Penetration Testing Report

HackersForYou

Prepared By: Onkar Mhaskar
Role: Penetration Testing Intern
Date: 16-Oct-2023

Client Information:

PingBreakers: https://pingbreakers.com/

Contact Details: +91 6353761464 | Address: Gandhinagar Gujarat, India

Objective:

The objective of this Penetration Testing Report is to assess the security posture of the target network infrastructure, identify vulnerabilities, and provide recommendations for remediation to enhance the overall security of the client network.

Table of Contents

Introduction

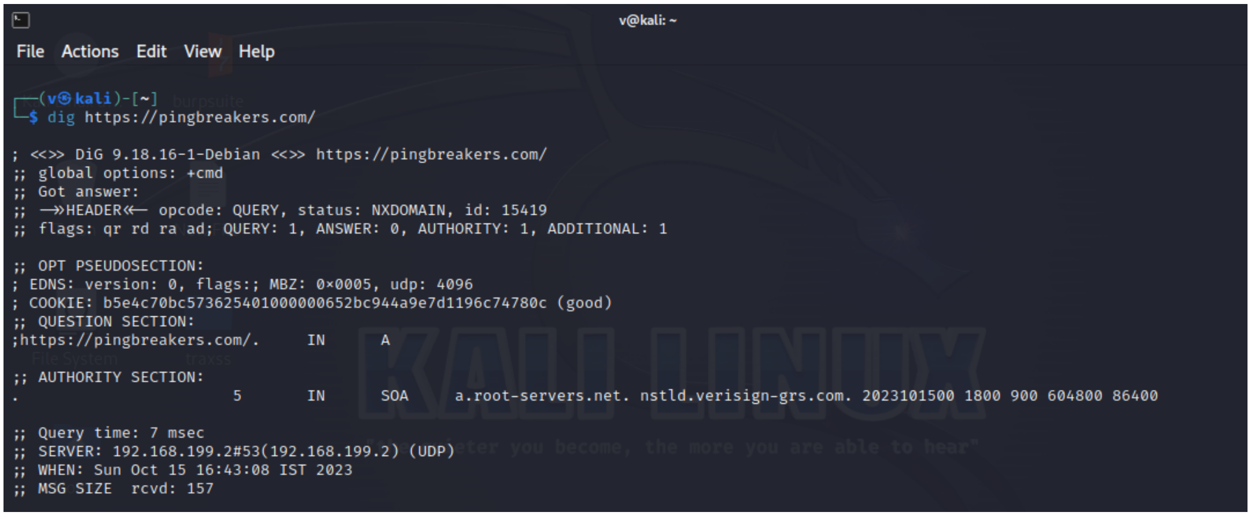
- **Scope:** I tested the web application part that is search bar.
- **Objectives:** The main goal was to find loop holes of pingbreakers so I used nmap and burpsuite.

Methodology

I apply the way that every pentester does that first I gather information about target using nmap, central ops tools and after that I check that target is vulnerable or not by using nmap scripts engine but no output I get so I use xss scripting that is cross side scripting. Cross-Site Scripting (XSS) is a type of security vulnerability that occurs when a web application allows users to inject malicious scripts into web pages viewed by other users. These scripts are typically written in JavaScript and can be executed in the context of a victim's browser, potentially leading to various forms of attacks, such as stealing cookies, session hijacking, defacement, and more

