Penetration Test Report

for

Acunetix Web Application

Contents

1. Executive summary

Securing a company's web applications is today's most overlooked aspect of securing the enterprise. Web application hacking is on the rise with as many as 75% of cyber attacks done at web application level or via the web. Most corporations have secured their data at the network level, but have overlooked the crucial step of checking whether their web applications are vulnerable to attack. Web applications, which often have a direct line into the company's most valuable data assets, are online 24/7, completely unprotected by a firewall and therefore easy prey for attackers.

Acunetix was founded with this threat in mind. We realised the only way to combat web site hacking was to develop an automated tool that could help companies scan their web applications for vulnerabilities. In July 2005, Acunetix Web Vulnerability Scanner was released - a tool that crawls the website for vulnerabilities to SQL injection, cross site scripting and other web attacks before hackers do.

2. Scope

The security assessment is conducted to validate that all the security controls and requirements have been successfully implemented in the Acunetix web application. Security testing validates against any possible remote adversaries and attacks by intruders, hackers, or malicious users of the web application with a clear and defined goal of making them secure.

The goal is to conduct penetration testing of the Acunetix web application.

2.1. Web Applications

The following web applications are in scope for ACUNETIX web application penetration testing.

Application Name	Test URL	Target Version
Acunetix	http://testasp.vulnweb.com	Test Environment

2.2. Out of scope

Considering the penetration testing of the Altoro Mutual web application, the below-mentioned components are out of scope.

- Segmentation checks from/ to any network/ IP.
- Virtualization and network infrastructure
- Intrusion detection/prevention systems
- Social engineering attacks
- Denial of service attack
- Fixing network infrastructure, software-related issues, third-party component/library issues, or hosting environment
- Fixing reported vulnerabilities from penetration testing
- Security review of code and architecture

2.3. Tools used for penetration testing.

The table below provides details about the tools used for penetration testing activities.

Tool	Usage
Burp Suite Community Edition.	Vulnerability and Web Security Testing.

3. Penetration Test Summary

The following sections provide detailed results of the penetration testing.

3.1. Vulnerability statistics

Below are the identified vulnerabilities arranged by severity distribution.

3.1.1. Severity Levels for Security Issues

1. **Critical**

   Critical vulnerabilities are the most severe and can result in the complete compromise of a system or network, allowing an attacker to gain full control and access to sensitive data. Such vulnerabilities are usually remotely exploitable and require immediate attention.

2. **High**

   High-severity vulnerabilities can also be exploited remotely and have a significant impact on system security. These vulnerabilities can allow attackers to gain privileged access, perform unauthorized actions, or steal sensitive data.

3. **Medium**

   Medium-severity vulnerabilities are less severe than critical and high vulnerabilities but can still pose a risk to the system's security. These vulnerabilities may not be remotely exploitable and may require user interaction or local access to the system to be exploited.

4. **Low**

   Low-severity vulnerabilities are generally not considered critical and may only result in minor impacts on the system. These vulnerabilities are often discovered during vulnerability assessments or penetration testing and may require a certain level of expertise to exploit.

5. **Informational**

   Informational vulnerabilities do not pose an immediate threat to system security and are usually only discovered during vulnerability scanning or auditing. These vulnerabilities do not require remediation but can provide valuable information about the system's security posture.

5.1.2. Severity of Vulnerabilities

Overview of the identified web application vulnerabilities grouped by severity.

- **High severity** – 4 Vulnerabilities
- **Medium severity –** 1 Vulnerability

5.2. Summary of security issues

This section provides a high-level overview of the results obtained during the penetration test. These results must be evaluated based on a Risk management process and the appropriate measures must be taken to mitigate security risks to an acceptable level based on OWASP requirements.

The following table summarizes the different security issues.

Ref. No	Name	Severity	Revalidation Status
6.1	Weak Lockout mechanism	High	Open
6.2	Cryptographic Failure	High	Open
6.3	SQL Injections	High	Open
6.4	Broken Access Control	High	Open
6.5	IDOR	Medium	Open

6. Vulnerabilities Details

6.1. Weak lockout mechanism

Risk Severity	Risk Impact	Risk of Likelihood	Ease of Discovery	Affected Security Objective
High	High	High	Moderate	Loss of confidentiality and Integrity.

Vulnerability Details

Account lockout mechanisms are used to mitigate brute force attacks. Some of the attacks that can be defeated by using lockout mechanism:

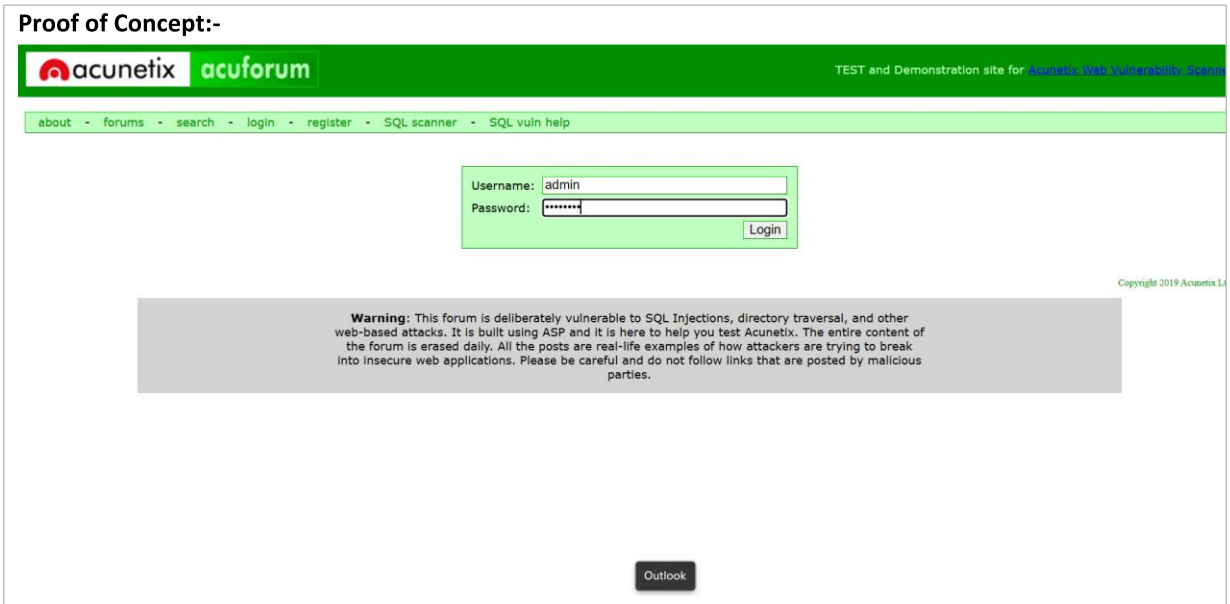
- Login password or username guessing attack.
- Code guessing on any 2FA functionality or Security Questions.

