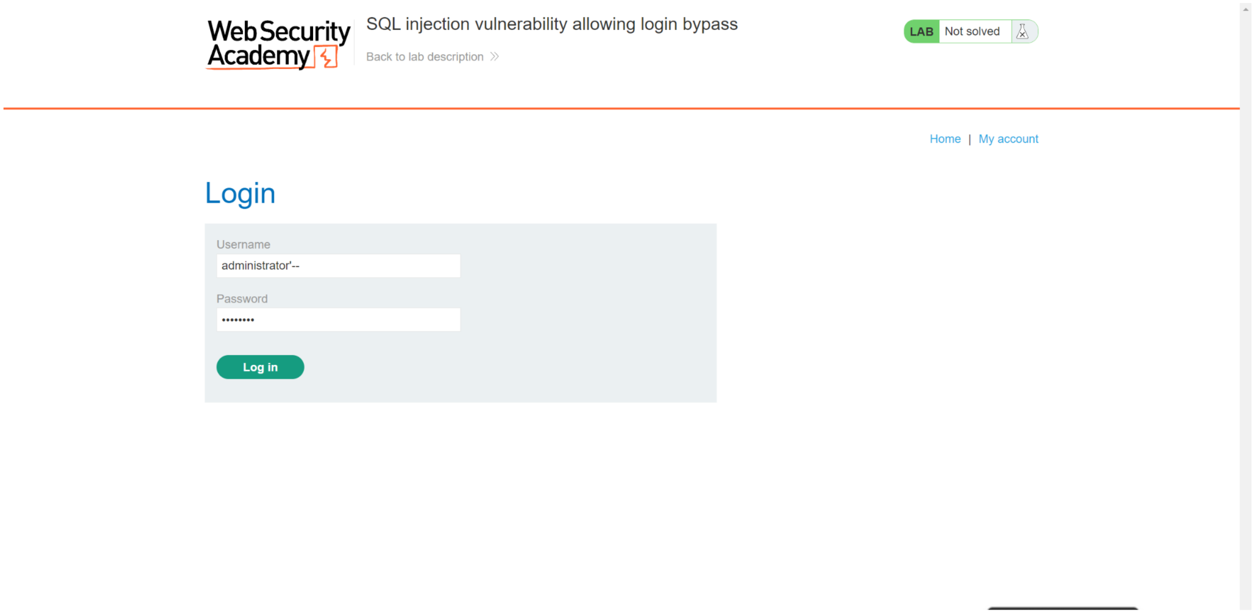
Assignment 1 Pramodh Krishna

OWASP top 10 vulnerabilities - any 5

1. SQL injection

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

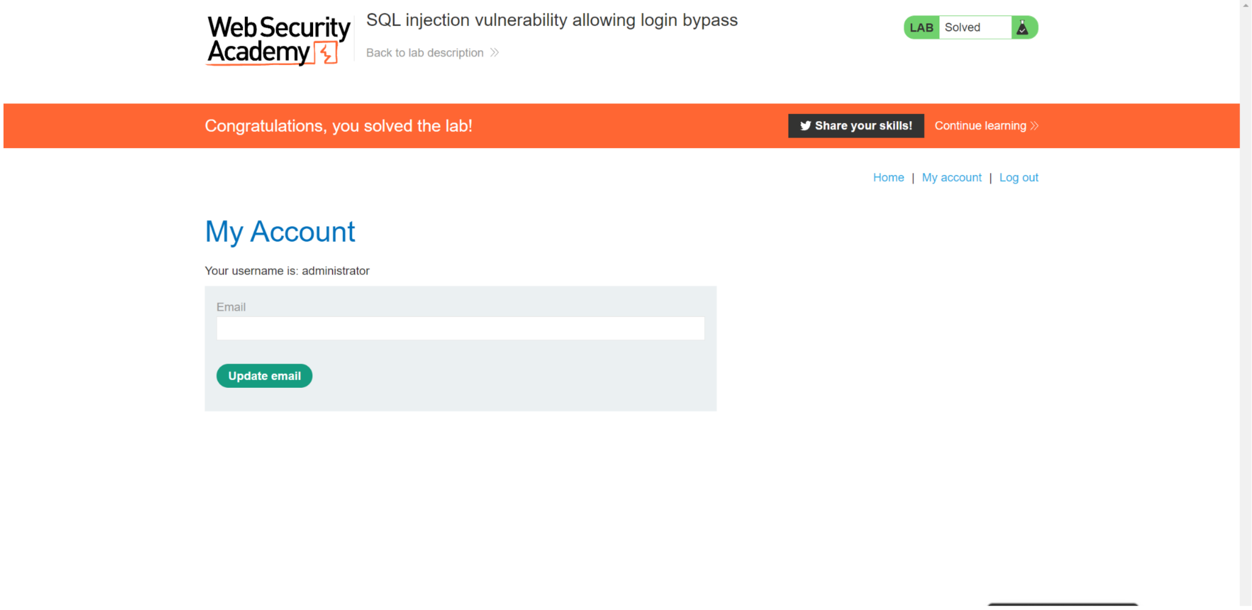


SQL injection vulnerability allowing login bypass

Login

Username: administrator'--

Password: ••••••••



Web Security Academy

SQL injection vulnerability allowing login bypass

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | My account | Log out

My Account

Your username is: administrator

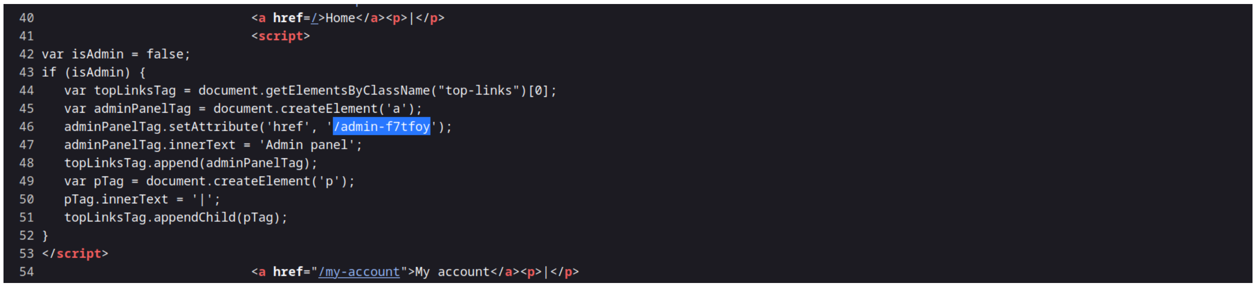
Email

Update email

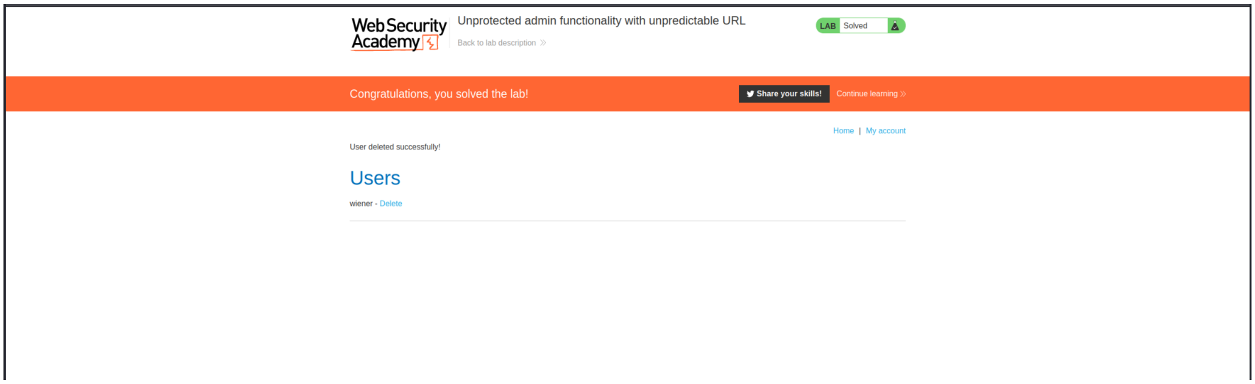
2. Broken Access Control

Broken access control vulnerabilities exist when a user can in fact access some resource or perform some action that they are not supposed to be able to access.

Page source contains admin url



```
                              <a href=/>Home</a><p>|</p>
                              <script>
var isAdmin = false;
if (isAdmin) {
   var topLinksTag = document.getElementsByClassName("top-links")[0];
   var adminPanelTag = document.createElement('a');
   adminPanelTag.setAttribute('href', '/admin-f7tfoy');
   adminPanelTag.innerText = 'Admin panel';
   topLinksTag.append(adminPanelTag);
   var pTag = document.createElement('p');
   pTag.innerText = '|';
   topLinksTag.appendChild(pTag);
}
</script>
                              <a href="/my-account">My account</a><p>|</p>
```



Unprotected admin functionality with unpredictable URL

Back to lab description »

Congratulations, you solved the lab!

