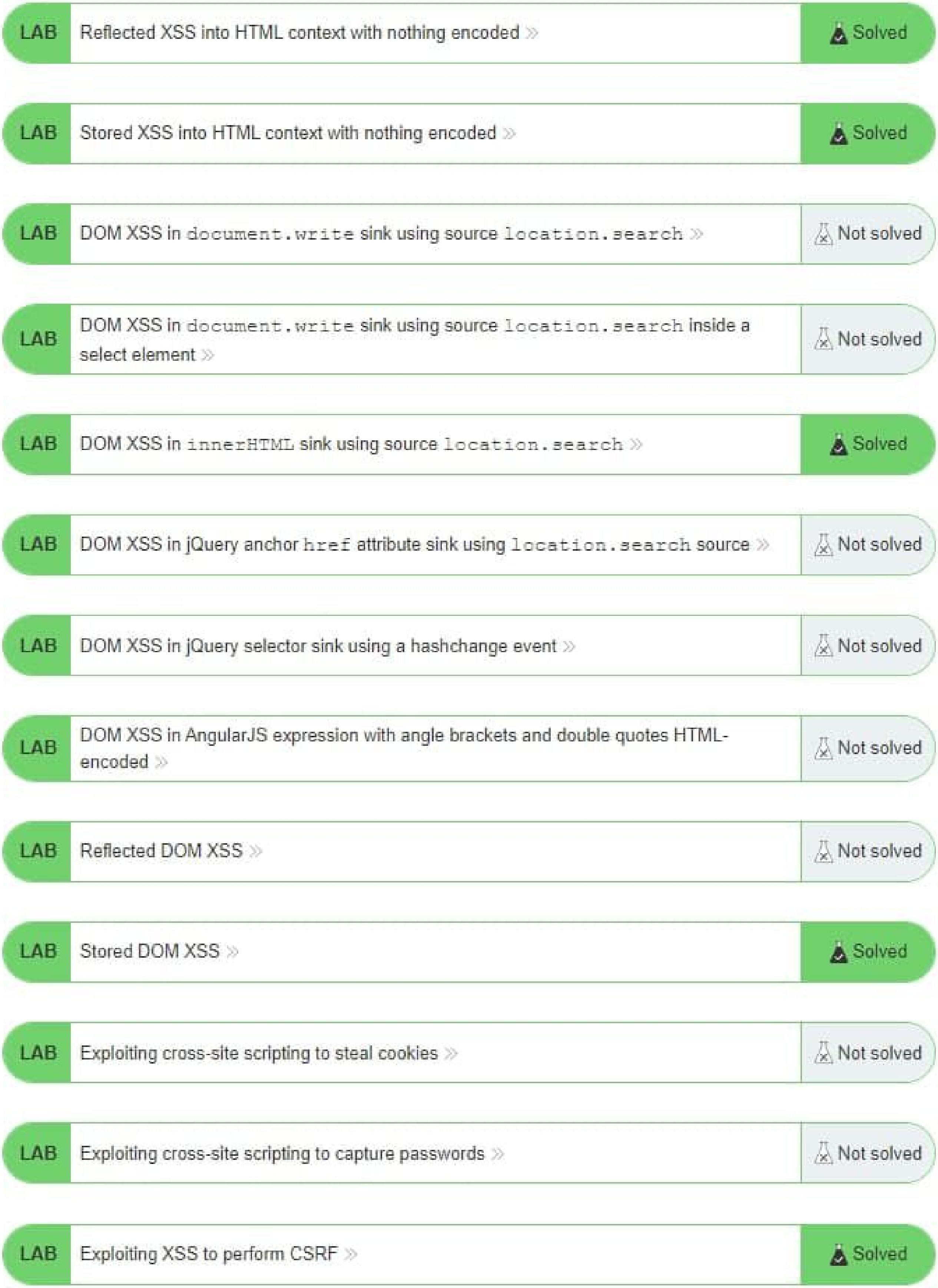
