University of Victoria, Software Engineering

Case Study 8: Application Security

Jordan Ell
V00660306

March 14, 2013

1 Application Security of Biergarten

This case study focuses on application security for the town of Biergarten. This town is currently involved in overseeing a large change to their technical infrastructure. This new infrastructure is replacing an existing legacy system and can be broken down into two large main components with some over lap between the two. The first component of the new system is designed to improve how the rest of the world views Biergarten. This involved tourism, and the large beer industry that resides in the town and promoting these services to the world. The second component is a web portal for residents of the town. This portal will allow municipal services to be transacted such as payment of property taxes, civil worker information, and more.

The rest of this case study will be laid out as follows. First, an attempt to classify the components common to both systems as well as mutually exclusive components will be made using the S.T.R.I.D.E methodology. Justification will be given for each classification as well. Next, the effects of cross site scripting will be investigated with the vulnerabilities detected in the previous section. This investigation will use the D.R.E.A.D framework as its basis for concern.

2 S.T.R.I.D.E

In this section, I will outline the potential security risks using the S.T.R.I.D.E methodology in regards to the common components of the two web portals as well as the com-

ponents specific to each web portal. I will give justification for each classification made.

2.1 Common Components

Here a list is presented of all S.T.R.I.D.E issues in the common components to each system.

- Site-specific templates will be user for overall look and feel. Using templates site wide opens the website to potential spoofing identity attacks such as phising. Once the attacker is able to duplicate the website template, emails with links to look a like sites can be sent out in an attempt to spoof the identity of the original site and lure in victims with passwords or other information.

- User creation and administration will be performed centrally. This can be identified as a tampering risk. Since all users and riskier yet, administrators, are stored in a central database, once access has been enabled on a potential attacker, all user information is now at risk. Worse yet, the attacker can create an administrator account for themselves and hide amongst the other user accounts. This would also be classified as an elevation of privileges.

- Users will be assigned roles and will have access to different information across the site based on said roles. This can be identified as spoofing and elevation of privilege. An attacker may be able to change his or her role inside of the database and thus gain access to higher level information inside the system or may be able to change said information. The spoofing comes from the fraudulent role and access an attacker would be able to achieve.

- A user friendly web interface for uploading general content. This can be identified as a tampering and spoofing risk as well as open the door to cross site scripting (XSS). Here, since the content being uploaded is general, any content including malicious software could be uploaded to the server. This type of content can be used to gain access to private or hidden information and can also communicate with the outside world in order to send the information to other malicious websites or servers. This all of course runs the risk of data tampering and spoofing of identities to gain further access to data.

- Cookies will be stored to allow users to remain logged in for extended periods of time. This can again be identified as tamper and spoofing. The spoofing here comes from session hijacking. If a user leaves themselves logged in on a public machine, as person coming along can use their account for an elevated privileges they may have. This can also be use to elevate another user's privileges. The tampering comes again from session hijacking and being able to change the currently logged in user's information.

- Finally, because of the nature of all these common components being centrally located, denial of service (DoS) attacks can be employed against the entire system.

These attacks can leave the entire website down as the traffic load is not distributed accross multiple machines.

2.2 Tourist Information Portal

Here a list is presented of all S.T.R.I.D.E issues in the tourist information portal.

- The portal is expected to be based on a content management system with a friendly web based interface. This raises the same concerns as the general content uploading with tampering and spoofing. However, this time, the security issues with the content managements system (CMS) are now placed on a third party, the developers of the CMS. This takes responsibility away from Biergarten but places concern of outside security implementations. And of course, this still can be labeled as potential tampering and spoofing with the content being uploaded. The content can once again be used for malicious purposes in both data access, identify spoofing and elevation of privileges.

- The sites will contain dedicated administrators but will also have the hopes of local businesses managing their own content. This can be identified as an information disclosure issue. The problem here is that the site will contain a large amount of administrators or users will high privileges. This being the case it may be easy for information to fall into the wrong hands of an administrator who should not have the information. This of course is also associated with elevation of privileges in that administrators will have access to a wide assortment of information.

