Probely

SECURITY REPORT

Binary Beasts - https://cloudfield.be

Report generated on 2021-12-07 at 16:37 CET

Summary

This section contains the scan summary

TARGET https://cloudfield.be

Report generated on 2021-12-07 at 16:37 CET

STARTED	ENDED	DURATION	SCAN PROFILE
Dec. 6, 2021, 16:20 CET	Dec. 7, 2021, 06:16 CET	13 hours, 56 minutes	Normal

NUMBER OF FINDINGS

	CURRENT SCAN	FROM LAST SCAN	PENDING FIX
HIGH	0	= 0	0
MEDIUM	1	= 0	1
LOW	2	= 0	2

TOP 5

SSL cookie without Secure flag	2
JQuery library with known vulnerabilities	1

Technical Summary

The following table summarizes the findings, ordered by their severity

#	SEVERITY	VULNERABILITY	STATE
7	MEDIUM	**SSL cookie without Secure flag** https://cloudfield.be/ **binary_beasts_session**	**NOT FIXED**
8	LOW	**SSL cookie without Secure flag** https://cloudfield.be/ **XSRF-TOKEN**	**NOT FIXED**
9	LOW	**JQuery library with known vulnerabilities** https://cloudfield.be/admin	**NOT FIXED**

Exhaustive Test List

The following pages contain the list of vulnerabilities we tested in this scan, taking into consideration the chosen profile

---

- Reflected cross-site scripting
- Cookie without HttpOnly flag
- Open redirection
- SQL Injection
- Missing cross-site request forgery protection
- Missing clickjacking protection
- Stored cross-site scripting
- Insecure crossdomain.xml policy
- SSL cookie without Secure flag
- HTTP TRACE method enabled
- Directory Listing
- ASP.NET tracing enabled
- Path traversal
- ASP.NET ViewState without MAC
- Session Token in URL
- Application error message
- Private IP addresses disclosed
- OS command injection
- XML external entity injection
- ASP.NET debugging enabled
- Insecure Silverlight clientaccesspolicy.xml policy
- PHP code injection
- Server-side JavaScript injection
- Python code injection
- SQL injection (second order)
- Server-side template injection
- Unencrypted communications
- HSTS header not enforced
- Mixed content
- Cross Origin Resource Sharing: Arbitrary Origin Trusted
- Certificate with insufficient key size or usage, or insecure signature algorithm
- Expired TLS certificate
- Insecure SSL protocol version 3 supported
- Outdated TLS protocol version 1.0 supported
- Secure TLS protocol version 1.2 not supported
- Weak cipher suites enabled
- Server Cipher Order not configured
- Untrusted TLS certificate
- Heartbleed
- Secure Renegotiation is not supported
- TLS Downgrade attack prevention not supported
- WordPress version with known vulnerabilities
- Joomla! version with known vulnerabilities
- Stored Open redirection
- Certificate without revocation information
- Full path disclosure

- Log file disclosure
- HSTS header set in HTTP
- HSTS header with low duration and no subdomain protection
- HSTS header with low duration
- HSTS header does not protect subdomains
- Inclusion of cryptocurrency mining script
- Insecure SSL protocol version 2 supported
- Browser XSS protection disabled
- Browser content sniffing allowed
- Referrer policy not defined
- Insecure referrer policy
- Potential DoS on TLS Client Renegotiation
- JQuery library with known vulnerabilities
- AngularJS library with known vulnerabilities
- Bootstrap library with known vulnerabilities
- JQuery Mobile library with known vulnerabilities
- JQuery Migrate library with known vulnerabilities
- TLS certificate about to expire
- Moment.js library with known vulnerabilities
- Prototype library with known vulnerabilities
- React library with known vulnerabilities
- SWFObject library with known vulnerabilities
- TinyMCE library with known vulnerabilities
- Backbone library with known vulnerabilities
- Mustache library with known vulnerabilities
- Handlebars library with known vulnerabilities
- Dojo library with known vulnerabilities
- jPlayer library with known vulnerabilities
- CKEditor library with known vulnerabilities
- DWR library with known vulnerabilities
- Flowplayer library with known vulnerabilities
- DOMPurify library with known vulnerabilities
- Plupload library with known vulnerabilities
- easyXDM library with known vulnerabilities
- Ember library with known vulnerabilities
- YUI library with known vulnerabilities
- Sessvars library with known vulnerabilities
- prettyPhoto library with known vulnerabilities
- jQuery UI library with known vulnerabilities
- WordPress plugin with known vulnerabilities
- Invalid referrer policy
- Insecure PHP Object deserialization
- Missing Content Security Policy header
- Insecure Content Security Policy
- GraphQL Introspection enabled

