IT Security Report 2022

Lars Bürger

301662

Angewandte Informatik
Lars Bürger
Deutschland
29. November 2022

Contents

Chapter 1

Exercise 1

CVE-2022-2986

Short Description: Enabling and disabling installed H5P libraries did not include the necessary token to prevent a CSRF risk.
Impact for university: Victim could be forced to perform state changing requests like transferring funds, changing their email adress etc.
Solution: A CSRF (Cross-Site-Request-Forgery) is an attack where the end user is forced to perform unwanted actions in a web application. With this risk as an It service provider i would Beware users of possible spam emails with malicious content or better shut down the vulnerbal feature.

CVE-2022-40316

Short Description: The H5P activity attempts report did not filter by groups, which in separate groups mode could reveal information to non-editing teachers about attempts/users in groups they should not have access to.
Impact for university: Reveal private information about users.
Solution: Access to this feature can be revoked by removing the mod/h5pactivity: review attempts capability from relevant users until the patch is applied.

CVE-2022-40315

Short Description: SQL injection in the administration page.
Impact for university: Could resolve in data loss for users or could reveal private information.
Solution: Wait until it is fixed, admins shouldnt be a thread to the website.

CVE-2022-40314

Short Description: A remote code execution risk when restoring backup files originating from Moodle 1.9 was identified.
Impact for university: Depending on what malicious code hackers would execute through this risk it could lead to data loss, uncover private information, etc about students and proffessors.
Solution: Inform students and proffessors that file backups should be avoided until this vulnerbility is fixed.

CVE-2022-40313

Short Description: Recursive rendering of Mustache template helpers containing user input could, in some cases, result in an XSS risk or a page failing to load.
Impact for university: maybe if possible disable these input buttons to avoid the risk of xss, but in the case where this isnt possible cant do much except maybe inform users about the risk.
Solution: Disable the user input that is vulnerbal to an attack.

CVE-2022-35653

Short Description: A reflected XSS issue was identified in the LTI module of Moodle.
Impact for university: Attacker could trick them into clicking on a link containing malicious content.
Solution: The vulnerbility didnt impact authenticated users. Warn unauthenticated users to not click on any suspicious links.

CVE-2022-35652

Short Description: An open redirect issue was found in Moodle due to improper sanitization of user-supplied data in mobile auto-login feature.
Impact for university: Successful exploitation of this vulnerability may allow a remote attacker to perform a phishing attack and steal potentially sensitive information.
Solution: Disable the feature until patch.

CVE-2022-35651

Short Description: A stored XSS and blind SSRF vulnerability was found in Moodle, occurs due to insufficient sanitization of user-supplied data in the SCORM track details.
Impact for university: Stealing of sensitive information, performing phishing attacks and drive-by-download attacks to victims.
Solution: Disable tracking feature until next patch.

CVE-2022-35650

Short Description: The vulnerability was found in Moodle, occurs due to input validation error when importing lesson questions.
Impact for university: Could lead to data loss and reveal sensitive information.
Solution: Wait for patch, maybe inform profs, managers and admin of this vulnerbility or disable the feature to import lesson questions.

CVE-2022-35649

Short Description: The vulnerability was found in Moodle, occurs due to improper input validation when parsing PostScript code.
Impact for university: Could lead to complete compromise of vulnerable system.
Solution: Ensure older versions of GhostScript are upgraded to 9.50 or newer.

CVE-2022-30600

Short Description: Failed login attempts counted incorrectly. Lead to bypassing login fail threshold.
Impact for university: Could probably lead to hacking attemps that try to get the password of users with automated login bots.
Solution: Cant do much, wait for patch by devs.

CVE-2022-30599

Short Description: SQL injection risk in Badges code relating to configuring criteria.
Impact for university: Reveal sensitive information and data loss.
Solution: Remove moode/badges:configurecriteria from user until patch.

CVE-2022-30598

Short Description: Global search results include author information on some activities where users otherwise not have access to.
Impact for university: reveal sensitive data.
Solution: Remove global search until next patch.

CVE-2022-30597

Short Description: Flaw where description user field was not hidden when being set as a hidden user field.
Impact for university: reveal possible sensitive and private information.
Solution: Inform users of this flaw, wait for next patch.

CVE-2022-30596

Short Description: Flaw where id numbers required additional sanitizing to prevent a stored xss risk when bulk allocating markers to assignments.
Impact for university: xss could lead to data loss etc.
Solution: disable markers to assignments until patch.

