Detecting Usernames Through Abuse of Functionality Vulnerabilities - Websecurity (English translation)

Виявлення логінів через Abuse of Functionality уразливості - Websecurity - Author not stated, websecurity.com.ua.

- Title in English: Detecting Usernames Through Abuse of Functionality Vulnerabilities - Websecurity
- Published: date not stated
- Original: <http://websecurity.com.ua/2840/>
- Preserved from: http://websecurity.com.ua/2840/ (live) on 2026-08-09
- Licence: unknown

Content (translated into English)

Machine translation of `websecurity-com-ua-abuse-functionality-websecurity.md`, which holds the source's own words. Code, payloads, type names, URLs and CVE identifiers were masked before translating and restored after, so they are byte-identical to the original.

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Detecting Usernames Through Abuse of Functionality Vulnerabilities - Websecurity - Web Security

---

Detecting Usernames Through Abuse of Functionality Vulnerabilities

22:46 30.01.2009

Over the past few years, I have encountered many times a feature on some websites (primarily email services and large projects) that makes it possible to check whether a given username is available. This allows a user to create a unique username when registering on the website. And so, in March 2008, when I developed my Brute force login identifier program (for discovering usernames, something I have to deal with during security audits), I decided to conduct a detailed study of the username-checking feature.

This feature allows an attacker to discover valid usernames in the system (login enumeration). In other words, the presence of this feature on a website gives rise to an Abuse of Functionality

vulnerability. I have provided examples of similar vulnerabilities, in particular, on hulu.com and on www.youtube.com.

Let us examine the algorithm for discovering a username on YouTube.

If you enter the username being checked in the Username field of the registration form (http://www.youtube.com/signup) and click Check Availability, the system will perform a check and provide a response (this feature is implemented using AJAX). If the response is “Username unavailable,” that username exists in the system; if the response is “Username available!”, that username does not exist in the system.

Thus, you need to check a list of usernames using the Check Availability feature and select those for which the response is “Username unavailable.” You can then create a list of valid usernames.

If this feature has no protection against automated attacks (that is, if there is an Insufficient Anti-automation vulnerability), as is the case most of the time, it allows automated discovery of usernames in the system. This can be done using username brute-forcers, for example, my Brute force login identifier program. The usernames discovered can subsequently be used to determine the passwords of the website's users.

This entry was posted on 22:46 30.01.2009 and is filed under Articles. You can follow any responses to this entry through the RSS 2.0 feed.

Leave a Reply

You must be logged in to post a comment.
