PRISM PENETRATION TESTING REPORT

Group IT Security

Security Vulnerability Management Apps

THIS IS AN INTERNAL DOCUMENT AND IS BEING SHARED WITH THE RECIPIENT(S) ON A NEED TO KNOW BASIS. IT SHOULD NOT BE SHARED OR FORWARDED TO ANY OTHER RECIPIENTS WITHOUT THE WRITTEN APPROVAL FROM THE GROUP IT CISO

Version: 1.0
Status: Published

Author: Matviiuk, Volodymyr

Date: 06-04-2025
Classification: SEC1: Company Confidential

Updates			
Version	Date	Author	Description of changes
0.1	28-05-2025	Volodymyr Matviiuk	First Draft
1.0	4-06-2025	Volodymyr Matviiuk	Initial Version

Table of Contents

1. Management Summary

1.1 Summary

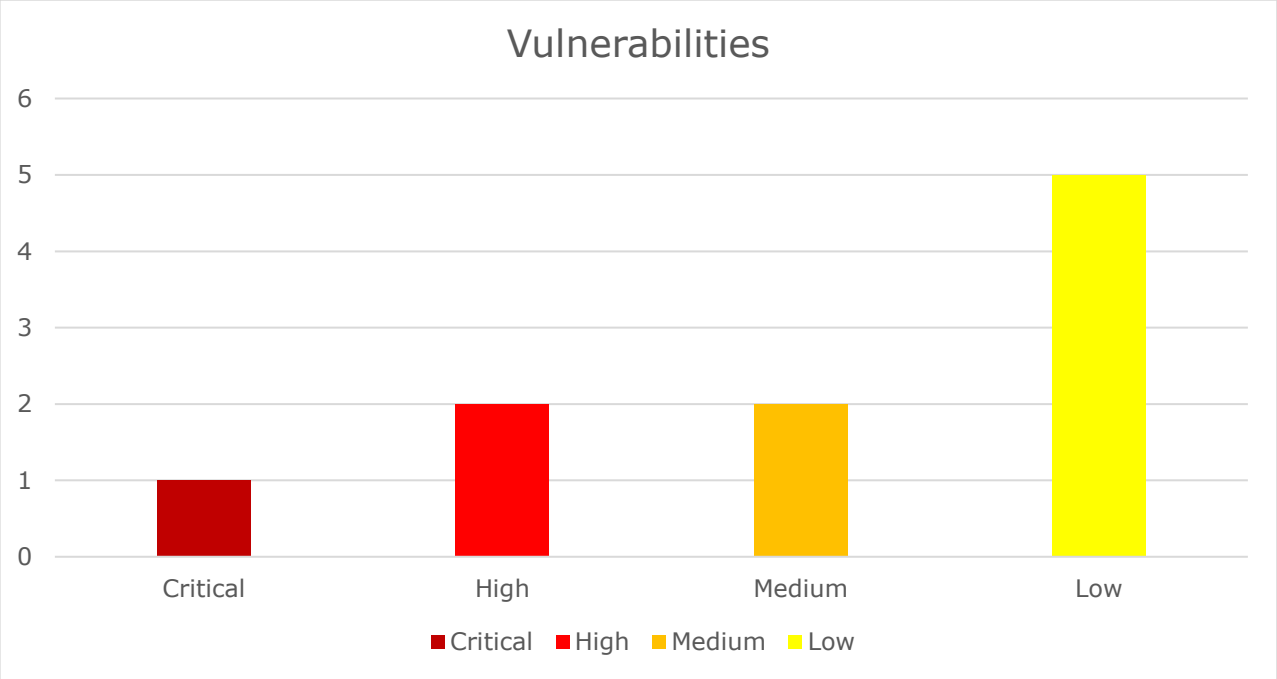
The Penetration Testing of the PRISM application was carried out in the month of May 2025. The penetration testing revealed **1 Critical, 2 High, 2 Medium and 5 low** risk vulnerabilities in the application. These are summarized and shown as below.

A summary of observations classified by Severity are presented below in the form of a Graph:

Current Security Testing Statistics

Application Vulnerabilities:

Test	Date	Critical	High	Medium	Low
Penetration Testing	04-06-2025	1	2	2	4



1.2 Risk Rating

Based on the vulnerabilities found, the penetration testing team concludes that the **PRISM** application is considered a **'Critical'** risk environment and recommends mitigating all the findings on priority.

2. Assignment

2.1 Scope of Security Testing

The following systems and underlying infrastructure were in scope for this assessment:

Asset	Scope	Description
PRISM	https://prism-preprod.capgemini.com 10.29.165.209	Preprod environment

2.2 Approach

The scope of our security testing includes Grey Box & Black Box Security Assessment of the Web application and its related Infrastructure. Grey Box Assessment takes **"Partial Knowledge"** approach while Black Box Assessment takes **"No Knowledge"** approach as an attacker. Security tester will Initiate attack against the Web application and its Infrastructure and try to bypass Specific restrictions on the same.

2.3 Objective of Security Testing

Objective behind carrying the Security Testing assignment is to perform detailed security assessment of Web application and its Infrastructure as per the scope to identify potential or realize weaknesses because of inadvertent misconfiguration, Insufficient error handling, Sensitive Information Leakage etc.… and bring in attention of the concern team to mitigate the risk.

2.4 Vulnerability Classification

The final risk consists of a combination of two factors, namely, the likelihood of a vulnerability being exploited and the impact that exploitation of the vulnerability could have for your organization (assuming the scenario with the highest impact).

