Security advisory

Multiple vulnerabilities in the DSKNet Intranet web application

Affected versions before 2.20.137.1

July, 2022

CVE-2022-24688
CVE-2022-24689
CVE-2022-24690
CVE-2022-24691
CVE-2022-24692
Release date: 15/07/2022
Department: POST Cyberforce
Roman Zakharov

Vulnerabilities summary

Product	DSKNet Intranet web application
Product homepage	https://dsk.lu/fr/produits/temps-de-presence
Affected product versions	before 2.20.137.0
MITRE ATT&CK	T1190, T1078, T1110, T1189, T1185, T1059, T1505.003
Workaround	Partially provided
Fixed product versions	2.20.137.1

Vulnerability	Broken access control
CVE ID	CVE-2022-24689
Severity	High: CVSS v3.1 base score - 7.5
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
OWASP	OWASP 2021-A1
CWE	CWE-732

Vulnerability	Unauthenticated SQL injection
CVE ID	CVE-2022-24690
Severity	Critical: CVSS v3.1 base score - 9.3
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N
OWASP	OWASP 2021-A3
CWE	CWE-89

Vulnerability	Multiple authenticated SQL injection
CVE ID	CVE-2022-24691
Severity	High: CVSS v3.1 base score - 8.5
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N
OWASP	OWASP 2021-A3
CWE	CWE-89

Vulnerability	Stored Cross-site scripting
CVE ID	CVE-2022-24692
Severity	Medium: CVSS v3.1 base score - 6.9
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:N
OWASP	OWASP 2021-A3
CWE	CWE-79

Vulnerability	Arbitrary file upload
CVE ID	CVE-2022-24688
Severity	High: CVSS v3.1 base score - 7.2
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
OWASP	OWASP 2021-A5
CWE	CWE-434

Exploitation impact:

- Unauthorized access
- Sensitive information disclosure
- Admin/User accounts takeover
- Remote code execution

Timeline

Date	Action
04 February 2022	Vulnerabilities identification, exploitation, and impact validation
07 February 2022	The vendor was notified and advised on mitigation actions
08 February 2022	The vendor acknowledged the vulnerabilities
09 February 2022	CVE-2022-24688 -> CVE-2022-24692 were assigned by MITRE
09 February 2022	The vendor was informed about assigned CVE IDs
09 February 2022	CIRCL was informed about assigned CVE IDs
09 February 2022	POST CSIRT was team informed about assigned CVE IDs
18 February 2022	Received an update from vendor, the COS team tested the updated version, not all vulnerabilities are fixed
11 March 2022	The vendor published a new release 2.20.137.1 addressing the issues
15 July 2022	Advisory publicly released by POST Cyberforce

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24688
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24689
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24690
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24691
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24692
- https://github.com/post-cyberlabs/CVE-Advisory/blob/main/CVE-2022-24688-92.pdf
- https://attack.mitre.org/techniques/T1190/
- https://attack.mitre.org/techniques/T1078/
- https://attack.mitre.org/techniques/T1110/
- https://attack.mitre.org/techniques/T1189/
- https://attack.mitre.org/techniques/T1185/
- https://attack.mitre.org/techniques/T1059/
- https://attack.mitre.org/techniques/T1505/003/
- https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- https://owasp.org/Top10/A03_2021-Injection/
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://cwe.mitre.org/data/definitions/79.html
- https://cwe.mitre.org/data/definitions/89.html
- https://cwe.mitre.org/data/definitions/732.html
- https://cwe.mitre.org/data/definitions/434.html

Product description

The DSKNet intranet application allows the employees to access their presence data:

- DSKNet offers interactive access to employee's presence time data from any extension connected to your network. Use is possible internally and from outside, on any computer or mobile. The interface is compatible with the main browsers including Internet Explorer, Firefox, Safari, or Google Chrome.
- Modular architecture allows selecting the features to be used.

More information can be found by visiting the product webpage:
https://dsk.lu/fr/produits/temps-de-presence.

Advisory

Several security vulnerabilities were discovered in the DSKNet web application that can be chained to achieve the Remote Code Execution as the webserver user. The affected application versions are before 2.20.137.1.