Target Information

- **Publicly Available Information:**
- **DNS Information:**
-
-



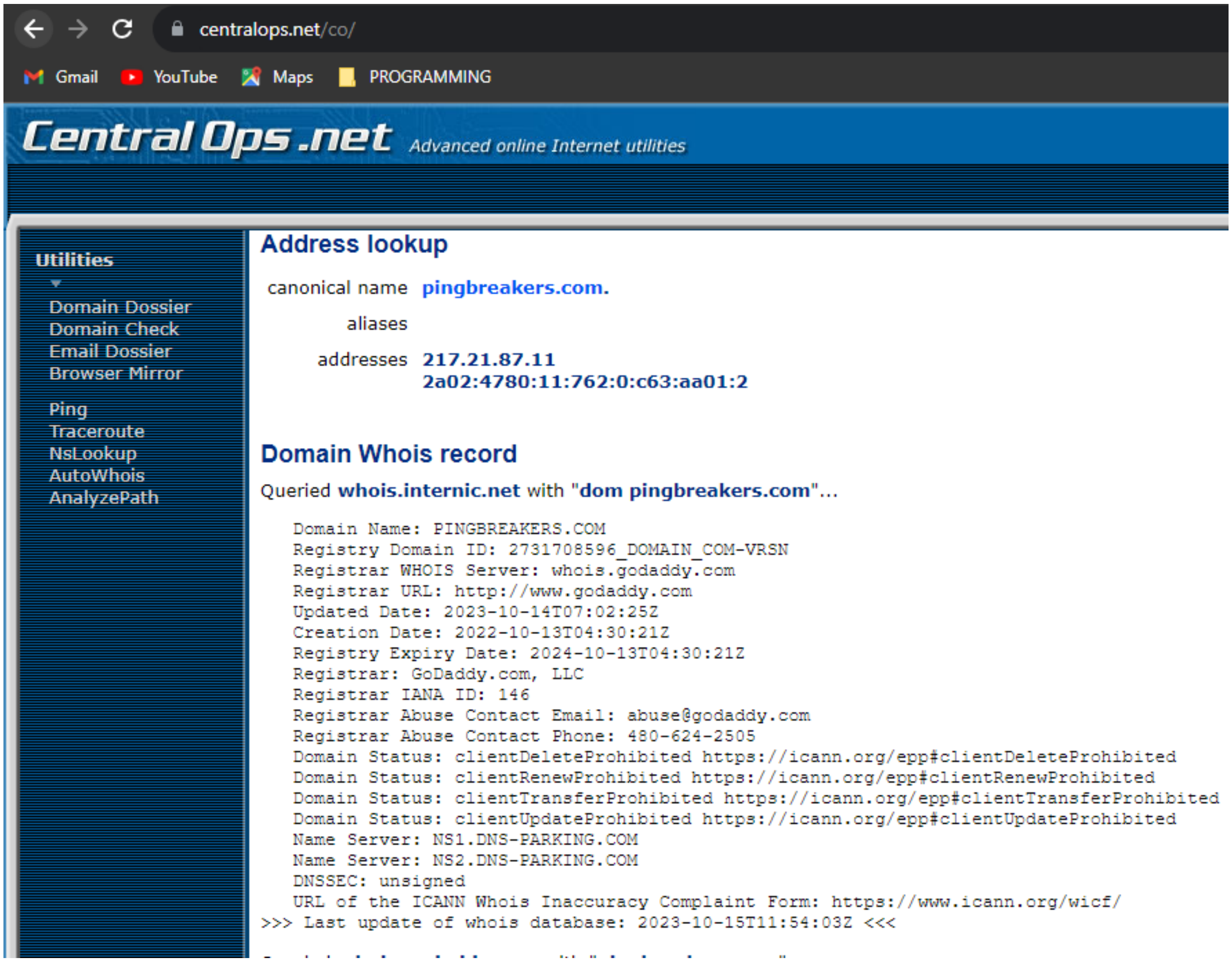
```
┌──(v㉿kali)-[~]
└─$ dig https://pingbreakers.com/

; <<>> DiG 9.18.16-1-Debian <<>> https://pingbreakers.com/
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 15419
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 4096
; COOKIE: b5e4c70bc573625401000000652bc944a9e7d1196c74780c (good)
;; QUESTION SECTION:
;https://pingbreakers.com/.     IN      A

;; AUTHORITY SECTION:
.                       5       IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023101500 1800 900 604800 86400

;; Query time: 7 msec
;; SERVER: 192.168.199.2#53(192.168.199.2) (UDP)
;; WHEN: Sun Oct 15 16:43:08 IST 2023
;; MSG SIZE  rcvd: 157
```



Address lookup

canonical name pingbreakers.com.