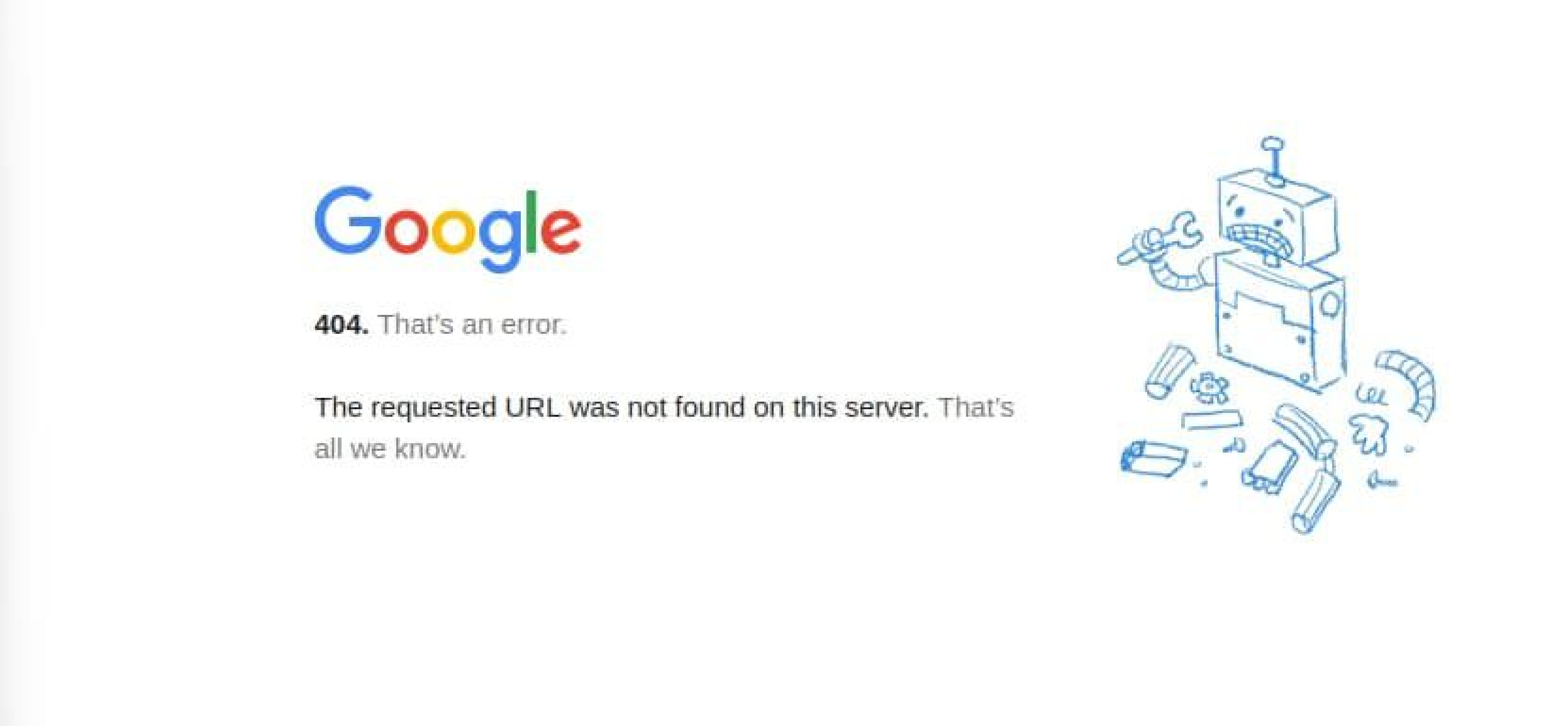