The broken access control allows unauthenticated attackers to access the application's endpoints that disclose information about users' full names, badge numbers, departments, emails, and including their personal data such as Luxembourgish "matricule". The attacker can get unauthorized access to the application by brute-forcing the badge PIN code. Some user accounts have the "default" PIN code configured that simplifies the brute-force attack.

Multiple endpoints are vulnerable to the blind SQL injection attack that can be executed by unauthenticated and authenticated users. This attack simplifies the process to get the highest privileges within the application in order to proceed with the next vulnerability exploitation.

Discovered Stored Cross-site Scripting (XSS) permits delivering the end-user malicious code, stealing their cookies, and/or keeping access to the application after the user's PIN code changes. This XSS attack was abused to deliver malicious code and achieve client-side code execution. The exploitation requires user privileges with access to a specific configuration page.

To achieve Remote Code Execution the attacker requires to hijack a user with access to the specific configuration page. There are at least 3 ways to achieve that:

- Abuse broken access control to discover the user's badge number and conduct a brute-force attack to find the user with desired access.
- Abuse broken access control and conduct SQL injection attack that does not require authentication.
- Abuse regular user access and conduct authenticated SQL injection attack to discover badge number and PIN code for the user with access to the specific page.

To achieve Remote Code Execution the attacker abuses the specific menu configuration by uploading the malicious file (mimicking PDF) and enabling displaying the PDF for touch devices. By visiting the URL for the "Touch" devices the uploaded file is placed in the special web folder resulting in Remote Code Execution on the webserver.