- Users will be able to access and edit their own personal information while some administrators information will be accessible for editing by the business users. Here elevation of privilege is the main cause for concern while XSS is also to be dealt with. The fact that users have access to so many types of information, even in some cases administrator information for businesses is a large concern. The user may act as a user with elevated privileges without even having to make an attack. This also concerns the tampering of data the user has access to. XSS is also an issue as there appears to be a large number of input forms for the user and each form is potential of XSS.

2.3 Municipal Service Site

Here a list is presented of all S.T.R.I.D.E issues in the municipal service site.

- Each department will have a separate subsection while functionality will be added with the core framework. This can be classified as a denial of service threat. The problem here is that many subsections are all hosted and operated through a core framework. If that core framework was to be attacked using a denial of service attack, all subsections would be lost and unreachable. The DoS will cause many systems to go down while only attacking a single server.

- Departments will have privileged users to edit content while civil employees will have read only access. This can be classified as elevation of privilege and tamping. The problem here again is that there are too many administrators on a single web server. These administrators have the capability to tamper with information stored on the central database as well as elevate the privileges of other users inside the system. A reduced number of administrators would help combat this issue.

- Users will be able to perform civil actions such as pay property taxes using the web portal. This can be classified as an information disclosure and denial of service threat. Here, the users are supplied very private and critical information to the system. If any attacker got a hold of this information, the attacked user may run into legal and financial issues from the disclosed information. And again, since the servers are centralized, the denial of service attack would bring down many critical components to the users such as paying taxes on time which may leave the town crippled.

- The website must be able to provide own information to users while hide it from others. This type of roles system can be vulnerable to elevation of privilege and data tampering attacks. Since the users are assigned roles which give them access to certain items of information, any user obtaining elevated privileges may be able to change data at will of another user or the system itself.

3 XSS AND D.R.E.A.D

3.1 XSS

The main concern with this website in terms of cross site scripting is the number of input forms a regular user has access to across the website. Each of these forms has the potential to be involved in a cross site scripting attack on the website and on the user. Input must be validated for each form to be able to stop this kind of attack. In terms of XSS being triggered as part of emails targeted at user and administrators of the web portal, the availability of information is a large concern. As stated in the requirements for the website, a regular user has access to all kinds of information of other users such as email. This will allow attackers to only target users of the website site from the get go. A second concern is the template of the website. Since the whole website shares a common template, a phising website will be created with relative ease by potential attackers. Here an email can be sent to users asking them to authenticate to the phising website and now the attackers have user names and passwords for the website. From here, the attacker can take advantage of the many elevation of privilege issues raised in the previous section in order to create data tampering or other malicious intents.

3.2 D.R.E.A.D

Damage Potential - The damage potential to these two web services is high (3). Elevation of privilege is such a high threat that the potential damage that could be made is esca-

lated solely because of this. The number of administrators and potential administrators on the website is so high that even if an elevation of privilege attack was made it would be almost impossible to trace it. Administrators also have too much access to information site wide. Administrators of a local business has access to almost any information they wish.

Reproducibility - The attacks that this website is vulnerable to can be reproduced at any given time and so this is rated as high (3). The privileges and denial of service attacks, the two most harmful attacks this web portal can face are not dependent on some timing or open window, they can be repeated at whim by any given attackers.

Exploitability - Since the two main attacks of elevation and DoS can be made by a novice and a skilled programmer, this will be rated as a (2.5). Here the elevation attacks could range from simply someone giving access where they shouldn't have through social engineering to attempting to break into the user database and change roles. The DoS attacks are more sophisticated in nature and require a somewhat skilled programmer to execute them.

Affected Users - This must be rated as high (3). Once an unauthorized attacker has gain elevated privileges, all user information across the site could be compromised as administrators have access to way too much information on the whole site. Secondly, in a denial of service attack, all users are affected. Since the web portals and subsections of all the businesses managed on the website are run through central servers and frameworks, a single DoS attack could bring down every user action. This would have extreme consequences in the case of paying property taxes.

Discoverability - This is rated as between medium and high (2.5). The phising attacks that could be used against the website are easily understood by attacks with all the information needed being public. These attacks can result in cross site scripting and eventually lead to data tampering issues within the web portal. The denial of service attacks are seldom used against such small websites and web businesses. They are mainly directed at large companies or federal government organizations.