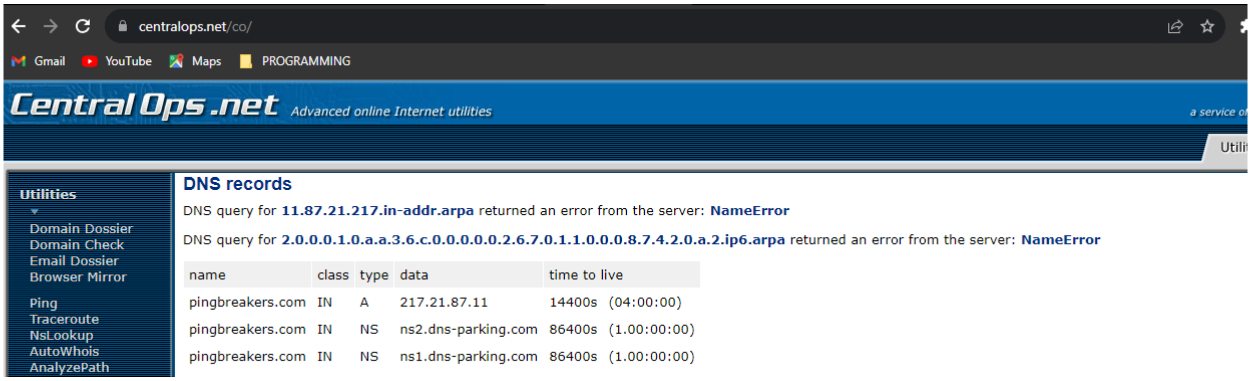
aliases

addresses 217.21.87.11
2a02:4780:11:762:0:c63:aa01:2

Domain Whois record

Queried **whois.internic.net** with "**dom pingbreakers.com**"...

```
   Domain Name: PINGBREAKERS.COM
   Registry Domain ID: 2731708596_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2023-10-14T07:02:25Z
   Creation Date: 2022-10-13T04:30:21Z
   Registry Expiry Date: 2024-10-13T04:30:21Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.DNS-PARKING.COM
   Name Server: NS2.DNS-PARKING.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-10-15T11:54:03Z <<<
```