Account lockout mechanisms require a balance between protecting accounts from unauthorized access and protecting users from being denied authorized access. Accounts are typically locked after 3 to 5 unsuccessful attempts and can only be unlocked after a predetermined period of time, via a self-service unlock mechanism, or intervention by an administrator.

Steps to reproduce:

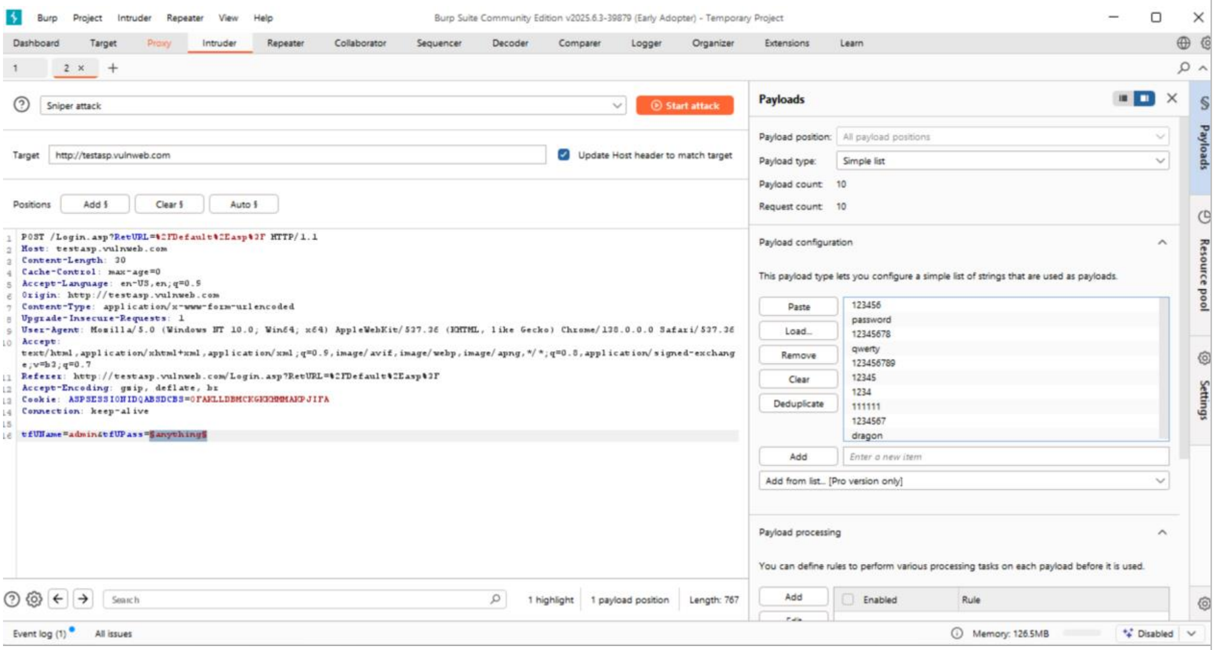
1. Visit the login page of website http://testasp.vulnweb.com
2. Enter a valid user name and an invalid password and intercept this request in Burp Suite.
3. Send the request to intruder and select the password as input field.
4. Select more than 10 payloads and start the attack.
5. Observe that the account does not lockout after 5 invalid password attempts.

Proof of Concept:-


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

Username: admin
Password: ••••••••

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.



Target: http://testasp.vulnweb.com
☑ Update Host header to match target

Positions

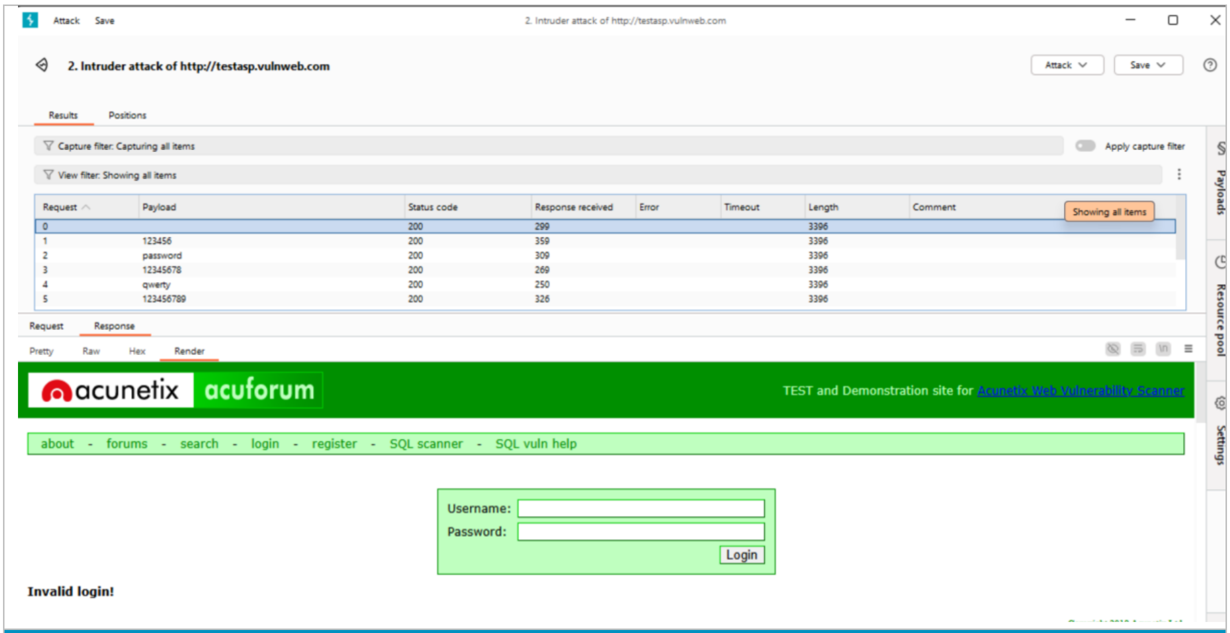
```
POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.com
Content-Length: 30
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://testasp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchang
e;v=b3;q=0.7
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Accept-Encoding: gzip, deflate, br
Cookie: ASPSESSIONIDQABSDCBS=OFAKLLDBMCKGKKMMMAKPJIFA
Connection: keep-alive

tfUName=admin&tfUPass=§anything§
```

Payload position: All payload positions
Payload type: Simple list
Payload count: 10
Request count: 10

This payload type lets you configure a simple list of strings that are used as payloads.

```
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
```

You can define rules to perform various processing tasks on each payload before it is used.



Attack
Save
2. Intruder attack of http://testasp.vulnweb.com
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Showing all items
Payloads
Resource pool
Settings
Request
Response
Pretty
Raw
Hex
Render
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
Login

2. Intruder attack of http://testasp.vulnweb.com

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	299			3396	
1	123456	200	359			3396	
2	password	200	309			3396	
3	12345678	200	269			3396	
4	qwerty	200	250			3396	
5	123456789	200	326			3396	

Username:

Password:

Invalid login!

Impact

1. Attackers can brute-force valid credentials and gain unauthorized access to user or admin accounts.
2. Once logged in, attackers may access sensitive personal, financial, or internal data tied to the compromised account.
3. If high-privilege accounts (e.g., admins) are targeted, it could lead to broader system control or data manipulation.