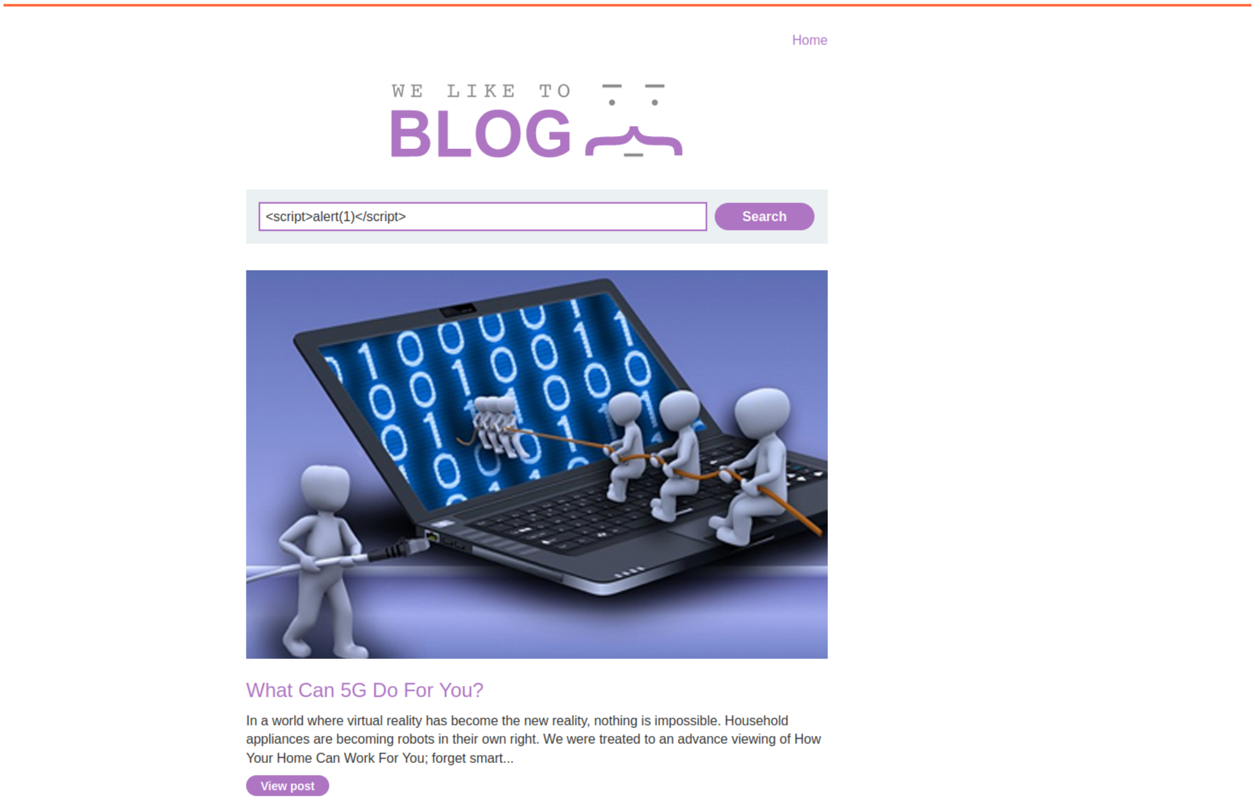
User deleted successfully!

Users

wiener - Delete

3. CSRF

Cross-Site Request Forgery (CSRF) is an attack that forces authenticated users to submit a request to a Web application against which they are currently authenticated. CSRF attacks exploit the trust a Web application has in an authenticated user. (Conversely, cross-site scripting (XSS) attacks exploit the trust a user has in a particular Web application). A CSRF attack exploits a vulnerability in a Web application if it cannot differentiate between a request generated by an individual user and a request generated by a user without their consent.

