[[1]](#footnote-1)

The Benefits of a Vulnerable ASP.NET Web Application (December 2016)

Nicholas G. Gilbert, Student, Covenant College

*Abstract* — Web based cyber-attacks are a major threat to any person or business with an online presence. Applications such as the Damn Vulnerable Web App exist to demonstrate the most common web attacks including SQL Injection, XSS attacks, and brute force attacks. While the DVWA is the go-to application for demonstrating attacks on PHP applications, there is no comparable application for ASP.NET. The goal of this project is to create a DVWA-like application built on ASP.NET.

*Index Terms* — ASP.NET, MVC, Data Security, Information Security, Relational Databases, Web Design, SQL Server

# INTRODUCTION

A

uthor and web developer Peter Welch maintains a blog about his experiences building web applications. Not one to be politically correct, he refers to the internet as “its own special hellscape” from a developer’s perspective [1]. There are many more problems and challenges a programmer faces writing web applications as opposed to traditional programs which are downloaded and installed for offline use. Such challenges include optimizing code so web pages load quickly, maintaining compatibility for multiple, potentially outdated but still used browsers, and scaling applications to handle millions of users. However, the challenge this project will focus on is writing secure web applications.

Most web developers do not start from scratch. Modern websites are built on preexisting frameworks provided by others. With choices ranging from development frameworks like ASP.NET and Ruby on Rails to Content Management Systems like Wix and SquareSpace, web developers rarely have to build from scratch in 2016.

Different Frameworks still have to handle common threats to the security of applications built on them. Regardless of the chosen framework, threats like SQL injection and XSS attacks must still be considered. Frameworks can also have vulnerabilities specific to them like the ASP.NET POET vulnerability which jeopardizes the confidentiality of information stored in an ASP.NET application [2].

To demonstrate cybersecurity threats that web developers face, Dewhurst Security has developed the Damn Vulnerable Web App (DVWA). The DVWA is an intentionally vulnerable PHP/MySQL web app that allows penetration testers to hone their skills and developers see the kind of attacks that their applications can face. Such attacks include SQL injection, XSS attacks, command injection, file upload vulnerabilities, brute forcing, and more.



**Figure 1: The Damn Vulnerable Web App. This application, developed by Dewhurst Security, is used to demonstrate vulnerabilities in web applications that developers need to be aware of when building their applications. It also allows penetration testers to hone their skills without illegally hacking applications.**

# Project Objective

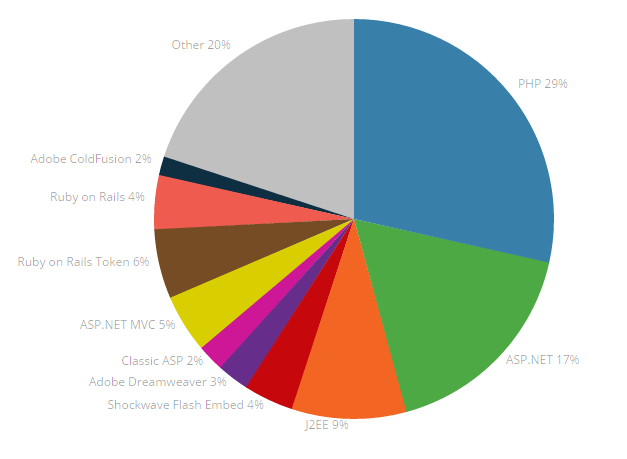
The DVWA is a great tool for demonstrating specific attacks that can occur against any web application. However, it does not take into account the role that frameworks play in the security of web applications. Only one version of the application exists which is written in PHP using a MySQL database. While that is a common combination of tools to use, it is far from the only combination.

The goal of this project is to provide a proof-of-concept for an application like the DVWA built using a non-PHP framework. This will not be a complete application as developing a complete application will take more time than can be given in a single semester. However, a proof-of-concept will be given in the form of an application that demonstrates a few of the most common attacks and how to secure against them. Data and test cases will also be provided to demonstrate the improved security of an application when it is coded to the standards given by the framework provider. The project is called Vulnerable .NET App (VDNA).