CVE-2022-0985

Short Description: Flaw allowed users with the moodle/site:uploadusers capability to delete users without having necessary moodle/user:delete capability.
Impact for university: Could lead to deleted users in the system.
Solution: Remove the moodle/site:uploadusers capability until the next patch.

CVE-2022-0335

Short Description:Flaw in the "delete batch alignment" feature that could lead to CSRF Risks.
Impact for university: CSFR Risk could lead to data loss, reveal of sensitive data, etc..
Solution: Remove the "delete batch alignment" feature until the next patch. Warn users of risk.

CVE-2022-0334

Short Description: Insufficient capability checks lead to users accessing their grade report where they did not have access to.
Impact for university: reveal grades that should not have been accessed.
Solution: Disable the grade report feature of all courses until this flaw is fixed.

CVE-2022-0333

Short Description: Flaw that allowed managers to acces or modify ANY calendar events.
Impact for university: Could lead to deleted or changed calendar events.
Solution: Wait for patch, due to the fact that only managers could exploit this feature the risk of any harms is pretty low.

CVE-2022-0332

Short Description: An SQL injection risk was identified in the h5p activity web service responsible for fetching user attempt data
Impact for university: Leads to reveal of sensitive data, data loss, etc...
Solution: Cant do much, maybe disable feature and wait for next patch by developers.

Chapter 2

Exercise 2

2.1

2.1.1 Rules for teleworkers/ Security policies for teleworkers

The paper explains that it has to be defined wich information (on paper and in IT systems) can be used outsite of the institution. In the case of the HTWG Constance I think those rules are not strictly defined enough because the majority of the work for students isnt done at the HTWG rather it is done in home office and with that pretty much all information and data is used outsite of the institution on private IT systems. This could lead to a lot of data loss and could possibly reveal much sensitive data of the HTWG the faculties and the persons studying or working at the university.

2.1.2 Sensitization of teleworkers

The section explains that teleworkers should be sensitized with the handling and the work of sensible data and information. Also in this section i can see a gap to our study work at the htwg constance. The handling of sensitive data and information has never been properly taught until now. It should have a higher priority to teach students how to handle such data and how to behave properly with it outside the university. To avoid accidents with sensitive data.

2.1.3 Access and access protection

The section informs about the needed access protection while working at home outsite of the institution. Also in this chapter you can see clear differences compared to students at the HTWG Konstanz. Many students live in large shared apartments and student dormitories, which means that permanent security of sensitive and important information is not guaranteed.

2.1.4 Security requirements for the IT systems used for teleworking IT systems used

No student IT system is properly tested for security requirements. Students including me work on external laptops mostly without VPN with all data and information of lectures and exercises. This can easily lead to vulnerabilities which could be used to steal, modify or delete this data. Another topic in the sheet is the use of screen protection against shoulder surfing and general consideration where and when to reveal information on your screen.

Many students work in crouded places like the library or the mensa and the majority of the students are not using any screen protection to secure private information and data.

2.1.5 Remote Access

Even the remote access isnt used enough. the University has a VPN but the most information can be accessed without it what could also lead to possible stealing of data. However, if you talk about working at the university, this point is at least partially fulfilled. A VPN is permanently used at the PC pools of the university, which is advantageous from a security point of view.

2.1.6 Data Backup

In this section, we will talk about proper data backup, that is, we will show the correct behavior in case of data loss when, for example, damage to hard drives occurs during transport or when losses occur due to theft.

At the university itself, data loss will probably not be too much of a problem, as I suspect that the htwg servers make daily if not more frequent backups of all data.

Speaking of work at home. I myself have most of the data on github this is of course a convenient way to backup data as all data is in the cloud as well as a very convenient tool to work on multiple it devices at the same time.

2.1.7 Working with third-party it systems

The only work I do for the htwg on external it systems is in the PC pool rooms of the htwg itself.

Since the htwg is trustworthy, this point is not particularly important for me as a student.

2.1.8 Attention phishing

On this point, too, the htwg's security precautions are adequate to deal with it.

There was one incident with phishing during my entire time as a student, but I was quickly made aware of these scam emails, which did not lead to any further problems.

2.1.9 Conclusion

In summary, while the rules and regulations in the handout are good and important in themselves to protect data and information effectively, many of these rules cannot be applied to students as they require a different set of requirements than a regular teleworker.

Nevertheless, as a student, you should always try to make the handling of data as compliant as possible in order to work safely.

2.2

2.2.1 NOT BASIC (NOT RELEVANT FOR EXCERCISE)

In the IT Basic Protection Compendium, it is also mentioned that the private use of a telework computer is strictly prohibited, as any private applications could compress sensitive data, which could lead to data theft or data loss. This section and therefore this "basic" security precaution was not mentioned in the leaflet.