Remediation/Mitigation

1. Temporarily lock accounts after a defined number of failed login attempts (e.g., 5 attempts, 15-minute lockout).
2. Restrict the number of login attempts per IP/user within a specific time window to slow down brute-force attempts.
3. Introduce CAPTCHA after several failed logins to block automated tools.
4. Require multi-factor authentication to add a second layer of defense even if credentials are brute-forced.

References

1. WSTG - v4.2 | OWASP Foundation
2. Brute Force Attack | OWASP Foundation

6.2. Cryptographic Failure

Risk Severity	Risk Impact	Risk of Likelihood	Ease of Discovery	Affected Security Objective
High	High	High	High	Loss of confidentiality, Authentication and Integrity.

Vulnerability Details

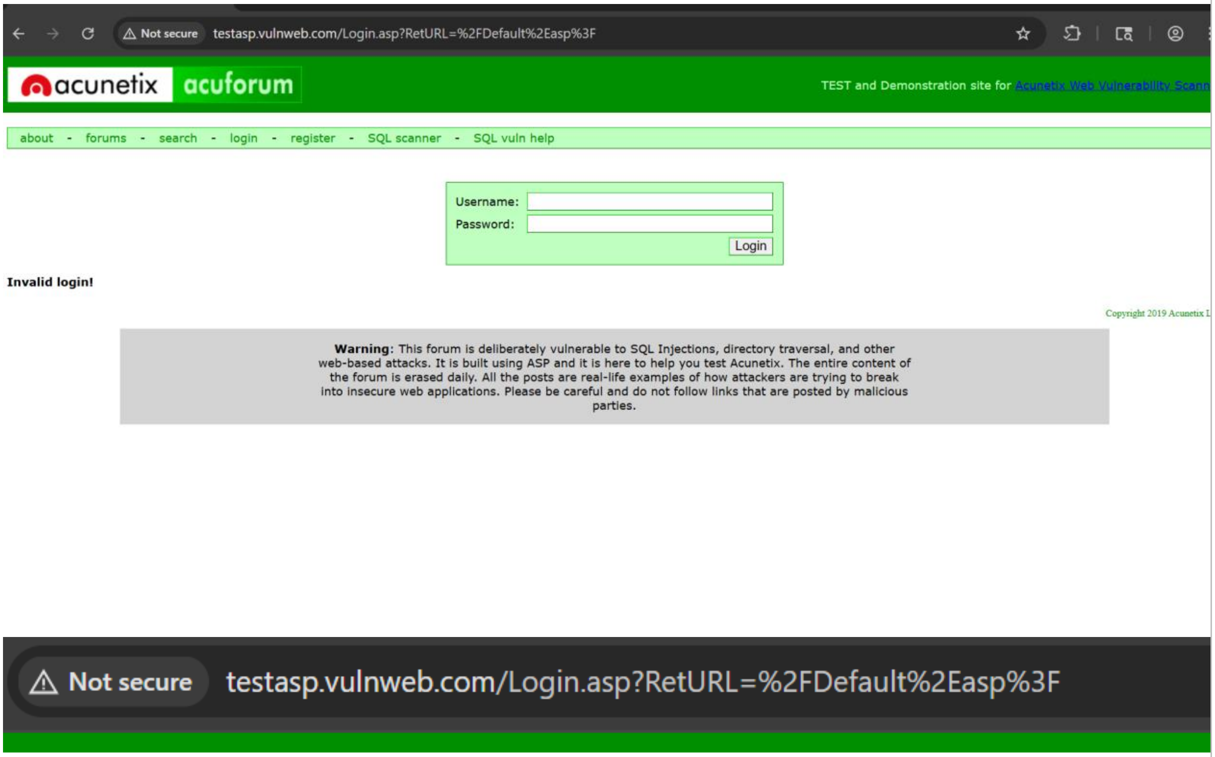
Cryptographic Failure (previously called *Sensitive Data Exposure* in OWASP Top 10 2017) occurs when sensitive data like passwords, credit card numbers, or session tokens are not properly protected using strong encryption. It includes issues in:

- Data transmission (over the network)
- Data storage (in databases or files)
- Encryption implementation

Steps to reproduce:

1. Visit the login page of website http://testasp.vulnweb.com
2. Simplest way is to see the website is using HTTP or HTTPS
3. Observe how the url starts in the address bar
4. If the website uses HTTP then it is insecure

Proof of Concept:-



Not secure
testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scann
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login
Copyright 2019 Acunetix L

Invalid login!

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.

Not secure testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F

Impact

1. Credentials can be stolen during login
2. Sensitive data (like personal info) gets exposed
3. Attackers can perform Man-in-the-Middle (MitM) attacks
4. Session tokens can be hijacked
5. Confidentiality of user data is lost
6. Violates data protection laws (like GDPR, PCI-DSS)
7. Damages user trust and company reputation
8. Enables attackers to move deeper into the system

Remediation/Mitigation

1. Use HTTPS (TLS 1.2 or higher) across the entire site
2. Never transmit sensitive data over HTTP
3. Store passwords using strong hashing (e.g., bcrypt, Argon2)
4. Avoid storing sensitive data unless absolutely necessary
5. Use up-to-date and trusted cryptographic libraries
6. Rotate and protect encryption keys properly
7. Set Secure and HttpOnly flags on session cookies

8. Perform regular cryptographic configuration audits
References
3. [WSTG - v4.2 | OWASP Foundation](#)
4. [A02 Cryptographic Failures - OWASP Top 10:2021](#)

6.3. SQL Injections

Risk Severity	Risk Impact	Risk of Likelihood	Ease of Discovery	Affected Security Objective
High	High	High	High	Loss of confidentiality and Integrity.

Vulnerability Details

SQL Injection is a critical vulnerability that occurs when user-supplied input is improperly validated and directly embedded into SQL queries. This allows attackers to manipulate database queries and potentially bypass authentication, retrieve or modify sensitive data, and in severe cases, gain full control over the backend database. During testing, it was observed that the login form is vulnerable to SQL injection by using input such as ' OR '1'='1 in the username field, which resulted in unauthorized access. This exposes both confidentiality and integrity risks, as attackers could extract user data or tamper with records. The vulnerability was easily discoverable using basic tools like Burp Suite and indicates a lack of input sanitization and the absence of parameterized queries on the backend.