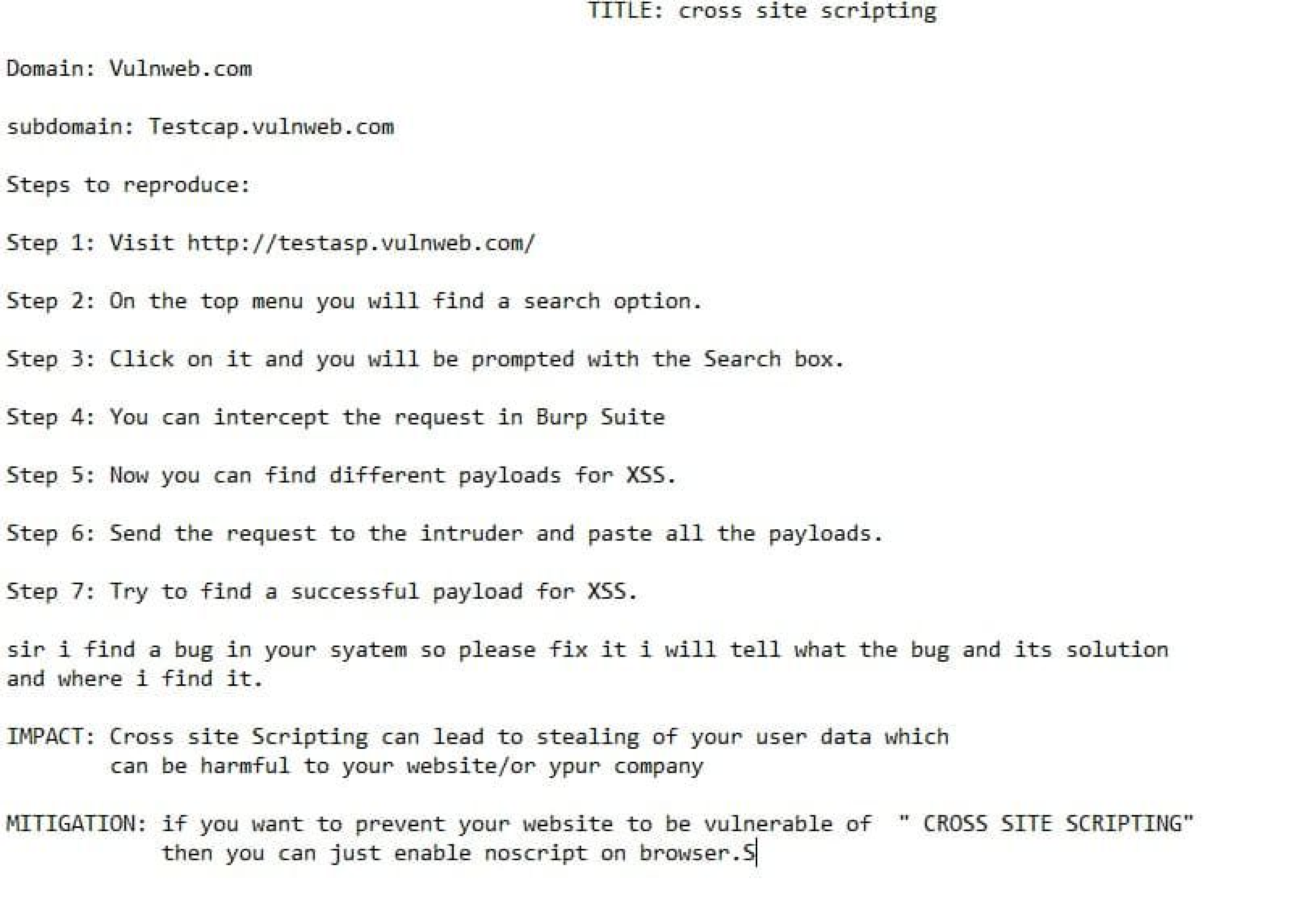


