Website: http://testasp.vulnweb.com
Endpoint: Search.asp

Summary

The search field on the page Search.asp is vulnerable to a reflected Cross-Site Scripting (XSS) attack. This vulnerability occurs because user input is not properly sanitized before being displayed on the page, allowing for the injection of malicious JavaScript.

Vulnerability Details

- **Type:** Reflected XSS
- **Affected Parameter:** search (or relevant query parameter, if different)

Steps to Reproduce

1. **Craft a JavaScript Payload:** Prepare a malicious JavaScript payload. For demonstration purposes, the payload will be:

```
<script>prompt() </script>
```

2. **Create a Malicious Request:** Use the following crafted URL to inject the payload into the search parameter:

http://testasp.vulnweb.com/Search.asp?tfSearch=%3Cscript%3Eprompt%28%29%3C%2Fscript%3E

3. **Execute the Request:** Send the crafted link to a victim or open it in a browser. The JavaScript alert will execute, displaying the user's cookies.

Injection Demonstration

- **Crafted URL Example:**

Copy code

```
http://testasp.vulnweb.com/Search.asp?tfSearch=%3Cscript%3Eprompt%28%29%3C%2Fscript%3E
```

Impact

With user interaction, an attacker could execute arbitrary JavaScript code in a victim's browser, potentially allowing:

- Access to sensitive information such as cookies or session tokens.
- Unauthorized actions on behalf of the user.
- Impersonation of the user within the application.

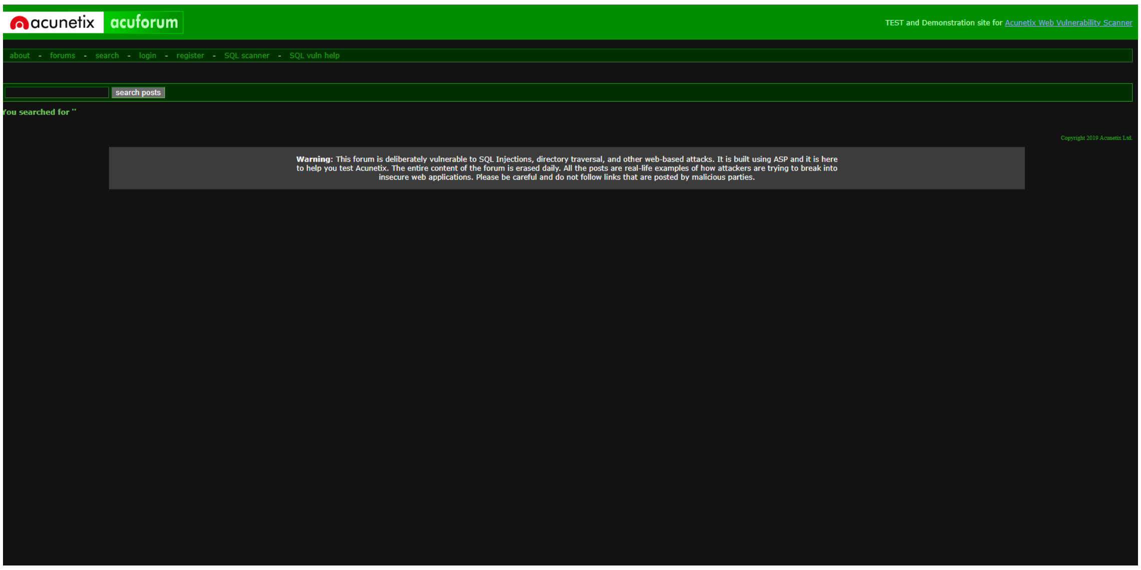
Supporting Material/References

- **Video Demonstration:** [Link to Video, if available]

- **Screenshots:** [Include any relevant screenshots here]

Mitigation Recommendations

1. **Input Validation:** Implement strict validation of all user inputs, especially in query parameters.
2. **Output Encoding:** Use context-aware output encoding methods to escape potentially dangerous characters.
3. **Content Security Policy (CSP):** Consider implementing CSP to mitigate the impact of XSS vulnerabilities.

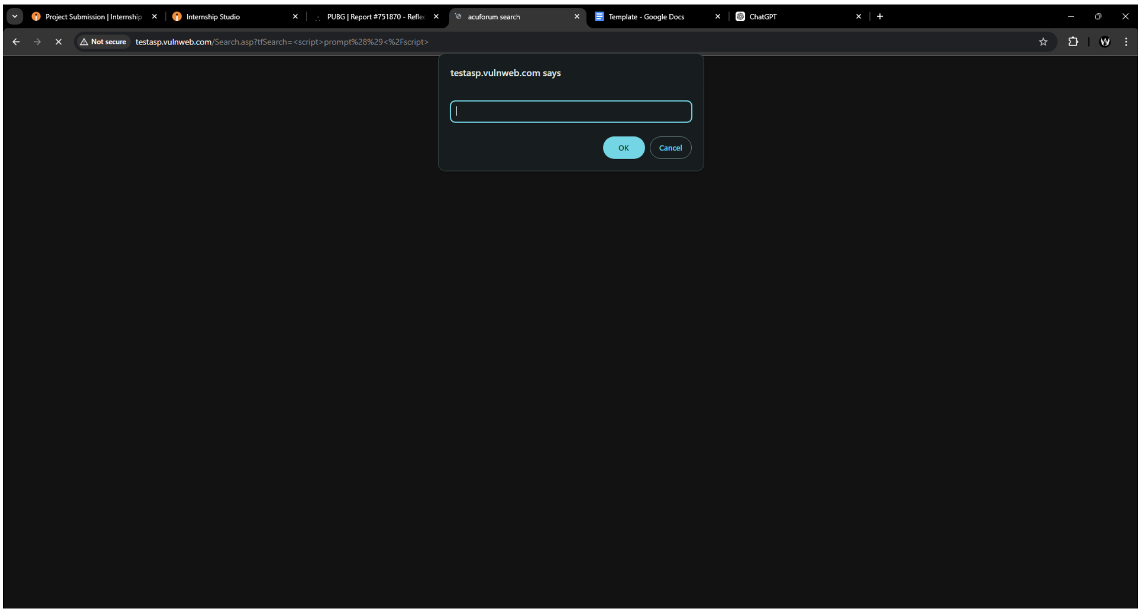

acunetix acuforum
about - forums - search - login - register - SQL scanner - SQL vuln help
search posts

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

You searched for ''

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.



testasp.vulnweb.com/Search.asp?tfSearch=<script>prompt%28%29<%2Fscript>

testasp.vulnweb.com says

Website: http://testasp.vulnweb.com
Endpoint: Login.asp

Summary

The login page located at
http://testasp.vulnweb.com/Login.asp?RetURL=%2FTemplatize%2Easp%3Fitem%3Dhtml%2Fabout%2Ehtml

is vulnerable to a SQL Injection (SQLi) attack. An attacker can bypass the authentication mechanism and gain unauthorized access by injecting malicious SQL code into the username field.

Vulnerability Details

- **Type:** SQL Injection
- **Affected Parameter:** Username (or "user")
- **SQL Injection Technique Used:** '-- (commenting out the remainder of the SQL query)
- **Payload Used:**
    - **Username:** admin'--
    - **Password:** admin

Steps to Reproduce

1. **Navigate to the Login Page:** Go to the following URL: http://testasp.vulnweb.com/Login.asp?RetURL=%2FTemplatize%2Easp%3Fitem%3Dhtml%2Fabout%2Ehtml
2. **Enter the Payload:**
    - **Username:** admin'--
    - **Password:** admin

The -- sequence comments out the rest of the SQL query, allowing an attacker to bypass authentication.

3. **Login Successfully:** After submitting the form with this payload, the login will be bypassed, and the attacker will be authenticated as an administrator (or another valid user).

Injection Demonstration

- **Payload Example:**

Username: admin'--

Password: admin

- **SQL Query After Injection:**
  The login query would look something like this:

SELECT * FROM users WHERE username = 'admin'--' AND password = 'admin';

The -- comments out the rest of the query, effectively ignoring the password check and logging the user in as "admin."