Steps to reproduce:

1. Visit the login page of website http://testasp.vulnweb.com
2. Input a valid username
3. In password field input ‘OR’1’=’1

- Imagine the backend SQL looks like:

SELECT * FROM users WHERE username = 'USER' AND password = 'PASS'

- If you inject:

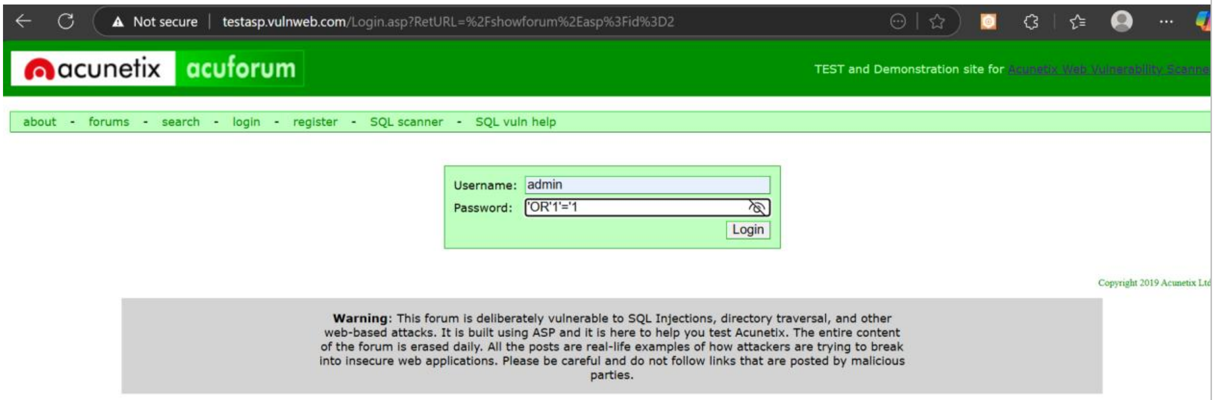
' OR '1'='1

- It becomes:

SELECT * FROM users WHERE username = '' OR '1'='1' AND password = ''

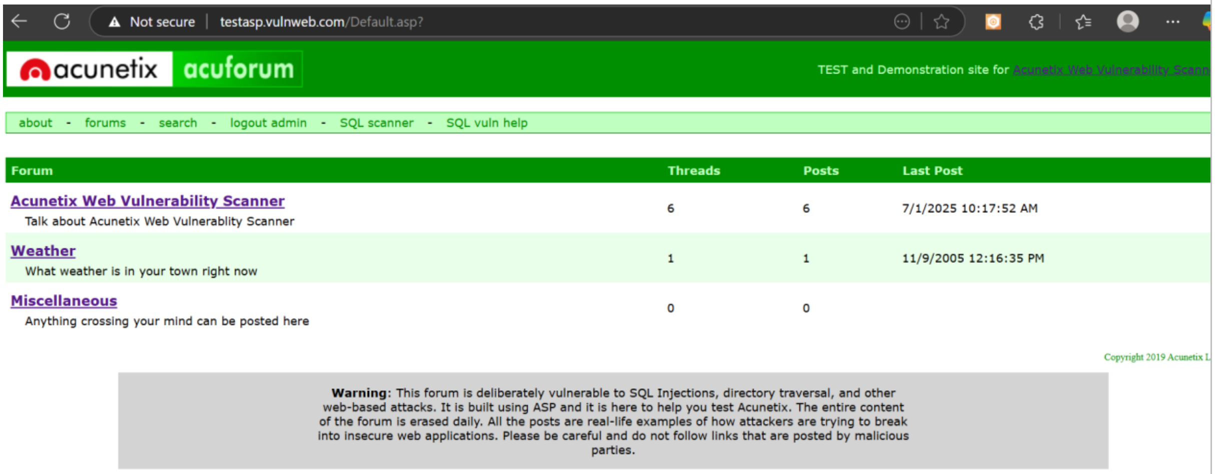
- Since '1'='1' is always true, login bypass succeeds.

Proof of Concept:-


Not secure
testasp.vulnweb.com/Login.asp?RetURL=%2Fshowforum%2Easp%3Fid%3D2
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanne
about - forums - search - login - register - SQL scanner - SQL vuln help
Login
Copyright 2019 Acunetix Ltd

Username: admin
Password: 'OR'1'='1

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.


Not secure
testasp.vulnweb.com/Default.asp?
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scann
about - forums - search - logout admin - SQL scanner - SQL vuln help
Copyright 2019 Acunetix L

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerablity Scanner	6	6	7/1/2025 10:17:52 AM
Weather What weather is in your town right now	1	1	11/9/2005 12:16:35 PM
Miscellaneous Anything crossing your mind can be posted here	0	0	

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.

Impact

1. Attackers can bypass login authentication
2. Unauthorized access to database records
3. Exfiltration of sensitive data (e.g., user info, passwords)
4. Potential for full database compromise
5. Application logic can be altered or broken

Remediation/Mitigation

1. Use parameterized queries (prepared statements)
2. Sanitize and validate all user inputs
3. Apply least privilege on database users
4. Use web application firewalls (WAFs)
5. Disable detailed error messages in production
6. Regularly test for injection with automated tools

References

1. WSTG - v4.2 | OWASP Foundation
2. A03 Injection - OWASP Top 10:2021

6.4. Broken Access Control

Risk Severity	Risk Impact	Risk of Likelihood	Ease of Discovery	Affected Security Objective
High	High	High	Moderate	Loss of confidentiality and Integrity.

Vulnerability Details

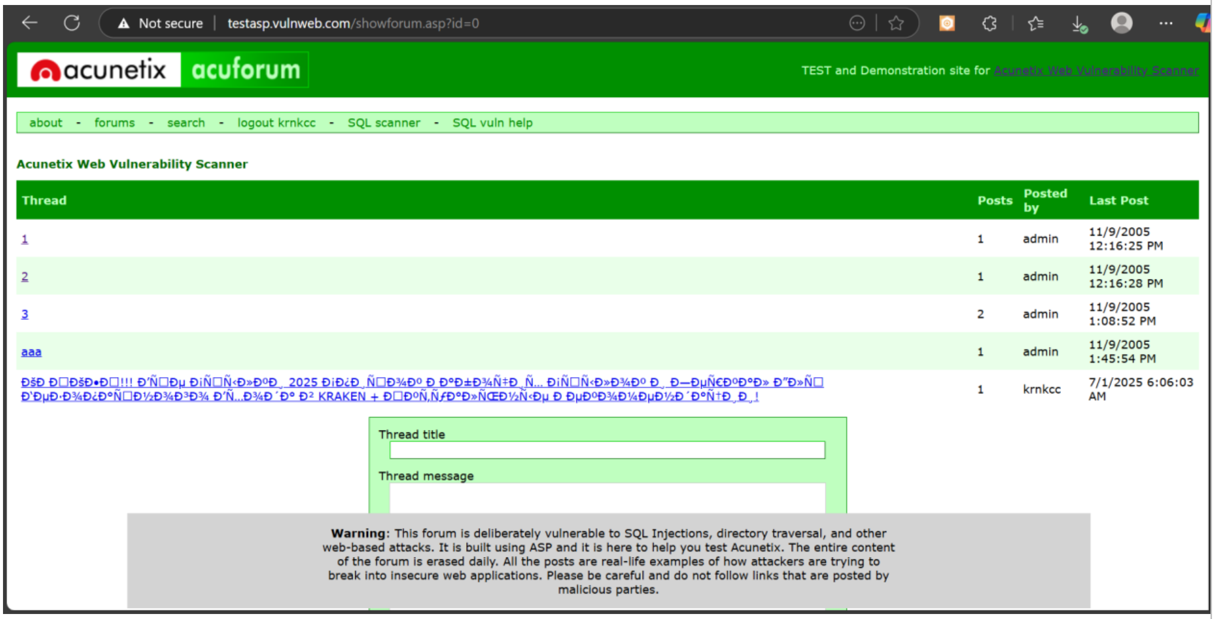
Broken Access Control occurs when the application fails to enforce proper authorization checks, allowing users to perform actions or access data beyond their intended permissions. During testing, it was found that by manipulating URL parameters such as id or forumid, authenticated users were able to access data belonging to other users. For example, changing the thread ID in the URL revealed forum posts that were not associated with the logged-in user. This indicates a lack of proper server-side validation of ownership or access rights.