Detailed Finding Descriptions

This section contains the findings in more detail, ordered by severity

7 SSL cookie without Secure flag

MEDIUM

CVSS SCORE
3.1

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

METHOD	PATH	COOKIE
GET	https://cloudfield.be/	binary_beasts_session

DESCRIPTION

The cookie secure flag is intended to prevent browsers from submitting the cookie in any HTTP requests that use an unencrypted c onnection, thus an attacker that is eavesdropping the connection will not be able to get that cookie.

A flag without the secure flag set will always be sent on every HTTP request that matches the scope of cookie, i.e. the domain for which it is set. What this means is that if your application inadvertently makes an HTTP request (without encryption), this request will carry the cookie and any attacker that can eavesdrop the victim traffic will be able to read that cookie.

If the cookie in question is the session cookie, the attacker will be able to hijack the victim account.

EVIDENCE

The cookie being set without the Secure flag:

```
Set-Cookie: binary_beasts_session=eyJpdiI6IlZVSVQxdlBZL294ZCs4bkhEbmt6R0E9PSIsInZhbHVlIjoiQmVaemQ5WThlWEhYTWZKaFk
xZjFXVkFUTnR4UnFUZ1BWT1R6SDkyMHZmbk5DVUZrbzcwQ0NuOFhMZUE3L2tRNFhranBvQWFaTisyQUNUb0VOVXJnYnFRQ2dEY3JOcXNWQUhDd1NJ
ak15cndTeStvRy9YUDlhY0MwazlxWk9UVXEiLCJtYWMiOiIzNTk3MWM3ZDNlZDNlMzhhN2I5ZTgxMGQ1NWFkNjEyMmU1OWUwM2ViNzEwMjNhMWRlZ
WU4N2RmOGRkNTIyZTQ2IiwidGFnIjoiIn0%3D; expires=Mon, 06-Dec-2021 17:21:41 GMT; Max-Age=7199; path=/; httponly; sa
mesite=lax
```

REQUEST

```
GET / HTTP/1.1
pragma: no-cache
cache-control: no-cache
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (compatible; +https://probely.com/sos)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3803.0 Safari/537.36
ProbelySPDR/0.2.0
sec-fetch-site: none
sec-fetch-mode: navigate
sec-fetch-user: ?1
sec-fetch-dest: document
accept-encoding: gzip, deflate
cookie: XSRF-TOKEN=eyJpdiI6IlNIQndEY29QL0ZUdi9TM0FCZG02ZUE9PSIsInZhbHVlIjoiTVZGQ
lJzUVZvR1hXWFZ1V01FbHIvWTEybEdRcS9zV0x6SEUwT3RCcmpZRzdoNWhZdFNaTEZZaXY3WUdkWmd0Z
mtLTGl3c0lpQ0MwZCtBZEg0S3UxZkduMWVRSzZGbWFVOEg2ZVR0SUVsNXlaN0FNbC9Qb1RJTFp5eXFJK
2VYVzciLCJtYWMiOiJlNmQ1MjMzZmUxOTU1MGE2YTcwNWMyYzExMDEyNDljMTU0ZDI0Mzk1YWU5ZmRlM
2ZmZTdlODE4ZTU1M2IxMDk1IiwidGFnIjoiIn0%3D; binary_beasts_session=eyJpdiI6ImtzMFd
NcGtDOS9hNVNCZDlMUTJ0amc9PSIsInZhbHVlIjoiWTM2cUxlL2RxYkRRUEx1bWpzYk43MGdhTTVraE4
2Nm9FQVppcmprdlAwcnRT...
Host: cloudfield.be
```