Possible attacks schema

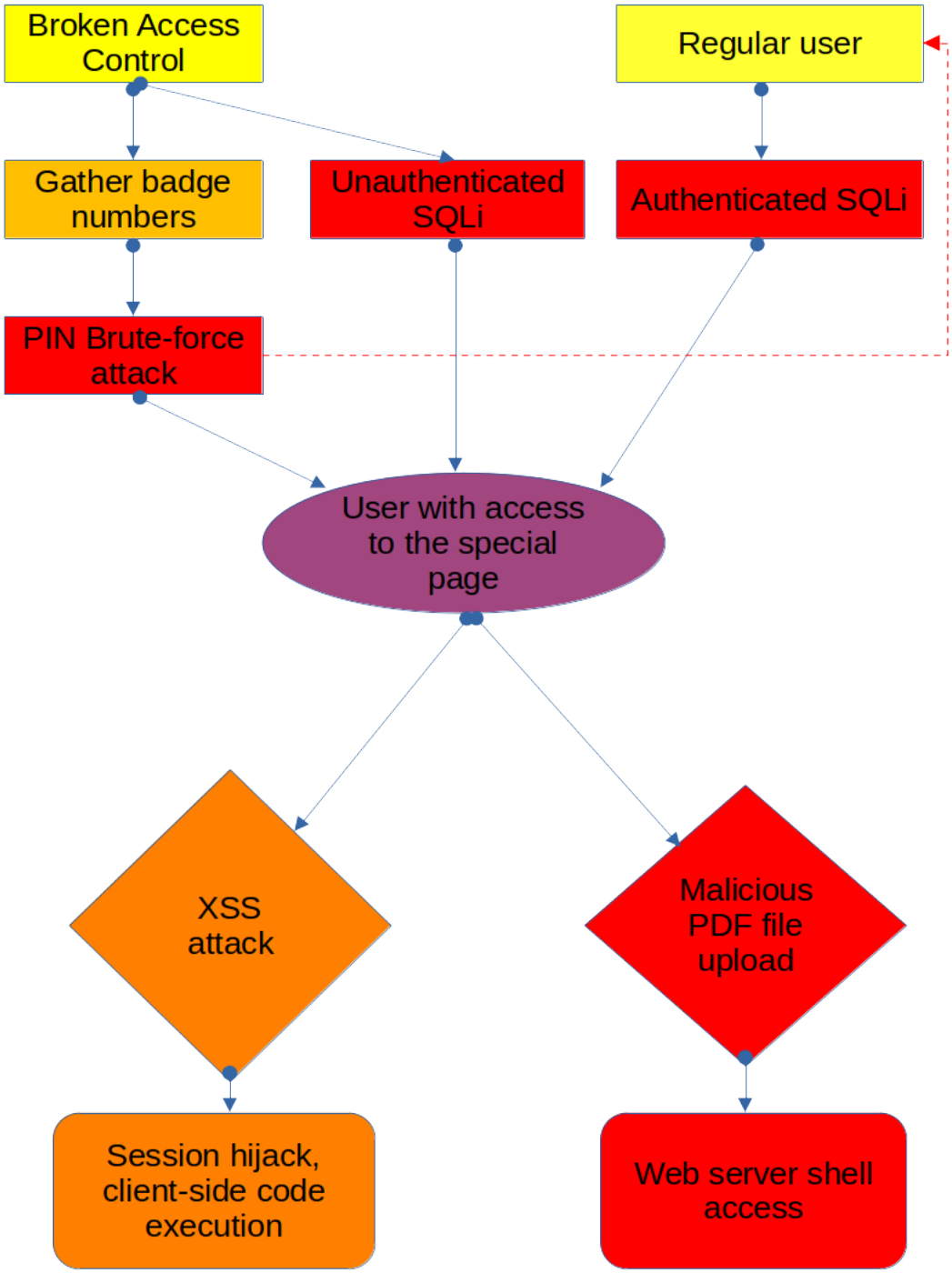

Figure 1: Attacks schema abusing discovered vulnerabilities

CVE-2022-24689: Broken access control vulnerability

Broken access control allows a remote attacker to access account information pages including personal data without being authenticated. The collected information includes the badge numbers that operate as user login name and has a PIN code.

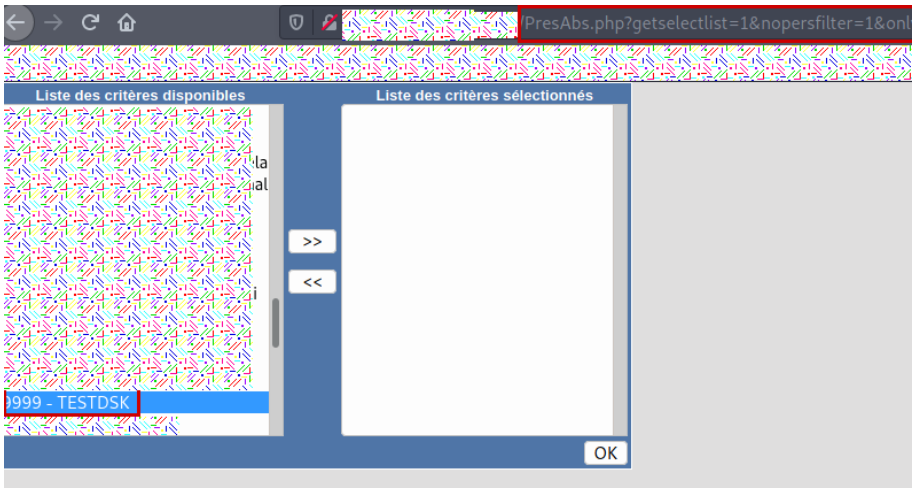

Figure 2: An example of the badge numbers gathering for a non-authenticated attacker

Figure 3: An example of the ”matricule” gathering for a non-authenticated attacker

Vulnerable endpoint:

GET /PresAbs.php HTTP/1.1

Vulnerable parameter:

nopersfilter

Proof of concept

GET /PresAbs.php?getselectlist=1&nopersfilter=11&onlyactivpers=0&onofffiltrevisu=0&filtrestatus=1&controllist=0menubar=no,status=no,scrollbars=no

The parameter ”nopersfilter” can be manipulated to collect different data from the application.

Remediation

Ensure to validate the user’s session before granting access to the application’s functional endpoints.

Reference

https://owasp.org/Top10/A01_2021-Broken_Access_Control/#how-to-prevent

CVE-2022-24690: Unauthenticated SQL injection

An improper neutralization of special elements used in an SQL Command ("SQL Injection") vulnerability in the DSKNet application allows an unauthenticated attacker to taint database data and extract sensitive information via crafted HTTP requests.