	Probability			
Impact		**Low**	**Medium**	**High**
	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

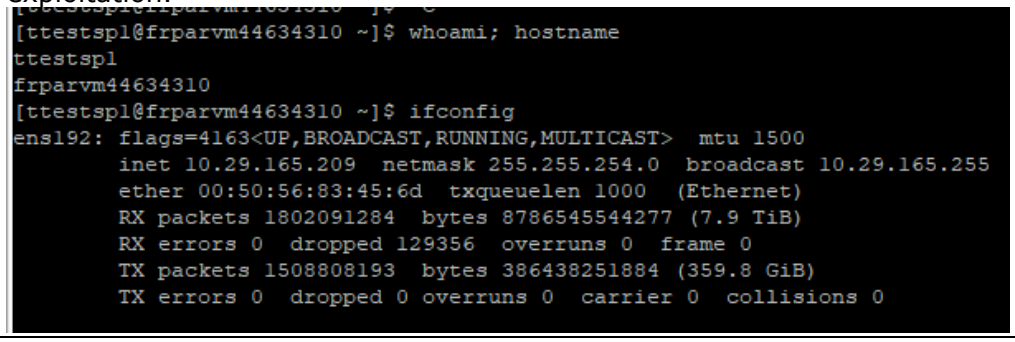
Critical Severity is assigned to those observations which can have direct impact on revenue losses, can lead to critical data loss, complete compromise of the system/application, and may lead to loss of goodwill legal implications.
Such observations need to be addressed on high priority basis and actions for improvement or changes required in process or system should be taken as soon as possible.
High Severity is assigned to those observations which can have adverse impact on revenue of the organization, can lead to loss of data, can hamper critical operations, and may lead to loss of goodwill legal implications.
Such observations need to be addressed on immediate basis and actions for improvement or changes required in process or system should be taken as soon as possible.
Medium Severity is assigned to those observations which may result in indirect revenue losses; resources are not being utilized effectively and efficiently, may lead to security breaches. However, impact may not be immediate as some compensatory controls exist in the overall process / system. Repeated occurrences of these natures would lead it to high severity.
Such observations need to be addressed and proper control shall be placed after considering existing compensating controls.
Low Severity is assigned to those observations which are deviations from the standard procedures defined. Repeated occurrence of such observations would lead to medium severity in long run. Impact of observations under this category may not result in the direct failure of any activities or overall process.

2.5 Vulnerabilities

<table>
<tr><th>#1</th><th>Sensitive Information Disclosure –Private Key</th></tr>
<tr><td>Affected components</td><td>10.29.165.255</td></tr>
<tr><td>Description</td><td>Files with sensitive information like multiple usernames, passwords, private key and payment documents are accessible through SSH.
This information might help an attacker to gain a greater understanding of the systems in use and potentially develop further targeted attacks.</td></tr>
<tr><td>Severity</td><td>
<table>
<tr><th></th><th colspan="4">Probability</th></tr>
<tr><th rowspan="4">Impact</th><th></th><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><th>Low</th><td></td><td></td><td></td></tr>
<tr><th>Medium</th><td></td><td></td><td></td></tr>
<tr><th>High</th><td></td><td></td><td>Critical</td></tr>
</table>
</td></tr>
<tr><td>Authentication Required for Exploitation</td><td>Required</td></tr>
<tr><td>How to Test</td><td>Check files:</td></tr>
</table>

```
/etc/httpd/ssl/2022/prism-uat_capgemini_com_interm.cer
/etc/httpd/ssl/2022/prism-uat_capgemini_com.pem
/etc/httpd/ssl/2022/prism-uat.capgemini.com.key
/etc/httpd/ssl/2022/prism-uat_capgemini_com_cert.cer
/etc/httpd/ssl/2022_int/kmd9-int_capgemini_com_interm (1).cer
/etc/httpd/ssl/2022_int/kmd9-int_capgemini_com.cer
/etc/httpd/ssl/2022_int/kmd9-int_capgemini_com.crt
/etc/httpd/ssl/2022_int/kmd9-int_capgemini_com_cert.cer
/etc/httpd/ssl/2022_int/kmd9-int_capgemini_com.pem
/etc/httpd/ssl/2022_int/wrong_ssl/kmd9-int.capgemini.com.key
/etc/httpd/ssl/2022_int/kmd9-int_capgemini_com_interm.cer
/etc/httpd/ssl/2022_int/kmd9-int.capgemini.com.key
/etc/httpd/ssl/2024/prism-preprod_capgemini_com.crt
/etc/httpd/ssl/2024/prism-preprod_capgemini_com.pem
/etc/httpd/ssl/2024/prism-preprod_capgemini_com_interm.cer
/etc/httpd/ssl/2024/prism-preprod_capgemini_com_interm (1).cer
/etc/httpd/ssl/2024/prism-preprod_capgemini_com.cer
/etc/httpd/ssl/2024/prism-preprod_capgemini_com_cert.cer
/etc/httpd/ssl/2024/prism-preprod.capgemini.com.key
/etc/httpd/ssl/2025/prism-preprod_capgemini_com_cert.cer
/etc/httpd/ssl/2025/prism-preprod.capgemini.com.key
/etc/httpd/ssl/2023/prism-preprod_capgemini_com.crt
/etc/httpd/ssl/2023/prism-preprod_capgemini_com.pem
/etc/httpd/ssl/2023/prism.capgemini.com.key
/etc/httpd/ssl/2023/prism_capgemini_com.crt
/etc/httpd/ssl/2023/prism-preprod_capgemini_com_interm-x509IOR.cer
/etc/httpd/ssl/2023/prism_capgemini_com_interm.cer
/etc/httpd/ssl/2023/prism-preprod_capgemini_com_interm.cer
/etc/httpd/ssl/2023/prism_capgemini_com.pem
/etc/httpd/ssl/2023/prism_capgemini_com_cert.cer
/etc/httpd/ssl/2023/prism-preprod_capgemini_com.cer
/etc/httpd/ssl/2023/prism-preprod_capgemini_com_cert.cer
/etc/httpd/ssl/2023/prism-preprod.capgemini.com.key
/etc/httpd/ssl/2023/prism_capgemini_com_interm-x509IOR.cer
/etc/httpd/ssl/2023/prism_capgemini_com.cer
/etc/httpd/conf.d/autoindex.conf
/etc/httpd/conf.d/php.conf
/etc/httpd/conf.d/userdir.conf
/etc/httpd/conf.d/welcome.conf
/etc/httpd/conf.d/ssl.conf
/etc/httpd/conf.d/phpmyadmin.conf
/etc/httpd/conf/httpd.conf
/etc/httpd/conf.modules.d/00-proxy.conf
/etc/httpd/conf.modules.d/10-h2.conf
/etc/httpd/conf.modules.d/00-mpm.conf
/etc/httpd/conf.modules.d/10-proxy_h2.conf
/etc/httpd/conf.modules.d/00-brotli.conf
/etc/httpd/conf.modules.d/00-dav.conf
/etc/httpd/conf.modules.d/00-optional.conf
/etc/httpd/conf.modules.d/00-ssl.conf
/etc/httpd/conf.modules.d/20-php.conf
/etc/httpd/conf.modules.d/00-base.conf
/etc/httpd/conf.modules.d/00-systemd.conf
/etc/httpd/conf.modules.d/01-cgi.conf
/etc/httpd/conf.modules.d/00-lua.conf
/etc/pki/consumer/cert.pem
/etc/pki/consumer/key.pem
/etc/pki/entitlement/8481773086710720003.pem
/etc/pki/entitlement/8481773086710720003-key.pem
/prism_files/asset/2006/12/28/Weekly Governance REPORT 11-17-2006 - CAP.pub
/prism_files/asset/2020/05/20/backup/Work at Home/khanguye.ppk
/prism_files/working_km3_migration/khanguye.ppk
/prism_files/working_km3_migration/Important Node For Migration - Don't Delete/khanguye.ppk
[ttestspl@frparvm44634310 /]$
```