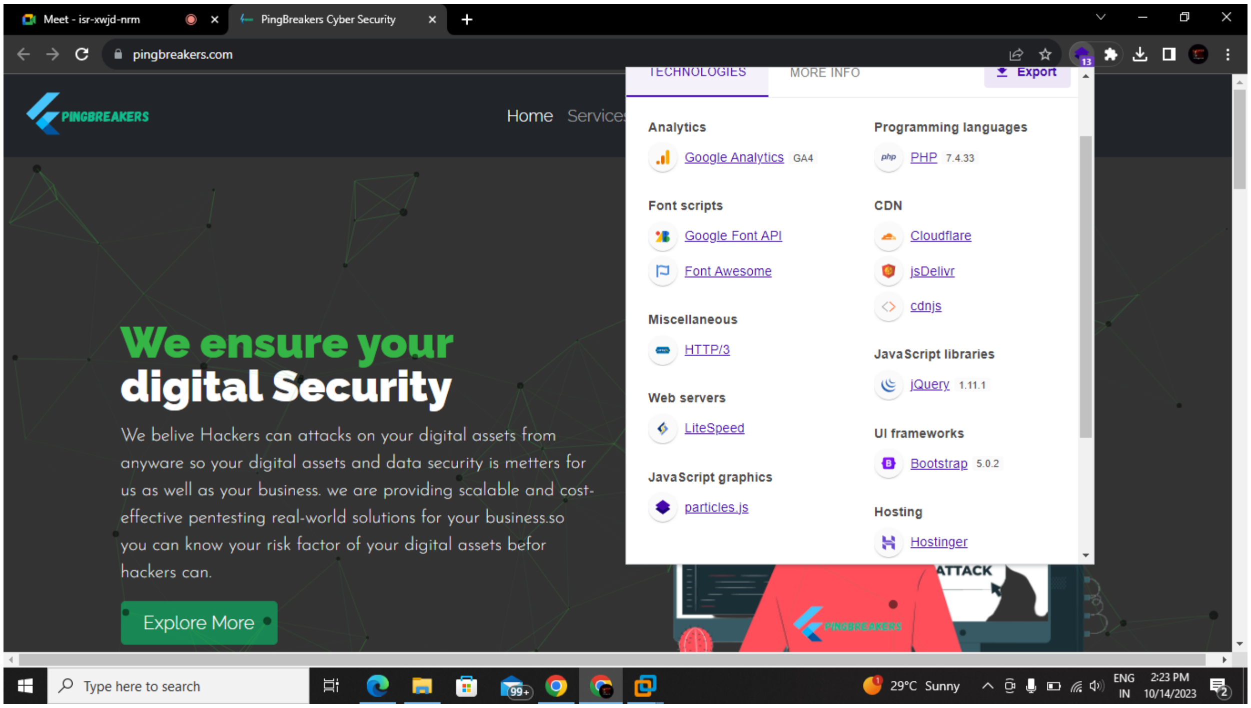
DNS records

DNS query for 11.87.21.217.in-addr.arpa returned an error from the server: NameError

DNS query for 2.0.0.0.1.0.a.a.3.6.c.0.0.0.0.0.2.6.7.0.1.1.0.0.0.8.7.4.2.0.a.2.ip6.arpa returned an error from the server: NameError

name	class	type	data	time to live
pingbreakers.com	IN	A	217.21.87.11	14400s (04:00:00)
pingbreakers.com	IN	NS	ns2.dns-parking.com	86400s (1.00:00:00)
pingbreakers.com	IN	NS	ns1.dns-parking.com	86400s (1.00:00:00)

- **Web Application Information:**



Analytics
Google Analytics GA4

Font scripts
Google Font API
Font Awesome

Miscellaneous
HTTP/3

Web servers
LiteSpeed

JavaScript graphics
particles.js

Programming languages
PHP 7.4.33

CDN
Cloudflare
jsDelivr
cdnjs

JavaScript libraries
jQuery 1.11.1

UI frameworks
Bootstrap 5.0.2

Hosting
Hostinger

We ensure your digital Security

We belive Hackers can attacks on your digital assets from anyware so your digital assets and data security is metters for us as well as your business. we are providing scalable and cost-effective pentesting real-world solutions for your business.so you can know your risk factor of your digital assets befor hackers can.

Findings and Vulnerability Assessment

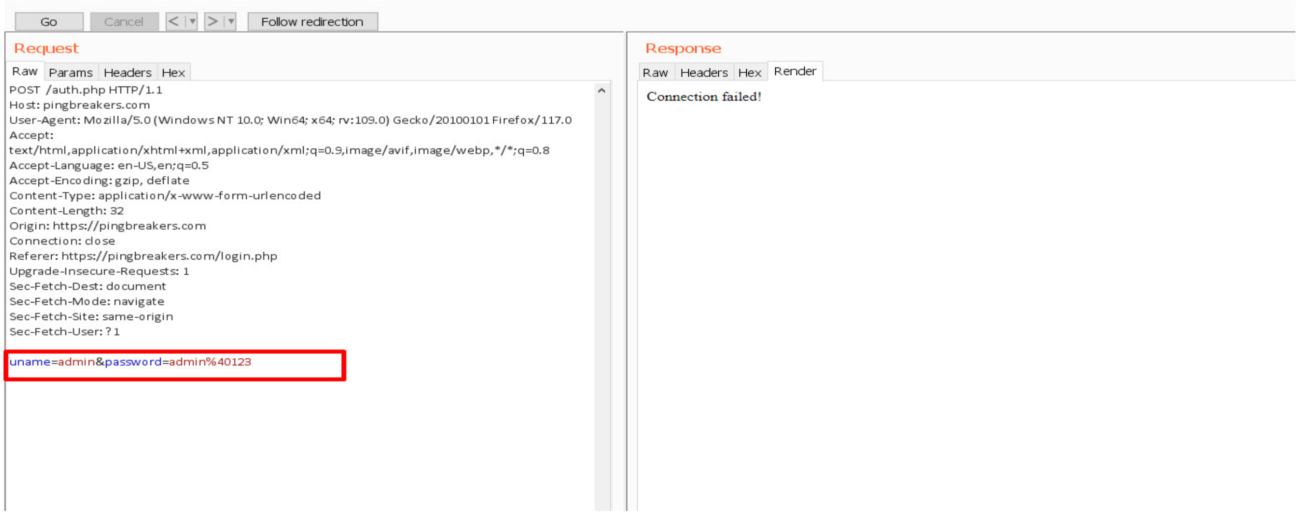
This is a detailed section that discusses each vulnerability and finding identified during the penetration test:

Finding [Unique ID]

- **Severity:** It’s assigned medium severity rating.
- **Description:** It’s a reflected XSS. In a reflected XSS attack, the malicious script is embedded in a URL or other input and is immediately executed when a user clicks on the manipulated link. The injected script is not stored on the target server and affects only the user who interacts with the manipulated URL. When Iput login.php in website URL its navigating directly to a login page and after I put username:admin and password:admin the error immediately reflected in URL.

Impact:

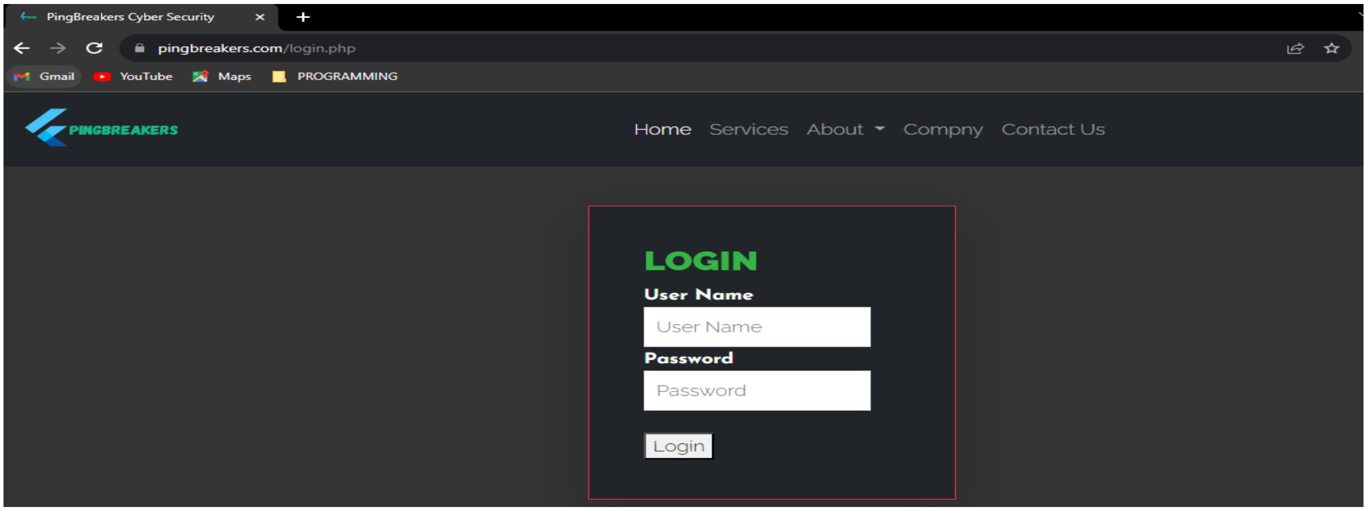
1. **Data Theft and Privacy Breach**: Attackers can use reflected XSS to steal sensitive information from users, such as login credentials, personal data, or financial details. This can lead to privacy breaches and damage a client's reputation.
2. **Financial Loss**: If attackers gain access to financial data or conduct fraudulent transactions on behalf of users, it can result in financial losses for both the client and their customers.
3. **Session Hijacking**: Reflected XSS can allow attackers to hijack user sessions, gaining unauthorized access to accounts and performing actions on behalf of the victim. This could disrupt the user experience and lead to loss of trust.
4. **Reputation Damage**: When users experience security issues or data breaches due to reflected XSS, they may lose trust in the client's web application or services. A damaged reputation can result in a loss of customers and revenue.
5. **Legal Consequences**: Depending on the jurisdiction and the nature of the data compromised, the client may face legal consequences, regulatory fines, or lawsuits related to the data breach.
6. **Loss of Customer Trust**: Security incidents can erode customer trust. Users may be hesitant to use the client's services or share their personal information if they perceive the web application as insecure.
7. **Disruption of Services**: If an attacker exploits reflected XSS to disrupt the web application's functionality, it can lead to service outages and downtime, causing inconvenience to users and loss of business

