Outpost24

STUDENT PROJECT PROPOSALS

Date	12th October 2018
Prepared By:	OUTPOST24 HR hr@outpost24.com

About Outpost24

Outpost24 is a leading cyber assessment company focused on enabling its customers to achieve maximum value from their evolving technology investments. By leveraging our full stack security insights to reduce attack surface for any architecture, Outpost24 customers continuously improve their security posture with the least effort.

Over 2,000 customers in more than 40 countries around the world trust Outpost24 to assess their devices, networks, applications, cloud and container environments and report compliance status for government, industry sector, or internal regulations.

We don't think it's fair that businesses are targets of cybercriminals. As a leading cyber assessment company, we're on a mission to help our customers tighten their cyber exposure before their business can be disrupted. Our ethical hackers and the tools they've created provide a complete view of your security posture with solution-based insights that facilitate and prioritize remediation efforts.

Working with us

If you are aiming to do your master thesis within the field of IT Security, it may be possible to do in collaboration with Outpost24. We have defined a number of projects in which there will be great opportunity to put theory into practice for mutual benefit for the student and Outpost24.

For the defined project duration, you will be given a supervisor for the project and support in critical thinking and evaluating your methodology. In several of the projects, you will in parts also work jointly with experienced specialists within the domain.
Some of the work will lead to publications of articles or studies. Others relate to confidential internal information and development and research. Any work performed together with Outpost24 will be the intellectual property of Outpost24, and there will be limitations as to what parts can be included in the published components of a thesis, while all abstracts and conclusions will be possible to publish in full.

We are looking for students who have a personal drive and desire to succeed. If you are uncertain that you will perform to your best, or if you are uncertain of your intentions to complete a project – you will not find a match with us. We are prepared to invest time, resources and efforts in your success - and expect of you to do the same.

In this document, you will find detailed descriptions of a range of project proposals. In cases where multiple students are interested in the same project, Outpost24 will make a choice between the candidates. An application of interest will be evaluated, and Outpost24 will screen candidates before acceptance. An interview is expected to ensure that both parties are comfortable with a cooperation and agree on project focus.

How to apply

We withhold the right to only taking in the number of candidates that we find qualified within this application round and that we can manage in a manner where we provide the support and quality assurance, which is needed for a successful delivery. As qualified applicants apply, we will invite these students in for an interview – therefore, please do not delay in applying, as we will close the openings for the projects once the right match has been found.

Please apply through our website https://www.outpost24.com/careers where you will find the master thesis openings.

PROJECT PROPOSALS

Static parsing of JavaScript to identify interactions and high risks in an application

Large applications often also load large application sets.
Hidden in those scripts are also often large sets of “unintentional exposures”, just as well as there are potential attacks against the script engine itself for what is known as DOM-based XSS exploitation.
Today there is good basic understanding of what DOM exploitation is based on, and there are techniques for identifying simple exploitations. However, the support for actual modelling of user-controlled input and its path through applications and ability to affect the DOM is lesser understood and poorly supported in practice.
To be able to translate JavaScript frameworks into risks, parsing the JavaScript and determine its intended interactions with an application will show more “actions” or interaction point with an application than those present in the interface, as often a lot of the interaction in applications occur on an API-level. The JavaScript frameworks define the API and often contain interaction points which are either hard to trigger in the interfaces via automation, or not even present directly in the content of the applications.

The DOM-based component of the project is observing points where Cross Site Scripting attacks can occur not in the server response as such, but locally via the browsers script engine interpreting JavaScript and the DOM. The most common is that the document location variable is parsed in a careless manner resulting in execution of script from an unexpected content.

This project is an advanced topic, and a focus of either of the areas or both is acceptable depending on the size of team (one or more) and experience of the student

Risk prioritization, bringing CVSS to the age of the web (20 years to late)

Web applications, although software, are not fit for traditional network security metrics in all cases. There are several proposed models to score risks, from the traditional CVSS v2 followed by the later more flexible CVSS v3, but also a range of others including OSSTMM risk ratings for systems and others.

Research is needed to identify an existing model, or propose applying a version of an existing model, to get a more fair, prioritized ranking of risks. Those should likely include legal risk such as that imposed by exposure of a PII element, as well as technical risks and context swapping risks, i.e. transition from application to operating system or database context via the exploitation.
The legal risk is the best to visualize the current problem – Not all information is created equal. User enumeration, i.e. the ability to pinpoint information about users via meta-data, has been treated as a minor annoyance and ranking as a low risk.
Exposure of a single or few users personal data would rank as a partial confidentiality issue.
However, even a single to few records constitute a breach against the GDPR legislation, and hence the need to address even those minor issues is critical. The instrument of measure is hence too blunt to reflect the current situation and its challenges, and extra elements are needed in the matrix and prioritization. This project is a heavy study project and will result in a joint publication whitepaper. It is not suitable for more than one student.

Visualize and explain vulnerabilities in web applications

Research methods to in secure and preferable graphical ways visualize exploitation of vulnerabilities to explain clearly what vulnerabilities are and how the work.
The simplest case is about finding good forms of visualizations to standard vulnerabilities and creating examples.
However, as application security remain less understood, formalizing steps for recreation of vulnerabilities and visually demonstrate the same to developers carry a direct value in driving remediation.
Likely it is possible to use technology such as selenium or similar to record or describe recreation, and then record the application behavior.
By creating standard steps for reproduction of some standard vulnerabilities, the method could be applied to not only demo application, but to real world instances of demoable vulnerabilities.
Pushing it further, by automating the flow and recording the interaction, it would be possible to replay an attack and show the interactions, creating an applied, real life example from an audited system. This would hugely benefit all non-technical staff in understanding, and hence resolving, technical vulnerabilities.