The type of SQL Injection is "blind boolean based". The unauthenticated attacker can discover the endpoint by abusing the Broken Access Control vulnerability with further exploit SQL injection attacks to gather all user's badge numbers and PIN codes.

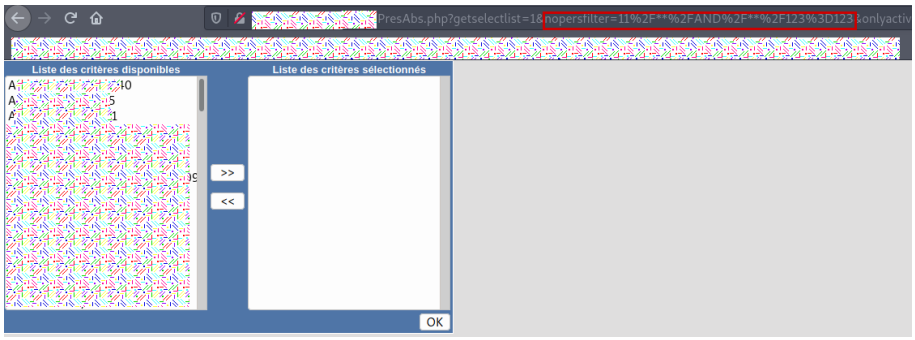

Figure 4: The truthful boolean expression submitted by the non-authenticated attacker shows the data

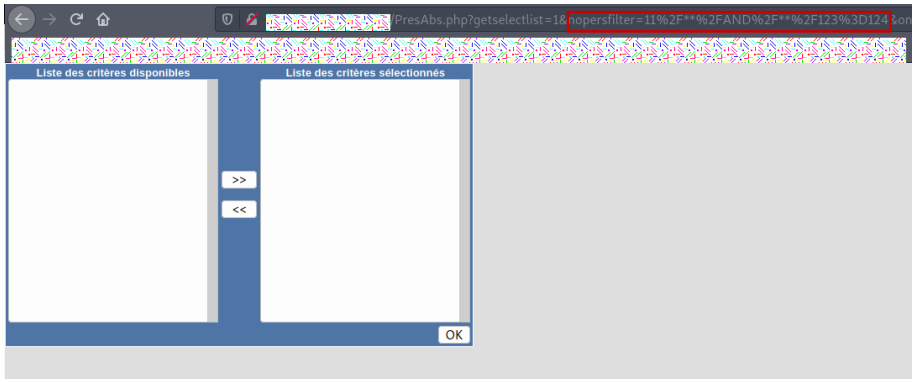

Figure 5: The false boolean expression submitted by the non-authenticated attacker shows no data

Vulnerable endpoint and parameter:

GET /PresAbs.php HTTP/1.1

Vulnerable parameter: nopersfilter

Proof of concept

GET /PresAbs.php?getselectlist=1&nopersfilter=11%2F**%2FAND%2F**%2F123%3D123&onlyactivpers=0&onofffiltrevisu=0&filtrestatus=1&controllist=1&menubar=yes,status=yes,scrollbars=no

GET /PresAbs.php?getselectlist=1&nopersfilter=11%2F**%2FAND%2F**%2F123%3D124&onlyactivpers=0&onofffiltrevisu=0&filtrestatus=1&controllist=1&menubar=yes,status=yes,scrollbars=no

The parameter ”nopersfilter” should return correct data before using this Proof of concept.

Remediation

- Use PDO with strongly typed parameterized queries
- Use of Stored Procedures
- Sanitize and escape user-supplied input

Reference

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

CVE-2022-24691: Multiple authenticated SQL injection

An improper neutralization of special elements used in an SQL Command (”SQL Injection”) vulnerability in the DSKNet application allows an unauthenticated attacker to taint database data and extract sensitive information via crafted HTTP requests.

The type of SQL Injection is ”blind boolean based”.

