VEGA Open Source Web Security Platform

Integer Overflow

AT A GLANCE

Classification	**Boundary Condition Error**
Resource	**/loginAction**
Parameter	**username**
Method	**POST**
Risk	**High**

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.

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

VEGA Open Source Web Security Platform

Session Cookie Without Secure Flag

AT A GLANCE

Classification	**Information**
Resource	**/**
Risk	**High**

REQUEST

GET /

RESOURCE CONTENT

```
connect.sid=s%3ACA9A-o5oTIyNpMkWSBtrg35HU8ic4TGv.lbXp2Rgy4I2DZ2jfWYm47RSpw2gm0r0KTPSmB268B9g; Path=/; Expires=Tue, 12 Jul 2022 23:59:08 GMT; HttpOnly
```

DISCUSSION

Vega has detected that a known session cookie may have been set without the secure flag.

IMPACT

» Cookies can be exposed to network eavesdroppers.
» Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

REMEDIATION

» When creating the cookie in the code, set the secure flag to true.

VEGA Open Source Web Security Platform

Integer Overflow

AT A GLANCE

Classification	**Boundary Condition Error**
Resource	**/loginAction**
Parameter	**username**
Method	**POST**
Risk	**High**

REQUEST

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

Shell Injection

AT A GLANCE

Classification	**Information**
Resource	**/loginAction**
Parameter	**password**
Method	**POST**
Risk	**High**

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.

IMPACT

» 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.

SQL Injection

AT A GLANCE

Classification	**Input Validation Error**
Resource	**https://server.tiger.lge.com/loginAction**
Parameter	**password**
Method	**POST**
Detection Type	**Blind Arithmetic Evaluation Differential**
Risk	**High**

REQUEST

POST /loginAction [username=anyone98@hotmail.com password=vega 0 0 - -]

RESOURCE CONTENT

```
Found. Redirecting to /
```

DISCUSSION

Vega has detected a possible SQL injection vulnerability. These vulnerabilities are present when externally-supplied input is used to construct a SQL query. If precautions are not taken, the externally-supplied input (usually a GET or POST parameter) can modify the query string such that it performs unintented actions. These actions include gaining unauthorized read or write access to the data stored in the database, as well as modifying the logic of the application.

IMPACT

- Vega has detected a possible SQL injection vulnerability.
- These vulnerabilities can be exploited by remote attackers to gain unauthorized read or write access to the underlying database.
- Exploitation of SQL injection vulnerabilities can also allow for attacks against the logic of the application.
- Attackers may be able to obtain unauthorized access to the server hosting the database.

Email Addresses Found

AT A GLANCE

Classification	**Information**
Resource	**/**
Risk	Low

REQUEST

GET /

RESOURCE CONTENT

```
anyone98@hotmail.com
```

DISCUSSION

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.

IMPACT

- 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.

Form Password Field with Autocomplete Enabled

AT A GLANCE

Classification	**Environment**
Resource	**/**
Risk	Low

REQUEST

GET /

DISCUSSION

Vega detected a form that included a password input field. The autocomplete attribute was not set to off. This may result in some browsers storing values input by users locally, where they may be retrieved by third parties.

IMPACT

- A password value may be stored on the local filesystem of the client.
- Locally stored passwords could be retrieved by other users or malicious code.

REMEDIATION

- 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	**Information**
Resource	**/**
Risk	Info

REQUEST

GET /

RESOURCE 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:

VEGA Open Source Web Security Platform

X-Frame-Options Header Not Set

AT A GLANCE

Classification	**Information**
Resource	**/loginAction**
Risk	Info

REQUEST

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

RESOURCE CONTENT

```
/loginAction
```

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: