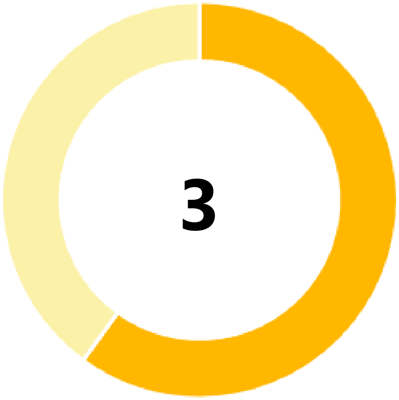
Target: **itsecgames.com**

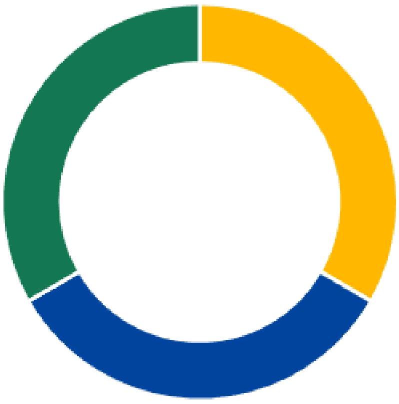
Date: **Sat Oct 11 2025**

Found Issues: **9**

scan **finished** within **2′ 40″** after **615** requests.



Risk



Issue Severity

Executive Summary

SmartScanner conducted a scan on the provided target to find security weaknesses and vulnerabilities. The scan took 2 minutes and 40 seconds. After performing 615 requests, SmartScanner found 9 issues in which 3 of them have medium severity. The overall security risk rating for the target is 3 out of 5. To reduce the security risk, please fix the found issues as soon as possible. Technical details, as well as remediation of results, can be found in the following. *

* DISCLAIMER: This report reflects only the findings discovered by SmartScanner during this scan and may not represent a comprehensive security assessment.

List of Issues

1.1 No Redirection from HTTP to HTTPS

SEVERITY	Medium
URL	http://itsecgames.com

DESCRIPTION

In scenarios where HTTPS is enabled but HTTP requests are not automatically redirected to HTTPS, users must explicitly use the HTTPS URL to ensure encrypted communication. Without redirection, HTTP traffic remains unencrypted and vulnerable to interception by attackers who can access the network interface.

RECOMMENDATION

To enhance security, enforce the use of HTTPS by configuring your application or web server to redirect any HTTP request to HTTPS. Additionally, utilize the **Strict-Transport-Security** HTTP response header to provide an extra layer of security.

CLASSIFICATIONS

CWE-16   CWE-311   OWASP 2010-A6   OWASP 2013-A5   OWASP 2017-A3   OWASP 2017-A6

OWASP 2021-A4   OWASP 2021-A5

2.1 Medium Impact Issue

SEVERITY	Medium
URL	http://itsecgames.com

This type of issue is only available in the Professional version

3.1 No HTTPS

SEVERITY	Medium
URL	http://itsecgames.com
AFFECTED URLS	itsecgames.com/js/html5.js itsecgames.com/download.htm itsecgames.com/bugs.htm itsecgames.com itsecgames.com/training.htm

DESCRIPTION

In HTTP communications, traffic is not encrypted and can be captured by an attacker who has access to a network interface. This exposes sensitive information such as login credentials and personal data to eavesdropping and interception.

RECOMMENDATION

Enable HTTPS and enforce its usage to encrypt communication between clients and servers. Implement HTTP Strict Transport Security (HSTS) to instruct browsers to always use HTTPS for all future requests.

CLASSIFICATIONS

CWE-319   OWASP 2017-A3   OWASP 2021-A2

4.1 Content-Security-Policy Header is Missing

SEVERITY	Low
URL	http://itsecgames.com
AFFECTED URLS	itsecgames.com/download.htm itsecgames.com/bugs.htm itsecgames.com itsecgames.com/training.htm