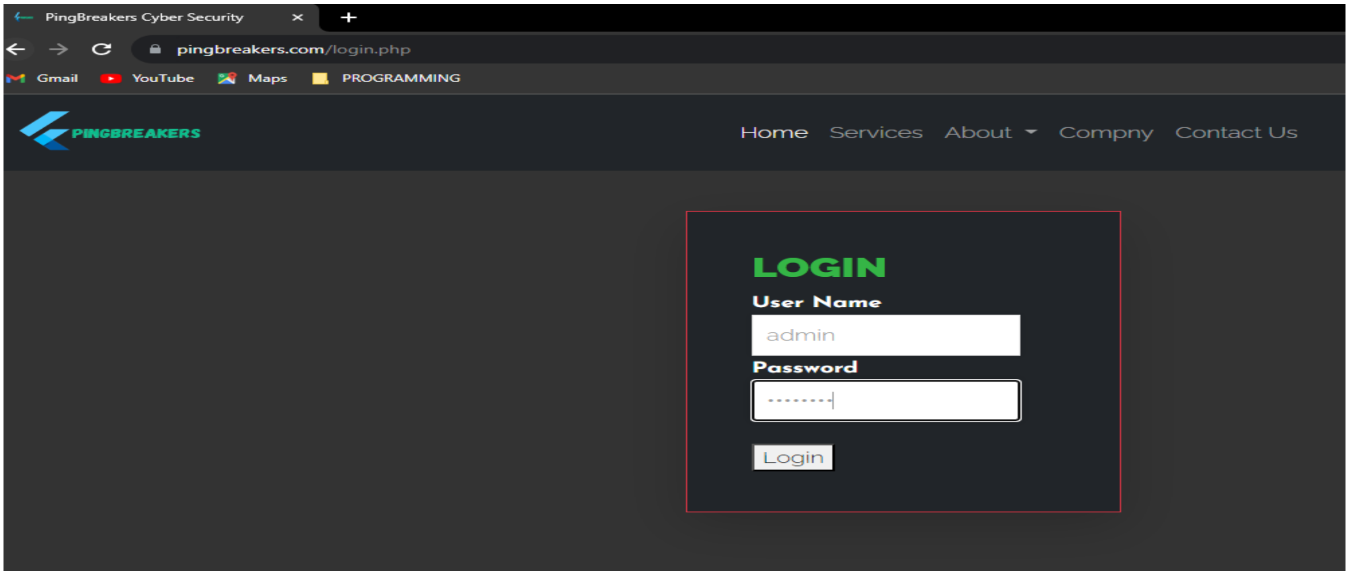


```
POST /auth.php HTTP/1.1
Host: pingbreakers.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: https://pingbreakers.com
Connection: close
Referer: https://pingbreakers.com/login.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

uname=admin&password=admin%40123
```

