PROJECT

Main Website Report

Team ID- Team-593479 (2.9)

Team members:

Ramar Priya Maha Lakshmi

Chevala Syam Sai

Panchada Varun

Mulumudi Prabhas

1. Exploring Vulnerabilities in the main website.

Chosen Website: https://smartinternz.com

a. **Vulnerability:** PHP Unsupported Version Detection

CWE: CWE-661

OWASP Category: A06:2021-Vulnerable and Outdated Components

Severity: High

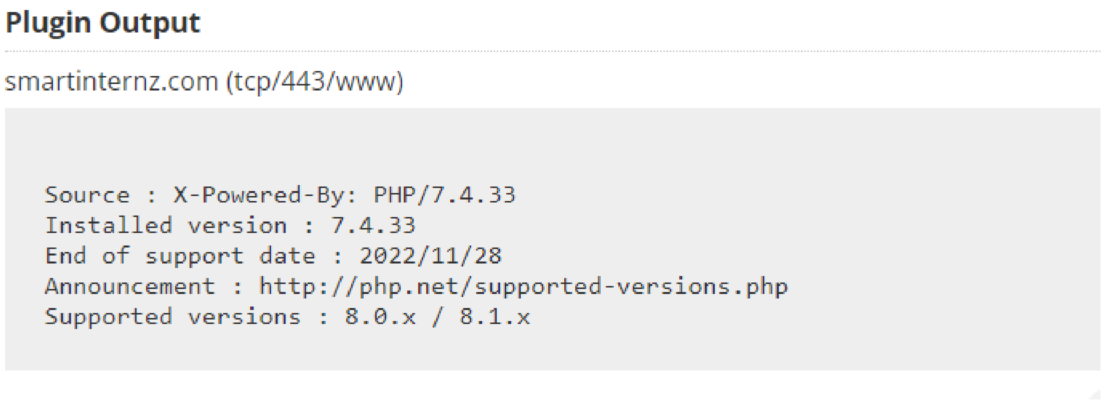
Description: According to its version, the installation of PHP on the remote host is no longer supported. As a result, it is likely to contain security vulnerabilities.

Business Impact: Anyone can connect to the NSClient and retrieve sensitive information, such as process and service states, memory usage, etc.

Vulnerability Path: https://smartinternz.com

Steps to Reproduce:

1. Nessus Scan reveals the PHP version supporting the website.



Plugin Output

smartinternz.com (tcp/443/www)

```
Source : X-Powered-By: PHP/7.4.33
Installed version : 7.4.33
End of support date : 2022/11/28
Announcement : http://php.net/supported-versions.php
Supported versions : 8.0.x / 8.1.x
```

Recommendations:

- Upgrade to a version of PHP that is currently supported.
- Find it on your network and fix it as soon as possible.

b. **Vulnerability:** Missing Anti-clickjacking tokens

CWE: CWE-451

OWASP Category: A04:2021 Insecure Design

Severity: High

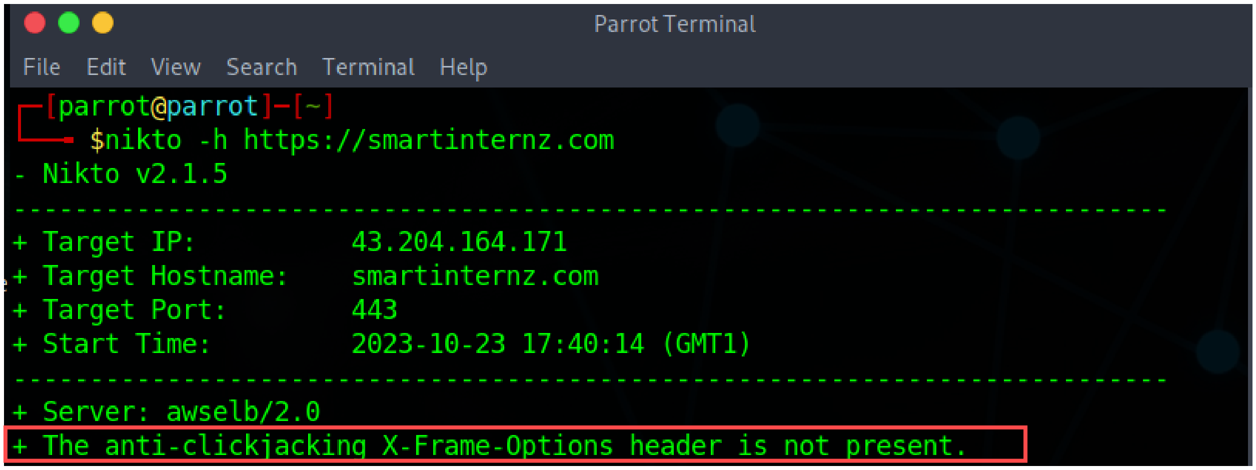
Description: The user interface (UI) does not properly represent critical information to the user, allowing the information - or its source - to be obscured or spoofed. This is often a component in phishing attacks.