The lack of integration into the company's internal information flow was also not mentioned in the leaflet. This can lead to the teleworker not receiving IT security relevant information until too late or not at all, leading to a possible security gap.

2.2.2 BASIC REQUIREMENT

OPS.1.2.4

The basic requirements in the IT security compendium chapter OPS.1.2.4 include the security requirements for the telework computer. This means that security requirements must be defined, it must be ensured that only authorized persons have access to the computer and that the telework computer can only be used for authorized purposes.

The first two requirements were clearly mentioned in the leaflet. The last requirement, which in itself prohibits private use, was not mentioned in detail in the leaflet.

On the other hand, the basic requirements also include the sensitization of employees, which was mentioned in detail in the leaflet in the second section "Sensitization of teleworkers".

INF. 8

Chapter INF.8 focuses on the basics of safety in the home workplace. It shows why the same infrastructural safety cannot be assumed at a home workplace as at the offices of the institution and why it can therefore more easily lead to vulnerabilities. The core objective of the module is to protect the institution's information at the home workplace.

I think all of the basic safety requirements mentioned in chapter INF.8 were also mentioned in the leaflet. In the leaflet, these points were especially mentioned in chapters three to five.

INF. 9

The last chapter INF. 9 deals with the requirements of a mobile workplace. This covers things like good network coverage, powerful IT devices and a good working environment. This module describes the security requirements for mobile workplaces. The aim here is to create a safety situation for such workplaces that is comparable to that of an office.

The basic requirements of this chapter include the appropriate selection and use of a mobile workplace.

This point is mentioned in the leaflet, but in less detail than in the compendium. The regulations governing which workstation environments are completely prohibited

or under which conditions sensitive information may be processed are only vaguely described in the leaflet.

Another basic requirement of this chapter are regulations for mobile workplaces that describe, among other things, which information may be transported and processed outside the institution or how the taking of it components and data carriers must be clearly regulated.

these points, in turn, were mentioned quite clearly in the leaflet, especially in chapters 5, 8 and 13. And the last two points concerning access protection and working with third-party it systems were also clearly mentioned in the leaflet in chapter 3 and chapter 11.

Conclusion and personal opinion

In conlusion you could say that the majority of the basic point that are listed in the big Compedium where also mentioned in a much shorter version in the leaflet. So I would say you are on the safe side if you as an institution teach your employees the rules and requirements from the leaflet to create a safe environment.

In my opinion, I also find some points very important to adhere to in order to have a safe and pleasant working environment as a teleworker, even as a student.

Especially in Chapter INF. 8 I found the standard point about the suitable equipment of the domestic workplace very important. Not only for increased safety, but also for a pleasant working environment, suitable furniture is very important.

I also find the point about disposing of confidential information very important, as this can easily lead to a weak point in a larger residential community and thus harm the university and oneself.

Chapter 3

Exercise 3

Application whitelisting is the practice of specifying an index of approved software applications or executable files that are permitted to be present and active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications.

3.1

Modules that address application whitelisting:

- SYS.1.1 General Server (Section: SYS.1.1.A31)
- SYS.2.1 General Client (Section: SYS.2.1.A33)
- SYS.2.2.3 Windows 10 Clients (Section: SYS.2.2.3.A5)
- SYS.2.2.2 Windows 8.1 Clients (Section: SYS.2.2.A14)
- SYS.2.3 Linux and Unix Clients (Section: SYS.2.3.A8)
- SYS.3.2.1 General Smartphones and Tablets (Section: SYS.3.2.1.A30)

3.2

3.2.1 SYS.1.1 General Server

According to this section application whitelisting must ensure that only programs that are allowed can be executed. Furthermore, exact paths and directories must be specified from where these programs are allowed to run. In addition, individual programs should be explicitly allowed to run as an alternative.

3.2.2 SYS.2.1 General Client

In addition to programs, specially named scripts may also run. The rules should be as restrictive as possible.

3.2.3 SYS.2.2.3 Windows 10 Client

If no protection has been implemented such as application whitelisting, special malware protection must be used on Win 10.

3.2.4 SYS.2.2.2 Windows 8.1 Clients

Applications in paths for which users have write privileges shouldnt be able to be executed by AppLocker or software restriction policies. Attempted violation of rules should be logged and evaluated. SPR or AppLocker should be tested on a test system or monitoring mode.