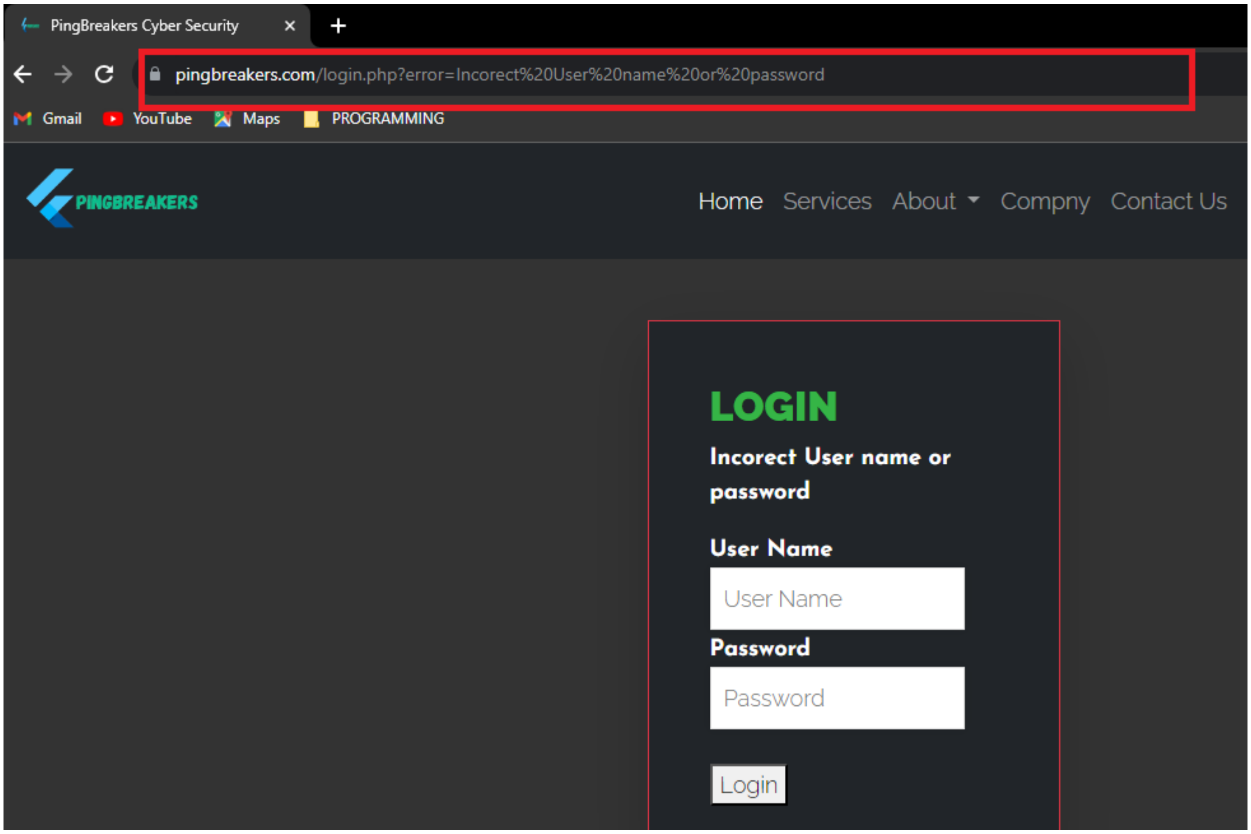
```
Connection failed!
```





User Name: admin

Password: ·········



pingbreakers.com/login.php?error=Incorect%20User%20name%20or%20password

Incorect User name or password

Recommendations:

1. **Input Validation**:
   - Sanitize and validate all user input, such as form data and URL parameters. Reject or sanitize any input that doesn't conform to the expected format.
2. **Use Appropriate Content Security Policy (CSP)**:
   - Implement a strict CSP to define which sources of content, scripts, and other resources are allowed to load and execute. This can help prevent the execution of unauthorized scripts.
3. **Escape Output**:
   - Before displaying user-generated content, encode it properly to ensure it's treated as data, not executable code. Use output encoding functions specific to your programming language (e.g., **htmlspecialchars** in PHP, **encodeURIComponent** in JavaScript).

- **References:** CVE-2021-29103

A reflected Cross Site Scripting (XXS) vulnerability in ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user&#8217;s browser.