As a result, sensitive user information can be disclosed, violating privacy and confidentiality. This vulnerability has a high impact and is moderately easy to discover using manual testing or simple tools like Burp Suite, making it a significant security risk.

Steps to reproduce:

1. Visit the login page of website http://testasp.vulnweb.com
2. Login to the website and browse other users who have posted on the website
3. Use those usernames and login with 'OR'1'='1
4. Using sql injection method we can browse and access other user's profiles

Proof of Concept:-



Not secure | testasp.vulnweb.com/showforum.asp?id=0

acunetix acuforum

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - logout krnkcc - SQL scanner - SQL vuln help

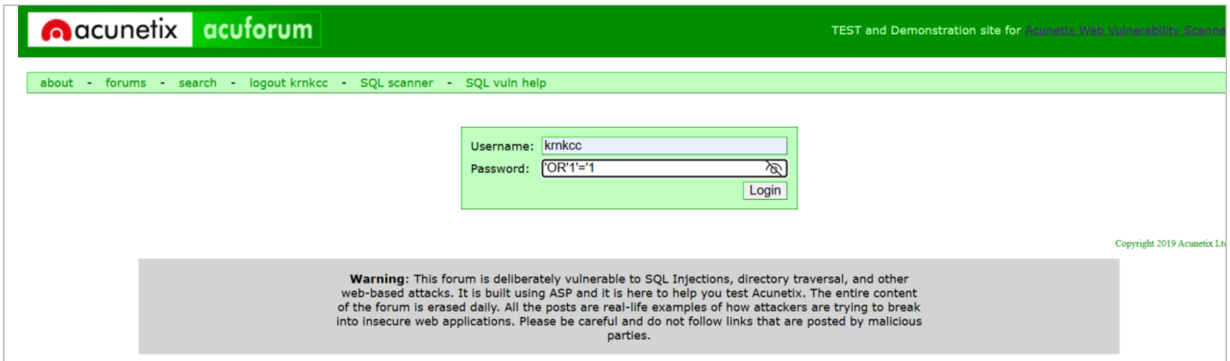
Acunetix Web Vulnerability Scanner

Thread	Posts	Posted by	Last Post
1	1	admin	11/9/2005 12:16:25 PM
2	1	admin	11/9/2005 12:16:28 PM
3	2	admin	11/9/2005 1:08:52 PM
aaa	1	admin	11/9/2005 1:45:54 PM
ĐšĐ Đ□ĐšĐ•Đ□!!! Đ'Ñ□Đµ ĐiÑ□Ñ‹Đ»ĐºĐ¸ 2025 ĐiĐ¿Đ¸Ñ□Đ¾Đº Đ ĐºĐ±Đ¾Ñ‡Đ¸Ñ… ĐiÑ□Ñ‹Đ»Đ¾Đº Đ¸ Đ—ĐµÑ€ĐºĐºĐ» Đ"Đ»Ñ□ Đ'ĐµĐ·Đ¾Đ¿ĐºÑ□Đ½Đ¾Đ³Đ¾ Đ'Ñ…Đ¾Đ´Đº Đ² KRAKEN + Đ□ĐºÑ‚ÑƒĐºĐ»ÑŒĐ½Ñ‹Đµ Đ ĐµĐºĐ¾Đ¼ĐµĐ½Đ´ĐºÑ†Đ¸Đ¸ !	1	krnkcc	7/1/2025 6:06:03 AM

Thread title

Thread message

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.

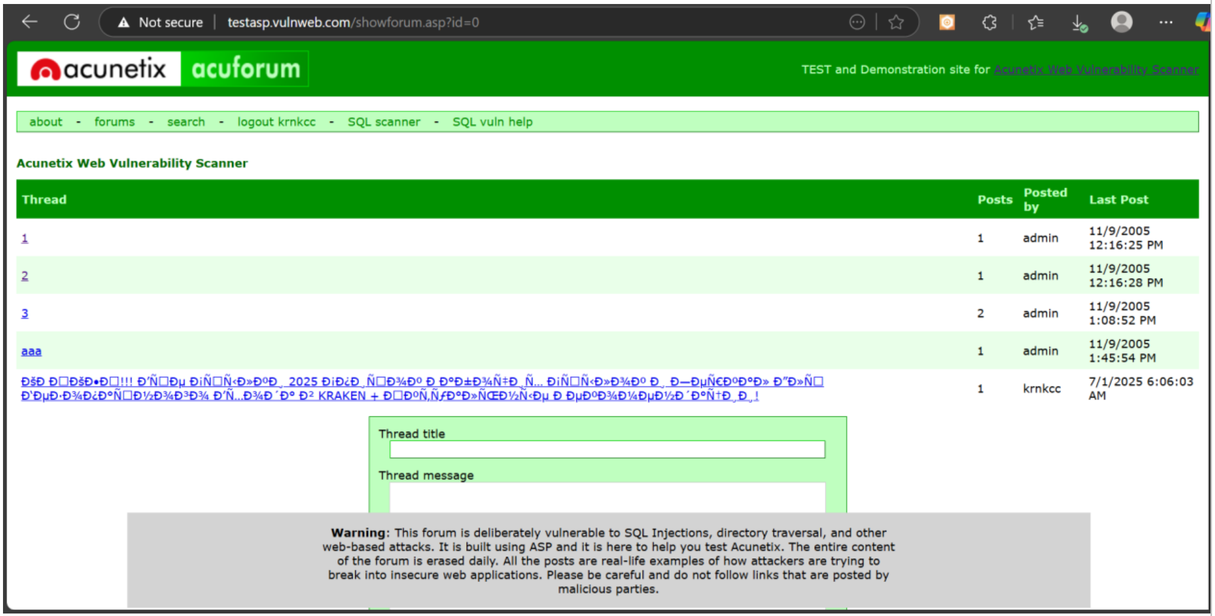


acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanne
about - forums - search - logout krnkcc - SQL scanner - SQL vuln help
Login
Copyright 2019 Acunetix Lt

Username: krnkcc

Password: 'OR'1'='1

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.