Business Impact: The Impact of Clickjacking The hacker has several ways they can use the redirected clicks for their own gain. A common form of clickjacking involves mirroring a login and password form on a website.

Vulnerability Path: https://smartinternz.com

Steps to Reproduce:

1. Tool Used: **Nikto.** Type the following Command.



```
┌─[parrot@parrot]─[~]
└──╼ $nikto -h https://smartinternz.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          43.204.164.171
+ Target Hostname:    smartinternz.com
+ Target Port:        443
+ Start Time:         2023-10-23 17:40:14 (GMT1)
---------------------------------------------------------------------------
+ Server: awselb/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
```

Recommendations:

- Implement X-Frame Options Header.
- Utilize Content Security Policy.
- Employ frame-busting JavaScript code.

c. **Vulnerability:** Disclosing webserver type

CWE: CWE-200

OWASP Category: A03:2017 Sensitive Data Exposure

Severity: low

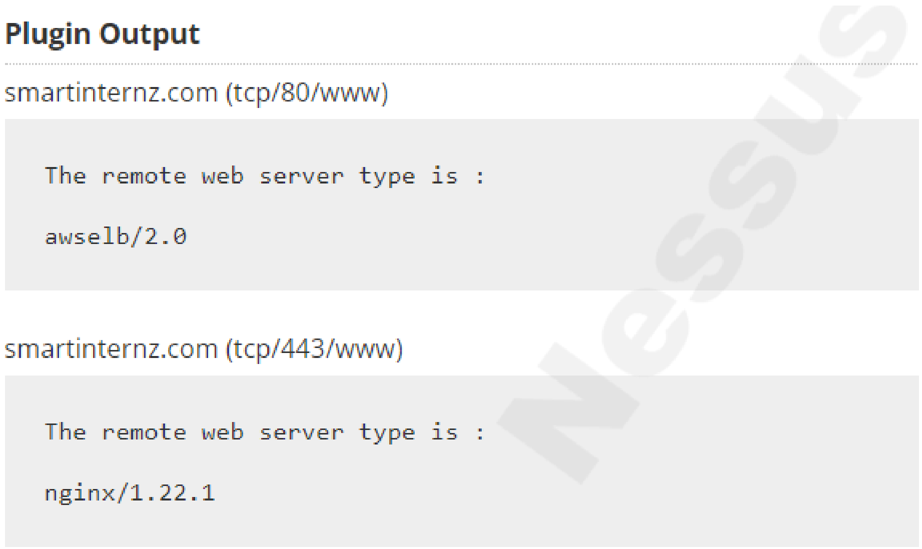
Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business Impact: Disclosing the web server type can pose a security risk by providing potential attackers with information that may be exploited. This disclosure can lead to more targeted attacks and increases the risk of vulnerabilities being exploited, potentially resulting in data breaches, service disruptions, and reputational damage. It's essential to minimize such disclosures to enhance the security of web applications.

Vulnerability Path: https://smartinternz.com

Steps to Reproduce:

1. Nessus Scan reveals the webserver version supporting the website.



Plugin Output

smartinternz.com (tcp/80/www)

```
The remote web server type is :

awselb/2.0
```

smartinternz.com (tcp/443/www)

```
The remote web server type is :

nginx/1.22.1
```

Recommendations:

- You can limit the information that nginx presents by creating/editing the following directive in *nginx.conf*.
- Replace it with false information.