# Approach

## Choosing a Framework and Database

Ideally, a version of the DVWA would exist for every framework and database combination used today. However, writing one for every such combination would go well beyond the time allotted for this project. Hopefully as an inspiration to start building versions in other frameworks, the VDNA is built on Microsoft’s ASP.NET framework (www.asp.net). ASP.NET has become the second most popular language of the web after PHP [3].



**Chart 1: The most popular web frameworks in 2016. The top four frameworks are based on four different languages. PHP, the most popular framework language, holds 29% of the market. ASP.NET, based on ASP/C#, holds 17%. Java’s enterprise edition is 3rd at 9% and Ruby on Rails is 4th at 10% [3].**

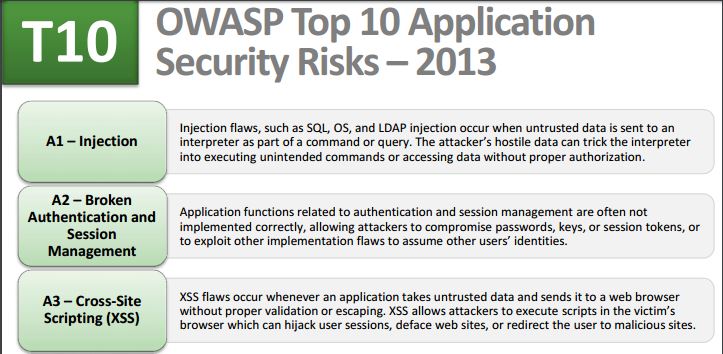
ASP.NET is compatible with most relational databases, but many developers choose to work with Microsoft’s SQL Server. Therefore, the database VDNA uses is SQL Server 2014.

## Which Attacks to Demonstrate

Web developers face numerous threats from malicious users; all of which could have been included in this project. For the sake of narrowing the scope of the project, the three most common threats were chosen to be demonstrated.

The Open Web Application Security Project (OWASP) monitors cyber-attacks and collects related statistics. With those statistics, OWASP compiles a list of the most common types of attacks which occur. Currently, the most common attacks are injection, cross-site scripting, and authentication [4].

OWASP’s number one ranked threat is injection. Injection involves tricking an application into running malicious code or commands provided by a malicious user. A common form of it, and the form demonstrated in this project, is SQL Injection. A poorly coded web application will take any input given by the user and stick it in the middle of a hard-coded SQL statement which is then issued to the database.



**Figure 2: These are the top three entries from OWASP’s list of the top ten greatest threats to web applications. Factors which go into ranking the attacks include frequency and extent of the damage that can be done by such an attack. The top three attacks, and therefore the three demonstrated in this application, are Injection, Broken Authentication, and Cross-Site Scripting attacks.**

The second greatest threat as ranked by OWASP is broken authentication. Many web applications, especially ones which store financial information, implement user accounts to grant everyone access to their information (and only their information). Unfortunately, that information is too often left accessible to users who know how to trick an application into revealing information they shouldn’t be able to. SQL Injection can actually be a form of broken authentication as well if users can trick a database into revealing passwords with it.

Another form of broken authentication, and the form demonstrated by VDNA, is brute-forcing into an account. Typically, brute-forcing is a last resort for a hacker. However, if a login screen has no preventative measures and a user chooses a weak password, a user can brute force their way into an account.

Finally, the third biggest threat to web applications as ranked by OWASP is cross-site scripting attacks (XSS). XSS attacks are similar to SQL Injection in that they trick an application into executing code not written or intended by the developer. However, unlike SQL or command injection where code is processed on the backend of an application, XSS attacks occur on the frontend of the application and can be used to alter the appearance and content of a web app.

Typically, a user will write a script and feed it into an input somewhere that the application accepts user input. If the application renders HTML based on that input, and the input is not filtered, a user can inject <script> tags to run JavaScript in the application.

There are two types of XSS attacks. The first is stored XSS where the results of an attack are not immediately viewable to the user but the application is altered in some way internally. The other type, and the type demonstrated by VDNA, is reflected XSS attacks where the user can see the results of a script injection. The type of XSS an application is vulnerable to depends on the context in which user input is processed.