LAB	Reflected XSS into HTML context with nothing encoded »	Solved
LAB	Stored XSS into HTML context with nothing encoded »	Solved
LAB	DOM XSS in `document.write` sink using source `location.search` »	Not solved
LAB	DOM XSS in `document.write` sink using source `location.search` inside a select element »	Not solved
LAB	DOM XSS in `innerHTML` sink using source `location.search` »	Solved
LAB	DOM XSS in jQuery anchor `href` attribute sink using `location.search` source »	Not solved
LAB	DOM XSS in jQuery selector sink using a hashchange event »	Not solved
LAB	DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded »	Not solved
LAB	Reflected DOM XSS »	Not solved
LAB	Stored DOM XSS »	Solved
LAB	Exploiting cross-site scripting to steal cookies »	Not solved
LAB	Exploiting cross-site scripting to capture passwords »	Not solved
LAB	Exploiting XSS to perform CSRF »	Solved



404. That's an error.

The requested URL was not found on this server. That's all we know.



TITLE: cross site scripting

Domain: Vulnweb.com

subdomain: Testcap.vulnweb.com

Steps to reproduce:

Step 1: Visit http://testasp.vulnweb.com/

Step 2: On the top menu you will find a search option.

Step 3: Click on it and you will be prompted with the Search box.

Step 4: You can intercept the request in Burp Suite

Step 5: Now you can find different payloads for XSS.

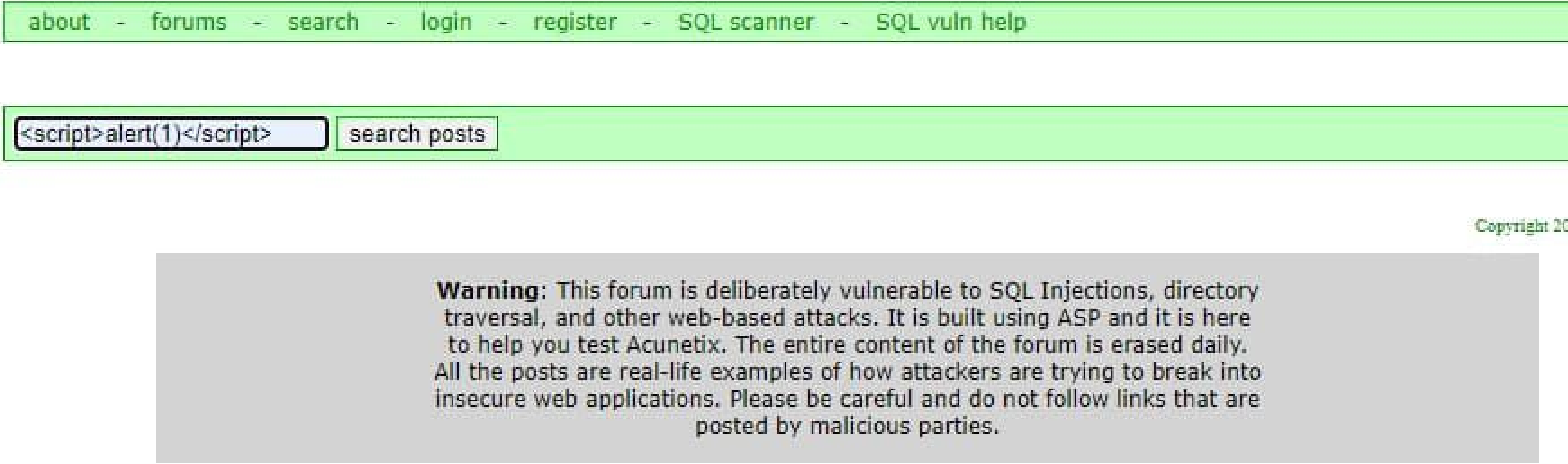
Step 6: Send the request to the intruder and paste all the payloads.

Step 7: Try to find a successful payload for XSS.

sir i find a bug in your syatem so please fix it i will tell what the bug and its solution
and where i find it.

IMPACT: Cross site Scripting can lead to stealing of your user data which
can be harmful to your website/or ypur company

MITIGATION: if you want to prevent your website to be vulnerable of " CROSS SITE SCRIPTING"
then you can just enable noscript on browser.S

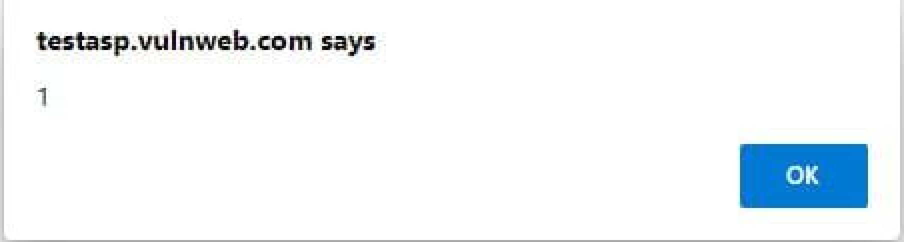


about - forums - search - login - register - SQL scanner - SQL vuln help
search posts

<script>alert(1)</script>

Copyright 20

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 says

1