RESPONSE

```
HTTP/1.1 302 Found
Date: Mon, 06 Dec 2021 15:21:42 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: nginx/1.20.0
X-Powered-By: PHP/8.0.8
Cache-Control: no-cache, private
Location: https://cloudfield.be/dashboard
Permissions-Policy: accelerometer=(self), ambient-light-sensor=(self),
autoplay=(self), battery=(self), camera=(self), cross-origin-isolated=(self),
display-capture=(self), document-domain=*, encrypted-media=(self), execution-
while-not-rendered=*, execution-while-out-of-viewport=*, fullscreen=(self),
geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self),
midi=(self), navigation-override=(self), payment=(self), picture-in-picture=*,
publickey-credentials-get=(self), screen-w...
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Frame-Options: sameorigin
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Set-Cookie: XSRF-TOKEN=eyJpdiI6Im9MOFE1N2FBQzljbVFTZ2Y4MGp2RlE9PSIsInZhbHVlIjoic
1BjMmdid2NvUmxXNlZlVUViUDROUTNMMGZzWHZDUHhsNW00UXRYODlIbnN4SWZvMEVoMXpPQW0zdWpvT
lhqV2ZGU3dOak1ZQ1kxVWlYNDRkWWgzNTJCY2VyQ2ZNV00ycGJ6d0pTeTJsbUl0c3kxZk9GbU94K1ZFd
GgzbFhuU0giLCJtYWMiOiJhOTg1NzgzYzIzYjBhZTc2Y2NjZThkM2U4NTFmMzgzODdjOGU5ZGZmNWU0N
2FiZGMwNmNkYjZkNTRjYWU1OGEwIiwidGFnIjoiIn0%3D; expires=Mon, 06-Dec-2021 17:21:41
GMT; Max-Age=7199; path=/; samesite=lax
Set-Cookie: binary_beasts_session=eyJpdiI6IlZVSVQxdlBZL294ZCs4bkhEbmt6R0E9PSIsIn
ZhbHVlIjoiQmVaemQ5WThlWEhYTWZKaFkxZjFXVkFUTnR4UnFUZ1BWT1R6SDkyMHZmbk5DVUZrbzcwQ0
NuOFhMZUE3L2tRNFhranBvQWFaTisyQUNUb0VOVXJnYnFRQ2dEY3JOcXNWQUhDd1NJak15cndTeStvRy
9YUDlhY0MwazlxWk9UVXEiLCJtYWMiOiIzNTk3MWM3ZDNlZDNlMzhhN2I5ZTgxMGQ1NWFkNjEyMmU1OW
UwM2ViNzEwMjNhMWRlZWU4N2RmOGRkNTIyZTQ2IiwidGFnIjoiIn0%3D; expires=Mon,
06-Dec-2021 17:21:41 GMT; Max-Age=7199; path=/; httponly; samesite=lax
<!DOCTYPE html>
<html>
     <head>
          <meta charset="UTF-8" />
          <meta http-equiv="refresh"
content="0;url='https://cloudfield.be/dashboard'" />
          <title>Redirecting to https://cloudfield.be/dashboard</title>
     </head>
     <body>
          Redirecting to <a
href="https://cloudfield.be/dashboard">https://cloudfield.be/dashboard</a>.
     </body>
</html>
```

8 SSL cookie without Secure flag

LOW

CVSS SCORE
3.1

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

METHOD	PATH	COOKIE
GET	https://cloudfield.be/	XSRF-TOKEN

DESCRIPTION

The cookie secure flag is intended to prevent browsers from submitting the cookie in any HTTP requests that use an unencrypted c onnection, thus an attacker that is eavesdropping the connection will not be able to get that cookie.

A flag without the secure flag set will always be sent on every HTTP request that matches the scope of cookie, i.e. the domain for which it is set. What this means is that if your application inadvertently makes an HTTP request (without encryption), this request will carry the cookie and any attacker that can eavesdrop the victim traffic will be able to read that cookie.

If the cookie in question is the session cookie, the attacker will be able to hijack the victim account.

EVIDENCE

The cookie being set without the Secure flag:

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6Im9MOFE1N2FBQzljbVFTZ2Y4MGp2RlE9PSIsInZhbHVlIjoic1BjMmdid2NvUmxXNlZlVUViUDROUTNMMG
ZzWHZDUHhsNW00UXRYODlIbnN4SWZvMEVoMXpPQW0zdWpvTlhqV2ZGU3dOak1ZQ1kxVWlYNDRkWWgzNTJCY2VyQ2ZNV00ycGJ6d0pTeTJsbUl0c3k
xZk9GbU94K1ZFdGgzbFhuU0giLCJtYWMiOiJhOTg1NzgzYzIzYjBhZTc2Y2NjZThkM2U4NTFmMzgzODdjOGU5ZGZmNWU0N2FiZGMwNmNkYjZkNTRj
YWU1OGEwIiwidGFnIjoiIn0%3D; expires=Mon, 06-Dec-2021 17:21:41 GMT; Max-Age=7199; path=/; samesite=lax
```

REQUEST