Vulnerable endpoints and parameters:

- GET /ListStat.php HTTP/1.1
- GET /PresAbs.php HTTP/1.1
- GET /CgeListall.php HTTP/1.1
- GET /PlanGraphCompact.php HTTP/1.1
- GET /RecapCge.php HTTP/1.1
- GET /Trombinoscope.php HTTP/1.1

Vulnerable parameters:

- selectionfpc
- nopersfilter
- lst**** parameter pattern

Proof of concept

GET /ListStat.php?fposted=1&cleared=0&quickview=0&filtrestatus=&lstaccount=&lstterminal=&lstworksite=&fperiode_du=01%2F01%2F2022&fperiode_au=31%2F01%2F2022&mode=fpc&selection2=&selection1=&selection4=&selection9=&selection5=&selection13=&selectionfpc=(CostCenter.CodeCostCenter)+IN+(1)+AND+1=1&f_tri1=&f_tri2=&f_tri3=&fperiode_btn=OK

GET /ListStat.php?fposted=1&cleared=0&quickview=0&filtrestatus=&lstaccount=&lstterminal=&lstworksite=&fperiode_du=01%2F01%2F2022&fperiode_au=31%2F01%2F2022&mode=fpc&selection2=&selection1=&selection4=&selection9=&selection5=&selection13=&selectionfpc=(CostCenter.CodeCostCenter)+IN+(1)+AND+1=2&f_tri1=&f_tri2=&f_tri3=&fperiode_btn=OK

The vulnerable parameter ”selectionfpc” should return correct data before using this Proof of concept.

Remediation

- Use PDO with strongly typed parameterized queries
- Use of Stored Procedures
- Sanitize and escape user-supplied input

Reference

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

CVE-2022-24692: Stored Cross-site scripting

The ”new menu” option within the special page is vulnerable to stored XSS. The attacker can create the menu option, make it visible to every application’s user, and conduct session hijacking, account takeover, or delivering malicious code with the final goal to achieve client-side code execution.