Not secure
testasp.vulnweb.com/showforum.asp?id=0
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout krnkcc - SQL scanner - SQL vuln help

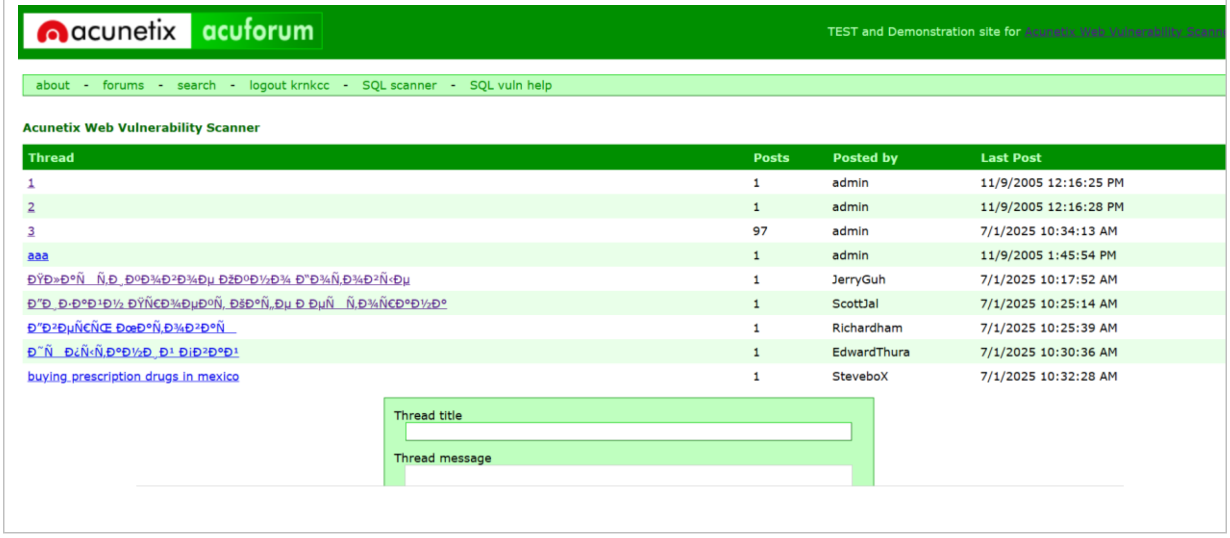
Acunetix Web Vulnerability Scanner

Thread	Posts	Posted by	Last Post
1	1	admin	11/9/2005 12:16:25 PM
2	1	admin	11/9/2005 12:16:28 PM
3	2	admin	11/9/2005 1:08:52 PM
aaa	1	admin	11/9/2005 1:45:54 PM
ÐšÐ Ð□ÐšÐ•Ð□!!! Ð'Ñ□Ðµ ÐiÑ□Ñ‹Ð»ÐºÐ¸ 2025 ÐiÐ¿Ð¸Ñ□Ð¾Ðº Ð Ð°Ð±Ð¾Ñ‡Ð¸Ñ… ÐiÑ□Ñ‹Ð»Ð¾Ðº Ð¸ Ð—ÐµÑ€ÐºÐ°Ð» Ð"Ð»Ñ□ Ð'ÐµÐ·Ð¾Ð¿Ð°Ñ□Ð½Ð¾Ð³Ð¾ Ð'Ñ…Ð¾Ð´Ð° Ð² KRAKEN + Ð□ÐºÑ‚ÑƒÐ°Ð»ÑŒÐ½Ñ‹Ðµ Ð ÐµÐºÐ¾Ð¼ÐµÐ½Ð´Ð°Ñ†Ð¸Ð¸!	1	krnkcc	7/1/2025 6:06:03 AM

Thread title

Thread message

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.



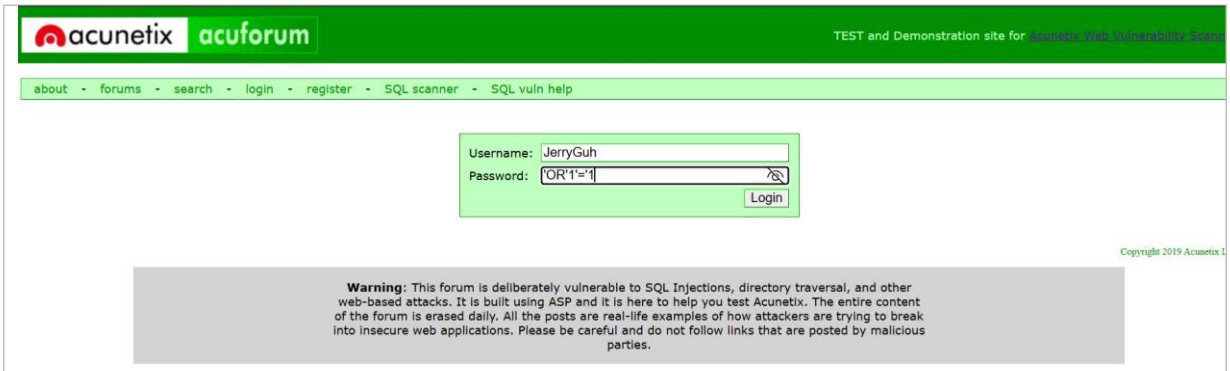
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scann
about - forums - search - logout krnkcc - SQL scanner - SQL vuln help

Acunetix Web Vulnerability Scanner

Thread	Posts	Posted by	Last Post
1	1	admin	11/9/2005 12:16:25 PM
2	1	admin	11/9/2005 12:16:28 PM
3	97	admin	7/1/2025 10:34:13 AM
aaa	1	admin	11/9/2005 1:45:54 PM
ÐŸÐ»Ð°Ñ Ñ‚Ð¸ Ð¿Ð¾Ð²Ð¾Ðµ ÐžÐ¿Ð½Ð¾ Ð"Ð¾Ñ‚Ð¾Ð²Ñ‹Ðµ	1	JerryGuh	7/1/2025 10:17:52 AM
Ð"Ð¸Ð·Ð°Ð¹Ð½ ÐŸÑ€Ð¾ÐµÐºÑ‚ ÐšÐ°Ñ„Ðµ Ð ÐµÑ Ñ‚Ð¾Ñ€Ð°Ð½Ð°	1	ScottJal	7/1/2025 10:25:14 AM
Ð"Ð²ÐµÑ€ÑŒ ÐœÐ°Ñ‚Ð¾Ð²Ð°Ñ	1	Richardham	7/1/2025 10:25:39 AM
Ð˜Ñ Ð¿Ñ‹Ñ‚Ð°Ð½Ð¸Ð¹ ÐiÐ²Ð°Ð¹	1	EdwardThura	7/1/2025 10:30:36 AM
buying prescription drugs in mexico	1	SteveboX	7/1/2025 10:32:28 AM

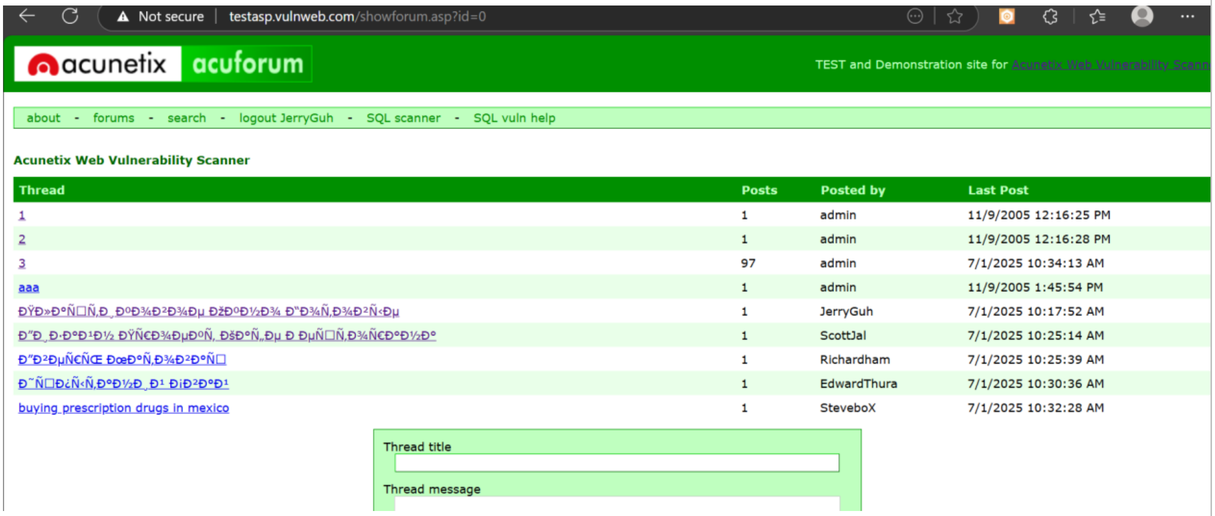
Thread title

Thread message


acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scann
about - forums - search - login - register - SQL scanner - SQL vuln help
Login
Copyright 2019 Acunetix L

Username: JerryGuh
Password: 'OR'1'='1

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.


Not secure
testasp.vulnweb.com/showforum.asp?id=0
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scann
about - forums - search - logout JerryGuh - SQL scanner - SQL vuln help
Thread title
Thread message

Acunetix Web Vulnerability Scanner

Thread	Posts	Posted by	Last Post
1	1	admin	11/9/2005 12:16:25 PM
2	1	admin	11/9/2005 12:16:28 PM
3	97	admin	7/1/2025 10:34:13 AM
aaa	1	admin	11/9/2005 1:45:54 PM
ÐŸÐ»Ð°Ñ□Ñ‚Ð¸ ÐºÐ¾Ð²Ð¾Ðµ ÐžÐºÐ½Ð¾ Ð“Ð¾Ñ‚Ð¾Ð²Ñ‹Ðµ	1	JerryGuh	7/1/2025 10:17:52 AM
Ð”Ð¸Ð·Ð°Ð¹Ð½ ÐŸÑ€Ð¾ÐµÐºÑ‚ ÐšÐ°Ñ„Ðµ Ð ÐµÑ□Ñ‚Ð¾Ñ€Ð°Ð½Ð°	1	ScottJal	7/1/2025 10:25:14 AM
Ð”Ð²ÐµÑ€ÑŒ ÐœÐ°Ñ‚Ð¾Ð²Ð°Ñ□	1	Richardham	7/1/2025 10:25:39 AM
Ð˜Ñ□Ð¿Ñ‹Ñ‚Ð°Ð½Ð¸Ð¹ Ð¡Ð²Ð°Ð¹	1	EdwardThura	7/1/2025 10:30:36 AM
buying prescription drugs in mexico	1	SteveboX	7/1/2025 10:32:28 AM

Impact

1. Unauthorized users can access restricted pages or data
2. Sensitive user or admin information may be exposed
3. Can lead to data leakage, manipulation, or account takeover
4. Serious damage if admin-level functions are accessible

Remediation/Mitigation

1. Enforce server-side access controls for every resource
2. Implement role-based access control (RBAC)
3. Avoid relying on client-side checks (JavaScript/UI-based controls)
4. Use access control libraries and middleware consistently
5. Regularly test access control logic with authenticated and unauthenticated roles

References

1. WSTG - v4.2 | OWASP Foundation
2. A03 Injection - OWASP Top 10:2021
3. A01 Broken Access Control - OWASP Top 10:2021

6.5. IDOR

Risk Severity	Risk Impact	Risk of Likelihood	Ease of Discovery	Affected Security Objective
Medium	Moderate	High	High	Loss of confidentiality and authorization.

Vulnerability Details

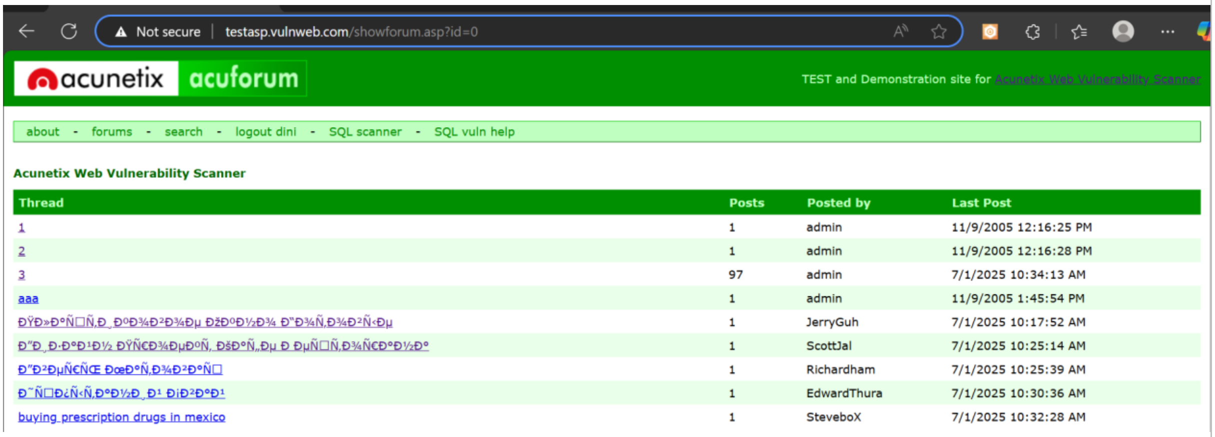
Insecure Direct Object Reference (IDOR) is a vulnerability that occurs when an application exposes internal object identifiers (like user IDs, record numbers, or document names) in URLs or request parameters, without properly validating the user's authorization to access them. During testing, it was observed that changing numeric values in the URL (such as showthread.asp?id=1) allowed access to different data records. Since the server does not enforce access control on these parameters, any user can manipulate the ID to retrieve or interact with data belonging to others.

This directly impacts the confidentiality of the application and may result in sensitive user information being exposed. The vulnerability is easily discoverable, as it requires only basic URL tampering and observation of the response behavior.