Impact

With this vulnerability, an attacker can:

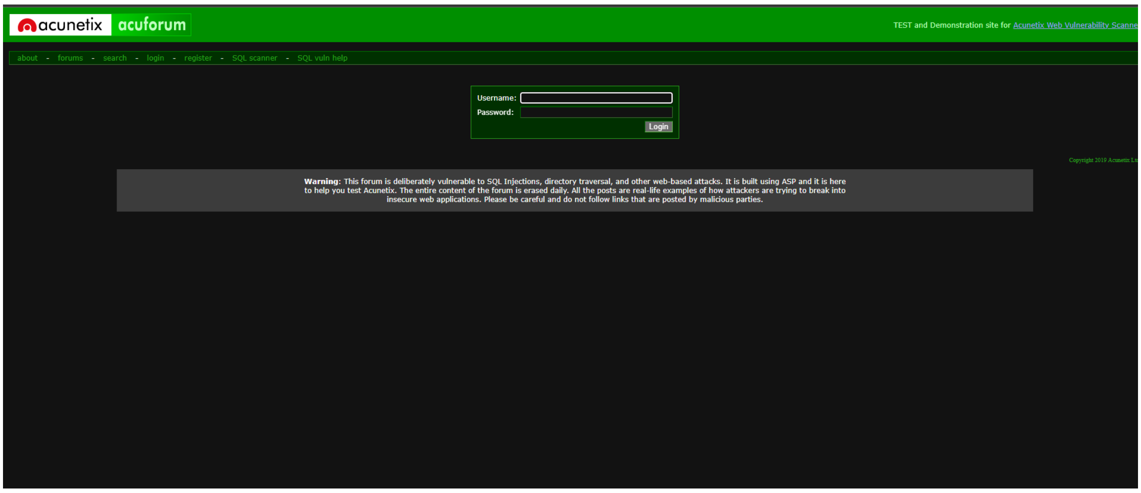
- **Bypass Authentication:** Log in as any user, including administrators, by injecting the appropriate SQL commands.
- **Access Sensitive Data:** Once logged in, an attacker could access sensitive user data, modify information, or perform other administrative actions.
- **Potential Data Compromise:** If the vulnerability extends to other parts of the site, it could be used to extract or manipulate sensitive information in the database.

Supporting Material/References

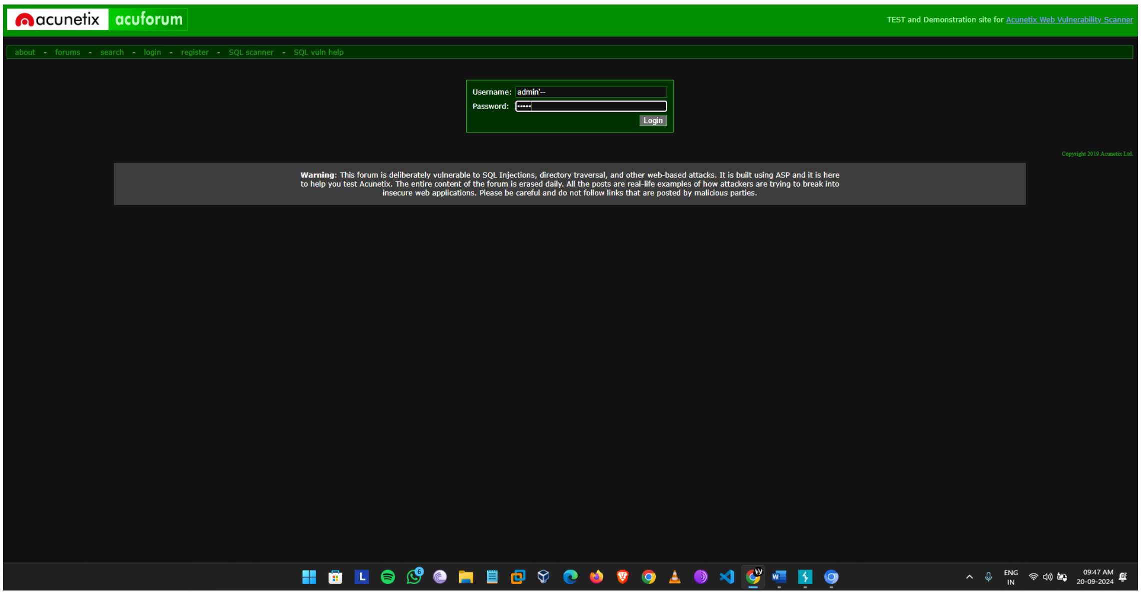
- **Screenshots:** [Include any screenshots that demonstrate the successful login]
- **Video Demonstration:** [Link to video if applicable]