3.2.5 SYS.2.3 Linux and Unix Clients

To restrict certain apps AppArmor or SELinux should be used. The solution with the best protection provided should be used.

3.2.6 SYS.3.2.1 General Smartphones and Tablets

Mobile end devices should only be able to install approved and tested apps. If an MDM system (Mobile-Device-Management) is used it should prevent other apps from being installed. It should immediatly remove software that was installed unauthorized.

3.3

Windows defender application control is designed to protect devices from malware and other untrusted software. This prevents malicious code from running by ensuring that only authorized processes are executed.

Before WDAC, the AppLocker application was introduced with Windows 7, which allows organizations to control which apps can run and which cannot. AppLocker helps end users to exclude unapproved software, but it is not recognized as a security feature.

3.3.1 How does Windows Defender Application Control (WDAC) support system administrators to implement Application Whitelisting?

The Windows Defender Application control feature allows the administrator to control which programs and scripts are allowed to run on the specific windows device with either windows 10 or 11 running as the operating system. This is achieved by setting policies that specify whether a driver or application is trusted. These policies include rules that control options like audit mode or file rules (or file rule levels) that specify how the process or the application is identified and trusted.

Rules

The policy rules are defined in an XML file that the admin can modify to add new rules or remove old rules. To access an existing XML file to modify the policy rules, the administrator must use the cmdlet "Set-RuleOption". Here there are countless possibilities to change and modify the rules of the current WDAC.

Among other things you can add new rule options for example with this command:

```
Set-RuleOption -FilePath <Path to policy XML> -Option 0
```

or remove already existing rule options:

```
Set-RuleOption -FilePath <Path to policy XML> -Option 0 -Delete
```

All adjustable rule options can be found in the microsoft article about Windows Defender Application Control.

File rule levels

As mentioned at the beginning of this chapter, administrators also have the ability to set policies that determine the file rule levels.

File rule levels allow the admin to specify the level at which they can trust their applications.

This allows the administrator to specify the level at which they can trust their applications and processes, making Windows Defender Application Control very flexible. As an example among others, there is a level for publishers that allows software from their software vendors, the "publishers" level or the "filename" level which specifies the original filename for each binary file.

File path rules

The administrator even has the ability to define rules for the filepaths. This rule set guarantees less security than others and works best in environments where most users do not have admin rights and work as standard users. However, it should be avoided to apply this ruleset to directories where standard users have the ability to modify ACLs (access control list) on the folder.

There are multiple options to generate new filepath rules. By using the `New-CIPolicy` a unique fully qualified path rule is generated for every file discovered in the scanned paths. By using the `New-CIPolicyRule` rules are generated that allow all files under a specific folder path and by using the `-FilePathRule` option you can define rules containing wildcards.

3.3.2 What benefits and limitations does this technique have?

Benefits:

- Administrator can create and modify different Windows Defender Application Control policies via XML files to implement certain rule sets to bring more security into a system.
- You have an incredibly large selection of different rules and policies to build a very specific and user-dependent environment.
- You have a lot of documentation and examples of how to use the different rules and policies and what they do. A very large part of the documentation and help can be found on the official Microsoft site in the article about WDAC.
- WADC is a big step forward compared to the older alternative AppLocker and offers a lot more functionality.

Limitations:

- The WDAC feature is only available for Windows 10 and 11 which limits the tool very much because it cant be runned on an other operating system like Linux or and older version of windows.
- Despite the many rule sets and policies, you are probably somewhat limited in some way by microsoft. I'm not sure how much, but I suspect you can't create your own fully customizable rules and have to make do with the existing options for the most part.
- Also limited is the targeting of the rules, which can only be applied to computers and not to users. If user-specific restrictions are required, Microsoft recommends using AppLocker in parallel.
- There is no graphical tool for defining custom rules, only PowerShell cmdlets. They only allow whitelisting in a narrower sense, where applications are explicitly allowed.

3.3.3 Which of the requirements in the identified IT-Grundschutz modules can be fulfilled by WDAC?

The requirements of SYS.1.1 General Server that adress application whitelisting could be fulfilled by the WDAC feature. (SYS.1.1.A31) Both application whitelisting that ensures only programs that are allowed can be executed and paths and directories must be specified are possible in the WDAC feature. With this also the requirement of General Clients are fulfilled what also fulfills the requirements of Windows 10 Clients as the WDAC can run on Win 10 (SYS.2.1.A33 and SYS.2.2.3.A5).

The requirements of the other modules couldnt really be fulfilled because the one module was for linux and unix client on which WDAC cant be executed. And the other module was specifically for general smartphones and tablets.