

AT A GLANCE

Classification Boundary Condition Error Resource /loginAction Parameter Method POST Risk

REQUEST

POST /loginAction [username=-2147483649 password=vega]

DISCUSSION

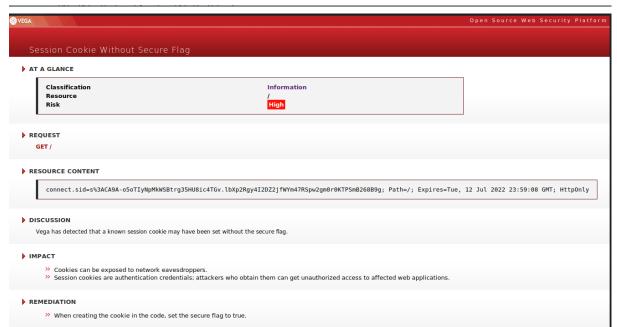
Integer overflows occur when integer data types exceed their maximum value. When this occurs in programs written in languages such as C. the resulting behavior can have security implications. In these cases, unsigned integers will be reduced, wrapping back to a lower numeric value. The potential impact on security depends on how the integer value is used. If it is used as the size of a data buffer, forcing it to wrap to a lower value may result in bypassing of size checks, introducing possible buffer overflow conditions.

- Integer overflow errors can have a variety of impacts, depending on the context and the purpose of the integer value.
 Integers used to check the size of a data buffer, if reduced, can incorrectly represent the total amount of data, resulting in a possible buffer overflow.

REMEDIATION

>> The developer should investigate the error and determine if a vulnerability is present.

REFERENCES



AT A GLANCE

Boundary Condition Error /loginAction Classification Resource Parameter username Method POST

POST /loginAction [username=-2147483648 password=vega]

DISCUSSION

Integer overflows occur when integer data types exceed their maximum value. When this occurs in programs written in languages such as C, the resulting behavior can have security implications. In these cases, unsigned integers will be reduced, wrapping back to a lower numeric value. The potential impact on security depends on how the integer value is used. If it is used as the size of a data buffer, forcing it to wrap to a lower value may result in bypassing of size checks, introducing possible buffer overflow conditions.

IMPACT

- Integer overflow errors can have a variety of impacts, depending on the context and the purpose of the integer value.
 Integers used to check the size of a data buffer, if reduced, can incorrectly represent the total amount of data, resulting in a possible buffer overflow.

REMEDIATION

>> The developer should investigate the error and determine if a vulnerability is present.

REFERENCES

Scan Info

AT A GLANCE

Classification Resource /loginAction Parameter Method password POST Risk

REQUEST

POST /loginAction [username=anyone98@hotmail.com password=vega"`true`"]

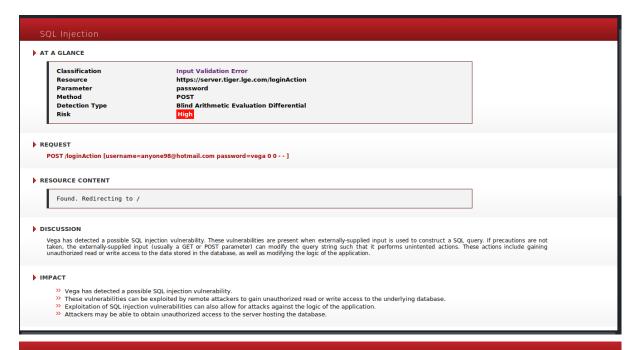
DISCUSSION

Command injection vulnerabilities often occur when inadequately sanitized externally supplied data is as part of a system command executed through a command interpreter, or shell. Vulnerabilities such as these can be exploited by using shell metacharacters to run additional commands that were not intended to be executed by the application developer. The system() function, and derivatives, are often responsible, as these functions are very simple to use. These vulnerabilities can grant remote access to attackers, if exploited successfully.

- No Vega has detected a possible command injection vulnerability.
 Attackers may be able to run commands on the server.
 Exploitation may lead to unauthorized remote access.

REMEDIATION

- >> Developers should examine the code corresponding to the page in detail to determine if the vulnerability exists.
- Execution of system commands through a command interpreter, such as with system(), should be avoided.
 If absolutely necessary, the developer should take extra care with validating the input before it is passed to the interpreter.



AT A GLANCE

Classification	Information	
Resource	1	
Risk	Low	

REQUEST

GET /

▶ RESOURCE CONTENT

anyone98@hotmail.com

Vega has found patterns that resemble e-mail addresses in scanned content. These may be user the addresses of system users, addresses inserted in user-supplied content, or third-party addresses embedded in components of the application (such as Javascript libraries). Automatically scraping websites is one way that spammers and phishers collect e-mail addresses for their distribution lists. It is recommended that e-mail addresses not be displayed on exposed parts of the web application, directly or indirectly.

- E-mail addresses exposed to the Internet will be scraped by spambots and added to spam lists.
 E-mail addresses can also be used in targeted and phishing attacks.
 E-mail addresses could be used to more accurately guess application usernames.

VEGA			Open Source Web Security Platform
Fo	rm Password Field with Autocomplete Enabled		
▶ AT	A GLANCE		
	Classification Resource Risk	Environment / Low	
▶ RE	QUEST		
	EET /		
▶ DI	CUSSION		
,	ega detected a form that included a password input field. The autocomple there they may be retrieved by third parties.	ete attribute was not set to off. This may result in some browsers storing v	alues input by users locally,
▶ IM	PACT		
	 A password value may be stored on the local filesystem of the clie Locally stored passwords could be retrieved by other users or mal 		
▶ RE	MEDIATION		
	>> The form declaration should have an autocomplete attribute with	its value set to "off".	

⇒ VEGA		Open Source Web Security Platform			
X-Frame-Options Header Not Set					
AT A GLANCE					
Classification Resource Risk	Information / Info				
REQUEST GET /					
PRESOURCE CONTENT /					

DISCUSSION

Vega has detected that the resource has not set the X-Frame-Options HTTP response header. This header allows the resource to specify its policy with regards to whether it may be included in frames in other domains as well as which domains are allowed. When the header has been set, this may help to mitigate clickjacking attacks against browsers that support this feature. If the header has not been set, the affected resource may be used in clickjacking attacks.

REMEDIATION

>> Set the X-Frame-Options header to DENY, SAMEORIGIN, or ALLOW-FROM according to policy.

REFERENCES

Some additional links with relevant information published by third-parties:

