

## Header Injection Vulnerability in Prestashop

**Title:** Header Injection Vulnerability in Prestashop  
**Release Date:** 2011/11/22  
**Vulnerable Application:** Prestashop (ver. 1.4.4.1)  
**Type:** Header Injection  
**Level:** Low (Low/High/Critical)  
**CVSS:** 4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)

**Dognædis Ref.:** DGS-SEC-7  
**CVE Ref.:** CVE-2011-4545  
**Other Ref.:**  
**Discover Credits:** CodeV - Code Analyzer  
**Bulletin Author(s):** RGouveia  
**Contact:** irt@dognædis.com

**Nível de Acesso do Documento:** Público

A informação expressa neste documento é propriedade da Dognædis. Pode ser, no entanto, lida, copiada, distribuída, impressa ou acedida por qualquer pessoa ou entidade, desde que os créditos da Dognædis sejam respeitados.

**Document Access Level:** Public

The information expressed in this document is property of Dognædis. Although can be disclosed, distributed, copied, read, used, printed or accessed by anyone, since all the Dognædis credits are respected.

### Overview:

PrestaShop is an e-commerce solution which is free for the basic kernel and open source. It supports payment gateways such as Google checkout, Paypal or payments pro via APIs.

### Scope:

**File:** /admin/displayImage.php

**Vulnerable Argument(s):** \$\_GET['name']

**Code:**

```
line 34: header('Content-Disposition: attachment; filename="'. $_GET['name'] .'.jpg');
```

**Proof(s) of Concept:**

GET:

```
http://<app_base>/admin/displayImage.php?img=<name_of_existing_file_in_md5_format>&name=asa.cmd"%0d%0a%0d%0a@echo off%0d%0aecho running batch file%0d%0apause%0d%0aexit
```

Note: The <name\_of\_existing\_file\_in\_md5\_format> is the name of one file existing on the "upload/" folder. It's name must be a MD5 hash, without any extension. ex: "435ed7e9f07f740abf511a62c00eef6e"

### Description:

The referred vulnerability could be exploited through a Header Split Injection.

This vulnerability could be exploited, leading the victim's browser to download an harmful script.

This may allow the attacker to send a remote shell or backdoor to the victim's computer.

This vulnerability is only exploitable on PHP versions prior to 4.4.2 and 5.1.2. Later versions prevent header split injection by limiting each header to a single line.

### Impact:

Generally, by using this kind of exploit, might be possible to send harmful scripts to the victim's computer.

### Resolution:

Aiming a correct resolution of the identified vulnerability, the data obtained through the \$\_GET['name'] input argument should be properly sanitized for HTML usage.

### Official Solution:

At the moment, there is no official solution for the reported vulnerabilities.

### External References:

[https://www.owasp.org/index.php/HTTP\\_Response\\_Splitting](https://www.owasp.org/index.php/HTTP_Response_Splitting)

<http://projects.webappsec.org/w/page/13246931/HTTP%20Response%20Splitting>

[http://en.wikipedia.org/wiki/HTTP\\_response\\_splitting](http://en.wikipedia.org/wiki/HTTP_response_splitting)



DOGNÆDIS

---

TRUSTABLE SOLUTIONS