Recommendation	Files containing sensitive information like plaintext passwords should be not be accessible for all users. Also, it is recommended to have strong long passwords with high complexity.
References	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

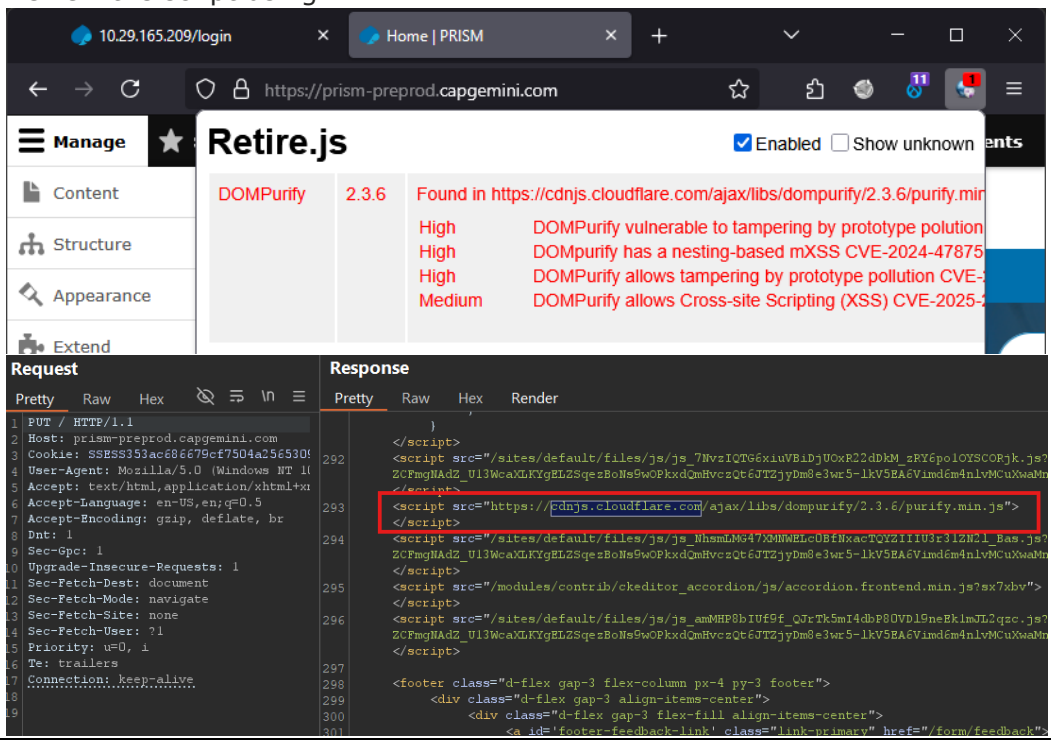
<table>
<tr><th>#2</th><th>SSH Access enabled for all users (CORP)</th></tr>
<tr><td>Affected components</td><td>10.29.165.255</td></tr>
<tr><td>Description</td><td>Allowing all CORP users to SSH into the Linux VM’s when access is not required introduces unnecessary risk by allowing users to access the devices terminal and exposing the environment to local-level vulnerabilities that could be used to escalate privileges/laterally move through the environment.</td></tr>
<tr><td>Severity</td><td>
<table>
<tr><th></th><th colspan="4">Probability</th></tr>
<tr><th rowspan="4">Impact</th><th></th><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><th>Low</th><td></td><td></td><td></td></tr>
<tr><th>Medium</th><td></td><td></td><td></td></tr>
<tr><th>High</th><td></td><td>High</td><td></td></tr>
</table>
</td></tr>
<tr><td>Authentication Required for Exploitation</td><td>Required</td></tr>
<tr><td>How to Test</td><td>SSH to host using CORP account. The screenshot below demonstrates that any Capgemini CORP domain users can SSH into host using their CORP credentials when connected to the internal network.
This provides access to many sensitive files that can be further used for exploitation.
 