REQUEST / RESPONSE

```
GET / HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-US,en;q=0.5
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.
0 Safari/537.3
content-length: 0
```

```
HTTP/1.1 200 OK
date: Sat, 11 Oct 2025 09:35:57 GMT
server: Apache
last-modified: Wed, 09 Feb 2022 13:14:08 GMT
etag: "e43-5d7959bd3c800-gzip"
accept-ranges: bytes
vary: Accept-Encoding
content-encoding: gzip
keep-alive: timeout=15, max=100
connection: Keep-Alive
content-type: text/html

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP, a buggy web application!</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>
```

```
    <table>

        <tr>

            <td><font color="#ffb717">Home</font></td>
            <td><a href="bugs.htm">Bugs</a></td>
            <td><a href="download.htm">Download</a></td>
            <td><a href="training.htm">Talks & Training</a></td>
            <td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>

        <
...[truncated]...
```

DESCRIPTION

The absence of the Content-Security-Policy (CSP) response header leaves a website vulnerable to various types of attacks, including Cross-Site Scripting (XSS) and data injection attacks. Without CSP, attackers can exploit vulnerabilities in the web application to execute malicious scripts, steal sensitive data, or deface the site.

RECOMMENDATION

To enhance security, configure your server to send the Content-Security-Policy header for all pages with a well-defined policy that restricts the sources from which content can be loaded and executed. Implementing CSP effectively requires careful consideration of the web application’s functionality and dependencies.

CLASSIFICATIONS

CWE-16   OWASP 2010-A6   OWASP 2013-A5   OWASP 2017-A6   OWASP 2021-A5

5.1 X-Frame-Options Header is Missing

SEVERITY	Low
URL	http://itsecgames.com
AFFECTED URLS	itsecgames.com/download.htm itsecgames.com/bugs.htm itsecgames.com itsecgames.com/training.htm

REQUEST / RESPONSE

```
GET / HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-US,en;q=0.5
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.
0 Safari/537.3
content-length: 0
```

```
HTTP/1.1 200 OK
date: Sat, 11 Oct 2025 09:35:57 GMT
server: Apache
last-modified: Wed, 09 Feb 2022 13:14:08 GMT
etag: "e43-5d7959bd3c800-gzip"
accept-ranges: bytes
vary: Accept-Encoding
content-encoding: gzip
keep-alive: timeout=15, max=100
connection: Keep-Alive
content-type: text/html

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP, a buggy web application!</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>
```

```
    <table>

        <tr>

            <td><font color="#ffb717">Home</font></td>
            <td><a href="bugs.htm">Bugs</a></td>
            <td><a href="download.htm">Download</a></td>
            <td><a href="training.htm">Talks & Training</a></td>
            <td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>

        <
...[truncated]...
```

DESCRIPTION

The absence of the `X-Frame-Options` HTTP response header leaves a website vulnerable to click-jacking attacks. Without this header, attackers can embed the site's content into malicious pages using iframes, potentially leading to phishing attacks or unauthorized transactions.

RECOMMENDATION

To mitigate this vulnerability, configure your server to send the `X-Frame-Options` header with an appropriate setting for all pages. Common settings include `DENY`, `SAMEORIGIN`, or `ALLOW-FROM` followed by a specific URI. Choose the setting that best fits your application's requirements. Ensure proper testing to verify that the header is correctly implemented and enforced by all browsers.

CLASSIFICATIONS

CWE-1021 CWE-16 OWASP 2010-A6 OWASP 2013-A5 OWASP 2017-A6 OWASP 2021-A4 OWASP 2021-A5

6.1 Subresource Integrity is Missing

SEVERITY	Low
URL	http://itsecgames.com
AFFECTED URLS	itsecgames.com/download.htm itsecgames.com/bugs.htm itsecgames.com itsecgames.com/training.htm
EXTERNAL RESOURCES	https://fonts.googleapis.com/css?family=Architects+Daughter

REQUEST / RESPONSE

```
GET / HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-US,en;q=0.5
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.3
content-length: 0
```

```
HTTP/1.1 200 OK
date: Sat, 11 Oct 2025 09:35:57 GMT
server: Apache
last-modified: Wed, 09 Feb 2022 13:14:08 GMT
etag: "e43-5d7959bd3c800-gzip"
accept-ranges: bytes
vary: Accept-Encoding
content-encoding: gzip
keep-alive: timeout=15, max=100
connection: Keep-Alive
content-type: text/html

...[truncated]...
>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?fa
...[truncated]...
```

DESCRIPTION

Subresource Integrity (SRI) is a security feature that allows browsers to verify that resources fetched, such as from a content delivery network (CDN), are delivered without unexpected manipulation. It achieves this by enabling you to provide a cryptographic hash that the fetched resource must match.