How far the thesis can be driven depends on time available and if the theoretical work of creating educational models, or the practical implementation of a subset of models, is prioritized.

Trust visualization for web applications

Applications frequently include information cross domains. As an example, opening bth.se without even navigating brings 13 separate domains into the trust boundary of the website. That cross domain includes of content in essence means both a cross domain trust – someone else is publishing content within the context of the domain, but also a degree of data leak via referrals. Script-driven cross domain posts and actions further the exfiltration of data from the perceived scope of an application.
In cases, those domains in turn can further include active content within the current context.

The implications of such includes are however not clear from just observing traffic, loading an image from the context of an image object in a browser will have less implications, than including active content such as scripts or HTML. iframe inclusions on the other hand generally execute out of scope of the current running application, and while the content of the frame is out of the website owners' control, the data within the current application is not exposed directly.

Further, as many sites still do not apply the HSTS directive, includes even within the same domain can mean non-encrypted reads of data. In combinations with cookies missing the secure-only directive, this means a step from perceived encryption to an intercept able plaintext communication.

The project aims at;
Documenting the behavior of different browsers in different forms of cross domain inclusion scenarios
Documenting different form of cross domain leakage
Test and develop a method for extracting lists of potentially risky cross domain trusts
Extended – In the method, include a "risk ranking" mechanism
Extended – Further enhance method to allow for whitelisting of trusted domains to focus on all unmanaged trust associated risks in an application
Extended – Propose visualization of cross domain trusts and dependencies including observed "chains" of inclusions

Breaking fully patched systems – Privilege escalation in windows environments

A smaller research project aimed at looking at ways to escalate privileges by abuse of file, path, service, registry and other system permissions on windows, which can be actively abused by attackers to establish an increased control over attacked systems and obtain persistence.
This likely apart from the listed issues include auditing if MSI-packages are treated as privileged installers by default, if executables carrying names such as setup- or installer will automatically escalate privileges for the purpose of distributed installs and other ways of reaching a privileged state when executing under a user context.

There are many studies on the topic, and there are many tools, that is why it is important to ensure that such a project looks at this from a new perspective.
The interesting part is that it is hacking without exploitation of vulnerabilities, but with exploitation of insufficient hardening, meaning it is security applicable also to an impeccably hardened system.

Detection of change in web applications

Applications change on a daily basis, either through dynamic content served to an individual user, or through agile DevOps processes pushing incremental changes to the application each day. In the case of the British Airways hack, a previously unchanged JavaScript file was altered to include code that resulted in the stealing of customers credit card information unknown to the developers.

This project looks at ways to automatically detect different type of web application changes, ways to categories them and allocate a risk profile to these types of changes. Suitable for 1 dedicated student.

The Methods identified in this study would be used to further enhance automated change detection and notifications

Detecting sensitive data

There is a certain subset of information that can generally be classified as sensitive, that includes personal information, credit/payment cards or other economy related data. Knowledge of how and where sensitive data is stored can be vital in focusing efforts to protect systems.

The project is aiming both to identify types of information that organizations in general would view as sensitive as well as methods to automatically detect the presence of such data on a system.

The methods developed in this project could be used to augment vulnerability reports by flagging systems with sensitive information. This would be useful for organizations in prioritizing their efforts to reduce vulnerabilities in their networks.

Group assessment

You can very often find more than one vulnerability on a system, and often these vulnerabilities can be used to perform different types of attack. We believe that certain combinations of vulnerabilities should be considered much more dangerous than others.

The study is aimed at investigating combinations of vulnerabilities, and finding a reliable method allowing for automatic classification of a system based on its vulnerabilities. For example, a system with a remote access vulnerability and a privilege escalation vulnerability should be considered more dangerous than a system with two privilege escalations etc.

The method from this study could later be used to give a better per host classification which can assist system administrators at focusing the patching to the hosts which need it the most.

Network access mapping

Knowing how traffic can flow in a network can greatly assist in figuring out possible attack vectors and paths that malware can spread. When deploying Outpost24 security scanners in a customer's network it is common to deploy several ones on different parts of the network.

One method to determine how traffic can flow would be to start probing all ports on all hosts and see what happens. This is often not a good solution due to the traffic load etc. We would therefore like a method for doing this in a more elegant and less intense and heavy way.

The project is aimed at finding a method for figuring out how traffic can flow in a network in a way which will cause as little load to the network and the hosts as possible.

This method can later be used to find possible spreading patterns and also find places where stricter firewall policies can be used to prevent attacks.

System role identification

Automatically identifying the type of device a host on a network is can in many cases be quite difficult. When Outpost24 scanners are deployed on a network they gather a lot of data about the hosts. This data consists of information regarding the operating system, open ports and running services etc.

The project is aimed at performing a statistical analysis using this type of information in order to allow for an accurate way to determine the type of the host i.e. server, client etc. the focus will mostly be towards devices running *NIX operating systems since those are the ones that are hardest to determine.

The information from this study could later be used to profile hosts and determine possibly dangerous network configurations such as the presence of o server on the client network.

Docker container analysis

In essence – Docker allows fast provisioning of servers. Earlier research exists with regards to the amount of Heartbleed/Shellshock affected images getting pushed out and scanning the packets installed on images.

This project focus on expanding this by investigating and finding a method to check which of the installed packets that are actually used. If it is not it is possible to get results which could be considered false, positives since some vulnerability can only be used when the program is running.

This method can be used to figure out which programs can or are used and this will allow for a more accurate vulnerability analysis of the installed packages.