Steps to reproduce:

1. Visit the login page of website http://testasp.vulnweb.com
2. Visit page acuforum Acunetix Web Vulnerability Scanner after logging in
3. Manipulate the id number in the url ?id=0

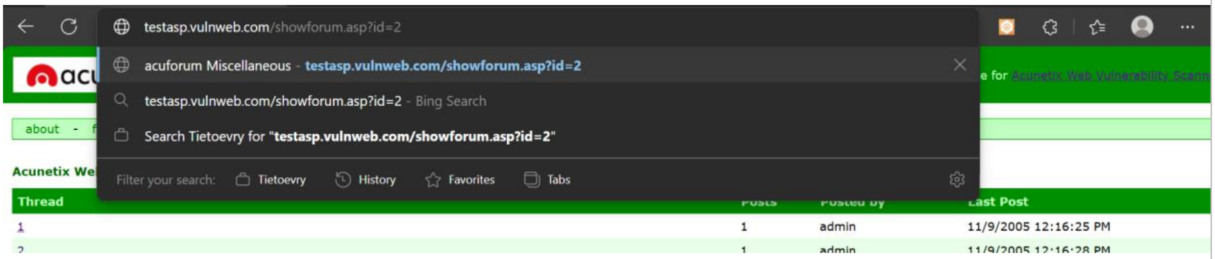
Proof of Concept:-



Not secure
testasp.vulnweb.com/showforum.asp?id=0
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout dini - SQL scanner - SQL vuln help

Acunetix Web Vulnerability Scanner

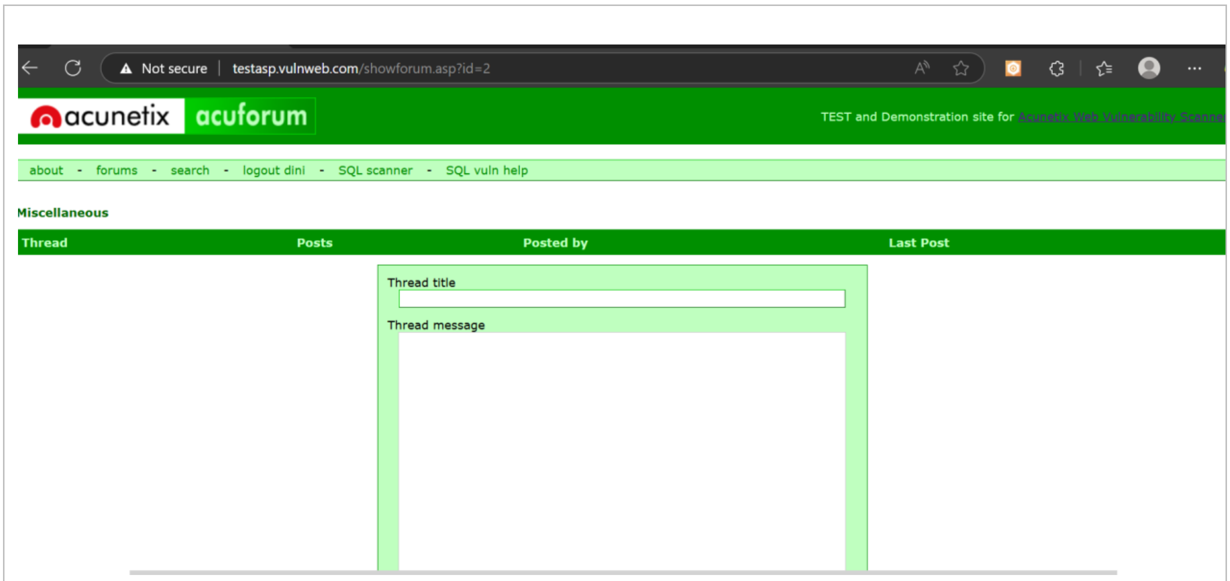
Thread	Posts	Posted by	Last Post
1	1	admin	11/9/2005 12:16:25 PM
2	1	admin	11/9/2005 12:16:28 PM
3	97	admin	7/1/2025 10:34:13 AM
aaa	1	admin	11/9/2005 1:45:54 PM
ĐŸĐ»Đ°Ñ□Ñ‚Đ¸ĐºĐ¾Đ²Đ¾Đµ ĐžĐºĐ½Đ¾ Đ"Đ¾Ñ‚Đ¾Đ²Ñ‹Đµ	1	JerryGuh	7/1/2025 10:17:52 AM
Đ"Đ¸Đ·Đ°Đ¹Đ½ ĐŸÑ€Đ¾ĐµĐºÑ‚ ĐšĐ°Ñ„Đµ Đ ĐµÑ□Ñ‚Đ¾Ñ€Đ°Đ½Đ°	1	ScottJal	7/1/2025 10:25:14 AM
Đ"Đ²ĐµÑ€ÑŒ ĐœĐ°Ñ‚Đ¾Đ²Đ°Ñ□	1	Richardham	7/1/2025 10:25:39 AM
Đ˜Ñ□Đ¿Ñ‹Ñ‚Đ°Đ½Đ¸Đ¹ Đ¡Đ²Đ°Đ¹	1	EdwardThura	7/1/2025 10:30:36 AM
buying prescription drugs in mexico	1	SteveboX	7/1/2025 10:32:28 AM



testasp.vulnweb.com/showforum.asp?id=2
acuforum Miscellaneous - testasp.vulnweb.com/showforum.asp?id=2
testasp.vulnweb.com/showforum.asp?id=2 - Bing Search
Search Tietoevry for "testasp.vulnweb.com/showforum.asp?id=2"
Filter your search: Tietoevry History Favorites Tabs
about
e for Acunetix Web Vulnerability Scann

Acunetix We

Thread	Posts	Posted by	Last Post
1	1	admin	11/9/2005 12:16:25 PM
2	1	admin	11/9/2005 12:16:28 PM


Not secure | testasp.vulnweb.com/showforum.asp?id=2
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanne
about - forums - search - logout dini - SQL scanner - SQL vuln help
Miscellaneous
Thread
Posts
Posted by
Last Post
Thread title
Thread message

All threads may be public, so changing the id just shows other public content.

The app is designed for vulnerability testing, not real data segregation — so everything is wide open.

Impact

1. Attackers can access other users' data by changing IDs in the URL
2. May lead to exposure of personal, financial, or sensitive records
3. Could allow modification or deletion of unauthorized resources
4. Enables enumeration of internal data structures
5. Potential legal and compliance issues if personal data is leaked

Remediation/Mitigation

1. Implement server-side checks to verify object ownership
2. Use access tokens or session-based references instead of raw IDs
3. Avoid using predictable object IDs (like sequential numbers)
4. Apply proper authorization controls on all endpoints
5. Perform security testing for IDOR scenarios during development

References

1. WSTG - v4.2 | OWASP Foundation
2. WSTG - Latest | OWASP Foundation

7. Conclusion

During the penetration test of the application, 4 High vulnerability and 1 Medium vulnerability have been identified. Also, there are a few suggestions provided as part of the testing.