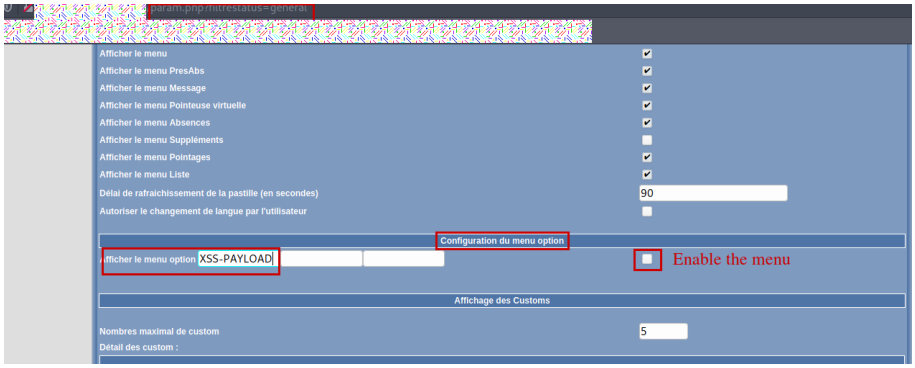

Figure 6: The place to inject JavaScript payload

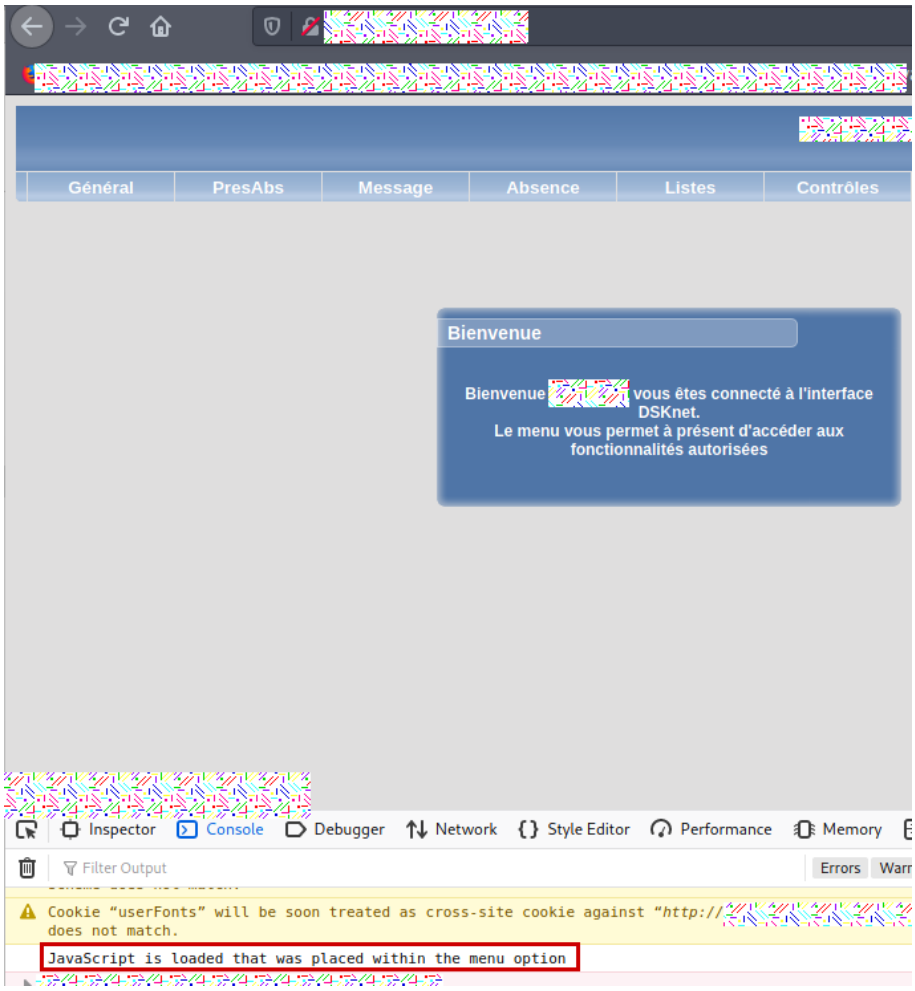

Figure 7: Injected JavaScript console.log output as a Proof of concept

Vulnerable endpoint:

POST /param.php?filtrestatus=general HTTP/1.1

Vulnerable parameter:

menuoptioncaption1

Proof of concept payload:

Update<BODY ONLOAD=eval(atob('Y29uc29sZS5sb2coJ3hzcy1wb2MnKQo='))>

Remediation

- Filter user-supplied input
- HTML Encode Before Inserting Untrusted Data into HTML Element Content
- Implement Content Security Policy

References

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

CVE-2022-24688: Arbitrary file upload

The ”Touch” settings allow unrestricted file upload (and consequently Remote Code Execution) via PDF upload with PHP content and ”PHP” extension. The attacker should hijack or obtain ”privileged” user access to the ”Parameters” page in order to exploit this issue which can be easily achieved by exploiting the Broken Access Control with further Brute-force attack or SQL Injection.

The uploaded file is stored within the database and copied to the specific web folder if the attacker visits a special page. The file is copied if the ”show the PDF” menu option is enabled.