</td></tr>
<tr><td>Recommendation</td><td>It is recommended to limit SSH access on the host to a limited number of approved accounts that require SSH access for maintenance and administration.</td></tr>
<tr><td>References</td><td>https://www.venafi.com/blog/best-practices-ssh-key-management-what-are-your-ssh-security-risks</td></tr>
</table>

#3	Vulnerable and Outdated Components – Drupal 10.3.9
Affected components	https://prism-preprod.capgemini.com/
Description	Detected Drupal Core version 10.3.9, which has the multiple vulnerabilities.

Severity	<table><tr><td rowspan="2"></td><td colspan="4">Probability</td></tr><tr><td rowspan="4">Impact</td><td></td><td>Low</td><td>Medium</td><td>High</td></tr><tr><td>Low</td><td></td><td></td><td></td></tr><tr><td>Medium</td><td></td><td></td><td></td></tr><tr><td>High</td><td></td><td>High</td><td></td></tr></table>
Authentication Required for Exploitation	Required
How to Test	**Drupal core** Drupal core 10.3.9 Recommended version: 10.4.7 (2025-May-08) Security update: 10.4.5 (2025-Mar-19) Security update: 10.3.14 (2025-Mar-19) Latest version: 10.5.0-beta1 (2025-May-25) Also available: 11.2.0-beta1 (2025-May-23)
Recommendation	Update Drupal Core to latest version.
References	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

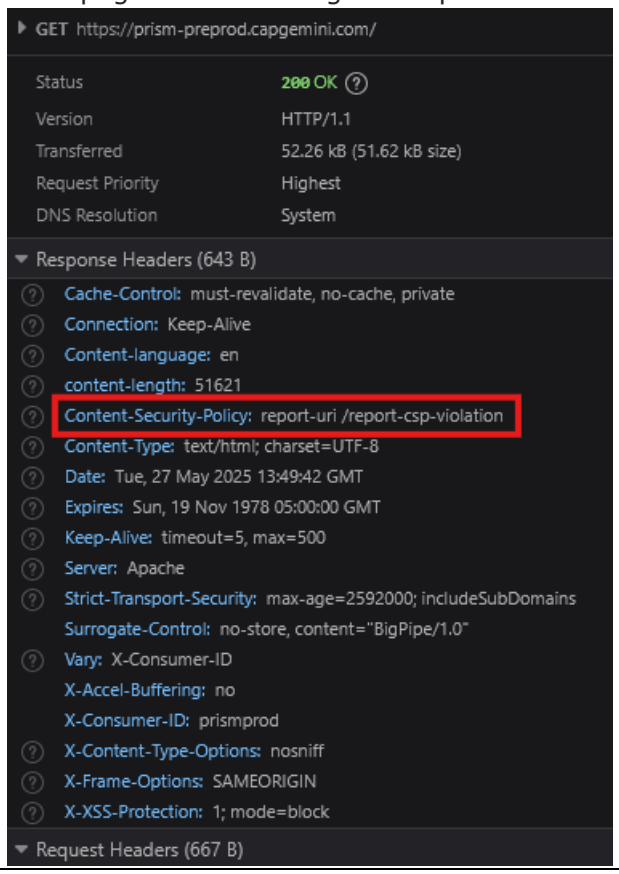
#4	Broken Authentication – Unauthorized access
Affected components	https://prism-preprod.capgemini.com/core/assets/vendor/ckeditor5/ckeditor5-dll/ckeditor5-dll.js https://prism-preprod.capgemini.com/libraries/ckeditor5-anchor-drupal/build/anchor-drupal.js https://prism-preprod.capgemini.com/modules/contrib/ckeditor_accordion/js/accordion.frontend.min.js https://prism-preprod.capgemini.com/modules/contrib/ckeditor_accordion/js/build/accordion.js https://prism-preprod.capgemini.com/modules/contrib/ckeditor_bidi/js/build/direction.js