d. **Vulnerability:** Cleartext Transmission of Credentials

CWE: CWE-319

OWASP Category: A05:2021 Security Misconfiguration

Severity: Medium

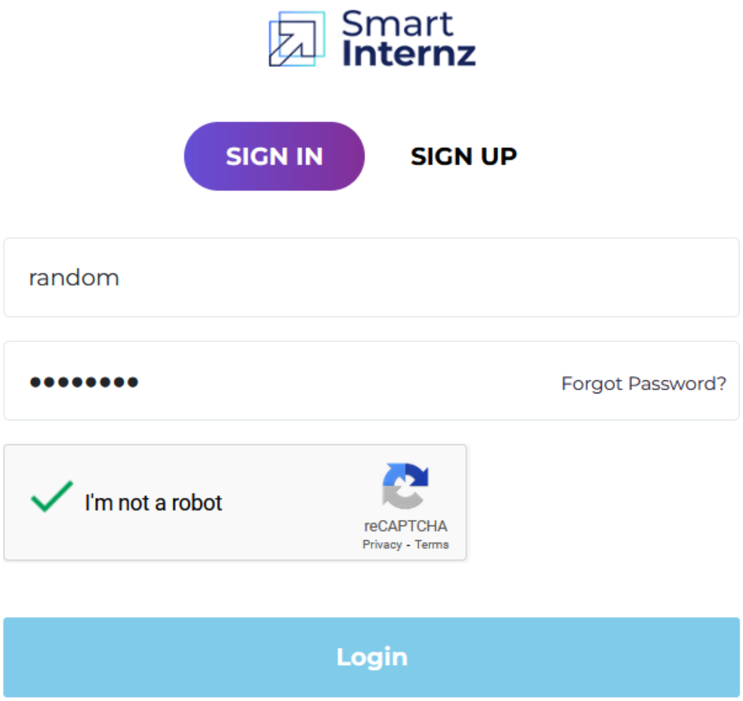
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact: Transmitting credentials in cleartext can result in unauthorized access, data breaches, loss of customer trust, legal and regulatory consequences, and reputation damage, impacting an organization's security and financial standing.

Vulnerability Path: https://smartinternz.com/student-login

Steps to Reproduce:

1. Navigate to the above-mentioned URL and login.

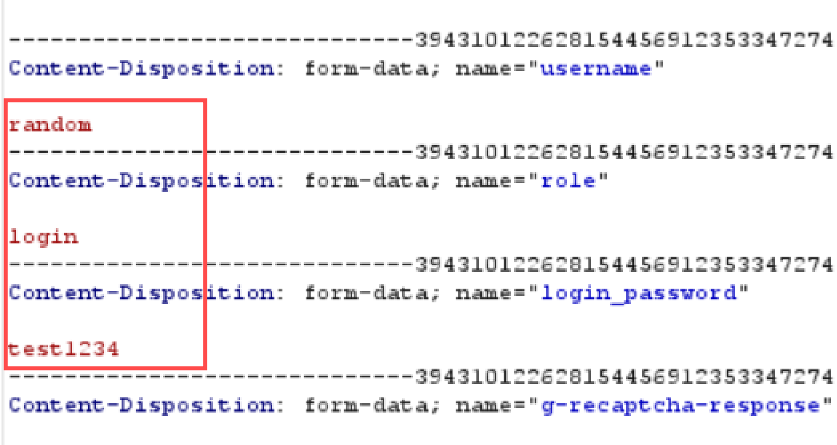


random

•••••••••

☑ I'm not a robot

2. Tool Used: **Burp Suite.** Capture the traffic.



```
-----------------------------394310122628154456912353347274
Content-Disposition: form-data; name="username"

random
-----------------------------394310122628154456912353347274
Content-Disposition: form-data; name="role"

login
-----------------------------394310122628154456912353347274
Content-Disposition: form-data; name="login_password"

test1234
-----------------------------394310122628154456912353347274
Content-Disposition: form-data; name="g-recaptcha-response"
```

Recommendations:

- Hash and Salt credentials.
- Implement Secure Protocols.