RECOMMENDATION

To enhance security, add a base64-encoded hash of the resource in the value of the `integrity` or calculate it yourself. See references for details.

CLASSIFICATIONS

CWE-353   OWASP 2021-A8

7.1 X-Content-Type-Options Header is Missing

SEVERITY	Informational
URL	http://itsecgames.com
AFFECTED URLS	itsecgames.com/js/html5.js itsecgames.com/download.htm itsecgames.com/bugs.htm itsecgames.com itsecgames.com/training.htm

REQUEST / RESPONSE

```
GET / HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-US,en;q=0.5
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.
0 Safari/537.3
content-length: 0
```

```
HTTP/1.1 200 OK
date: Sat, 11 Oct 2025 09:35:57 GMT
server: Apache
last-modified: Wed, 09 Feb 2022 13:14:08 GMT
etag: "e43-5d7959bd3c800-gzip"
accept-ranges: bytes
vary: Accept-Encoding
content-encoding: gzip
keep-alive: timeout=15, max=100
connection: Keep-Alive
content-type: text/html

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP, a buggy web application!</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>
```

```
<div id="menu">

    <table>

        <tr>

            <td><font color="#ffb717">Home</font></td>
            <td><a href="bugs.htm">Bugs</a></td>
            <td><a href="download.htm">Download</a></td>
            <td><a href="training.htm">Talks & Training</a></td>
            <td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>

        <
...[truncated]...
```

DESCRIPTION

The absence of the `X-Content-Type-Options` response HTTP header may expose a website to MIME sniffing attacks. MIME sniffing, performed by browsers when the MIME type is not explicitly declared, can lead to the interpretation of non-executable content as executable, potentially exposing users to security risks.

RECOMMENDATION

To mitigate this risk, configure your server to send the `X-Content-Type-Options` header with the value set to `nosniff`. This instructs browsers not to perform MIME sniffing and to strictly respect the declared content type.

CLASSIFICATIONS

CWE-16   OWASP 2010-A6   OWASP 2013-A5   OWASP 2017-A6   OWASP 2021-A5

8.1 Referrer-Policy Header is Missing

SEVERITY	Informational
URL	http://itsecgames.com
AFFECTED URLS	itsecgames.com/download.htm itsecgames.com/bugs.htm itsecgames.com itsecgames.com/training.htm

REQUEST / RESPONSE

```
GET / HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-US,en;q=0.5
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.
0 Safari/537.3
content-length: 0
```

```
HTTP/1.1 200 OK
date: Sat, 11 Oct 2025 09:35:57 GMT
server: Apache
last-modified: Wed, 09 Feb 2022 13:14:08 GMT
etag: "e43-5d7959bd3c800-gzip"
accept-ranges: bytes
vary: Accept-Encoding
content-encoding: gzip
keep-alive: timeout=15, max=100
connection: Keep-Alive
content-type: text/html

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP, a buggy web application!</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>
```

```
    <table>

        <tr>

            <td><font color="#ffb717">Home</font></td>
            <td><a href="bugs.htm">Bugs</a></td>
            <td><a href="download.htm">Download</a></td>
            <td><a href="training.htm">Talks & Training</a></td>
            <td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>

        <
...[truncated]...
```

DESCRIPTION

The `Referrer-Policy` HTTP header controls the amount of referrer information (sent via the `Referer` header) included with requests. The `Referer` header contains the address of the previous web page from which a link to the currently requested page was followed. While it has many legitimate uses such as analytics and logging, it can also pose privacy and security risks if not handled properly.

RECOMMENDATION

Configure your server to send the `Referrer-Policy` header for all pages with the value set to `strict-origin-when-cross-origin`. This policy ensures that the full URL is included as a referrer when navigating within the same origin, while only sending the origin when navigating from one origin to another. You can explore other possible values based on your specific requirements and security considerations.

CLASSIFICATIONS

CWE-16   OWASP 2010-A6   OWASP 2013-A5   OWASP 2017-A6   OWASP 2021-A5

9.1 Target Information

SEVERITY	Informational
URL	http://itsecgames.com
SERVER BANNER	apache
WEB SERVER	apache