Injection, broken authentication, and XSS attacks are the three biggest threats to the security of web applications. Therefore, they are the three attacks demonstrated in this project.

# Features

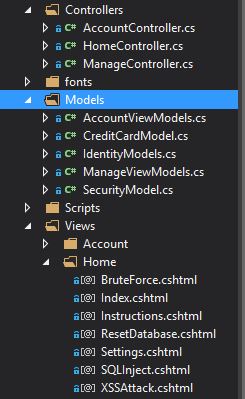
## MVC Model

Given all the challenges web developers face, the code base for a web project can become complex quickly. The speed at which a project is developed can be sharply reduced by poor project organization. In the face of that problem, the philosophy of Model-View-Controller (MVC) has risen [5]. ASP.NET provides a template geared toward that philosophy which was used to build this project.

The model of the application represents the data stored within it. In the case of VDNA, the model is made up of C# classes representing the tables of the database. Each instance of those classes is a record stored in the corresponding table. Working with models that way bypasses the need for user-declared SQL connections which helps secure ASP.NET applications from SQL Injection

The views shown by VDNA are the web pages rendered to the user. Views display information from the model as well as provide the interface through which the user can provide input to the controller.

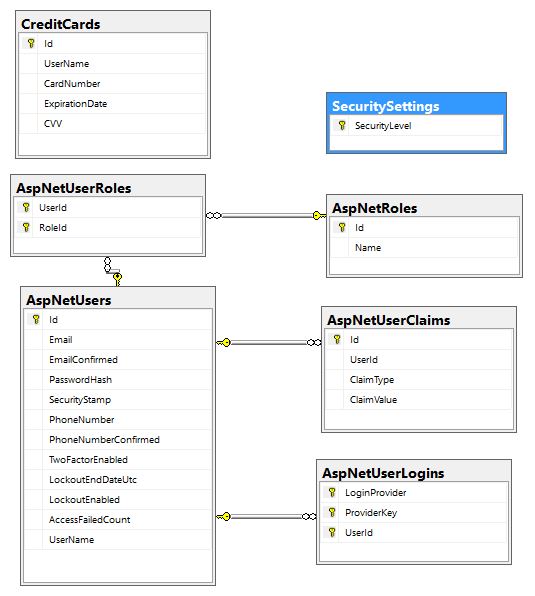
The controllers for VDNA take user input and operate on the model based on that input. The logic for the attack pages, as well as generating and manipulating the database, is contained in the controllers.



**Figure 3: The file structure for the VDNA with the MVC files shown. The model is made up of C# classes correlating to the SQL Server database. The views display the models to the user and provide the interface through which users feed input to the controllers.**

## Database Structure

The database is based off of Microsoft’s ASP.NET Identity library. ASP.NET Identity provides the required infrastructure for user accounts in ASP.NET applications. Each user account is uniquely identified by its ID which acts as the primary key in most of the other tables.



**Figure 4: The database diagram for the SQL Server 2014 database used by the VDNA. The database is normalized to BCNF and provides the tables necessary for the application to have user accounts. It also provides the different security level options for the application. Finally, it lets users store credit card data which acts as sample data for the attacks.**

The database is normalized to BCNF. Each user account has a username (which is the email address) and password with which they can log in. The SecuritySettings table stores two strings, “low” and “high”, to tell the attack pages how difficult to make each attack. An admin user is created by default and every other registered user has user-level permissions.

## Attack Pages

The views provided by the VDNA consist of instruction pages, a home page that provides a starting point, and the attack pages. Each attack page provides an explanation of what attack the page demonstrates and a realistic scenario through which to demonstrate it.

As specified by the philosophy of MVC, the views show the appropriate parts of the model to the user depending on the page they are on. The views also provide an interface through which the user can conduct the attacks the VDNA demonstrates.

## Security Level

Finally, the VDNA provides two different security levels to test. The low setting tells the application to execute insecure code to process the input given to each view. The low setting is akin to an ASP.NET application poorly developed from a security perspective. Test cases are provided that successfully exploit each attack when the security is set to low.

