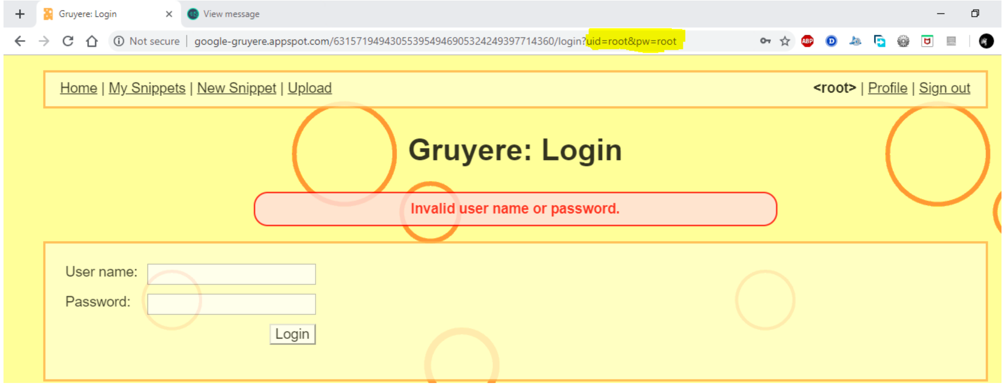
Penetration testing vulnerable web application

URL: http://google-gruyere.appspot.com/631571949430553954946905324249397714360

Vulnerability 1: Clear Text password over HTTP


Gruyere: Login
View message
Home | My Snippets | New Snippet | Upload
<root> | Profile | Sign out
User name:
Password:
Login

Not secure | google-gruyere.appspot.com/631571949430553954946905324249397714360/login?uid=root&pw=root

Gruyere: Login

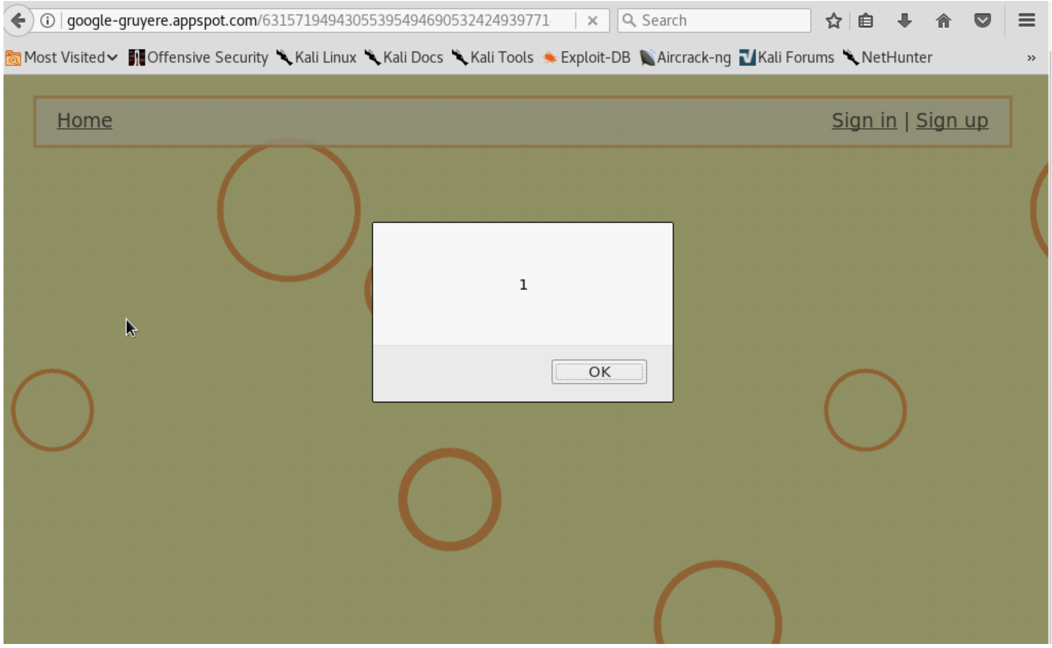
Invalid user name or password.

Description: username and passwords are sent over network without encryption. An attacker can sniff packets and easily view the passwords in plain text.

Risk Level: High

Remediation: Passwords must be encrypted or sent over secure channels such as HTTPS.

Vulnerability 2: Cross Site Scripting



google-gruyere.appspot.com/63157194943055395494690532424939771

1

Description: Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of invalidated or unencoded user input within the output it generates.

Risk Level: High

Remediation:

- Validating input fields
- Sanitizing input data
- Make sure the server does not display error messages that contain input received from the user.

URL: https://hackyourselffirst.troyhunt.com/

Vulnerability: Session Cookie without Secure Flag

Description: Cookies can be exposed to network eavesdroppers. Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

Risk Level: High

Remediation: When creating the cookie in the code, set the secure flag to true.

Vulnerability: Internet Explorer Cross-site Scripting Filter Disabled

Description: The cross-site scripting filter is a security feature in Internet Explorer 8 and later that is intended to mitigate some categories cross-site scripting attacks. It is enabled by default in supported versions of Internet Explorer but servers may disable the filter via the "X-XSS-Protection" response header. Disabling the filter presents a risk to users of browsers that support this feature as the filter will no longer protect them from certain cross-site scripting vulnerabilities in the website that has disabled the filter.

Risk Level: Low

Remediation: Do not disable the cross-site scripting filter. If possible, proactively enable the filter by setting the following response header: "X-XSS-Protection: 1; mode=block"

URL: http://demo.testfire.net/

Vulnerability: **URL Injection**

Description: URL injection is when a malicious individual attacks your website through the insertion of dangerous code that makes it appear as though your website gives credit to a detrimental site.

Risk Level: Medium

Remediation: The developer should examine the tag and determine the possible security implications of the use of a remotely supplied URI.

Vulnerability: SQL Injection

Description: SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

Risk Level: High

Remediation:

- The developer should review the request and response against the code to manually verify whether or not vulnerability is present.
- The best defense against SQL injection vulnerabilities is to use parameterized statements.
- Sanitizing input can prevent these vulnerabilities. Variables of string types should be filtered for escape characters, and numeric types should be checked to ensure that they are valid.
- Use of stored procedures can simplify complex queries and allow for tighter access control settings.
- Configuring database access controls can limit the impact of exploited vulnerabilities. This is a mitigating strategy that can be employed in environments where the code is not modifiable.
- Object-relational mapping eliminates the need for SQL.