```
GET / HTTP/1.1
pragma: no-cache
cache-control: no-cache
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (compatible; +https://probely.com/sos)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3803.0 Safari/537.36
ProbelySPDR/0.2.0
sec-fetch-site: none
sec-fetch-mode: navigate
sec-fetch-user: ?1
sec-fetch-dest: document
accept-encoding: gzip, deflate
cookie: XSRF-TOKEN=eyJpdiI6IlNIQndEY29QL0ZUdi9TM0FCZG02ZUE9PSIsInZhbHVlIjoiTVZGQ
lJzUVZvR1hXWFZ1V01FbHIvWTEybEdRcS9zV0x6SEUwT3RCcmpZRzdoNWhZdFNaTEZZaXY3WUdkWmd0Z
mtLTGl3c0lpQ0MwZCtBZEg0S3UxZkduMWVRSzZGbWFVOEg2ZVR0SUVsNXlaN0FNbC9Qb1RJTFp5eXFJK
2VYVzciLCJtYWMiOiJlNmQ1MjMzZmUxOTU1MGE2YTcwNWMyYzExMDEyNDljMTU0ZDI0Mzk1YWU5ZmRlM
2ZmZTdlODE4ZTU1M2IxMDk1IiwidGFnIjoiIn0%3D; binary_beasts_session=eyJpdiI6ImtzMFd
NcGtDOS9hNVNCZDlMUTJ0amc9PSIsInZhbHVlIjoiWTM2cUxlL2RxYkRRUEx1bWpzYk43MGdhTTVraE4
2Nm9FQVppcmprdlAwcnRT...
Host: cloudfield.be
```

RESPONSE

```
HTTP/1.1 302 Found
Date: Mon, 06 Dec 2021 15:21:42 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: nginx/1.20.0
X-Powered-By: PHP/8.0.8
Cache-Control: no-cache, private
```

```
Location: https://cloudfield.be/dashboard
Permissions-Policy: accelerometer=(self), ambient-light-sensor=(self),
autoplay=(self), battery=(self), camera=(self), cross-origin-isolated=(self),
display-capture=(self), document-domain=*, encrypted-media=(self), execution-
while-not-rendered=*, execution-while-out-of-viewport=*, fullscreen=(self),
geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self),
midi=(self), navigation-override=(self), payment=(self), picture-in-picture=*,
publickey-credentials-get=(self), screen-w...
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Frame-Options: sameorigin
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Set-Cookie: XSRF-TOKEN=eyJpdiI6Im9MOFE1N2FBQzljbVFTZ2Y4MGp2RlE9PSIsInZhbHVlIjoic
1BjMmdid2NvUmxXNlZlVUViUDROUTNMMGZzWHZDUHhsNW00UXRYODlIbnN4SWZvMEVoMXpPQW0zdWpvT
lhqV2ZGU3dOak1ZQ1kxVWlYNDRkWWgzNTJCY2VyQ2ZNV00ycGJ6d0pTeTJsbUl0c3kxZk9GbU94K1ZFd
GgzbFhuU0giLCJtYWMiOiJhOTg1NzgzYzIzYjBhZTc2Y2NjZThkM2U4NTFmMzgzODdjOGU5ZGZmNWU0N
2FiZGMwNmNkYjZkNTRjYWU1OGEwIiwidGFnIjoiIn0%3D; expires=Mon, 06-Dec-2021 17:21:41
GMT; Max-Age=7199; path=/; samesite=lax
Set-Cookie: binary_beasts_session=eyJpdiI6IlZVSVQxdlBZL294ZCs4bkhEbmt6R0E9PSIsIn
ZhbHVlIjoiQmVaemQ5WThlWEhYTWZKaFkxZjFXVkFUTnR4UnFUZ1BWT1R6SDkyMHZmbk5DVUZrbzcwQ0
NuOFhMZUE3L2tRNFhranBvQWFaTisyQUNUb0VOVXJnYnFRQ2dEY3JOcXNWQUhDd1NJak15cndTeStvRy
9YUDlhY0MwazlxWk9UVXEiLCJtYWMiOiIzNTk3MWM3ZDNlZDNlMzhhN2I5ZTgxMGQ1NWFkNjEyMmU1OW
UwM2ViNzEwMjNhMWRlZWU4N2RmOGRkNTIyZTQ2IiwidGFnIjoiIn0%3D; expires=Mon,
06-Dec-2021 17:21:41 GMT; Max-Age=7199; path=/; httponly; samesite=lax
<!DOCTYPE html>
<html>
     <head>
          <meta charset="UTF-8" />
          <meta http-equiv="refresh"
content="0;url='https://cloudfield.be/dashboard'" />
          <title>Redirecting to https://cloudfield.be/dashboard</title>
     </head>
     <body>
          Redirecting to <a
href="https://cloudfield.be/dashboard">https://cloudfield.be/dashboard</a>.
     </body>
</html>
```

9

JQuery library with known vulnerabilities

LOW

CVSS SCORE
4.2

CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

METHOD	PATH
GET	https://cloudfield.be/admin

DESCRIPTION

The application uses an outdated version of the JQuery library, which has known vulnerabilities.

The following CVE(s) affect this library version:

- CVE-2020-11023
- CVE-2020-11022
- CVE-2015-9251
- CVE-2019-11358

EVIDENCE

We have found this evidence(s) in the response:

```
<script src="https://code.jquery.com/jquery-1.12.4.js">
```

REQUEST

```
GET /admin HTTP/1.1
pragma: no-cache
cache-control: no-cache
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (compatible; +https://probely.com/sos)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3803.0 Safari/537.36
ProbelySPDR/0.2.0
sec-fetch-site: none
sec-fetch-mode: navigate
sec-fetch-user: ?1
sec-fetch-dest: document
accept-encoding: gzip, deflate
cookie: XSRF-TOKEN=eyJpdiI6IkswUGlveHNVcUNwZmVGWElkVEx6T3c9PSIsInZhbHVlIjoicVdXW
k5QajYrRDJ1dU9PU3ZLL2NRUGhmQzBkWmR1MG53bDdZSTJlQ0xoY2c4RDF5VnF2TEoyYjI5dzhuMGFWU
1FOMUp5ckRqbXJpWENFUUtQbjlCL3BUa2ROTlFXNllsN1FhMWZCQmtjQ2I4TWNRdlBXR0lZaUJLc1B2S
GpuM3kiLCJtYWMiOiI1MzVkZWRjZWU4Y2FjNmMwNDcwZDg2ZDk5MThkY2MwOTlhNjFiYzQ3NmY3NDFkM
jRhZWU2NDRkNTBjMjJkYjExIiwidGFnIjoiIn0%3D; binary_beasts_session=eyJpdiI6IkE3ZGk
4QStsM0JZd2ZzWXpDK09nOUE9PSIsInZhbHVlIjoiWGU5dUdJNzEwVitCalJmNDFDdVdoeEF6NWV1alZ
ob01NTVpGKzl1UWZCZTJi...
Host: cloudfield.be
```

RESPONSE

```
HTTP/1.1 200 OK
Date: Mon, 06 Dec 2021 15:22:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: nginx/1.20.0
X-Powered-By: PHP/8.0.8
Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private
```