<table>
<tr><td></td><td>https://prism-preprod.capgemini.com/modules/contrib/ckeditor_div_manager/js/build/divManagerPlugin.js
https://prism-preprod.capgemini.com/modules/contrib/ckeditor_emoji/js/build/emojiPlugin.js
https://prism-preprod.capgemini.com/modules/contrib/ckeditor_iframe/js/build/iframeembed.js
https://prism-preprod.capgemini.com/modules/contrib/ckeditor5_custom_paste/js/build/pasteFilter.js
https://prism-preprod.capgemini.com/modules/contrib/ckeditor5_dark_mode/js/build/darkMode.js
https://prism-preprod.capgemini.com/modules/contrib/ckeditor5_findandreplace/js/build/find-and-replace.js
https://prism-preprod.capgemini.com/modules/contrib/ckeditor5_fullscreen/js/build/fullscreen.js
https://prism-preprod.capgemini.com/modules/contrib/ckeditor5_line_height/js/build/ckeditor5_line_height.js
https://prism-preprod.capgemini.com/modules/custom/ckeditor5_image_map/js/build/ckeditor5_image_map.js</td></tr>
<tr><td>Description</td><td>The js files in the application do not require authentication. Broken authentication occurs when the web application has insecure authentication mechanism implemented. This can result in user’s accessing web application sensitive pages/files without any authentication which can be further misused. While some of these files are expected to be public (such as libraries for UI and styling), others may contain sensitive business logic or internal application functions, which could be exploited by an attacker.</td></tr>
<tr><td>Severity</td><td>
<table>
<tr><th></th><th colspan="4">Probability</th></tr>
<tr><th rowspan="4">Impact</th><th></th><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><th>Low</th><td></td><td></td><td></td></tr>
<tr><th>Medium</th><td></td><td>Medium</td><td></td></tr>
<tr><th>High</th><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Authentication Required for Exploitation</td><td>Not Required</td></tr>
<tr><td>How to Test</td><td>Close all active sessions and go to provided URL’s</td></tr>
<tr><td>Recommendation</td><td>The pages of the web application should be made accessible only when the requestor is authenticated. Analyze these files to confirm if they expose sensitive logic, credentials, or API endpoints.</td></tr>
<tr><td>References</td><td>https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/</td></tr>
</table>

<table>
<tr><th>#5</th><th>Vulnerable JavaScript dependency</th></tr>
<tr><td>Affected components</td><td>https://prism-preprod.capgemini.com/
https://cdnjs.cloudflare.com/ajax/libs/dompurify/2.3.6/purify.min.js</td></tr>
<tr><td>Description</td><td>Detected DOMpurify version 2.3.6, which has multiple vulnerabilities.</td></tr>
<tr><td>Severity</td><td>
<table>
<tr><th></th><th colspan="4">Probability</th></tr>
<tr><th rowspan="4">Impact</th><th></th><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><th>Low</th><td></td><td></td><td></td></tr>
<tr><th>Medium</th><td></td><td>Medium</td><td></td></tr>
<tr><th>High</th><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Authentication Required for Exploitation</td><td>Required</td></tr>
<tr><td>How to Test</td><td>Review the script using link
 
</td></tr>
<tr><td>Recommendation</td><td>Update all components to latest version.</td></tr>
<tr><td>References</td><td>https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities
https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/</td></tr>
</table>

<table>
<tr><th>#6</th><th>CSP header misconfiguration</th></tr>
<tr><td>Affected components</td><td>https://prism-preprod.capgemini.com/</td></tr>
</table>

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files. Properly configuring CSP directives helps control all content sources, significantly reducing the risk of attacks. It's crucial to always set restrictions for script-src and style-src as these directly impact XSS protection. 1. default-src Defines the default sources for all types of content (scripts, styles, images, etc.) if more specific directives are not set. Why it's important: Setting a default source ensures a base level of control for all resources, reducing the risk of loading unwanted content. 2. script-src Controls the sources for JavaScript. This is one of the most crucial directives for XSS protection. Why it's important: Limiting JavaScript sources is essential for blocking XSS attacks, which often exploit JavaScript injection vulnerabilities. 3. style-src Controls the sources for CSS styles. Why it's important: Inline CSS can also be a vector for XSS. Restricting sources for CSS helps mitigate this risk. 4. img-src Controls the sources for images. Why it's important: Restricting image sources can prevent the loading of images from untrusted domains, reducing the risk of content spoofing. 5. frame-src Controls the sources for embedded resources within iframes. Why it's important: Limiting iframe sources prevents content embedding from untrusted domains, protecting users from potentially harmful content. 6. frame-ancestors Specifies which sources are allowed to embed your site within frames. This is effective against clickjacking attacks. Why it's important: Setting frame-ancestors prevents unauthorized framing of your site, which is critical for protecting users from clickjacking. 7. object-src Controls sources for <object>, <embed>, and <applet> elements. Why it's important: Limiting object sources helps prevent the loading of potentially malicious plugins and other content, which can be exploited for XSS and other attacks. 8. worker-src Specifies sources for running Web Workers and Shared Workers. Why it's important: Restricting worker sources prevents unauthorized scripts from running in the background, enhancing security for complex applications. 9. form-action Specifies where forms are allowed to be submitted.