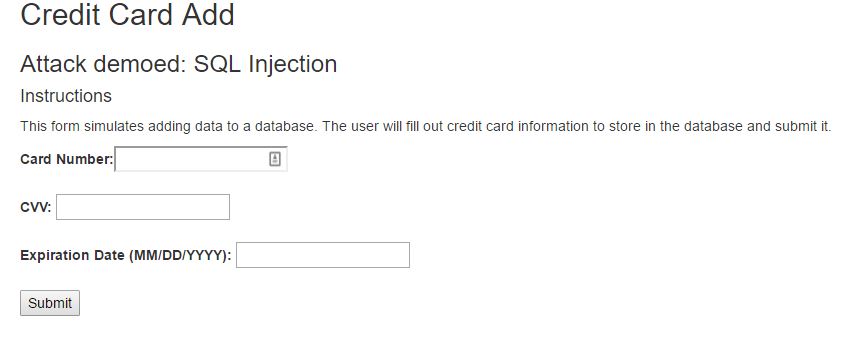
On the other hand, the high security setting tells the application to use code written to Microsoft’s standards of security [6]. Theoretically, only zero-day attacks should succeed against the attack pages when the security level is set to high.

# Collecting Data

## SQL Injection

The greatest threat to web applications as ranked by OWASP, Injection, is demonstrated by VDNA in the form of SQL Injection. The SQL Injection view displays a form through which the signed-in user can add a credit card to associate with their account.

If the security is set to low, a SQLConnection object is used in the controller to process the user’s input. The input is not checked beforehand leaving the application vulnerable to SQL Injection. If the security is set to high, a DBContext object is used to update the database through the credit card model class.



**Figure 5: The view for the SQL Injection demo. This page simulates a form which allows a user to associate a credit card with their account.**

The test cases in table one are used to demonstrate the benefit of using the DBContext over a SQLConnection.

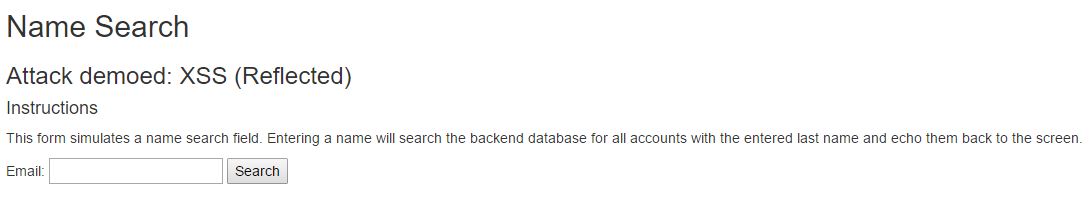
|  |  |  |
| --- | --- | --- |
| **Input** | **Result (Low)** | **Result (High)** |
| 1111222233334444 | No Attack | No Attack |
| 1111222233334444' -- | Invalid SQL Error | Dangerous Input Error |
| 1111222233334444', '111', '20160801'); -- | Record inserted  Attack successful | Dangerous Input Error |
| 1111222233334444', '111', '20160801'); DROP TABLE CreditCards; -- | Record inserted, table dropped  Attack successful | Dangerous Input Error |

**Table 1: The test cases given to the SQL Injection view and**

**the result for each case.**

## Cross-site Scripting (XSS)

OWASP’s second-greatest threat, XSS attacks, are demonstrated by VDNA in the form of reflected XSS attacks. The XSS attack view displays a form through which the signed-in user can search for other registered users. If the security level is set to low, the form is vulnerable to XSS attacks. If it is set to high, the controller behind the view filters input for HTML tags.



**Figure 6: The view for the Reflected XSS demo. This page simulates a form which allows a user to search for other registered users in the application.**

