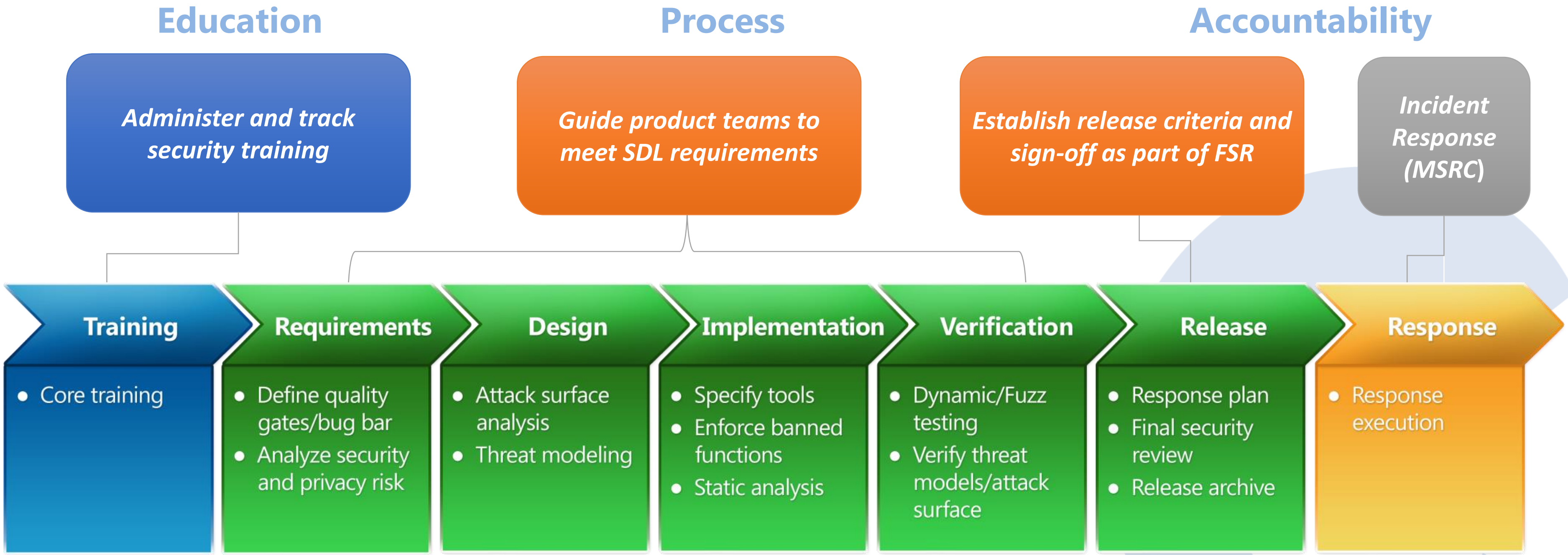
Summary Report

Last 90 Days ▾ | Aug 18th 2018 3:00pm – Nov 16th 2018 3:59pm

Filter by domain, campaign, etc

Hello darkness my old friend

Microsoft Security Development Lifecycle (SDL)



Education
Process
Accountability
Administer and track security training
Guide product teams to meet SDL requirements
Establish release criteria and sign-off as part of FSR
Incident Response (MSRC)
Training
Requirements
Design
Implementation
Verification
Release
Response

Training	Requirements	Design	Implementation	Verification	Release	Response
• Core training	• Define quality gates/bug bar • Analyze security and privacy risk	• Attack surface analysis • Threat modeling	• Specify tools • Enforce banned functions • Static analysis	• Dynamic/Fuzz testing • Verify threat models/attack surface	• Response plan • Final security review • Release archive	• Response execution

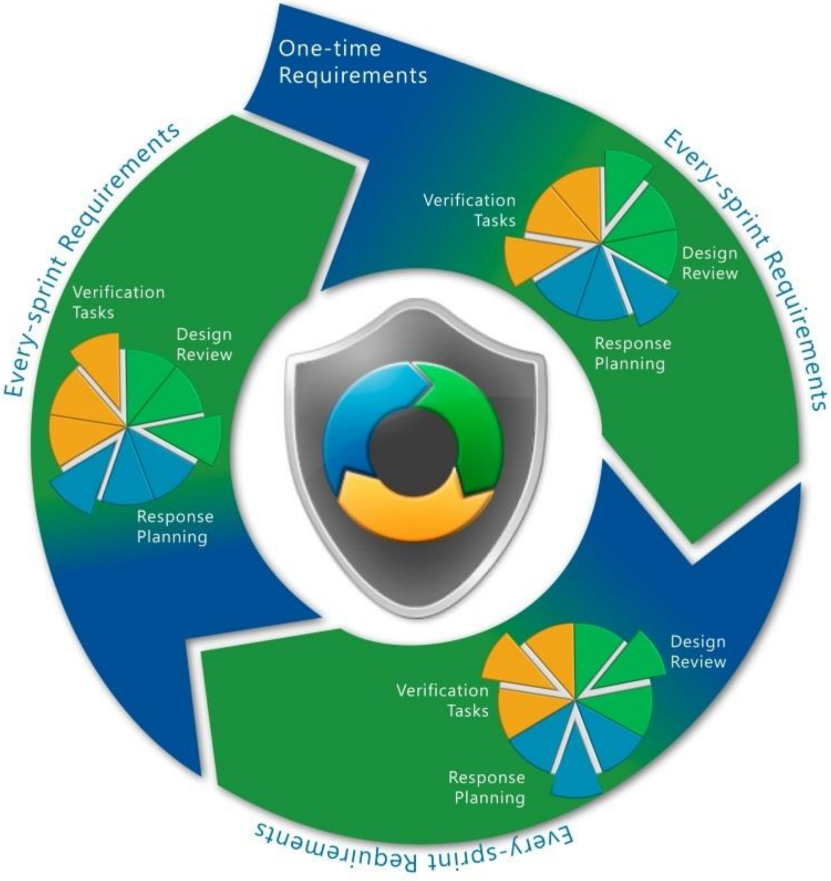
SDL Process Guidance for LOB Apps

- Line-of-Business applications are a set of critical computer applications that are vital to running an enterprise, such as accounting, human resources (HR), payroll, supply chain management, and resource planning applications.
- Many of the requirements and recommendations in the SDL for online services are closely related to what is required for Line-of-Business applications.
- Line-of-Business SDL process guidance allows you to tailor a process specific to your LOB application development while meeting SDL requirements.

Training	Requirements	Design	Implementation	Verification	Release
LOB-specific training	Risk assessment • Application portfolio • Application Risk assessment • Determine service level	Asset-centric threat modeling • Threat model • Design review	Internal review • Incorporate security checklists and standards • Conduct self code review • Security Code analysis	Pre-production assessment • Comprehensive security assessment • Bug remediation	Post-production assessment • Host level scan

Guidance for Agile

- Requirements defined by frequency, not phase
  - Every-Sprint (most critical)
  - One-Time (non-repeating)
  - Bucket (all others)



Synthetic sugar

- Use a preconfigured project boilerplate:
  - Default headers;
  - Error pages;
  - Default encoder AntiXSS or HtmlSanitizer;
- Centralized exception handling:
  - Standardize the out of boundaries response;
  - Control the information that you are sharing outside of your system;
- [IgnoreDataMember] for serialization;
- Custom CriticalData attribute;
- Stop doing fancy generic solutions and use parametrized procedures;

Introducing Signals

- Open source, USE Case driven framework which sets your focus on your business logic;

Thanks!

Any Questions?