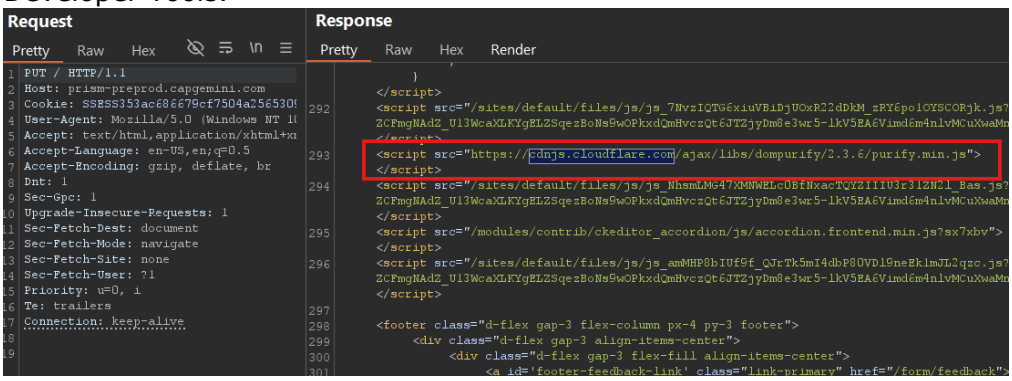
<table>
<tr><td></td><td>Why it’s important: Limiting form submission destinations prevents data from being sent to untrusted sources, reducing the risk of data theft.
10. upgrade-insecure-requests
Automatically upgrades all HTTP requests to HTTPS where possible.
Why it’s important: This directive improves security by enforcing HTTPS, protecting against man-in-the-middle attacks and data interception.</td></tr>
<tr><td>Severity</td><td>
<table>
<tr><th rowspan="2"></th><th colspan="4">Probability</th></tr>
<tr><th rowspan="4">Impact</th><th></th><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><th>Low</th><td></td><td></td><td></td></tr>
<tr><th>Medium</th><td>Low</td><td></td><td></td></tr>
<tr><th>High</th><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Authentication Required for Exploitation</td><td>Required</td></tr>
<tr><td>How to Test</td><td>View page headers using developer tool
 
</td></tr>
<tr><td>Recommendation</td><td>Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
It’s crucial to always set restrictions for script-src and style-src as these directly impact XSS protection, also “unsafe-eval” and “unsafe-inline” should not been used.</td></tr>
<tr><td>References</td><td>https://www.zaproxy.org/docs/alerts/10055-4/
https://www.zaproxy.org/docs/alerts/10055-5/
https://www.zaproxy.org/docs/alerts/10055-6/
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/</td></tr>
</table>

	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

#7	Cross-Domain JavaScript Source File Inclusion
Affected components	https://prism-preprod.capgemini.com/
Description	The page includes one or more script files from a third-party domain.
Severity	

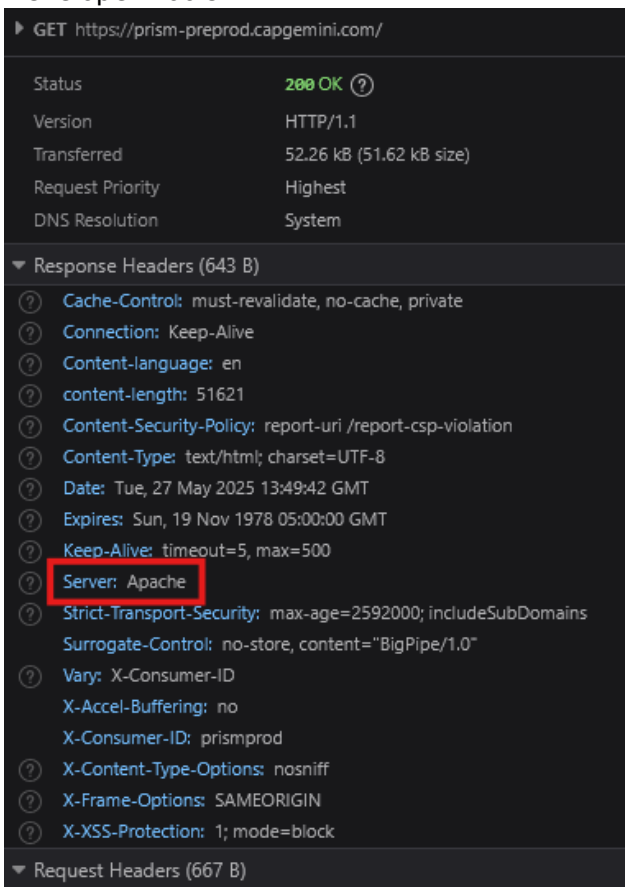
		Probability		
		Low	Medium	High
Impact	Low	Low		
	Medium			
	High			

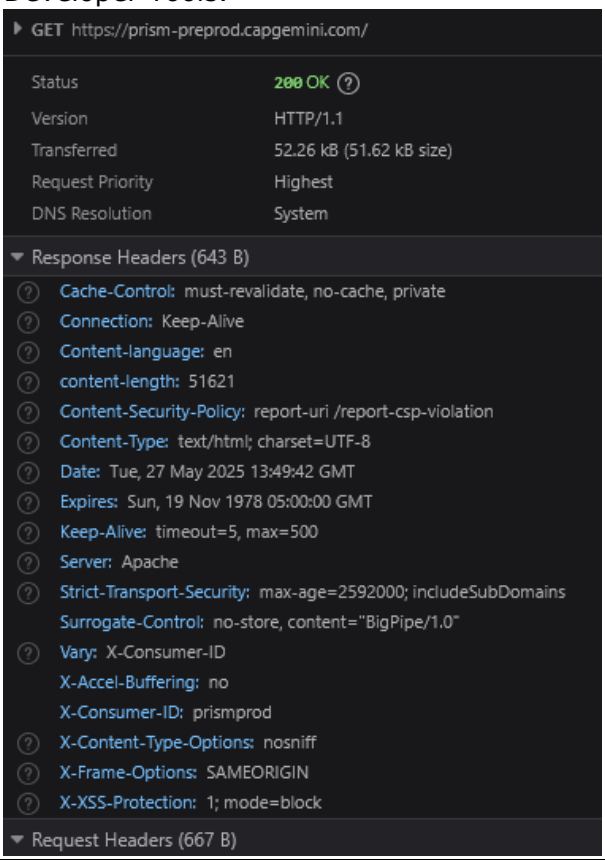
Authentication Required for Exploitation	Required
How to Test	Review the source page provided by the web through the Web browser's Developer Tools.