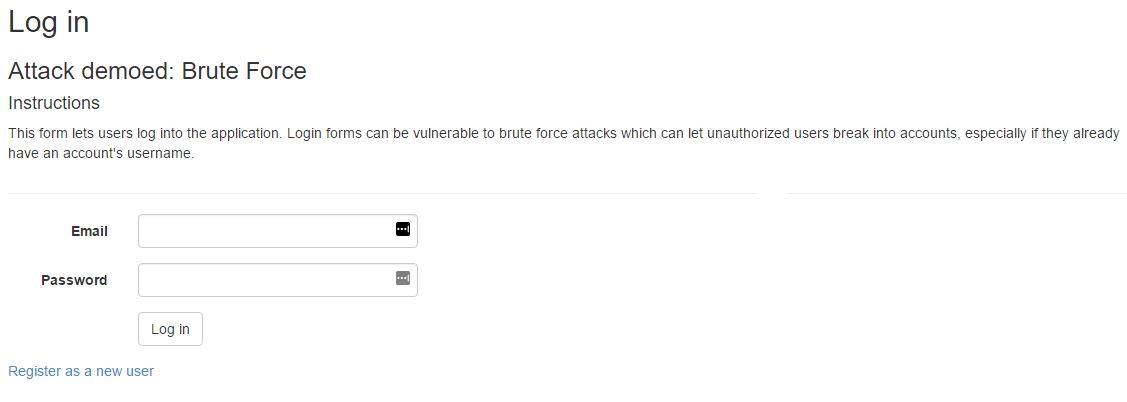
The test cases in table two are used to demonstrate the benefit of filtering user input for dangerous input before it is processed.

|  |  |  |
| --- | --- | --- |
| **Input** | **Result (Low)** | **Result (High)** |
| nick | No Attack | No Attack |
| <script>alert(“XSS”) </script> | Alert box shown  Attack successful | < > stripped  Attack failed |
| nick <script> alert(“XSS”) </script> | Search for nick  Alert box shown  Attack successful | < > stripped  Attack failed |

**Table 2: The test cases given to the XSS Attack view and the result for each case.**

## Brute Force Authentication

Finally, the third threat listed by OWASP is poor implementation of authentication. To demonstrate this point, the VDNA has a login form that is vulnerable to brute-forcing login attempts. When the security level is set to low, the admin password is “mockingjay”; a weak password. When the security level is high, the admin password is “q1S2@fXZETG9433!2”; a strong password rendering brute-forcing impossible.



**Figure 7: The view for the broken authentication view. The page simulates a login form which is vulnerable to brute-force attacks.**

It is typically a last resort, but when hackers decide to take the brute-force approach, a strong password is the best defense against the attack. Malicious users have multiple tools at their disposal to brute-force login forms. The tool used to demonstrate the brute-force attack is THC-Hydra. The included bash script can be run on any Linux machine with THC-Hydra installed.

|  |  |
| --- | --- |
| **Security Level** | **Time to Brute-Force** |
| Low |  |
| High | Attack failed |

# Faith Integration

# Conclusion

References

1. P. Welch, "Programming Sucks," in Still Drinking, 2014. [Online]. Available: https://www.stilldrinking.org/programming-sucks. Accessed: Nov. 28, 2016.
2. Microsoft, "Microsoft security bulletin MS10-070 - important," 2010. [Online]. Available: https://technet.microsoft.com/library/security/ms10-070. Accessed: Nov. 28, 2016.
3. "Framework technologies Web Usage Statistics", *Trends.builtwith.com*, 2016. [Online]. Available: http://trends.builtwith.com/framework. [Accessed: 06- Apr- 2016].
4. J. Williams and D. Wichers. OWASP top 10 2013: The Ten Most Critical Web Application Security Risks. *OWASP Foundation*, April 2013
5. Microsoft, "Model-view-controller". [Online]. Available: https://msdn.microsoft.com/en-us/library/ff649643.aspx. Accessed: Nov. 30, 2016.
6. Microsoft, "Basic security practices for web applications". [Online]. Available: https://msdn.microsoft.com/en-us/library/zdh19h94.aspx. Accessed: Dec. 1, 2016.

1. This paper was submitted for review on December 5, 2016 to Dr. Jeffrey Humphries, Associate Professor of Computer Science at Covenant College in Lookout Mountain, GA. This paper serves as the Bachelor’s Thesis of Nicholas G. Gilbert, fulfilling the requirement of COS492: SIP in Computer Science

   Nicholas G. Gilbert is an undergraduate student studying Computer Science at Covenant College, 14049 Scenic Highway Box 222, Lookout Mountain, GA 30750 USA (email: nickgilbert1994@gmail.com). [↑](#footnote-ref-1)