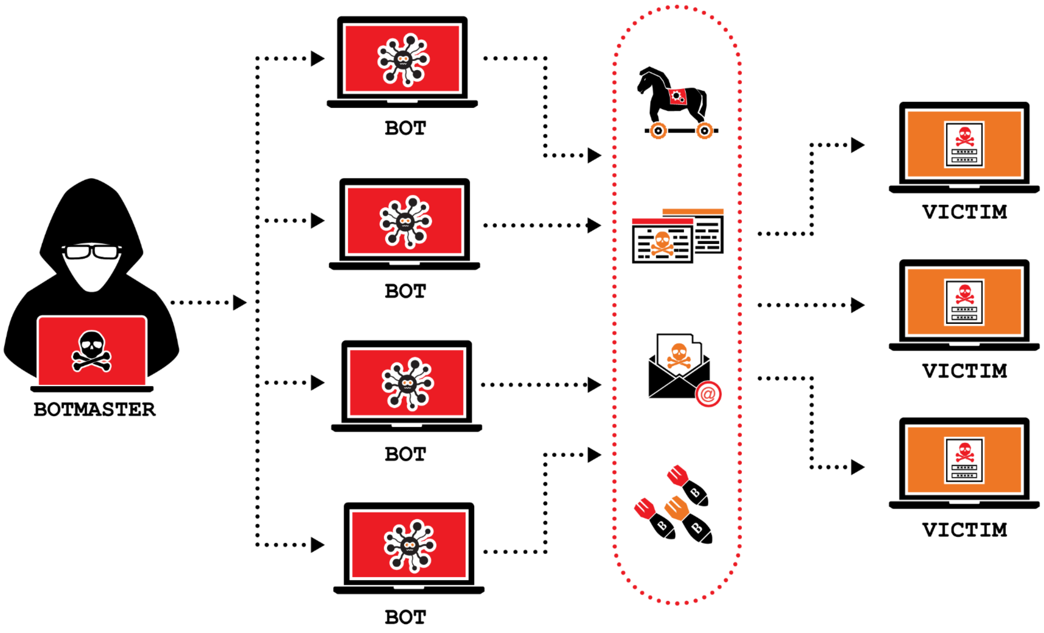


<script>alert(1)</script>

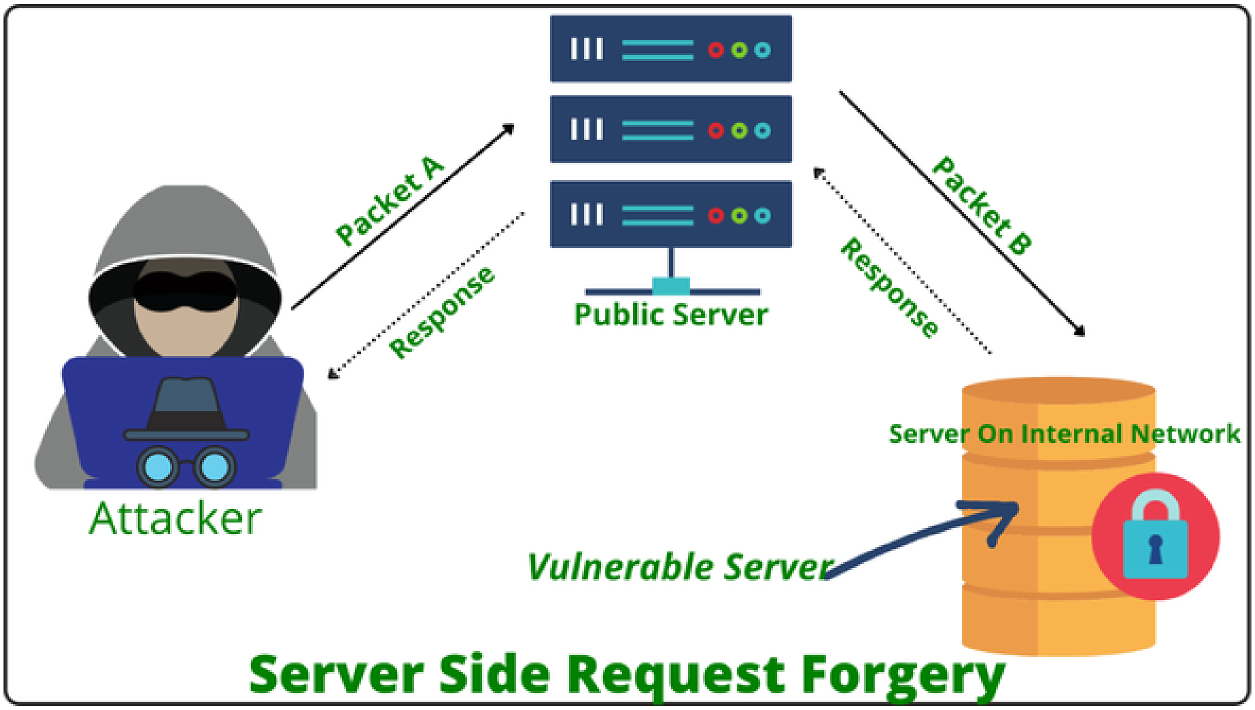
What Can 5G Do For You?

In a world where virtual reality has become the new reality, nothing is impossible. Household appliances are becoming robots in their own right. We were treated to an advance viewing of How Your Home Can Work For You; forget smart...

4. DDoS (Distributed Denial of Service):
Attackers overwhelm web servers with a flood of traffic from multiple sources, causing them to become inaccessible to legitimate users, disrupting services.



5. Server-Side Request Forgery (SSRF):
Attackers manipulate a web server into making requests to internal or external resources, potentially leading to data exposure, unauthorized access, or information leakage.


Packet A
Response
Public Server
Packet B
Response
Attacker
Server On Internal Network
Vulnerable Server
Server Side Request Forgery