```
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Permissions-Policy: accelerometer=(self), ambient-light-sensor=(self),
autoplay=(self), battery=(self), camera=(self), cross-origin-isolated=(self),
display-capture=(self), document-domain=*, encrypted-media=(self), execution-
while-not-rendered=*, execution-while-out-of-viewport=*, fullscreen=(self),
geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self),
midi=(self), navigation-override=(self), payment=(self), picture-in-picture=*,
publickey-credentials-get=(self), screen-w...
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Frame-Options: sameorigin
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Set-Cookie: XSRF-TOKEN=eyJpdiI6ImZ3T25LWnl6TmNhb2grWE5XU25wZXc9PSIsInZhbHVlIjoiS
jdqOUdHeEl1RG9FSm5SdFhweTBNamZOdU1Ld2JVNE11R0NOajhwdTRtN1RjMzNUUVhGRmUyb3U3N2FEb
3BnbTd1S0lMaUUzK01WcmNlS2xHS2ZtRXZzTGpPdXJYelpvL2dmNlA5R0pESi90TWZPTmZSQWkxYUIzd
m5JdUxGVGQiLCJtYWMiOiJhOGRjOGNhYTMyOGZkNjQyOGZkYjVkNTFmMDNkMGRkOWMyYTlkNjg1MDI0Y
jMxZDJlZmE2YThlY2Y5OWNmZjU3IiwidGFnIjoiIn0%3D; expires=Mon, 06-Dec-2021 17:22:59
GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: binary_beasts_session=eyJpdiI6Imc5anNibU5RMDgwOWFqekVKL1pSMnc9PSIsIn
ZhbHVlIjoiREJENjZGWWwyNlRKNzJrc1ZtbVQ0Q2NLUjh3MTA3Q3dsenh6Tk5vS1dPY0x1bnZyRk1uSU
g1bGhyZyt2VzNHOW5vbTNRSHlteTlKUEZRT2pTMHNuVjIyUUtUaVZTbzVJeDhMUlorNWxQLzcyQ09ral
FrbmdKZHJNYk1pdS9oYXUiLCJtYWMiOiJlZmIzZGI2ZDQwM2NmOWZlNTA5ZGFjMzNlOGFmNzhhNWM4OT
NhZmYzZWIzYTBhMWY5Mzk5MmVjZWU2MTg0MzY1IiwidGFnIjoiIn0%3D; expires=Mon,
06-Dec-2021 17:22:59 GMT; Max-Age=7200; path=/; httponly; samesite=lax
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta name="csrf-token" content="gJIBs4KNfhY1uz1z2vVj5hP2LVfxXuMViSqcMpgQ">
  <title>Binary Beasts</title>
  <!-- Fonts -->
```

Glossary

Term	Definition
Vulnerability	A type of security weakness that might occur in applications (e.g. Broken Authentication, Information Disclosure). Some vulnerabilities take their name not from the weakness itself, but from the attack that exploits it (e.g. SQL Injection, XSS, etc.).
Findings	An instance of a Vulnerability that was found in an application.

Severity Legend

To each finding is attributed a severity which sums up its overall risk

The severity is a compound metric that encompasses the likelihood of the finding being found and exploited by an attacker, the skill required to exploit it, and the impact of such exploitation. A finding that is easy to find, easy to exploit and the exploitation has high impact, will have a greater severity.

Different findings of the same type could have a different severity: we consider multiple factors to increase or decrease it, such as if the application has an authenticated area or not.

The following table describes the different severities:

Severity	Description	Examples
HIGH	These findings may have a direct impact in the application security, either clients or service owners, for instance by granting the attacker access to sensitive information.	SQL Injection OS Command Injection
MEDIUM	Medium findings usually don't have immediate impact alone, but combined with other findings may lead to a successful compromise of the application.	Cross-site Request Forgery Unencrypted Communications
LOW	Findings where either the exploit is not trivial, the impact is low, or the finding cannot be exploited by itself.	Directory Listing Clickjacking

Category Descriptions

The following pages contain descriptions of each vulnerability. For each vulnerability you will find a section explaining its impact, causes and prevention methods.
These descriptions are very generic, and whenever they are not enough to understand or fix a given finding, more information is provided for that finding in the Detailed Finding Descriptions section.

SSL cookie without Secure flag

Description

The cookie secure flag is intended to prevent browsers from submitting the cookie in any HTTP requests that use an unencrypted connection, thus an attacker that is eavesdropping the connection will not be able to get that cookie.

A flag without the secure flag set will always be sent on every HTTP request that matches the scope of cookie, i.e. the domain for which it is set. What this means is that if your application inadvertently makes an HTTP request (without encryption), this request will carry the cookie and any attacker that can eavesdrop the victim traffic will be able to read that cookie.

If the cookie in question is the session cookie, the attacker will be able to hijack the victim account.

Fix

To fix a vulnerability of this type, you just need to set the Secure flag on the vulnerable cookie, effectively preventing it from being transmitted in unencrypted connections, i.e. over HTTP.

Depending on the language and technologies you are using, setting the Secure flag could mean to enable it or setting it to true, either on the code of the application itself or in a configuration file of the webserver or Content Management System (CMS) you are using.

JQuery library with known vulnerabilities

Description

The application uses an outdated version of the JQuery library, which has known vulnerabilities.

Fix

To fix this issue, please update JQuery to the latest available version on its official website.

Do not forget to update all the JQuery files you have on the server.