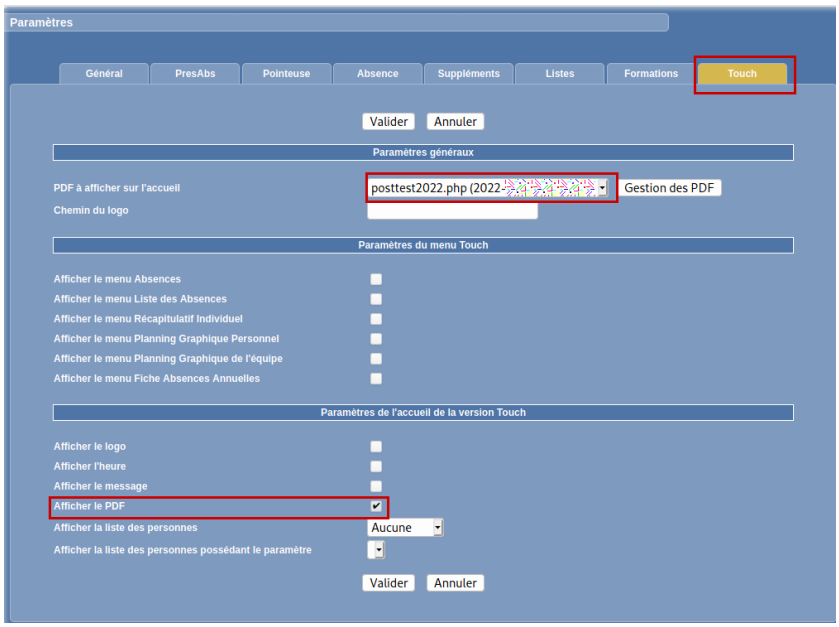

Figure 8: Uploaded php file and enabled menu option

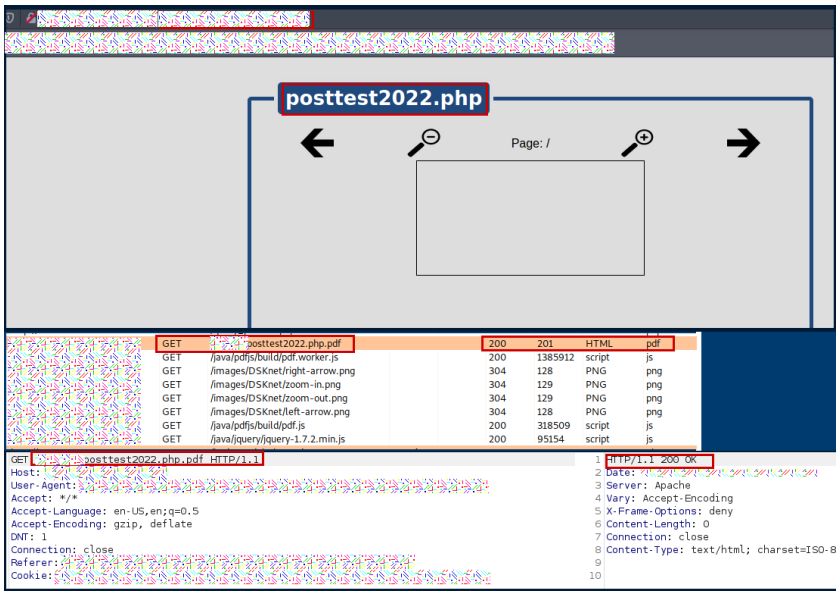

Figure 9: Visiting loginspecial page and identified the location of the ”PDF” file

Figure 10: Achieving remote code execution

Vulnerable endpoint:

POST /selpdfupload.php HTTP/1.1

Vulnerable parameters:

pdfname (uploaded filename)

pdfdata (malicious file content)

Proof of concept payload:

The simple php file containing ”<?php phpinfo(); ?>” can be used for Proof of Concept.

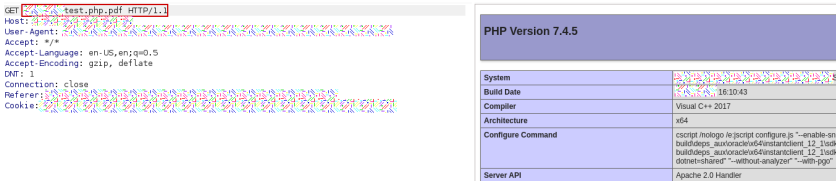

Figure 11: phpinfo proof of concept

Remediation

- Implement input validation before validating file extensions
- Ensure that files with double extensions (e.g. ”file.php.pdf) cannot be executed especially in Apache
- Ensure to validate uploaded file type, do not trust the ”Content-Type” header
- Ensure to change the filename to randomly generated

References

https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Recommendation

Contact DSK Systems S.A. to receive an updated version.

Workaround

Before receiving the updated version we advise placing the application behind the VPN solution.

Please consider taking these additional actions to reduce the risk of exploitation:

- Disable PIN code authentication.
- Ensure that application' users use strong passwords.
- Place the Web Application Firewall in front of the application and configure extensive checks for the affected endpoints.