e. Vulnerability: Web Server Directory Enumeration

CWE: CWE-548

OWASP Category: A04: Insecure Design

Severity: low

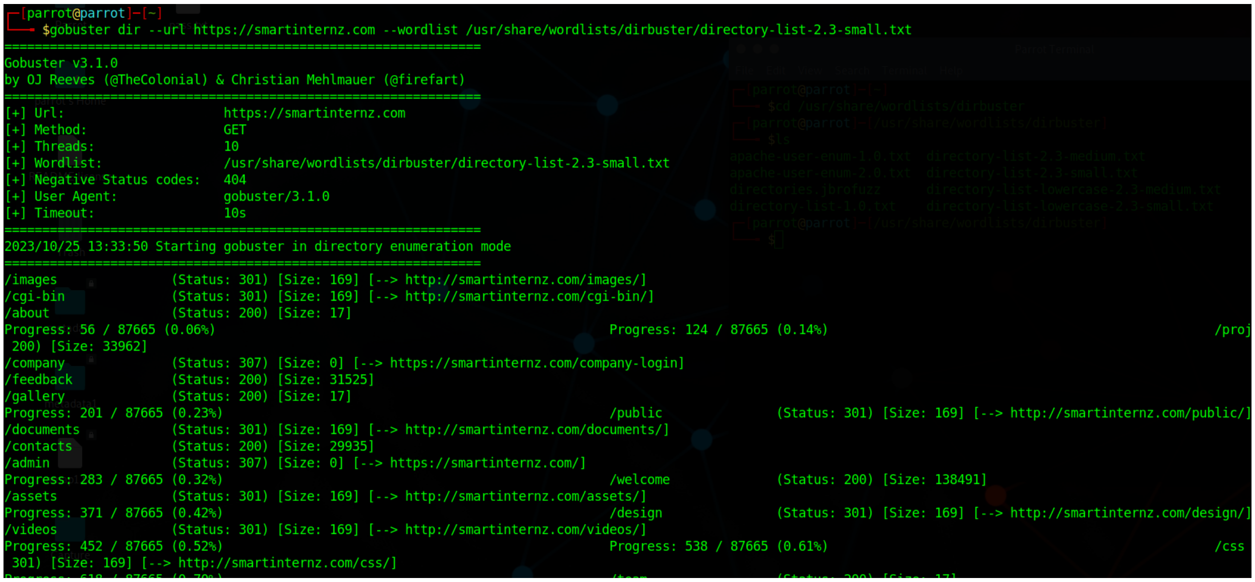
Description: A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers.

Business Impact: Webserver directory enumeration, often through techniques like directory listing, can have significant business impacts. By revealing the structure of a web server's directories and files, it provides potential attackers with insights into the system's architecture and potential vulnerabilities. This can lead to unauthorized access, data exposure, and even service disruptions. The business consequences include reputational damage, legal liabilities, financial losses, and the potential compromise of sensitive information. Mitigating directory enumeration is crucial to maintaining a secure online presence.

Vulnerability Path: https://smartinternz.com

Steps to Reproduce:

1. Tool Used: **Gobuster.** Type the following command.



```
┌─[parrot@parrot]─[~]
└──╼ $gobuster dir --url https://smartinternz.com --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://smartinternz.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2023/10/25 13:33:50 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://smartinternz.com/images/]
/cgi-bin              (Status: 301) [Size: 169] [--> http://smartinternz.com/cgi-bin/]
/about                (Status: 200) [Size: 17]
Progress: 56 / 87665 (0.06%)                                               Progress: 124 / 87665 (0.14%)                                               /proj
 200) [Size: 33962]
/company              (Status: 307) [Size: 0] [--> https://smartinternz.com/company-login]
/feedback             (Status: 200) [Size: 31525]
/gallery              (Status: 200) [Size: 17]
Progress: 201 / 87665 (0.23%)                                              /public               (Status: 301) [Size: 169] [--> http://smartinternz.com/public/]
/documents            (Status: 301) [Size: 169] [--> http://smartinternz.com/documents/]
/contacts             (Status: 200) [Size: 29935]
/admin                (Status: 307) [Size: 0] [--> https://smartinternz.com/]
Progress: 283 / 87665 (0.32%)                                              /welcome              (Status: 200) [Size: 138491]
/assets               (Status: 301) [Size: 169] [--> http://smartinternz.com/assets/]
Progress: 371 / 87665 (0.42%)                                              /design               (Status: 301) [Size: 169] [--> http://smartinternz.com/design/]
/videos               (Status: 301) [Size: 169] [--> http://smartinternz.com/videos/]
Progress: 452 / 87665 (0.52%)                                              Progress: 538 / 87665 (0.61%)                                               /css
 301) [Size: 169] [--> http://smartinternz.com/css/]
Progress: 618 / 87665 (0.70%)                                              /team                 (Status: 200) [Size: 17]
```

Recommendations:

- Disable directory listing.
- Restrict access to sensitive files and directories.
- Use Strong Authentication mechanisms to control access.