Risk Assessment

1. Vulnerability Description:Vulnerability Type: Reflected Cross-Site Scripting (XSS)

Description: The login.php page of the web application does not properly validate and sanitize user inputs, allowing malicious scripts to be executed in a victim's browser, primarily through input fields like username and password.

2. Impact Assessment:Data Exposure: The vulnerability can lead to the exposure of sensitive login credentials, which could include usernames and passwords.

Unauthorized Access: An attacker could potentially gain unauthorized access to user accounts through credential theft.

Privacy Breach: A successful attack can result in a privacy breach, causing harm to affected individuals.

Reputation Damage: A security incident related to the login page can damage the client's reputation and erode trust among users.

Legal Consequences: Regulatory fines or lawsuits may result if user data is compromised.

3. Risk Level:

The risk level is determined by the intersection of the potential impact and likelihood:

High Risk: A high likelihood of exploitation with a significant impact on data exposure, unauthorized access, privacy, finances, reputation, and potential legal consequences.

Medium Risk: Either a moderate likelihood with significant impact or a high likelihood with moderate impact.

Low Risk: A low likelihood of exploitation with minimal impact.

4. Risk Mitigation:

Implement Strong Input Validation: Apply thorough input validation and sanitize user inputs on the login page to prevent malicious script injection.

Output Encoding: Encode user-generated content before displaying it, especially on error messages or feedback pages related to login.

Regular Security Testing: Conduct regular security assessments and testing, including specific testing for the login page.

Security Awareness: Train staff to follow secure coding practices and raise awareness of security risks.

Incident Response Plan: Develop an incident response plan to mitigate and recover from XSS attacks if they occur on the login page.

5. Risk Acceptance or Remediation:

Given the high risk level associated with a Reflected XSS vulnerability on a login page, remediation efforts should be a top priority. Swiftly implement security measures to mitigate the risk.

This revised risk assessment specifically addresses the potential impact and likelihood of a Reflected XSS vulnerability on a login.php page and provides guidance for risk mitigation in that context.

- **Recommendations:**
-
- **Medium Priority Recommendations:**

Regular Security Testing:

- Perform regular security assessments, including penetration testing and automated scanning, to identify and address XSS vulnerabilities promptly.

Security Training and Awareness:

- Train development and IT staff to follow secure coding practices, emphasizing the risks associated with XSS vulnerabilities and the importance of input validation and output encoding.

Web Application Firewall (WAF):

- Implement a Web Application Firewall that can detect and block malicious requests and payloads before they reach the web application.

Conclusion

Key Findings:

1. The web application has one or more instances of Reflected Cross-Site Scripting (XSS) vulnerabilities, notably on the login.php page.

2. These vulnerabilities expose the application to significant risks, including data exposure, unauthorized access, privacy breaches, financial loss, reputation damage, and potential legal consequences.

3. The likelihood of exploitation is notable due to the visibility and sensitivity of the login page, making it an attractive target for attackers.

Risks:

1.Data Exposure: Reflected XSS attacks could lead to the exposure of sensitive user data, including login credentials.

2.Unauthorized Access: Attackers can exploit the vulnerability to gain unauthorized access to user accounts, posing a serious threat to user data security.

3.Privacy Breach: A successful attack can result in a privacy breach, damaging trust and potentially leading to regulatory or legal consequences.

4.Reputation Damage: Security incidents related to the login page can harm the client's reputation and erode user trust.

5.Financial Loss: Reflected XSS vulnerabilities can lead to financial losses, particularly if attackers steal financial information or engage in unauthorized transactions.

Medium Priority: 5. **Regular Security Testing**: Conduct regular security assessments, including penetration testing and automated scanning, to detect and address XSS vulnerabilities.

Security Training and Awareness: Train development and IT staff on secure coding practices and the risks associated with XSS vulnerabilities.

Web Application Firewall (WAF): Implement a WAF to detect and block malicious requests and payloads.

Acknowledgments

Thanks for this opportunity that you give me and that will create more transferency between cyber world and humans.

Contact Information

Mail: onkarvmhaskar@gmail.com

Mobile: +91 9623918184