Mitigation Recommendations

1. **Use Parameterized Queries:** All database queries should use prepared statements or parameterized queries to prevent SQL injection attacks.
2. **Input Validation:** Implement strict input validation and sanitization for all user inputs.
3. **Use Least Privilege Principle:** Ensure that database connections use the least privilege necessary to operate, reducing the impact of a successful SQL injection.
4. **Error Handling:** Avoid displaying detailed error messages to users, as these can give attackers clues about the database structure.


acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanne
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login
Copyright 2019 Acunetix Lt

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.



acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help

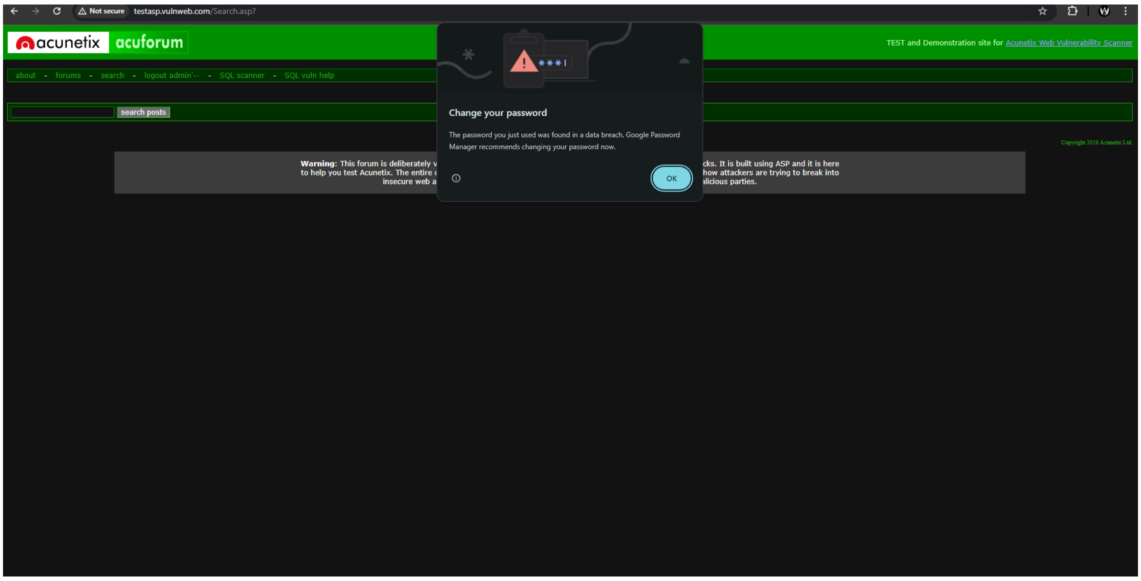
Username: admin'--

Password: •••••

Login
Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

ENG
IN
09:47 AM
20-09-2024



Not secure
testasp.vulnweb.com/Search.asp?
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout admin'-- - SQL scanner - SQL vuln help
search posts
Copyright 2019 Acunetix Ltd.

Change your password

The password you just used was found in a data breach. Google Password Manager recommends changing your password now.

Warning: This forum is deliberately v… cks. It is built using ASP and it is here
to help you test Acunetix. The entire c… how attackers are trying to break into
insecure web a… alicious parties.