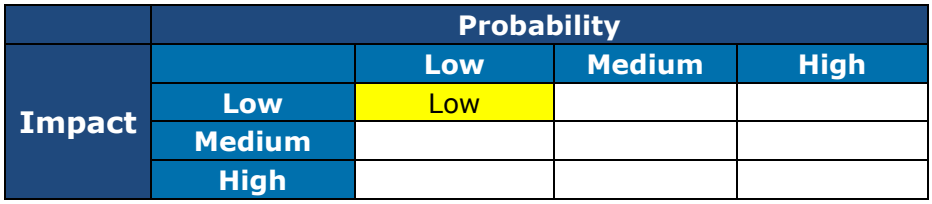
Recommendation	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
References	https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/

#8	Server Leaks Information via "Server HTTP Response Header Field(s)
Affected components	https://prism-preprod.capgemini.com/
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web

<table>
<tr><td></td><td>application is reliant upon and the vulnerabilities such components may be subject to.</td></tr>
<tr><td>Severity</td><td>
<table>
<tr><td rowspan="2"></td><td colspan="4">Probability</td></tr>
<tr><td rowspan="4">Impact</td><td></td><td>Low</td><td>Medium</td><td>High</td></tr>
<tr><td>Low</td><td></td><td></td><td></td></tr>
<tr><td>Medium</td><td>Low</td><td></td><td></td></tr>
<tr><td>High</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Authentication Required for Exploitation</td><td>Required od Not Required</td></tr>
<tr><td>How to Test</td><td>Review the headers provided by the web through the Web browser's Developer Tools.
 
</td></tr>
<tr><td>Recommendation</td><td>Ensure that your web server, application server, load balancer, etc. is configured to suppress "Server " headers.</td></tr>
<tr><td>References</td><td>http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html</td></tr>
</table>

<table>
<tr><th>#9</th><th>Permissions Policy Header Not Set</th></tr>
<tr><td>Affected components</td><td>https://prism-preprod.capgemini.com/</td></tr>
<tr><td>Description</td><td>Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.</td></tr>
<tr><td>Severity</td><td>
<table>
<tr><th></th><th colspan="4">Probability</th></tr>
<tr><th rowspan="4">Impact</th><th></th><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><th>Low</th><td></td><td></td><td></td></tr>
<tr><th>Medium</th><td>Low</td><td></td><td></td></tr>
<tr><th>High</th><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Authentication Required for Exploitation</td><td>Required</td></tr>
<tr><td>How to Test</td><td>Review the headers provided by the web through the Web browser's Developer Tools.
 
</td></tr>
<tr><td>Recommendation</td><td>Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.</td></tr>
</table>

References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy https://developers.google.com/web/updates/2018/06/feature-policy https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/

#10	Cached View of Logged Out Site
Affected components	https://prism-preprod.capgemini.com
Description	Browsers can store information for purposes of caching and history. Caching is used to improve performance, so that previously displayed information doesn't need to be downloaded again. History mechanisms are used for user convenience, so the user can see exactly what they saw at the time when the resource was retrieved.
Severity	
Authentication Required for Exploitation	Required
How to Test	After logging out of the application, click the "back" button in the browser and see if the browser still caches the information in the web application.
Recommendation	Setting Cache-Control: must-revalidate
References	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses

3. Risk Correlation

This chapter contains an overview of classified findings and describes the risks between the identified vulnerabilities.

3.1. Overview of Classified findings

.

#	Vulnerability	Severity
1	Sensitive Information Disclosure –Private Key	Critical
2	SSH Access enabled for all users (CORP)	High

3	Vulnerable and Outdated Components – Drupal 10.3.9	High
4	Broken Authentication – Unauthorized access	Medium
5	Vulnerable JavaScript dependency	Medium
6	CSP header misconfiguration	Low
7	Cross-Domain JavaScript Source File Inclusion	Low
8	Server Leaks Information via "Server HTTP Response Header Field(s)	Low
9	Permissions Policy Header Not Set	Low
10	Cached View of Logged Out Site	Low

4. Conclusion and Recommendations

4.1. Conclusions

During the assessment multiple vulnerabilities were identified which pose a **'Critical'** risk to the users and data of the PRISM application environment from an insider perspective.

Based on the findings, the penetration testing team concludes that the PRISM environment security level can be improved to guarantee the confidentiality, integrity and availability of data and the users' digital safety. Furthermore, the identified vulnerabilities could indirectly damage Capgemini via reputational damage or fines (AVG/GDPR). Therefore, the penetration testing team recommends fixing the identified issues.

4.2. Recommendations

Based on the risks arising from the identified vulnerabilities we make the following recommendations:

- Files containing sensitive information like plaintext passwords should be not be accessible for all users.
- It is recommended to limit SSH access on the host to a limited number of approved accounts that require SSH access for maintenance and administration.
- Update Drupal Core to latest version.
- The pages of the web application should be made accessible only when the requestor is authenticated.
- Update all components to latest version.
- Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
- Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
- Ensure that your web server, application server, load balancer, etc. is configured to

suppress "Server " headers.

- Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
- Setting Cache-Control: must-revalidate

Overview and Baseline

Determining a cybersecurity baseline to reduce cyber risks is tailor-made as the needs are different for every organization. One of the reasons is that unnecessary costs for implementing measures should be avoided. Furthermore, some company properties may require protection. For this reason, when determining a security baseline for each company property, it is necessary to analyze what degree of protection is required. The most crucial company properties are called "crown jewels". It is essential to be always clear what the crown jewels are for your organization. It can then be determined where they are located, which people have access to them and for what reason. This information helps to identify the associated cyber risks. When taking measures, it is therefore important to maintain the right balance between the costs, the level of protection and the risk appetite of the organization. To define the appropriate security baseline (with security measures) for your organization, use can be made of security "good practices" such as ISO 27002, ISF Standard of Good Practice and NIST Cyber Security Framework. Also, the acceptable practices measures can be supplemented with findings from the risk analyses performed. Based on the information mentioned above, you can define the generic security baseline for your organization.

Awareness

In the area of cybersecurity, the human factor is often the weakest link. This means that human error by employees leads to risky situations. Although technical measures can be taken to limit risks, it is also essential to pay attention to the human factor. A technical measure, such as an enforced password policy, can help implement strong passwords. However, this does not guarantee that passwords cannot be guessed by an attacker. Without the right knowledge, employees can sometimes adhere to the enforced rules but still make choices that lead to a password easily cracked by a hacker. We, therefore, recommend training employees periodically in the area of awareness. This can, for example, be done with the help of target group-specific awareness training (e-learning) and phishing simulations. Risks can also be limited by drawing up a Fair Use Policy which contains rules for the careful handling of data. This will reduce the number of risks due to the human factor. In addition, your security organisation must entirely focus on making the security functionalities in IT systems and IT facilities "more human-friendly". Think of applying fingerprint scanning for access or standard encryption of all e-mails. By making the security functionalities more human-friendly, your employees' motivation to use these security functionalities is strengthened.

Periodic testing of measures

Due to dynamic IT landscapes and constant cybersecurity developments, maintaining and increasing the cybersecurity level is a continuous process. It is therefore recommended to test the measures taken periodically for both technical and non-technical "operation" of the measures. This is to determine improvement potential and, where necessary, to improve existing measures or to implement new measures. On a non-technical level (for example, security processes), one can think of conducting interviews throughout the organization, at specific functions and roles or at certain business units where cybersecurity is of great importance. When conducting this fieldwork, it is tested to what extent the organizational structure and its employees can respond adequately to incidents. On a technical level, more could be thought of conducting code reviews or penetration tests. With the help of code reviews, vulnerabilities in an application's code can be identified to resolve it at an early stage. Penetration testing simulates a possible attack by hackers to expose vulnerabilities in a system, network, or application. All these periodic testing methods can form the basis for a plan to keep the security level up to date.

Detection and response

To adequately limit cybersecurity risks, measures must be taken throughout the chain of prevention, detection, and response. Due to the ever-changing IT landscape and the rapid developments in cybersecurity, there is no such thing as completely safe. Sooner or later, they will find a way to access systems and data. To limit the risks as much as possible, your organization must be able to detect such an incident and respond to it appropriately. By implementing or improving detection and response capabilities, such as network monitoring or training employees by incident response training, your organization can identify potential threats at an early stage. This will limit the potential impact of cyber risks as much as possible because the action can be taken before the damage suffered is significant for your organization.

Governance

A well-considered governance structure can form your organization's foundation to realize the IT strategies set up to support your organizational goals. This, therefore, also applies to the achievement of your security strategies. The governance structure can align the security strategy of your organization with the overall business strategy and organizational culture. In this way, driving forces for your organization, such as the need for flexibility and innovation, can be limited to the right degree to remain secure. In addition, a good governance structure brings peace and overview to your employees by clearly placing responsibilities in the right place. For example, the understanding of these responsibilities and communication between internal and external stakeholders will be made more flexible by reducing mutual misconceptions as much as possible. A good governance structure ensures that the resources of your organization are deployed as efficiently as possible without losing sight of the associated risks and responsibilities. In this way, a good governance structure ensures that your security strategy supports your general business objectives.

Partners

Unfortunately, it often happens that a partner organization or a third party is the source of a cyber-incident. This can lead to unexpected costs, reputational damage, or a weakened business relationship with the relevant partner organization. This can be due to several factors. For example, IT suppliers may sometimes be provided with an account with more rights than they need. They can also be granted access to sensitive data without knowing whether the relevant supplier is also handling data safely.

For this reason, we recommend that you assess the associated risks for each new partnership and continue to review them periodically thereafter. This can be done, for example, by requesting certifications, such as ISO 27001, or by looking critically at the rights that they are granted. By identifying all risks that arise from working with partner organizations, these can also be carefully and adequately reduced. To gain insight into the security status of your partners, we advise you to make concrete agreements with your partners about taking cybersecurity measures and how your organization will monitor your partners.

Hardening of systems

Hardening guidelines (benchmarks) can be used for the safe configuration (hardening) of systems. Such guidelines are available on the URL below for Linux, Microsoft Windows, and various web server software such as Apache. If no standard hardening documentation is available, we advise you to possibly develop this together with your supplier.

https://www.cisecurity.org/cis-benchmarks/

About Capgemini

Capgemini is a global leader in consulting, digital transformation, technology and engineering services. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year+ heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. Today, it is a multicultural company of 270,000 team members in almost 50 countries. With Altran, the Group reported 2019 combined revenues of €17billion.

Learn more about us at

www.capgemini.com

People matter, results count.