Lab 09 Template – Ethan Roepke

1. **Screenshot of default Django landing page**

(10 points)

A screenshot of a computer

Description automatically generated

1. **Screenshot of testapp “Hello World” page**

(10 points)

A screenshot of a computer

Description automatically generated

1. **Screenshot of testapp debug information**
   1. Identify 5 potentially dangerous facts revealed by the debug page.
   2. How do you turn off the display of information?

(10 points)

* + 1. 5 dangerous facts that are revealed on the debug page are giving away python path, exception location, python executable, variable names, and how the application works.
    2. To turn off the display of information open the web.config file for the application and set the debug attribute to false for the compilation element

A screenshot of a computer

Description automatically generated

1. **Screenshot of XSS javascript alert**
   1. Explain why the javascript isn’t being displayed on the page

(10 points)

A screenshot of a computer

Description automatically generated

The JavaScript isn’t being displayed on the page because the line of code is giving an alert and inside the parenthesis will act like a message box so that’s why we get 1. If we were to change “1” to “Hello World” the alert message box would say “Hello World”.

1. **Screenshot of alert(document.cookie)**
   1. How did we get this value?
   2. Is it good or bad that we have that value?

(10 points)

A screenshot of a computer

Description automatically generated

A) We got this value by injecting HTML without any problems and alerted document.cookie to verify that XSS is present, hence the value we get.

B) This is bad that we have that value because this is how hackers use Reflected XSS and steal his cookies to gain access to ones account.

1. **Screenshot of username/password captured with BeEF**

(10 points)

A screenshot of a computer

Description automatically generated

1. **Screenshot of fixed XSS page**
   1. Screenshot and explanation of the problem and how you fixed it.

(10 points)

A screenshot of a computer

Description automatically generated

A black screen with colorful text

Description automatically generated  
In out html file, I have changed {% autoescape off %} to {% autoescape on %}. Changing from off to on causes HTML code in variables to be escaped. So it will print out the query exactly.

1. **Lookup the three types of XSS**
   1. Which did we use in this lab?

(10 points)

The three types of XSS are Stored XSS, Reflected XSS, and DOM-based XSS. Stored XSS is when an untrusted sources receives data and includes that data with HTTP responses in an unsafe way(permanently stored). Reflected XSS is when the web server is injected with a script that would give an error message, search result. DOM-based XSS is when the attacker modifies the users document object model environment in the browser.

We used reflected XSS in this lab because when we would open the website, everything seemed normal but, we were able to view the contents in BEEF for the attacker.

1. **Screenshot of NAT rule**

(10 points)

A screenshot of a computer

Description automatically generated

1. **Screenshot of Nagios with django services successfully running**

(10 points)

A screenshot of a chat

Description automatically generated